Module: 2

Data link layer & medium Access Sub layer

Error Detection and Error Correction

Error Detection

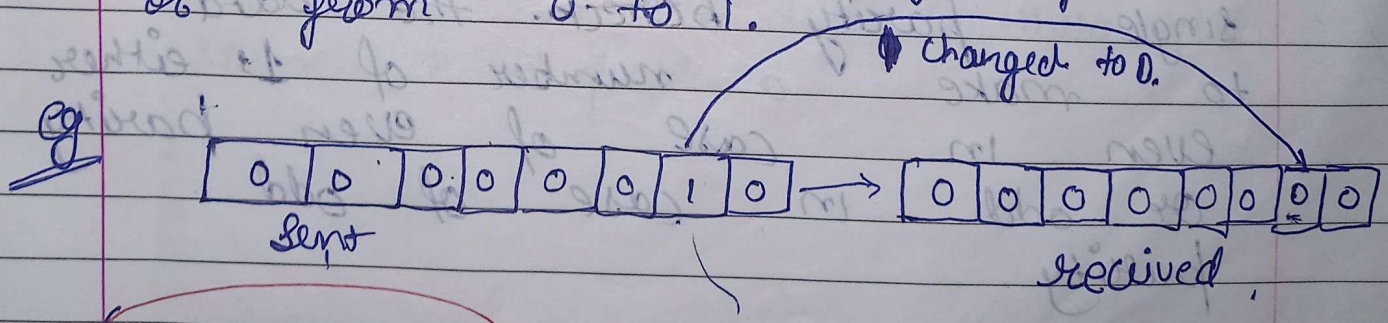
Data is transmitted from one device to another device the system does not guarantee whether the data received by the device is identical to the data transmitted by another device.

Types of errors

- Single Bit Error
- Burst Error

Single Bit Error :-

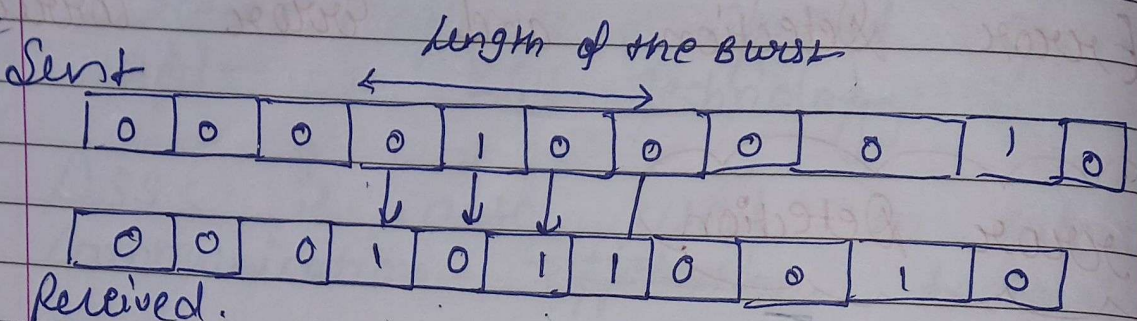
The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



Burst Error :-

Two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

eg



The most popular Error detecting Techniques are

- Single parity check
- Two dimensional parity check
- check sum
- cyclic redundancy check.

* Single parity check:

The single parity check is done by adding an extra single bit called single parity bit to the data to make a number of 1's either even in case of even parity or odd in case of odd parity.

1 is added to the block if it contains odd number of 1's and

• 0 is added if it contains even number of 1's.

in case of single parity bit we used. $m+1$ (m = number of bits)

It is lease expensive method.

no of 1 should be even in case of even parity

eg: 1 0 10

here number of 1s even

1 0 1 0 0

0 1 1 1 0

Here number of 1's oddd

1 1 1 0 1

Sent 1 1 1 0 1

Change → 0 1 0 1 detect there is some kind of error

2. Two dimensional parity check:-

Parity bits are calculated for each row which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.

eg → Step:-

- Arrange the data being sent a table

1	1	0	1	0	0	0	1
0	0	1	0	0	0	0	0
1	0	0	1	0	0	0	1

b. add the parity bits

1	1	0	1	0	0	0	1	0
0	0	1	0	0	0	0	0	1
1	0	0	1	0	0	0	1	0
0	1	0	1	1	1	0	0	1

Step: now the data will be transmitted.

(d) again at receivers end we need to calculate the parity bit and if it matches the data transfer is successful otherwise not.

1	1	0	0	1	0	0	1	0
0	0	1	0	0	0	0	0	1
0	0	1	1	1	1	0	0	0
1	0	0	1	0	0	0	1	1
0	1	0	0	0	1	0	0	0

Advantage:

It is more efficient than single dimensional parity technique

- It can detect multiple bit error.

3. **Checksum**:

In this each word is added to the previous word and total sum [checksum] is calculated. Then the checksum is transmitted along with the data.

eg Idea of checksum

Suppose send (7, 11, 12, 0, 6) these are number w1 to w5 be send.

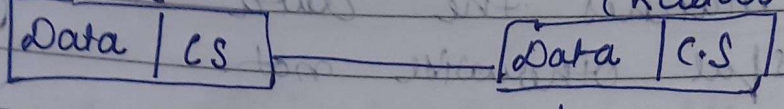
$w_1 + w_2 + w_3 + w_4 + w_5$

└ Checksum

$7 + 11 + 12 + 0 + 6$

$= 36$

Transmitter to sender



↓

Here we will calculate checksum again.

If CS = C.S.
↳ No Error.

Other example using one's complement

Checksum 36

100 100

10

0110 (6)

↳ Inverse

1001 (9)

Sender | 7, 11, 12, 0, 6 | 9 |

↳ Receiver

7 + 11 + 12 + 0 + 6 + 9

= 45

binary representation [10 11 01] 45

↳

10110

↳ + 10

1111

↳ Inverse 0000] There is no error

* Cyclic Redundancy Check

An error detection technique using a polynomial to generate a series of two-bit block check characters that represent the entire block of data. These block check characters are incorporated into the transmission frame and then checked at the receiving end.

CRC

How Check work:-

CRC is error detection code used for verifying the integrity of data. It works just like a checksum and is appended to the end of payload data and transmitted along with the data. The check value is called redundant because it doesn't add any additional information to the message.

CRC use generator polynomial which is available on the both sender & receiver side.

An example:

generator polynomial is of the form like $x^3 + x^2 + 1$

This generator polynomial represents key 1011.

n:- number of bits in data to be sent from sender side.

k: number of bits in key obtained from generator polynomial.

Sender side:-

(1) The binary data is first augmented by adding k-1 zeros in the end of data

(2) use modulo-2 binary division to divide binary data by the key and store remainder of division.

(3) Append the remainder at the end of the data to form the encoded data and send the same.

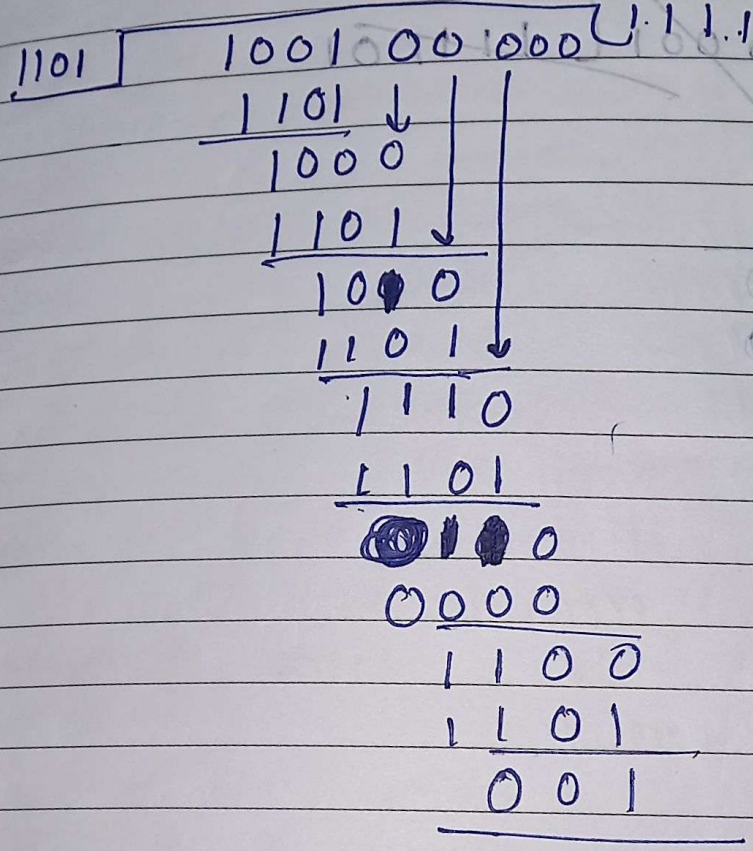
Receiver side (Check if there are errors introduced in transmission)

Perform modulo-2 division again and if the remainder is 0 then there are no errors.

Date: YOUVA

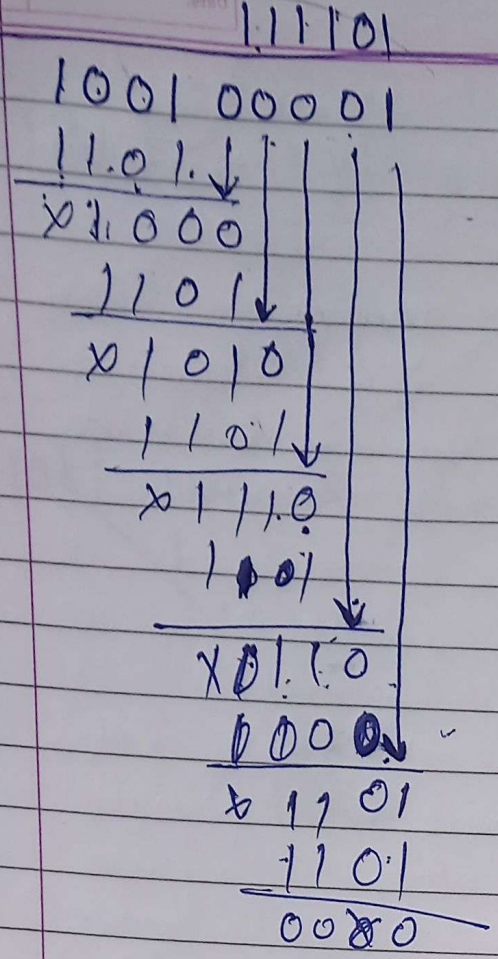
Data word to send 1001 0 0
key - 1101 [or generator polynomial x^3+x^2+1]

Sender side



Therefore the remainder is 001 hence the encoded data sent is 1001 00 001.

Receiver side:
Code word received at the receiver side 1001 0000 1



Therefore the remainder is all zeros Hence the data received has no error.

Error correction

Error correction codes are used to detect and correct the error when data is transmitted from the sender to the receiver.

Error correction can be handled in two ways.
fundamental.

- **Backward error correction:-**
  Once the error is discovered the receiver request the sender to retransmit the entire data unit

- **forward error correction:-**
  In this case the receiver use the error - correcting code which automatically correct the errors.

Hamming DISTANCE :-

Hamming distance is a metric for comparing two binary data strings while comparing two binary strings of equal length, Hamming distance is the number of bit positions in which the two bits are

different.

The Hamming distance b/w two strings a and b is denoted as d(a,b)

It is used for error detection or error correction when data is transmitted over computer network. It is also using in coding theory for comparing equal length data words.

Example :->

These are two strings
1. work → 2 Hamming distance.
2. walk

we have to calculate hamming distance these two string so hamming distance is number of mismatches occuring in two string at the same position

point
paint → 1 hamming distance

XOR Table

Input		Out
0	0	0
0	1	1
1	0	1
1	1	0

Step 1 : 0 1 0 1 1 0 0
Step 2 : 0 1 1 1 1 0 1 0 = 3
0 0 1 0 0 1 1 0

Step 1 : 1 1 0 1 0 1 0
Step 2 : 1 0 0 0 1 1 1 → 4

```
  0 1 0 1 1 1 0 0
x 0 1 1 1 1 0 1 0
-----------------
  0 1 0 0 0 1 1 0   → (3)
-----------------
```

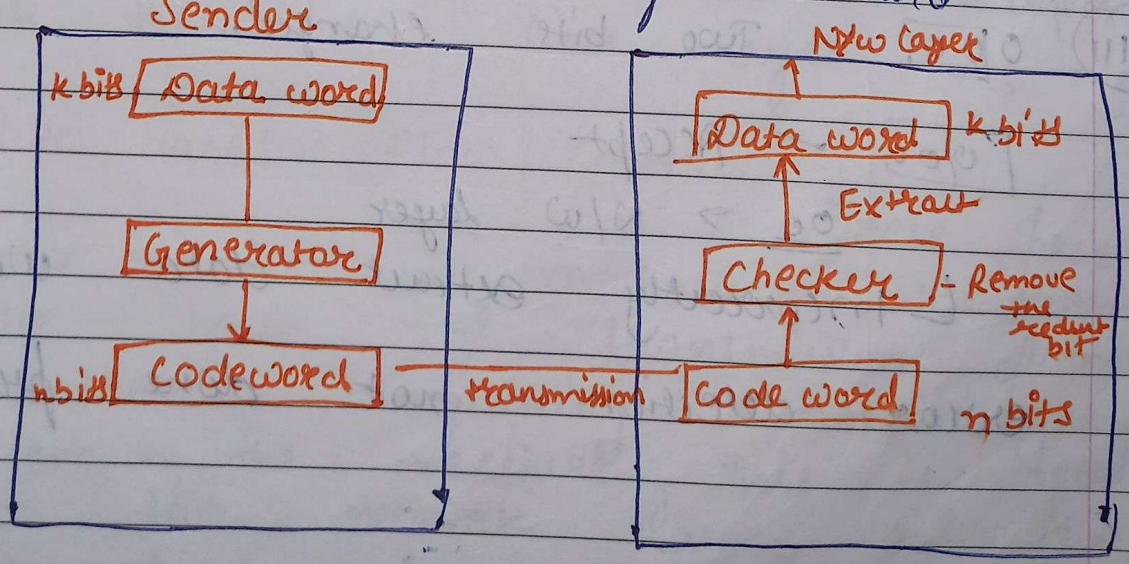
Application :-
Error detection is correction.

* Block Coding

Dividing a message into a block

- data words → each block carry k bit
  & redunt bit
- Codeword → n bits = k + r

Now we sender send the codeword. receiver receive the codeword its remove the redundent bit at last extract the data word actual message codeword



for eg How error is detect in block coding :

K = 2 ; n = 3

data word contains 2 bit — code word contains 3 bit

Data word	Code word
0 0	0 0 0
0 1	0 1 1
1 0	1 0 1
1 1	1 1 0

going to send Data word

0 1

↓

0 11 codeword.

during the transmission three case is occured

1. 0 1 → 0 1 → N/W There no problem here

(ii) 1 1 1 getting what happen there one bit has changed. → discarded

(iii) 0 0 0 Two bits changed.

0 0 0 — Accept

0 0 → N/W layer

└ Incorrectly extract data word

error detection not done properly

* Flow control Protocols :-

Flow control is a technique that allows two stations working at different speed to communicate with each other. It is a set of measures takes to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver. Flow control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver.

flow control classified into two categories

- **feedback based flow control :-** In these protocol the sender sends frames after it has received acknowledments from the user. This is used in the data link layer.

- **Rate based flow control :-** These protocol have built in mechanism to restrict the rate of transmission of data without requiring acknowledgment from the receiver. This is used in the network layer and the transport layer.

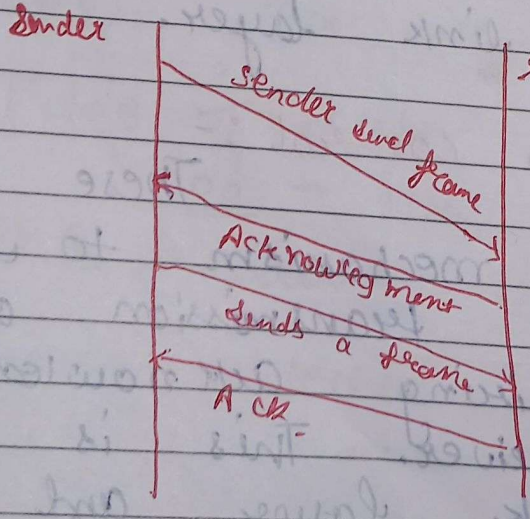
flow control techniques

- Stop-and-wait
- Sliding window

Stop and wait :-

The sender sends a frame and wait for acknowledgment

- Once the receiver receives the frame it sends an acknowledgment frame back to the sender.
- On receiving the acknowledgment frame the sender understand that the receiver is ready to accept the next frame. So it sender the next frame in queue.



M T W T F S S
Page No.:
Date:
YOUVA

Sliding window:-

This protocol improve the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledment.

The working principle of this protocol can be described as.

- Both the sender and the receiver has finite sized buffer called windows The sender and receiver agrees upon the number of frames to be sent based upon the number of frames to be sent based upon the buffer size.
- The sender sends multiple frames in a sequence withaut waiting for acknowledgment. when its sending window is filled. it waits for acknowlegment. when its sending window is filled it waits for acknowlegment on receiving acknowledg -ment it advances the window and transmit the next frames according to the number of acknowledgment received.

Error control PROTOCOL:

Error control in the link layer is the process of detecting and correcting data frames that have been corrupted or lost during transmission.

In case of lost or corrupted frames the receiver does not receive the correct data frame and sender is ignorant about the loss.
Data link layer follows a technique to detect transmit errors and take necessary action, which is retransmission of frames whenever error is detecting or frame is lost.
The process is called Automatic Repeat Request.

Phases in error control

- Detection of error:- Transmission error of any is detected by either the sender or the receiver.

- Acknowledgment:
  acknowledgment may be positive or negative

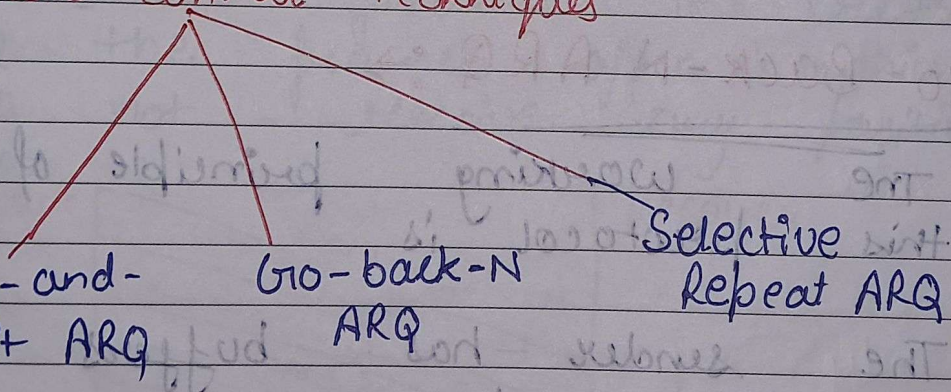
Positive Ack :→ On receiving a correct frame

Negative Ack :→ On receiving a damaged frame.

-Retransmission :→ The sender maintains a clock and sets a timeout period. If an acknowledgment of a data frame previously transmitted does not arrive before the timeout or if a negative acknowledgment is received the sender retransmits the frame.

There are Three main techniques for error control

-Error control techniques



STOP & WAIT ARQ :-

This protocol involves the following transitions

- A Timeout counter is maintained by the sender which is started when a frame is sent.
- If the sender receives acknowledgment of the sent frame within time the sender is confirmed about successful delivery of the frame. It then transmits the next frame in queue.
- If the sender does not receive the acknowledgment within time the sender assumes that either the frame or its acknowlegment is loss in transmit it then retransmit the frame.
- If the sender receives a negative acknowledgment the Sender retransmit the frame.

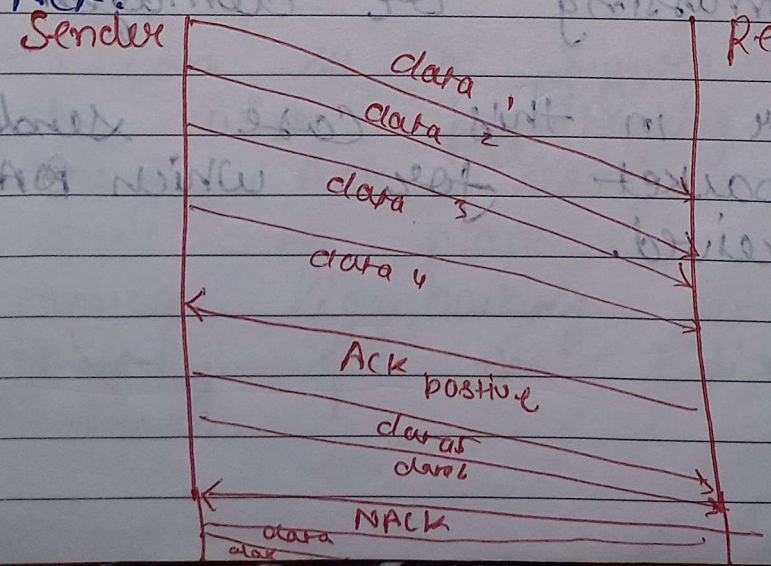
GO-BACK-N ARQ :→

The working principle of this protocol is

- The sender has buffers called sending window.
- The sender sends multiple frames based upon the sending window size

without receiving the acknowledgment of the previous ones.

- The receiver receives frames one by one & keeps track of incoming frame's sequence number and sends the corresponding acknowledgment frames.
- After the sender has sent all the frames in window it checks up to what sequence number it has received positive acknowledgment.
- If the sender has received positive acknowledgment for all the frames it sends next set of frames.
- If sender receives NACK or not receive any ACK for a particular frame it retransmits all the frames after which it does not receive any positive ACK.



Selective Repeat ARQ :-

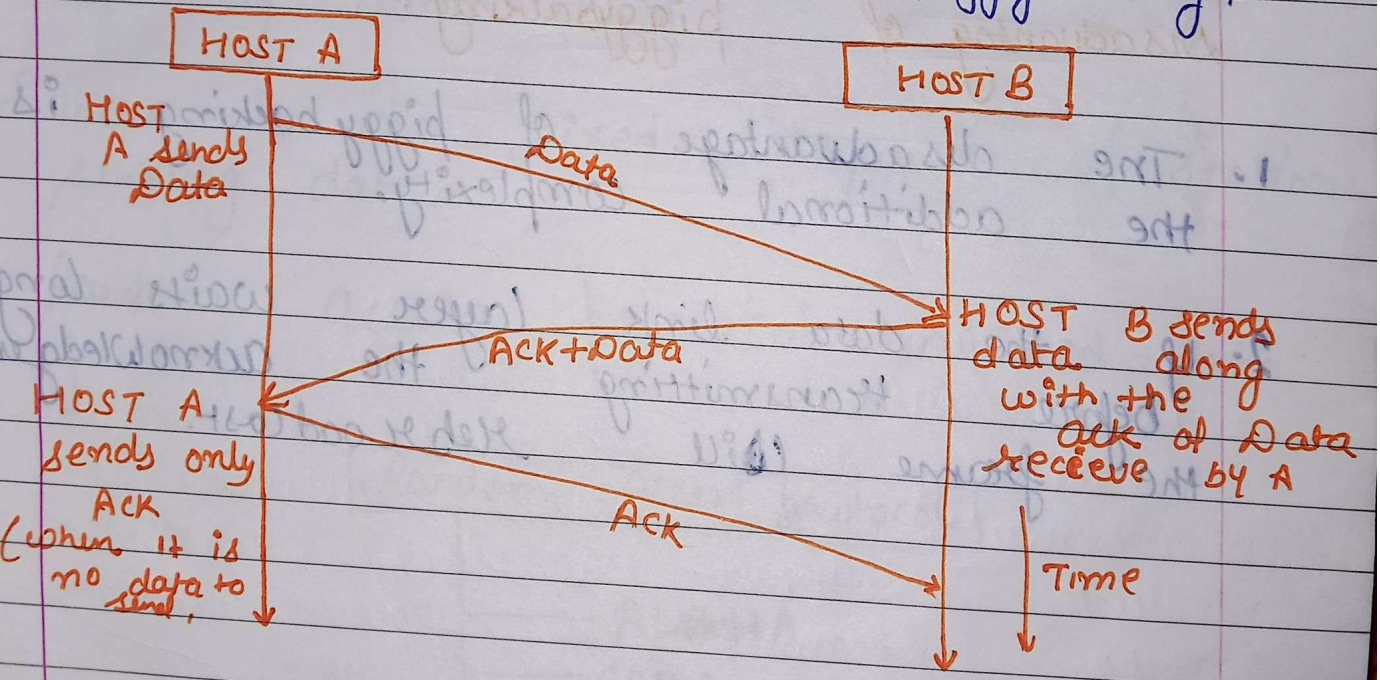
Both the sender and the receiver have buffers called sending window and receiving window respectively.

- The sender sends multiple frames based upon the sending - window size without receiving the acknowledgment of the previous ones.
- The receiver also receives multiple frames within the receiving window size.
- The receiver keeps track of incoming frame's sequence number buffers the frames in memory.
- It sends ACK for all successfully received frames and sends NACK for only frames which are missing or damaged.
- The sender in this case sends only packet for which ACK is received.

Piggybacking :-

A preferable solution would be to use each channel to transmit the frame both ways. ~~with both ways~~ with both channels having the same capacity.

This technique of temporarily delaying the acknowledgment so that it can be hooked with next outgoing data frame is known as piggybacking.



We can see in figure we can see with piggybacking a single message (ACK + DATA) over the wire in place of two separate message. Piggybacking improves the efficiency of the bidirectional protocols.

Advantage of piggybacking :-

- The major advantage of piggybacking is better use of available channel bandwidth. This happens because an acknowledgement frame needs not to be sent separately.
- usage cost reduction
- improves Latency of data transfer.

Disadvantag of piggybacking :-

1. The disadvantage of piggybacking is the additional complexity.
2. If the data link layer waits long before transmitting the acknowledgement the frame will retransmit.

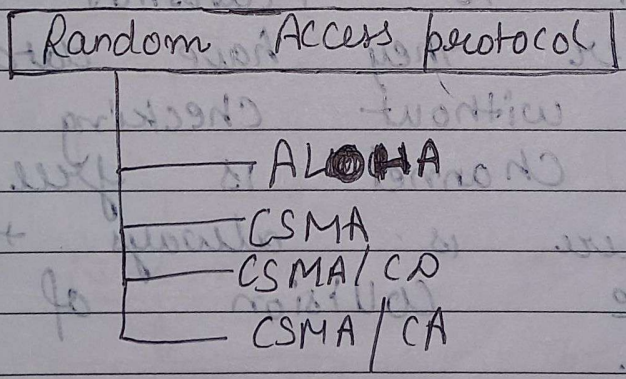
Random Access Protocol :-

In this all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state (idle or busy).

It has two features

1. There is no fixed time for sending data.
2. There is no fixed sequence of stations sending data.

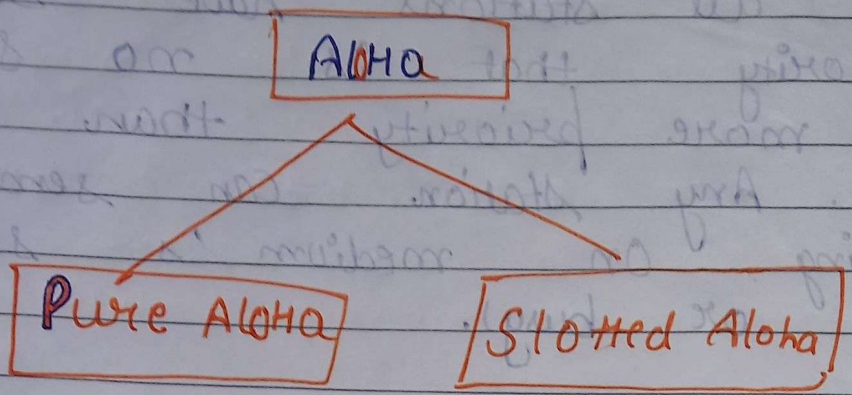
Random access protocol divided into further.



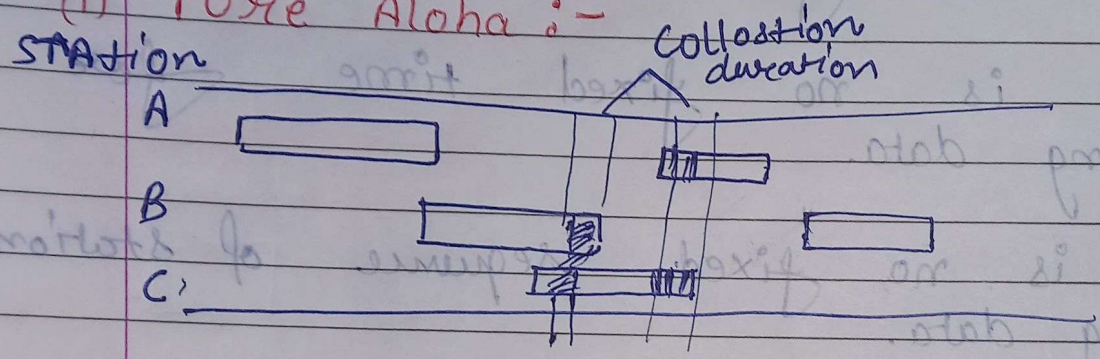
ALOHA :-

It was designed for wireless LAN but also applicable for shared medium.

- Here multiple stations can transmit data at the same time & can hence lead to collision



(1) Pure Aloha :-



Pure ALOHA

- Pure ALHO just allows every station to transmit the data whenever they have data to be sent without checking whether the channel is free or not. So there is always the possibility of the collision of data frames.

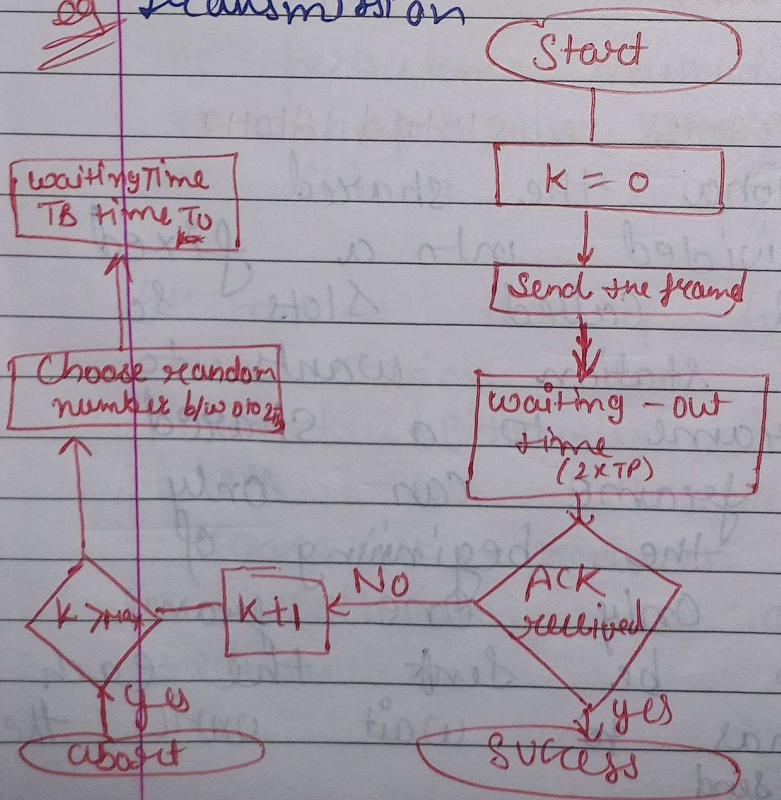
- In Pure Aloha after transmittion of the data frame station waits some time for the acknowlegement from the receiving station.

- when transmission station receives an acknowledgement from the receiving station it assumes that the transmission is successful.

- If transmitting station does not receive any acknowledgment within specified time $(2 \times TP)$ it assumes that the transmission is unsuccessful.

- In pure alho transmitting station uses a Backoff strategy & wait for some random amount of time

- After back off time transmitting station transmit the frame again & it keeps trying until the backoff limit is reached off which it abort the transmission

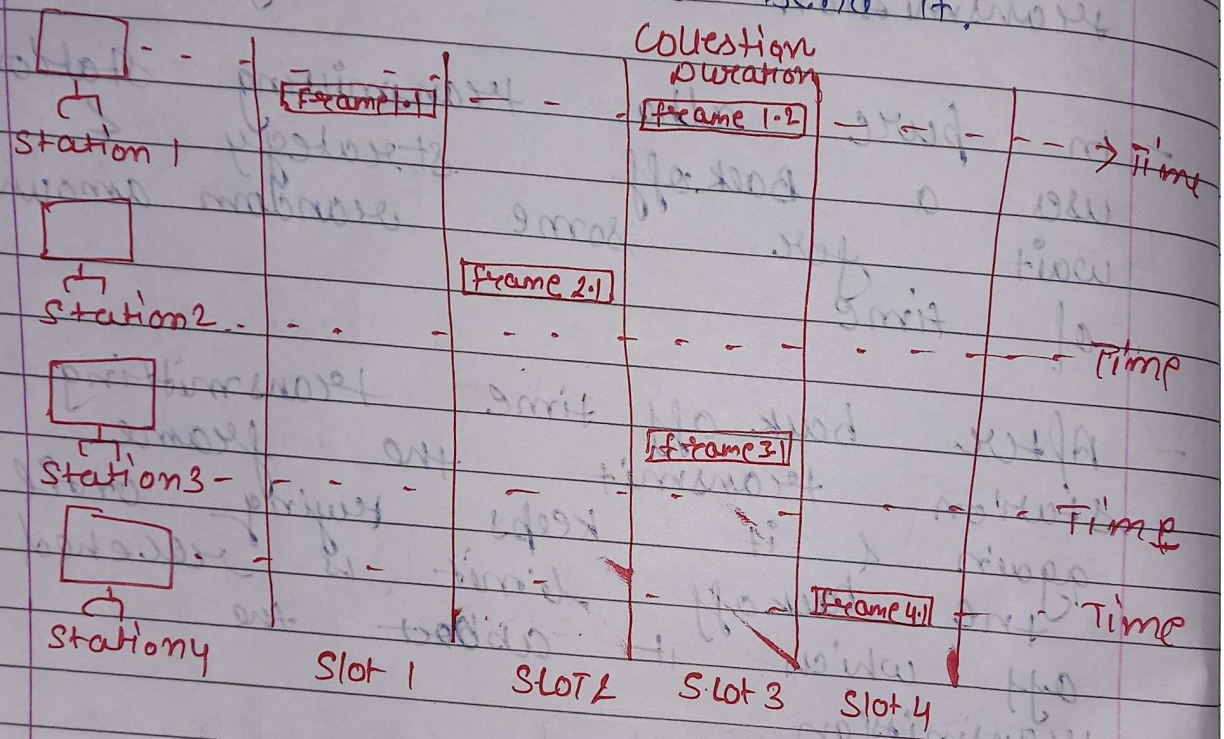


k = no of attempts

TP = Max propagation time

TB = Back off time

(ii) Sloted Alho :→ There is high possibility of ~~frame~~ frame hitting in pure alho so slotted alho is designed to overcome it. slotted alho does not allow the transmission of data whenever the station wants to send it.



frames in sloted Aloha

In Slotted Aloha the shared channel is divided into a fixed time interval called slots so that if a station wants to send a frame to a shared channel the frame can only be sent at the beginning of the slot and only one frame is allowed to be sent the each slot. [data it has to wait until the
↳ station is failed to send

next slot

However there is still possibility of a collision because suppose if two station try to send a frame at the beginning of time slot.

CSMA :-

(Carrier sense multiple Access)

This method was developed to decrease the chances of collisions when two or more station start sending their signals over the data link layer. Carrier sense multiple access requires that each station first check the state of the medium before sending.

The persistence methods can be applied to help the station take action when the channel is busy / idle.

1- means that if the channel is idle the station can send data to the channel. Otherwise it must wait until the channel become idle. Hence it reduces the chances of a collision on a transmission medium.

CSMA Access modes :-

1 Persistent :-

In the 1-Persistent mode of CSMA that defines each node first sense the shared channel and if the channel is idle it immediately sends the data. Else it must wait and keep track of status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

Non-persistent :-

It is the access mode of CSMA that defines each node transmitting the data. Before transmitting the data, it must sense the channel and if the channel is inactive it immediately sends the data. Otherwise the station must wait for a random time (not continously) & when the channel is found to be idle it transmit the frames.

P Persistent :-

It is the combination of 1-persistent and non persistent modes. The P-persistent mode defines that each node senses the channel and if the channel is inactive it send a frame with a P

probability. If the data is not transmitted it waits for random time and resumes the frame with the next time slot.

O Persistent :-

It is an o-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel if it is found that the channel is inactive each station waits for its turn to retransmit the data.

CSMA/CD :-

It is a carrier sense multiple access / collision detection network protocol to transmit data frame. The CSMA/CD protocol works with a medium access control layer. Therefore it first senses the shared channel before broadcasting the frame. & if the channel is idle it transmit a frame to check whether the transmission was successful or not. If the frame is successfully received the station sends another frame. If the collision is detected in the CSMA/CD the station sends a jam / stop signal to shared channel to shared channel to terminate data

transmission. After that it waits for a random time before sending a frame to a channel.

CSMA/CA :-

Carrier sense multiple access with collision avoidance. The process of collision detection involves sender receiving acknowledgement signals. If there is just one signal then the data is successfully sent but if there are two signals then it means a collision has occurred. To distinguish b/w these two cases collision must have a lot of impact on received signal. However it is not so in wired network so CSMA/CA is used in this case.

1. Interframe space:-

station waits for medium to become idle & if the medium found idle it does not immediately send data rather it waits for a period of time called interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.

2. Contention window:-
It is the amount of time divided into slots. If the sendere is ready to send data it choose a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process rather it restarts the timer when the channel is found idle again.

3. Acknowledgement:-
The sender re-transmit the data if acknowledgement is not recived before time-out.

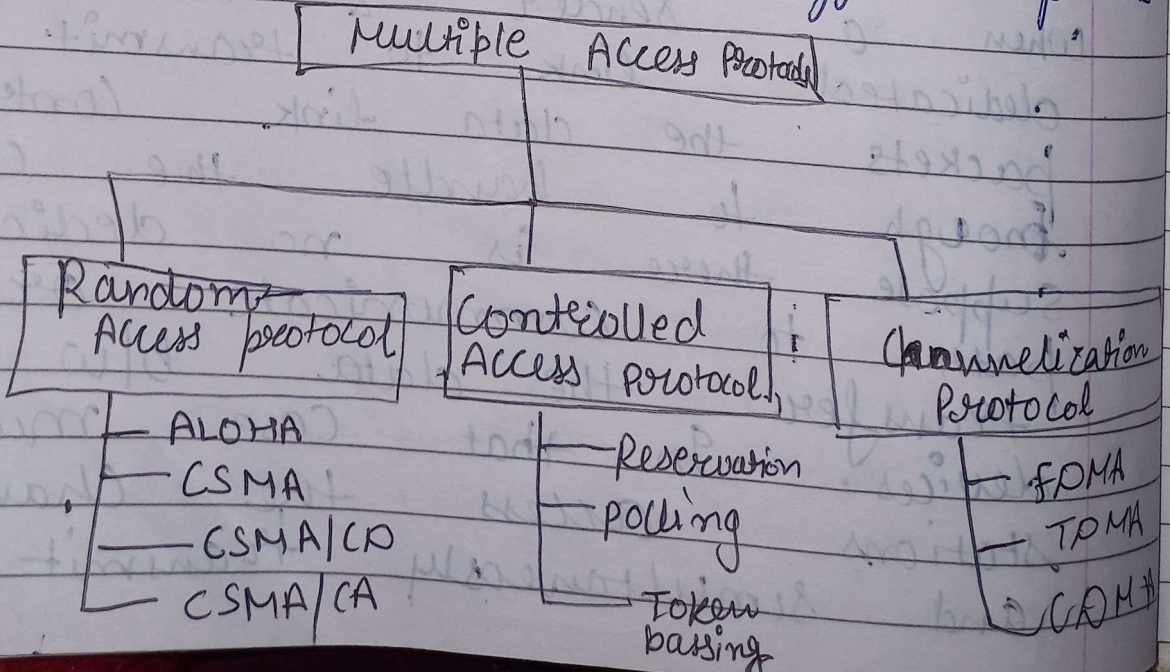
MULTIPLE ACCESS PROTOCOL

When a sender & receiver have a dedicated link to transmit data packets the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data b/w two devices. In that case multiple stations access the channel and simultaneously transmit the

data over the channel. It may create collision and cross talk. Hence the multiple access protocol is required to reduce the collision & avoid crosstalk b/w the channels.

for eg:-
Suppose that there is a classroom full of student when teacher ask a question all the student in the class start answering the question at the same time. All the student respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the student & make them one answer.

Multiple access protocol that is sub divided into the different process as.



Controlled Access Protocol :-

In controlled access the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time to avoid collision of message on shared medium. The Three controlled access method are.

1. Reservation
2. Polling
3. Token passing

Reservation :→

In the reservation method a station needs to make a reservation before sending data.

- The Time line has two kinds of periods

1. Reservation interval of fixed time length.
2. Data transmission period of variable frame.

Polling :-

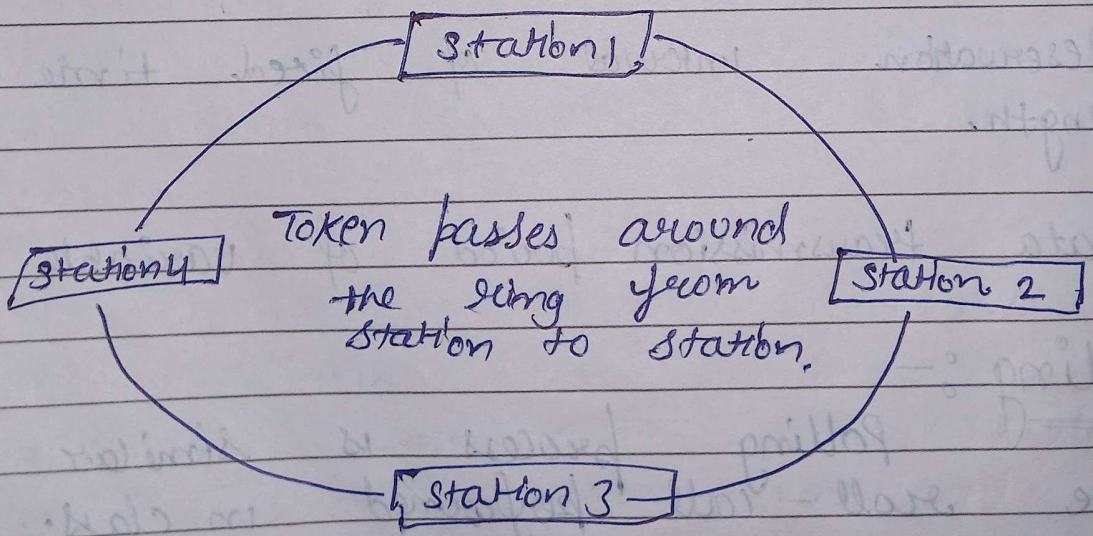
Polling process is similar to the roll-call performed in class. Just like the teacher a controller sends a message to each node in turn.

in this one acts as a primary station (controller) and the others are secondary stations. All data exchange must be made through the controller.

Token passing:

In token passing schema the stations are connected logically to each other in form of ring and access to stations is governed by tokens.

- A token is a special bit pattern or a small message which circulate from one station to the next in predefined order.
- In token ring, token is passed from one station to the another adjacent station in the ring. whereas incase of Token bus each station uses the bus to send the token to the next station in some predefined order.



3. **Channelization**:

In this the available bandwidth of the link is shared in time frequency and code to multiple stations to access channel simultaneously

FDMA (frequency Division multiple access)
The available bandwidth is divided into equal bands so that each station can be allocated its own band.

TDMA :-
In this the bandwidth is shared b/w multiple stations. To avoid collision time is divided into slots & station are allotted these slots to transmit data.

CDMA :-
Code division multiple Access : one channel carries all transmission simultaneously There is neither division of bandwidth nor division of time. For example If there are many people in a room all speaking at the same time then also perfect reception of data is possible if only two person speak the same language. Similarly data from different stations can be transmitted simultaneously in different code language.