Unit-5

06/01/22

CSMA :-

Carrier Sense multiple access

→ Carrier is that media through which data is transmitted from source to distination. It may be of guided type or unguided wire based or wireless.

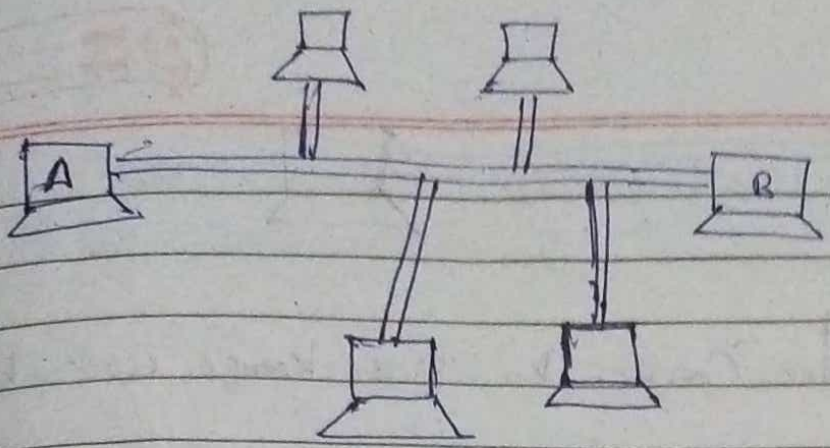
→ Sense :- Sensing the Carrier means, sender senses the Carrier in order to know that whether the Carrier is free or not. data from other station is belonging to carrier at that point of time. Carrier ko Sense karne ka matlab hai ki Carrier me koi aur Station ka data hai kya ; becoz it is multiple access (media is multipoint)

Multiple no. of Stations are accessing the Carrier simultaneously that's why there is a chance of collision. Since we have allowed multiple access that's why sensing is important.

Two categories : (i) CSMA/CD (with collision detection) → Corrective measure (after the collision)

(ii) CSMA/CA (with collision) → Preventive measure (before the collision)

It Stands for Carrier Sense multiple access : It is a multiple access method in which a sender first "Senses" a Carrier before Starting its transmission. Here the term Sense means to check the Carrier for the amount of traffic on it before Sending new packets. Such a Sensing is intended to reduce Collision.



Transmission start hone se pehle carrier ko sense karenge, aur traffic ki amount ko dekh lenge. Agar pehle se traffic nhi h to carrier free huga aur Collision ki probability reduce ho jyegi but cannot be eliminated.
machine A senses carrier and senses that no traffic is there, koi PKT agar kahi se chalta hai uska jo associated current or signal hai, uss signal ka koi propagation delay hota hai. Due to propagation delay 'A' is unable to sense ~~If A~~ traffic, but possible that there may be traffic.

→ It is said that CSMA can reduce the chances of collision but cannot be eliminated. This is due to propagation delay. Here propagation delay refers to the time needed to reach first bit sent by a sender to the receiver. For an instance a station can sense the carrier and can find it idle only because the first bit sent by another station has not yet been received.

Machines which are maximum distance apart, ~~data~~ time required to send data from one end to other end is called Vulnerable time.
Ek sender se dusre sender tak ~~of~~ data jane me jo time lagta hai usko propagation time bolte hai.
Extreme case me Prop. & Vulnerable time Equal ho jyega jab sender & receiver maximum distance apart honge.

10110011 01

* CSMA/CD

Jab koi station Carrier ko sunta karega, uss can have 3 cases :-

(i) Jab koi v signal nhi milega, i.e. Carrier is idle. No data present over there. (ii) If it senses Carrier, Sender will get its own data.

(iii) When Sender Sees Carrier it gets two signal, one its own & one of other station's data or signal or frequency.

20/01/22

* CSMA/CD (Collision Detection)

It stands for Carrier Sense multiple access with Collision detection. It uses the approach of Carrier Sensing through which a transmitting station attempts to detect the station by sensing transmission from other station while it is transmiting the frame. The idea is when there is no collision the station receive its own signal by Carrier Sensing, when there is collision the station receive two signal, its own signal & the signal sent by another station.

When the collision condition is detected the station stops the frame being transmitted, transmits a JAM signal and then wait for a random amount of time, before trying to retend the frame.

In summary we can say that CSMA/CD improves the performance of CSMA by terminating transmission as soon as collision detected.

In CSMA/CD the following steps are carried to perform transmission :-

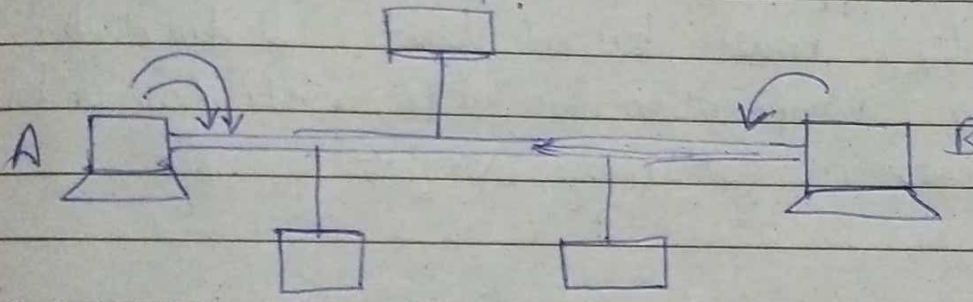
Step 1 : See whether a frame is ready for transmission or not, if not then wait.

Step 2 : Is media/channel free? If not then wait

Step 3 : Start transmission and monitor for collision during that.

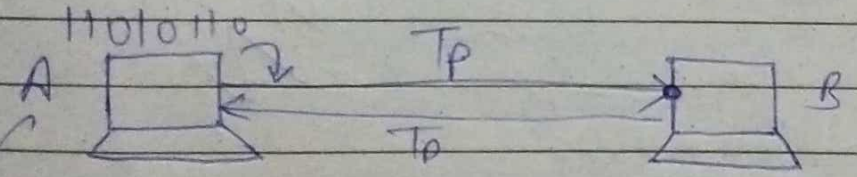
Step 4 : Data collision occur? If yes then perform "collision detection procedure".

Step 5 : Reset transmission counter and complete the transmission.



T_p = propagation time

T_{frame} = Time Completion of one frame



~~$T_{frame} = 2T_p$~~ $T_{frame} >= 2T_p$

for first bit, Time required T_p, worst case scenario is when collision happens near to B, due to collision signals ne jo intermingling hui hai current ka value jo disturb hua hai, to collision ka return hone me bhi T_p time lagega.

Time to send one frame, ~~T_{frame}~~.

So Total time is $2T_p$

So we have to Ensure that

$T_{frame} >= 2T_p$

So Conceptual question is why T_{frame} is greater than or equal to $2T_p$

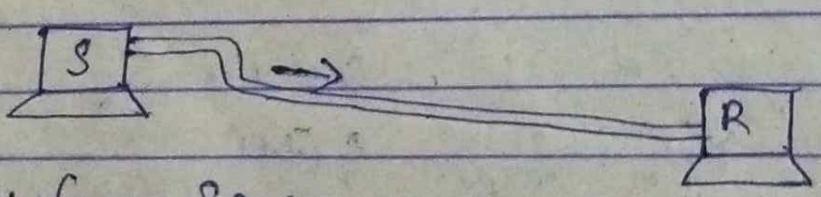
Working method of CSMA/CD

for CSMA/CD to work we must have a restriction on the frame size. This is because, in practical implementation before sending the last bit of the frame, the sending station must detect a collision. if collision is detected, transmission should be aborted.

For this approach to work the frame transmission time (T_{fr}) must be at least 2 times the maximum propagation time (T_p). We can understand the reason in the following way.

Let us think about worst case scenario where two stations involved in collision are maximum distance apart. Here the signal from the 1st takes T_p time to reach the 2nd. After collision, the effect of collision again takes T_p time to reach the 1st. Hence, it is necessary that the 1st station should still be transmitting after $2T_p$ so that it can abort the transmission.

Collision Avoidance (CSMA/CA)



(1) Interframe Space → Random time

(2) Contention window ÷ time slot

T, 2T, 4T

(3) Acknowledgement:

CSMA/CA,

Since Collisions cannot be detected anywhere (such as in wireless network) there must be some approach to avoid the collisions. for this CSMA/CA is used. Three approaches used for Collision Avoidance in CSMA/CA are :-

(i) Interframe Space
(ii) Contention window
(iii) Acknowledgment

(a) Interframe Space :- In simplest approach collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station will not send the data immediately but it waits for a period of time known as IFS (interframe space).
This is due to the reason that, even though the channel is idle when it is sensed, a distant station may have already started transmitting, however the signal from there has not yet reached the sensing station. Then the IFS time allows the signal from distant station to reach the sensing station.

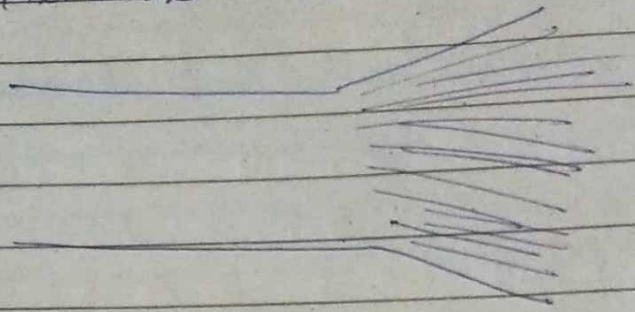
(b) Contention Window : Essentially, contention window is amount of time divided into slots. A station that is ready to send, chooses the random no of slots as its wait time. The no. of slots in the window changes according to a binary exponential back-off strategy. It means that it is set to

1 slot the first time and then double each time the station cannot detect an idle channel after IFS.

(c) Acknowledgment :- with all this precautions, collision can still occur. Hence, the acknowledgment can simply guarantee that receiver has received the frame.

* CDMA (Code Division Multiple Access)

Channelization & framing Concept:
↳ another name "Channel" often called medium.



Channelizing the flow of data means, Path has been decided and according to that path data flow in that direction. Bandwidth is divided into different parts. Entire bandwidth ko multiple parts me divide kar diyiye.
Bandwidth is Channelized we get benifit in bit rate.

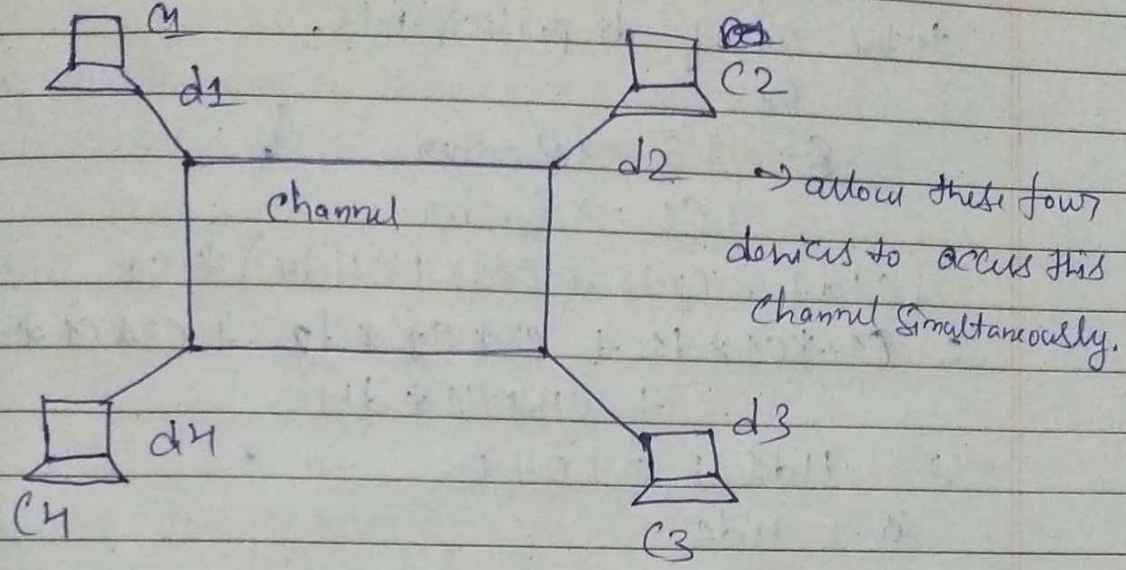
Baseband transmission (Low pass channel) → overall speed is gained.
Broad band transmission (high pass channel) → multiple user gain speed.

Channelization may be based on → frequency
→ amplitude
→ wavelength
→ Code.

CDMA → Multiple access means allowing multiple devices to access the bandwidth. Simultaneously. Second thing, if dividing multiple devices in bandwidth means Entire bandwidth is shared among them.

Code ke basis Par kaise Share hogi

Sinral devices are allowed to accus bandwidth simultaneously and their data will utilize bandwidth on the basis of Pre-established Code. Working logic is based on code so called CDMA.



→ allow these four devices to accus this channel simultaneously.

All devices which are accessing Entire channel simultaneously they are assigned pre-defined code. Code has two basic Properties :-

(i) When same codes are multiplied together then no. of participants will be produced.

$$C1 * C1 = 4$$
$$C2 * C2 = 4$$

(ii) When different codes are multiplied '0' will be produced. Eg: $C2 * C3 = 0$, $C4 * C3 = 0$, $C1 * C4 = 0$

To form packet of data of a device we have rule

→ Packet will be formed by multiplication of code and the data of at a particular station.

→ Because multiple access is allowed, all the devices are allowed to send the data simultaneously, that's why at a particular processing cycle the data which is existing onto the channel will be

$$C1d1 + C2d2 + C3d3 + C4d4.$$

How data will be received?

When any machine will try to attempt then
→ machine will multiply (which wants to receive data) the data with Code of the Sender.
→ The result after multiplication will be divided by total no. of participants.

Ex:

C3 → Receiver

C1 → Sender

$(C1d1 + C2d2 + C3d3 + C4d4) * C1$

$= C1*C1*d1 + C2*C2*d2 + C3*C1*d3 + C4*C1*d4$

$= 4d1 + 0 + 0 + 0$

$= 4d1$

$\frac{4d1}{4} = d1$

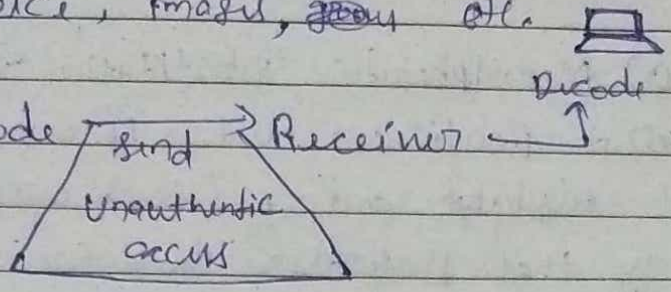
* Introduction to Network Security,

Security means we prohibit Unauthentic access.
Security in network ÷ When data is transmitted by Sender and in between Path if we are prohibiding Unauthentic access then we say that are implimenting network Security.

With respect to networks Security refers to implementation of those techniques which can Ensure that no one apart from intended Sender and receiver Conclude the message (meaning which is being transmitted; No third Party can conclude the meaning of message.

It means we are implementing a mechanism, data is changed to particular code and then transmit. If anyone get the signal of the code, then Coded signal will get and needs decoding logic.

Most of the messages transmitted are in the form of text. other includes, voice, images, etc.



Coding → Encryption of data } Collectively known
Decoding → Decryption of data } as Cryptography.

* Stignography ÷ Texts are hiding using the image, (Graphical Processing involved). Coded form is in the graphic.
* Cryptography ÷ text to text coding is known as Cryptography.

27/01/22

* Plaintext ÷ That particular message which is to be sent. It can't be transmitted as it is because it is understandable. Before transmission, it should transform into such a form that no one will be able to know the meaning of it. Only receiver knows how to decrypt it.

Cipher text ÷ It is the coded form of plain text. Before transmission, plain text should be transformed to coded form.

To Create Cipher text we have two broad categories :-

(1) Substitution Cipher :- This approach says if each alphabet in the plain text is substituted by another character from character set then that substituted text is known as substituted cipher.

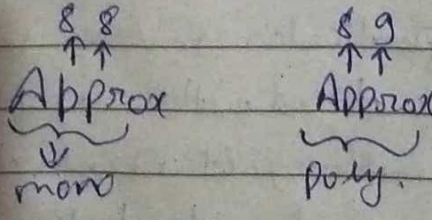
(a) Monoalphabitic Substitution :- Mono means single for a particular letter if we substitute a different alphabet and for each occurrence of that alphabet only that particular character which is selected earlier ~~is~~ ~~occurrence~~ of always. Then it is monolithic

(b) Polyalphabetic :- If we are substituting different alphabets for a particular letter in a plain text, then it is polyalphabetic.

Q) Why polyalphabetic Ciphers are more secure than monoalphabetic ?

Ans :- In polyalphabetic multiple types of substitution, so they are harder to decode as compared to monoalphabetic ciphers.

Ex:



(2) Transposition Cipher :- Position of the alphabets are transformed i.e. their relative positions are transformed in order to form the cipher.