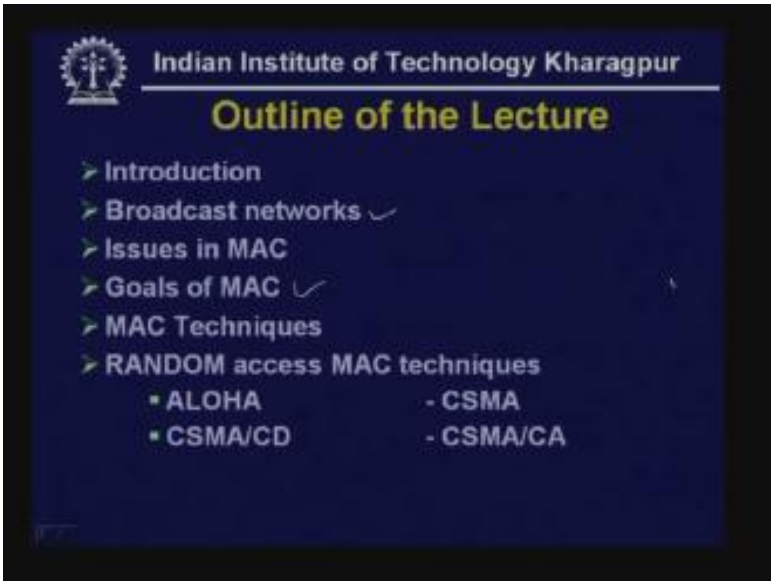
Data Communications
Prof. Ajit Pal
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
Lecture # 25
Medium Access Control - I

Hello and welcome to today's lecture on Medium Access Control. This is the first lecture on Medium Access Control. We shall cover this topic with two or three lectures. So far we have discussed about the areas switch communication network where communications were mainly done by using multiplexing, by using switching through the transmission media. But here you will see that the communication will be done using a broadcast media which will require some MAC technique. Let us have a look at the outline of today's lecture.

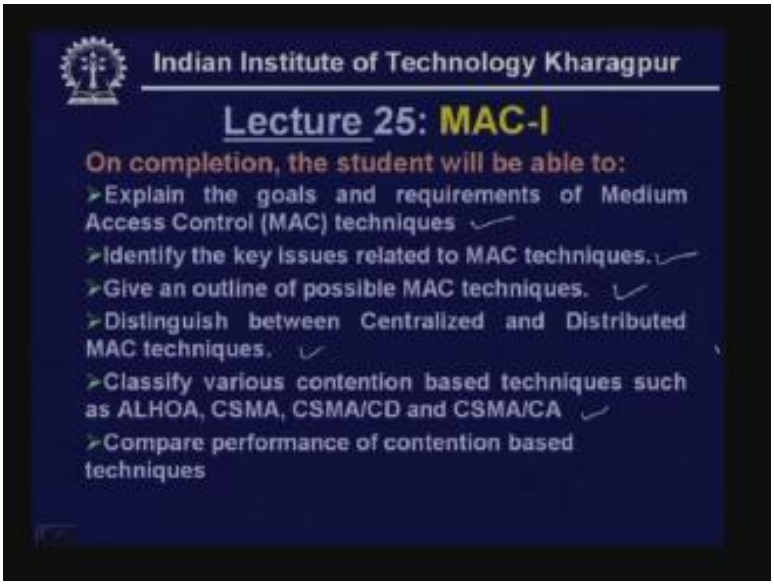
(Refer Slide Time: 02:12)



First I shall introduce to you the need for MAC technique and explain to you the various broadcast networks in which MAC technique is relevant. Then we shall discuss various issues in MAC techniques and consider various goals of Medium Access Controls. Then I shall give an overview of various MAC techniques.

However, in this lecture we shall discuss only RANDOM access MAC techniques such as ALOHA, CSMA/CD and CA. This one we shall cover in the next lecture.

(Refer Slide Time: 03:00)

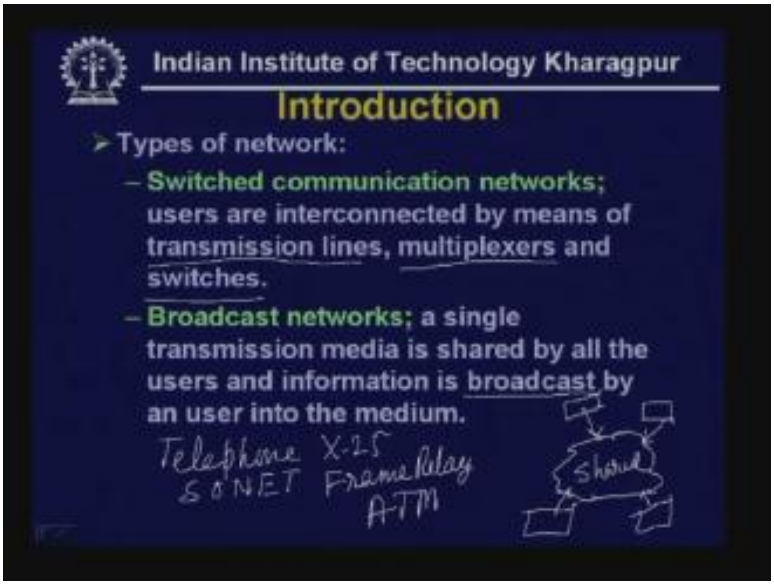


And on completion the student will be able to explain the goals and requirements of MAC techniques, they will be able to identify key issues related to MAC techniques and they will be able to give an outline of possible MAC techniques. Then they will be able to distinguish between centralized and distributed MAC techniques and classify various contention based techniques such as ALOHA, CSMA, CSMA/CD and CSMA/CA. and finally they will be able to compare performance of contention based techniques.

As I mentioned the networks can be broadly divided into two types. One is switched communication network where **pier to pier** communication is performed with the help of transmission lines, multiplexers and switches. We have already discussed about switched communication network where you have seen how the multiplexing and circuit switching techniques are used in networks such as telephone network, SONET network then we have also discussed various packets switched networks such as X.25 then you have frame relay and ATM. These are essentially switched communication network either packet switching or circuit switching is used where techniques like multiplexing and switching are used.

Now let us consider a different kind of scenario in which we have a medium which is shared by a number of users, say this is the shared medium and here this is user one (Refer Slide Time: 4:40), this is user two, this is user three, this is user four and so on. A particular user will broadcast the data into the network. So any user will broadcast data into the network. Now whenever it is broadcasted obviously there is a possibility that several users will try to broadcast simultaneously, that is one problem. The second problem is whenever a particular network is broadcasting, particular user is broadcasting it has to go to proper destination so this is some kind of shared medium where essentially broadcasting is being done.

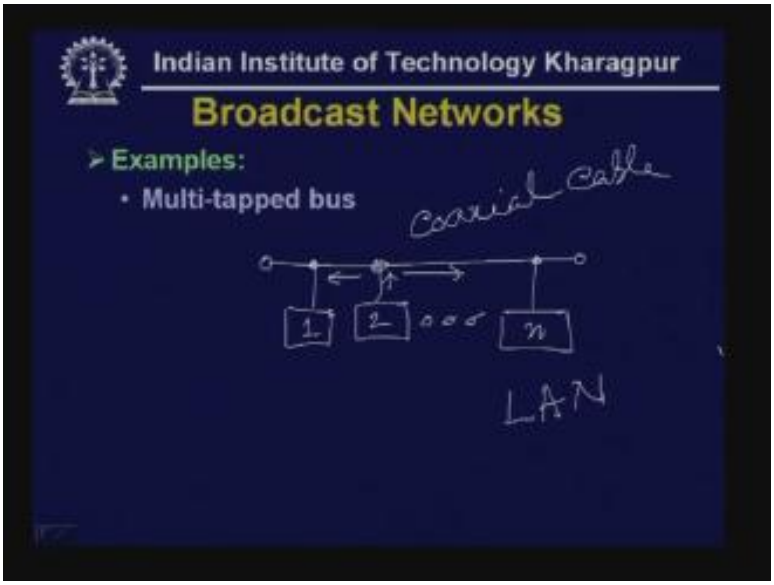
(Refer Slide Time: 05:33)



Let us have a look at some of the examples. One important example is multi-tapped bus. Say you have got a bus realized may be by using a coaxial cable and you can have taps to which different users can be connected, you can make several taps and then n users can be connected like user 1, user 2 and user n. So in this way n users can be connected to a common medium that is coaxial cable.

Now if A launches some data on the medium it will proceed in both directions and it will reach 1 and n and all the other stations connected to the medium. That means here a particular user is broadcasting and it is being received by all other users which are connected to the medium. So this is the multi-tap bus and you will see that this type of multi-tap bus is used in Local Area Networks LAN and WAN.

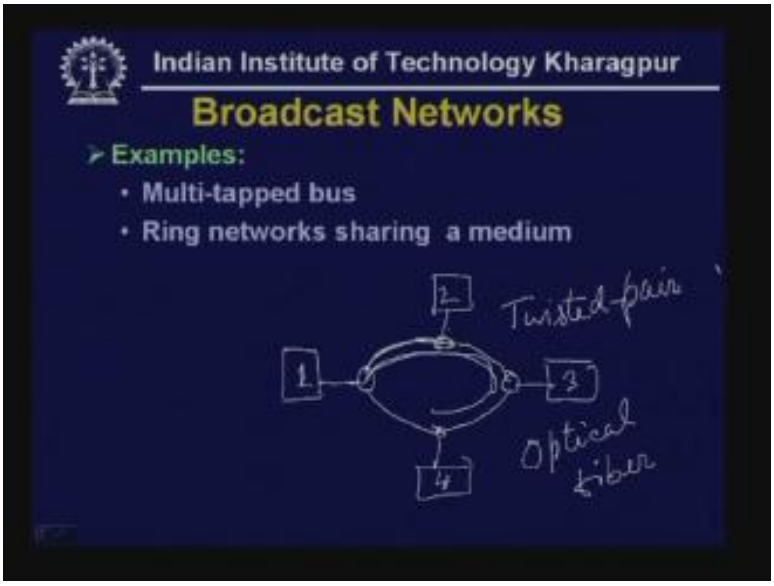
(Refer Slide Time: 06:51)



Let us consider another example that is ring networks sharing a medium. You have got a number of users say user 1 2 3 4 and here by the term users we mean they are essentially the computers. They are connected with the help of point-to-point link and you see they form a ring. So this particular user 2 is connected to its neighbors 1 and 3, 3 is connected to 2 and 4 and 1 is connected to 2 and 4 so in this way they are connected and this particular medium may be realized by using twisted-pair or it may be realized by using optical fiber which is possible in this type of point-to-point communication. In both cases you will see that this medium is being shared by all the users.

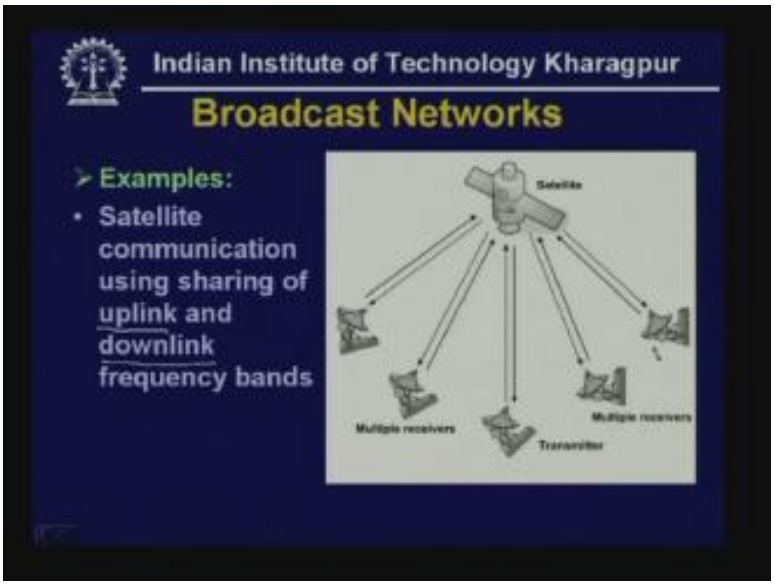
For example, whenever user 1 or station 1 wants to send to 3 it has to go through this part of the medium. Whenever it sends to 4 it will go in this manner. So this part of the medium is being shared by all the users for data communication. So this is ring networks using a shared medium. This is another example of broadcast networks.

(Refer Slide Time: 08:24)



Third example is satellite communication. Here we see that sharing is being done by using uplink and downlink frequency bands. For example, as you can see each ground station is communicating with the help of a transponder and there are two frequencies one is uplink frequency another is downlink frequency. You can see the uplink frequency is being shared by all the users for communication with the satellite (Refer Slide Time: 8:56). On the other hand the downlink frequency is broadcast it is going to all the ground stations. So, if this particular ground station wants to broadcast it will send it using uplink frequency then the satellite will receive it and retransmit or broadcast to all the other ground stations.

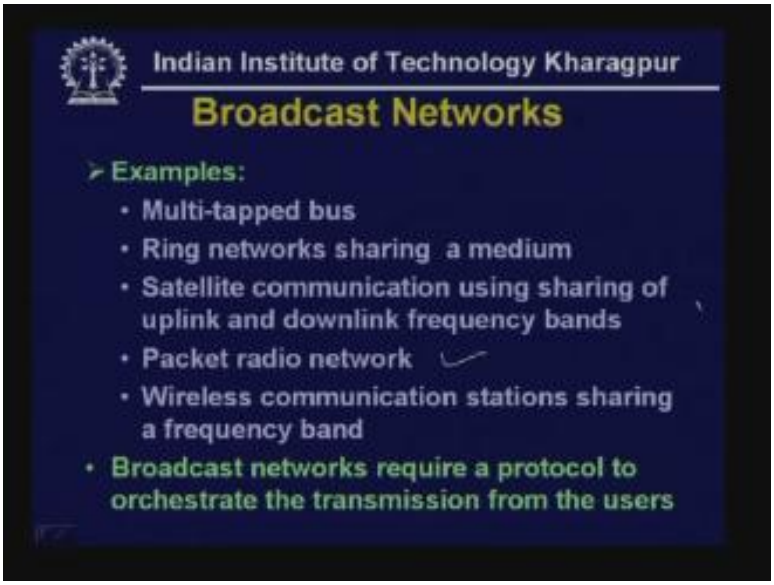
(Refer Slide Time: 09:16)



This is the example of satellite communication where the uplink frequency is being shared by a number of ground stations. Of course the downlink frequency is broadcasted so it is being received by everybody. But the uplink frequency is shared by all by using some mechanism. So this is another example of broadcast networks.

Then apart from satellite, multi-tap bars and ring networks there is packet radio networks as we shall see. There are also we use broadcast networks and wireless communication stations sharing a frequency band. We shall see that in wireless communication such as cellular network or packet radio and all such cases some frequency bands are shared. These are all examples of broadcast networks.

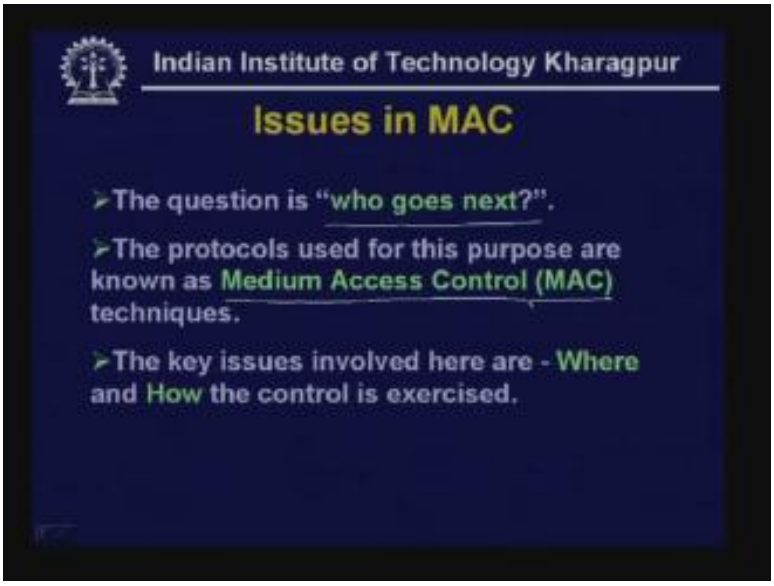
(Refer Slide Time: 10:15)



Now question arises how different users will send through the shared media. It is necessary to have a protocol or technique to orchestrate the transmission from the users. That means at a time only one user can send through the media and that has to be decided with the help of this Medium Access Control (MAC) technique. So the communication has to be orchestrated using some protocol or technique and that is essentially MAC technique.

So question arises, who goes next? This is the question to be answered. We have seen there are a number of users of stations who are trying for communication, who are trying to get hold of the medium for transmission, who will go next, and that will be decided by the Medium Access Control (MAC) techniques. So the protocol used for this purpose is known as Medium Access Control (MAC) techniques.

(Refer Slide Time: 11:25)



The key issues in MAC techniques are where and how, these are the two basic questions which are to be answered whenever we consider MAC techniques. Let us see what these two means.

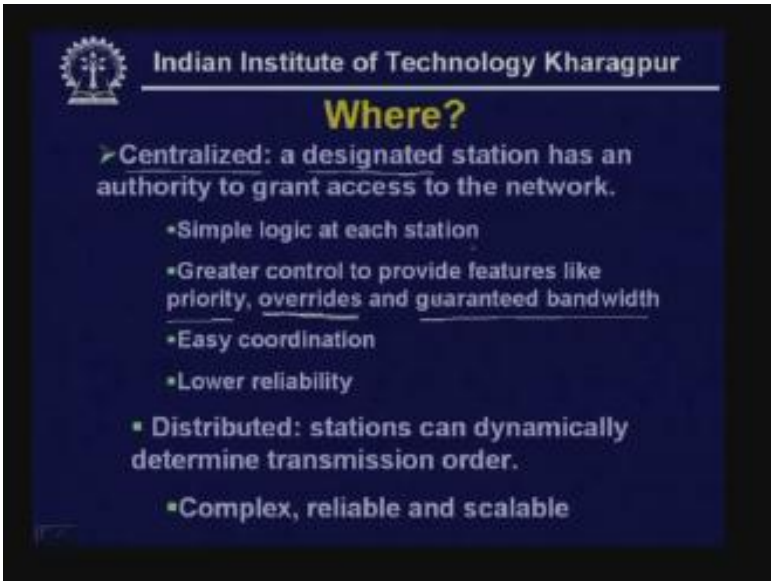
By a fair mean who does the control, whether it is performed in a centralized manner or it is done in a distributed manner. Let us see the case of centralized one.

In the centralized one a designated station has an authority to grant access to the network. That means a designated station will grant access to the network to the remaining stations. So it is somewhat like there is a meeting going on and there is a chairman and chairman can permit any other person who is in the meeting to speak so it is somewhat like that.

This centralized scheme has a number of advantages because the stations will have very simple logic because the Medium Access Control is being performed by a centralized station but the other stations will have very simple logic so when they will be permitted they will simply transmit the data. So they will know Medium Access Control logic necessary in each station, only the central station will have the logic. So the hardware or the software whatever is used that will be minimum in case of this scheme in all other stations except the central control.

It has another advantage; it is capable of greater control provided features like priority, overrides and guaranteed bandwidth. By priority we mean, there may be a number of users and some of them may have some important data to send so the central controller can give priority to a group of users compared to others. So whenever a high priority user tries to send data a low priority data transmission can be stopped. So it can be overridden with the help of this centralized controller and it can also guarantee the bandwidth that can be allowed to its user.

(Refer Slide Time: 13:50)



So these are the controls which can be very easily performed with the help of this centralized controller and it can do a very easy coordination.

However, it suffers from lower reliability because if the central controller fails then there will be nobody to control so the reliability is poor here if it is dependent on the failure of the central controller. So if the central controller fails the Medium Access Control cannot be performed by other users. This is the limitation of the centralized controller and that's why distributed control is preferred in many situations. In distributed control stations can dynamically determine the transmission order. Here each and every station take part in the Medium Access Control operation so it is done in a mutually agreed upon rule or protocol, that's why the distributed control performs it in a dynamic manner where each and every station takes part. Obviously it is much more complex, however it is much more reliable so it can tolerate some failure. If some of the stations fail it does not matter but it will continue.

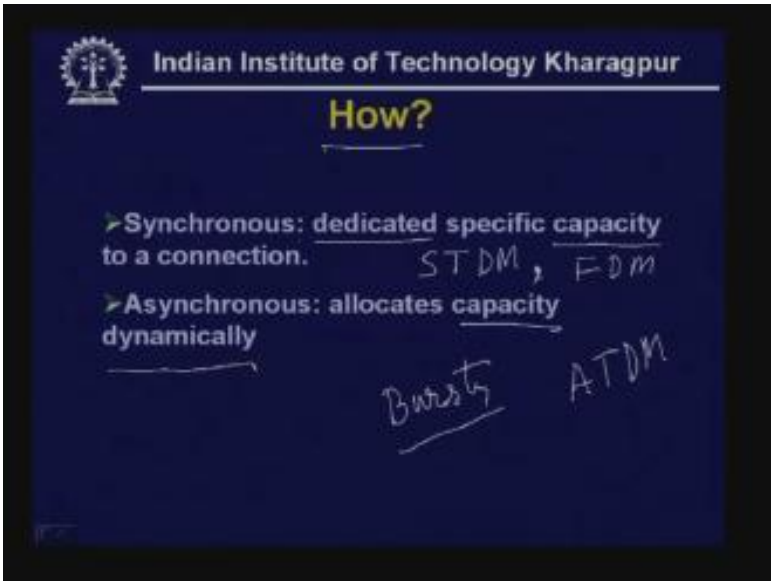
It is also scalable. By scalable we mean it is easier to have, whenever a station joins the network or a particular station is switched off all these things can be taken care of in a distributed MAC technique in easy manner and it is very scalable. You can keep on increasing the number of stations very easily in a distributed environment. These are the two questions to be answered.

The second question is how? Where and how?

It can be performed in a synchronous manner or it can be performed in asynchronous manner. We have already discussed about that Synchronous Time Division Multiplexing STDM where we have seen that specific capacity is dedicated. We have seen that each slot is allocated to a particular user or station and as a result the bandwidth or capacity is dedicated in Synchronous Time Division Multiplexing, it can be also done by using Frequency Division Multiplexing, here these are all synchronous stations.

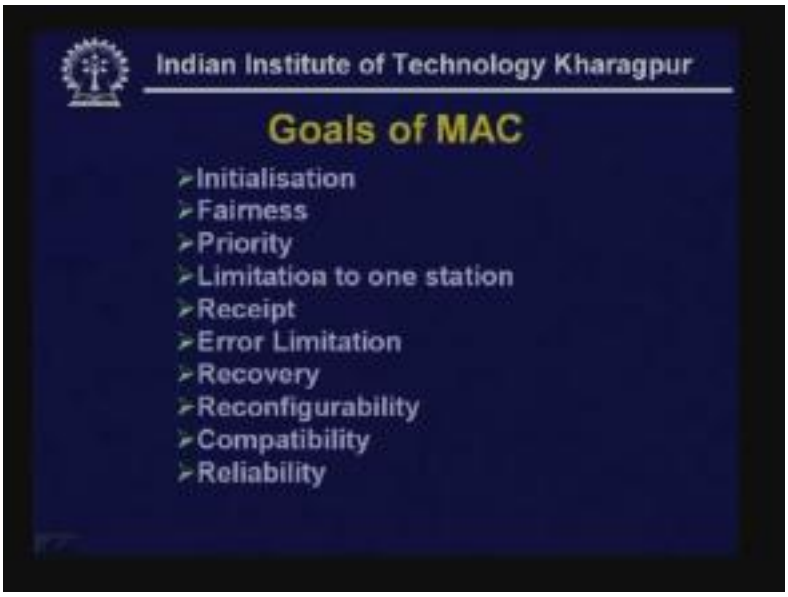
On the other hand in asynchronous technique the capacity is allocated dynamically. This asynchronous technique is very important for data communication. The reason for that is you know that the data is bursty in nature. So whenever the data is bursty in nature there is no point in providing dedicated capacity. Because if dedicated capacity is allocated it will not be utilized that's why in bursty environment it is necessary to use asynchronous technique such as Asynchronous Time Division Multiplexing ATDM where the capacity can be allocated dynamically. And how means it is in an asynchronous manner. That's why most of the MAC techniques that we shall discuss will be based on asynchronous techniques.

(Refer Slide Time: 17:32)



Now the MAC technique designer has a number of goals to satisfy. These are the various goals or objectives.

(Refer Slide Time: 17:55)



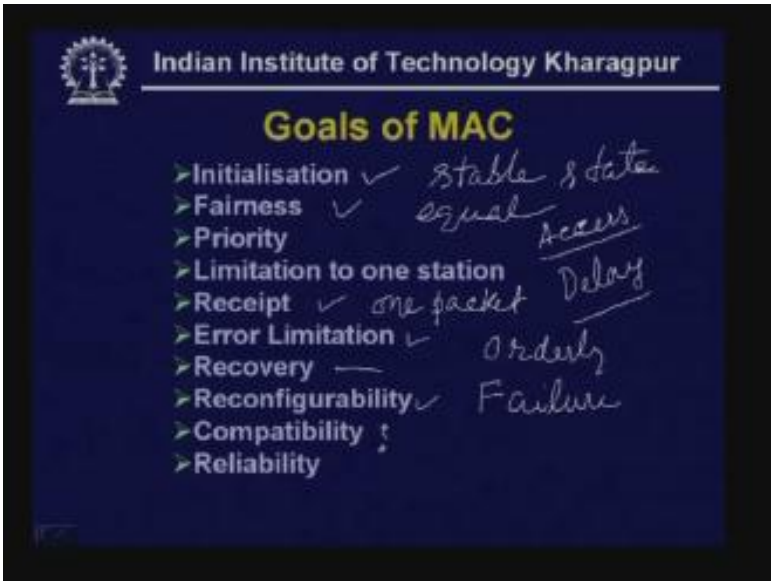
First one is initialization. What you mean by initialization? Whenever you put the network on in the beginning then it should go towards stable state. That means it should know who will be transmitting first, who will be transmitting next and so on, there should not be any chaos. As the network is first turned on it should go to a stable state that is your initialization, the initial condition will be satisfied.

Second is fairness. We have seen that you have got a number of stations who are trying to send data through a shared medium. Obviously each and every node has to be given equal opportunity. By that we mean the time for access provided to each station has to be fixed and the delay where after some amount of time each station has to wait for some time so that delay should also be same for each and every station. This is your fairness which has to be guaranteed by the MAC technique.

Then another important is limitation to one station. We have seen that there are a number of stations trying to send so at the end MAC technique should ensure that only one station transmits and also it is being received by one station and already one packet of data is received and not multiple packets will be received by the station. And if multiple packets are there it should be sent in an orderly manner. So, receipt of packets should be sent in an orderly manner. It will also perform error limitation, it will do error detection and correction.

Then we have the recovery. So, whenever there is failure the Medium Access Control should be designed in such a way that it is able to recover from the failure and then comes the question of reconfigurability. As I have mentioned stations will be added or removed from the network so the Medium Access Controls will be able to reconfigure the network so that it can perform the Medium Access Control in an effective manner.

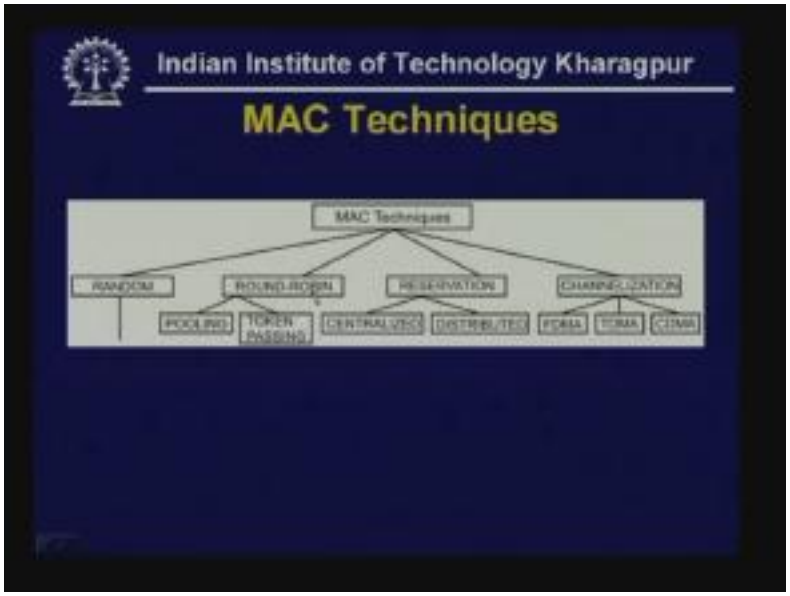
(Refer Slide Time: 20:40)



Then comes the question of compatibility. Compatibility is important because there will be some standard Medium Access Control (MAC) technique if different manufacturers build equipment they should be able to operate with each other, so that is your compatibility that has to be ensured.

Finally comes the question of reliability. The MAC technique should be able to work under the condition of failure and other problems. So reliability has to be ensured by the MAC techniques. Now let us consider the various MAC techniques that is being used.

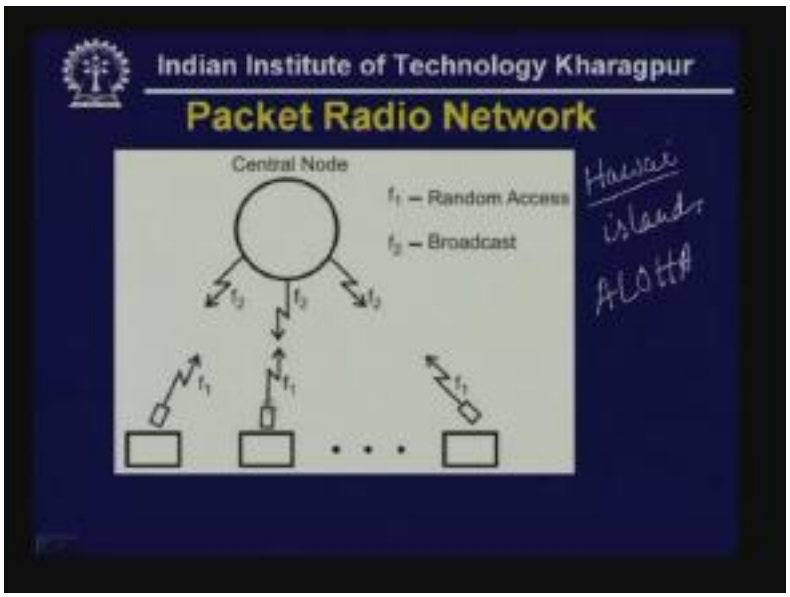
(Refer Slide Time: 21:30)



As you can see it can be broadly divided into four types; random, round-robin, reservation and channelization. These four categories are needed in different situations. And in this lecture we shall focus on the random techniques. We shall discuss about the other techniques in subsequent lectures. Let us focus on the random technique which is very suitable for bursty nature of traffic.

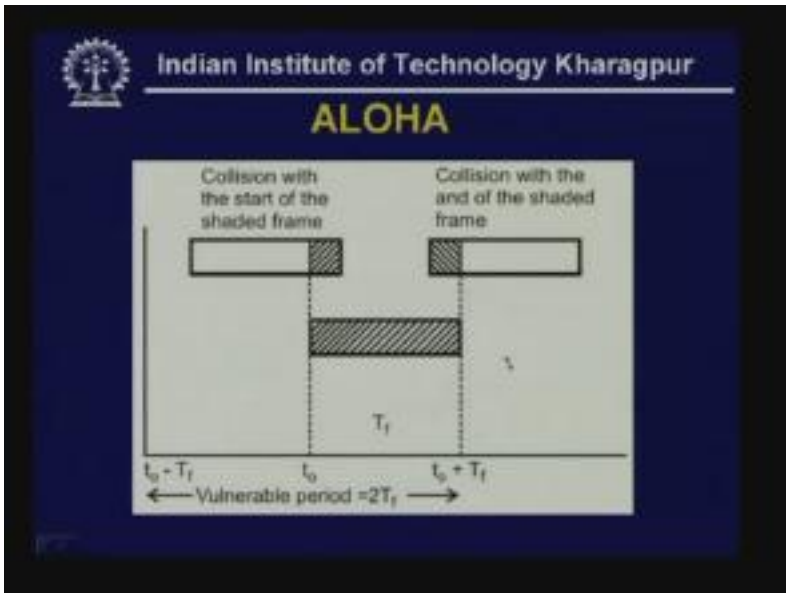
These random MAC techniques again can be divided into four different types; ALOHA, CSMA, CSMA/CD and CSMA/CA. We shall discuss each of them one by one. Let us first consider the first one that is your ALOHA. This ALOHA was developed for packet radio network by University of Hawaii. As you know this particular location comprises of a number of islands and obviously you cannot setup wired network in these islands so in the University of Hawaii there was a centralized computer central computer and there were terminals distributed to different islands so it was necessary for the central computer to communicate with the terminals and for that purpose Abramson developed a protocol which is known as ALOHA for this kind of environment. The basic environment is mentioned here.

(Refer Slide Time: 23:16)



This central node is essentially the central computer located in the University of Hawaii and these are the various terminals. This is the terminal one (Refer Slide Time: 23:22) this is terminal two and this is terminal n located in different islands. So they communicate by using a wireless technique which is known as packet radio. Now the basic technique is shown here. Each of these stations can transmit by using uplink frequency f_1 which is RANDOM access shared by all the terminals. On the other hand the central node after receiving whatever is being received from all other stations is retransmitted by using a downlink frequency f_2 from the central computer and this is being received by all other stations. So this is the basic environment for which the ALOHA protocol was designed.

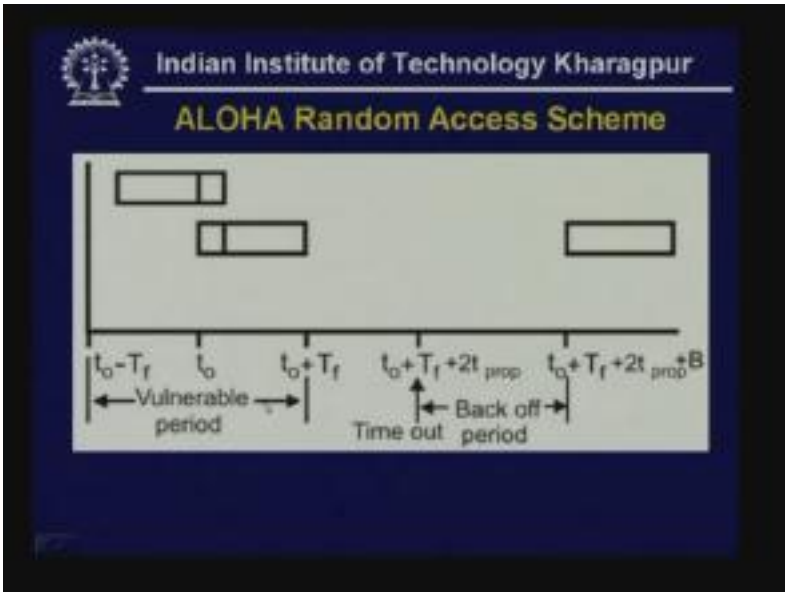
(Refer Slide Time: 24:25)



It works like this. Any station that has some data to send will send it. So it can be considered as a free for all. So anybody who has data to send will send it. Now, in such a case obviously T_f this is the frame transmission time, this is the packet duration. As you can see the vulnerable period is 2 into T_f. so if a packet is transmitted anywhere within this range will overlap with this. This packet will overlap with any packet transmitted within the range $2T_f$. Thus as a result what will happen is collision will occur and this central node will send the garble packet and whenever the garble packet is received by all other stations they will know that packet has not been transmitted successfully so the terminals will perform retransmission. The retransmission technique is used here whenever there is a collision.

Now let us see how it is being done.

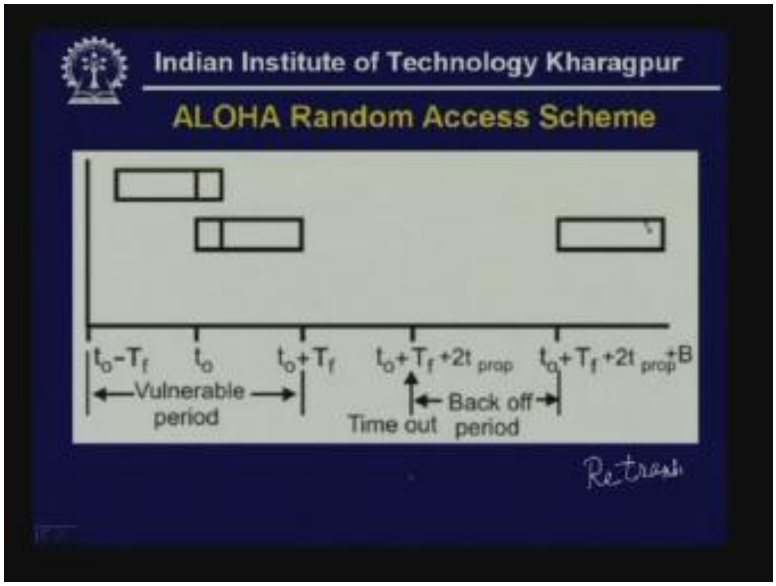
(Refer Slide Time: 25:55)



As I mentioned this is the vulnerable period which is equal to $2T_f$ and a collision can occur within this period whenever there are multiple stations where multiple terminals sends data. There is a maximum propagation time. We have seen that from the terminal it will go to the central node and from central node again it will come here. So this round trip delay is essentially this 2 into T propagation time. This is the time out period. that means after the vulnerable period you can see that T_0 plus T_f and $2T_f$ so after a successful transmission this is the vulnerable period and within this time the T_0 plus T_f plus $2T_f$ and all other stations will come to know that collision has occurred.

Now, if multiple stations start sending data at the same time then collision occurs. And if they immediately send data one after the other again there are chances of another collision. That's why stations wait for some random amount of time known as back off. So the stations wait for random amount of time then again they do the retransmission, so this is your retransmission. This retransmission is being performed by all the stations but the back off time is different for different stations. After a packet is transmitted it has to wait for this much duration for when it is retransmitted and this back off time is random in nature so that the collision does not occur second time in this.

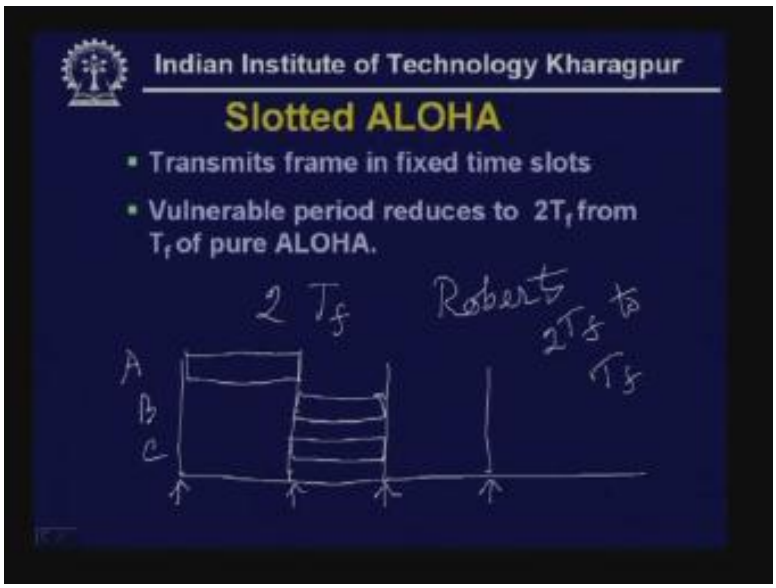
(Refer Slide Time: 27:50)



Let us see how the performance can be improved in this case.

Now as we have seen in the previous case known as pure ALOHA the vulnerable period is 2 into T that is your transmission time. Now Roberts proposed a technique which is known as slotted ALOHA and in this technique the time is divided in equal slots. Then the packet transmission can be started only in the beginning of the time slots like here, here, here or here and not in between.

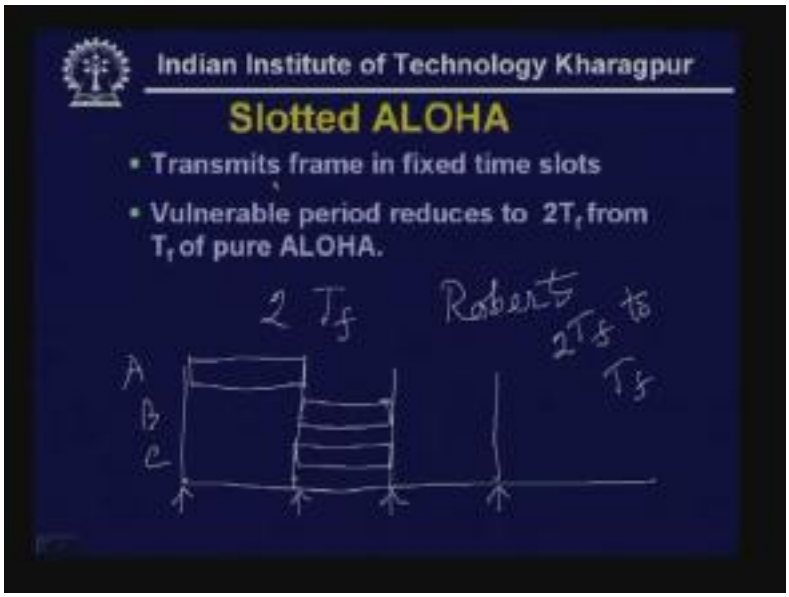
(Refer Slide Time: 28:30)



So in case of pure ALOHA transmission can start any time. So as a consequence there will be no collision and say this is your sender A, this is your sender B, this is your sender C so if there is overlap there will be overlap for the entire frame and not part of the frame as it happened in case of pure ALOHA and as a consequence in this case the vulnerable period is reduced from $2T_f$ and this will lead to a better performance of this slotted ALOHA technique.

Let us see how the performance varies.

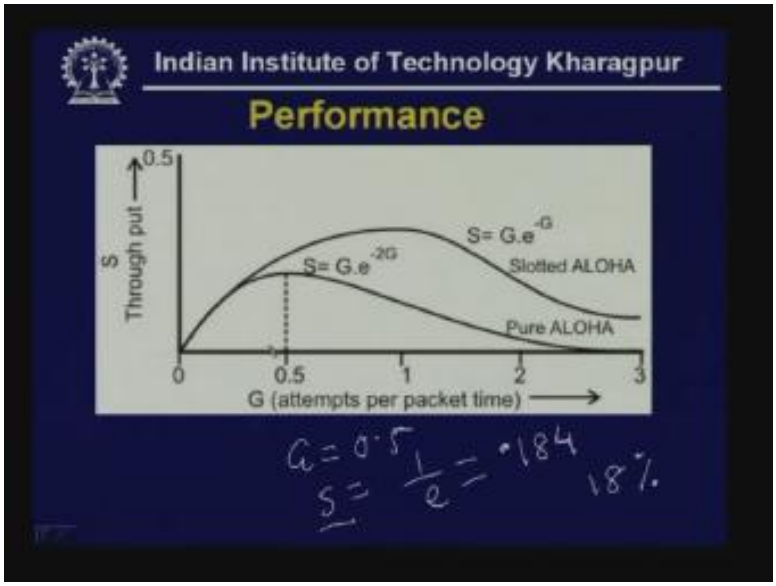
(Refer Slide Time: 29:18)



Now as you can see this G is the offered load and the number of attempts made per packet time. and if the number of attempts made per packet time increases as you can see if it reaches 0.5 in case of pure ALOHA then you get maximum throughput and maximum throughput is S is equal to G into e to the power minus 2G and this happens when G is equal to 0.5. So in this case the value of S is equal to 0.5 into e to the power minus 2G where G is equal to 0.5 so it will be equal to 1 by e so value is eventually 0.184 roughly. That means we can see that the maximum throughput S that can be achieved is roughly equal to 185 and which happens whenever the offered load is 0.5 that means number of attempts per packet is 0.5 and as more packets are introduced the throughput decreases and it may become 0 whenever the offered load is very high.

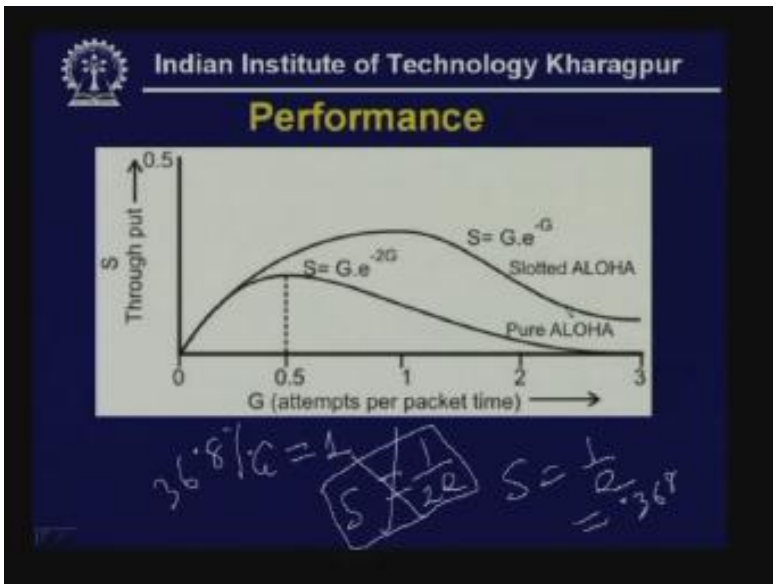
That means as the load increases there is a possibility that the throughput will become 0. This ALOHA works only when the traffic is very small and the network is very lightly loaded which is less than 18%.

(Refer Slide Time: 30:55)



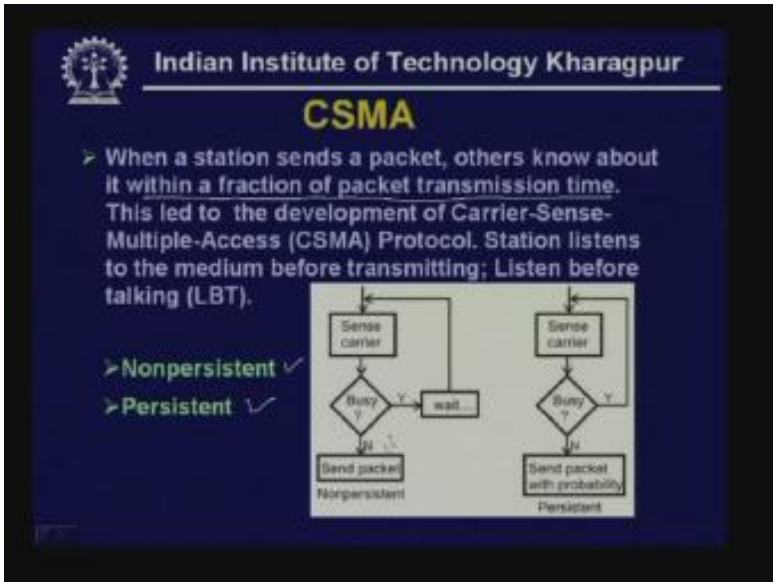
However, by using slotted ALOHA we can see that performance improves and as we can see here the throughput the maximum throughput is received whenever G is equal to 1. So whenever G is equal to 1 the maximum throughput that you can get in this particular case is S is equal to 1 by e is equal to 0.368, in the previous case for pure ALOHA it was ½. So we find that the maximum performance throughput you can achieve in this case is roughly about 36.8% which is double that of pure ALOHA. So by using slotted ALOHA the performance is doubled in slotted ALOHA compared to pure ALOHA.

(Refer Slide Time: 32:10)



Now let us look at the limitation of this technique.

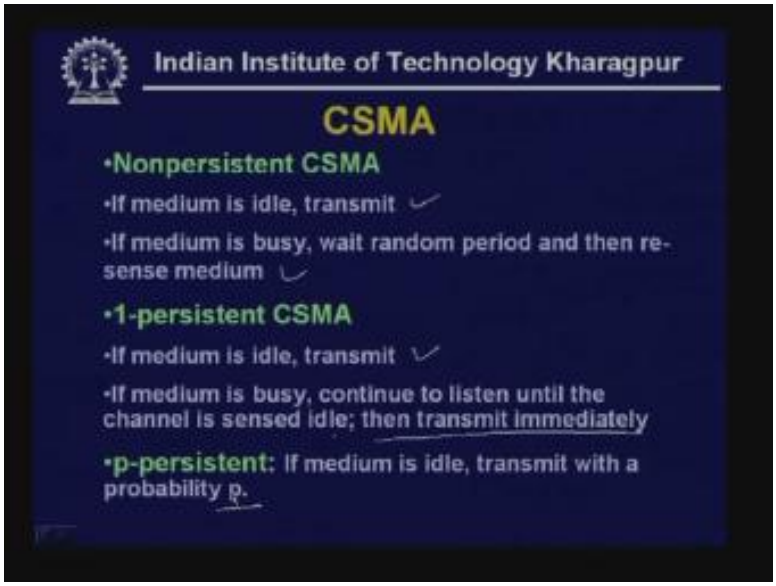
(Refer Slide Time: 32:19)



When a station sends a packet others know about it within a fraction of packet transmission time. So usually the packet transmission time is much longer than the propagation time because these are very closely located. But in case of pure ALOHA or slotted ALOHA the medium was not checked before sending the packet. If already a packet transmission is going on then the station starts sending packets that is being overcome in CSMA.

Therefore based on this observation that the other stations come to know about it within a fraction of the packet transmission time why not monitor the medium. this lead to the development of Carrier Sense Multiple Access protocol which is essentially based on stations listen to the medium before transmitting or it is based on Listen before talking (LBT). That means first you check the medium, if it is free only then you send it so the collision will reduce. It has got two varieties nonpersistent and persistent. Let us see what happens in non persistent.

(Refer Slide Time: 34:20)



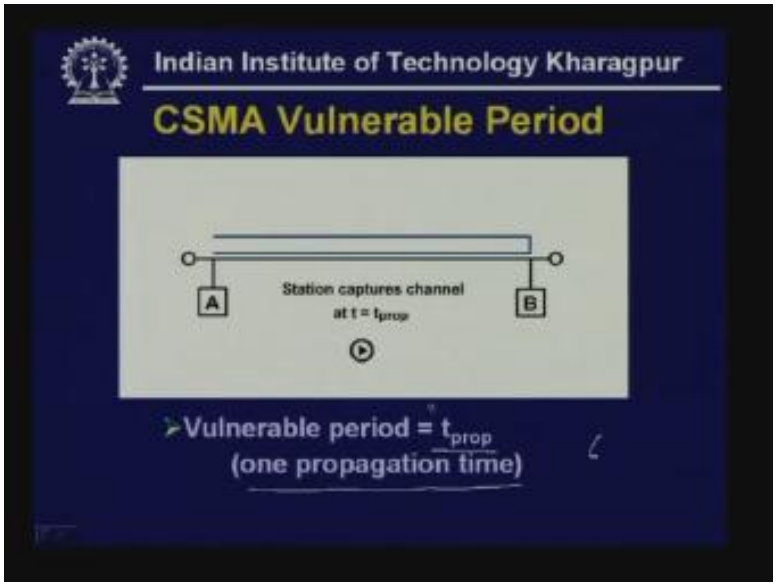
In non-persistent each station senses a carrier and if it is busy then it waits for random amount of time. On the other hand if it is not busy then the packet is sensed. On the other hand in case of persistent protocol if the medium is busy it again senses a signal, it does not wait for random amount of time but it keeps on sensing and then whenever it is not busy it senses the packet with some probability. These are the two basic variations. Let us see how exactly it happens.

Thus we have seen that in case of non persistent if the medium is idle the packet is transmitted. On the other hand if the medium is busy wait random period then re-sense the medium once again. So, after re-sensing if it is busy again wait for random amount of time and if it is not busy it is transmitted. In case of that persistent there are two varieties. In case of 1-persistent if the medium is idle it transmits and if the medium is busy continue to listen until the channel is sensed idle, then transmit immediately so it does not wait for probability rather it transmits the probability one.

On the other hand in p-persistent if the medium is idle transmit with a probability p. So it may transmit or it may not transmit and that is the advantage of p-persistent. So these are the three basic techniques used here and in this particular case let us see what the vulnerable period is because vulnerable period plays a very important role so far as the throughput is concerned.

In case of CSMA as you can see the packet is going from one end to the other end of the network and by the time it reaches the other end and if no collision takes place then within one propagation time a station captures the medium. In other words we can tell that the vulnerable period is t propagation time and we know that the propagation time is usually small compared to the transmission time. That’s why the vulnerable period is relatively smaller in case of CSMA technique.

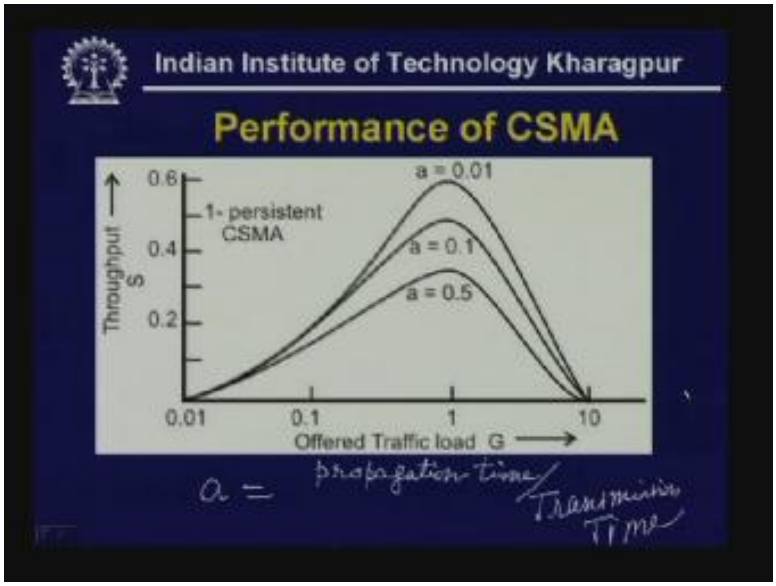
(Refer Slide Time: 36:16)



However, the throughput depends on a parameter known as ‘a’ where ‘a’ equals to the ‘propagation time’ by ‘transmission time’ of a packet. So this ratio propagation time by transmission time plays a very important role and that decides the throughput. As you can see we have not given any analytical expression for throughput but here it shows how the throughput varies as the value of ‘a’ changes. As you can see whenever ‘a’ is going to 0.5 that means propagation time by transmission time is 0.5 that means propagation time is relatively high compared to transmission time which is about half of the transmission time then a is equal to 0.5 then this is the throughput it is about 0.36 which is very close to the slotted ALOHA.

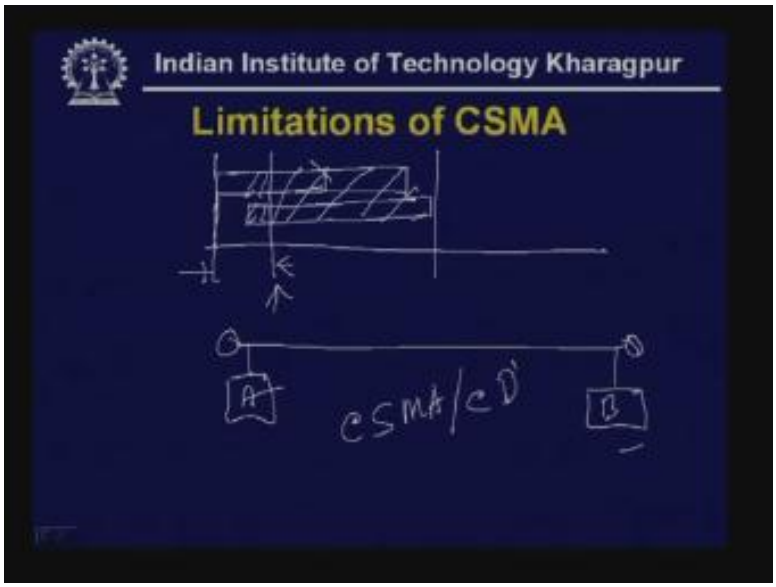
On the other hand as the value of ‘a’ becomes smaller and smaller the throughput increases and that’s why that parameter plays a very important role so it is necessary to have smaller propagation time and relatively larger transmission time to have higher throughput in CSMA protocol.

(Refer Slide Time: 37:58)



Now we find that this CSMA protocol has a very serious limitation. the limitations come from the fact that, suppose here a particular station starts transmission of a packet and this is the maximum propagation time to a particular medium (Refer Slide Time: 38:39) say this is the network, this is one station A and here at the other end we have got another station B. Now B comes to know about it within this time but the packet transmission time can be quite long.

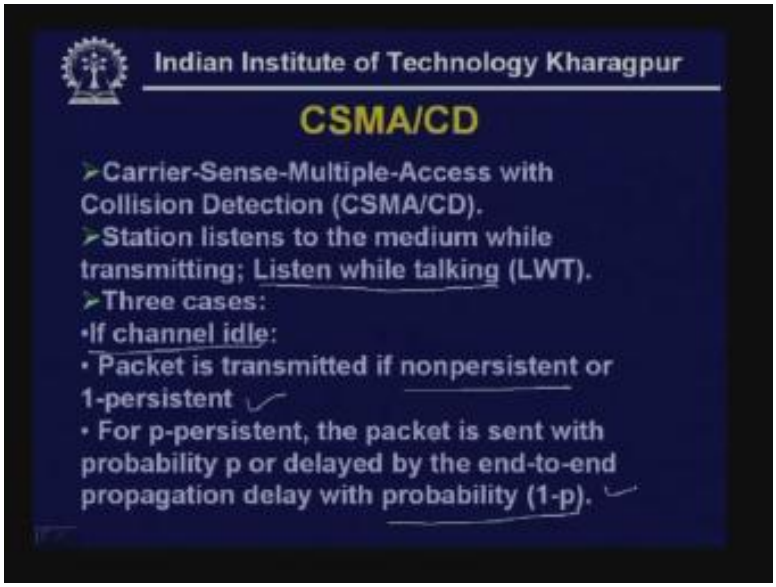
(Refer Slide Time: 39:52)



So although a particular station transmits it and then the other end receives that packet it can easily find out whether the medium is busy or not. but what happens is if this particular station has started transmission somewhere here and even after detecting a collision it will still continue transmission so during this point in time both the packets will overlap and not only this part but also this part of the time so by this time this station has come to know that collision has occurred in spite of that it has not stopped transmission and neither the previous station stops transmission. As a result what happens is the time is wasted. This wastage of time is minimized in CSMA/CD Carrier Sense Multiple-Access with Collision Detection.

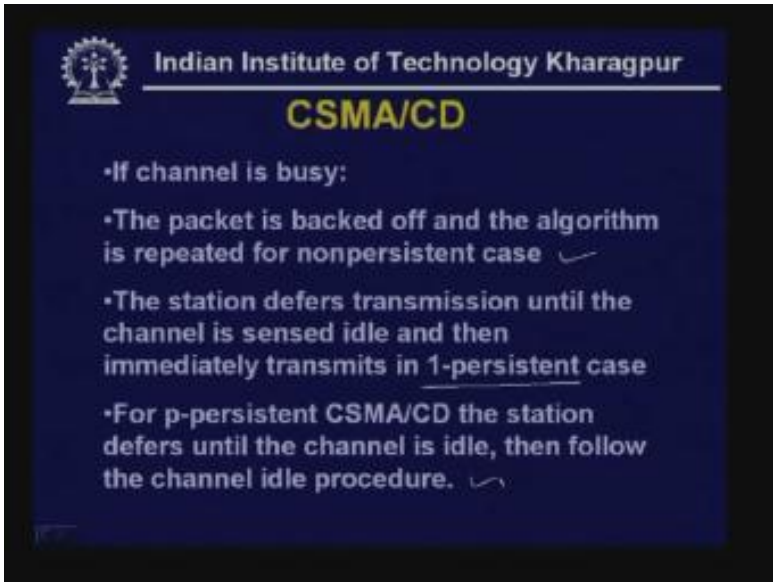
So, in Carrier Sense Multiple-Access with Collision Detection the station listens to the medium while transmitting that not only it listens to the medium before transmission as you do in carrier sense multiple access but it does some additional thing, that it listens while transmitting, that's why it is called listen while talking (LWT). And here also there are three cases; nonpersistent, 1-persistent and p-persistent and as you know if the channel is idle the packet is transmitted if nonpersistent or 1-persistent. For p-persistent the packet is sent with probability p or delayed by the end-to-end propagation delay with probability 1 minus p.

(Refer Slide Time: 40:58)



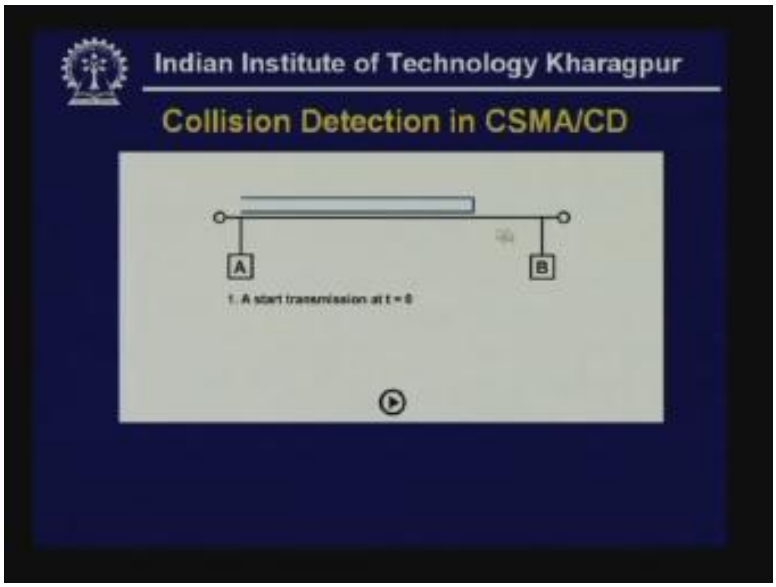
For p-persistent even when the channel is idle it may be sent it may not be sent. On the other hand if the channel is busy the packet is backed off and the algorithm is repeated for nonpersistent case. And the station defers transmission until the channel is sensed idle and immediately transmits in case of one persistent case. For p-persistent CSMA/CD the station defers until the channel is idle then follows the channel idle procedure.

(Refer Slide Time: 41:30)



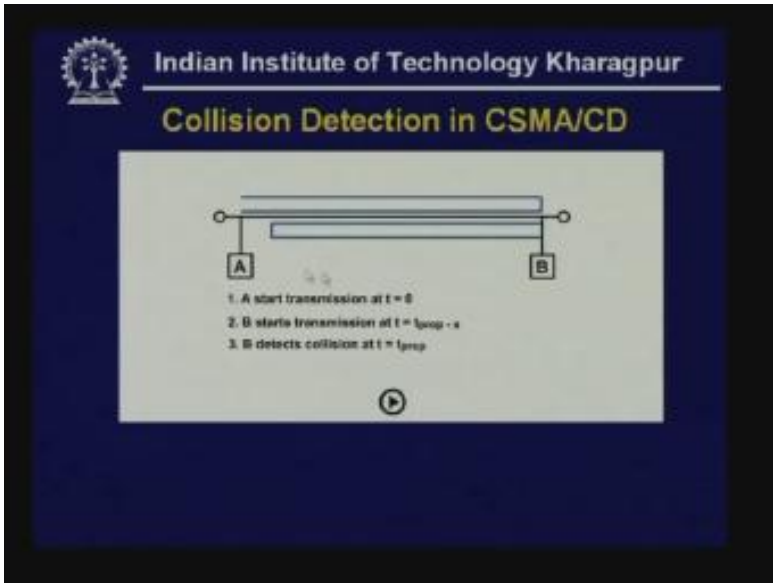
We have to understand the channel idle procedure to understand the CSMA/CD protocol. But the basic idea is this that whenever the channel is found to be idle packet transmission is started and the stations keep on monitoring the medium and whenever a collision is detected some jamming signal is introduced to inform all the stations that collision has occurred. Therefore all the stations backs off and they wait random amount of time before transmitting another packet, that is the basic idea, let's see how it really happens. But before that let's see what is the minimum requirement of collision detection in CSMA/CD.

(Refer Slide Time: 42:33)



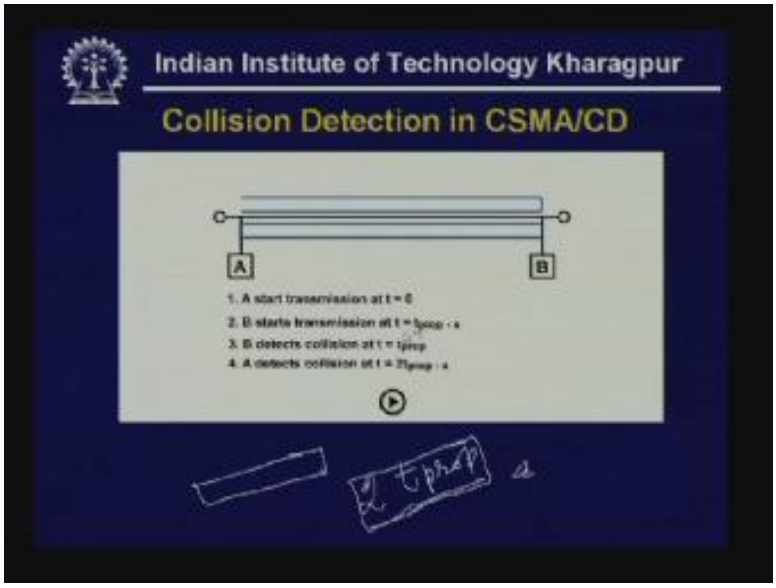
Here suppose station A starts transmission at time t is equal to 0 and the packet moves towards the direction of B which is at the other end and before this packet reaches B it starts transmission again with another packet which goes towards another direction and whenever this packet reaches it detects collision (Refer Slide Time: 42:45) and whenever this packet reaches the other end it detects collision so we find that for detection of collision by both ends the period that is required is 2 t propagation that is twice the propagation time is required for collision.

(Refer Slide Time: 42:44)



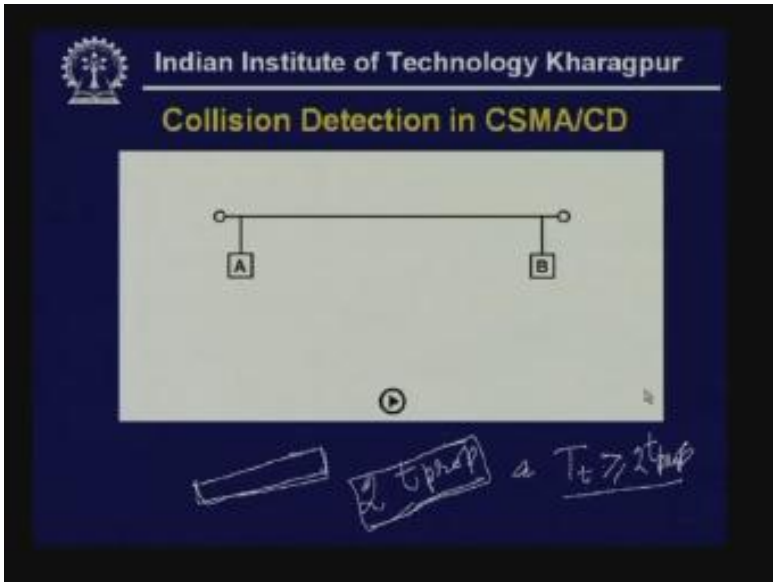
Here what it means is the transmission of the packet should be longer than the two propagation time, that is the requirement for detection of collision.

(Refer Slide Time: 43:20)



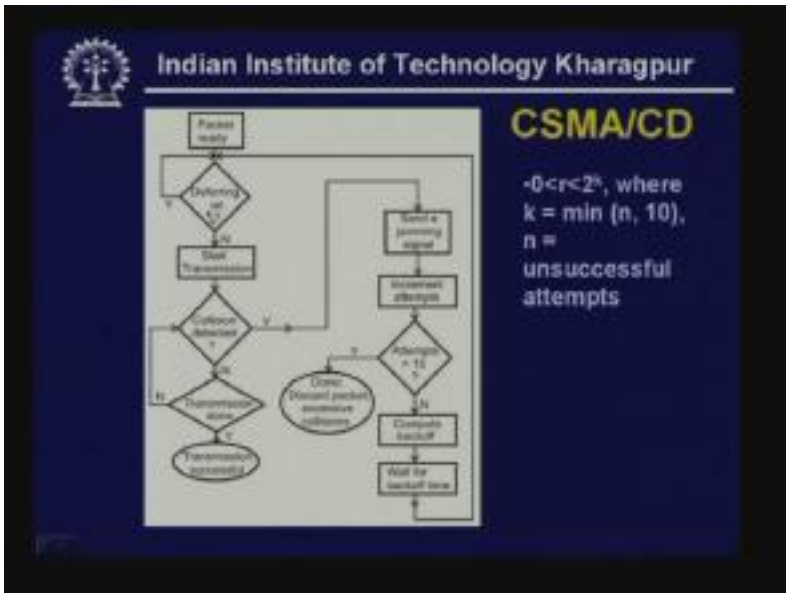
That means collision is detected when a particular station is transmitting a packet and if it receives some other signal some other carrier then it detects collision. To do that the requirement is that the transmission time that is T transmission time should be greater than equal to 2 into t propagation time. If this condition is satisfied all the stations will be able to detect collision. If it is smaller than that in this situation what can happen is the packets may collide in the middle that means if the packet is small it may go in this direction and before it reaches this the transmission is finished and whenever the transmission starts from here it will send another packet and again both the packets will cross each other in the middle and collision will only be detected by the middle station but not by all other stations, not by the senders, so to ensure that this is the requirement.

(Refer Slide Time: 44:38)



Now I mentioned about the back off time. This is the binary back off algorithm that is being used in CSMA/CD protocol.

(Refer Slide Time: 45:00)



Here we see that whenever the packet is ready it checks whether it is deferring or not deferring, whether it is waiting for some time or not. If it is not waiting then it starts transmission. And as I mentioned while transmitting it keeps on monitoring to detect collision. If collision is not detected then the transmission is finished. However, then the transmission is done, transmission is successful.

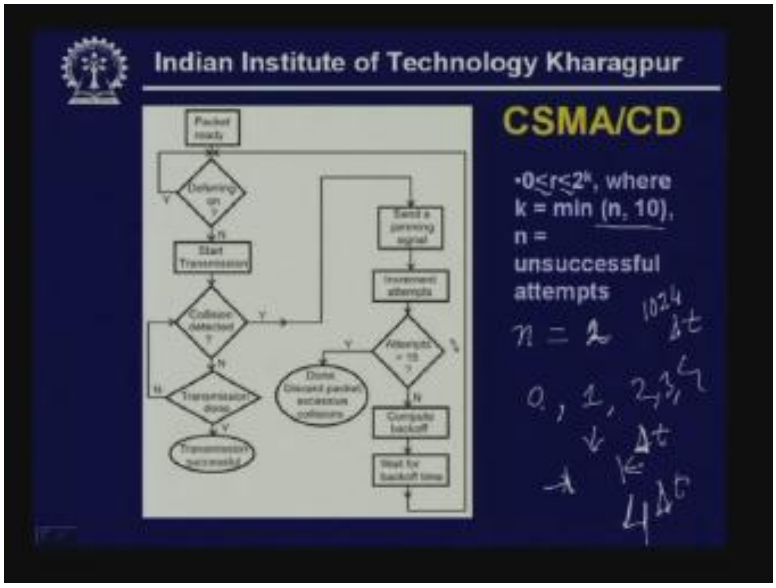
On the other hand if the transmission is not finished and collision is detected then it sends a jamming signal. After sending the jamming signal it has to decide about how long it will back off. For that purpose it has to find out for how many attempts it has already done so it will increment the attempt from the previous one and it will check whether the number of attempt has exceeded 50 or some maximum number that is allowed. If the maximum number is allowed it computes back off and waits for the back off time.

Let us see how the back off time is collected. For that purpose a number 'r' is found out. How it is found out? It finds out a value between 'n' and 10, 'n' is the number of unsuccessful attempts. Whenever it is the first attempt then value of n is equal to 1. So in such a case it will wait between 0 and 2 to the power 1 is equal to 2, the first attempt is unsuccessful attempt which is 1 so it will be 0, 1 and 2. These are the three possible cases and this is being multiplied with some time slot and that time slot is multiplied by delta t. So the delta t is multiplied with this and that is the back off time.

Now after two back off say whenever n is equal to 2 this k is equal to 2 and value will be 0, 1, 2, 3 and 4 so it will choose between 1 and 4, 0 and 4 then it may send immediately or it will send up to 4 delta t amount of time. So in this way it will keep on increasing and maximum time can be 2 to the power k 2 to the power 10 that means 1024 delta t which is quite high. That means the back off time randomly increases as the number of attempts increase. So whenever the number of attempts exceeds fifteen then the packet is discarded because excessive collision is occurring which means the network is heavily loaded. So in such a situation the rate transmission is not performed. So you find that in case of CSMA/CD protocol whenever the number of collisions exceeds 15 the packet will not be transmitted.
so we cannot guarantee that packets will always be delivered to the destination.

However, whenever the traffic is less that means load is less the number of collisions will be less then the packet will be delivered.

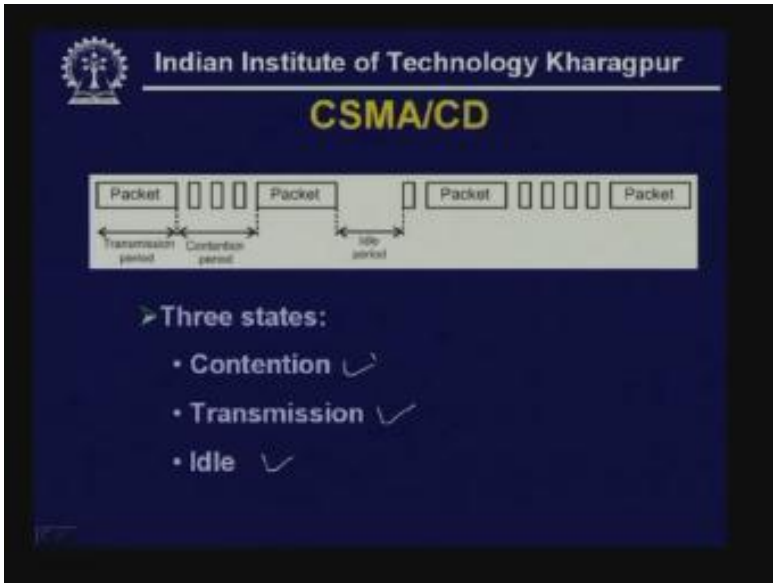
(Refer Slide Time: 48:38)



In other words that CSMA/CD protocol works fine whenever the load is less. The CSMA/CD protocol has got three distinct states. First one is contention period. After a successful transmission there will be some contention period. Contention period is essentially during which all the stations will try to content to get hold of the medium and we have already seen that binary back off algorithm which is being used to resolve the contention and after the contention is resolved a particular station gets hold of the medium and it performs the transmission.

However, if the network is very lightly loaded there may be some idle period and after the idle period again there can be some contention period, then packet transmission, then contention period, then packet transmission or idle period. So we find that in the CSMA/CD protocol it will be in one of the three states, either it will be transmitting a packet or through the medium or there will be some kind of contention algorithm going on contention mechanism going on by using binary back off algorithm then all the stations will try to get hold of the medium and ultimately one of the station will be able to get hold of the medium and send the packet. This is how the CSMA/CD works.

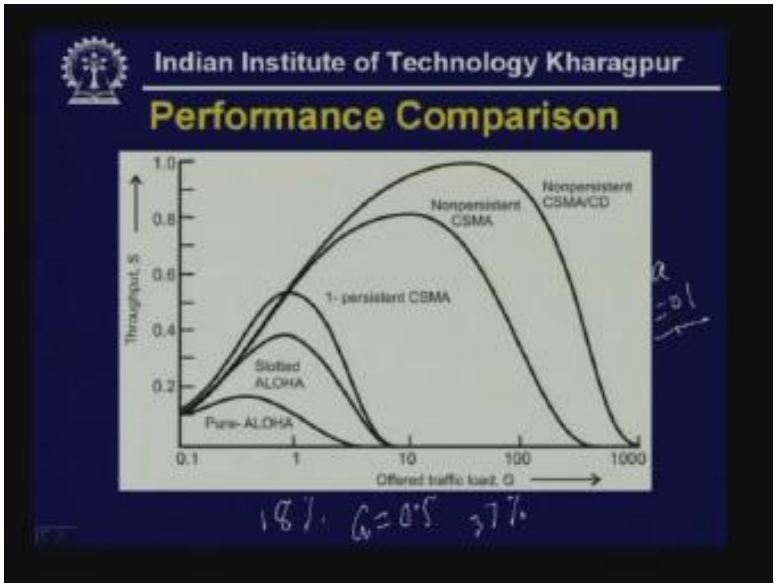
(Refer Slide Time: 50:00)



Now let us look at the performance of various protocols. Let us compare the performance of different protocols that we have discussed so far. Here we see that in case of pure ALOHA the maximum throughput we can achieve is only 18% and that happens whenever the value of G is equal to 0.5. in case of slotted ALOHA the performance improves to about 37% which occurs when G is equal to 1 and for 1-persistence CSMA we find that the throughput is roughly very close to 60% and for nonpersistent CSMA the throughput is increasing. Here actually for these two values nonpersistent CSMA and nonpersistent CSMA/CD we find that for non persistent CSMA/CD we get the maximum throughput which is very close to 1.

However, whenever the load becomes very high then of course it becomes unstable and throughput reduces and it reaches the thrashing situation in case of both nonpersistent CSMA and nonpersistent CSDMA/CD. Here all these curves have been plotted for a particular value of A which may be roughly equal to 0.01. That means the packet transmission time is roughly hundred times that of propagation time.

(Refer Slide Time: 52:20)



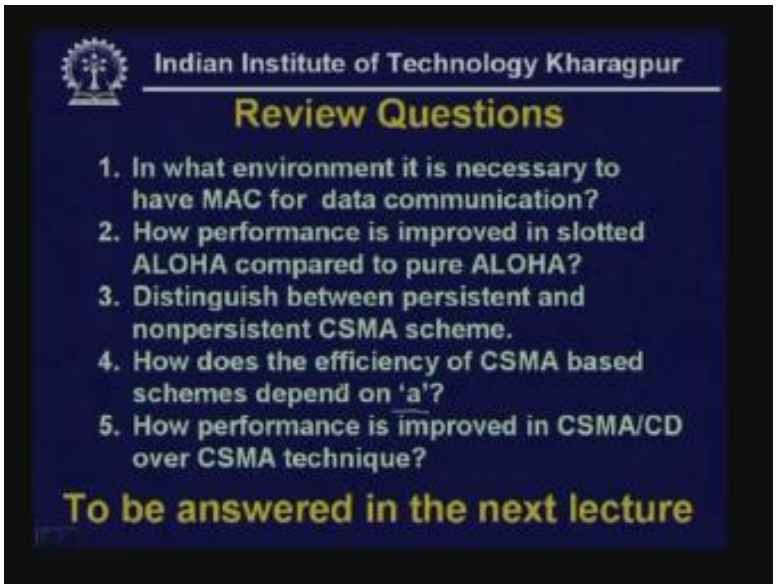
The propagation time is assumed to be very small compared to the transmission time. However, if the propagation time is not very small then there is a possibility that the throughput will not be very high. In this lecture we have discussed about various techniques based on contention or which are based on random techniques. There is another protocol which is known as CSMA/CA which is also based on contention used in wireless applications which I shall discuss in the next lecture. But let me summarize the techniques that we discussed in this lecture.

here we have seen that ALOHA which is the simplest one works fine whenever the traffic load is very very small and it is the simplest contention based technique, then the slotted ALOHA which is an improvement over CSMA/CA, there the performance is little better double that of pure ALOHA, however, in this case the packets are to be synchronized and as a result some synchronization mechanism has to be devised, the central controller may keep on sending some signal to all the stations and they will send them in a synchronized manner.

On the other hand in case of CSMA that means by monitoring the medium, Carrier Sense Multiple Access that means which is essentially listen before talk, by monitoring the medium the performance can be significantly improved in this case over slotted ALOHA or pure ALOHA and as you can see the nonpersistent CSMA performs better than 1-persistent CSMA and the reason for that is the 1-persistent CSMA is prone to more collisions because it is a greedy approach compared to nonpersistent CSMA.

By using Carrier Sense Multiple Access with Collision Detection throughput can be significantly improved and as you can see it may reach very close to 1. However, whenever the load is very high then they will not be stable and the throughput will decrease and it may reach thrashing situation. Now it is time to give you review questions based on this lecture.

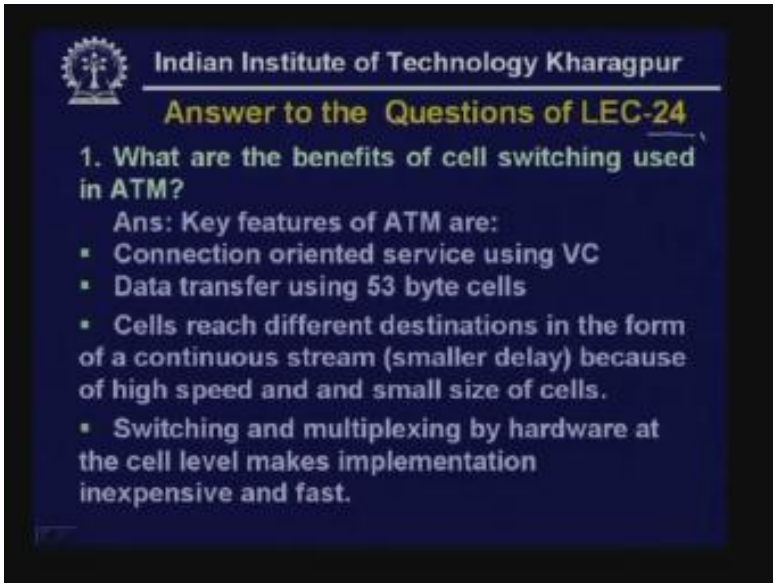
(Refer Slide Time: 55:30)



1) In what environment it is necessary to have Medium Access Control for data communication?
2) How performance is improved in slotted ALOHA compared to pure ALOHA?
3) Distinguish between persistent and non persistent CSMA scheme.
4) How does the efficiency of CSMA based schemes depend on 'a' which is the parameter propagation time by transmission time?
5) How performance is improved in CSMA/CD over CSMA technique?

These are the five questions based on today's lecture and these questions will be answered in the next lecture. Here are the answers to the questions of lecture minus 24.

(Refer Slide Time: 55:57)



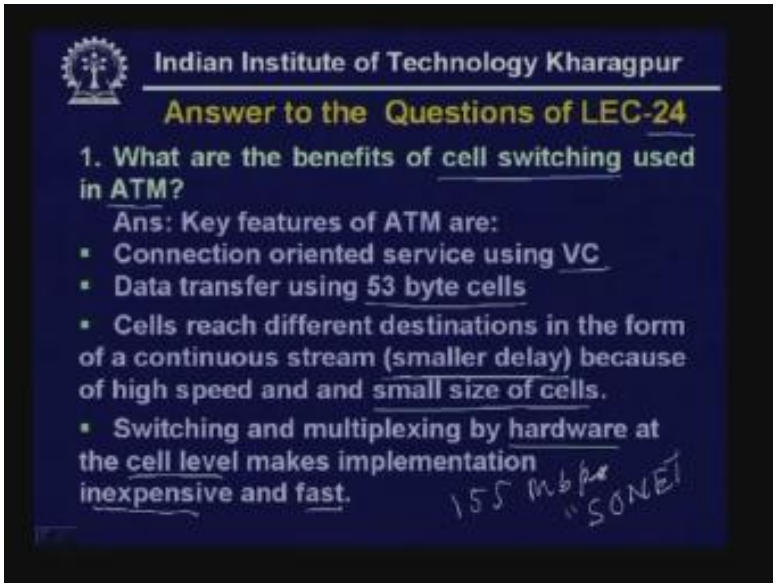
1) What are the benefits of cell switching used in ATM?

In the last lecture we had discussed the ATM network and we have seen that in ATM network cell switching is being performed.
The key features of ATM are:

- Connection oriented service using virtual circuit
- Data transfer using 53 byte cells

So it does cell switching. By using cell switching we have seen that cells reach different destination in the form of a continuous stream that means the delay is small because of high speed and small size of cells. So the cell switching has a benefit of smaller delay in ATM network and also switching and multiplexing by hardware at the cell level makes the implementation inexpensive and fast. So ATM networks as you know is very very fast, the minimum speed is 1545 Mbps and the other speeds are still higher and actually the physical layer that is being used is SONET Synchronous Optical Network and this is the minimum speed that is being used.

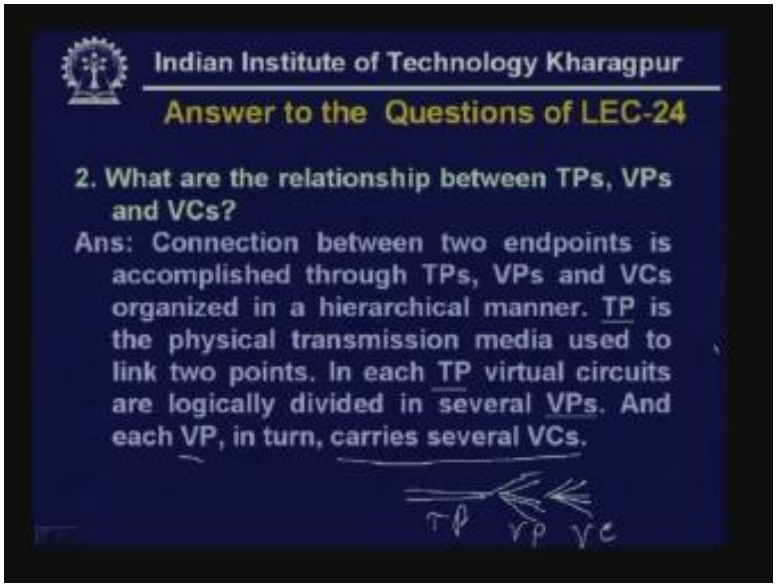
(Refer Slide Time: 57:08)



2) What are the relationship between TPs, VPs and VCs?

The connection between two endpoints is accomplished with the help of the TP Transmission Paths, Virtual Paths and Virtual Circuits organized in a hierarchical manner. As we know the Transmission Path is the physical transmission media. Usually in case of ATM it is optical fiber used to link two points and in each transmission path Virtual Circuits are logically divided in several virtual paths and each virtual path in turn carries several virtual circuits, so it is a hierarchy so each transmission path will have several Virtual Paths, this is your VP, (Refer Slide Time: 58:06) this is your TP and each Virtual Path will have several Virtual Circuits, and this is your VC. This is the relationship between TP, VP and VC.

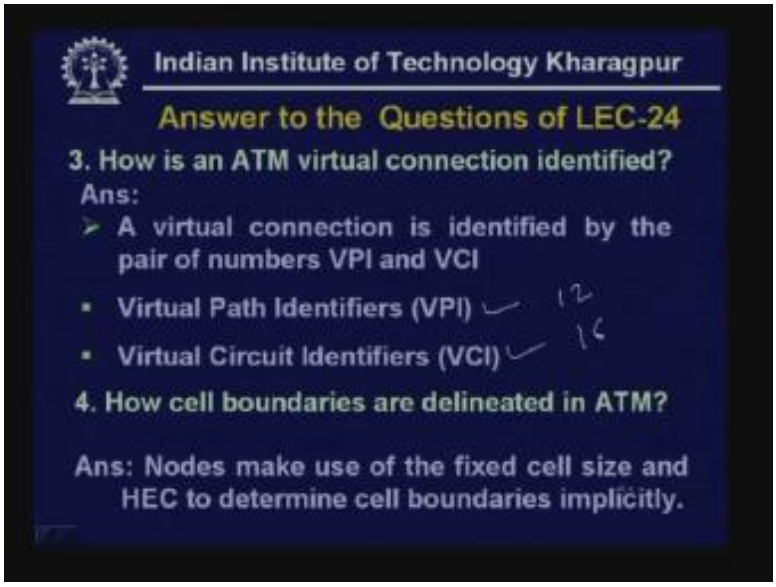
(Refer Slide Time: 58:14)



3) How is an ATM virtual connection identified?

The virtual connection is identified by a pair of numbers VPI and VCI that is your virtual path identifier and virtual circuit identifier. We know that this is a 12-bit umber and this is a 16-bit number and with the help of this it is identified.

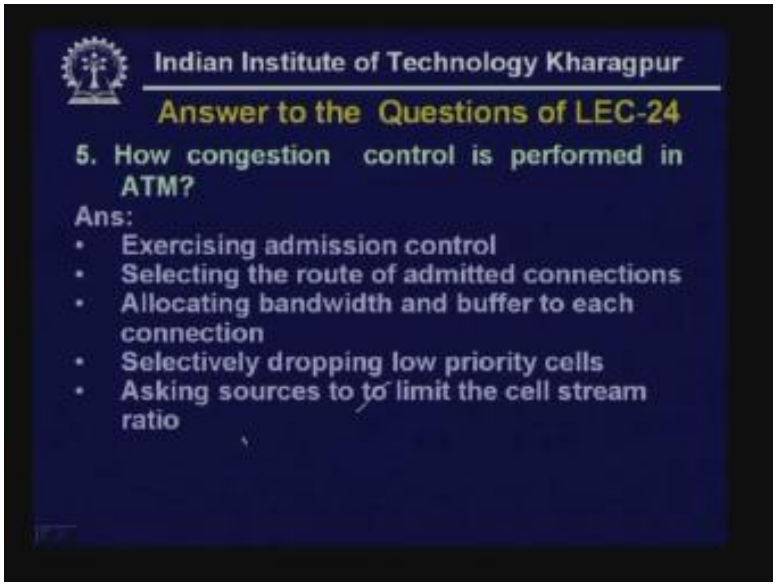
(Refer Slide Time: 58:47)



4) How cell boundaries are identified in ATM?

The nodes make use of fixed cell and HEC that is your header error control to determine the cell boundaries implicitly.

(Refer Slide Time: 59:15)



5) How congestion control is performed in ATM?

- Exercising admission control
- Selecting the route of admitted connections
- Allocating bandwidth and buffer to each connection
- Selective dropping low priority cells
- Asking sources to limit the cell stream ratio

These were the five questions given in lecture - 24 and with this we come to the end of today's lecture. In the next lecture we shall discuss about that CSMA/CA protocol and also we shall discuss about the control access techniques, thank you.