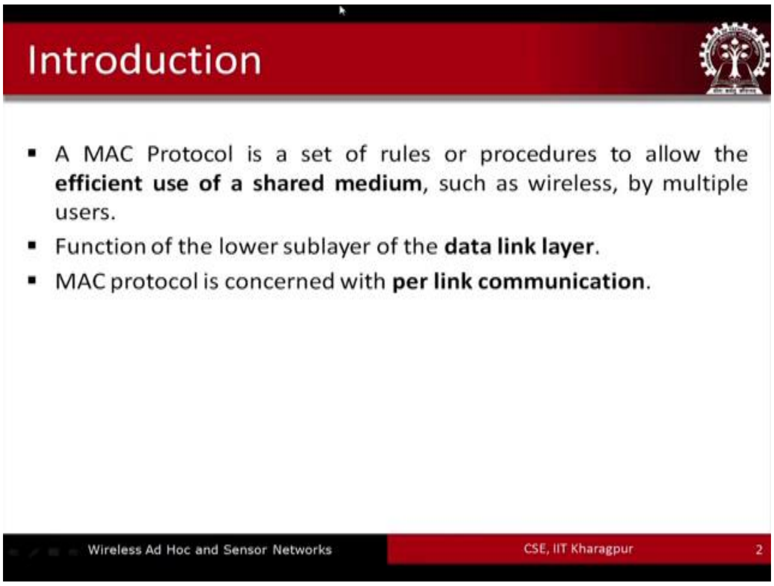
Wireless Ad Hoc and Sensor Networks
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 06
MAC Protocols in MANETs-Part-I

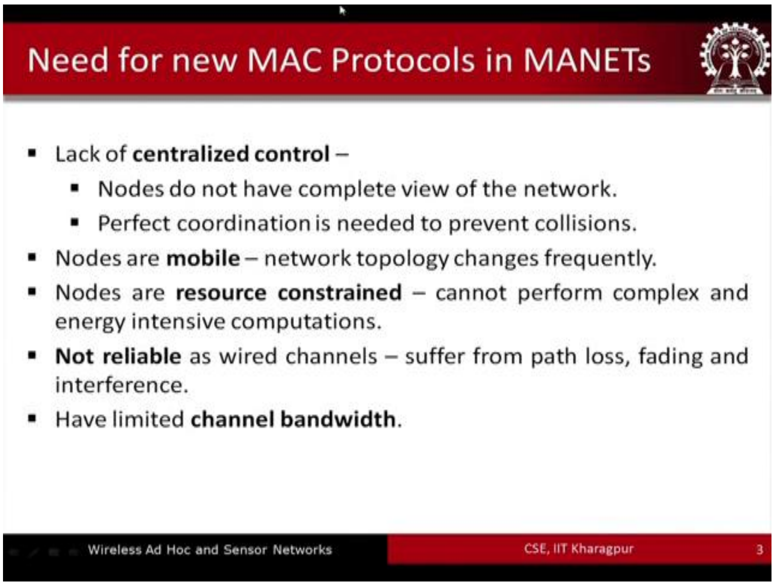
(Refer Slide Time: 00:27)



MAC protocols for mobile ad hoc networks. So, a MAC protocol is basically a set of rules or procedures, that can help in efficiently using this shared medium which can be wireless or you know which be even wired. And the protocol a MAC protocol will help for multiple users to be able to communicate over the shared medium. So, in this particular case for ad hoc networks we have a wireless environment and in the wireless environment there are number of stations or you know wireless nodes which want to communicate with one another over a multiple of path. So, what is required is to offer a mechanism by which these nodes to would be able to talk to one another over the shared medium. So, a MAC protocol for ad hoc network can help in doing so.

So, any MAC protocol basically in the OSI stack or in the TCP IP protocol architecture. It belongs to the sub layer which is called the MAC sub layer. So, the MAC sub layer basically runs all the functionalities of the MAC protocol. And the MAC protocols are concerned with per link communications; that means, that between 2 nodes which are within the transmission range, how they are going to you know talk to one another how they are going to share the medium. So, this is what the MAC protocol deals with.

(Refer Slide Time: 02:07)



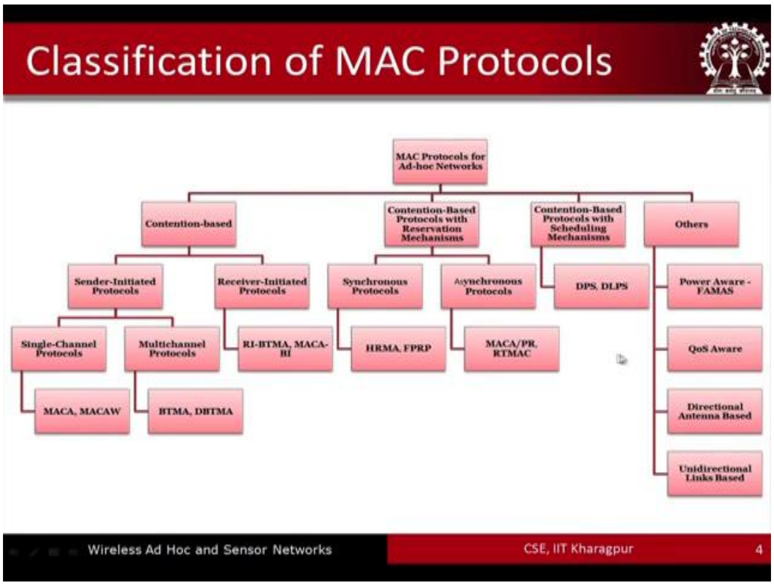
So, the one issue is that there is a lack of centralized control in mobile ad hoc networks. So, basically the nodes they do not have complete view of the network, and this is something that we have already seen that this I S 1 of the important features of a mobile ad hoc network, that there is lack of centralized control and at the same time you know what is required is that there should be perfect coordination that is required to prevent collisions between the packet that is sent by the different nodes which are sharing the medium.

So, this I S 1 problem. The second problem is that in a MANET the nodes are mobile. So, consequently what happens is that topology that is available at one point of time it changes at the later instants of time. So, that topology changes frequently because in MANETs typically the nodes they move quite fast. And consequently the you know the topology of the network changes quite fast the nodes are resource constraint resource constraint in different ways. So, resource constraint in terms of the energy. So, basically you know they cannot perform too much energy hungry you know algorithms or computations of different kinds and at the same time too many you know complex processes cannot be run you know in the different nodes of these networks.

So, this I S 1 problem the other problem is with respect to reliability. And reliability in the case of wireless channels is you know much less compared to the wired channels because the you know these channels wireless channels they suffer from path loss fading and interference. Additionally, compared to other wireless networks basically mobile ad hoc networks they are in environment which are even less reliable. Finally, in the other channel challenge is basically that you know there is very limited channel bandwidth and the different nodes they have to share that bandwidth and because of that channel bandwidth limitation you know.

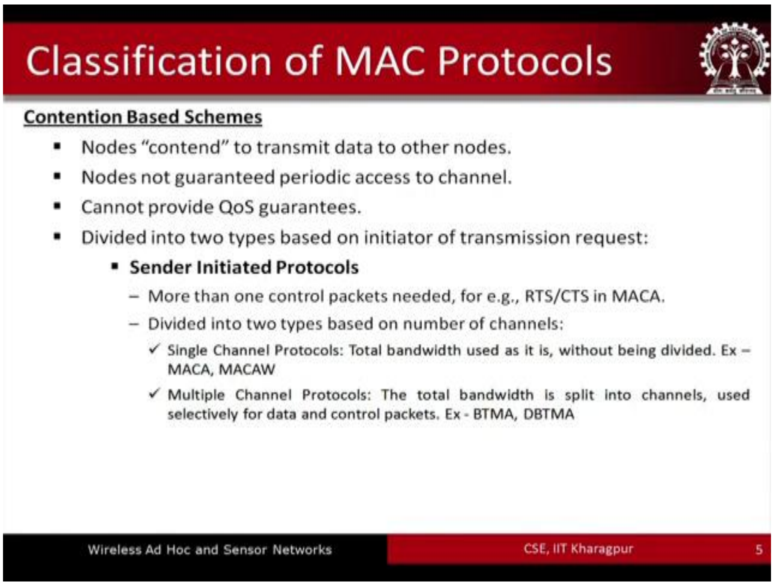
So, the existing MAC protocols that have been proposed for other wired or wireless networks are unusable for mobile ad hoc networks. So, what is required is that because of all these different challenges that we have just gone through we need to have a new set of protocols new set of MAC protocols that should be that should be available for use in MANETs. So, that these networks they do not suffer from too much of performance degradation you know. So, that the performance of these networks do not degrade too much.

(Refer Slide Time: 05:17)



So, there are different MAC protocols, that have been proposed since mobile ad hoc networks came into being. And what you seen in front of you is a taxonomy is a classification of the different types of MAC protocols that have been proposed. So, the MAC protocols that have been proposed for ad hoc networks they can be classified into contention based then contention based protocols with reservation mechanisms, contention based protocols with scheduling mechanisms, and there are different other classes of MAC protocols that have also been proposed. So, within the contention based again you know it can be further sub classified the MAC protocols can be further sub classified into sender initiated protocols, sender receiver initiated protocols. Again in sender initiated protocols you have single channel protocols multi channel protocols and so on. So, these are the different examples of the different protocols belonging to each of these categories and sub categories of you know MAC protocols that have been proposed for ad hoc networks.

(Refer Slide Time: 06:21)

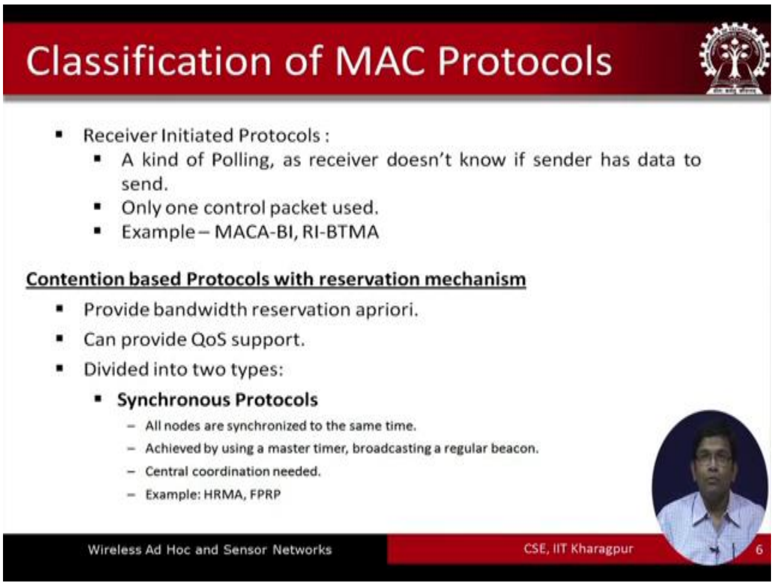


So, first let us look at the contention based schemes. So, in contention based schemes as the name suggests. So, what we have is we have a shared medium a common medium and we have different nodes which want to communicate with each other. In other words, in a very simple form the nodes they want to transmit their data out. So, transmit means that one node would like to send the data to one or more other nodes in the network. So everybody also wants to do the same. So, consequently what happens is we have some kind of a scenario where the nodes would have to content or compete with one another in order to get access to the medium. So, this is the feature of contention based protocols. Here the nodes are not guaranteed any kind of periodic access to the channel there is no access I mean it is a competition kind of scenario the nodes have to contend with one another. So, there is no guaranteed access to the channel. So, consequently QoS guarantees or other types of performance guarantees are also difficult to achieve using this kind of schemes.

So, belonging to the contention based you know MAC protocols we have the sender initiated protocol. And the other one is the receiver initiated protocols. As we can see this slide in the in the sender initiated protocols basically more than one control packets are needed. So, more than one control packets are needed. So, basically the sender initiates instead of sending the data right away the sender, what he does is it will first start with sending a RTS or a CTS you know will look at you know this these kind of packets that are sent. So, the RTS CTS packets are first sent before the data is actually sent out.

So, these senders initiated protocols can be of single channel proto can be of the class single channel protocols. There are 2 very well known protocols that we are going to cover MACA and MACAW which basically belongs to the single channel category. So, in single channel protocols basically; that means, MACAW and MACA these protocols they use the total bandwidth for running these algorithms or the protocols. So, that entire bandwidth is used by them. So, without dividing it into or dividing or a splitting it into you know sub channels and so on. So there is there are other classes of protocols which are like for example, you know DBTMA another protocol that we are going to go through BTMA etcetera these belong to the multi channel class of protocols. So, in multi channel class basically the total bandwidth is split into different channels. So, that the data and the control packets can be sent through the different channels.

(Refer Slide Time: 09:32)

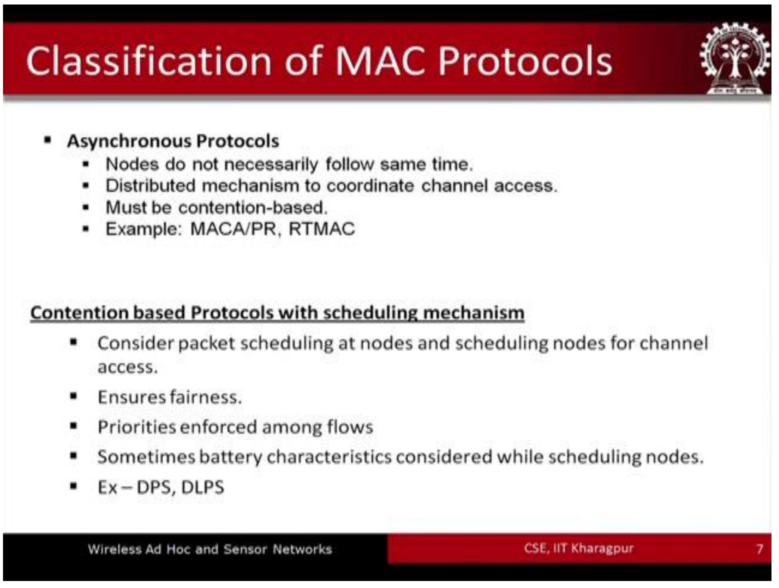


Then we have the receiver initiated protocols as I was telling you. So, in receiver initiated protocol what happens is the receiver. Basically you know initial does not know that whether the sender has data to send or whether the sender is sending the data or not initially the receiver does not know. So, the only way for the receiver to know whether the sender has a data to send or not is by periodically pulling the sender right. So there are different protocols call named as different protocols called named as MACA-BI then RI receiver initiate DBTMA a different variant of BTMA. This belong these belong to the receiver initiated category.

Then we have the contention based protocols with reservation mechanisms. So, I think you know this basically speaks for what it does. So, basically you know not only that these protocols help the different nodes to content for getting access to the medium, but also these protocols they provide some kind of bandwidth reservation facilities apriori. So, that there is some kind of a bandwidth reservation you know guarantees that can be offered. So, belonging to this category are 2 other sub classes of protocols called the synchronous protocols and the asynchronous protocols. So, again as the name suggests these names are quite indicative.

So, as this name suggests for example, the synchronous protocols all the nodes are synchronized to the same time. So, all the nodes are basically running the same timer. So there is a master timer and the nodes in a through some kind of a periodic broadcasting of a you know some kind of beacons or something like that or the maybe there is some kind of a centralized coordinator which basically keeps track of the time and that timer is the master timer and the other stations will come to know about the time by sharing by sharing the time from the master timer. So, these are the synchronous protocols HRMA and FPRP are 2 protocols belonging to the synchronous protocols category.

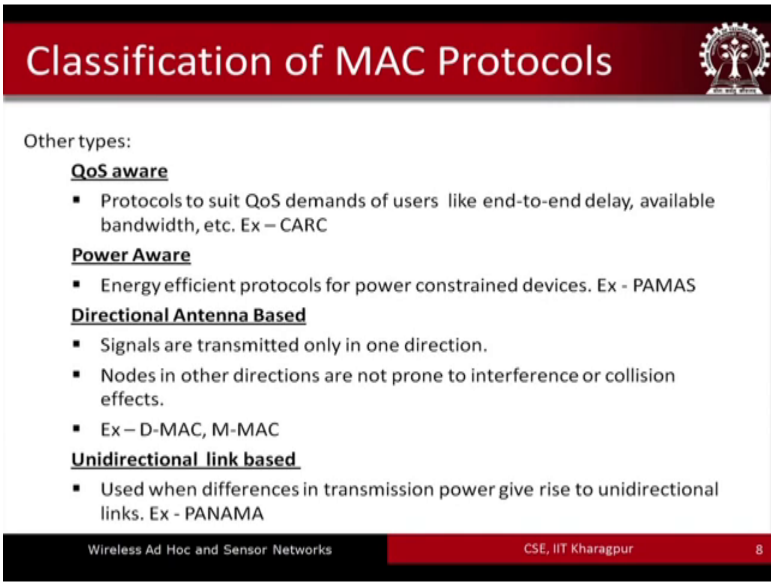
(Refer Slide Time: 11:41)



Asynchronous protocols basically are different completely opposite, where there is no requirement for the different nodes which want to get access to the medium to follow the same time clock. So, there is a I mean this basically class of protocols follow a distributed mechanism to get channel access. So, the other category is contention based protocols with scheduling mechanisms here the you know. So, what is required is you know some kind of fairness this kind of protocols they ensure some kind of fairness by enforcing priorities among the different flows of packets in between the different notes in the network.

So, these protocols they considered packet scheduling at the nodes and the scheduling nodes for channel access. So, there are few names of protocols belong to this category that are mentioned over here.

(Refer Slide Time: 12:44)



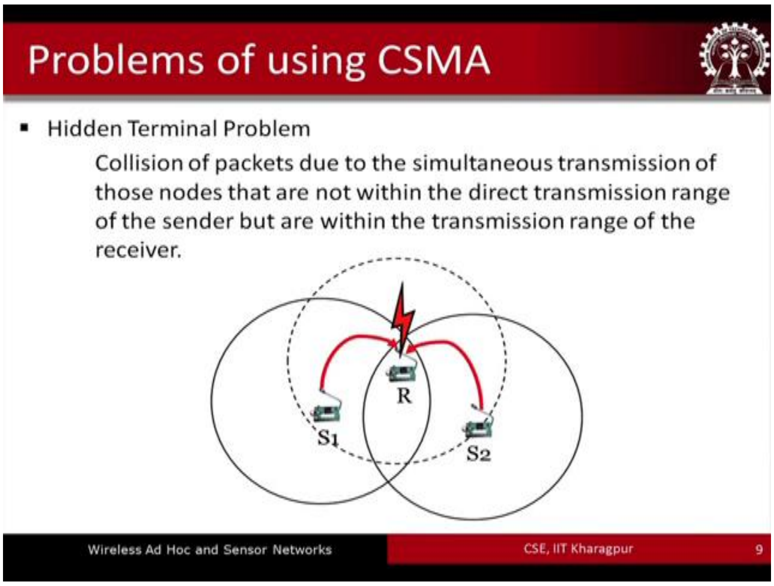
Additionally, there are other classes of protocols QoS aware protocols quality of service awareness. So, basically there are some quality of service demands of users like end to end delay you know gtor bandwidth packet loss etcetera. So, these protocols basically ensure that the there is some kind of guarantees some kind of quality of service guarantees and that can be offered while executing them; that means, while executing these protocols.

Power aware protocol basically you know as this name suggests again they are power efficient energy efficient, and you know there are many such protocols that are been proposed which are power aware one of the examples is PAMAS protocol, which is a very popular protocol which is power aware directional antenna based. So, directional antenna means like that you know. So, the signals that are transmitted are transmitted in a specific direction only. Not omni directionally not like in all the directions the signals are sent almost in equal amounts it is not like that. So, in a particular direction the signals are transmitted in a you know with a specific strength in a particular direction the signals are transmitted.

So, the nodes in other directions while using these protocols are not known to interference or collision effects. So, this is a good thing about using this kind of protocol because seldom you will have required all the nodes in all the directions for a particular node to be able to communicate with one another. So, you know if the beam is sent in a specific direction. So, that will avoid you know interference or collision problems that are common in wireless networks in between the different other nodes in the network feature surround this particular node which want to send the signal out.

Unidirectional link based these are used when differences in transmission power give rise to unidirectional links. So, that is quite understood that; that means, that in certain direction there is more power transmission power compared to the other and you know that basically leads to some kind of unidirectionality in links, and belonging to this category is belonging to this category is an example of this protocol the of this kind of protocol is the panama protocol.

(Refer Slide Time: 15:07)

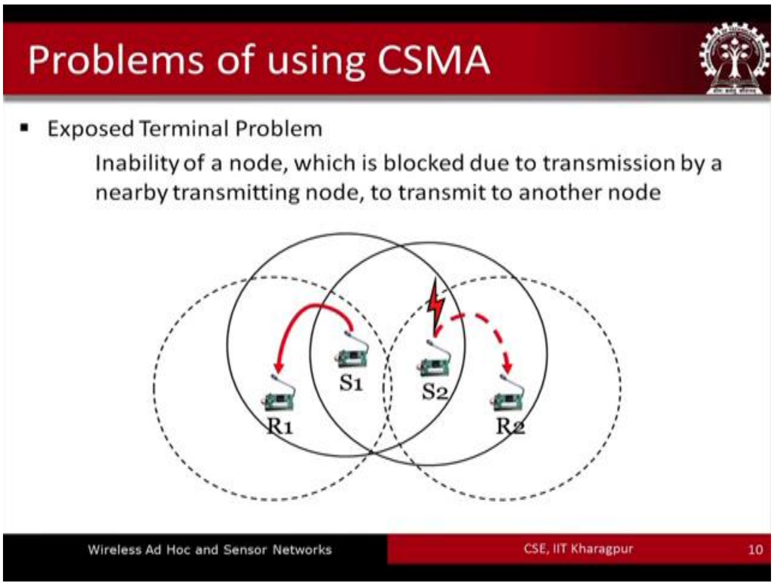


Now, let us look at some of the problems, a classical problem of you know using CSMA which is a very well known contention based protocol for use in MANETs. So, the first problem that is typically encountered while using CSMA class of protocols in MANETs is known as the hidden terminal problem. So, let us try to understand what this hidden terminal problem is. So, hidden terminal problem means that you know if there are 2 nodes which are hidden from one another, and both of who wants to send the data to a common sender. So, then what happens is there can the sender packet that are sent from each of the senders they can collide at the receiver end. So, this is and that is because these nodes which want to send the data to the common recipient, did not know that there is the other node which wants to send the packet at the same time. So, in order to understand this particular thing, let us look at this particular figure. So, what we see are 3 different nodes node S 1 with it is transmission range as soon over here in the form of the circular surrounding it. Node S 2 which again has transmission range as shown in the figure and node R which is the receiver node with it is transmission range as shown here.

So, both S 1 and S 2 they are hidden from each other. The reason is that S 2 is not within the transmission range of S 1 and vice versa that mean S 1 is not within the transmission range of S 2. Whereas, the nodes S 1 and R are and S 2 and R are which means that S 1 and R are in the direct transmission range of each other. And similarly S 2 and R are in the direct transmission range of each other. So, S 1 night attempt a transmission to R and at the same time S 2 might also attempt to do the same.

So, because S 1 and S 2 are hidden from each other they do not know that the other one other node also is attempting transmissions. So, it might so happen in the both, they both attempt transmission at the same time and at the receiver end there will be collision of packets. And collision of packets is basically a very undesirable thing. So, this is a very well known problem of using CSMA class of protocols in ad hoc networks.

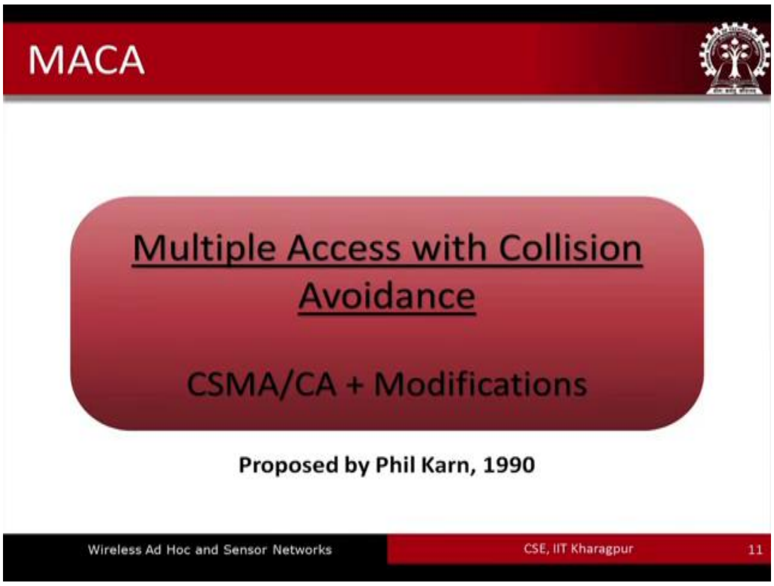
(Refer Slide Time: 17:57)



The other problem is well known and it is known as the exposed terminal problem. And exposed terminal problem again occurs because of using CSMA. So, exposed terminal problem is basically you know what it means is the inability of a node which is blocked due to transmission by a nearby transmitting node to transmit to another node. So, the problem is you see if we look at this figure once again there is a you know. So, here unlike the previous case here what we have are push 2 senders and 2 receivers sender, S 1 and S 2 and receivers R 1 and R 2, and who is within the transmission range of whom of these 4 nodes is something that we can infer by looking at this particular figure. So, in this particular case what we have S 1 and R, they are in the direct transmission range of each other similarly S 2 and R 2 and also S 1 and S 2.

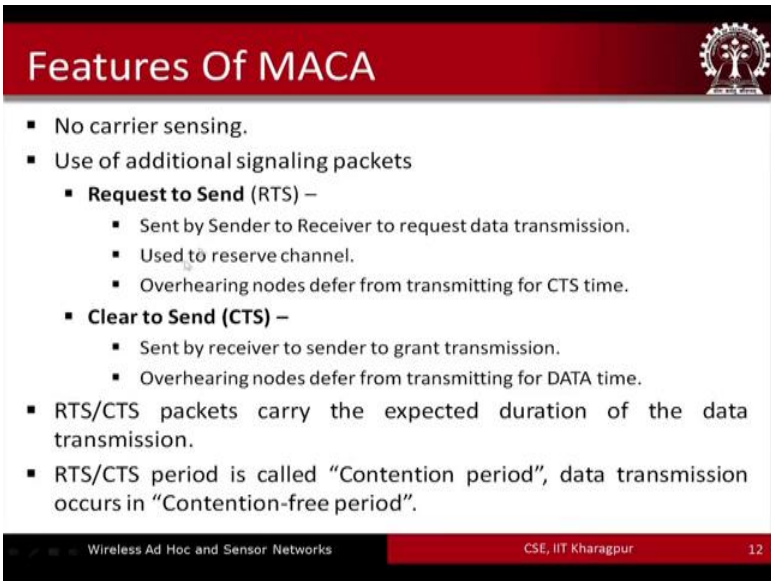
So, we have perfect case of multi hop communication that we discussed in a previous lecture. So, as we can see over here that when S 1 transmits to R 1 node S 2 is exposed to it is transmission because S 2 is within the direct transmission range of S 1. So, what we have is because the node S 2 is within the direct transmission range of S 1. It feels that it is exposed to it is transmission. So, it feels that there is another transmission going on and consequently it is going to differ it is transmission to R 2 unnecessarily. Although it is unnecessary because it was not required, because S 1 was sending to R 1 and S 2 was sending to R 2 to and R 1 and R 2 are 2 different receiver nodes, which again are not within the direct transmission range of each other. So, this is called the exposed terminal problem.

(Refer Slide Time: 20:08)



Now, let us look at some of the well known solutions that have been proposed. The first one is the MACA protocol which was proposed by Phil Karn 1990.

(Refer Slide Time: 20:19)



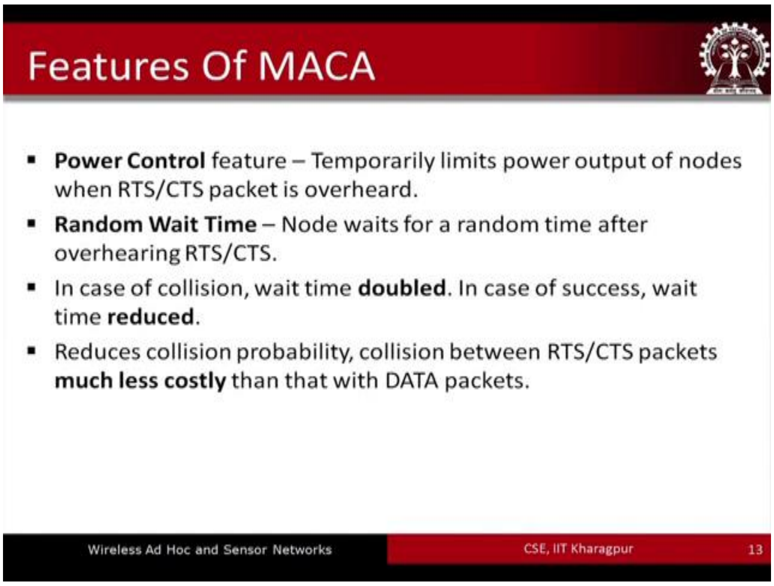
So, there are different features of the MACA protocol. So, here MACA is quite similar to the CSMSCA, because here what it does is it uses the well known RTS CTS control signaling packet RTS, CTS. RTS stands for request to send and CTS for clear to send. So, these are 2 additional signaling packets that are sent before actually sending the data. So, RTS basically is sent by the sender to the receiver to request the data transmission sent by the sender to the receiver. So, it is you know sender is notifying the receiver that it wants to send some data to the receiver, and by this way what it is trying to do is before actually sending the data out it is indirectly trying to reserve the channel for it is data communication.

So, what happens is the over hearing nodes will differ the transmission for CTS duration of time. And the CTS packet is sent by the receiver to the sender to grant transmission. And here the over hearing nodes would differ transmission for data units of time. So, these RTS and CTS packets, if you look at their packet format they basically one of the fields is expected duration of data transmission. So, when the RTS packet is sent out along with it the receiver also knows that how long the sender intends to send the data out, the expected duration of the data transmission is also notified to the receiver.

And CTS by sending the CTS back the sender basically confirms that it now knows that this is the expected duration of time, plus it is what it is going to do is by sending the CTS packet it is going to differ you know. So, it is notifying the sender that you know it gets; that means, the sender gets the permission to send that data out and the over hearing nodes; that means, the nodes which are getting you know over hearing this transmission; that means, the nodes which are in the range of the receiver for instance. So, direct transmission range they are going to differ the transmission for that particular duration of time.

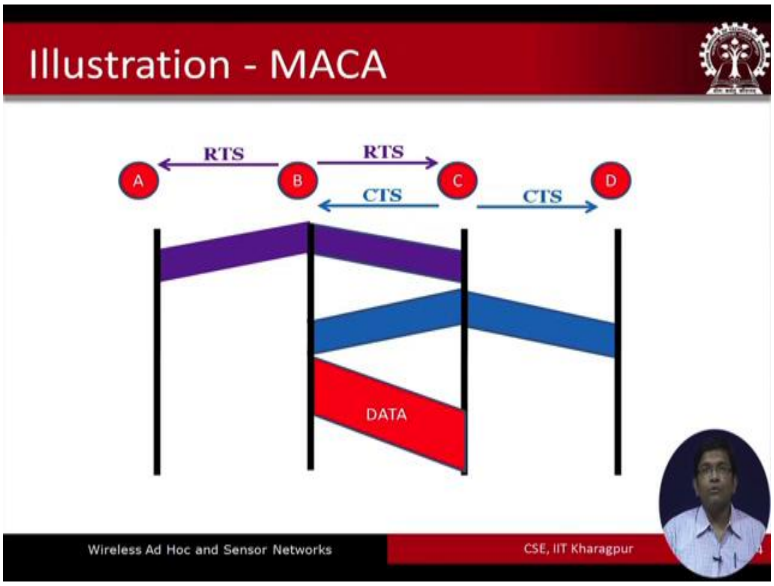
So, this RTS CTS period are known as technically these are known as the contention period. And the details transmission basically actually occurs during the contention free period. So, during the contention period the RTS CTS exchange takes on and in the contention free period the actual date transmission goes on.

(Refer Slide Time: 23:31)



So, MACA has different features which I am not going to go through one by one, but let me just mention one thing that even after using MACA, if there is a case of collision then what MACA suggests is that the wait time. It should be doubled. So, if there is a collision you double the wait time if it is a success case of success; that means, the packet transmission went through successfully without any collision then the wait time should be reduced. So, this by doing this basically what you do is you try or MACA tries to reduce the collision probability.

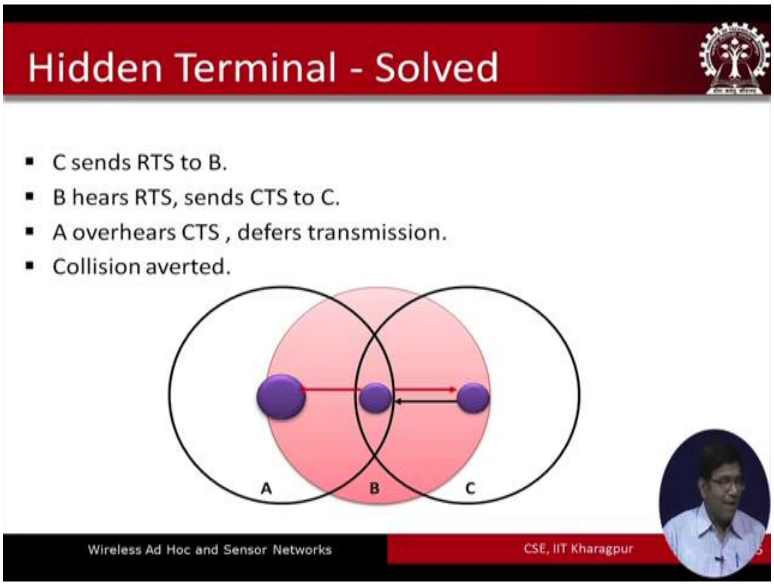
(Refer Slide Time: 24:16)



Let us now look at the basic functioning of MACA. The main steps that are proposed for MAC a. So, as you can see that it will be a very primitive form of contention based medium access. So, first node B. So, we have a scenario where we have 4 nodes A B C and D. So, let us assume that node B first sends RTS to node A. B sends RTS to A, a copy of it is received at node C because it is exposed to the transmission of node B. Then node C what it does is it sends ACTS back it is sends ACTS back to B.

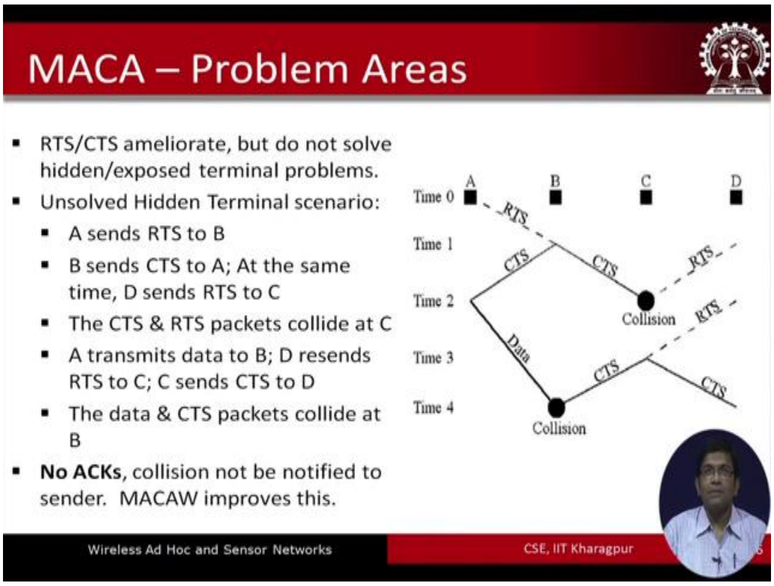
So, let me just let me just clarify this once again. So, what happens is we have a scenario A B C D. So, node B wants to send a packet to C before it does. So, first it sends RTS to C the node C basically sends the CTS back and the copies of the RTS and the CTS are overheard by nodes a and B. And after these RTS CTS exchange node B basically sends the data to the node C. So, this is the RTS CTS hand shaking followed by you know followed by that there is data transmission.

(Refer Slide Time: 25:55)



So, in a way basically the traditional the classical problem of hidden terminal is solved using the MACA protocol in this way. So, C sends RTS in this particular scenario to B; that means, C wants to send some data to B, but before doing that it sends a request to send that packet to B. B hears the RTS sends the CTS back to C. A over hears the particular transmission of the CTS and A basically differs it is transmission and this is how the collision is averted through the use of RTS CTS.

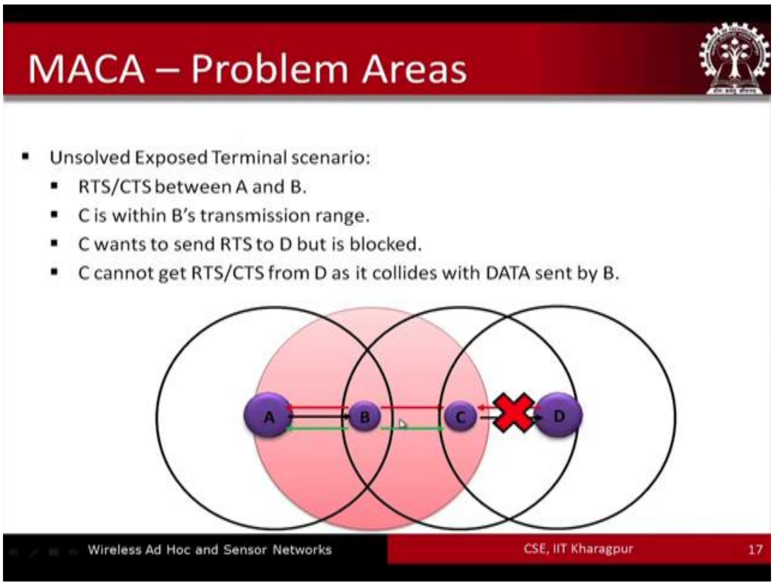
(Refer Slide Time: 26:40)



Having said that we cannot completely say that MACA solves all the problems; that means, the RTS CTS data exchange solves all the problems. RTS CTS basically reduces the problems, but do not fully solve the hidden and exposed terminal problem. So, let us look at this particular scenario. So, we have nodes A B C and D A B C and D and there is, so, let us look at the scenario like this, that we have node A node A which sends RTS to B, B sends CTS to A and at the same time D sends in this particular example D sends an RTS to c. So, as we can see over here that there is going to be case of collision at C between this RTC packet that is sent by D and the copy; that means, the overheard CTS packet that was sent by B to A. So, between this packet CTS and this RTS there is going to be a collision at node C

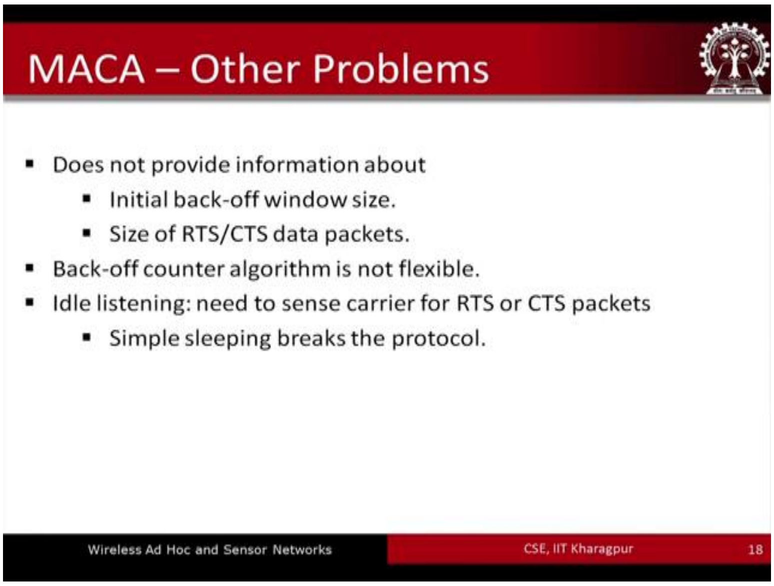
So, the other cases is that after this data is sent and let us say that at this particular time instant, the data is received at node B. So, here again corresponding to this particular RTS the CTS might be sent back and a copy of it will be received at B. So, this particular in this particular case what we can see is that there is a chance of collision between this particular data packet and this particular CTS packet.

(Refer Slide Time: 28:50)

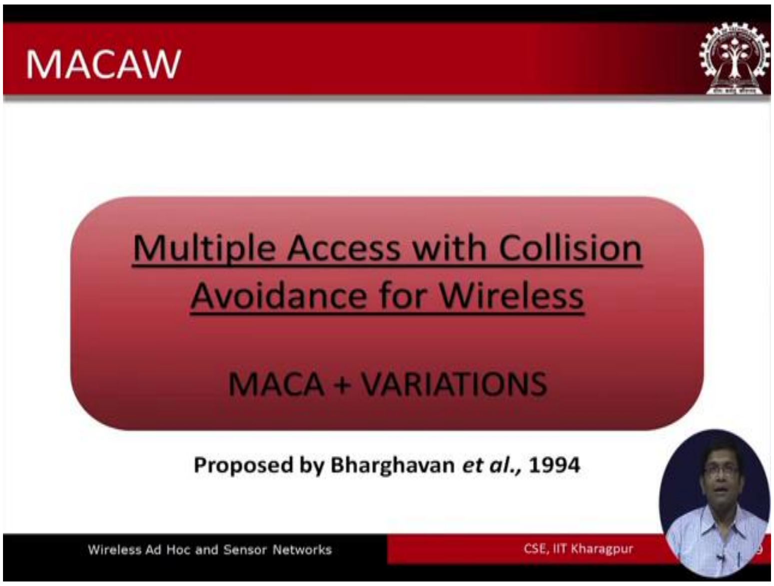


So, let us now look at the other problem areas unsolved exposed terminal scenario. So, let us say that we have 4 nodes A B C and D once again. So, there is RTS CTS between exchange RTS CTS exchange between A and B RTS CTS as we can see over here. So, C node C is within the direct transmission range of node B. C at the same time wants to send ARTS to B C C wants to send RTS to D. And, but it is blocked from doing it doing. So, because it is exposed to the transmission of B. So, cannot get RTS CTS from D as it collides with data sent by B.

(Refer Slide Time: 29:42)



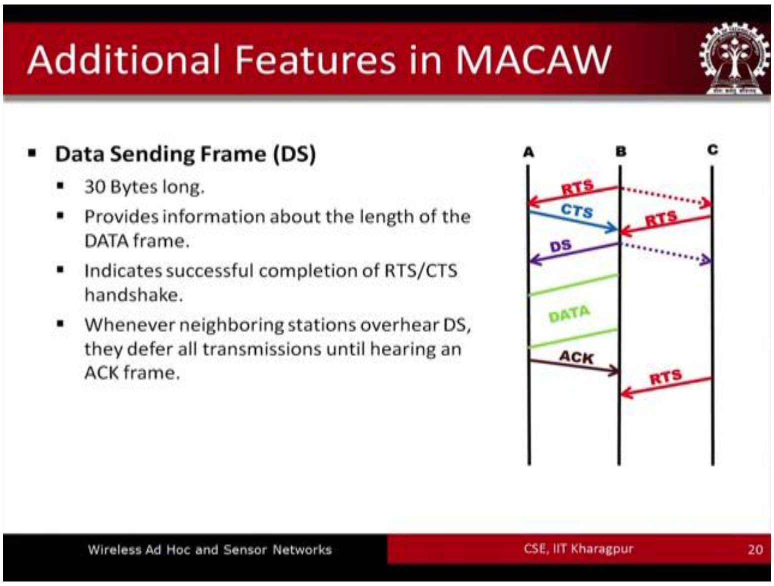
(Refer Slide Time: 29:53)



So, MACA also has other problems which I am going to not go through in detail. So, it is available for you to have a look. So, it is look at another protocol an advanced protocol which is better in some respects than the traditional MACA, and it is known as the MACAW.

So, it was proposed by Bharghavan et al in 1990 four.

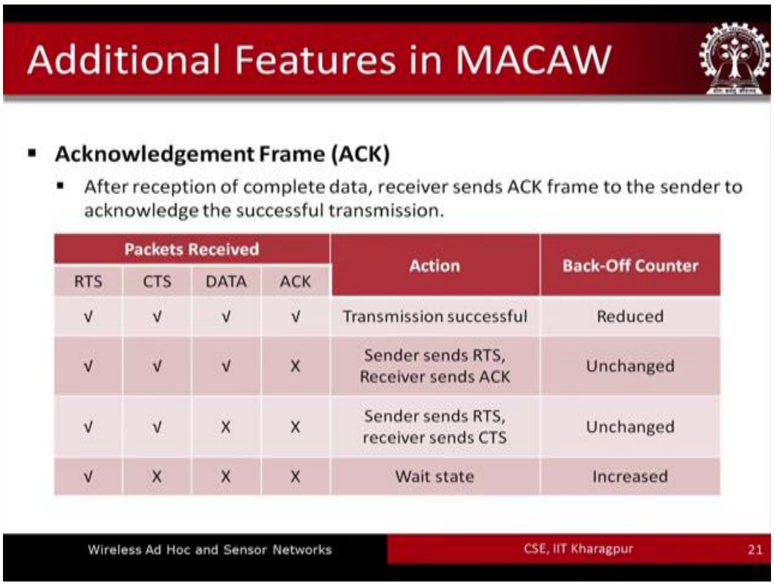
(Refer Slide Time: 30:09)



So, in this case in MACAW. So, in the case of MACA as we have seen that it was RTS CTS and data exchange. So, in this particular case there are 2 new packets data sent one is called the DS frame not packets sorry frames because the PDO in the MAC layer is termed as the frame right. So, not a packet is the name of the PDO in the network layer. So, data sending frame DS frame is sent it is used. So, it is basically 30 bytes long it provides information about the length of the data frame. And it indicates successful completion of the RTS CTS handshake this is like this that B sense RTS gets the CTS back and after that before actually sending the data out. So, this DS frame is sent. And the purpose of the DS frame is to provide information about the length of the data frame that is actually going to be sent by the sender node. So, the DS frame will notify the receiver node that this is going to be the expected length of the data frame.

And this also signifies that the RTS CTS handshaking was completed successfully. So, what happens is when, so, this DS frame is sent and it is over heard by the neighbors. So, node C also gets a copy of it. So, whenever the neighboring stations like node C over hear the data send packet; that means, the DS packet DS frame, this send all the transmission until hearing they differ all the transmissions until hearing the acknowledgement frame. So, as we can see over here. So, transmissions are deferred until the acknowledgement frame is received. So, the data was sent an acknowledgement was received by node B and only after that you know the RTS packet RTS frame is going to be sent.

(Refer Slide Time: 32:28)

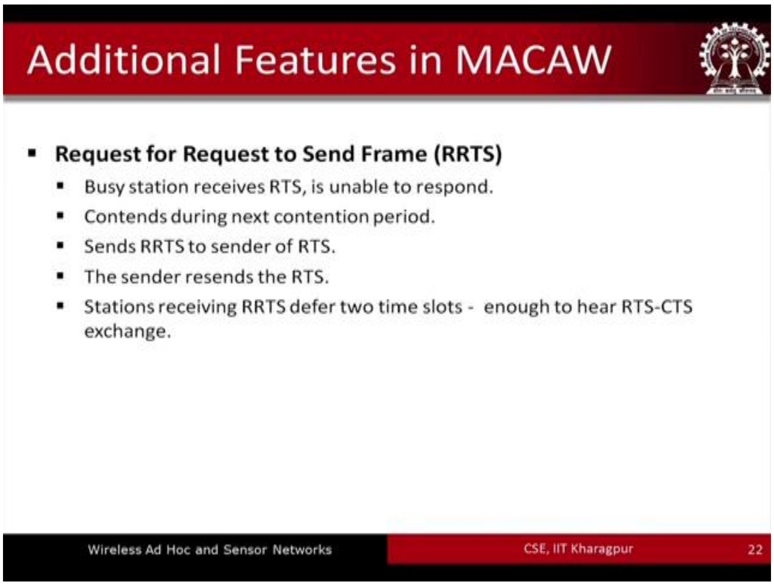


Packets Received				Action	Back-Off Counter
RTS	CTS	DATA	ACK		
√	√	√	√	Transmission successful	Reduced
√	√	√	X	Sender sends RTS, Receiver sends ACK	Unchanged
√	√	X	X	Sender sends RTS, receiver sends CTS	Unchanged
√	X	X	X	Wait state	Increased

So, the acknowledgement frame depending on the issue; that means, the frame that are received. So, let us look at this particular scenario. So, we have the case like you know the RTS. If the RTS CTS data and acknowledgement all these transmissions are successful. Then the action suggested by MACAW is that transmission is successful and the back off counter be reduced. If RTS CTS and data are successful, but acknowledgement is unsuccessful to send the basically sends the RTS and the receiver then sends the acknowledgement and the back off can counter in this case is remained unchanged is kept unchanged.

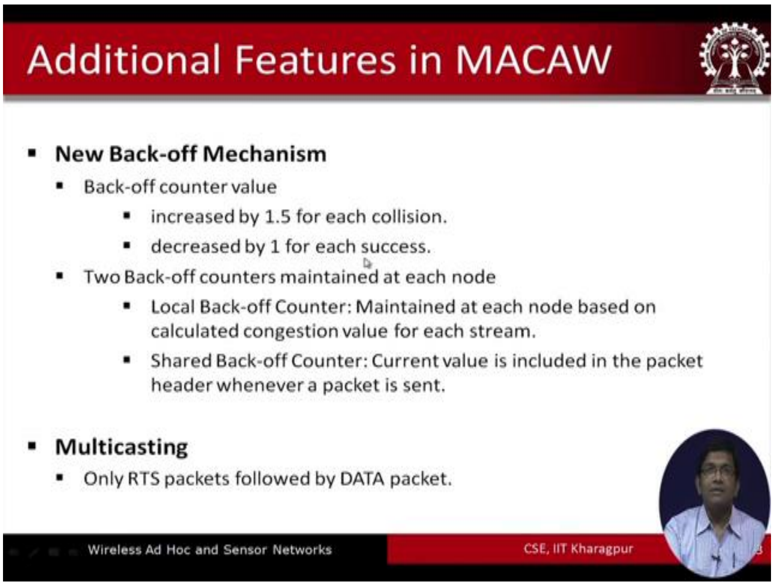
If RTS is successful CTS is successful, but data and acknowledgments are not then the sender sends the RTS receiver sends the CTS and the back off counter is unchanged. If the RTS is successful, all the other are not then the action becomes putting the sender in the wait state and the back off counter is increased.

(Refer Slide Time: 33:48)



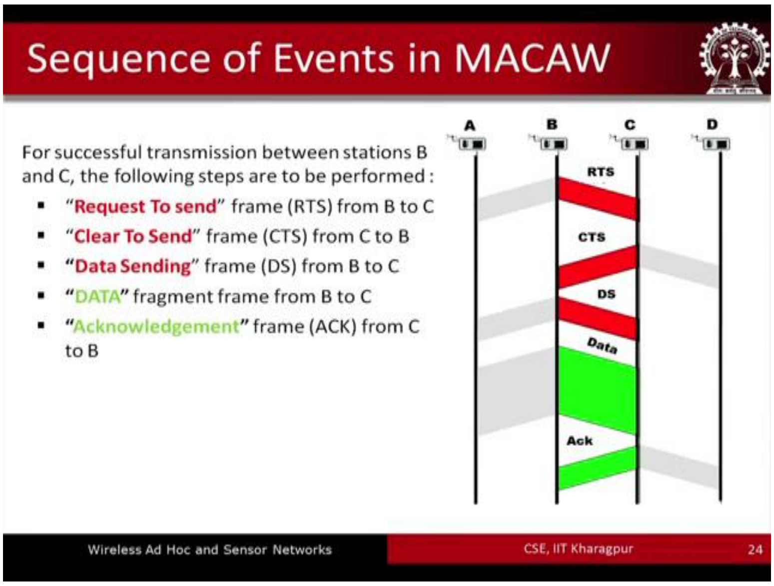
So, very another additional feature in MACAW, that is the use of the RRTS frame RRTS. Basically stands for request for request to send frame right. So, basically when the busy station receives the RTS, that it is unable to respond it is unable to respond. Because the busy station you know it is already busy you know it knows that there is some other transmission that is going on and it receives the RTS. So, what MACAW says is that the busy station they know that there is another station which is attempting transmission. So, what it will do is when this busy station becomes free it proactively sends the RRTS to the sender of the RTS. And this sender basically sends the RTS and then the regular mechanisms of RTS CTS data exchange is carried out.

(Refer Slide Time: 34:51)



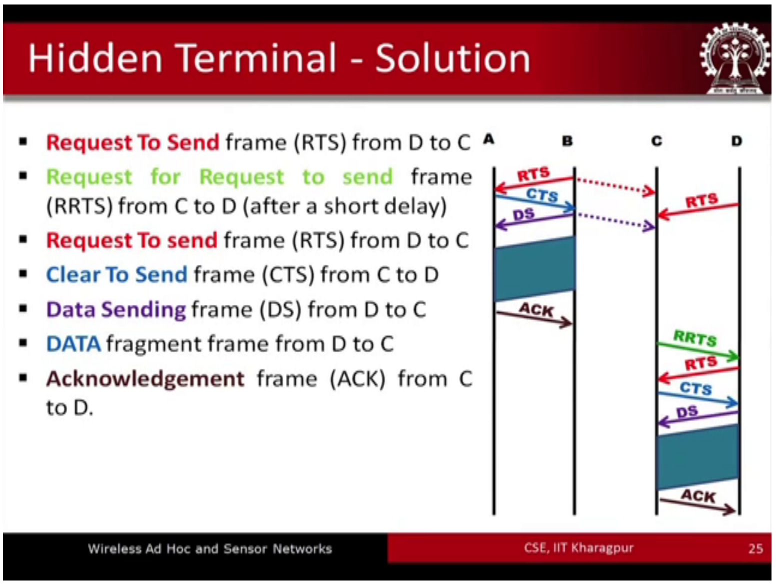
So, MACAW again proposes few other additional improvements. So, the back off mechanism is improved so; that means, that if there is a collision then the back off counter value is increased one and a half times. If it is a case of success, then it is decreased by one unit. So, there are other different you know different mechanisms in the new back of you know back of mechanism that is proposed by MACAW and their other features that are also proposed.

(Refer Slide Time: 35:27)



Now, let me highlight a simple sequence of a case of sequence of events in MACAW. So, RTS CTS DS data acknowledgement. So, this is basically a sequence or chain of packet frame exchanges that go on between the sender and the receiver that is B and C in this particular case. And as we can see over here these other neighboring nodes they are exposed to the transmission; that means, A and D are exposed to the transmission from B and C.

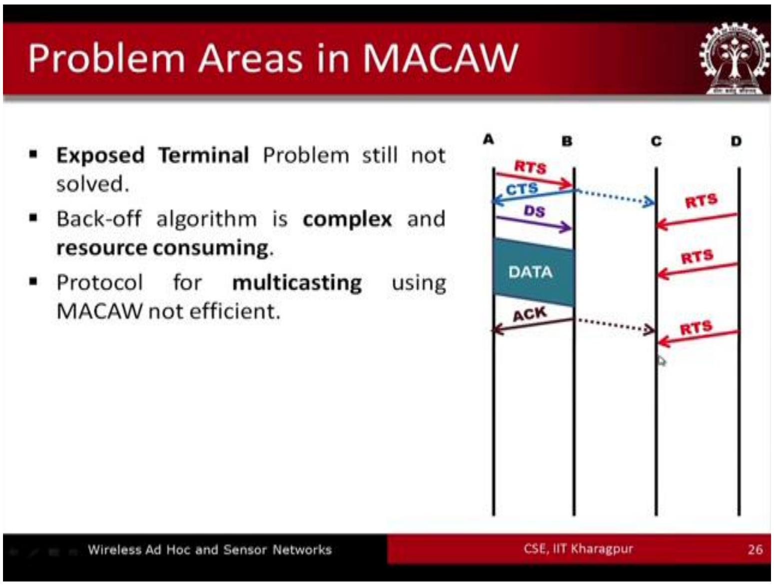
(Refer Slide Time: 36:06)



So, how does this solve the R solve the hidden terminal problem. So, we can see over here that we have the RTS sent CTS sent back DS and then the data are sent acknowledgement is received. So, after that basically. So the nodes C was in the busy state because it knew that there is some kind of transmission that was going on. So, when there was a ARTS packet RTS frame which was sent by another node D. It was not able to respond back, but at the same time it knew that D was attempting transmission; that means, he knew that D was attempting transmission.

So, what it will do it after the completion of this chain of this chain of data frame the chain of frame exchanges control and data frame exchanges then C because it knew that RTS was attempted by D it is going to proactively sent RRTS packet RRTS frame to D. Then D on receiving that RRTS will send the RTS that it was attempting to send earlier and then the CTS DS data and acknowledgement. So, the acknowledgement is sent out at the end of the transmission of the actual data frame.

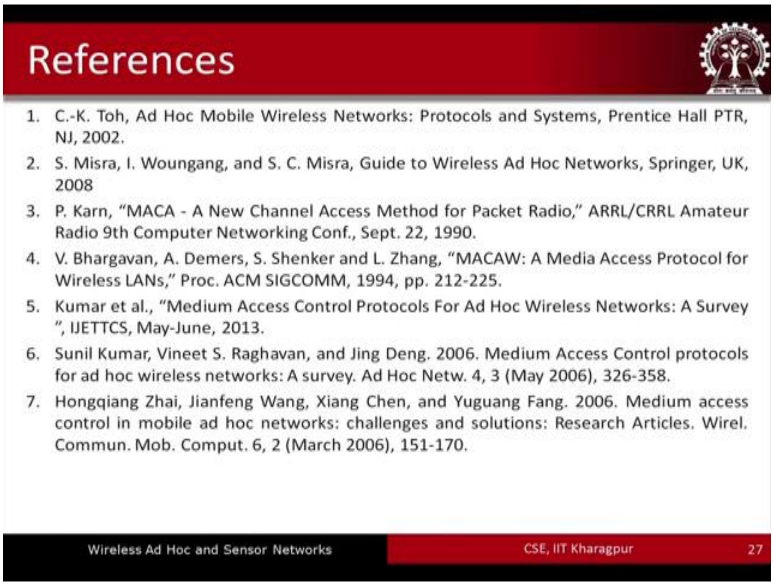
(Refer Slide Time: 37:39)



But still there are other problem areas that are still remaining with the help of MACAW. So, we are not going to go through it in detail over here, but I think this figure having gone through the features once. I feel that the figure is quite you know quite easy to understand and you know. So, what we have over here is RTS was attempted it you know nothing was happening again RTS was attempted. Because he knows that there is some other transmission that was going on.

So, it did not do anything. So, C is the exposed terminal over here. So, the exposed terminal problem is still not solved using MACAW right. So, RTS will be sent again and again and the final RTS will be received; that means, after these basically the CTS can be sent back because the acknowledgement C has got a copy of the acknowledgement frame that was sent by B to A. So, then after that only it can be received by C and correspondingly it will be shifted back by CTS back to D.

(Refer Slide Time: 38:49)



So, with this we come to an end of the first part of MAC protocols for ad hoc networks. So, these are some of the references that have been given to you. So, the first 2 references are definitely quite useful these are the 2 books that are available quite widely. And there are few other papers which might be of interest to you to read. So, with this we come to an end of the first part of are the MAC protocols for MANETs.

Thank you.