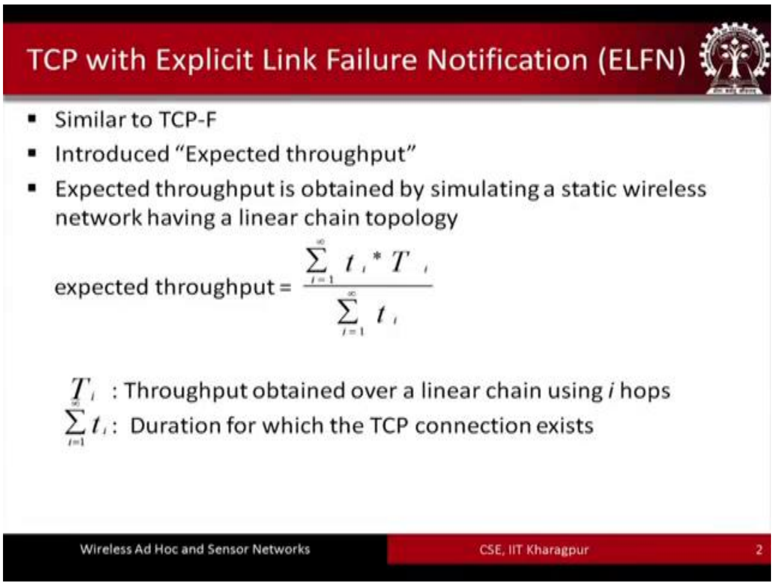
Wireless Ad Hoc and Sensor Networks
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 14
Transport Protocols for MANETs-Part-II

(Refer Slide Time: 00:26)

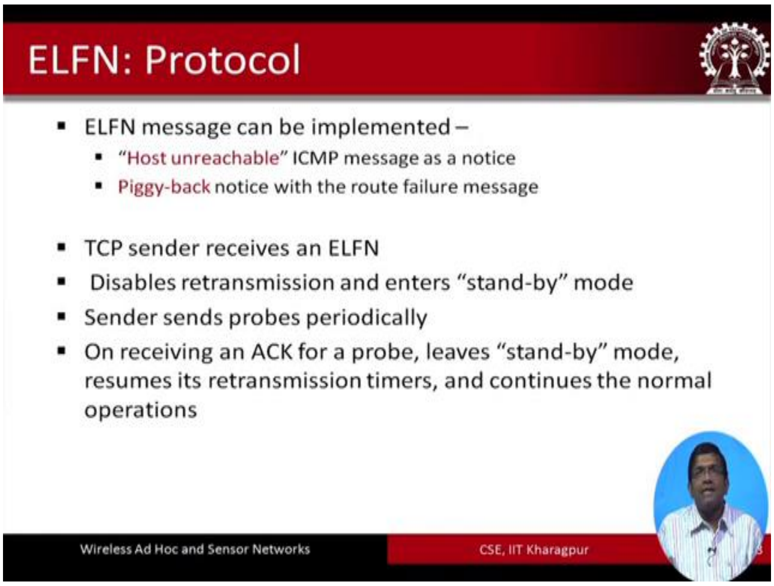


Transport Protocol for mobile Ad Hoc networks part II. We will now go through another protocol; another transport protocol that has been designed for use in MANETs. We have already gone through in the first part of transport protocols; we have gone through the protocol TCP-F which has been designed specifically for MANETs, taking into consideration some of the issues that would arise in using the regular TCP in MANETs. So, here is the second protocol which is called the ELFN.

So, the ELFN protocol is basically very similar in functionality to the TCP-F protocol the TCP feedback protocol that we have already gone through. So, in ELFN basically the concept of expected throughput is introduced and this expected throughput is a formula that is given by the authors it is obtained; this expected throughput is obtained by simulating a static wireless network using a linear chain topology. So, that the topology that is used is a linear chain topology; that means, all the nodes starting from the source to the destination, there is a chain of nodes all in one line. So, that kind of topology very simple kind of topology is considered and using that topology analytically mathematically the authors came up with this formula for expected throughput.

So, basically it is a function of 2 different things. One is the duration for which the TCP connection exists the duration for which the TCP connection exists and the throughput obtained over a linear chain using i hops because it is a multi hop network. So, over i hops in number of hops i number of hops what is a throughput that is obtained using this kind of topology.

(Refer Slide Time: 02:27)



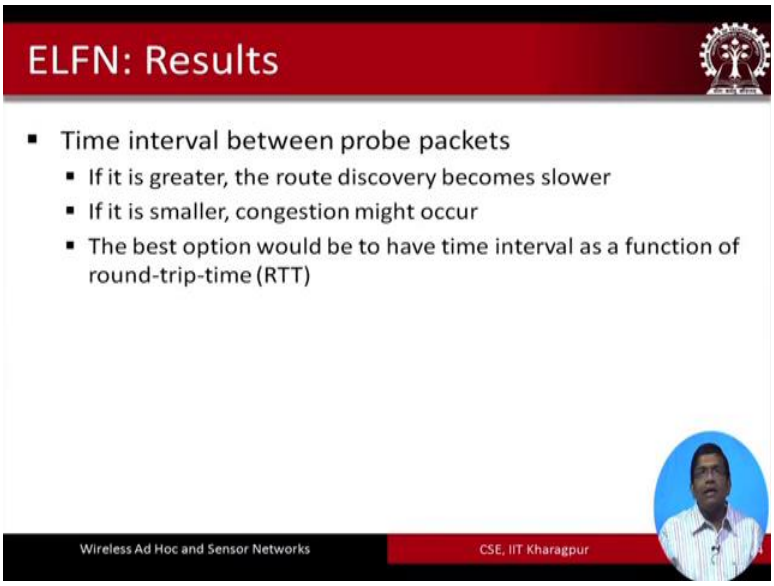
So, ELFN message can be either implemented using the host unreachable ICMP message as a notice because ICMP is running on bottom. So, I either; you know it can be you know the one can use the host unreachable message of ICMP for informing explicitly to the sender or this notification this explicit notification the failure notification.

Can also be sent through the through a piggybacked mechanism. So, basically with the message the failure message that goes this failure notification can also be piggybacked. The TCP sender basically receives this message the ELFN message which can be sent using either the host unreachable ICMP message or the piggyback mechanism that we have just seen. So, the TCP sender receives this message disables the retransmission and enters the standby mode, the sender sends the probes periodically on receiving an acknowledgment for the probe it leaves the standby mode resumes its retransmission timers and continues the normal operation. So, you see that this part of it is quite similar to TCP-F. So, it is all about.

So, earlier in TCP-F we talked about the smooth state here it is talking about ELFN it is talking about the standby state in the standby state the transmission is disabled it is closed it is you know it is suspended, but one thing is different that here the sender basically periodically it is going to send some probes and when the sender receives an acknowledgement for the probe it is going to transit from the standby mode and it is going to continue in the normal mode.

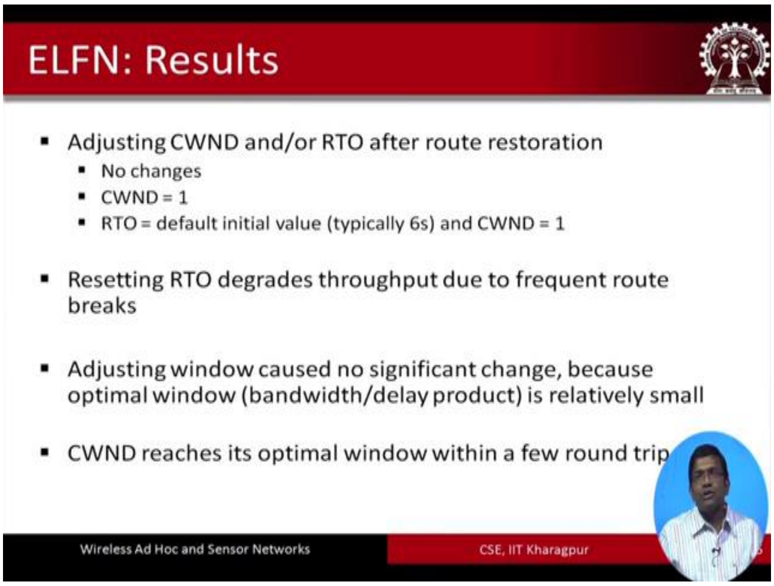
The time interval between these probe packets because you see that periodically the probes are being sent. So, how often you are going to send these probes.

(Refer Slide Time: 04:41)



So, if it is too much if it is too big then the route discovery becomes slower if it is smaller than quite evidently congestion might occurred and so what is suggested by the authors is that the best option would be to have the time interval as a function of the RTT.

(Refer Slide Time: 05:20)

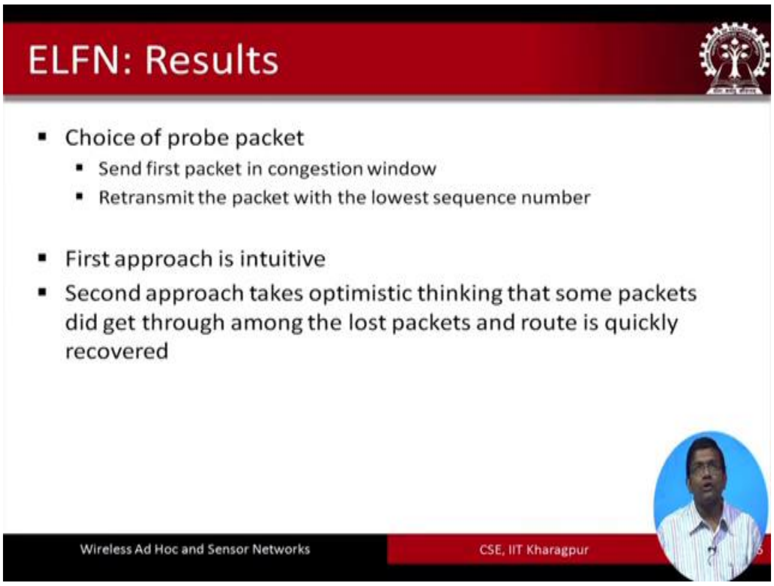


So, after the route restoration is done at the network layer then at the transport layer the congestion window and the RTO values, congestion window size c window size and the RTO values have to be reset they have to be readjusted they have to be adjusted. So, this is these are the 3 different ways the adjustments can be made. So, first of all the basic thing that do not make any adjustments at all the second is that set the congestion window size to unity one. The third is that set the congestion window to one and the RTO to a default initial value which in the paper they have shown that it is better to use 6 seconds.

Resetting the RTO basically degrades the throughput due to frequent route breaks and this is quite obvious that resetting of the RTO is not a very good option because there will be more you know frequent if there is frequent route breaks then frequently the retransmission timeout timer is going to be invoked and if that is going to be invoked; obviously, the throughput is going to be reduced. Adjusting the window caused causes no significant change because optimal window is window size; that means, optimal window size is a product of the bandwidth and the delay.

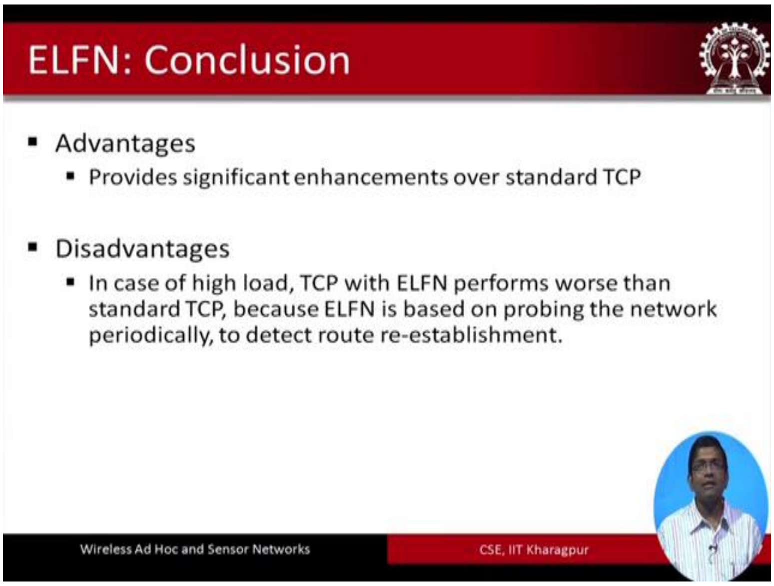
So, this is something that we know from our basic understanding of in at CP for the internet. So, the optimal window size is a product of the bandwidth and the delay bandwidth delay product basically governs the optimal window size and that is going to be relatively small the congestion window size reaches its optimal value within a few round trip time seconds.

(Refer Slide Time: 07:25)



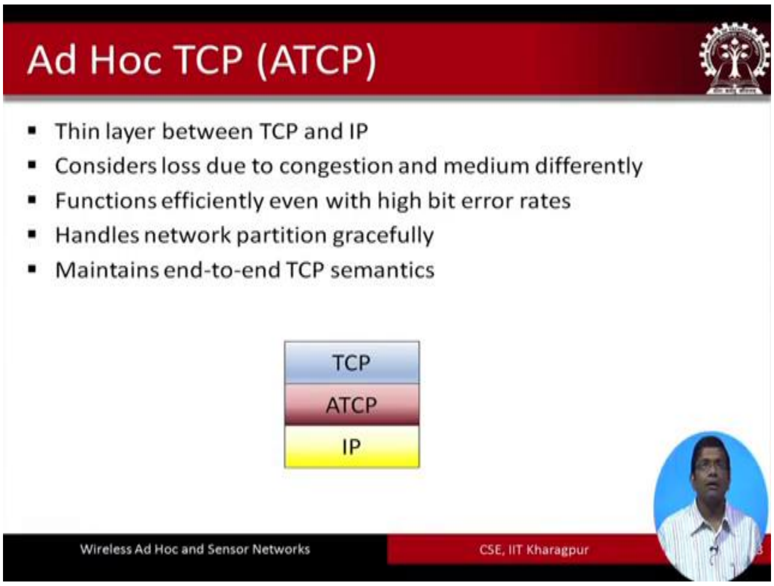
Now, the choice of the probe packets one possibility is that you send the first packet in the congestion window retransmits the packet with the lowest sequence number. So, these are the 2 different choices. So, using the first approach is quite intuitive the second approach basically takes an optimistic thinking that some packets did get through among the lost packets and the route is quickly recovered.

(Refer Slide Time: 07:59)



The advantages of using ELFN is that it provides significant enhancements over the standard TCP, the disadvantage is that in case of high load TCP with ELFN performs worse than the standard TCP because ELFN is based on probing the network periodically and that basically leads to more overhead which again will indirectly affect the overall delay in the network and as I hold the overall performance in the network.

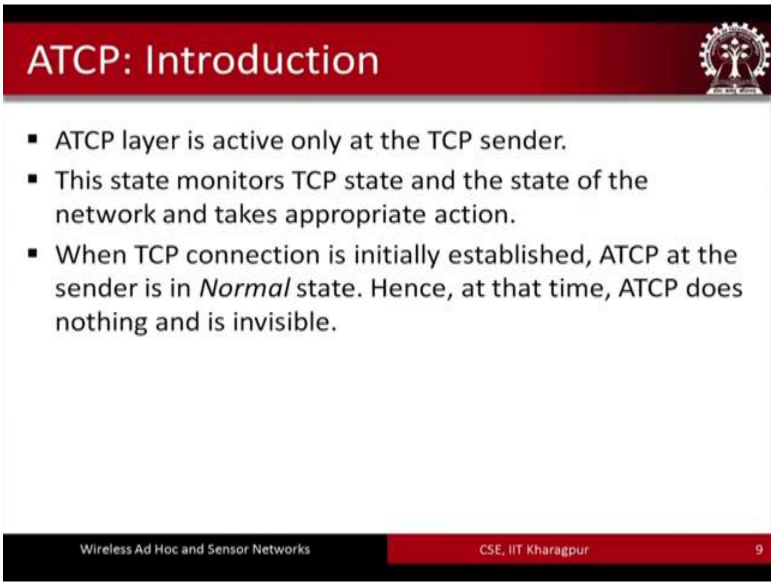
(Refer Slide Time: 08:33)



The next protocol; so we have already gone through the TCP-F, ELFN and the next protocol that we are going to go through and the features of it only is the ATCP ad hoc TCP protocol. So, characteristically ATCP is not a separate protocol by itself. So, ATCP is like a thin layer which basically has been introduced between the IP; that means, the network layer and the transport layer. So, it is like a thin layer as we can see in the figure in front of us. So, this is a thin layer lying between IP and TCP. So, the ATCP is sort of like the way it is designed is it is sort of like a broker, a broker which observes the network conditions and on the basis of that it is going to control the functioning of the TCP.

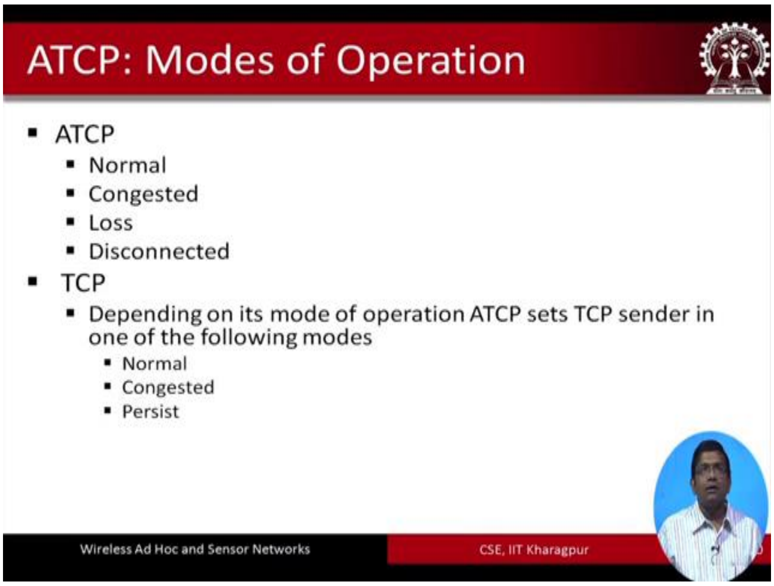
So, the distinction between the ATCP protocol and the previous protocols like TCP-F and ELFN is that here ATCP has been introduced as a layer which basically does not touch the TCP. So, it lets TCP function the way it is supposed to function the normal TCP for internet the way it is supposed to function it lets it function that way, but over here it keeps on observing the network conditions and based on the network conditions it is going to keep a control on the functioning of the TCP the regular TCP.

(Refer Slide Time: 10:33)



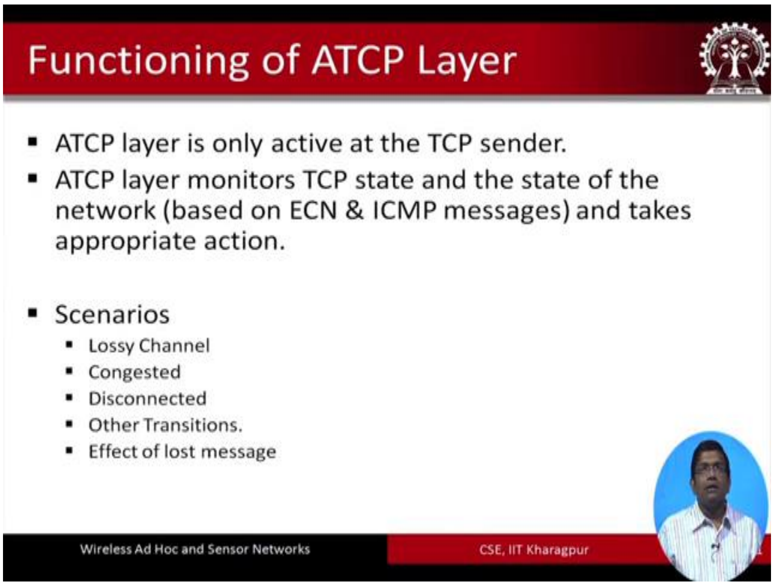
The TCP layer is active only at the TCP sender, so this is another thing. So, ATCP is introduced only at the sender. So, this state monitors; that means, the ATCP basically monitors the TCP state and the state of the network and takes the appropriate action when TCP connection is initially established ATCP at the sender is in the normal state hence at that time ATCP does nothing and is invisible.

(Refer Slide Time: 11:05)



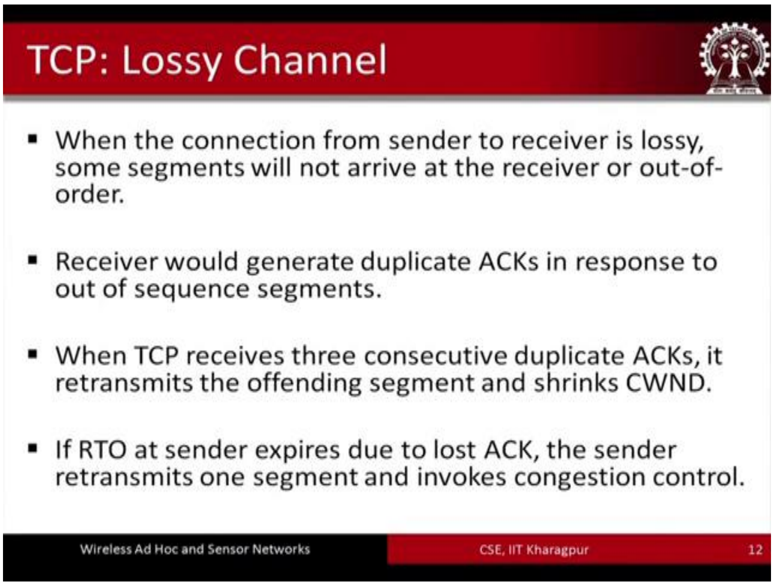
ATCP can operate in any of these modes normal congested loss and disconnected. So, I will show you what each of these modes of operation do. TCP depending on its mode of operation ATCP sets the TCP sender to one of the following modes. So, depending on the mode of operation the above modes of operation normal congested loss and disconnected ATCP what it will do is it will basically control the TCP sender and it will put it in any of these modes TCP goes to any of these modes normal congested and persist.

(Refer Slide Time: 11:52)



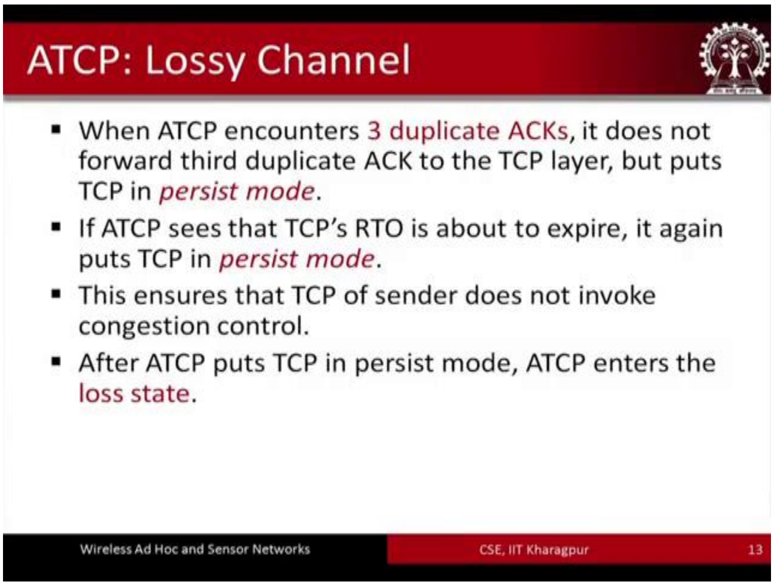
So, ATCP layer is only active at the TCP sender ATCP layer monitors the TCP state and the state of the network and takes an appropriate action. So, there could be different scenarios that might be encountered when using ATCP these scenarios we are going to go through one by one lossy channel, congested, disconnected, other transitions and effect of lost message. So, one by one we are going to go through them.

(Refer Slide Time: 12:22)



So, first a lossy general scenario; so, when the connection from the sender to the receiver is lossy some segments will not arrive at the receiver or they are going to arrive out of sequence the receiver would generate duplicate acknowledgments in response to the out of sequence segments. When the TCP receives these 3 consecutive acknowledgments it retransmits the offending segment and shrinks the congestion window size because it thinks that it is a case of congestion. If RTO and the sender expire due to the lost acknowledgement the sender retransmits one segment and invokes the congestion control when ATCP encounters 3 duplicate ACKs; that means, the 3 acknowledgments.

(Refer Slide Time: 13:14)

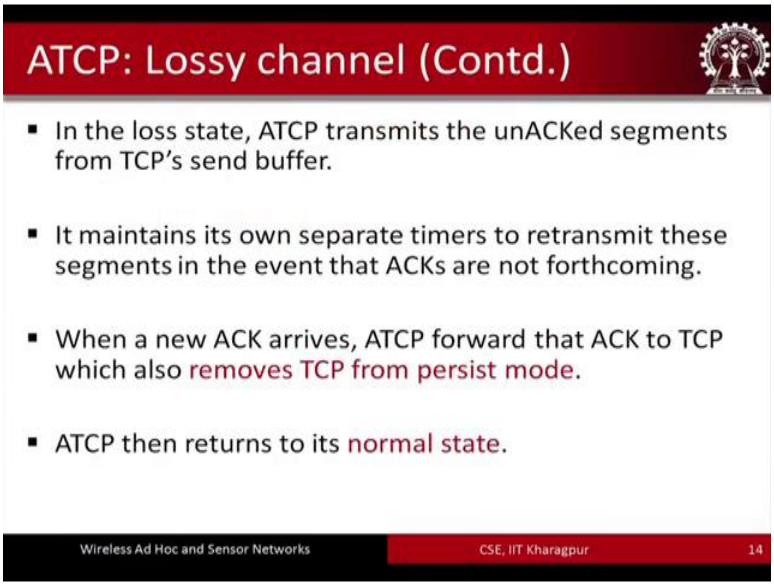


So, this is basically the previous thing is what normally happens in the case of TCP used in the case of lossy channel. So, in the case of lossy channel basically 3 acknowledgments TCP thinks that 3 acknowledgments means it is a congestion case and it invokes congestion control mechanisms it will shrink the congestion window size maybe it will bring it down to one so; that means, that you send one segment get a get an acknowledgment back send the second segment get another acknowledgment back and so on, so; that means, that it is going to overall it is going to put reduce the overall; throughput of the network.

So, what? So, this is what normal TCP would do? So, now, what ATCP does in such a lossy channel is that when ATCP which is sitting just below TCP it gets 3 acknowledgments it does not 3 duplicate acknowledgement; that means, that in the same acknowledgment 3 times, 3 times the same acknowledgment. It does not forward that third duplicate acknowledgment to the TCP layer it will not forward this that that acknowledgment because it is a duplicate acknowledgment and it puts the TCP in the persist mode. So, this is the overall philosophy in which by which TCP is able to ATCP is able to handle the lossy channel. So, it is what it is doing is it is observing that 3 acknowledgments have come. So, then I should not inform this to the TCP and I will sit here and I will just what I will do is I will control. I will change the TCP to the persist mode.

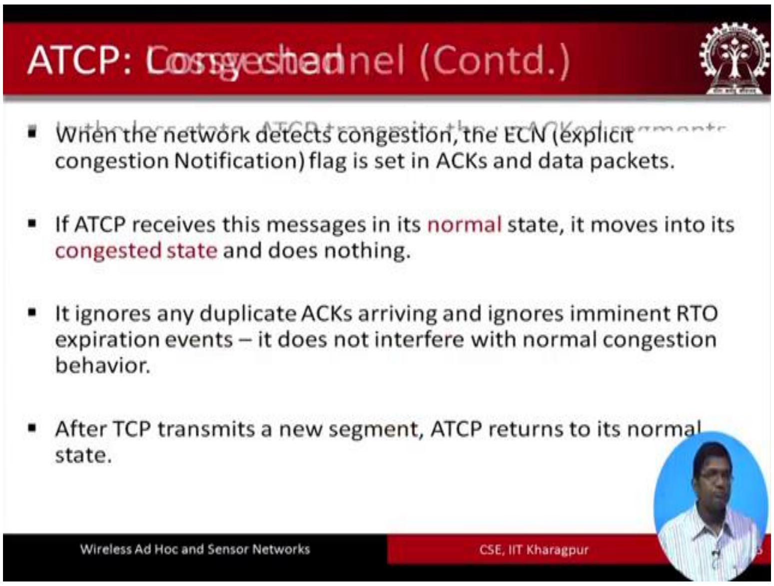
If ATCP sees that TCP is RTO is about to expire it again puts TCP in the persist mode and this ensures that our TCP of the sender does not invoke the congestion control after TCP puts TCP in the persist mode ATCP enters the loss state. So, persist modes by the way is something that is there if you recall in the normal this mode is there in the normal TCP. So, persist mode is like you know frozen kind of mode right normal mode. So, after ATCP puts TCP to the persist mode ATCP enters the loss state. So, what is ATCP doing? 3 acknowledgments inform TCP to go to the persist mode and it itself it is going to go to the loss state. So, this is what ATCP does in the case of you know using it in the case of lossy channels.

(Refer Slide Time: 16:02)



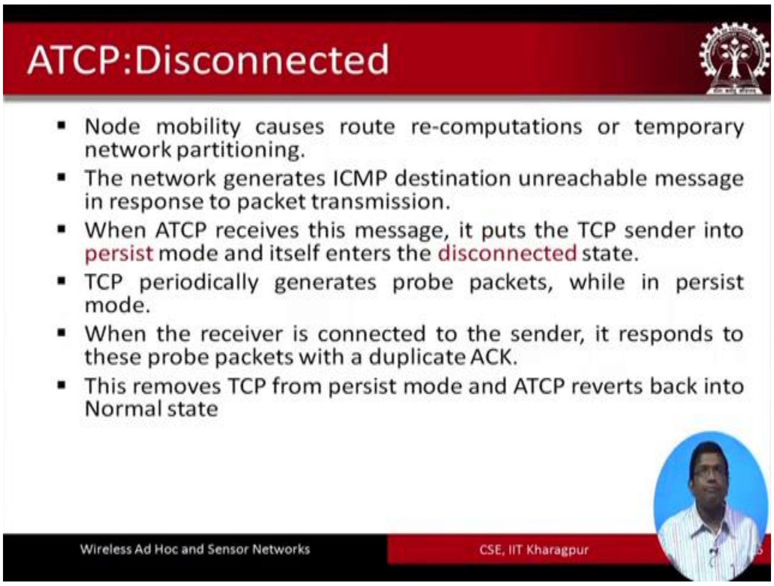
In the loss state ATCP transmits the unacknowledged segments from the TCPs send buffer it maintains its own separate timers to retransmit these segments in the event that acknowledgments are not forthcoming when a new acknowledgement arrives ATCP forwards that acknowledgement to the TCP which also removes the TCP from the persist mode. So, basically when ATCP gets then acknowledgment a proper acknowledgement; that means that now everything is fine right. So, acknowledgement means that everything is fine. So, then it forwards that acknowledgement to the TCP by forwarding it TCP is going to go to the persist mode is going to remove from the persist mode and is going to be this ATCP then is going to go to the normal mode normal state.

(Refer Slide Time: 17:00)



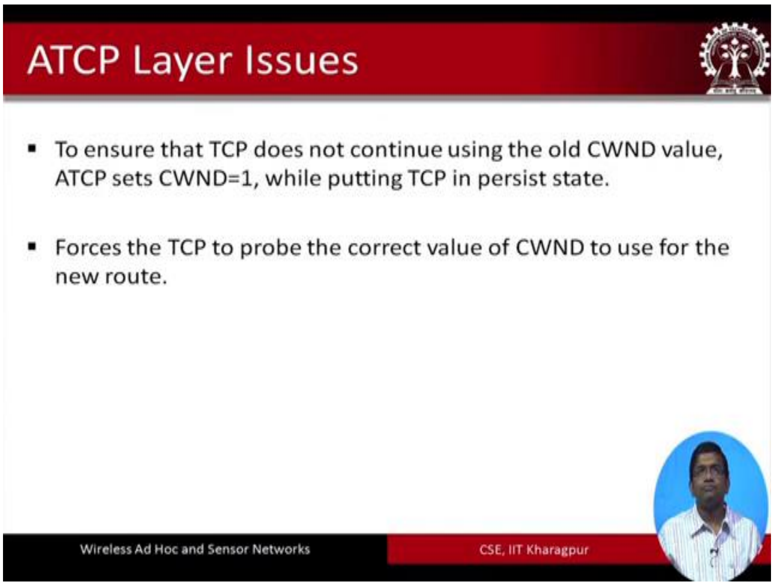
In the congested scenario when the network detects congestion. So, you need congestion. So, earlier we have seen scenarios where congestion actually did not happen, but you know it was misunderstood the sender basically misunderstood that there is congestion, but here we are talking about that indeed congestion has been detected then this is what happens. So, in this particular case when congestion is detected the easy and explicit congestion notification flag is set in the acknowledgments and the data packets explicit congestion notification flag is; so every data packet every acknowledgment that you know. So, this ECN flag is set and this is what normally happens in the case of TCP. So, if ATCP receives this message in its normal state it moves into its congested state and it does nothing over there. It ignores any duplicate acknowledgments that are arriving and ignores the imminent RTO expiration events it does it does not interfere with the normal congestion behavior after TCP transmits a new segment ATCP retransmits normal state.

(Refer Slide Time: 18:18)



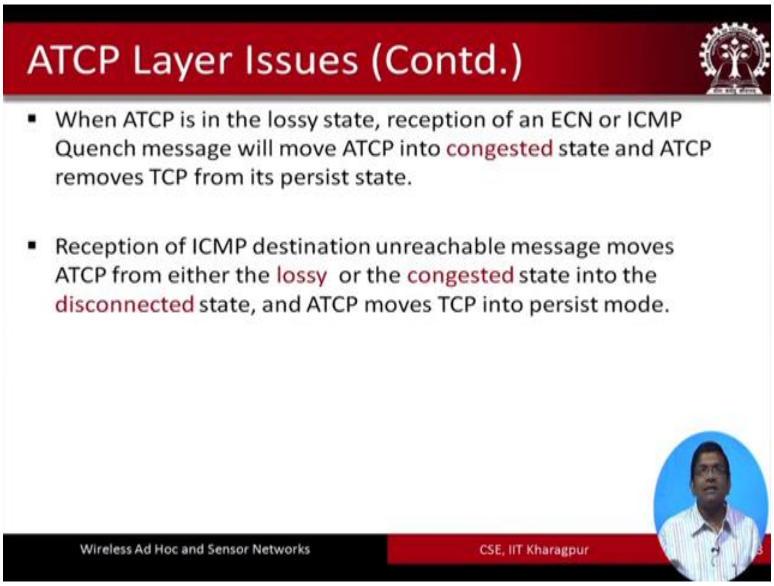
Now, the disconnected scenario; so the node mobility causes route re-computations or temporary network partitioning. The network generates the ICMP destination unreachable message in response to the packet transmission. When ATCP receives this message it puts the TCP sender to the persist mode and itself enters the disconnected state. The TCP periodically generates the probe packets while in the persist mode. When the receiver is connected to the sender it responds to those probe packets with a duplicate acknowledgment, this removes ATCP from the persist mode and ATCP reverts back into the normal state.

(Refer Slide Time: 19:01)



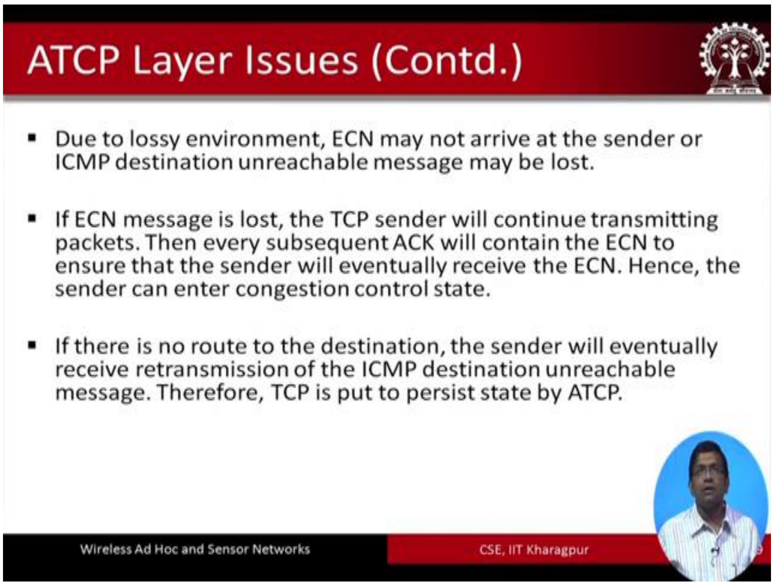
Now there are different issues with respect to the different layers of ATCP. So, to ensure that TCP does not continue using the old congestion window values ATCP, what it does is it changes it resets the congestion window to one while putting the TCP in the persist state it forces the TCP to probe the correct value of the congestion window to use for the new route. So, this is what it does because it does not allow old congestion window values to be used because that will lead to incorrectness.

(Refer Slide Time: 19:39)



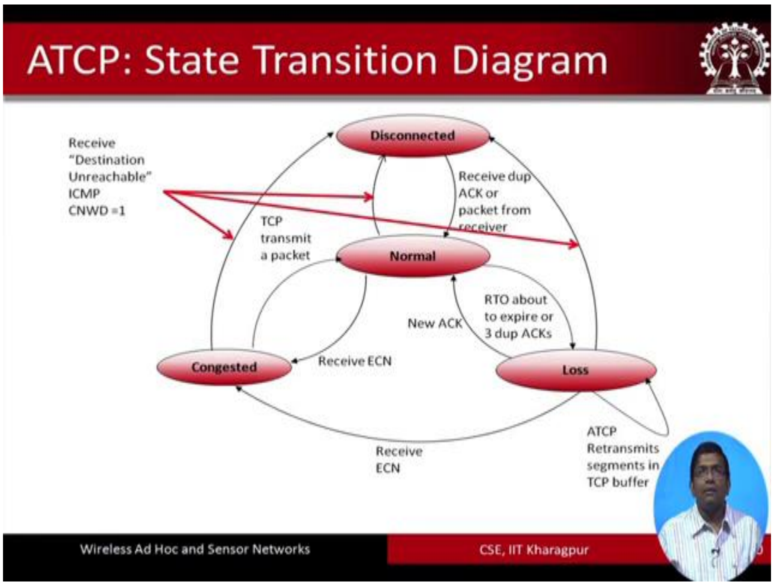
When ATCP is a lossy state reception of an ECN or ICMP quench message will move the ATCP into the congested state and the ATCP removes the TCP from its persist state reception of ICMP destination unreachable message moves the ATCP from either the lossy or the congested state into the disconnected state.

(Refer Slide Time: 20:05)



And ATCP moves the TCP into the persist mode. So, like this that there are different issues that have been considered one by one these different scenarios few of which I just read out for you and there are few other issues that are there using the ATCP layer, how it works.

(Refer Slide Time: 20:22)

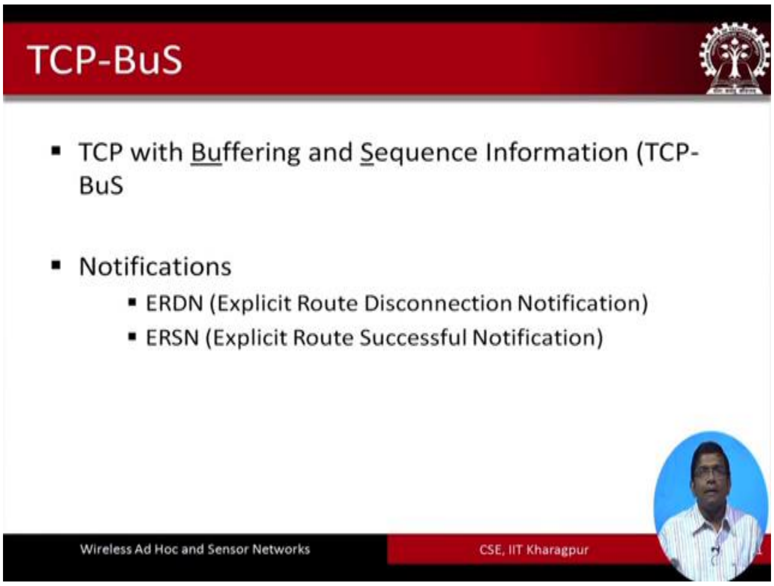


And finally, we come over here and this figure what it does is it captures the different states of the ATCP and the different transitions and this state transition diagram for ATCP is as shown on the slide. So, as we can see that there are 4 states the normal state.

Loss state congested state and the disconnected state. So, from the; it is so; if the TCP sender receives an ECN message irrespective of whether it was in the normal state or it was in the loss state it transitions to the congested state. So, that is basically depicted with the help of these transition these transitions over here. So, the sender basically goes to the congested state if it receives the ECN and if the ICMP message is received then it is ICMP destination unreachable message is received then the sender basically goes from the congested state to the disconnected state or it goes from the normal state to the disconnected state or from the lost state to the disconnected state.

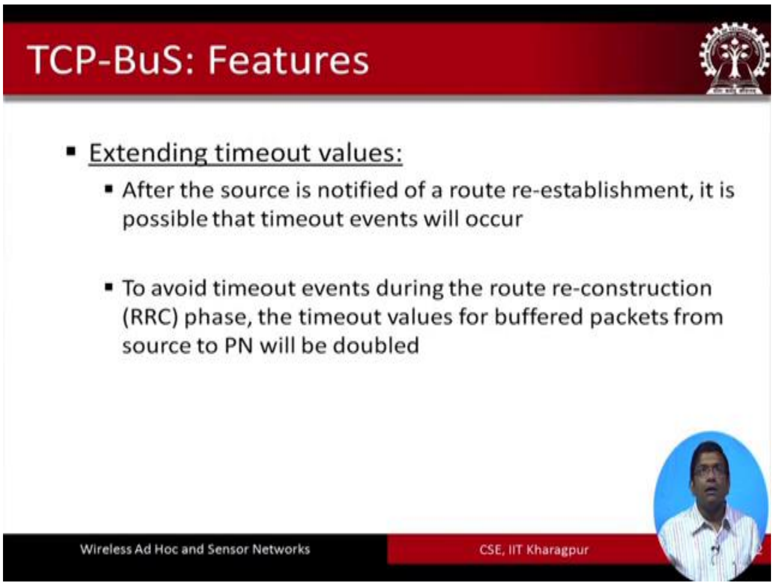
So when the destination unreachable message is received it is an indication that there is some kind of disconnection. So, irrespective of whether the sender is in the congested state the normal state or the loss state it is going to transition to the disconnected state. So, the other states are quite obvious other transitions are quite obvious. So, I would like you to go through it and so this is basically the overall state transition diagram for the ATCP functioning at the sender.

(Refer Slide Time: 22:43)



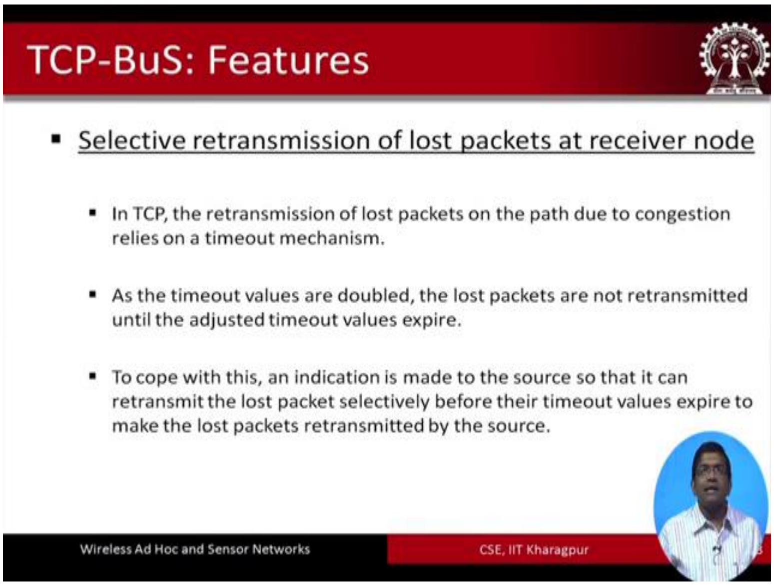
Now, the last protocol transport layer protocol that we are going to cover to some extent and I am just going to go through some of the features because you know it also be as some similarities to similarities with the other protocols the TCP-F and ELFN more particularly. So, I am just going to go through some of these features and then i will show you some of these additional features that are that it has with respect to over the existing protocols. So, in this protocol there are 2 types of notifications that are used the ERDN explicit route disconnection notification message ERDN explicit route disconnection notification message and the ERSN explicit route success notification usage disconnection and success notification explicitly these are informed inform to whom to the sender and we will see how it works.

(Refer Slide Time: 23:49)



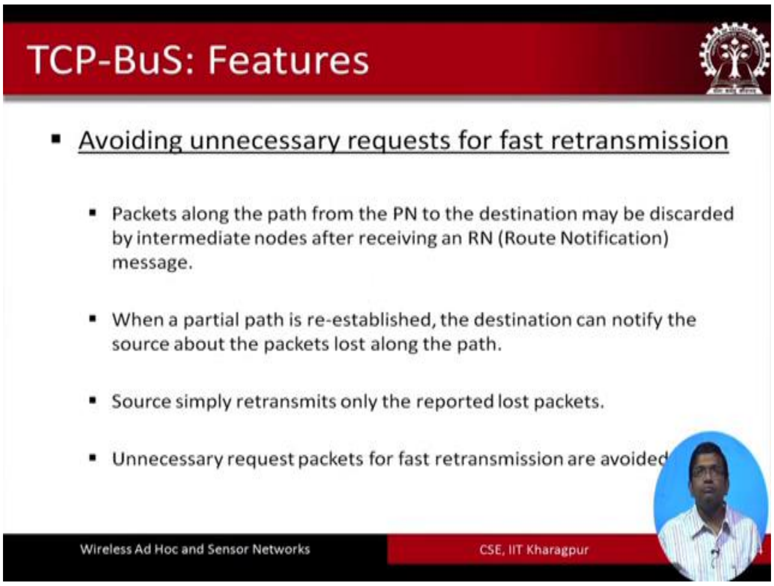
So, some of the features extending the timeout values after the source is notified of a route reestablishment and recall that route is reestablishment is done at the network layer TCP is sitting on top of the network layer. So, after the source is notified of the route reestablishment it is possible that timeout events will occurred to avoid the timeout events during the route re-computation phase the timeout values for the buffered packets from the source to the pivot node will be doubled. So, pivot node the concept of pivot node is used in the case of TCP bus pivot node is an intermediate node through which the packets the segments are going to flow. So, the pivot node is the node which basically detects that there is some route failure that has occurred pivot node detects it and then this pivot node basically informs the TCP sender.

(Refer Slide Time: 24:57)



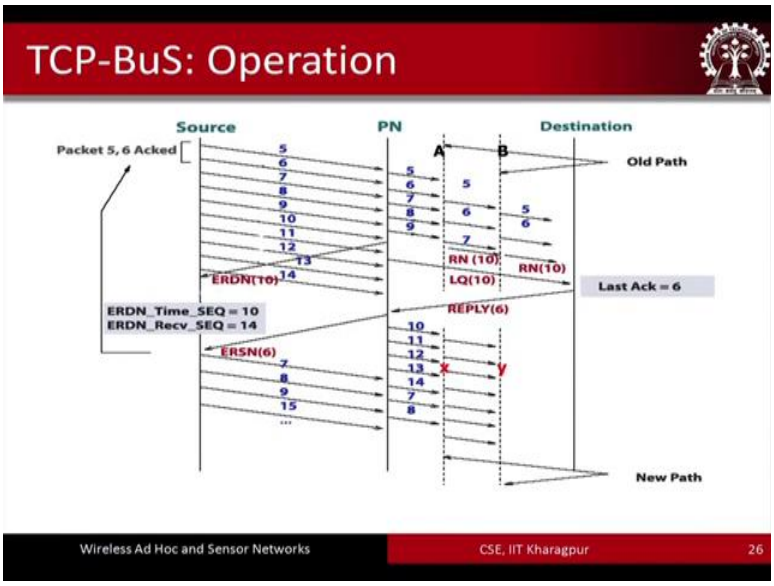
Selectively next feature is selective retransmission of lost packets at the receiver node if in TCP the retransmission of lost packets on the path due to congestion relies on a timeout mechanism as the timeout values are doubled the lost packets are not retransmitted until the adjusted timeout values expire. So, to cope with this an indication is made to the source. So, that it can retransmit the lost packets selectively before their timeout values expire to make the lost packets retransmitted by the source.

(Refer Slide Time: 25:33)



The other feature is avoiding unnecessary requests for fast retransmission packets along the path from the pivot node to the destination may be discarded by the intermediate nodes after receiving an RN message route notification message. When a partial path is reestablished the destination can notify the source about the packets lost along the path. The source simply retransmits only the reported lost packets and unnecessary request packets for fast retransmissions are avoided. So, these are some of the different features of TCP bus.

(Refer Slide Time: 26:13)



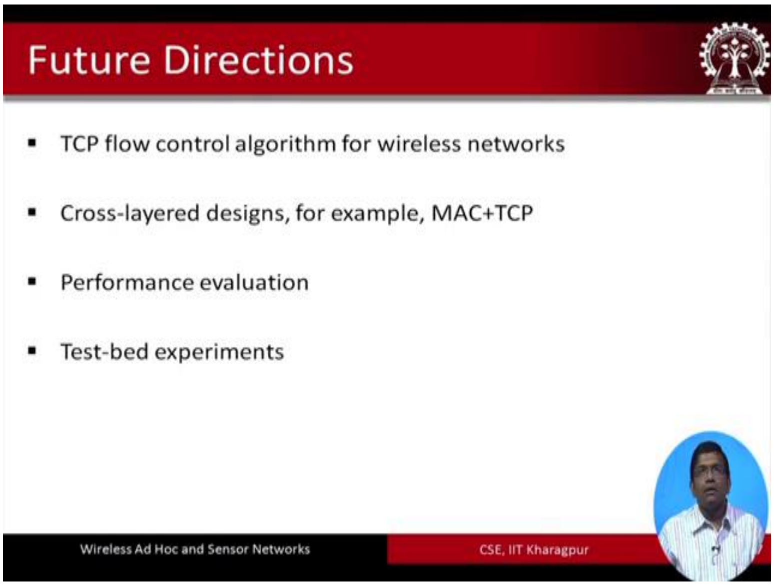
So, there are few other features as well which I am not going to go through and we now come to the overall picture showing the timeline diagram showing how TCP bus functions. So, this is quite intuitive one can you know one can follow this picture and can understand for how things happen, but let us now look at it look at few of the things little bit more closely which are more specific to TCP bus. So, we have the scenario source to destination via intermediate nodes the pivot node A and node B.

So, what did I say before pivot node is the one which basically detects the failure notification failure scenario of failure and it notifies the source. So, you see that segments 5, 6, 7, 8, etcetera come then after some time the pivot node finds that going forward there is some root breakage. So, if some disconnection that has happened; so what it does is it notifies with the help of the ERDN the disconnection notification message explicit route disconnection notification message it informs the source node that up to 10 sorry, yeah.

So, up to 10, I have received properly and then there is a disconnection. So, this ERDN 10 message will inform the source that up to 10 things have been received properly and then the ERDN time sequence is set to 10 and the ERDN receiver sequence is set to 14; 14 means what 14 means that the sender basically has by that time it receives the 10 ERDN 10 message it has already sent the 14th packet. So, what it does is it knows that what it has already sent out the source knows about it then what happens is in the meanwhile the next off node after the pivot since the r n message forward which is taken even forward and so, on and finally, the reply is obtained to the pivot node for the segments that are last acknowledged and then the pivot node basically what it does is it sends the explicit route notification message that things have been; that means, the route has already been repaired.

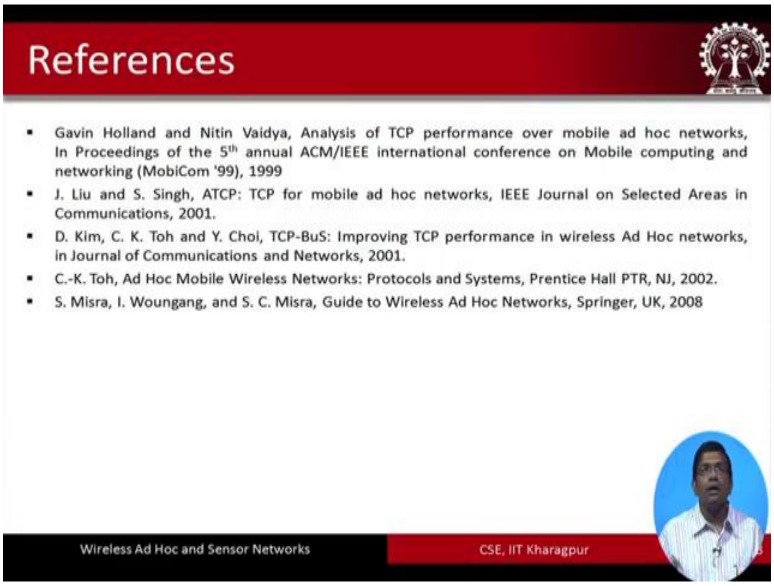
So, then what happens is the and because of these 2 values after receiving this ERSN 6 message then what happens is the source sends the other segments you know. So, 7, 8, 9 and so on and it starts from fifteen because the last segment that it had sent was 14. So, after 14 it resumes with fifteen and so on. So, this is these are some of the salience is in the working of this protocol TCP bus.

(Refer Slide Time: 29:55)



In terms of the future direction TCP flow control algorithm for wireless networks have to be designed these are already designed actually, but there are more there are better flow control mechanisms that can be designed. Cross layered designs taking into account MAC layer issues cross layering between MAC network and so on with the transport layer. Different types of performance evaluations in different environments should be carried on comparisons of them and test bed experiments test bed because most of the experiments using these proposed protocols have been done through simulations. So, test bed based experiments should also be performed.

(Refer Slide Time: 30:46)



So, these are some of the differences TCP bus, this ELFN, ATCP the corresponding references are given over here.

Thank you.