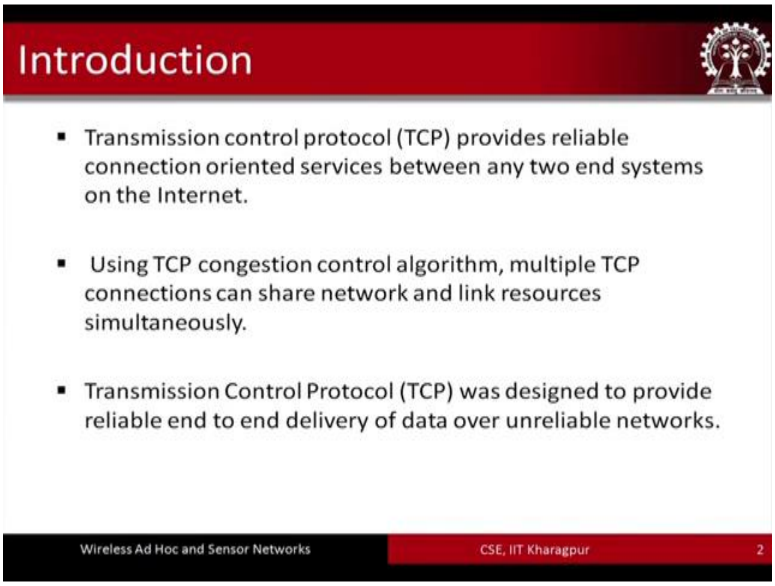
Wireless Ad Hoc and Sensor Networks

Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 13
Transport Protocols for MANETs- Part- I

Transport protocol for mobile Ad-Hoc networks. This topic has been divided into 2 lectures. So, first we are going to go through the basics of transport protocols and their use in MANETs and thereafter in the second part we are going to go through some of the specific protocols that have been designed transport protocols that have been designed for use in these networks.

(Refer Slide Time: 00:47)



Introduction

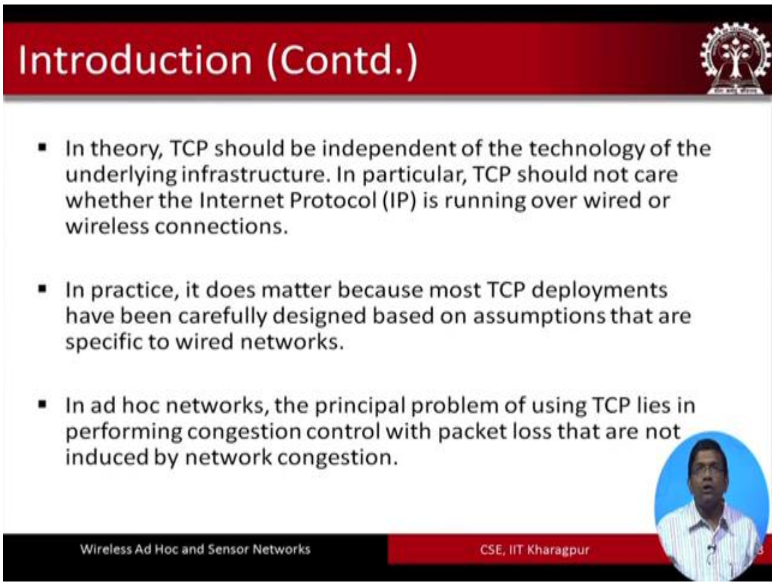
- Transmission control protocol (TCP) provides reliable connection oriented services between any two end systems on the Internet.
- Using TCP congestion control algorithm, multiple TCP connections can share network and link resources simultaneously.
- Transmission Control Protocol (TCP) was designed to provide reliable end to end delivery of data over unreliable networks.

Wireless Ad Hoc and Sensor Networks | CSE, IIT Kharagpur | 2

So, when we talk about transport protocols in the case of the internet the TCP is the most common the most popular transport protocol the reliable transport protocol that has been designed for use in the internet; however, TCP and it is use in the inter in Ad-Hoc networks, basically has some problems. So, we are going to examine why the TCP that has been designed for the internet, the TCP that works very well for the internet why it cannot be used in the case of Ad-Hoc networks.

So, this is what we are going to assess. So, using the TCP congestion control algorithm multiple TCP connections can share network and link resources simultaneously. TCP was designed to provide reliable into end delivery of data over unreliable networks. And that is what that is why TCP was proposed you know. So, TCP for the internet took into consideration that whatever the network may be whether it is reliable or it is unreliable, but what it is required to offer end to end reliability of delivery of data. And that is why TCP was proposed and this is what TCP does to offer guarantees of delivery of data.

(Refer Slide Time: 02:19)



Introduction (Contd.)

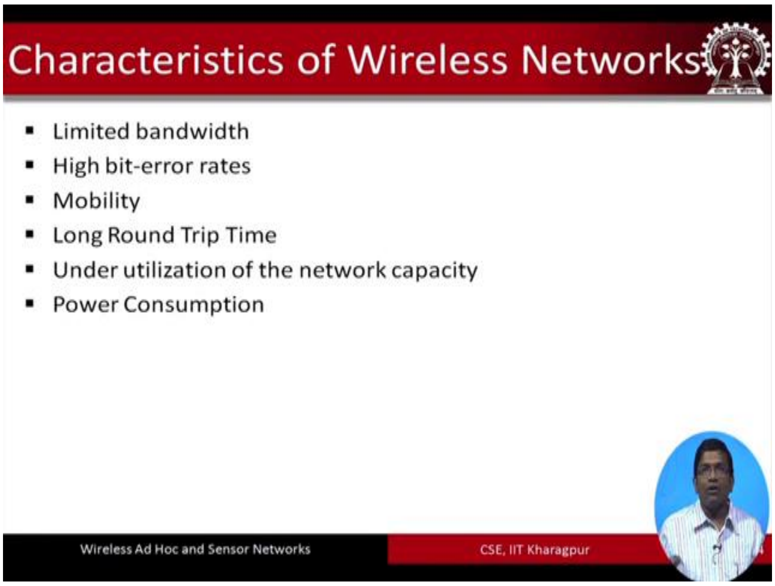
- In theory, TCP should be independent of the technology of the underlying infrastructure. In particular, TCP should not care whether the Internet Protocol (IP) is running over wired or wireless connections.
- In practice, it does matter because most TCP deployments have been carefully designed based on assumptions that are specific to wired networks.
- In ad hoc networks, the principal problem of using TCP lies in performing congestion control with packet loss that are not induced by network congestion.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

In theory TCP should not be dependent on what is the underlying infrastructure that is used. So; that means, that whether one is using IP over a wired network or a wireless network. So, TCP should not be bothered about it. So, that is theoretically what should happen; however, what happens is in practice most of the TCP deployments they basically take into consideration some of the assumptions that are specific to wired networks. So, in Ad-Hoc networks the principle problem of using this TCP lies in performing congestion control with packet loss that are not induced by network congestion. So, this is the main problem of using TCP in the case of Ad-Hoc networks and we are going to examine this in further more detail as we go ahead.

(Refer Slide Time: 03:21)



Characteristics of Wireless Networks

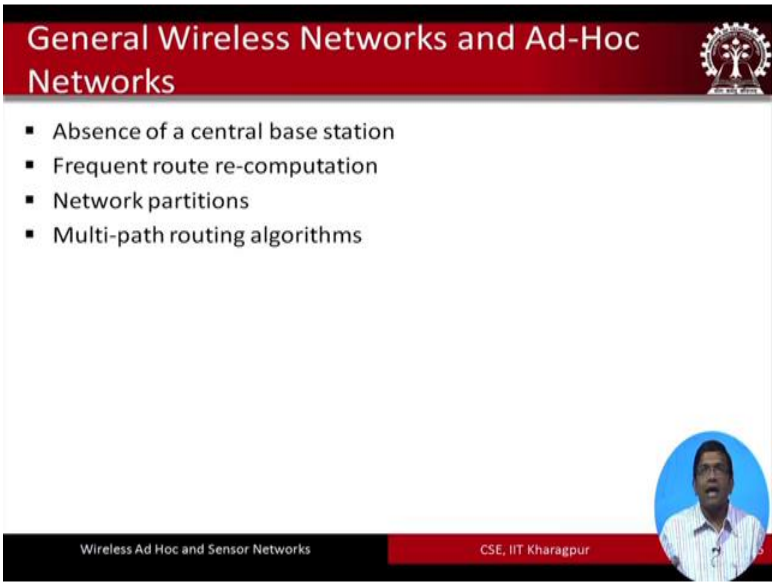
- Limited bandwidth
- High bit-error rates
- Mobility
- Long Round Trip Time
- Under utilization of the network capacity
- Power Consumption

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, when we talk about wireless networks in general Ad-Hoc or non head of Ad-Hoc. There are different characteristics of these wireless networks these networks have limited bandwidth, they have very high bit error rate this is a very important thing much higher bit error rates, these are more error prone environments they have more bit error rates compared to the wired counterpart mobility is another very important aspect. Typically, in a wireless network the nodes are mobile the round trip times is typically much longer compared to the RTT in the case of Ad-Hoc in the case of wired networks. Then power consumption is also a very important concern, because in wired networks power is not an issue so, but in the case of wireless networks power is a very important power consumption is a very important issue.

(Refer Slide Time: 04:22)



General Wireless Networks and Ad-Hoc Networks

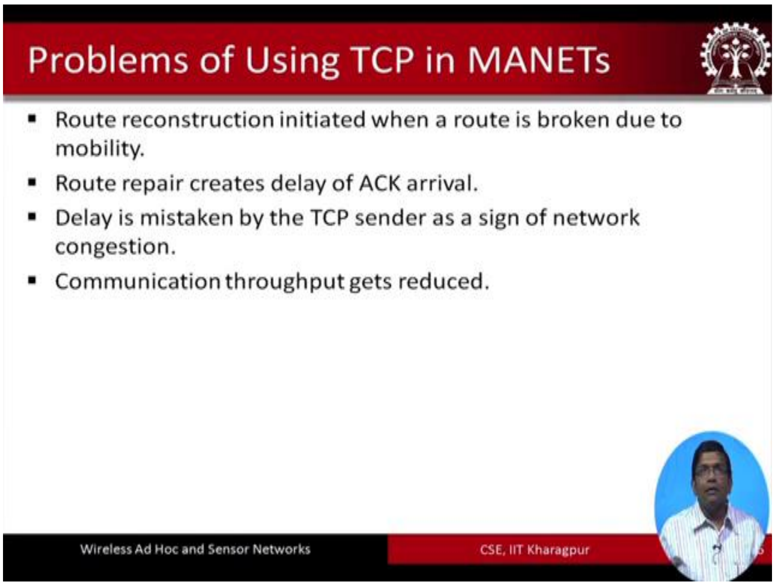
- Absence of a central base station
- Frequent route re-computation
- Network partitions
- Multi-path routing algorithms

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

Now, when we look at both the wireless networks and the Ad-Hoc networks Ad-Hoc wireless networks more specifically, the Ad-Hoc networks unlike any other wireless network does not have a central base station. There is frequent route re computation because of the mobility of the nodes the topology of the network changes over time and sometimes they change quite fast, and that leads to frequent route re computations at the network layer. And also often it happens that because there is not no centralized coordinator or a centralized base station unlike other where other general wireless networks, the networks often get partitioned. And that network partitioning is a typical feature in an Ad-Hoc network. And there are other associated problems because of the use of multipath routing in these networks. So, each of these and the problems they pose we are going to go through them in more detail.

(Refer Slide Time: 05:35)



Problems of Using TCP in MANETs

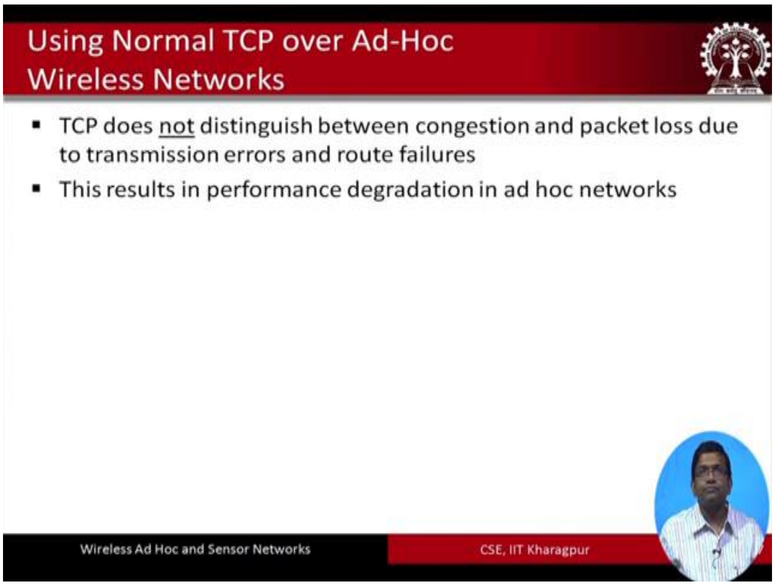
- Route reconstruction initiated when a route is broken due to mobility.
- Route repair creates delay of ACK arrival.
- Delay is mistaken by the TCP sender as a sign of network congestion.
- Communication throughput gets reduced.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, I at the beginning I mentioned that the use of TCP, that was the pure TCP that was designed for the internet, the use of it in the case of MANETs is a problem. TCP is a transport layer protocol the transport layer sit is on top of the network layer. So, basically when there is a link failure; that means, a route in a multi hub path is broken, often due to mobility the process of route re construction is initiated at the network layer. Now this route re construction of the route repair basically creates a delay of acknowledgement arrival at the transport layer corresponding to a segment that is sent out by the sender to the receiver. Now that delay in the receipt of the acknowledgment at the sender that delay of the receipt of the acknowledgement at the sender is mistaken by the sender as a sign of network condition. And consequently the congestion control mechanisms like binary exponential back off etcetera are invoked and what because of that the overall communication throughput gets reduced drastically.

(Refer Slide Time: 07:03)



Using Normal TCP over Ad-Hoc Wireless Networks

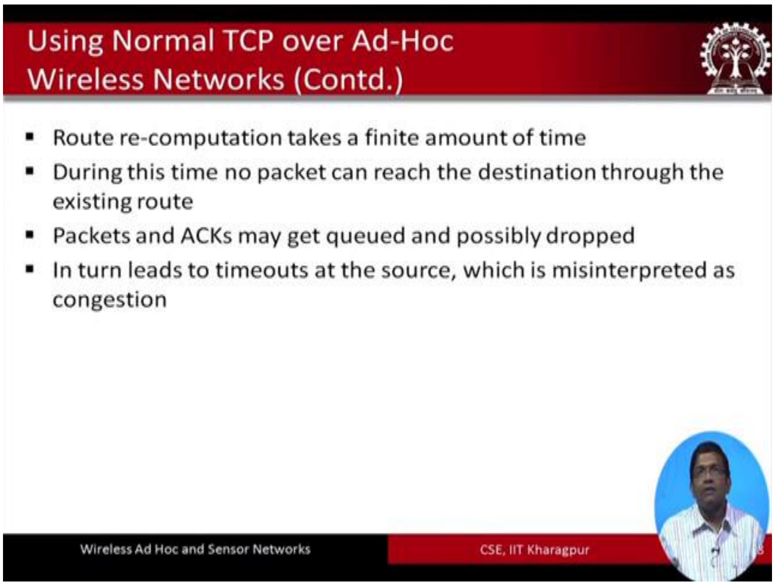
- TCP does not distinguish between congestion and packet loss due to transmission errors and route failures
- This results in performance degradation in ad hoc networks

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, TCP does not distinguish between congestion and packet loss due to transmission errors and route failures. These basically results in performance degradation as well in Ad-Hoc networks. So, congestion is happening due to route failures or due to packet loss due to transmission errors. TCP the TCP for internet does not distinguish that. And that basically leads to performance issues of running TCP on an Ad-Hoc network.

(Refer Slide Time: 07:38)



Using Normal TCP over Ad-Hoc Wireless Networks (Contd.)

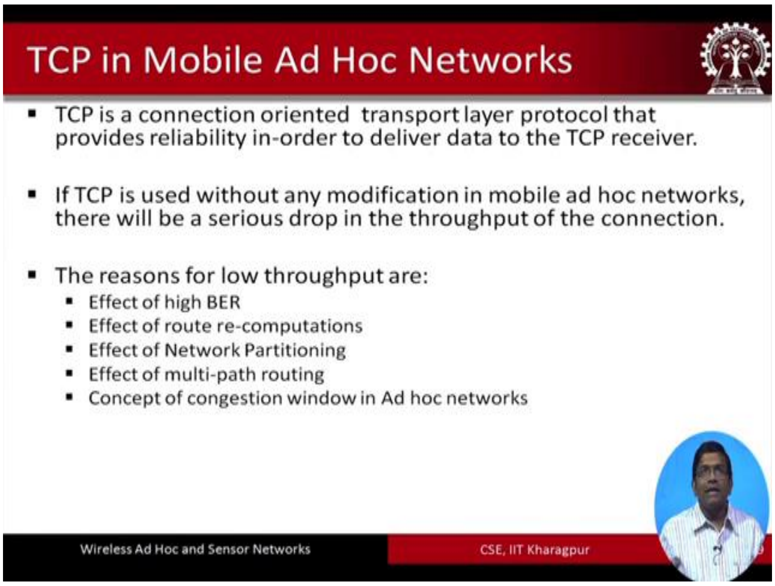
- Route re-computation takes a finite amount of time
- During this time no packet can reach the destination through the existing route
- Packets and ACKs may get queued and possibly dropped
- In turn leads to timeouts at the source, which is misinterpreted as congestion

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, the route re computation of let us say that one still wants to use TCP in Ad-Hoc networks. So, that route re computation takes a finite amount of time. A finite amount of time is taken by the route re computation process, that is executed at the network layer now that process of route re computation, and the time it takes during this time no packet can reach the destination through the existing route. The packets because it is quite obvious to the existing routes no packets can reach the destination. The packets and acknowledgments get queued and sometimes they can be dropped also if they cannot be queued any further. And in turn that leads to timeouts and the source which is misinterpreted as a sign of congestion.

(Refer Slide Time: 08:40)



TCP in Mobile Ad Hoc Networks

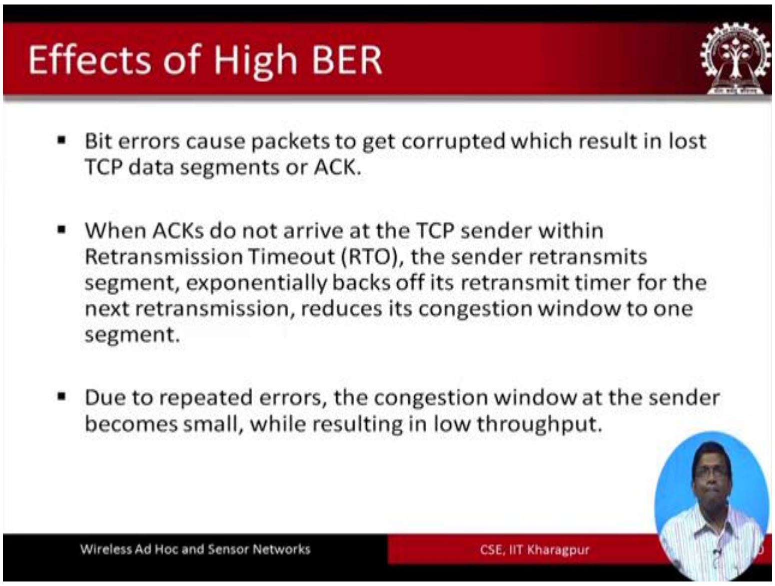
- TCP is a connection oriented transport layer protocol that provides reliability in-order to deliver data to the TCP receiver.
- If TCP is used without any modification in mobile ad hoc networks, there will be a serious drop in the throughput of the connection.
- The reasons for low throughput are:
  - Effect of high BER
  - Effect of route re-computations
  - Effect of Network Partitioning
  - Effect of multi-path routing
  - Concept of congestion window in Ad hoc networks

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, TCP for the internet it is a connection oriented transport layer protocol. It is designed to provide reliable in order delivery of data to the receiver. So, if TCP is used without any modification is in MANETs. As we have seen that throughput can go down drastically in these networks. And the reasons for the low throughput are linked with many different issues. One issue is what I already mentioned, but there are many other issues, effect of high bit error rate effect of route re computations effect of network partitioning effects of multipath routing and so on. So, we are going to take up each one of them and we are going to analyze how or rather why this becomes an issue when we want to run TCP on these networks.

(Refer Slide Time: 09:45)



Effects of High BER

- Bit errors cause packets to get corrupted which result in lost TCP data segments or ACK.
- When ACKs do not arrive at the TCP sender within Retransmission Timeout (RTO), the sender retransmits segment, exponentially backs off its retransmit timer for the next retransmission, reduces its congestion window to one segment.
- Due to repeated errors, the congestion window at the sender becomes small, while resulting in low throughput.

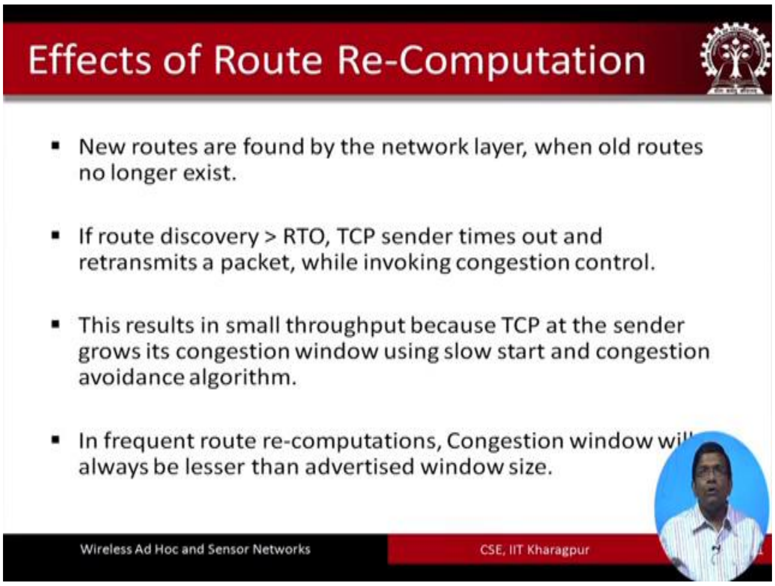
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, first we will look at the bit error rate. So, Ad-Hoc networks are highly error prone environments much, higher errors then in a general wireless network or; obviously, much higher errors than much higher error prone compared to the wired networks. So, these bit errors cause the packets to get corrupted which result in lost TCP data segments of or the lost acknowledgments, when these acknowledgments do not arrive at the TCP sender within a particular duration of time which is known as the RTO time or the retransmission timeout time. The sender retransmit is the segment exponentially backs off it is retransmit timer for the next retransmission reduces it is congestion window to one segment and so on.

So, due to the repeated errors the congestion window at the sender will remains small and if the congestion window is small the c window typically small means like typically it starts, with one value which means that you know only one segment can be transmitted at any point in time. So, if that happens basically what is going to happen is the through put is going to go down drastically. So, one segment at a time. So, you send one segment get an acknowledgement back sent this next segment get the second acknowledgment back and so on. So, that is not a very good thing.

(Refer Slide Time: 11:13)



Effects of Route Re-Computation

- New routes are found by the network layer, when old routes no longer exist.
- If route discovery > RTO, TCP sender times out and retransmits a packet, while invoking congestion control.
- This results in small throughput because TCP at the sender grows its congestion window using slow start and congestion avoidance algorithm.
- In frequent route re-computations, Congestion window will always be lesser than advertised window size.

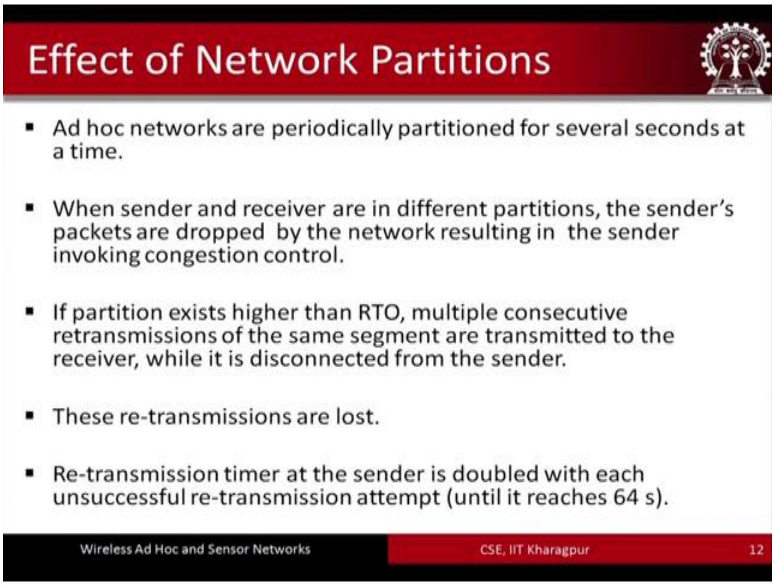
Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Now, let us look at what happens with respect to route re computation. This is the one that I mentioned at the beginning. So, route re computation. So, basically you know. So, what happens is due to the mobility of the nodes the topological changes are first the over time, the network topology is going to change. So, no roots are found by the network layer when the old roots no longer exist. And consequently what is going to happen is the network layer is going to start the route re computation process.

So, if the route discovery time is greater than the retransmission timeout time RTO time, when the TCP sender times out and retransmit a packet while invoking the congestion control. So, it invokes the congestion control and retransmit the packet. So, this result seems small throughput because the TCP at the sender grows it is congestion window without you using the slow start mechanism; that means, additive increase multiplicative decrease and the congestion avoidance algorithm.

In case of frequent route re computations the congestion window will always be lesser than the advertised window size. So, this again brings down the throughput drastically.

(Refer Slide Time: 12:30)



Effect of Network Partitions

- Ad hoc networks are periodically partitioned for several seconds at a time.
- When sender and receiver are in different partitions, the sender's packets are dropped by the network resulting in the sender invoking congestion control.
- If partition exists higher than RTO, multiple consecutive retransmissions of the same segment are transmitted to the receiver, while it is disconnected from the sender.
- These re-transmissions are lost.
- Re-transmission timer at the sender is doubled with each unsuccessful re-transmission attempt (until it reaches 64 s).

Wireless Ad Hoc and Sensor Networks

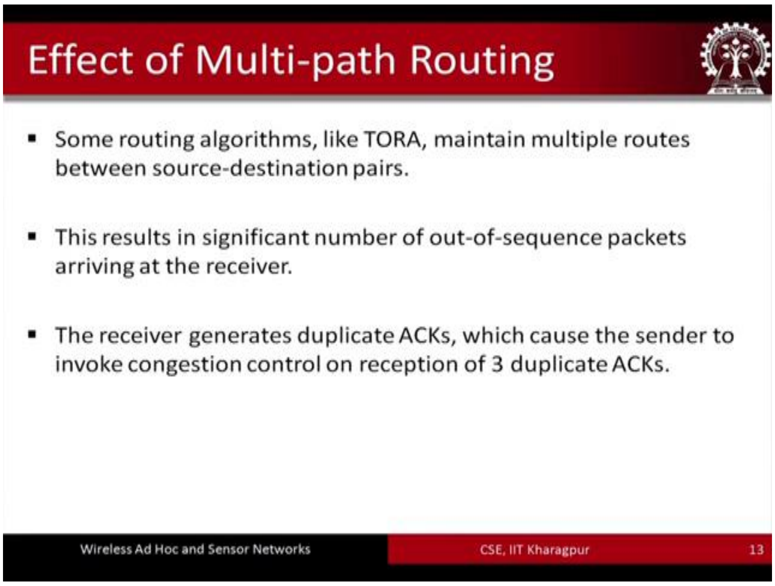
CSE, IIT Kharagpur

12

When we are trying to use TCP the internet TCP in the case of MANETs Ad-Hoc networks are also subjected to network partitions at different points in time. And there is no centralized coordinator which can keep track or even control the partitioning process. So, Ad-Hoc networks are periodically partitioned for several seconds at a time. So, when the sender and the receiver are in different partitions. So, this might happen that at one point of time all of the nodes they are in the same partition, but the because the nodes are moving and there is no one to keep track of where the nodes go etcetera it might.

So, happen that at one point both the sender and the receiver are in the same partition, and at a later instant of time the sender and the receivers are in 2 different partitions. So, when the sender and the receiver are in different partitions, the senders' packets are dropped by the network resulting in the sender invoking condition control. If partition exists higher than the retransmission timeout time then multiple consecutive retransmissions of the same segment are transmitted to the receiver, while it is disconnected from the sender and these re transmissions are lost and the re transmission timer at the sender is doubled with each unsuccessful re transmission attempt. So, doubled we are assuming over here that the binary by exponential back off mechanism is used.

(Refer Slide Time: 14:10)



Effect of Multi-path Routing

- Some routing algorithms, like TORA, maintain multiple routes between source-destination pairs.
- This results in significant number of out-of-sequence packets arriving at the receiver.
- The receiver generates duplicate ACKs, which cause the sender to invoke congestion control on reception of 3 duplicate ACKs.

Wireless Ad Hoc and Sensor Networks

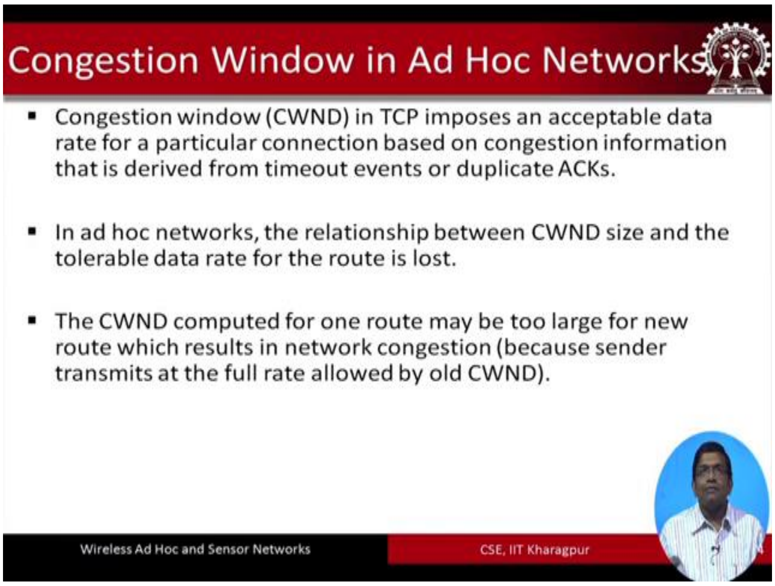
CSE, IIT Kharagpur

13

So, effect of multipath routing. This is again because multipath routing is something. That is quite common in different routing algorithms at the network layer, that have been proposed for Ad-Hoc networks tora is one such algorithm which maintains multiple routes between the source and destination pairs of nodes. So, this results in significant number of out of sequence packets arriving at the receiver. So, this is the problem the problem here is bit different in nature then the problems that we have seen in the previous scenarios.

This particular case the receiver generates duplicate acknowledgments which cause the sender to invoke congestion control on reception of 3 duplicate acknowledgment. Because this is a standard practice actually in TCP. So, basically if 3 copies of an acknowledgment arise that basically is taken as a sign of congestion. And the congestion control mechanisms are invoked at the sender. And, but you know if one is using multipath routing mechanisms. Then this is a common thing that is going to happen in the case of Ad-Hoc networks.

(Refer Slide Time: 15:28)



Congestion Window in Ad Hoc Networks

- Congestion window (CWND) in TCP imposes an acceptable data rate for a particular connection based on congestion information that is derived from timeout events or duplicate ACKs.
- In ad hoc networks, the relationship between CWND size and the tolerable data rate for the route is lost.
- The CWND computed for one route may be too large for new route which results in network congestion (because sender transmits at the full rate allowed by old CWND).

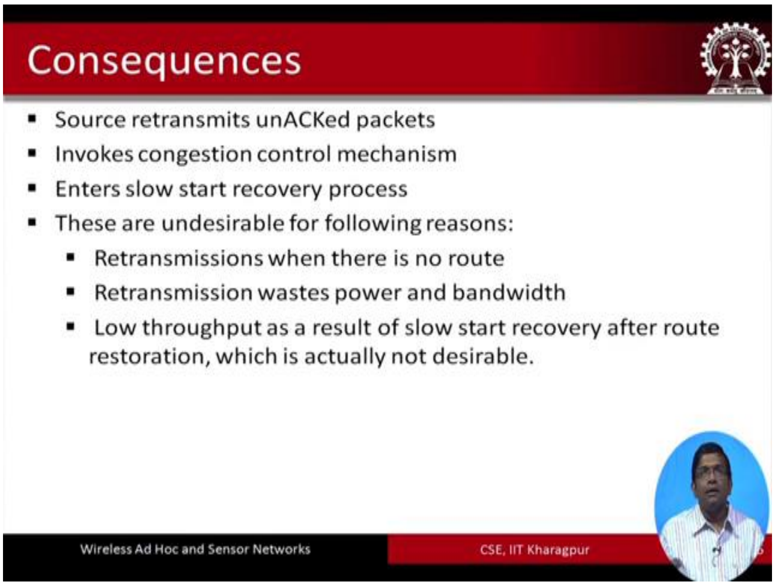
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

Now, with respect to the congestion window, these are few things that we have to keep in mind. The congestion window in TCP imposes an acceptable data rate for a particular connection based on congestion information that is derived from time out events or duplicate acknowledgments in Ad-Hoc networks. The relationship between the congestion window size and the tolerable data rate for the route is lost.

So, what it means is that the congestion window size basically dictates the rate at which the data is going to flow between the sender and the receiver, and in the case of Ad-Hoc networks due to disc connections etcetera this could lead to a problem .because you cannot implement such a mechanism as such in the case of these networks the congestion window is size is computed for one route the congestion window size computed for one route may be too large for new route which results in network congestion. Because the sender transmit is at the full rate that is allowed by the old congestion window size.

(Refer Slide Time: 16:42)



Consequences

- Source retransmits unACKed packets
- Invokes congestion control mechanism
- Enters slow start recovery process
- These are undesirable for following reasons:
  - Retransmissions when there is no route
  - Retransmission wastes power and bandwidth
  - Low throughput as a result of slow start recovery after route restoration, which is actually not desirable.

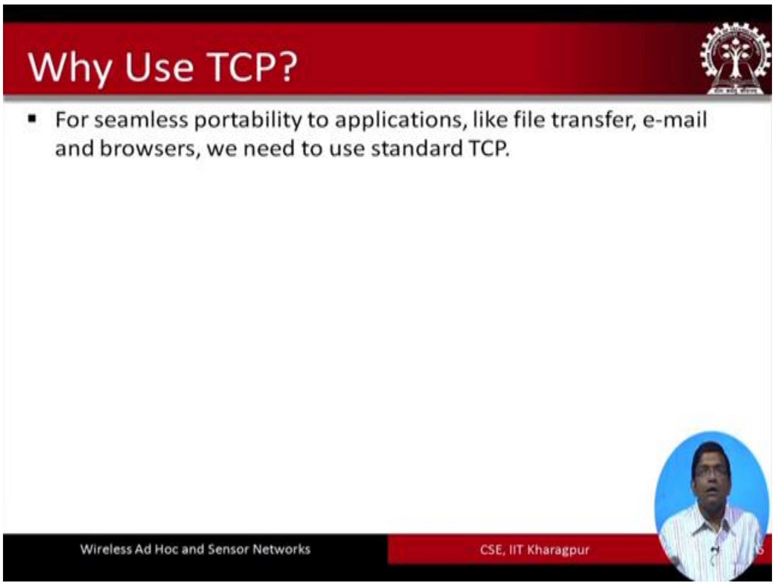
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

In terms of the consequences what is going to happen, the source is going to retransmit the unacknowledged packets the source invokes the congestion control mechanism. It enters the slow start recovery process, but these are undesirable because of the following reasons. So, retransmission is started. So, when the returns menses. So, retransmissions are started when there is no route. So, this is a problem retransmission is basically wastes power and bandwidth. So, more power consumption more bandwidth consumption. So, these are unwanted undesired. The low throughput is obtained as a result of slow start recovery after the route restoration process which is actually not very desirable, slow start slow start means that you additively increase. So, the AIMD scheme the additive increase multiplicative decreased scheme is typically adopted in such cases.

So, the congestion window size is additively increased whereas, if there is a sign of congestion then the size congestion window size is multiplicatively decreased.

(Refer Slide Time: 17:55)

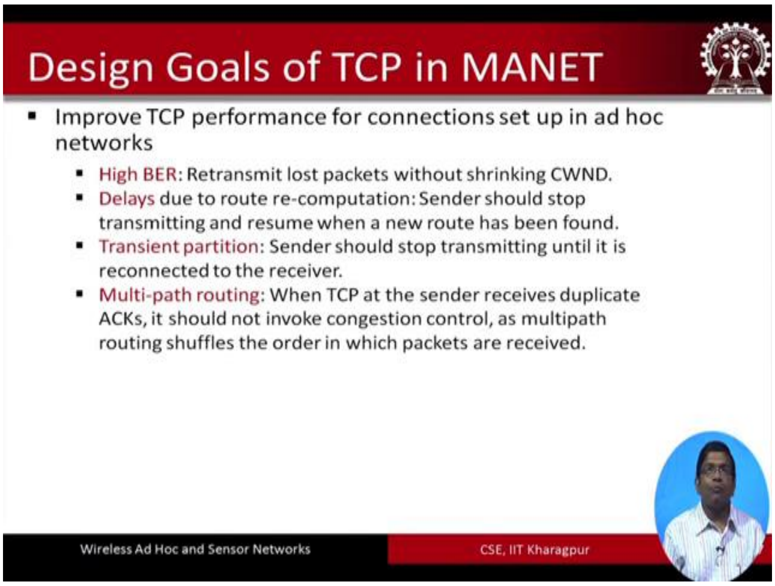


Why Use TCP?

- For seamless portability to applications, like file transfer, e-mail and browsers, we need to use standard TCP.

So, why we use the TCP, then because you know if we did not have the TCP ultimately we have to run at the application layer different protocols such as the FTP email we need to run our browsers which will use SMTP and so on. At the application layer, but for each of them for reliability sake etcetera we need to have between the transport layer and the application layer we need to have a reliable transport protocol that TCP is typically the standard one that is used in the case of internet, but we still want to run these applications email file transfer etcetera. We still want to run them in the case of minutes as well and that is why we need a new type of a modified TCP a new TCP solution not the old TCP for internet for use in MANETs.

(Refer Slide Time: 18:53)



Design Goals of TCP in MANET

- Improve TCP performance for connections set up in ad hoc networks
  - High BER: Retransmit lost packets without shrinking CWND.
  - Delays due to route re-computation: Sender should stop transmitting and resume when a new route has been found.
  - Transient partition: Sender should stop transmitting until it is reconnected to the receiver.
  - Multi-path routing: When TCP at the sender receives duplicate ACKs, it should not invoke congestion control, as multipath routing shuffles the order in which packets are received.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, let us now look at from a positive point of view we have already seen the different challenges that may be encountered by using TCP in case of MANETs. So, let us now we now have an objective that we need to design a TCP, a new TCP we need to design a new transport layer protocol for use in minutes. So, what are the design goals of the TCP or the transport layer protocol that we are going to design?

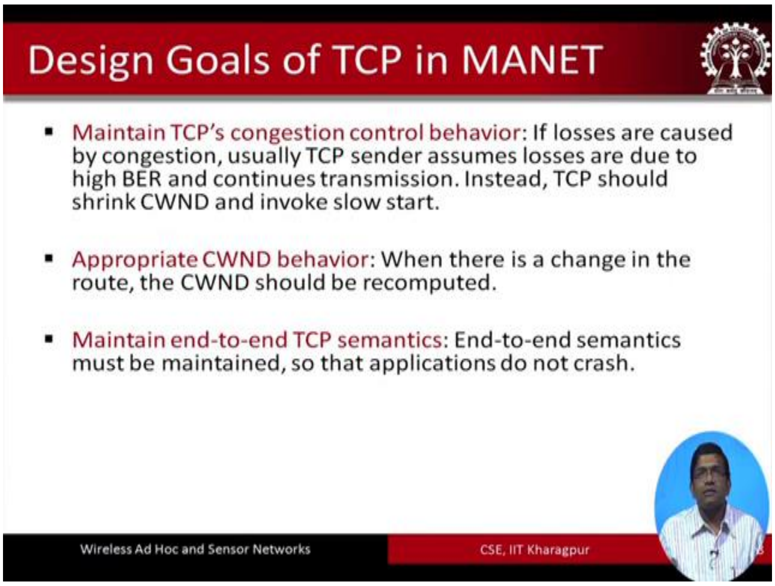
So, these are some of the goals and these are basically in a different way we have already gone through. In terms of the high bit error rate which is exhibited in MANETs. It is instead of reducing the congestion window size at when there is an imminent congestion or route failure or there is packet drop and so on. So, rather it would be better, we transmit the lost packets without basically shrinking this congestion window size.

Delays due to route re computation, the sender should stop transmitting and resume when a new route has been found. Transient partition sender should stop transmitting until it is reconnected to the receiver. Multipath routing and we have already seen that multiple routing possesses a problem in the case of MANETs. So, when TCP at the sender receives duplicate acknowledgments it should not invoke congestion control as multipath routing shuffles the order in which packets are received.

So, congestion though in the whole idea if you look at behind each of these performance measures performance goals is basically as or the corrective measures is that TCP should not be allowed to invoke congestion control for mere reasons, which basically not may not be associated with congestion at all, with may not be associated with congestion at all, maybe the problem is due to the bit error rate high bit error rate maybe there are packet drops that are there because of which TCP sender thinks that there is congestion going on maybe there is some link failure in between in a multi hop path because of which the congestion because of which the sender my think that there is some congestion going on due to the delay in the receipt of the acknowledgment at the sender and due to partitions and so on.

So, all these things make the sender feel that there is some congestion that is going on and congestion control should be invoked. So, this is what has to be stopped. This is what has to be stopped the sender should be disallowed to be start congestion control as such which it was supposed to do if it was run over if TCP was run over the regular internet.

(Refer Slide Time: 22:03)



Design Goals of TCP in MANET

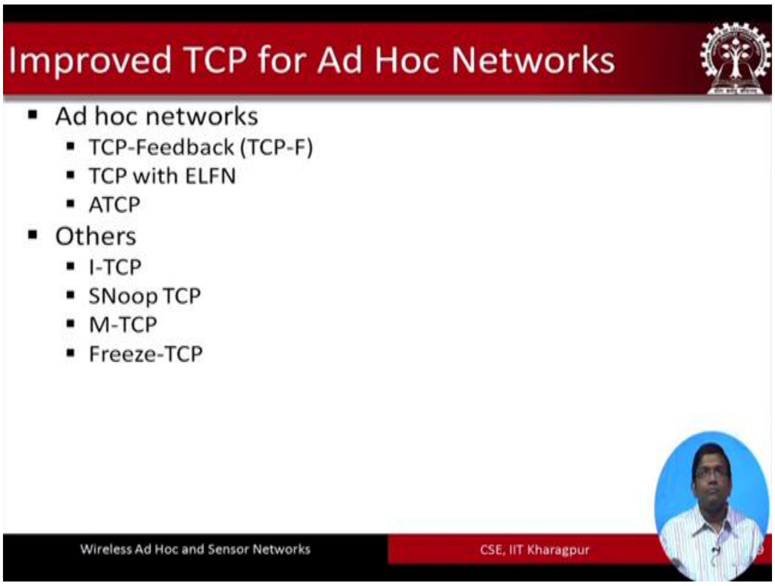
- Maintain TCP's congestion control behavior: If losses are caused by congestion, usually TCP sender assumes losses are due to high BER and continues transmission. Instead, TCP should shrink CWND and invoke slow start.
- Appropriate CWND behavior: When there is a change in the route, the CWND should be recomputed.
- Maintain end-to-end TCP semantics: End-to-end semantics must be maintained, so that applications do not crash.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, maintaining TCP congestion control behavior, if losses are caused by congestion usually TCP sender assumes that the losses are due to high bit error rate, and continues the transmission this is what I just said just now. So, instead the TCP should shrink the congestion window and invoke slow start. Appropriate congestion window behavior when there is a change in the route the congestion window should be recomputed. Maintaining end to end TCP semantics, end to end semantics must be maintained. So, that the applications do not crash. So, this is a very important issue an issue of different kind applications is running on top applications would crash if this thing is not insured. So, end to end semantics and matching the semantics maintaining the semantics end to end is very important otherwise the applications that are running on top are not going to function.

(Refer Slide Time: 22:59)



Improved TCP for Ad Hoc Networks

- Ad hoc networks
  - TCP-Feedback (TCP-F)
  - TCP with ELFN
  - ATCP
- Others
  - I-TCP
  - SNoop TCP
  - M-TCP
  - Freeze-TCP

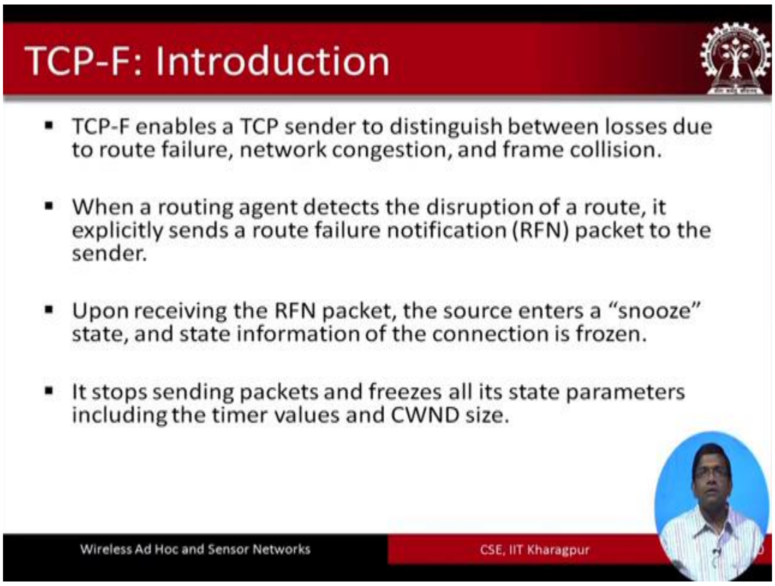
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, in order to run transport layer protocols on Ad-Hoc networks we have already seen that there are problems. There are problems of using TCP. The TCP for internet, now what is required is to come up with new solutions that can be used for MANETs for Ad-Hoc networks in general. So, the solution should be custom designed for these networks. So, there are different large number of transport layer protocols that have been proposed for these networks.

TCP-F is one such primitive transport layer protocol TCP feedback, is it primitive transport layer protocol TCP with ELFN explicit failure notification. ELFN is the second mechanism a TCP is another mechanism and like this there are different other mechanisms which basically modify the existing TCP of the internet and they try to use it in a modified way in the case of MANETs. So, will go through some of these protocols.

(Refer Slide Time: 24:20)



TCP-F: Introduction

- TCP-F enables a TCP sender to distinguish between losses due to route failure, network congestion, and frame collision.
- When a routing agent detects the disruption of a route, it explicitly sends a route failure notification (RFN) packet to the sender.
- Upon receiving the RFN packet, the source enters a "snooze" state, and state information of the connection is frozen.
- It stops sending packets and freezes all its state parameters including the timer values and CWND size.

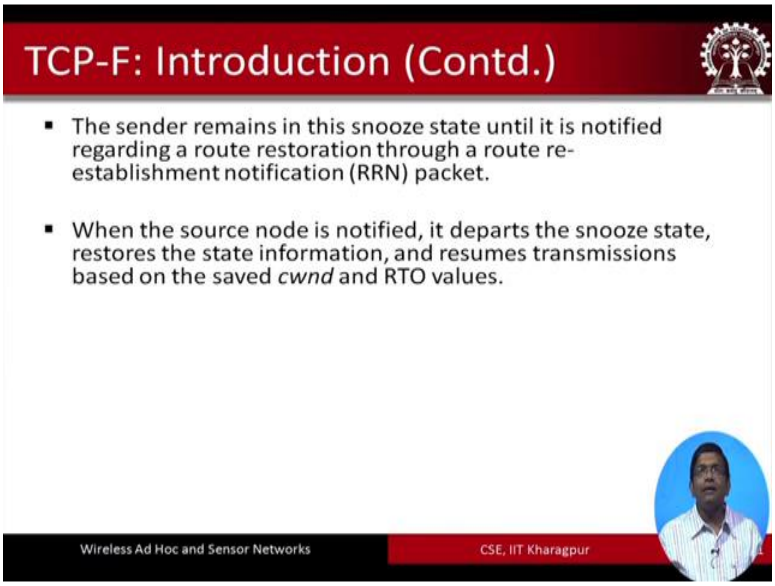
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, first we will start with TCP-F and in the next lecture we are going to go through few other transport layer protocols like the TCP-F. So, TCP layer f is a primitive protocol a primitive transport layer protocol for Ad-Hoc networks. So, it basically enables a TCP sender to distinguish between the losses due to route failure network congestion and frame collision. So, this is very important. I mean whether the loss is really due to congestion or there is something else going on because the topology has changed that the routes have changed etcetera or there is some kind of collision and so on.

So, all these things have to be distinguished and TCP-F basically takes that into account. So, when a routing agent detects the disruption of a route it explicitly sends a route failure notification packet to the sender. Upon receiving the route failure notification packet the source enters a snooze state and the state information of the connection is frozen. If it stops sending the packets and freezes all it is state parameters including the timer values and the congestion window size. So, who stops the sender stops, when does it stop it stops when the route failure notification packet is received by it. So, when the route failure notification packet is received at the sender, what it does is it basically freezes it you know it freezes all it is parameters it goes to the snooze state. It is going to the snooze state it is slips for a while and it freezes all it is state parameters, state parameters. For example, the congestion window size it freezes for example, the RTO value it freezes and so on. So, all the state variables are frozen and the sender goes to the snooze state.

(Refer Slide Time: 26:22)



TCP-F: Introduction (Contd.)

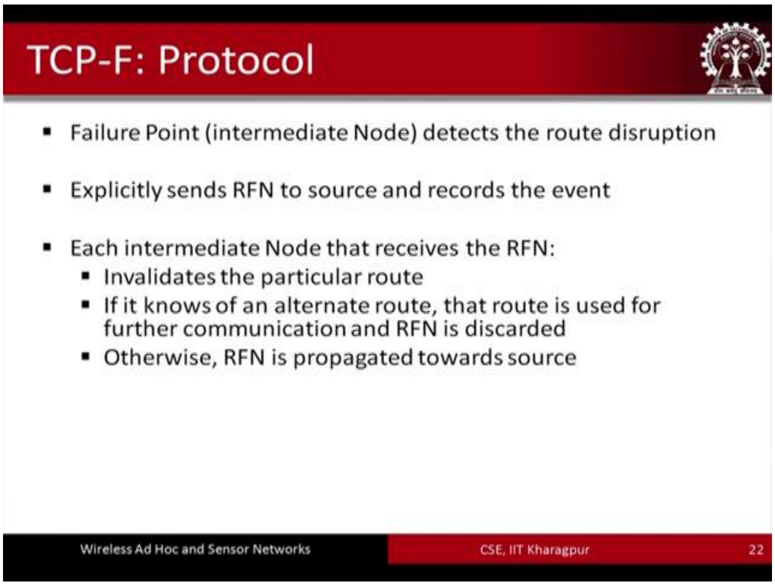
- The sender remains in this snooze state until it is notified regarding a route restoration through a route re-establishment notification (RRN) packet.
- When the source node is notified, it departs the snooze state, restores the state information, and resumes transmissions based on the saved *cwnd* and RTO values.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

The sender remains in this snooze state until it is notified that the route has been restored using the RRN packet route reestablishment notification packet route reestablishment notification packet. Basically informs the sender that the route is now restored. Now you can start from where you left before. So, when the source is notified it departs from the snooze state. Restores the state information and resumes transmissions based on the saved values of the c window and the RTO. So, this is what was frozen before right the c window size c window value the RTO values when the sender went to the snooze state everything was frozen. So, so basically it is going to resume from the same state where it left after the route is reestablished.

(Refer Slide Time: 27:19)



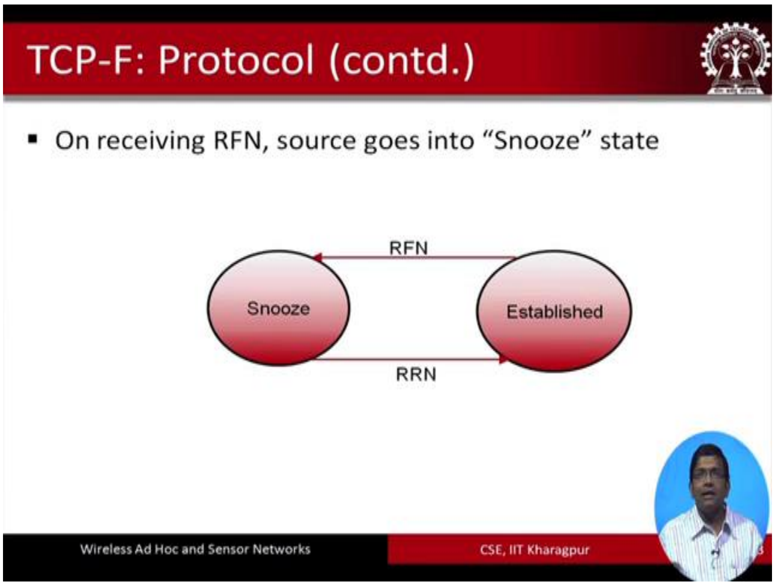
TCP-F: Protocol

- Failure Point (intermediate Node) detects the route disruption
- Explicitly sends RFN to source and records the event
- Each intermediate Node that receives the RFN:
  - Invalidates the particular route
  - If it knows of an alternate route, that route is used for further communication and RFN is discarded
  - Otherwise, RFN is propagated towards source

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 22

So, in the case of a TCP-F this protocol, the failure point because it is a multi hop it is a multi hop network. So, the failure points the intermediate node basically failures any intermediate node is going to be a failure point because the link in between has broken. So, it basically detects are out disruption first. Then after that that node which has detected that the route has failed it explicitly sends the RFN to the source and records the event. Each intermediate node that receives the RFN that route failure notification invalidates the particular route, if it knows of an alternate route that route is used for further communication and the RFN is discarded or otherwise the route failure notification is propagated towards the source.

(Refer Slide Time: 28:11)



TCP-F: Protocol (contd.)

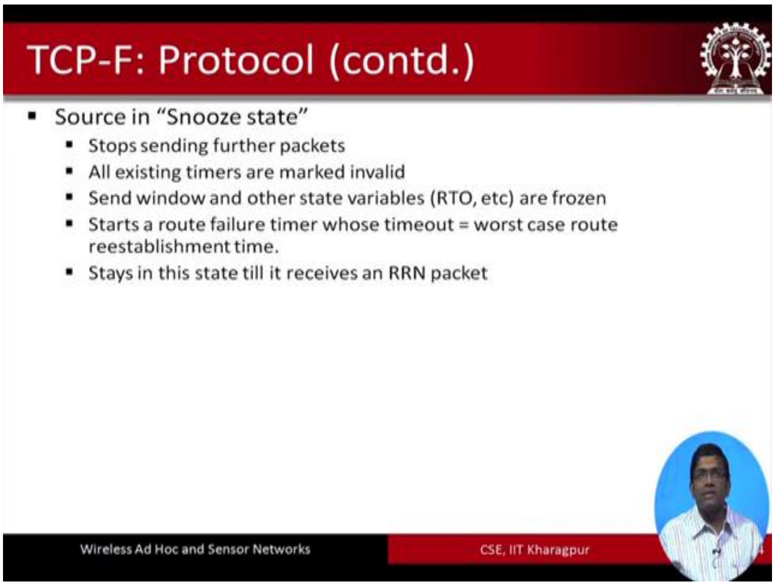
- On receiving RFN, source goes into “Snooze” state

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, pictorially this is how this protocol works. So, on receiving. So, there are 2 states in this protocol. One is the snooze state the other one is the established state. So, on receiving the route failure notification, packet the source basically goes to the snooze state. And then when the order in packet is received at the sender, the sender is transited from the snooze state back to the normal state the established state. So, this is the small state transition diagram and the showing the states the snooze and established states and the transitions that are going to happen.

(Refer Slide Time: 28:55)



TCP-F: Protocol (contd.)

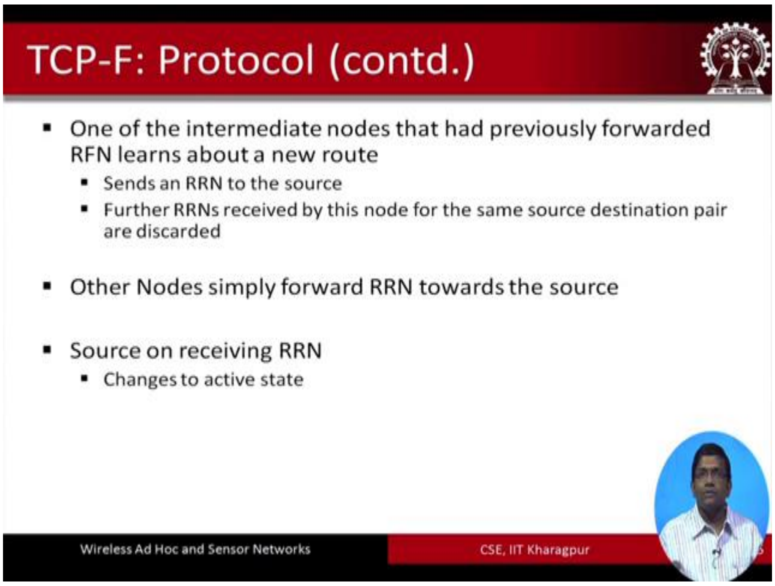
- Source in “Snooze state”
  - Stops sending further packets
  - All existing timers are marked invalid
  - Send window and other state variables (RTO, etc) are frozen
  - Starts a route failure timer whose timeout = worst case route reestablishment time.
  - Stays in this state till it receives an RRN packet

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, what does the source do more specifically in the snooze state. It does the following it stops sending the packets further all the existing timers are marked as invalid. It sends the window and other state variables window means the see window basically the congestion window size and other state variables and these are frozen. It starts a route failure timer whose timeout is equal to the worst case route we establishment time and it stays in this state till it receives an RRN packet.

(Refer Slide Time: 29:33)



TCP-F: Protocol (contd.)

- One of the intermediate nodes that had previously forwarded RFN learns about a new route
  - Sends an RRN to the source
  - Further RRNs received by this node for the same source destination pair are discarded
- Other Nodes simply forward RRN towards the source
- Source on receiving RRN
  - Changes to active state

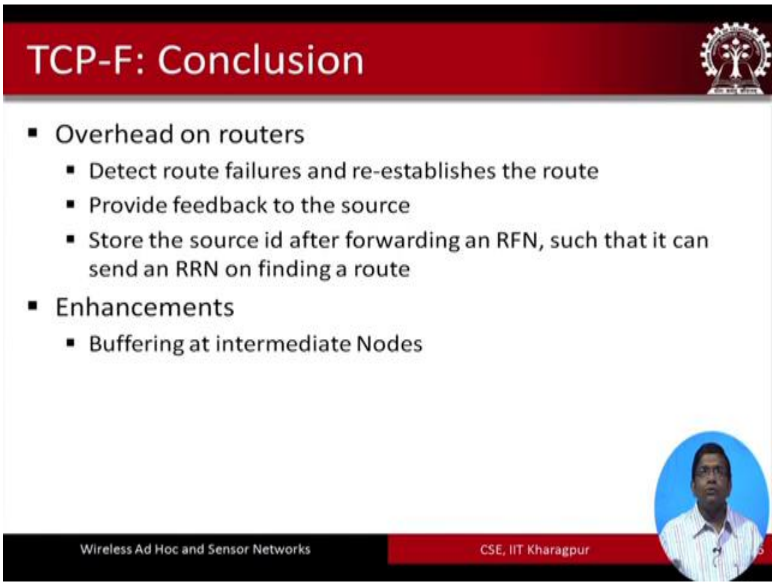
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

One of the intermediate nodes that had previously forwarded the RFN learns about a new route. Since the RRN to the sources because you know. So, it knows that the source has to be informed. The source has to be informed. So, what he does is it knows that earlier the RFN was sent through it now this intermediate node what it is going to do is it takes the ownership of informing the source by sending the RRN packet.

So, since an RRN to the source, further RRN received by this node for the same source destination pair are then discarded. Because it has send RRN 5 again increase the overall overhead communication overhead in the network. The other node simply forwards the RRN towards the source and the source on receiving the RRN changes to the active state.

(Refer Slide Time: 30:22)



TCP-F: Conclusion

- Overhead on routers
  - Detect route failures and re-establishes the route
  - Provide feedback to the source
  - Store the source id after forwarding an RFN, such that it can send an RRN on finding a route
- Enhancements
  - Buffering at intermediate Nodes

So, to conclude TCP-F gives an enhancement over running the regular TCP on Ad-Hoc networks; however, the routers in between the routers the nodes that are used routers means the nodes in the network. They are they have been basically subjected to additional overhead in terms of detection of route failures and reestablishment of route providing feedback to the source. Another overhead in terms of storing the source id after forwarding an RFN such that it can send the RRN on sending a route and so on.

So, these are the additional overheads on each of these different nodes each of these routers. I mean routers means you do not have a designated router in Ad-Hoc network. So, each of these nodes which act as a host are also acting as a router right and in terms of enhancement the buffering. So, what can be done is the TCP-F can be enhanced further in the future. So, that can be done by buffering at the intermediate nodes. So; that means, that the intermediate nodes instead of simply forwarding this packet that packet they can wait and wait and you know wait for these nodes to for the for the further acknowledgement to come, saying that the route has been restored and then you know starting from that point on instead of informing the source node.

(Refer Slide Time: 32:00)

References

- K. Chandran, S. Raghunathan, S. Venkatesan and R. Prakash, A feedback-based scheme for improving TCP performance in ad hoc wireless networks, IEEE Personal Communications
- C.-K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall PTR, NJ, 2002.
- S. Misra, I. Woungang, and S. C. Misra, Guide to Wireless Ad Hoc Networks, Springer, UK, 2008

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, these are some of the references the first references will give you the TCP-F, it is discussion on the TCP-F and the other 2 are the books, that we normally refer to for the other lectures of this course.

Thank you.