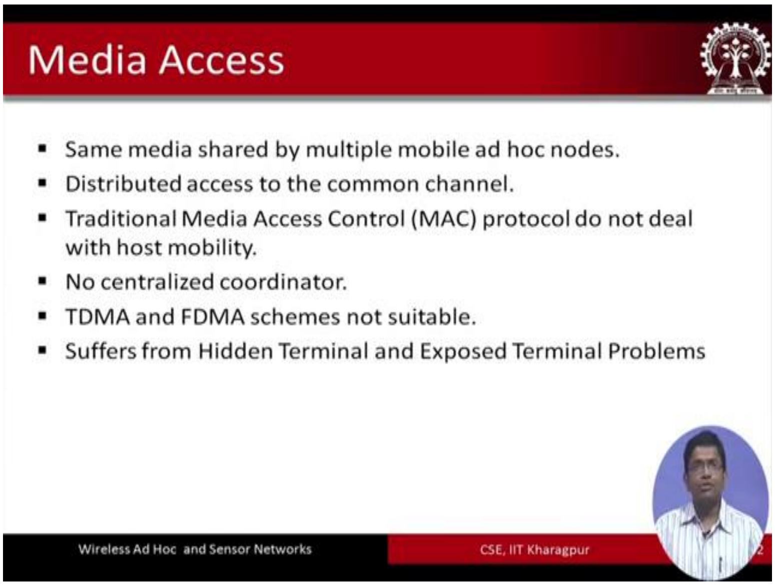
Wireless Ad Hoc and Sensor Networks

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

Lecture – 02
Introduction: Wireless Ad Hoc Network-Part-II

So, this is the second module for Wireless Ad Hoc networks. So, here in the first module we have already seen that there are different challenges that have to be overcome in order to implement and deploy these kind of networks, Ad Hoc networks. These indeed are very attractive, but at the same time the challenges are also huge. So, what are the different challenges that we will see over all the different lectures on Ad Hoc networks, but now for the next few moments we are going to go through some of the other challenges that are involved in deploying these networks we are going to look at them at high level and then in the next lectures we are going to go through them in more detail.

(Refer Slide Time: 01:23)



Media Access

- Same media shared by multiple mobile ad hoc nodes.
- Distributed access to the common channel.
- Traditional Media Access Control (MAC) protocol do not deal with host mobility.
- No centralized coordinator.
- TDMA and FDMA schemes not suitable.
- Suffers from Hidden Terminal and Exposed Terminal Problems

Wireless Ad Hoc and Sensor Networks

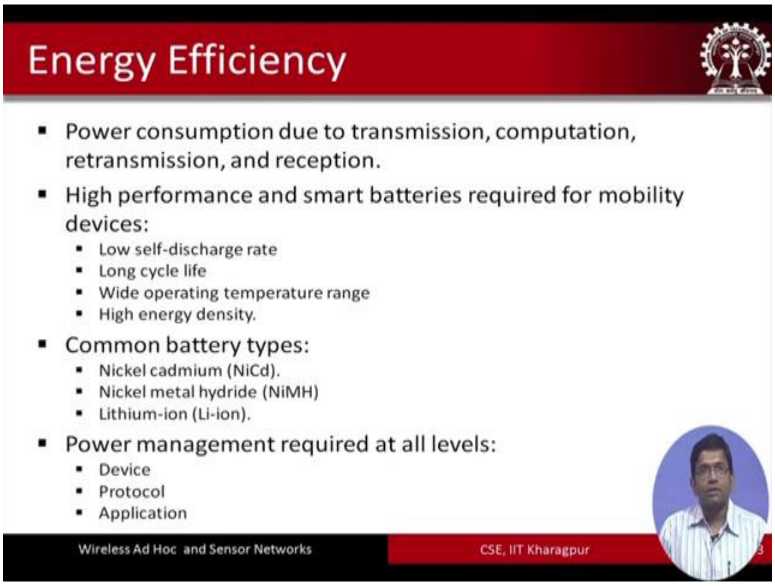
CSE, IIT Kharagpur

So, the first one is medium axis. So, as you know that medium axis is a property in the second layer, is a function in the second layer which is the link layer of the OSI stack and the medium access is all about that you have a collection of different nodes and these nodes this we share that the same medium and how one can you know, you know one can offer access to these different nodes in a fair manner is what medium access control is all about.

Now, there are different protocols that have been proposed for medium access control in different wire and wireless networks, but these are not very useful, these are not very useful in this kind of Ad Hoc network because what is required is to offer distributed access it is required in these networks to offer distributed access to the common channel. So, the channel is one and with in that particular channel there is a single channel and in this particular channel distributed axis has to be offered. So, the traditional MAC protocols that one is familiar of basically they do not deal with you know this kind of problem, additionally there is problem of host mobility in minutes which are also not dealt with in the traditional MAC protocols. And additionally what we have is an environment where there is no centralized coordinator.

So, consequently if there is no centralized coordinator the traditional schemes such as the TDMA time division multiple access or frequency division multiple access FDMA, these are schemes which are not very suitable for implementing in this kind of networks because you know if there is no centralized coordinator a designated one which can help in polling and you know in offering different slide time slots or frequencies to the different you know the different nodes. So, who is going to take care of this, because we do not have such an entity there is no centralized coordinator. And additionally there are issues called the hidden terminal problem and exposed terminal problems which basically haunt this kind of networks. So, there are multiple problems of medium access in these networks.

(Refer Slide Time: 03:59)



Energy Efficiency

- Power consumption due to transmission, computation, retransmission, and reception.
- High performance and smart batteries required for mobility devices:
  - Low self-discharge rate
  - Long cycle life
  - Wide operating temperature range
  - High energy density.
- Common battery types:
  - Nickel cadmium (NiCd).
  - Nickel metal hydride (NiMH)
  - Lithium-ion (Li-ion).
- Power management required at all levels:
  - Device
  - Protocol
  - Application

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Let us now talk about energy efficiency, a very important issue when it comes to Ad Hoc networks. As I said in module 1, that these networks the nodes in these networks the nodes in Ad Hoc networks they are battery powered. So, there is no infinite battery that powers these nodes and it is very limited so typically you know once the battery is fully charged it can be from you know it can last the batteries can last for you know couple of minutes to you know to a couple of hours right, a couple of hours at the most. So, that is the maximum that a fully charged battery in these networks, in the use, in these nodes in these networks they can last for.

So, there are different you know there are different ways in which energy has to be considered you know. So, energy is consumed due to transmission, due to computation, re transmission, by the different nodes the intermediate nodes who returns meet the packets that that it receives re transmission and reception of nodes. So, all of these computation, communication, reception, transmission, retransmission all of these things you know these tasks they consume power or energy.

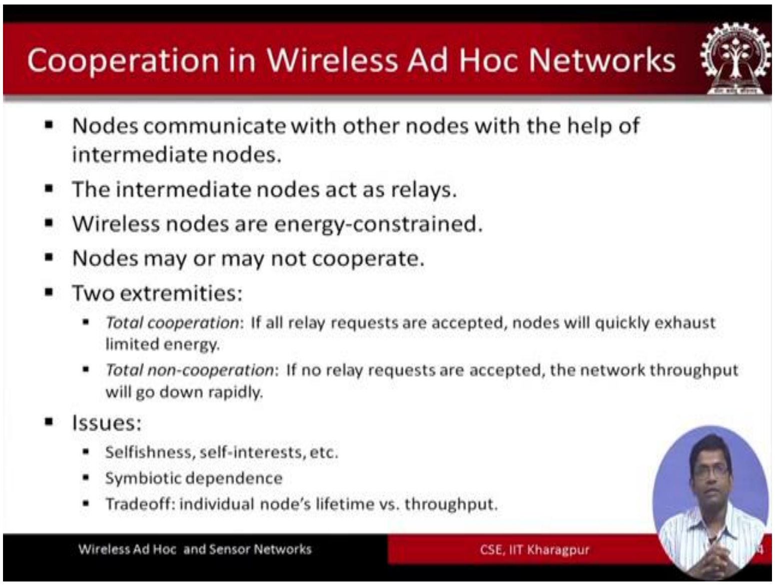
Now, at the same time we have seen that the batteries they have very limited life cycle they can operate you know once fully charged you know they will not be able to last for too long. So, additionally there are other issues with these batteries they have very you know, they have very highs discharge rate typically know the current they every batteries that are used in these Ad Hoc networks these have very high discharge rate, low you know life cycle and so on and so forth.

So, what is required is for using the nodes of these networks it is required to have high performance and smart batteries and which will support mobility of the devices also; that means, the mobile which can be used in the mobile devices and these batteries should have low self discharge rate, this would have long life cycle, they should be able to be operate, they should be able to operate in wide temperature ranges and they should have high energy density.

So, the commonly used batteries in this different nodes of these networks include the nickel cadmium NICD, NIMH nickel metal hydride, lithium ion; lithium ion is more common you know lithium ion batteries and, because the energy is very scarce in the different nodes of these networks what is required is to take care of energy, manage the energy at all levels of this networks bit at the device level the different protocols that are designed for these networks or the different applications that are you know design for use in these networks, at all different levels energy management is a very crucial issue.

Now, one thing you might have already observed that we are using the term energy and power in an interchangeable manner. So, as you are probably aware that energy and power they are you know inversely related, so sorry I am sorry energy and power, power is basically energy consumed per unit time. So, this is how energy and power are related and you know, so that is why we often interchangeably used these two terms.

(Refer Slide Time: 07:47)



Cooperation in Wireless Ad Hoc Networks

- Nodes communicate with other nodes with the help of intermediate nodes.
- The intermediate nodes act as relays.
- Wireless nodes are energy-constrained.
- Nodes may or may not cooperate.
- Two extremities:
  - *Total cooperation*: If all relay requests are accepted, nodes will quickly exhaust limited energy.
  - *Total non-cooperation*: If no relay requests are accepted, the network throughput will go down rapidly.
- Issues:
  - Selfishness, self-interests, etc.
  - Symbiotic dependence
  - Tradeoff: individual node's lifetime vs. throughput.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, next is cooperation, next issue is cooperation in wireless Ad Hoc networks, this is a very important issue this is that is typical of Ad Hoc networks because you know what we have is a multihop scenario source node sending to the destination node and this is something that we have already seen source node, sending the data to the destination node, the destination node is not within the direct transmission range of the source node.

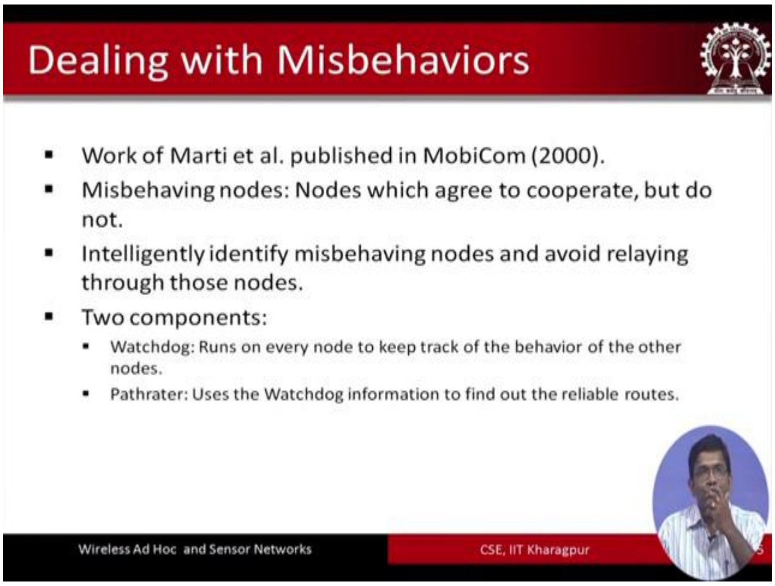
So, there are intermediate nodes which will act as relays for the data that is sent by the source node to be delivered to the intended destination node. So, we have these intermediate nodes which are acting as relays. So, quite understandably quite; obviously, these nodes they have to cooperate the intermediate relays would have to cooperate with the source and the destination node for retransmission to be successfully completed. And at the same time these nodes as we have already seen, all these nodes the relay nodes indeed are very much energy constrained.

So, naturally what happens like in a social network; that means a network of human beings for examples when there is you know scarcity of resources there is an issue of cooperativeness you know, some nodes may or may not be willing to cooperate. So, this sort of thing is typical of Ad Hoc networks. So, there are two extremities that is encountered with respect to cooperation in Ad Hoc networks - one is the case a case of total cooperation. So, if all the relay requests are accepted then we have a case of total cooperation; that means, the nodes they cooperate fully and that is not a very good thing because the nodes they themselves have very limited energy and if they relate all the requests that are you know that are sent to them then they are going to be there, they are going to exhaust of their energy quite fast and we have the case of total non cooperation on the other extremity where none of the relay requests that are sent to a particular node are accepted by it.

So, any packet that is sent to the node would be dropped by that particular node. So, the network throughput in such a case is going to go down quite rapidly; that means, the network is not going to function for too long. So, neither of these two extremities; that means, the extremity of total cooperation or the estimate of total non cooperation is ideal for implementing in these networks.

So, there are additional issues with respect to cooperation because of the above things that I just mentioned issues of selfishness, selfishness then self interest symbiotic dependence; that means, the nodes you know ideally would like to you know symmetrically depend on each other. So, if one node basically helps another node in relaying its packets though it would also expect that the other node is also going to help it in relaying, so there is some kind of mutual dependence symbiotic dependence that is basically you know typified in this between the different nodes in these networks.

(Refer Slide Time: 10:55)



Dealing with Misbehaviors

- Work of Marti et al. published in MobiCom (2000).
- Misbehaving nodes: Nodes which agree to cooperate, but do not.
- Intelligently identify misbehaving nodes and avoid relaying through those nodes.
- Two components:
  - Watchdog: Runs on every node to keep track of the behavior of the other nodes.
  - Pathrater: Uses the Watchdog information to find out the reliable routes.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

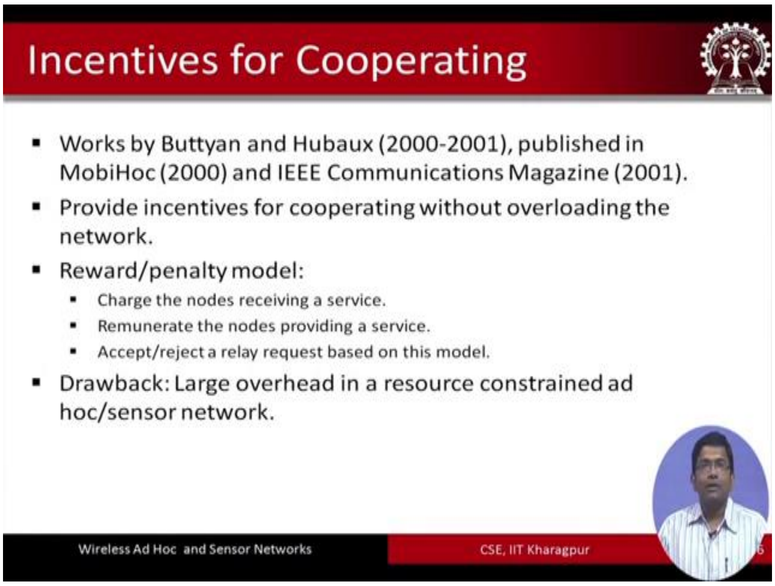
So, these networks because cooperation is a very important issue these networks have nodes which have a tendency to misbehave. So, one of the first works, one of the first on misbehavior in minutes was done by a group of a scientists Marti and others and it was published in a paper in a c m MobiCom in 2000. So, in their work in Marti et al's work they basically defined the misbehaving nodes to be the ones which agree to cooperate, but eventually who which do not write. So, initially they would agree to cooperate with the other nodes, but eventually when it comes to actually cooperating they do not.

So, what is important is to intelligently identify the misbehaving nodes and avoid relaying through these nodes this is what basically is important, that is this is basically fundamental thing that has to be implemented and this is what was proposed by Marti et al in their particular work.

So, in their proposed solution they have you know their solution to this particular problem has two components - one component is known as the watchdog which basically runs on every node to keep track of the behavior of the other nodes in the network and the other one is the path rater which basically uses the watchdog information to find out the reliable roots. So, watchdog is keeping an eye on the behavior or the misbehavior of the different nodes in the network, where as the path rater based on the observations of the watchdogs the path rater is determining that what which routes are the reliable ones;

that means, which nodes in the different nodes roots would help the packets to be delivered successfully to the intended destination node.

(Refer Slide Time: 12:48)



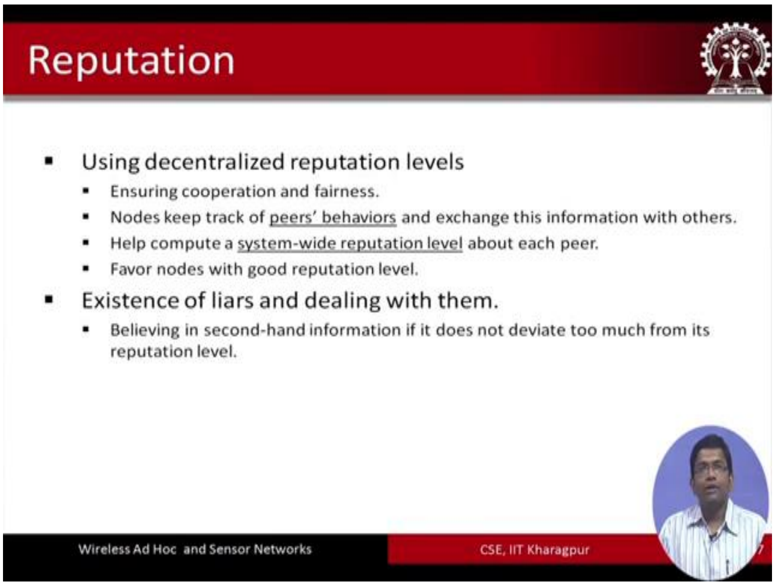
Incentives for Cooperating

- Works by Buttyan and Hubaux (2000-2001), published in MobiHoc (2000) and IEEE Communications Magazine (2001).
- Provide incentives for cooperating without overloading the network.
- Reward/penalty model:
  - Charge the nodes receiving a service.
  - Remunerate the nodes providing a service.
  - Accept/reject a relay request based on this model.
- Drawback: Large overhead in a resource constrained ad hoc/sensor network.

So, there are you know there were different other works with respect to cooperation works on incentive offering incentives for cooperation a bunch of European scientists Buttyan and Hubaux in the year 2000-2001. They published couple of works in MobiHoc and IEEE Communications Magazine where did suggest providing incentives for cooperation without overloading the network. So, what they proposed is some kind of a reward penalty model. In this particular model the nodes that are receiving a service are charged and the nodes which are providing the service they are immunerated and based on this particular model the different relay requests at the nodes they are either accepted or rejected.

So, the drawback of such a model is that there is large overhead that is involved in implementing such a model or such a solution and that is not very good in resource constrained networks that of networks and sensor networks alive.

(Refer Slide Time: 13:59)



Reputation

- Using decentralized reputation levels
  - Ensuring cooperation and fairness.
  - Nodes keep track of peers' behaviors and exchange this information with others.
  - Help compute a system-wide reputation level about each peer.
  - Favor nodes with good reputation level.
- Existence of liars and dealing with them.
  - Believing in second-hand information if it does not deviate too much from its reputation level.

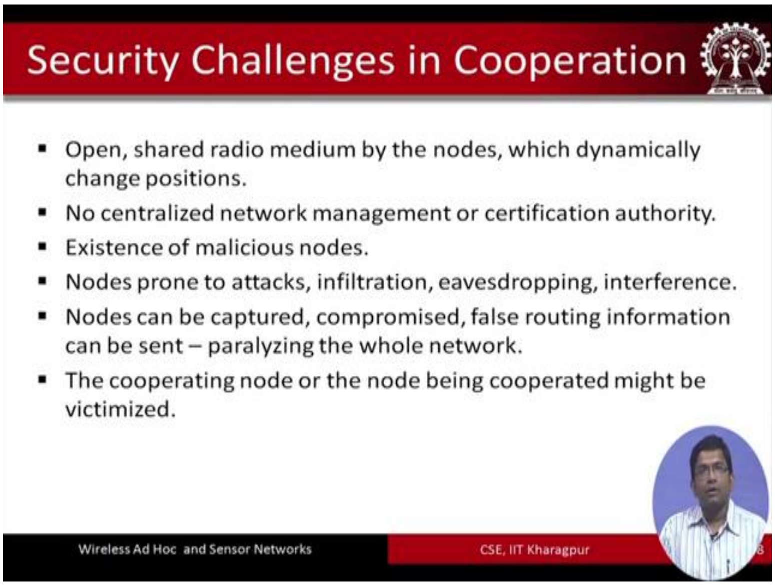
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

One of the ways of handling the issue of cooperation is to promote reputation promote you know keeping track of reputation of the behavior of the different nodes in the network. So, reputation means that how the different nodes are behaving so; that means, that if a particular node is sent a packet, keeping track that whether it is forwarding it or it is dropping it in between.

So, keeping track of this thing is a very important thing and how one keeps track of the reputation of the difference. So, if a node basically drops the packet; that means, it is not a node which is reliable. So, its reputation level is going to go down and if a node forwards then its reputation level is going to go up. And at the same time it is also important to track, to identify and track the liars in these networks you know which nodes are liars; that means, that the nodes which are believed to be able to cooperate, but which basically do not you know cooperate much they are not much cooperative. So, these are termed as the liars.

(Refer Slide Time: 15:11)



Security Challenges in Cooperation

- Open, shared radio medium by the nodes, which dynamically change positions.
- No centralized network management or certification authority.
- Existence of malicious nodes.
- Nodes prone to attacks, infiltration, eavesdropping, interference.
- Nodes can be captured, compromised, false routing information can be sent – paralyzing the whole network.
- The cooperating node or the node being cooperated might be victimized.

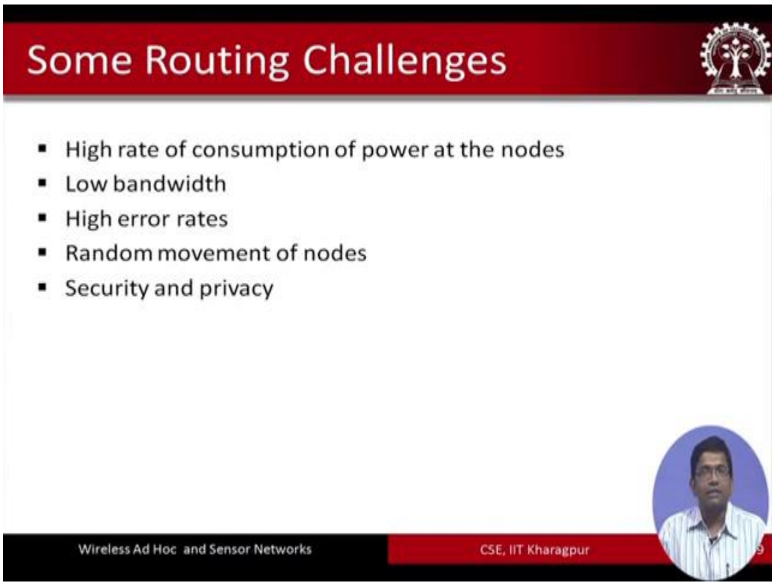
Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

There are security challenges in cooperation as well because you know ideally cooperation is very good you know it is a open medium you know which is shared by different nodes, same medium is shared by different nodes and these nodes they dynamically change positions. At the same time there is no centralized network management or certification authority and at the same time because it is open medium any node can get into the network and can be malicious and can hurt the functioning of any of the existing nodes in the network. So, these nodes are prone to attacks infiltration eavesdropping interference so on and so forth, all these different types of common attacks.

The main problem is that with the existing solutions one could have handled these problems because there are well known solutions how to handle attacks infiltration eavesdropping it etcetera etcetera, but here we cannot have we cannot assume that we will have you know a server which basically a server or a you know centralized authority which can you know keep track of the behavior and which can help in preventing these attacks. So, such a thing is not possible in these networks the Ad Hoc networks ok.

And on top of that if a node is cooperating with the other nodes it might so happen that it can fall victim from a malicious node because you know a malicious node can take advantage of the cooperating node it can send number of you know it continuously it can stream different data and this good node the co operative node it is going to soon run out of its existing limited resources, energy etcetera etcetera. So, it is very imp very easy to launch a denial of service kind of attack in these you know cooperative network environments.

(Refer Slide Time: 17:11)

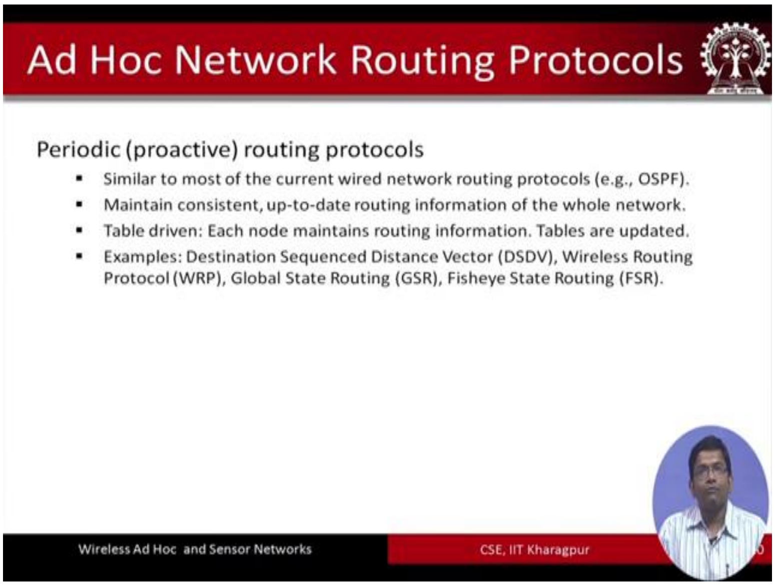


Some Routing Challenges

- High rate of consumption of power at the nodes
- Low bandwidth
- High error rates
- Random movement of nodes
- Security and privacy

There are some routing challenges as well because you know, so not only that we have a multihop kind of scenario, but at the same time we also have an environment which has high rate of consumption of power at the different nodes which has low bandwidth high error rates because the environment is such that there is high error rate and you know, what we have are the nodes that randomly they move from one point to another and so on. So, routing becomes a very important challenge and secured routing privacy aware routing are other different routing challenges that are you know very important considerations in these networks.

(Refer Slide Time: 17:53)



Ad Hoc Network Routing Protocols

Periodic (proactive) routing protocols

- Similar to most of the current wired network routing protocols (e.g., OSPF).
- Maintain consistent, up-to-date routing information of the whole network.
- Table driven: Each node maintains routing information. Tables are updated.
- Examples: Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR), Fisheye State Routing (FSR).

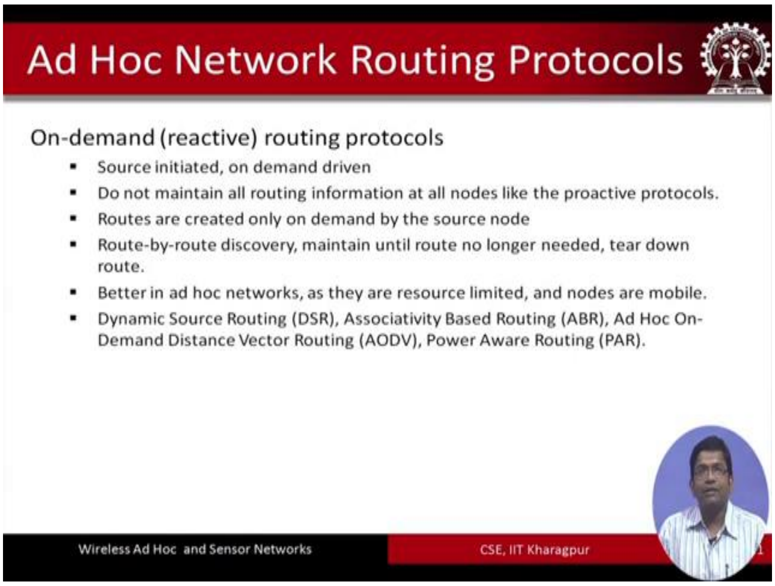
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, when we talk about routing in Ad Hoc networks let me just give you a very high level overview of what are the different routing solutions that are proposed for Ad Hoc networks. For using Ad Hoc networks the there are two classes of two main classes there are few others also, we will talk about now two main classes of routing protocols that are proposed for Ad Hoc networks. So, one is called the proactive routing protocols or periodic routing protocols sometimes these are also known as table based routing protocols.

So, the traditional weared routing protocols for example, OSPF which are table based belong to this particular category. So, these protocols they maintain consistent up to date routing information of the whole network and examples. So, that means, that at every node in the network the routing information is stored and these tables are updated periodically. So, examples of these networks are the DSDV protocol, the WRP protocol, GSR, FSR and so on and so on, there are many many more you know Ad Hoc network routing protocols belonging to this particular category that have been that has been proposed in the literature.

(Refer Slide Time: 19:10)



Ad Hoc Network Routing Protocols

On-demand (reactive) routing protocols

- Source initiated, on demand driven
- Do not maintain all routing information at all nodes like the proactive protocols.
- Routes are created only on demand by the source node
- Route-by-route discovery, maintain until route no longer needed, tear down route.
- Better in ad hoc networks, as they are resource limited, and nodes are mobile.
- Dynamic Source Routing (DSR), Associativity Based Routing (ABR), Ad Hoc On-Demand Distance Vector Routing (AODV), Power Aware Routing (PAR).

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

The other category of Ad Hoc network routing protocols is called the on demand or dative routing protocols. So, as this name suggests that whenever there is a demand the source node basically initiates route exploration discovery of route you know disk; that means, the you know the source node whenever it has to send some data and that you know it is not able to find the route to the intended destination node it is going to start the route discovery process. So, these solutions basically unlike the previous category which where table based here basically there are that you know these different nodes in these networks they do not maintain routing information like in the previous category.

So, the routes are created only on demand by the source node and, so typically there is a three phase kind of approach that is used in any kind of our most of the kinds of on demand reactive routing protocols. It first starts with the route discovery process phase route discovery phase then comes the route maintenance phase; that means, the roots are once discovered they are maintained until the root is no longer required and finally, when the root is no longer required there is the teardown phase; that means, the root is gone down.

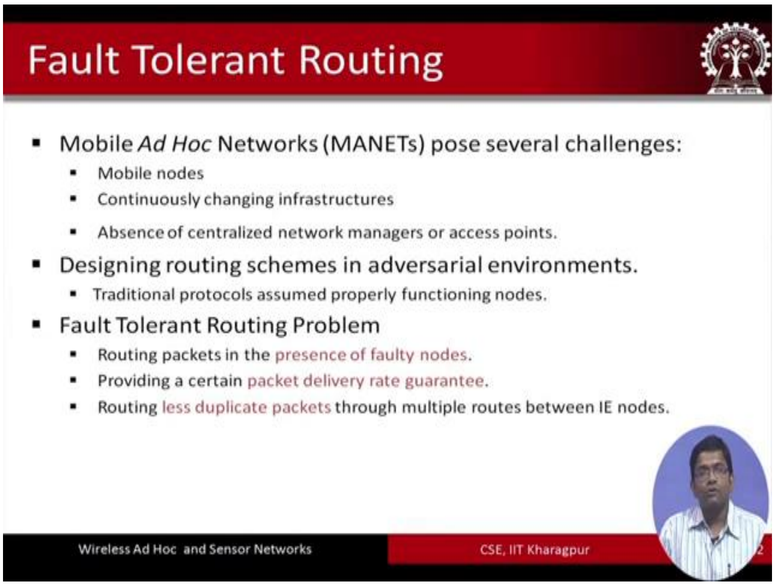
So, these are better in Ad Hoc networks you know these reactive routing protocols they are better in Ad Hoc networks as they are you know resource limited and the nodes are mobile, so because the nodes are mobiled, because the resource is very limited, so it is very important to you know to track the mobility of the nodes in the network and discover the roots whenever it is require. Because it is quite unlikely that in a very mobile environment you know the existing topology information is going to stay interact over time. So, the topology information gets changed over time and consequently it is better to you know discover the roots in these networks.

But keeping in mind this particular advantage we also should understand that when we talk about Ad Hoc networks it is not that all the time the topology is going to be you know made and broken quite fast in these networks. There are some networks where the topology may not be changing quite fast in such a case every time discovering the route maintaining etcetera etcetera as in a reactive routing protocol may not be a very good approach. So, in such cases maybe that using the proactive approach; that means, the table based approach would be a better solution. So, probably that you know in such a situation it might be better, it might be efficient to use the proactive routing protocols.

Deactivate routing are on the other hand as I just mentioned would be more efficient when we are using them in networks where the nodes are changing their positions quite fast; that means, the nodes are quite mobile and it is important to keep track of the mobility of the different nodes and based on that not keep track of the mobility of the nodes it is difficult to keep track of the mobility of the nodes and, so accordingly find the different routes in the network. So, some of the you know examples of Ad Hoc routing protocols belonging to the reactive category are the DSR dynamic source routing, associatively based routing ABR, UDV is a very popular protocol Ad Hoc on demand distance vector routing protocol and power aware routing protocol PAR.

So, like in the proactive category there are many more types of routing protocols belonging to this category that has been proposed in the literature.

(Refer Slide Time: 23:03)



Fault Tolerant Routing

- Mobile *Ad Hoc* Networks (MANETs) pose several challenges:
  - Mobile nodes
  - Continuously changing infrastructures
  - Absence of centralized network managers or access points.
- Designing routing schemes in adversarial environments.
  - Traditional protocols assumed properly functioning nodes.
- Fault Tolerant Routing Problem
  - Routing packets in the presence of faulty nodes.
  - Providing a certain packet delivery rate guarantee.
  - Routing less duplicate packets through multiple routes between IE nodes.

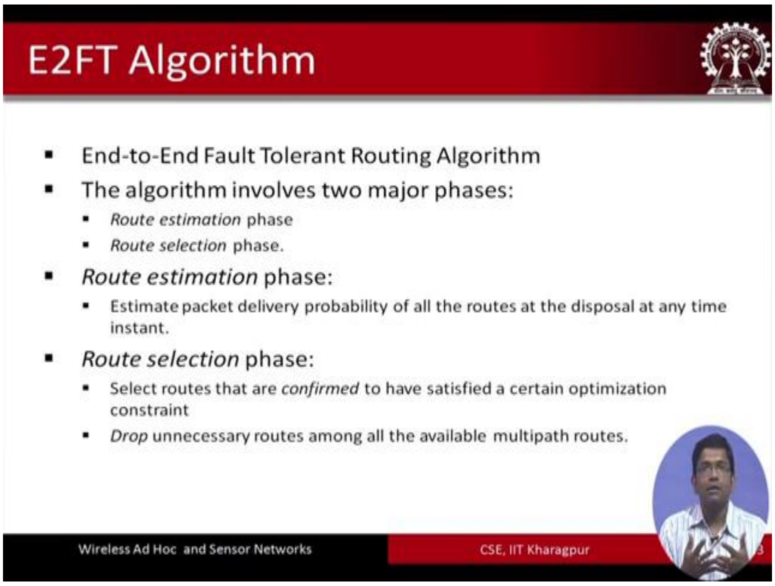
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

Another very important you know issue is fault tolerant routing which is something that I have worked on in my research before. So, this is this has been one of my research paper this led to one of my research papers that was published in the telecommunication systems journal.

So, here we talk about that you know false are quite common in minutes, so that is something that we have seen and packet drops result due to false, false could arise because maybe two nodes which were in the proximity of each other they are no longer in the proximity, maybe when one node moves and consequently packet is dropped in between. What there could be different other reasons why you know false could develop between different nodes in the network. So, there could be problems in the link; that means, failure in the link there could be faults in the node and so on. So, we basically proposed a fault tolerant solution to this particular problem.

(Refer Slide Time: 24:09)



E2FT Algorithm

- End-to-End Fault Tolerant Routing Algorithm
- The algorithm involves two major phases:
  - *Route estimation* phase
  - *Route selection* phase.
- *Route estimation* phase:
  - Estimate packet delivery probability of all the routes at the disposal at any time instant.
- *Route selection* phase:
  - Select routes that are *confirmed* to have satisfied a certain optimization constraint
  - *Drop* unnecessary routes among all the available multipath routes.

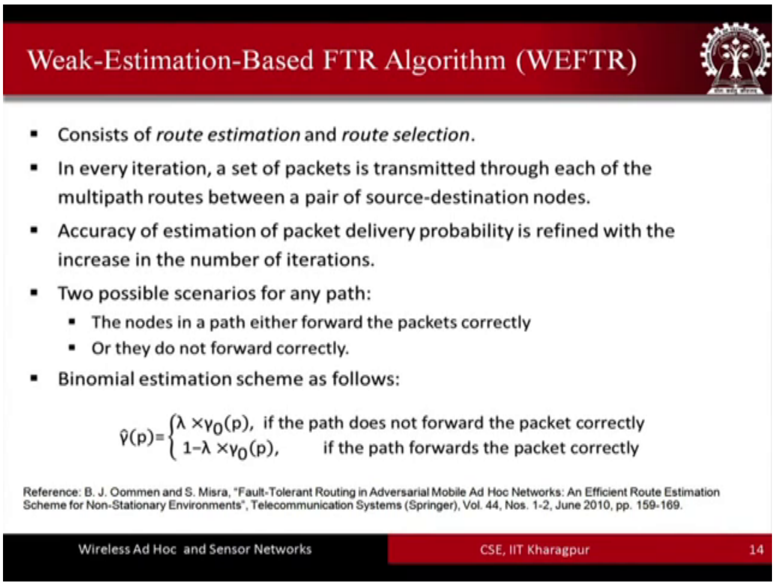
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, the fault tolerant routing problem it basically says that in the presence of fault how to efficiently route packets. So, faults are inevitable in Ad Hoc network. So, in the presence of faults how to route packets. So, one of the you know before our work, one of the previous works was the E to E F T algorithm, end to end fault tolerant routing algorithm this algorithm basically involves two major phases - one is called the route estimation phase the other one is the route selection phase. In the route estimation phase as the name suggests what is required is to estimate the packet delivery probability of all the routes at the disposal at any time instant.

So, you have number of possible routes. So, what is required between a source and destination pair. So, what is required is to estimate probabilistically estimate the packet delivery probability; that means, you know the probability of packet delivery through each of these different you know options which of these different routes. After that estimate is obtained then what the E to E F T algorithm does is it you know selects one of these routes that have confirmed to have satisfied a certain optimization constraint a particular threshold let us say a particular, particular threshold when it crosses that threshold. So, that particular route is selected and the other routes other possible routes are basically dropped and are not made available for routing.

(Refer Slide Time: 25:37)



Weak-Estimation-Based FTR Algorithm (WEFTR)

- Consists of *route estimation* and *route selection*.
- In every iteration, a set of packets is transmitted through each of the multipath routes between a pair of source-destination nodes.
- Accuracy of estimation of packet delivery probability is refined with the increase in the number of iterations.
- Two possible scenarios for any path:
  - The nodes in a path either forward the packets correctly
  - Or they do not forward correctly.
- Binomial estimation scheme as follows:

$$\hat{\gamma}(p)=\begin{cases}\lambda \times \gamma_0(p), & \text{if the path does not forward the packet correctly}\\ 1-\lambda \times \gamma_0(p), & \text{if the path forwards the packet correctly}\end{cases}$$

Reference: B. J. Oommen and S. Misra, "Fault-Tolerant Routing in Adversarial Mobile Ad Hoc Networks: An Efficient Route Estimation Scheme for Non-Stationary Environments", Telecommunication Systems (Springer), Vol. 44, Nos. 1-2, June 2010, pp. 159-169.

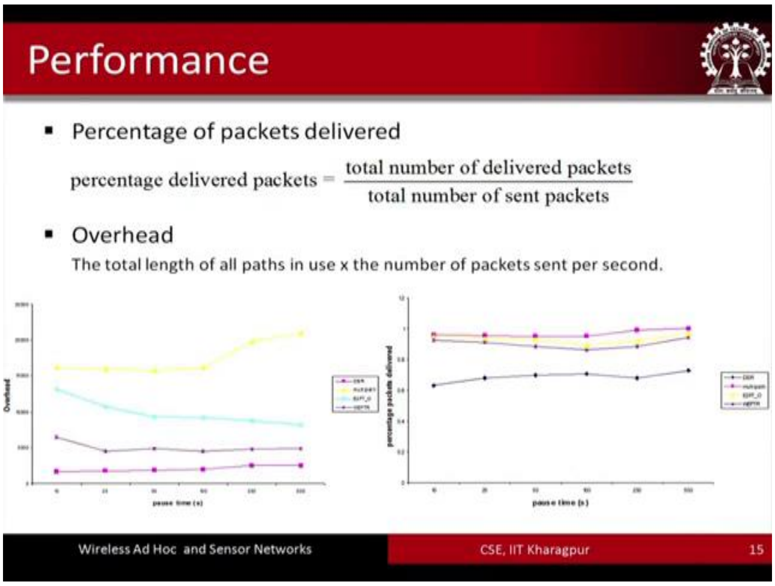
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

14

So, our algorithm that we proposed was as I told you it was published in the telecommunication systems journal by Springer and it is known as the WEFTR week estimation based FTR fault tolerant routing algorithm. So, here also we have the route estimation on the route selection phase, but the way we estimate the packet delivery probability through each of these different alternatives that we have seen in the you know E to E F T algorithm. So, that basically does not exist you know, so we have improved upon that we have proposed a week estimation based learning mechanism for estimating the probability of delivering packets through the different routes. So, this is the improvement that we have done over the E to E F T algorithm.

(Refer Slide Time: 26:31)



Performance

- Percentage of packets delivered

$$\text{percentage delivered packets} = \frac{\text{total number of delivered packets}}{\text{total number of sent packets}}$$

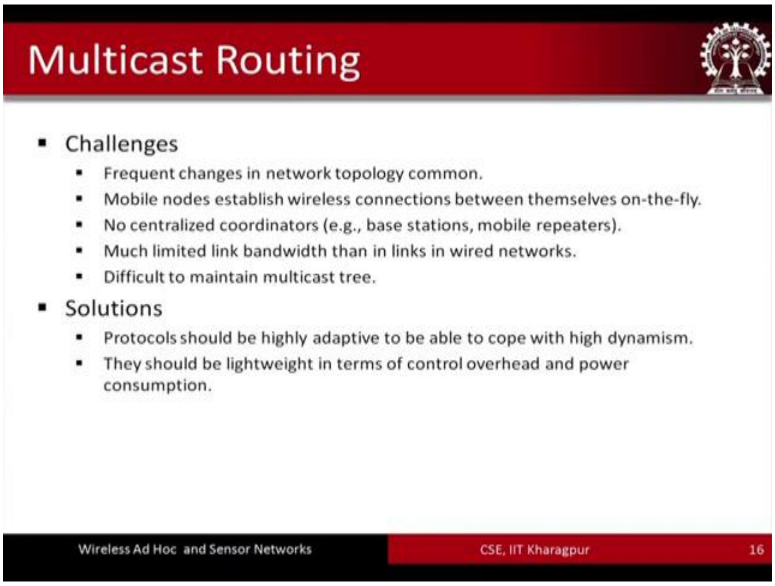
- Overhead

The total length of all paths in use x the number of packets sent per second.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 15

And here is a comparison of performance with respect to criteria such as the percentage of delivered packets the overhead etcetera and we have seen that you know the proposed algorithm performs you know better with respect to you know; that means, that it has a lower overhead and hire packet delivery probability; that means, that there is better probability of delivering packets to the intended destination by using the WEFTR algorithm. So, what we talked about is unicast routing.

(Refer Slide Time: 27:03)



Multicast Routing

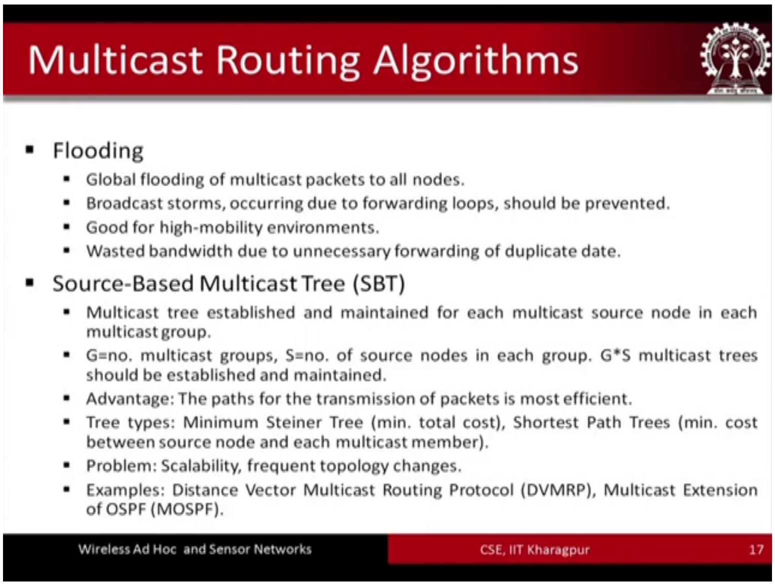
- Challenges
  - Frequent changes in network topology common.
  - Mobile nodes establish wireless connections between themselves on-the-fly.
  - No centralized coordinators (e.g., base stations, mobile repeaters).
  - Much limited link bandwidth than in links in wired networks.
  - Difficult to maintain multicast tree.
- Solutions
  - Protocols should be highly adaptive to be able to cope with high dynamism.
  - They should be lightweight in terms of control overhead and power consumption.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 16

Now, what about multicast? So, we have as we have seen in minutes we have an environment where the topology changes quite first we have frequent changes in the network topology and the nodes they move on the fly connections are made and broken on the fly and so on and on at the same time we do not have we cannot assume the existence of a centralized coordinator like a base station or a mobile repeater.

So, the traditional approaches to multi casting which are typically based on forming and maintaining trees known as multicast trees are not quite useful in these environments. So, protocols have to be proposed, new protocols have to be proposed which will be highly adaptive to be able to cope with the high degrees of dynamism that is typical of these environments.

(Refer Slide Time: 28:00)



Multicast Routing Algorithms

- Flooding
  - Global flooding of multicast packets to all nodes.
  - Broadcast storms, occurring due to forwarding loops, should be prevented.
  - Good for high-mobility environments.
  - Wasted bandwidth due to unnecessary forwarding of duplicate date.
- Source-Based Multicast Tree (SBT)
  - Multicast tree established and maintained for each multicast source node in each multicast group.
  - G=no. multicast groups, S=no. of source nodes in each group. G*S multicast trees should be established and maintained.
  - Advantage: The paths for the transmission of packets is most efficient.
  - Tree types: Minimum Steiner Tree (min. total cost), Shortest Path Trees (min. cost between source node and each multicast member).
  - Problem: Scalability, frequent topology changes.
  - Examples: Distance Vector Multicast Routing Protocol (DVMRP), Multicast Extension of OSPF (MOSPF).

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 17

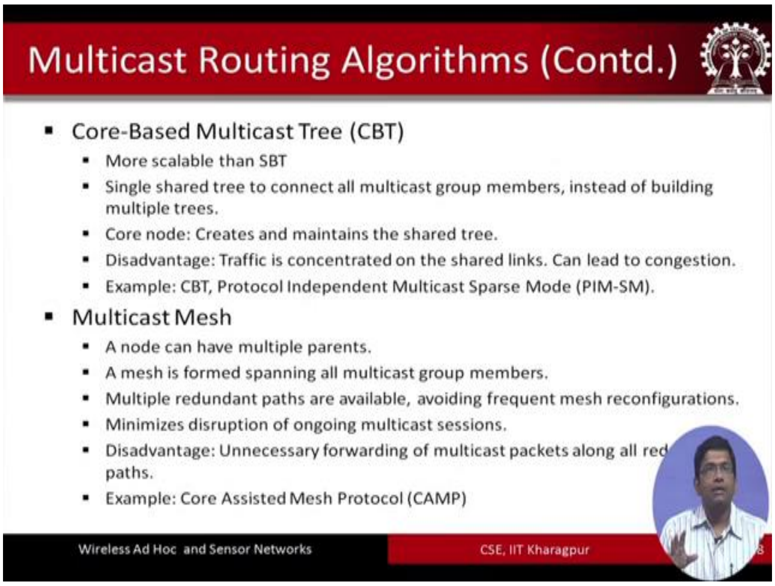
So, there are different classes of multicast routing algorithms that have been proposed we will talk about these in detail later on. So, broadly they can be classified as flooding algorithms or source based tree algorithms, core based multicast routing and group based multicast routing. So, these are some of the different categories of multicast routing algorithms that have been proposed purely for use in Ad Hoc networks. Flooding algorithms are like other flooding algorithms that you might be familiar with, if you have taken a networks course before.

So, where global, where basically you know the packets the multicast packets are basically flooded globally in the network. So, you know, so that this sort of approach is good if the environment itself is highly mobile; that means, the nodes are moving quite fast; however, it leads to wasted bandwidth due to unnecessary forwarding of duplicate data and that is also not a quite good thing for use in Ad Hoc networks because we have a very limited you know resource constrained environment and that is not very good. But at the same time if the nodes are moving quite fast you do not have any other option was do, but to go for a knife flooding based approach.

Source based multicast tree, so here multicast trees are established and maintained for each multicast source node in each multicast group. So, if we have G number of multicast groups and S number of source nodes in each group. So, what is required is to have maintained, it is required to maintain g times s number of multicast trees and that is not a very good thing because that will lead to you know a solution which is not very scalable. That means, if the number of nodes increase if the number of you know multicast groups increase or the number of source nodes per group increases. So, it will lead to soon it will lead to a very you know not a very elegant solution in these networks.

Examples of this include you know different multicast source based multicast tree approach protocols include the DVMRP protocol, MOSPF protocol and so on.

(Refer Slide Time: 30:14)



Multicast Routing Algorithms (Contd.)

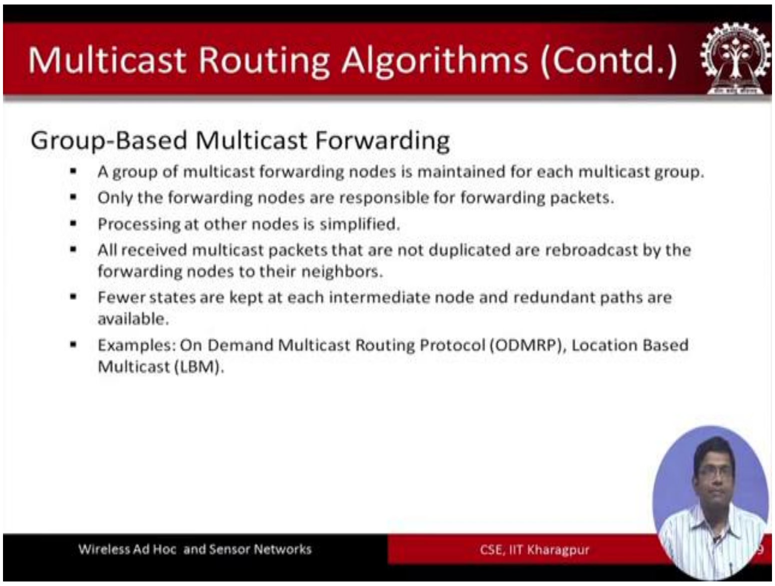
- Core-Based Multicast Tree (CBT)
  - More scalable than SBT
  - Single shared tree to connect all multicast group members, instead of building multiple trees.
  - Core node: Creates and maintains the shared tree.
  - Disadvantage: Traffic is concentrated on the shared links. Can lead to congestion.
  - Example: CBT, Protocol Independent Multicast Sparse Mode (PIM-SM).
- Multicast Mesh
  - A node can have multiple parents.
  - A mesh is formed spanning all multicast group members.
  - Multiple redundant paths are available, avoiding frequent mesh reconfigurations.
  - Minimizes disruption of ongoing multicast sessions.
  - Disadvantage: Unnecessary forwarding of multicast packets along all red paths.
  - Example: Core Assisted Mesh Protocol (CAMP)

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Core base tree basically you know what is done is it is, what it does is it creates and maintains a single shear tree connecting different multicast group members, so that is the approach that is adopted in the core based multicast trees. And this is a very you know this is a better solution than the SBT is; that means, the source based trees, but at the same time this also had this disadvantages because traffic is concentrated in the solutions on the share links only and that can often lead to condition in these share links.

Multicast mesh is another one where a node can have multiple parents and mesh is formed spanning all multicast group members and it is good in terms of ensuring reliability, but it is bad, it is advantageous because there is unnecessary forwarding of multicast packets along all the redundant paths. Example of multicast mesh routing protocol for Ad Hoc networks is the camp protocol which is the full form of which is the core assisted mesh network protocol.

(Refer Slide Time: 31:22)



Multicast Routing Algorithms (Contd.)

Group-Based Multicast Forwarding

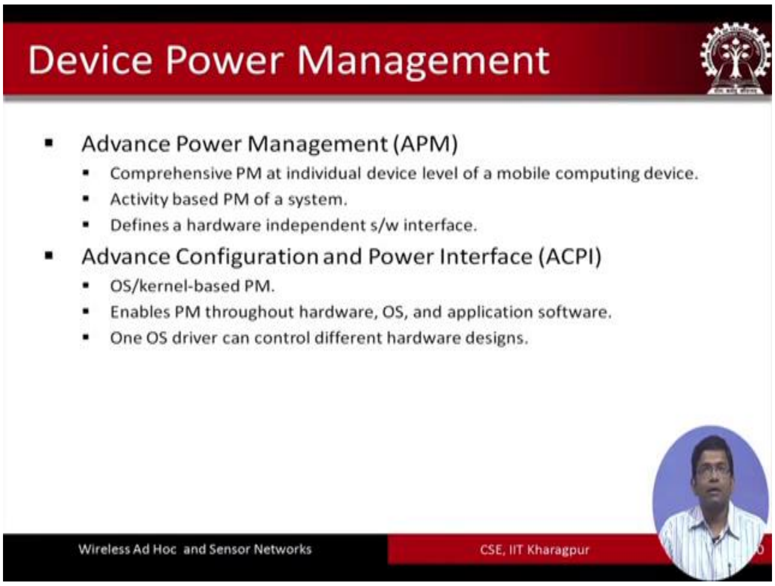
- A group of multicast forwarding nodes is maintained for each multicast group.
- Only the forwarding nodes are responsible for forwarding packets.
- Processing at other nodes is simplified.
- All received multicast packets that are not duplicated are rebroadcast by the forwarding nodes to their neighbors.
- Fewer states are kept at each intermediate node and redundant paths are available.
- Examples: On Demand Multicast Routing Protocol (ODMRP), Location Based Multicast (LBM).

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

And finally, the group based you know a multicast forwarding where a group of multicast forwarding nodes is maintained for each multicast group only the forwarding nodes are responsible for forwarding the packets processing at other nodes is simplified. All received multicast packets that are not duplicated and rebroadcasted by the forwarding nodes to the all received pack or multicast packets are not duplicated and are rebroadcast by the forwarding nodes to their neighbors. And, example of group based multicast forwarding include on demand multicast routing protocol ODMRP and the location based multicast routing protocol.

(Refer Slide Time: 32:03)



Device Power Management

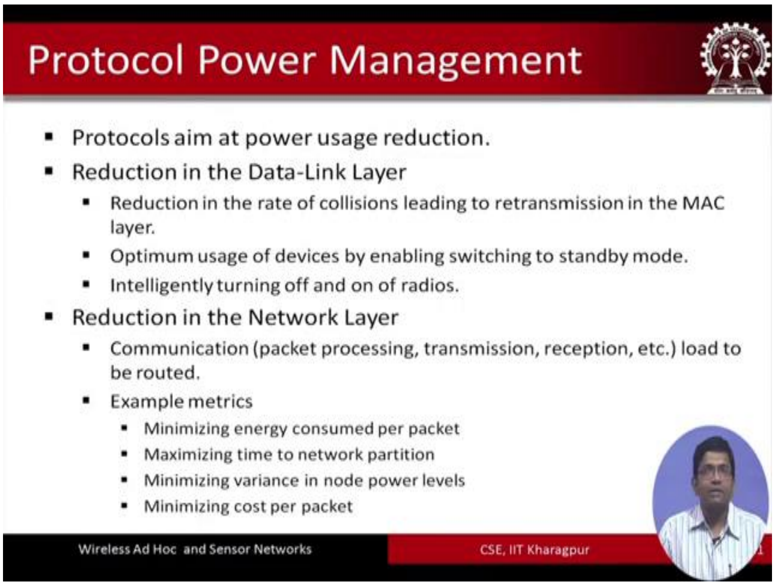
- Advance Power Management (APM)
  - Comprehensive PM at individual device level of a mobile computing device.
  - Activity based PM of a system.
  - Defines a hardware independent s/w interface.
- Advance Configuration and Power Interface (ACPI)
  - OS/kernel-based PM.
  - Enables PM throughout hardware, OS, and application software.
  - One OS driver can control different hardware designs.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

And few you know a few other important issues in Ad Hoc networks power is an important issue that we have already seen. So, what is required is not only at the protocol level not only at the algorithmic level it is also required to have devices manage the power right. So, there are different manager device manager, device power management techniques that have been proposed APM is one, ACPI is another. APM stands for advanced power management which basically comes with a comprehensive power management scheme at individual device level of the mobile computing devices and which divine defines a hardware independent software solution. ACPI is also quite similar, we will talk about this later, but just as a cursory level this is what device power management does.

(Refer Slide Time: 32:54)



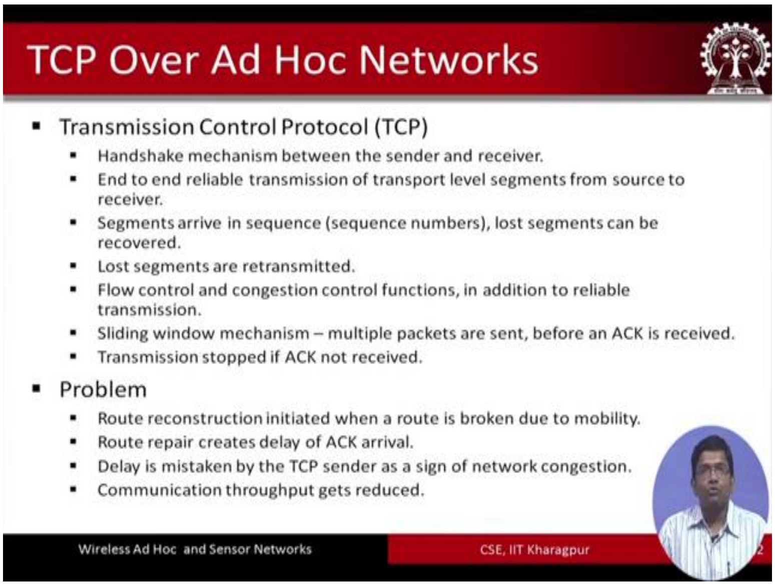
Protocol Power Management

- Protocols aim at power usage reduction.
- Reduction in the Data-Link Layer
  - Reduction in the rate of collisions leading to retransmission in the MAC layer.
  - Optimum usage of devices by enabling switching to standby mode.
  - Intelligently turning off and on of radios.
- Reduction in the Network Layer
  - Communication (packet processing, transmission, reception, etc.) load to be routed.
  - Example metrics
    - Minimizing energy consumed per packet
    - Maximizing time to network partition
    - Minimizing variance in node power levels
    - Minimizing cost per packet

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Protocol power management is required, protocol we know at all different layers the different protocols that are proposed in the protocol architecture, they you know they all have to ensure that you know they consume very less power, reduction there should be reduction in the data link layer, reduction in power consumption in data link layer. There should be deduction in power consumption at the network layer at the transport layer and so on. So, these are the different things that have to be taken care of at the different layers.

(Refer Slide Time: 33:24)



TCP Over Ad Hoc Networks

- Transmission Control Protocol (TCP)
  - Handshake mechanism between the sender and receiver.
  - End to end reliable transmission of transport level segments from source to receiver.
  - Segments arrive in sequence (sequence numbers), lost segments can be recovered.
  - Lost segments are retransmitted.
  - Flow control and congestion control functions, in addition to reliable transmission.
  - Sliding window mechanism – multiple packets are sent, before an ACK is received.
  - Transmission stopped if ACK not received.
- Problem
  - 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

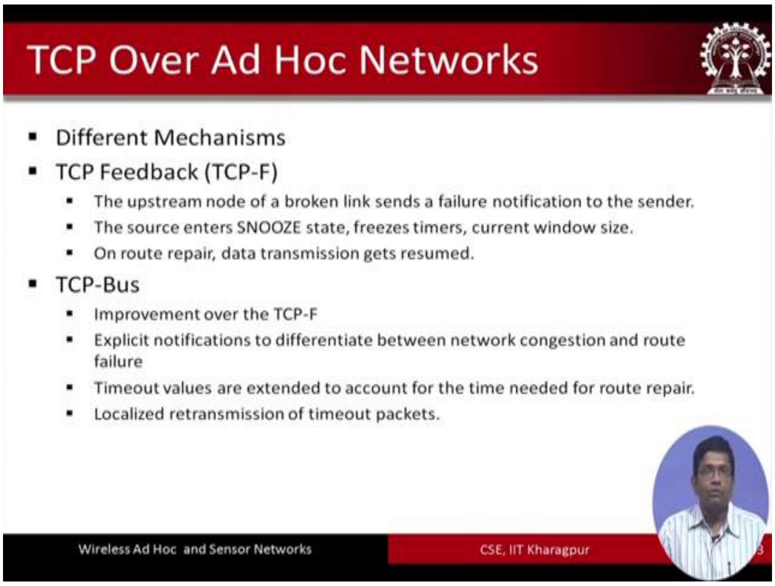
So, one other important thing is that we have talked about routing on top of routing is the transport layer protocol common transport layer protocol that is used in the internet is the transmission control protocol TCP, and as we know that in TCP there is some kind of a handshaking door that goes on between the sender and the receive receiver right. So, basically you know segments are sent from the sender and in a sequence and these segments in the sequence they are supposed to be received at the receiver intended receiver.

But it might so happen that some of these segments can be lost in between and these lost segments have to be retransmitted. So, there are different other issues that are associated which are like you know control of flow of these segments between the intended transmit transmitter between the transmitter and the receiver. So, flow control, congestion control; that means, that you know if the receiver is receiving at a rate which is more than how it can handle or the rate at which it can handle then what is going to happen is that at the receiver end the you know there will be congestion and consequently there will be packet drop, so that is undesirable ok.

So, this problem has to be you know handled, but the main problem is that if you want to use the TCP in Ad Hoc networks. So, typically you know the network layer first what it does is once a link is broken one of the existing routes is broken, due to maybe no mobility or something like that the you know it basically you know initiates, the route the network layer would initiate the route repair and this route repair basically creates delay of acknowledgement arrival and this delay is mistaken by the TCP sender; that means, the transmitter as a sign of network congestion and consequently the congestion control mechanisms are invoked by the transport layer and because of this basically the communication throughput who is going to go down drastically.

So, this is the problem with using the traditional TCP. The TCP that was proposed for you know internet for use in the internet using it for Ad Hoc networks is a big challenge.

(Refer Slide Time: 35:57)



TCP Over Ad Hoc Networks

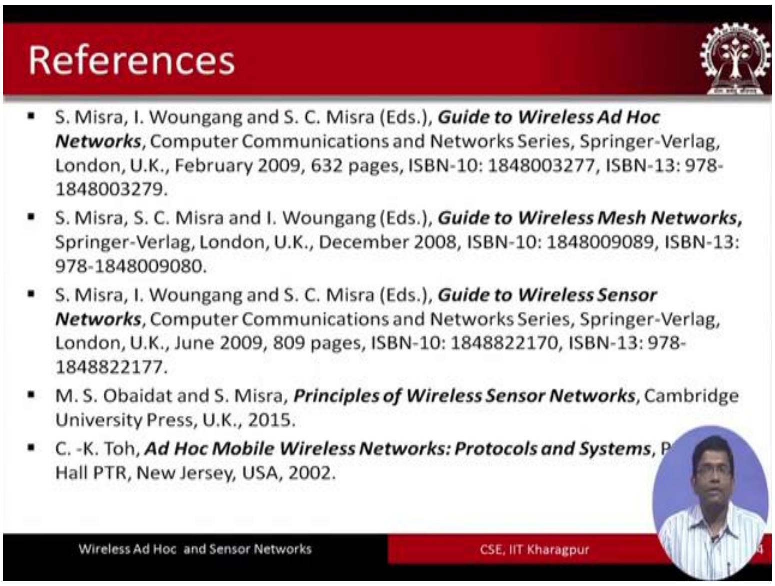
- Different Mechanisms
- TCP Feedback (TCP-F)
  - The upstream node of a broken link sends a failure notification to the sender.
  - The source enters SNOOZE state, freezes timers, current window size.
  - On route repair, data transmission gets resumed.
- TCP-Bus
  - Improvement over the TCP-F
  - Explicit notifications to differentiate between network congestion and route failure
  - Timeout values are extended to account for the time needed for route repair.
  - Localized retransmission of timeout packets.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, there are different protocols we will talk about these protocols that perform better than the traditional TCP for use in Ad Hoc networks. TCP feedback is one TCP bus is another one there are many other different types of mechanisms that have been proposed for use transport, for taking care of transport layer issues in Ad Hoc networks.

(Refer Slide Time: 36:21)



References

- S. Misra, I. Woungang and S. C. Misra (Eds.), ***Guide to Wireless Ad Hoc Networks***, Computer Communications and Networks Series, Springer-Verlag, London, U.K., February 2009, 632 pages, ISBN-10: 1848003277, ISBN-13: 978-1848003279.
- S. Misra, S. C. Misra and I. Woungang (Eds.), ***Guide to Wireless Mesh Networks***, Springer-Verlag, London, U.K., December 2008, ISBN-10: 1848009089, ISBN-13: 978-1848009080.
- S. Misra, I. Woungang and S. C. Misra (Eds.), ***Guide to Wireless Sensor Networks***, Computer Communications and Networks Series, Springer-Verlag, London, U.K., June 2009, 809 pages, ISBN-10: 1848822170, ISBN-13: 978-1848822177.
- M. S. Obaidat and S. Misra, ***Principles of Wireless Sensor Networks***, Cambridge University Press, U.K., 2015.
- C. -K. Toh, ***Ad Hoc Mobile Wireless Networks: Protocols and Systems***, P Hall PTR, New Jersey, USA, 2002.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

So, here are some of the references for the first two modules you know, so you know one can consult any of these different books some of these materials and the different concepts are borrowed from these books. So, the first two modules you know the references are given over here.

Thank you.