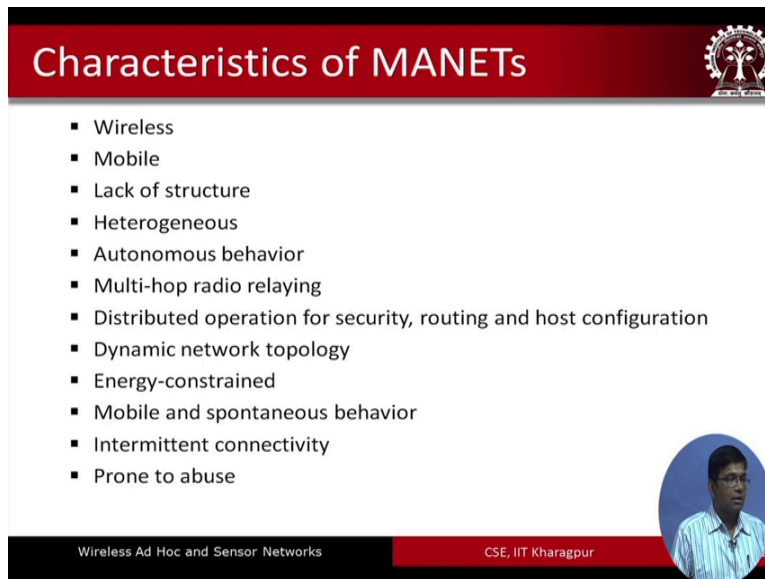


Wireless Ad Hoc and Sensor Networks
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 04
Cooperation in Mobile Ad Hoc Networks-Part-I

The next topic is cooperation in ad hoc networks. Cooperation as we have seen in the introduction is a very important issue, a very important topic when it concerns ad hoc networks. Without cooperation, without successful cooperation between the different nodes in the network, the networks are not going to survive at all. So, let us look at the different ways in which cooperation is ensured in ad hoc networks.

(Refer Slide Time: 00:55)



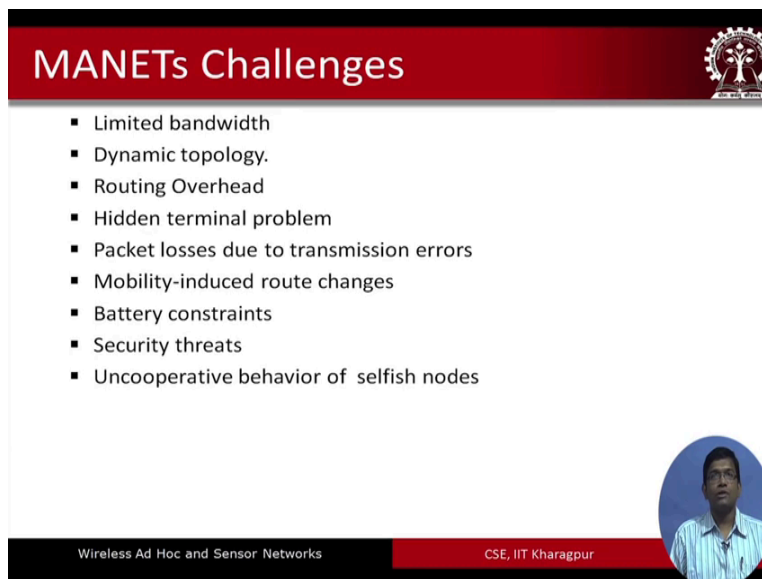
The slide displays the title "Characteristics of MANETs" in a red header bar. To the right of the title is the IIT Kharagpur logo. Below the title is a list of 13 characteristics of MANETs, each preceded by a square bullet point. At the bottom of the slide, there is a footer with the text "Wireless Ad Hoc and Sensor Networks" on the left and "CSE, IIT Kharagpur" on the right. A small circular portrait of Prof. Sudip Misra is located in the bottom right corner of the slide content area.

- Wireless
- Mobile
- Lack of structure
- Heterogeneous
- Autonomous behavior
- Multi-hop radio relaying
- Distributed operation for security, routing and host configuration
- Dynamic network topology
- Energy-constrained
- Mobile and spontaneous behavior
- Intermittent connectivity
- Prone to abuse

So, before we do so let us first review some of the characteristics of ad hoc networks. So, this is what we have already seen, we know that ad hoc networks operate the nodes in the networks. They operate in the wireless environment, wireless medium, they are mobile, the nodes are mobile, there is no definite structure of these networks. So, basically a collection of nodes, they are going to talk to one another and there is no 1 topology that governs these networks. The nodes could be heterogeneous having different specifications. They have, you know the ad hoc networks they basically exhibit autonomous behavior; that means, they should be able to, you

know, to survive on their own. They should be able to operate on their own and whenever there is some kind of abnormality, they would be able to survive through such kind of situations. Multi hop radio relaying is another that we have already seen, distributed operation for security routing and host configuration is another property. So, I do not need to elaborate this we have already understood this particular aspect. Dynamic network topology is another, energy constrained behavior, mobile and spontaneous behavior, intermittent connectivity and the different nodes in the networks are prone to different types of abuse, different kinds of attacks and so on, these are some of the typical characteristics of mobile ad hoc networks.

(Refer Slide Time: 02:39)



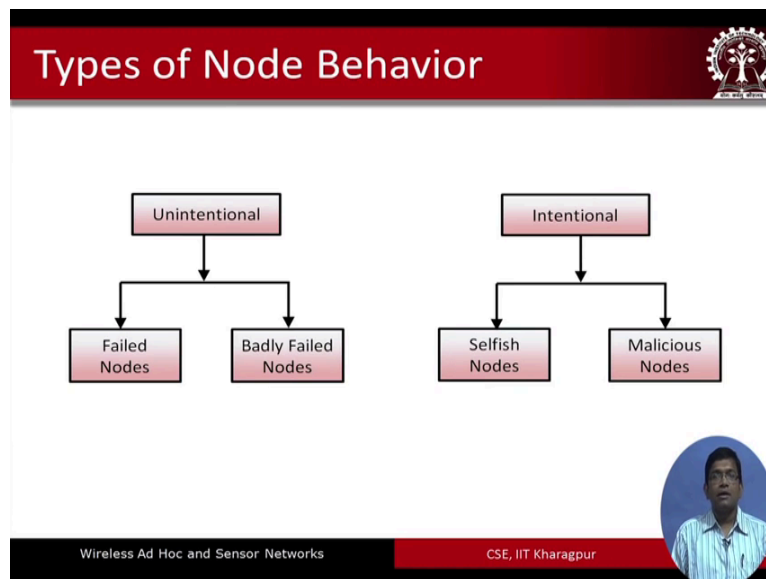
The slide is titled "MANETs Challenges" and features a list of ten challenges. In the top right corner, there is a circular logo of IIT Kharagpur. In the bottom right corner, there is a circular portrait of a man in a blue shirt. The slide footer contains the text "Wireless Ad Hoc and Sensor Networks" and "CSE, IIT Kharagpur".

- Limited bandwidth
- Dynamic topology.
- Routing Overhead
- Hidden terminal problem
- Packet losses due to transmission errors
- Mobility-induced route changes
- Battery constraints
- Security threats
- Uncooperative behavior of selfish nodes

Let us look at some of the challenges in enabling these networks. So, all these things we have already gone through. So, let us just review them quickly. So, the first is the limited bandwidth of the environment, dynamic changes in the topology. So, the nodes are supposed to be very mobile in a MANET particularly. So, there the topology is all also going to be made and broken quite fast and reformed faster. So, routing overhead is another, because you know whenever the nodes move, the topology changes and there is going to be overhead in you know in discovering the routes once again and maintaining the route information at the different nodes. So, all these things basically bring in a lot of routing overhead.

Hidden terminal problem this is something that we will look at when we you know when we look at a medium access control, hidden terminal problem and exposed terminal problems, packet losses due to transmission errors, mobility induced route changes, battery constraints we have seen already in the introduction. So, there are different, you know, severe constraints on energy consumption in these different nodes because the batteries have very small amount of energy that comes with them, security threats and uncooperative behavior of the selfish nodes.

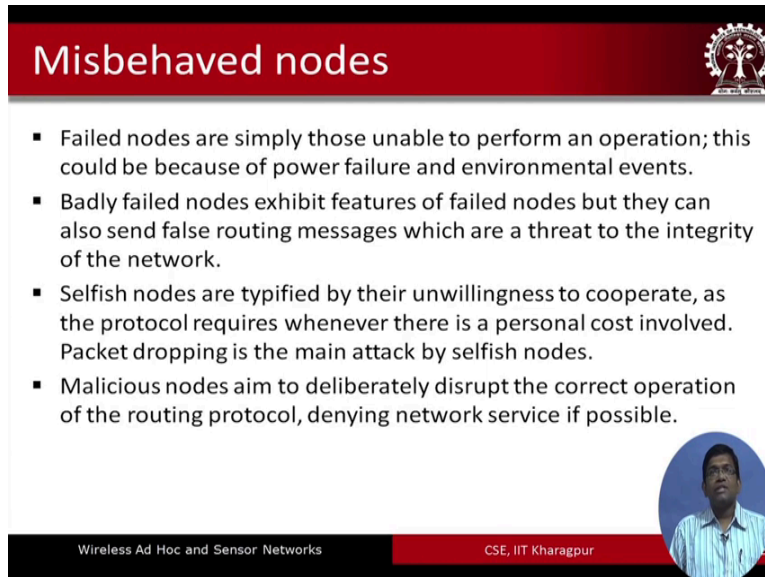
(Refer Slide Time: 04:11)



(Refer Time: 04:33)

Now, in this particular backdrop; that means, that we have looked at the characteristics of MANETs, we have looked at the different challenges in implementing MANETs. So, in this backdrop we have to understand the issue of cooperation. So, before we do that we need to understand that the nodes in MANETs they they may operate ideally, they may operate properly or they may not. So, based on the behavior of the different nodes, these nodes in MANETs they can be classified into 2 categories, unintentional and intentional. In the unintentional category we have the failed nodes and the badly failed nodes whereas; in the intentional category we have selfish nodes and malicious nodes. So, let us look at each of these different types of node behaviors each of these different types of nodes and what they mean in more detail.


(Refer Slide Time: 05:11)



Misbehaved nodes

- Failed nodes are simply those unable to perform an operation; this could be because of power failure and environmental events.
- Badly failed nodes exhibit features of failed nodes but they can also send false routing messages which are a threat to the integrity of the network.
- Selfish nodes are typified by their unwillingness to cooperate, as the protocol requires whenever there is a personal cost involved. Packet dropping is the main attack by selfish nodes.
- Malicious nodes aim to deliberately disrupt the correct operation of the routing protocol, denying network service if possible.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur



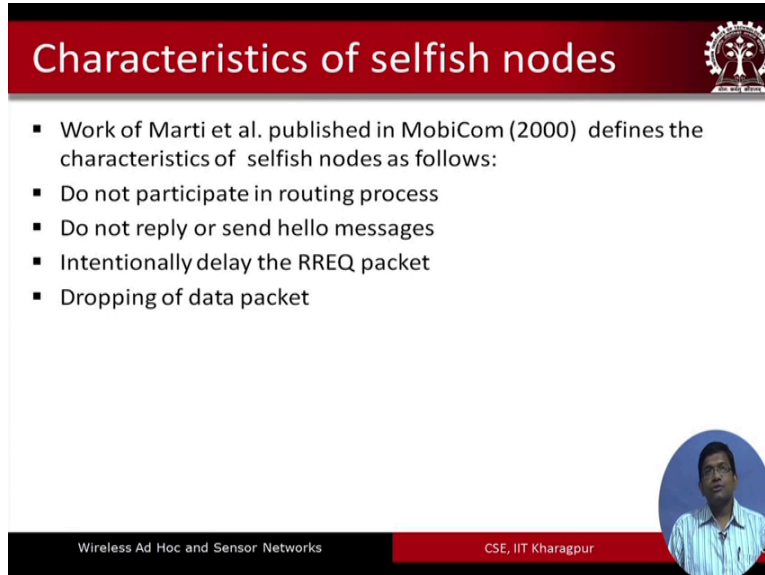
So, failed nodes are simply those, which are unable to perform an operation maybe due to different reasons such as power failure or maybe there is some kind of an environmental condition, an environmental event that has made a particular node to fail the way it is supposed to do. The second is the badly failed nodes which basically exhibit features of failed nodes, but they also send false routing messages which can be a threat to the overall integrity of the network. The selfish nodes are typically those which basically are willing to cooperate initially, but later on they are unwilling to cooperate.

So, initially they are willing to cooperate, but later on due to their different constraints such as, you know they have very limited energy in them they have very limited computational power and so on. So, initially they agree to cooperate, but later on they do not cooperate right. So, they are unwilling to cooperate because they want to be miser, they want to save their own limited resources and they do not want to help the other nodes in routing their messages through them. So, packet dropping is the main attack and that is done by the selfish node.

So, what it means is a selfish node, when it receives a packet because initially it agreed to forward the packets, so, when it receives the packet then instead of forwarding it to the next hop neighbor or it is going to do is it is going to silently it is going to drop the packet and that is the selfish node. So, the other nodes are not going to know that it has, in fact, dropped the packet

right and malicious nodes basically, what they do is unlike the selfish nodes these nodes do it silently, what they do is they deliberately they disrupt the correct operation of the routing protocol or other protocols that are running in these different nodes, thereby denying network service if it is possible.

(Refer Slide Time: 07:23)



The slide features a red header with the title "Characteristics of selfish nodes" and a small circular logo on the right. Below the header, a bulleted list describes the characteristics of selfish nodes. In the bottom right corner, there is a circular portrait of a man in a light blue shirt. The footer contains the text "Wireless Ad Hoc and Sensor Networks" on the left and "CSE, IIT Kharagpur" on the right.

Characteristics of selfish nodes

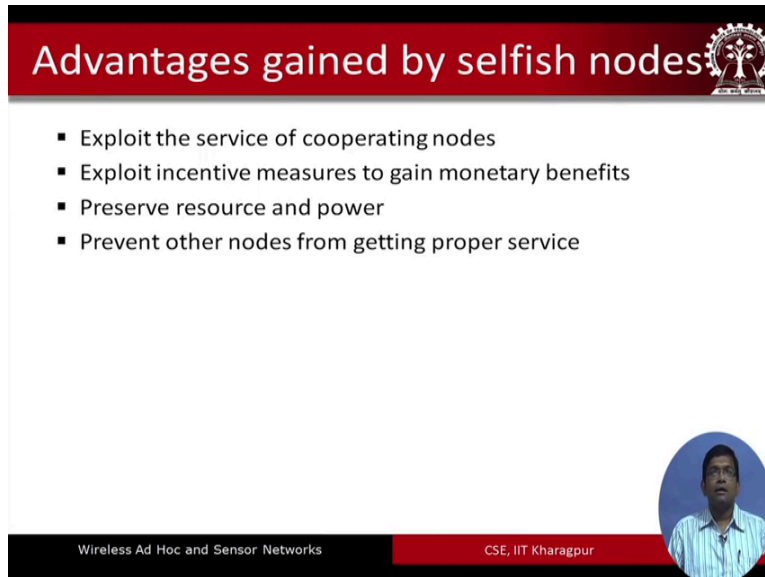
- Work of Marti et al. published in MobiCom (2000) defines the characteristics of selfish nodes as follows:
- Do not participate in routing process
- Do not reply or send hello messages
- Intentionally delay the RREQ packet
- Dropping of data packet

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

So, there are different characteristics of the selfish nodes and these were enumerated in a work published by Marti et al in MobiCom conference in 2000. So, as per their definition selfish nodes are the ones which exhibit characteristics such as, they do not participate in the routing process, they do not reply or send hello messages and they intentionally delay the RREQ packet, we will see what is what it means by RREQ, RREQ and RREP. So, RREQ means the route request packet and RREP means that route reply packet.

So, whenever a route request packet arrives, they would intentionally, they would delay forwarding them or whenever there is a RREP the route reply packet that arrives at a particular node, they would delay forwarding it. So, these are the behaviors of the selfish nodes the other one is dropping of the data packet that we have already seen.


(Refer Slide Time: 08:30)



Advantages gained by selfish nodes

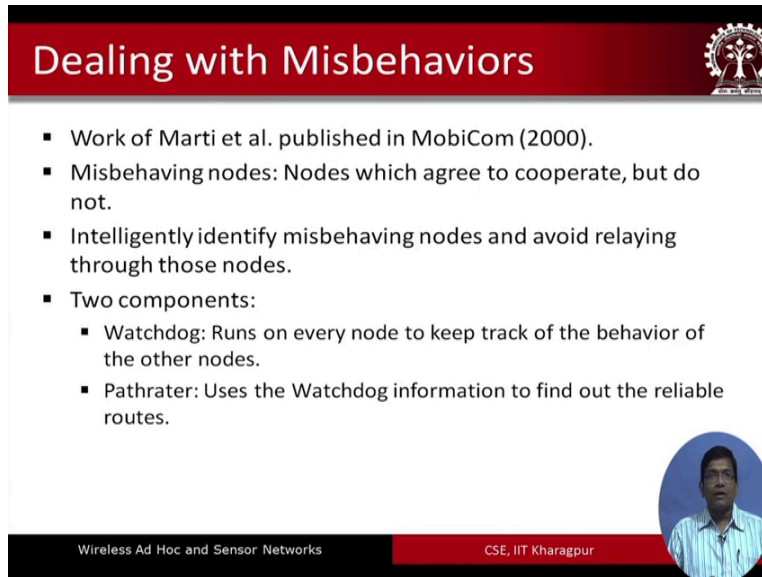
- Exploit the service of cooperating nodes
- Exploit incentive measures to gain monetary benefits
- Preserve resource and power
- Prevent other nodes from getting proper service

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur



So, whenever a selfish node receives the packet instead of forwarding it further these nodes are going to drop the packets. So, the advantages that are gained by the selfish nodes are like this, that they exploit the service of the cooperating node, so, there are other nodes which cooperate. So, the selfish nodes whereas they are enjoying the services offered by the other peers which are cooperating nodes, these nodes they did not actually cooperate in turn with these cooperating nodes. So, they do not reciprocate in terms of cooperation. They exploit the incentive measures to gain monetary benefits and they preserve the resource and power and they prevent other nodes from getting proper service. So, these are some of the advantages that are gained by the selfish nodes. To deal with these misbehaviors the scientists Marti et al again in the paper published in MobiCom in 2000 what they have done is they have tried to propose a solution.

(Refer Slide Time: 09:17)



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, in their work what they do is, they define misbehaving nodes to be the ones which initially agree to cooperate, but eventually they do not. So, what they do is in their solution they intelligently try to identify the misbehaving nodes and avoid relying through these particular nodes, these specific nodes. So, what is important is to identify which nodes are misbehaving and then it is obvious that once the nodes are misbehaving just you know avoid them while routing decisions are made; that means, you know avoid them through the routing paths when the routing paths are determined.

So, in their solution they primarily use 2 components, 1 is called the watchdog, which basically runs on every node to keep track of the behavior of the different other nodes in its proximity. So, every node runs a watchdog process and that watchdog, basically the task of the watchdog is to keep an eye on the behavior of the neighbors of that particular node and based on the information that is supplied by the watchdog, every node finds out what are the reliable routes to the other intended destination nodes in the network and that is done through the component which is known as the path rater. So, there are 2 components ,watchdog and the path rater.

(Refer Slide Time: 11:03)

Dealing with Misbehaviors



Watchdog

Detects misbehaving nodes by overhearing transmission



- Maintain a buffer of recently sent packets
- Compare each overheard packet with the packet in the buffer to see if there is a match
- If a packet remained for longer than timeout, increments a failure tally for the node responsible
- If the tally exceeds a threshold, the node is determined to be misbehaving and the source will be notified



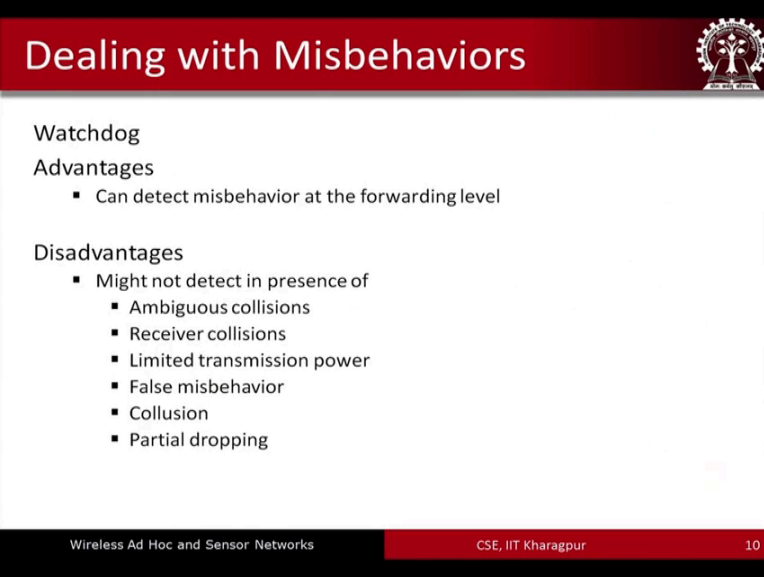
So, watchdog basically detects misbehaving nodes by overhearing transmission. So, let us look at the figure in front of us. So, what we have is a multi hop scenario. We have a source node and a destination node. The source node intends to send the packet to the destination node D via the intermediate relay nodes A, B and C, via A, B and C. So, what it is going to do is, sends to let us say A. So, A and every node; that means, B, C, D etcetera, what they also do is they all of them in the network, they would maintain a buffer of the recently sent packets. All of them, they are going to maintain a buffer of the recently sent packet. So, so let us say that A sends the packet to B it forwards the packet to B. So, then what it B does is, B would in turn forward the packet to C after it has received it. So, when this is forwarded to C, node A because, it is within the transmission range of node B because, it is a neighbor of B overhears this particular transmission. So, when it overhears this transmission, then it basically you know what it does is, that buffer information that it had or originally when it had sent that packet to B it is going to delete it. It is going to remove that particular information because, it is now confirmed that B has sent it forward right.

So, basically, it would compare, node A would compare each overhead packet with the packet in the buffer to see if there is a match. If the packet remained for longer than timeout, that means; that it is likely that B has not forwarded it right. So, if it has remained longer time than the timeout then it increments a failure tally; that means, some kind of you know table it is going to maintain, a tally table for the node that is responsible; that means, in this particular case node B.

So, it is going to do that and if the tally exceeds a threshold the node is determined to be misbehaving and the source will be notified. So, what it is going to do is, it will observe for certain duration of time or certain number of times. You know how many times node b for example, is not forwarding. So, it could be that, I mean one instance may not suggest that node b is a malicious node or a selfish node or a misbehaving node in general.

So, it might be that due to some other reason, node you know that overhearing that was supposed to happen for the Bs transmission at A, that has not taken place. So, that you know. So, 1 or 2 instances may not suggest. So, there should be some you know number of times, in a certain number of times, a pre-configured number of times, a threshold number of times, that if such a phenomena occurs then both B can be tagged as a misbehaving nodes as a misbehaving node. Otherwise may not be that the node B is a misbehaving node.

(Refer Slide Time: 14:40)



The slide features a red header with the title "Dealing with Misbehaviors" and a logo of a tree with a gear. The main content is on a white background with a black footer. The footer contains the text "Wireless Ad Hoc and Sensor Networks" on the left, "CSE, IIT Kharagpur" in the center, and "10" on the right.

Dealing with Misbehaviors

Watchdog

Advantages

- Can detect misbehavior at the forwarding level

Disadvantages

- Might not detect in presence of
 - Ambiguous collisions
 - Receiver collisions
 - Limited transmission power
 - False misbehavior
 - Collusion
 - Partial dropping

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 10

So, the advantage, this particular mechanism by which the watchdog operates. It is advantageous, because you know this way one can detect misbehaviors at the you know forwarding level, but this approach also comes with different disadvantages. So, let us look at different cases where you know such a mechanism may not actually detect the presence of misbehavior. So, let us look at some of these ok.

(Refer Slide Time: 15:09)

Dealing with Misbehaviors

Watchdog

- Ambiguous collisions
- The ambiguous problem prevents node A from overhearing transmission from B

The diagram shows a network topology with nodes S, A, B, C, and D. Node S is on the left, and node D is on the right. Node A is in the center, and node B is to its right. Node C is further to the right. A solid line with an arrow labeled '2' points from S to A. A solid line with an arrow labeled '1' points from B to C. A dashed line with an arrow labeled '1' points from B to A. There are two 'X' marks on the lines between S and A, and between B and A, indicating collisions. Node D is shown as a box with no connections.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

So, ambiguous collision is the first case. So, as we can see over here. So, what might happen is there could be some kind of collision that might happen at A. So, so what might happen is that you know when B. So, A has sent to B, B has forwarded to C and a copy of that message that B has sent to C is overheard by node A, but when A receives that overheard message, maybe another packet arrives from S, the second packet and there is a collision at A's end. So, due to that collision, A would not be able to overhear the transmission from B.

(Refer Slide Time: 16:05)

Dealing with Misbehaviors

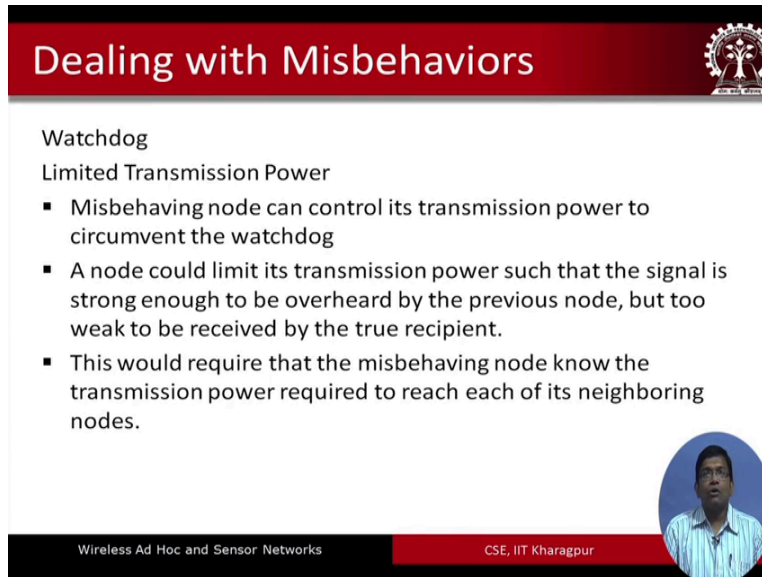
Watchdog
Receiver collisions
Node A can only tell whether node B sends the packet to node C, but it cannot tell if C receives it

The diagram shows a network topology with nodes S, A, B, C, and D. Node S is on the far left. Node A is to the right of S. Node B is to the right of A. Node C is to the right of B. Node D is on the far right. A dashed arrow labeled '1' points from B to A, indicating that A overhears B's transmission. A solid arrow labeled '1' points from B to C. A solid arrow labeled '2' points from D to C. Both arrows pointing to C are crossed out with an 'X', indicating a collision at node C. In the bottom right corner of the slide, there is a circular portrait of a man in a blue shirt.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Let us look at another scenario, the receiver side collision. So, in this particular case as we can see that, A forwards the packet to B, B forwards to C, A overhears that. But when C gets it there is another packet that were sent by D. So, at the receiver side C there is a collision between the packet that is sent by B and the packet that was sent by D. So, there is a collision between these 2 packets. So, consequently node A can only tell whether node B sends the packet to node C, but it cannot tell in this particular scenario for example, that node C has actually received it or not. Node A cannot tell it, it can only confirm that node B has sent it, but it cannot really confirm whether node C has received the packet.

(Refer Slide Time: 17:09)



Dealing with Misbehaviors


Watchdog

Limited Transmission Power

- Misbehaving node can control its transmission power to circumvent the watchdog
- A node could limit its transmission power such that the signal is strong enough to be overheard by the previous node, but too weak to be received by the true recipient.
- This would require that the misbehaving node know the transmission power required to reach each of its neighboring nodes.

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur



Limited transmission power is another issue. So, the misbehaving node can control its transmission power to circumvent the watchdog. So, what it means that a node could limit its transmission power such that the signal is strong enough to be overheard by the previous node, but it is too weak to be received by the true recipient. So, it can control you know, because the more transmission power with which the packet is sent, the more number of nodes in the proximity would be able to receive the packet. So, you know, this particular node it can basically manipulate it. So, that you know the true recipient does not receive, but, the watchdog actually thinks that it has received. So, actually, so this is some kind of you know getting around, you know the watchdog right So, this would require that the misbehavior node knows the transmission power that is required to reach each of its neighboring nodes and that is an assumption under which you know this kind of scenario might occur.

(Refer Slide Time: 18:19)

Dealing with Misbehaviors

Watchdog

False misbehavior

- When nodes falsely report other nodes as misbehaving

```
graph LR; S[S] -.- A[A]; A[A] -.- B[B]; B[B] -- C[C]; C[C] -.- D[D]; B[B] -.- S[S];
```

Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

False misbehavior. So, here as we can see that what might so happen is any node, any node over here, it can falsely report to the other nodes that one of its neighbors is a misbehaving node because it is you know, so, there is some kind of trust that goes on between the different nodes you know. So particularly, you know, for instance A might report to S that node B is a misbehaving node and there is no way that S can ensure whether A is reporting correctly about the behavior of B or not.

(Refer Slide Time: 19:10)

Dealing with Misbehaviors

Watchdog

Collusion

- Multiple nodes in collusion can mount a more sophisticated attack
- For example, B and C could collude to cause mischief. In this case, B forwards a packet to C, but does not report to A when C drops the packet.
- Because of this limitation, it may be necessary to disallow two consecutive untrusted nodes in a routing path.

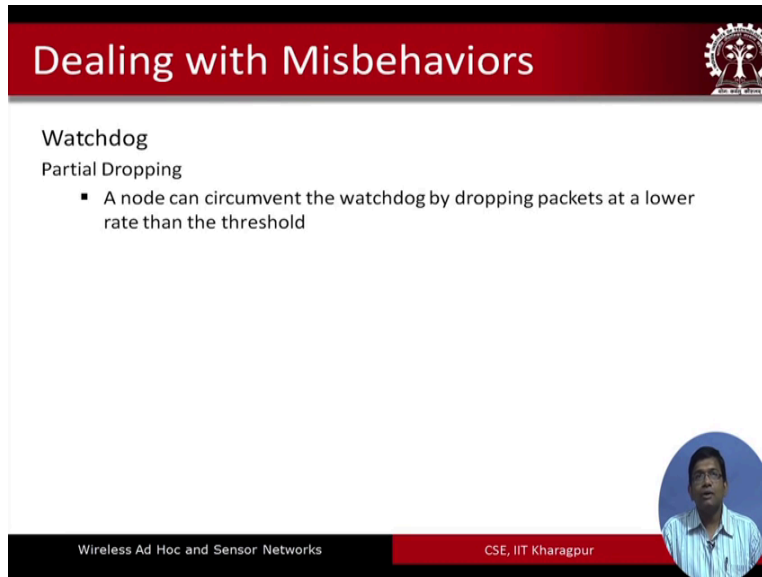
Wireless Ad Hoc and Sensor Networks

CSE, IIT Kharagpur

Collusion. Collusion means that you know couple of nodes together they are going to collude, they are going to form some kind of a group and they are going to launch the attack. So, let us look at the figure on the slide. So, as we can see over here the nodes B and C they can collude; that means, they can group together to launch a more powerful, a more sophisticated attack.

So, in this particular case B forwards the packet to C, but does not report to A. B sends to C, but it can manipulate in such a way that it does not report to A, when C drops the packet you know. So, B will come to know about it whether C has dropped the packet or not, whether the packet that was sent by B has been received by C or not, B will come to know about it, but if B is also malicious, I mean not malicious, misbehaving then together what it can do is it will not report to A. So, A will not come to know that whether B and C together have launched some kind of a collective misbehavior. So, that is why it is suggested that, because of this limitation it is suggested that one should disallow 2 consecutive untrusted nodes in a routing path. So, you know. So, if B is also an untrusted node, not a trustworthy node, C is also not a trustworthy node, then, you know, 2 of them successively should be avoided in a particular routing path.

(Refer Slide Time: 20:52)




Dealing with Misbehaviors

Watchdog

Partial Dropping

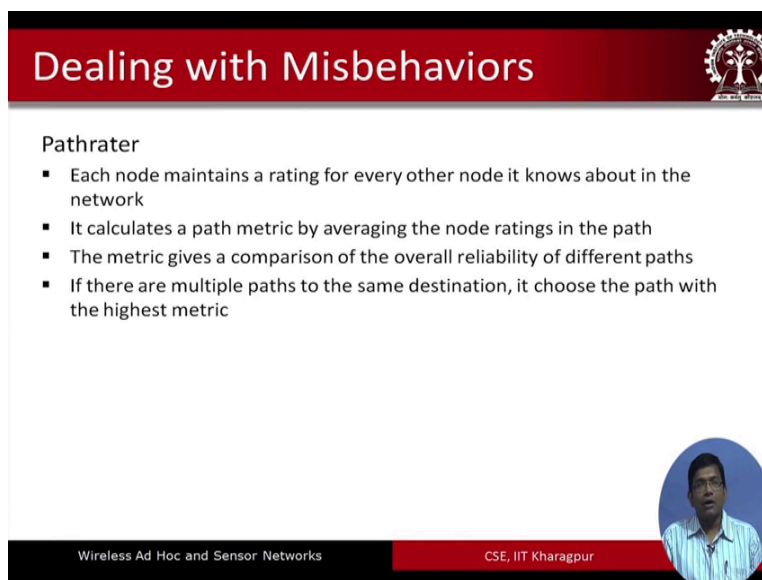
- A node can circumvent the watchdog by dropping packets at a lower rate than the threshold

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur



Partial dropping is a case where a node can circumvent the watchdog by dropping packets at a lower rate than the threshold you know. So, the rate at which, I mean there is some kind of a threshold that is maintained by the watchdog. So, if you basically drop the packets at a lower rate than that, then the watchdog will never be able to know about whether you know any node is misbehaving or not.

(Refer Slide Time: 21:20)




Dealing with Misbehaviors

Pathrater

- Each node maintains a rating for every other node it knows about in the network
- It calculates a path metric by averaging the node ratings in the path
- The metric gives a comparison of the overall reliability of different paths
- If there are multiple paths to the same destination, it choose the path with the highest metric

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

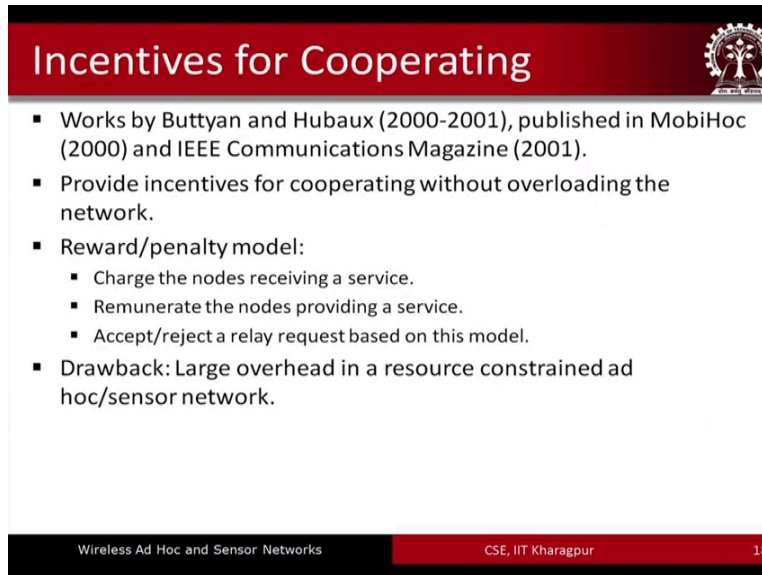


So, we have seen how the watchdog behaves, how the watchdog can keep an eye on the behavior of the different nodes around it and we have also seen that this kind of approach that is adopted typically by the watchdog can be circumvented, you know can be manipulated and we have seen the different, you know scenarios under which the watchdog mechanism that we have, you know we have explained that may not work properly.

So, assuming that it works properly and the watchdog keeps an eye on the behavior of the different nodes in its vicinity, that information is collected. The watchdog information is collected by the other component in Marti et al solution which is known as the pathrater and what the pathrater does is, so, each node maintains a rating for every other node it knows about in the network it calculates a path metric by averaging the node ratings in the path. The metric gives a comparison of the overall reliability of the different paths and if there are multiple paths to the same destination it then chooses the path with the highest metric.

So, what does it mean? that based on the observations by the watchdogs done, the watchdog processes running at the different nodes in the network, the pathrater is going to collect that information from this different you know, watchdogs and then it is going to determine that which path or paths are the most reliable ones; that means, where the nodes are least non trustworthy; that means, more trustworthy nodes are residents (Refer Time: 23:18) it will determine those paths and it will forward, the pathrater will then forward that information to the nodes. So, that the nodes forward the packet only through those paths which are more reliable once; that means, which have least number of untrustworthy nodes.

(Refer Slide Time: 23:42)



Incentives for Cooperating

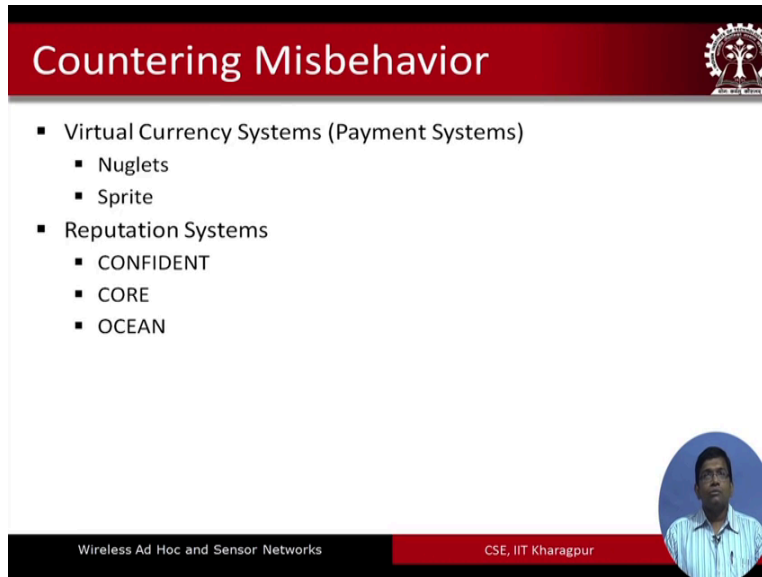
- Works by Buttyan and Hubaux (2000-2001), published in MobiHoc (2000) and IEEE Communications Magazine (2001).
- Provide incentives for cooperating without overloading the network.
- Reward/penalty model:
 - Charge the nodes receiving a service.
 - Remunerate the nodes providing a service.
 - Accept/reject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

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 18

So, there are different incentive mechanisms that have been proposed for cooperation. 1 of these was proposed by Buttyan and Hubaux in 2000-2001 where they talk about providing different kinds of incentives in the form of reward penalty without overloading the network. So, in the reward penalty model, they proposed charging the nodes that receive a service, remunerating the nodes that offer the surface and then based on the above model; that means, charging remunerating model, accepting or rejecting a relay request that comes to a particular node.

So, charging the node, receiving the service, remunerating the nodes providing a service and accepting or rejecting a relay request based on this particular model. So, the drawback is that there is large overhead in a resource constrained ad hoc sensor network, if we adopt this kind of reward penalty based model. Because, large number of packets, unnecessary packets, control packets are going to fly all around in the network, that leads to, you know, that is undesirable because already the network you know these kind of networks are resource constrained and we not want to overload these networks even further.


(Refer Slide Time: 25:11)



Countering Misbehavior

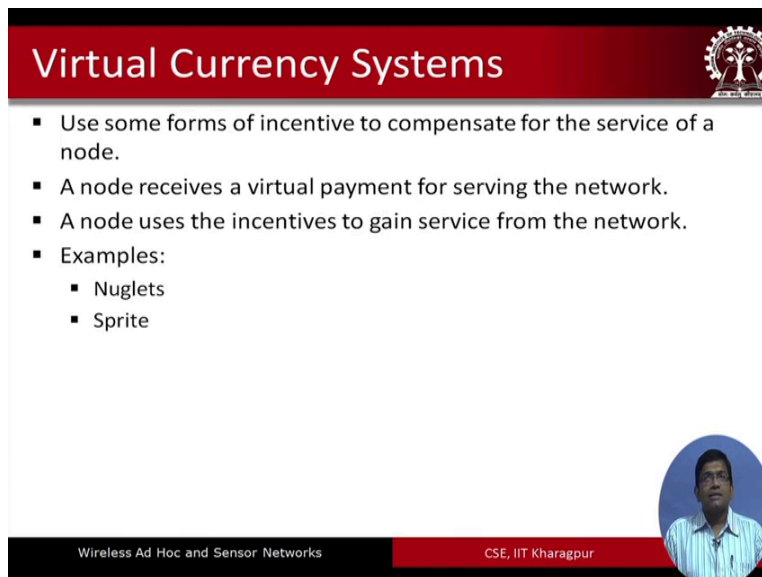
- Virtual Currency Systems (Payment Systems)
 - Nuglets
 - Sprite
- Reputation Systems
 - CONFIDENT
 - CORE
 - OCEAN

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur



So, there are 2 types of systems, two types of solutions that have been proposed in the literature. 1 is called the virtual currency system and the other one is called the reputation system. Virtual currency systems, belonging to this category are 2 types of systems called the Nuglets and the Sprite and the reputation systems examples are confident, core and ocean.


(Refer Slide Time: 25:44)



Virtual Currency Systems

- Use some forms of incentive to compensate for the service of a node.
- A node receives a virtual payment for serving the network.
- A node uses the incentives to gain service from the network.
- Examples:
 - Nuglets
 - Sprite

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur



So, in virtual currency systems, these systems use some form of incentive to compensate for the surface that is offered by a node. A node basically receives a virtual payment for serving the network and it uses the incentives to gain service from the network. So, basically that a node would basically get paid, when it is serving the other nodes in the network in the form of some kind of a virtual payment and that is the incentive that it gets, that if I serve, if I forward the packet of another node I am going to get serve. I am going to get some kind of a payment and it is that payment that serves as the incentive for this particular node to serve the other nodes for forwarding their packets. So, nuglets and sprites are examples belonging to this particular category; that means the virtual currency systems.

So, with this we come to an end of the first module. In the next module on cooperation we will be continuing with the virtual currency systems, then we will talk about the reputation systems and we look at some of the protocols that have been proposed for each of these classes of systems.

Thank you.