

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

Lecture - 38
Security of Wireless Sensor networks-Part-II

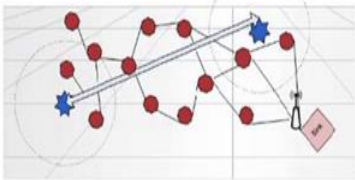
Security in wireless sensor networks part 2. So, in part 1 we had seen we had gone through some of the important security requirements in wireless sensor networks. And we had also looked at looked into the different challenges of implementing security mechanisms in wireless sensor networks due to different constraints different limitation and so on.

And thereafter we also in first part we had gone through some of the few attacks that are possible on these networks. So, in the second part we are going to go through the list of the different types of attacks that have possible in sensor networks of course, I mean we are not going to cover all of them, but only few important well known ones different types of attacks that are possible and finally, some solutions that have been proposed for security in sensor networks.

(Refer Slide Time: 01:18)

Wormhole Attack

- One or more malicious nodes are present who fake the route.
- There is a tunnel between these malicious nodes.
- The malicious node captures the packets and transmits them to other location.
- Wormhole attack can be launched without any knowledge of the network.



Wormhole attack

Source: Dimitrievski, Pejovska and Dacev, International Journal of Peer to Peer Networks, 2011

Wireless Ad Hoc and Sensor NetworksCSE, IIT Kharagpur2

So, this is another attack a very popular one which is called the wormhole attack. So, in the wormhole attack as we can see that we have the network like this, we have the network of like orange colored nodes. And in the network an attacker can come in. And

the attacker basically what it does that it is going to maliciously, you know it is going to maliciously get access to the data that is in transit in this network, and it is when tunnel that data away from the network to another node which is again the other part of this malicious entity right.

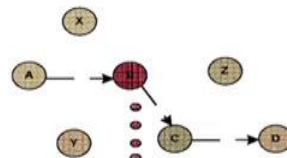
So, basically siphoning you know through a tunnel it is going to siphon the data from the network out of the network. So, one or more malicious nodes are present who faked the route one or more molecule accessible. So, they are going to faked the route they are you know. So, it is sort of like you know this malicious entity it is going to retain as if it is part of the routing process. So, it is going to send the siphon the data out it is going to pretend that it is a legitimate user. And this route is part of the regular network and which actually is not and the data is going to be siphoned out of the network to another malicious entity like this.

So, the malicious node basically captures the packets and transmit is them to the other location. The wormhole attack can be launched without any knowledge of the network right. So, this is this is why it is called an attack. So, if you if it was known to the different nodes then it would not be an attack. So, nobody knows that this is happening. And this is why it is an attack and it is called wormhole because of the existence of this tunnel between the 2 entities through 2 malicious entities.

(Refer Slide Time: 03:27)

Selective Forwarding Attack

- One malicious node denies to forward packets.
- Malicious node can deny packets which are coming from a particular node or from selective nodes.
- **Sinkhole attack** is one type of selective forwarding attack.
 - One compromised node attracts all the traffic going to the base station



Shila and Anjali, ElectroInformation Technology, 2008. IEEE

Selective forwarding attack:
Node B drops the packets and disrupt the network operation

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 3

Then we have the selective forwarding attack. So, in selective forwarding basically the malicious node, let us say that this is the malicious node, this malicious node what it is going to do it is going to deny the packets which are coming from a particular node or from selected nodes. So, then these know these packets are going to be dropped. So, if it is coming from particular selectively, you know if it is coming from certain node or couple of nodes then selectively that data is going to be dropped. So, sinkhole attack is a type of selective forwarding attack, where one compromised node basically attracts all the traffic going to the base station.

So, that is why it is called this particular node is called the sinkhole. So, this sinkhole you see that this becomes a sinkhole and the data. So, that that node itself is compromised and it attracts on the data from the network that is going through it and it would be. So, that the data is going to be dropped in between instead of forwarding to the base station. Acknowledgement spoofing as this name suggests basically the attacker intercepts between the sender and the receiver spoof the acknowledgement packets and the main goal is to make the sender convince that a dead node is alive right.

(Refer Slide Time: 04:41)

Acknowledgement Spoofing

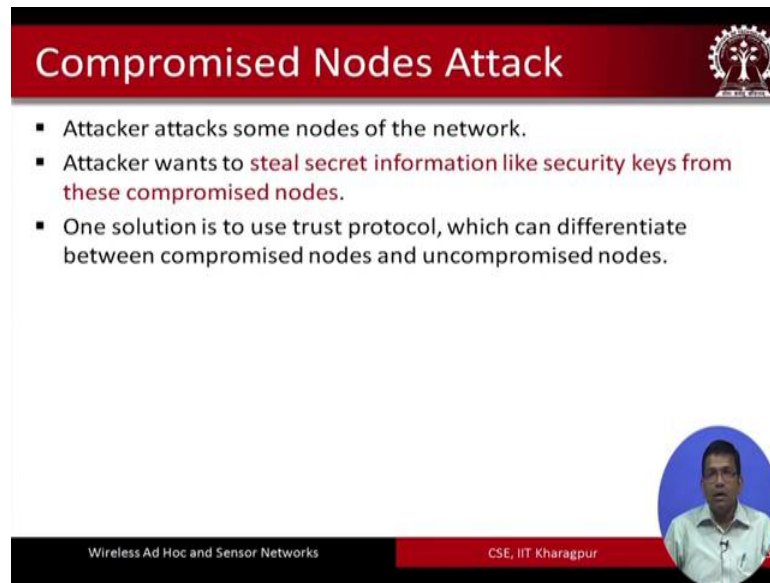
- Attacker intercepts between sender and receiver.
- Spoof the acknowledgement packets.
- The main goal is to **make the sender convince that a dead node is alive.**
- It makes the sender confuse and mislead the routing process.

Acknowledgement Spoofing

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 4

So, basically it is spoofing just spoofing, the acknowledgement and pretending or convincing the sender that the dead node is alive.

(Refer Slide Time: 05:05)



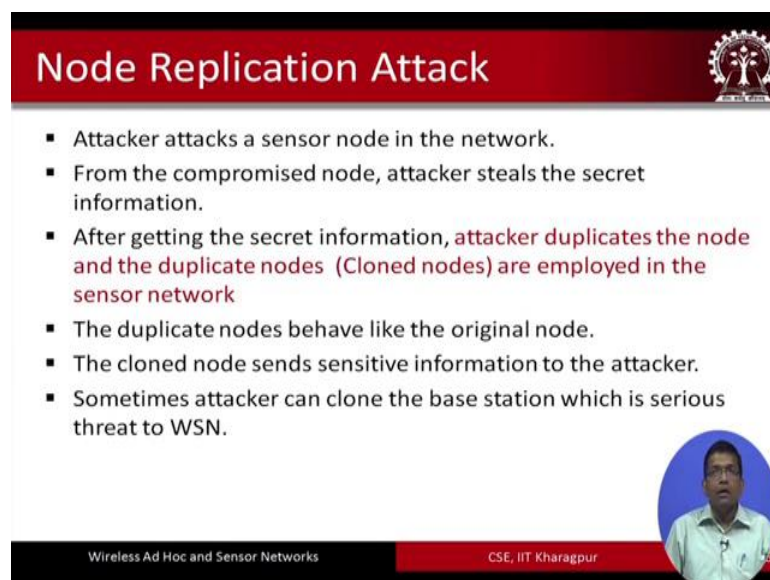
Compromised Nodes Attack

- Attacker attacks some nodes of the network.
- Attacker wants to steal secret information like security keys from these compromised nodes.
- One solution is to use trust protocol, which can differentiate between compromised nodes and uncompromised nodes.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Compromised nodes attack the attacker attacks some nodes in the network, and steals the secret information like the security keys from this compromised node. So, physically the nodes are attacked right. So, the nodes they themselves become compromised. And once the node is compromised the security keys and other sensitive information are basically stolen completely stolen from these compromised nodes.

(Refer Slide Time: 05:36)



Node Replication Attack

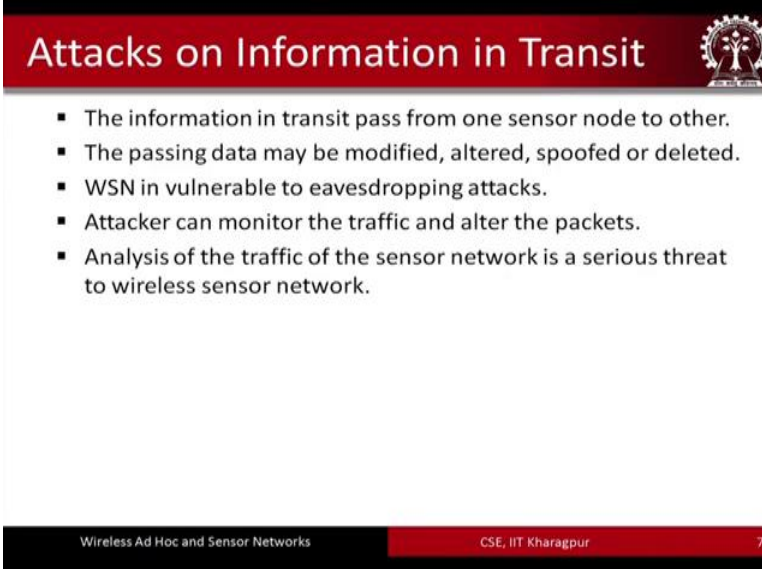
- Attacker attacks a sensor node in the network.
- From the compromised node, attacker steals the secret information.
- After getting the secret information, attacker duplicates the node and the duplicate nodes (Cloned nodes) are employed in the sensor network
- The duplicate nodes behave like the original node.
- The cloned node sends sensitive information to the attacker.
- Sometimes attacker can clone the base station which is serious threat to WSN.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Node replication attack: Here the attacker basically duplicates the node and the duplicated nodes; that means, the cloned nodes are employed in the sensor networks. So,

these cloned nodes are actually not the real nodes, but these are just like virtual ones which have been created by that attacker and because of this this clone nodes 0 data are going to be sent through the clone nodes, which are actually not existing one physically existing ones and because of which this becomes an attack and the data can be data can be lost data can be tampered with that are flowing through these clone nodes.

(Refer Slide Time: 06:15)



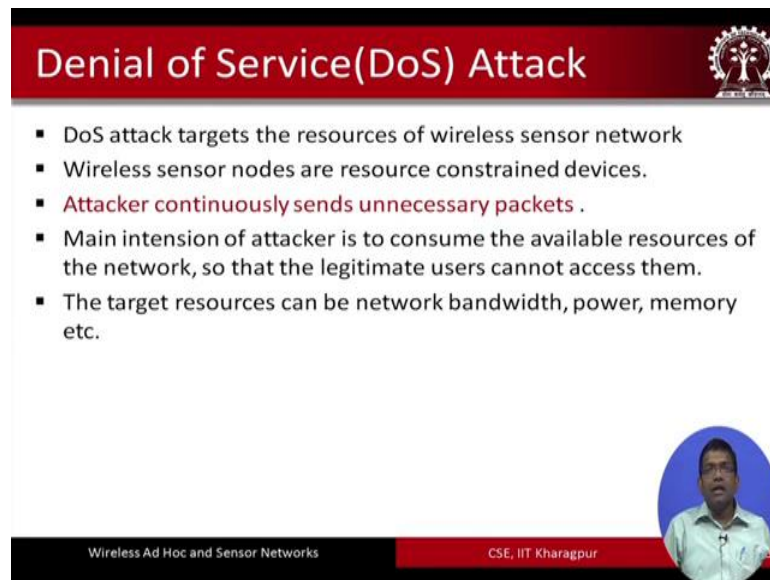
Attacks on Information in Transit

- The information in transit pass from one sensor node to other.
- The passing data may be modified, altered, spoofed or deleted.
- WSN in vulnerable to eavesdropping attacks.
- Attacker can monitor the traffic and alter the packets.
- Analysis of the traffic of the sensor network is a serious threat to wireless sensor network.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 7

Attacks on information in transit the name says it all the data that are passing between the different nodes they could be modified altered spoofed deleted and so on. So, this is this is very important. So, the data can be the integrity of the data can be modified, I mean the data may not be the integrity of the data may not be maintained, and the data can be altered in different ways.

(Refer Slide Time: 06:42)



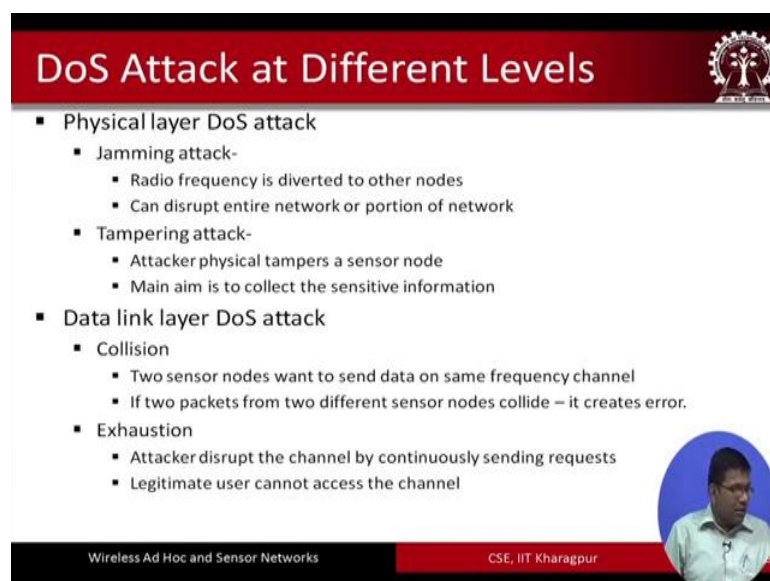
Denial of Service(DoS) Attack

- DoS attack targets the resources of wireless sensor network
- Wireless sensor nodes are resource constrained devices.
- **Attacker continuously sends unnecessary packets .**
- Main intension of attacker is to consume the available resources of the network, so that the legitimate users cannot access them.
- The target resources can be network bandwidth, power, memory etc.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Denial of service attack is very well done. Denial of service attack basically know what you do is unnecessarily you want to send large number of different types of packets to the networks unnecessary packets are going to be sent to the network by the attacker. And that basically it is a resource constrained environment sensor networks the resource constraint, as I said before and that basically is going to consume the target resources such as the network bandwidth power memory there may be etcetera because of the unnecessary flow of too many large number of packets.

(Refer Slide Time: 07:15)



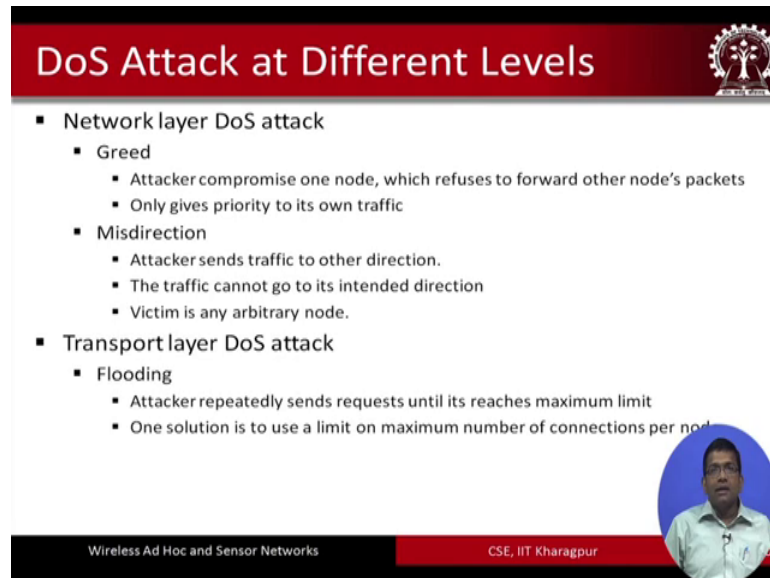
DoS Attack at Different Levels

- Physical layer DoS attack
 - Jamming attack-
 - Radio frequency is diverted to other nodes
 - Can disrupt entire network or portion of network
 - Tampering attack-
 - Attacker physical tampers a sensor node
 - Main aim is to collect the sensitive information
- Data link layer DoS attack
 - Collision
 - Two sensor nodes want to send data on same frequency channel
 - If two packets from two different sensor nodes collide – it creates error.
 - Exhaustion
 - Attacker disrupt the channel by continuously sending requests
 - Legitimate user cannot access the channel

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

There are different types of denial of service attacks that are possible. Denial of service attacks and the physical layer data link layer network layer and transport layer.

(Refer Slide Time: 07:24)

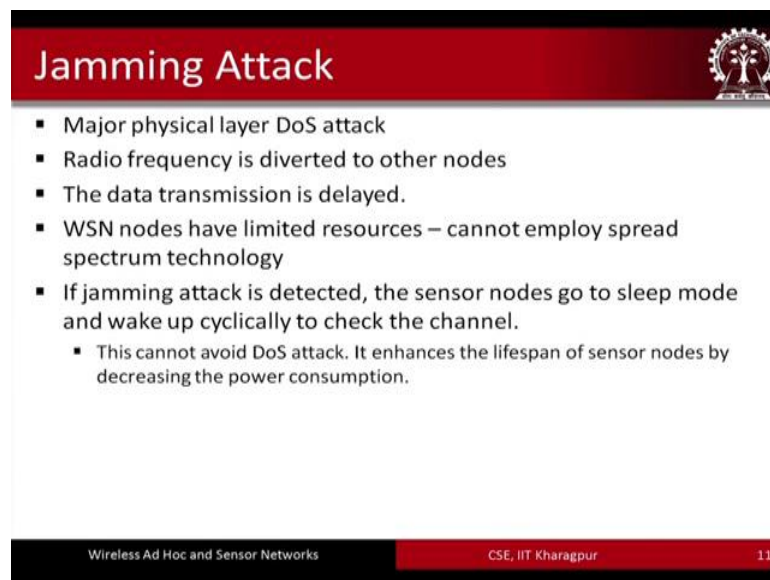


DoS Attack at Different Levels

- Network layer DoS attack
 - Greed
 - Attacker compromise one node, which refuses to forward other node's packets
 - Only gives priority to its own traffic
 - Misdirection
 - Attacker sends traffic to other direction.
 - The traffic cannot go to its intended direction
 - Victim is any arbitrary node.
- Transport layer DoS attack
 - Flooding
 - Attacker repeatedly sends requests until its reaches maximum limit
 - One solution is to use a limit on maximum number of connections per node

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

(Refer Slide Time: 07:29)



Jamming Attack

- Major physical layer DoS attack
- Radio frequency is diverted to other nodes
- The data transmission is delayed.
- WSN nodes have limited resources – cannot employ spread spectrum technology
- If jamming attack is detected, the sensor nodes go to sleep mode and wake up cyclically to check the channel.
 - This cannot avoid DoS attack. It enhances the lifespan of sensor nodes by decreasing the power consumption.

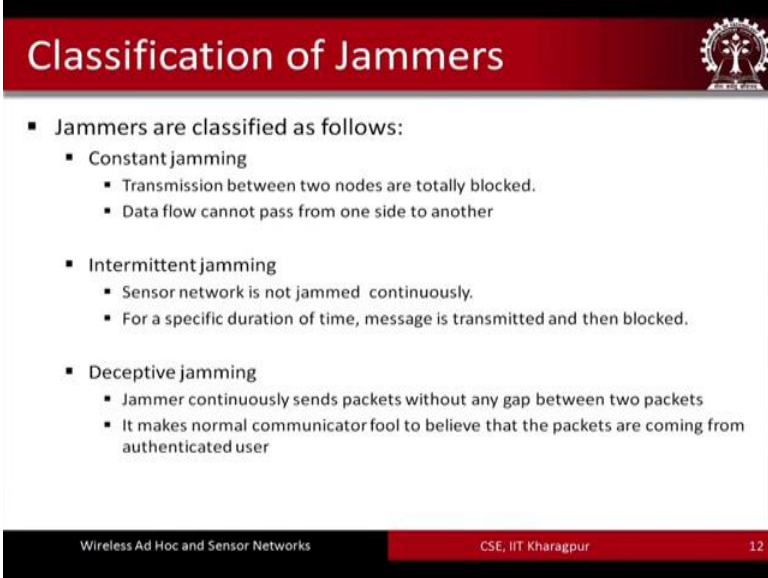
Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 11

So, I am not going to go through each of them, but I am just going to highlight that this is a denial of service attack which is called the jamming attack. And this jamming attack typically occurs at the physical layer. So, it is a major physical layers denial of service attack, where the radio frequency is diverted to the other nodes the data transmission is delayed and the wireless sensor network nodes have limited resources. So, if jamming

attack is detected the sensor nodes go to the sleep mode and wake up cyclically to check the channel. This cannot avoid the denial of service attack. It enhances the lifespan of the sensor nodes by decreasing the power consumption

So, essentially what happens is that there is a high frequency high powered attacker which is going to come and send signals at high strength into the network. And because of which the existing communication that is taking place between the different nodes that is going to be affected right.

(Refer Slide Time: 08:39)



The slide is titled "Classification of Jammers" and features a red header with a logo on the right. The main content is a bulleted list describing three types of jammers. The footer contains the text "Wireless Ad Hoc and Sensor Networks", "CSE, IIT Kharagpur", and the number "12".

- Jammers are classified as follows:
 - Constant jamming
 - Transmission between two nodes are totally blocked.
 - Data flow cannot pass from one side to another
 - Intermittent jamming
 - Sensor network is not jammed continuously.
 - For a specific duration of time, message is transmitted and then blocked.
 - Deceptive jamming
 - Jammer continuously sends packets without any gap between two packets
 - It makes normal communicator fool to believe that the packets are coming from authenticated user

And that basically diverts the data that was originally being sent between the different nodes in the network. And also the overall transmission gets delayed. There are different types of jammers that are possible. Constant jammers, intermittent jammers, deceptive jammers then we have random jammers and reactive jammers.

(Refer Slide Time: 08:50)

Classification of Jammers(Cont.)

- Random jammer
 - Jammer switches between napping and jamming.
 - At the time of jamming, attacker may act as constant jammer or deceptive jammer.
- Reactive jammer
 - When channel is not active, jammer remains silent.
 - When the traffic becomes active, immediately it starts sending signal.
- Deceptive jammer
 - Jammer sends packets without any gap between 2 packets.
 - Makes the normal communicator fool to believe that the packets are communicated are coming from an authenticated user.

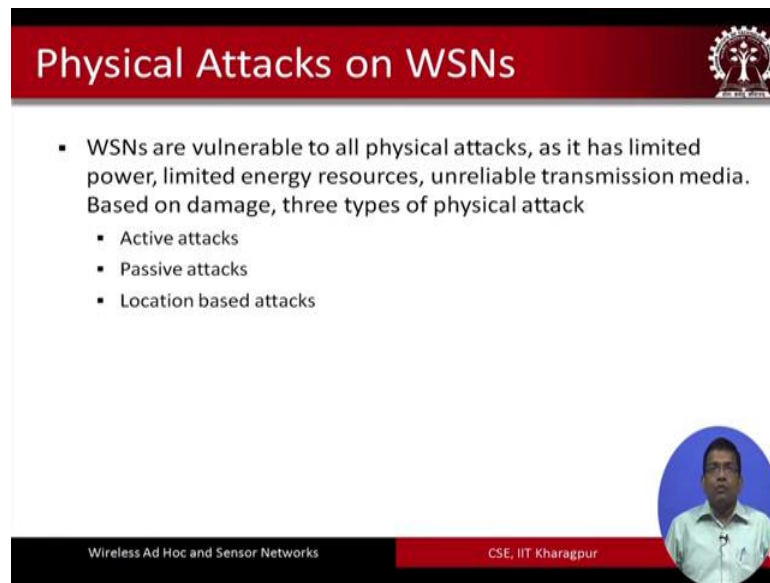
Wireless Ad Hoc and Sensor Networks | CSE, IIT Kharagpur

So, in constant jamming basically, transmission between the different nodes are totally blocked. So, the data flow cannot pass from one side to another. It is a constant jamming it is a constant totally blocked between the 2 nodes there is no transmission that can take place constantly blocked. So, it is called constant jammer. It is done by the constant jammer. It is called constant jamming, then intermittent jammer basically intermittently it will have jammed intermittent it is going to jammed the sensor work is not jammed continuously or constantly like before, but for a specific duration of time and intermittently the message is going to be transmitted and then blocked

Deceptive jammer continuously sends packets without any gap between 2 packets. It makes the normal communicator fool to believe that the packets are communicated are coming from an authenticated user. In the random jammer the jammer basically randomly it switches between jamming and napping been slipping. So, at the time of jamming the attacker may act as a constant jammer or a receptive jammer, but then it will go into the sleep mode, and it is going to alternately it is going to you know jams nap, jam nap etcetera, but that is that cycle is or itself going to be random; when it is going to jam when it is going to nap etcetera that itself is random.

Reactive jammers basically when the channel is not active the jammer remains silent when the traffic becomes active immediately it starts sending signal. So, reactively does it. So, whenever the channel is active jam whenever it is not active go to the sleep state.

(Refer Slide Time: 10:51)



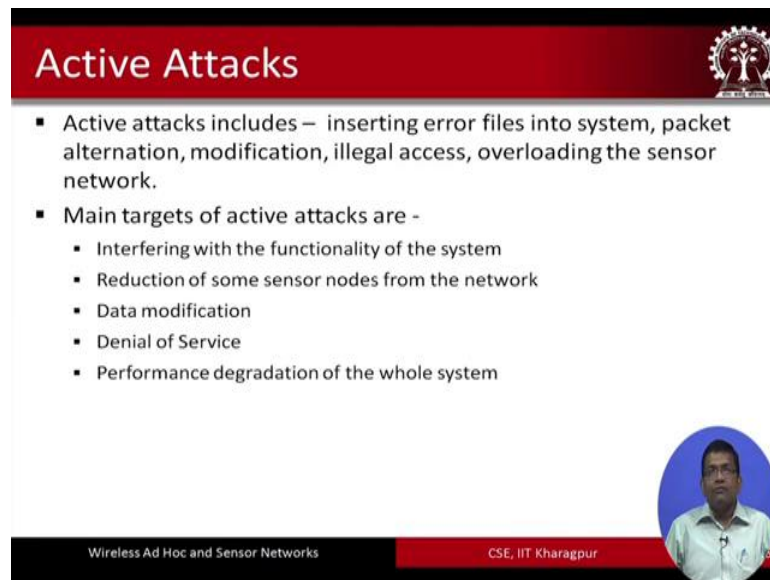
Physical Attacks on WSNs

- WSNs are vulnerable to all physical attacks, as it has limited power, limited energy resources, unreliable transmission media. Based on damage, three types of physical attack
 - Active attacks
 - Passive attacks
 - Location based attacks

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

The physical attacks are also possible on sensor networks. These physical attacks can be of 3 types active attacks passive attacks and location based attacks.

(Refer Slide Time: 11:04)



Active Attacks

- Active attacks includes – inserting error files into system, packet alteration, modification, illegal access, overloading the sensor network.
- Main targets of active attacks are -
 - Interfering with the functionality of the system
 - Reduction of some sensor nodes from the network
 - Data modification
 - Denial of Service
 - Performance degradation of the whole system

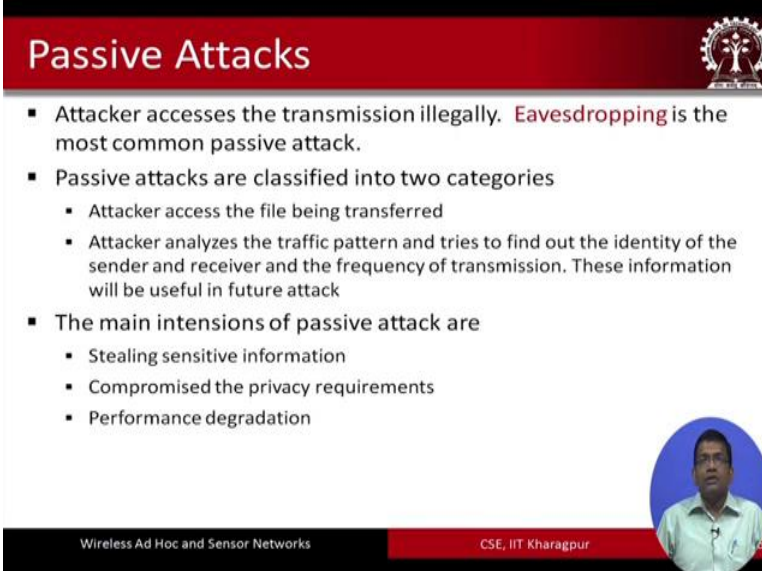
Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

You know active attacks can take different forms such as inserting error files into the system, alter altering the actively altering the packets modifying the packets illegal access to the network overloading the sensor network etcetera.

The main targets of active attacks are interfering with the functionality of the system reduction of some sensor nodes, from the network modification of data denial of service

performance degradation of the whole system. This is the these are the different targets or objectives of performing active attacks.

(Refer Slide Time: 11:47)



Passive Attacks

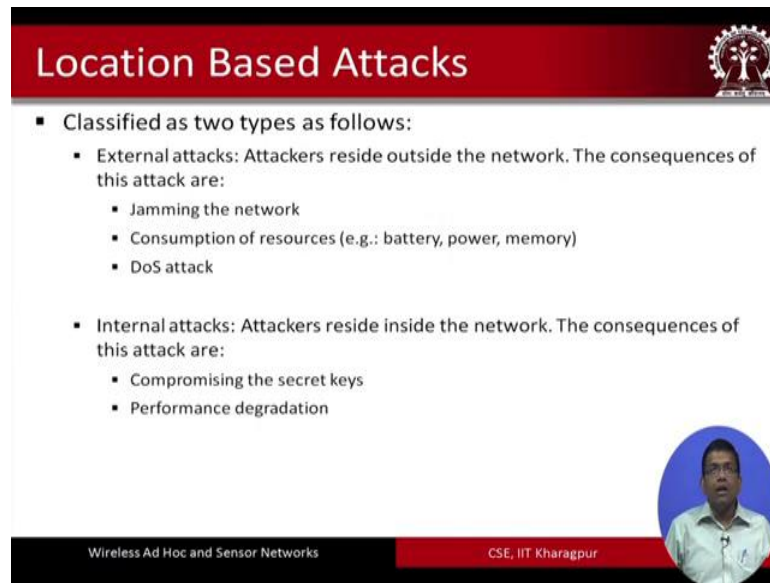
- Attacker accesses the transmission illegally. **Eavesdropping** is the most common passive attack.
- Passive attacks are classified into two categories
 - Attacker access the file being transferred
 - Attacker analyzes the traffic pattern and tries to find out the identity of the sender and receiver and the frequency of transmission. These information will be useful in future attack
- The main intensions of passive attack are
 - Stealing sensitive information
 - Compromised the privacy requirements
 - Performance degradation

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Passive attacks eavesdropping which we commonly know is a form of passive attack. And these passive attacks can be classified into 2 categories. So, first is the attacker assessing the file being transferred, and the attacker then analyzes the traffic pattern and tries to find out the identity of the sender and the receiver and the frequency of transmission. And this information will be useful in future attacks. So, this is just collecting different attacks silently eavesdropping collecting different information for use in the future.

So, it is sort of like stealth, some kind of you know stealth that stealing the sensitive information passively quietly. So, actively it is not cutting the network at that time, but later on that sensitive information that is collected, through these processes like you eavesdropping that is going to be you know used in the future for launching other active attacks.

(Refer Slide Time: 12:47)



The slide features a red header with the title "Location Based Attacks" and a logo of a tree with a gear. The main content is a bulleted list. At the bottom, there is a black bar with the text "Wireless Ad Hoc and Sensor Networks" and a red bar with "CSE, IIT Kharagpur". A small circular inset photo of a man is in the bottom right corner.

Location Based Attacks

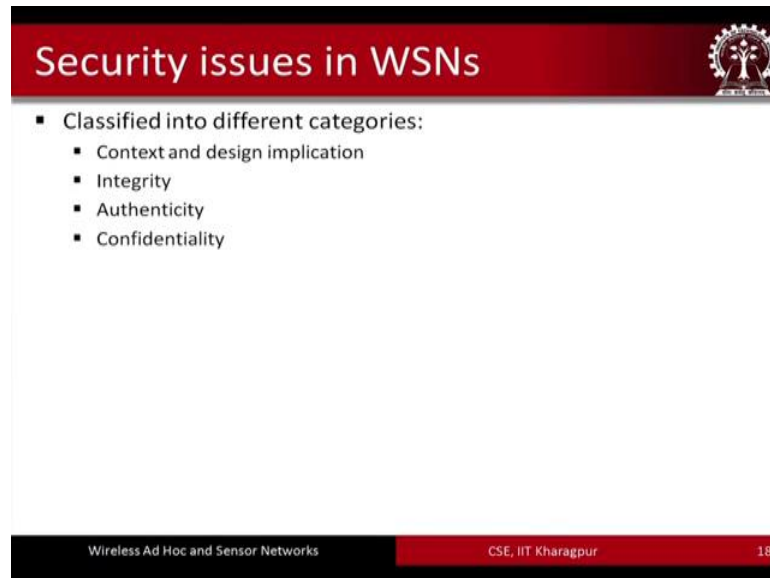
- Classified as two types as follows:
 - External attacks: Attackers reside outside the network. The consequences of this attack are:
 - Jamming the network
 - Consumption of resources (e.g.: battery, power, memory)
 - DoS attack
 - Internal attacks: Attackers reside inside the network. The consequences of this attack are:
 - Compromising the secret keys
 - Performance degradation

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Location based attacks classified into 2 types, external attacks and internal attacks. Attackers in the external attacks reside outside the network jamming is one such example. So, the jammer can be residing outside so in fact, jamming it is also possible to have the jammer inside the network as well, but typically it is assumed that the jammers are located externally away from the network. And they are sending high powered beams with high signal strength which are going to be disrupt the proper communication between the different nodes, because it is a low signal strength you know environment signals are very of very low strength in these sensor nodes and so, if there is a high powered signal that is sent to these different nodes in the network, that is going to affect the proper functioning of these networks.

Internal attacks the attackers reside inside the network they compromise the because of these kind of attacks the secret keys are compromised and the overall performance gets degraded.

(Refer Slide Time: 13:59)



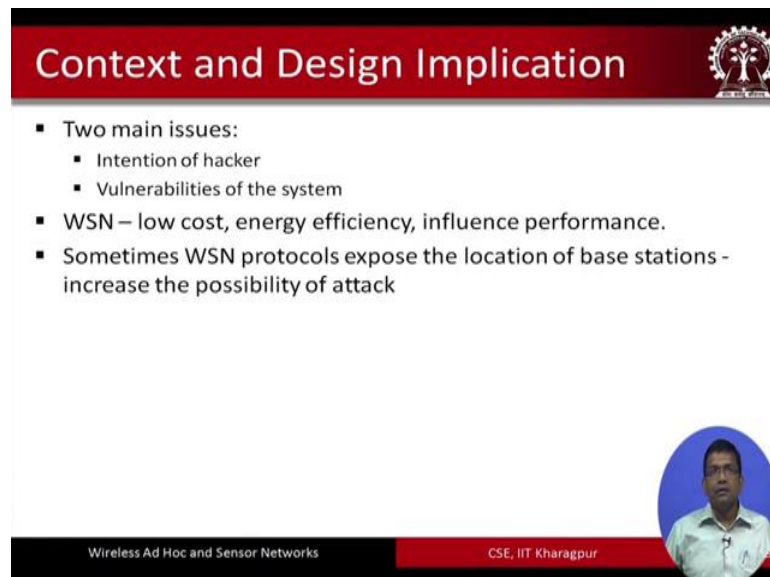
Security issues in WSNs

- Classified into different categories:
 - Context and design implication
 - Integrity
 - Authenticity
 - Confidentiality

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 18

So, there are different security issues that have to be taken care of in wireless sensor networks as well. Context and design implications are their integrity authenticity and confidentiality in different forms we have seen them earlier in the first part of this topic on security in sensor networks.

(Refer Slide Time: 14:20)



Context and Design Implication

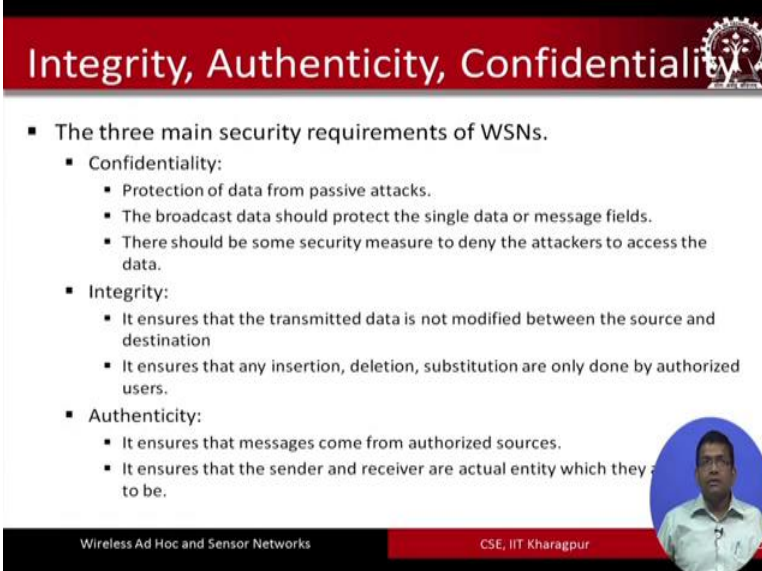
- Two main issues:
 - Intention of hacker
 - Vulnerabilities of the system
- WSN – low cost, energy efficiency, influence performance.
- Sometimes WSN protocols expose the location of base stations - increase the possibility of attack

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Context and design implications are there. So, you know one has to consider the intention of the hacker and the vulnerabilities of the system, in order to take care of these issues. And we just remind that we are dealing with a low cost you know low energy

wireless sensor network with too many different types of other constants as well, and these type of you know you know these type of issues become very important.

(Refer Slide Time: 14:53)



The slide features a red header with the text "Integrity, Authenticity, Confidentiality" and a small logo on the right. The main content is a bulleted list of security requirements for WSNs. At the bottom, there is a black footer with the text "Wireless Ad Hoc and Sensor Networks" and "CSE, IIT Kharagpur". A small circular inset image of a man in a light blue shirt is visible in the bottom right corner of the slide.

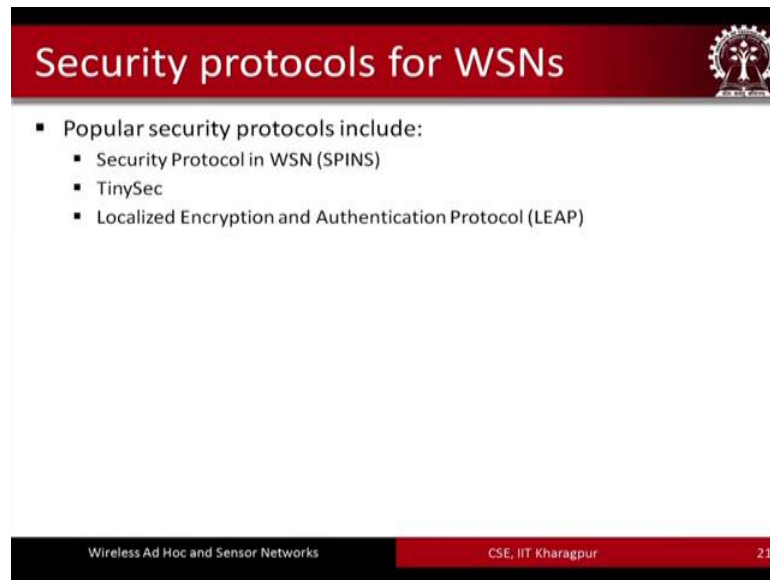
Integrity, Authenticity, Confidentiality

- The three main security requirements of WSNs.
 - Confidentiality:
 - Protection of data from passive attacks.
 - The broadcast data should protect the single data or message fields.
 - There should be some security measure to deny the attackers to access the data.
 - Integrity:
 - It ensures that the transmitted data is not modified between the source and destination
 - It ensures that any insertion, deletion, substitution are only done by authorized users.
 - Authenticity:
 - It ensures that messages come from authorized sources.
 - It ensures that the sender and receiver are actual entity which they are to be.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Integrity authenticity and confidentiality we have already seen before confidentiality talks about protecting the data from passive attacks. So, nobody you know who is not authorized should be able to get access to the data integrity is about that the data should be modified in transit. And the authenticity is that the data should be coming from the authorized sources and these are the things that we have already gone through just to have a recap of these basic fundamental requirements of security on sensor networks.

(Refer Slide Time: 15:24)



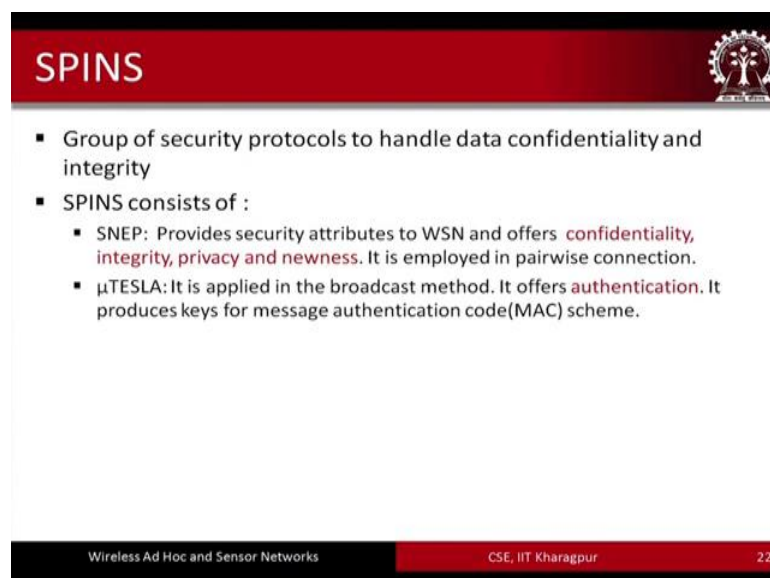
Security protocols for WSNs

- Popular security protocols include:
 - Security Protocol in WSN (SPINS)
 - TinySec
 - Localized Encryption and Authentication Protocol (LEAP)

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 21

So, security protocols for wireless sensor networks. There were there are large number of different types of protocols, that have been proposed I am just going to highlight these 3 protocols one is the security protocol in wireless sensor network called the spins protocol. In short a second is the tiyns tiynsec protocol, and the third is the leap protocol localized encryption and authentication protocol.

(Refer Slide Time: 15:49)



SPINS

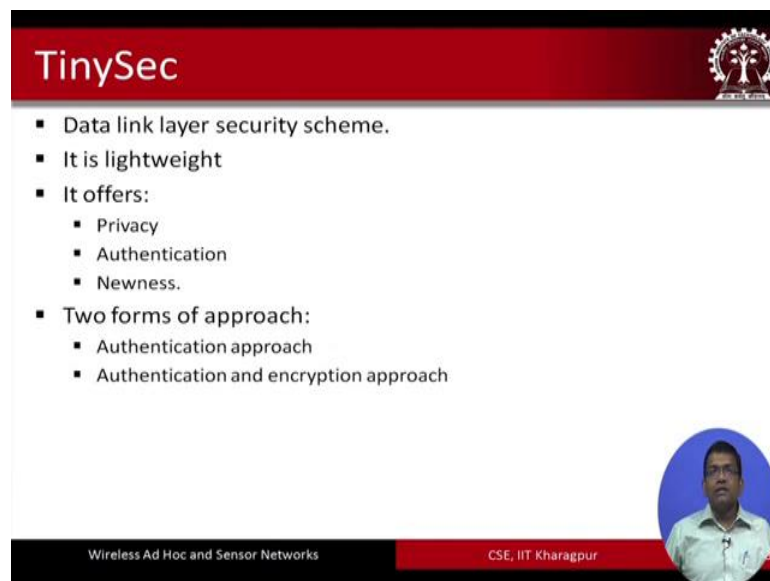
- Group of security protocols to handle data confidentiality and integrity
- SPINS consists of :
 - SNEP: Provides security attributes to WSN and offers **confidentiality, integrity, privacy and newness**. It is employed in pairwise connection.
 - μ TESLA: It is applied in the broadcast method. It offers **authentication**. It produces keys for message authentication code(MAC) scheme.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 22

Spins is a group of security protocols it is not just one protocol it is a group of protocols, which will take care of issues such as confidentiality and integrity. And so, spins

basically have 2 parts. One is called the SNEP, SNEP protocol basically provides you know provides you know requirements in fulfillment of requirements with respect to confidentiality integrity privacy and newness, and it is employed in pairwise connection between the different nodes. So, pairwise for pairwise scheme SNEP basically does that and the other part is the microtesla, and it is applied in the broadcast method it basically offers authentication and produces keys for message authentication code scheme.

(Refer Slide Time: 16:37)



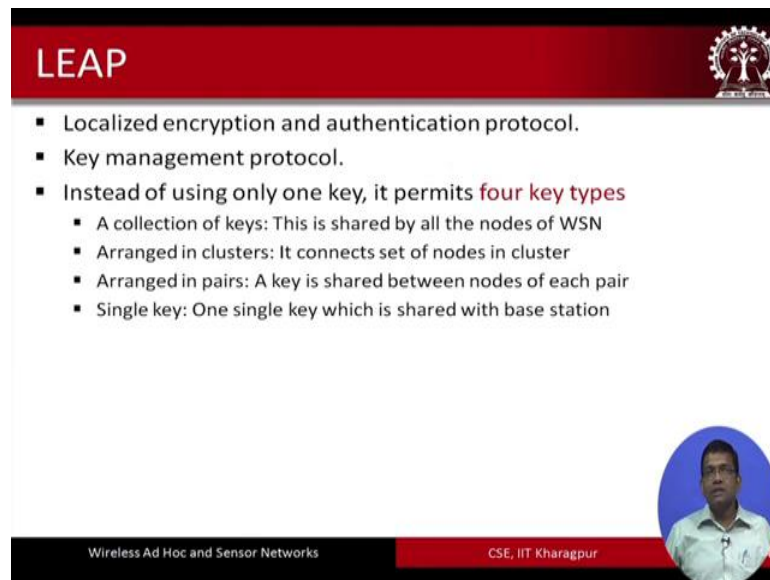
TinySec

- Data link layer security scheme.
- It is lightweight
- It offers:
 - Privacy
 - Authentication
 - Newness.
- Two forms of approach:
 - Authentication approach
 - Authentication and encryption approach

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Tiny sec it is a lightweight data link security protocol, it offers privacy authentication and newness. And there are 2 types of approaches that are adopted into a tiny sec one is the authentication approach the other one is authentication and encryption approach.

(Refer Slide Time: 16:53)



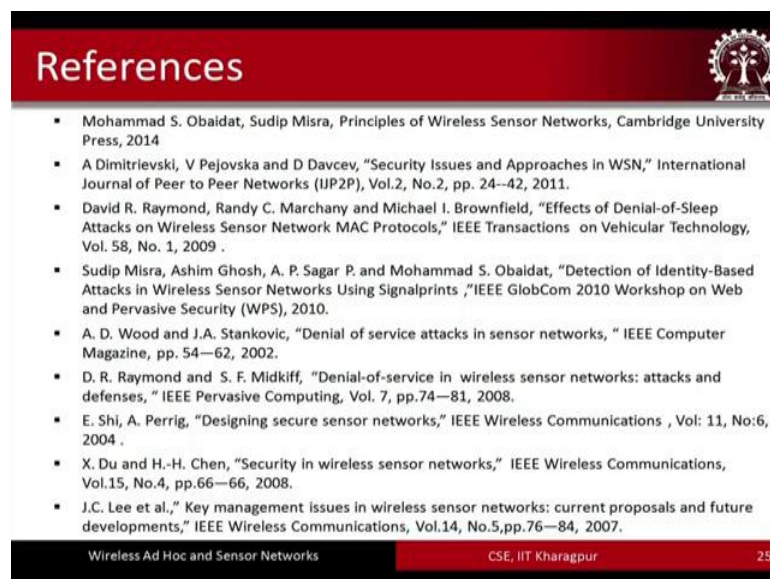
LEAP

- Localized encryption and authentication protocol.
- Key management protocol.
- Instead of using only one key, it permits **four key types**
 - A collection of keys: This is shared by all the nodes of WSN
 - Arranged in clusters: It connects set of nodes in cluster
 - Arranged in pairs: A key is shared between nodes of each pair
 - Single key: One single key which is shared with base station

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur

Leap protocol I am not going to go through it, but just to give a glimpse of this particular protocol. There are 4 different types of keys that are used a collection of keys this is shared by all the nodes in the network, arranged in arrangement in the form of clusters it connects the set of nodes in the form of a cluster, arranged in pairs these keys are arranged in pairs a key is shared between the nodes of each pair, and the single key is also used also which shared with the base station this particular CBP is shared with the base station.

(Refer Slide Time: 17:26)



References

- Mohammad S. Obaidat, Sudip Misra, Principles of Wireless Sensor Networks, Cambridge University Press, 2014
- A Dimitrievski, V Pejovska and D Davcev, "Security Issues and Approaches in WSN," International Journal of Peer to Peer Networks (IJPPN), Vol.2, No.2, pp. 24--42, 2011.
- David R. Raymond, Randy C. Marchany and Michael I. Brownfield, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Transactions on Vehicular Technology, Vol. 58, No. 1, 2009 .
- Sudip Misra, Ashim Ghosh, A. P. Sagar P. and Mohammad S. Obaidat, "Detection of Identity-Based Attacks in Wireless Sensor Networks Using Signalprints," IEEE GlobCom 2010 Workshop on Web and Pervasive Security (WPS), 2010.
- A. D. Wood and J.A. Stankovic, "Denial of service attacks in sensor networks," IEEE Computer Magazine, pp. 54--62, 2002.
- D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," IEEE Pervasive Computing, Vol. 7, pp.74--81, 2008.
- E. Shi, A. Perrig, "Designing secure sensor networks," IEEE Wireless Communications , Vol: 11, No:6, 2004 .
- X. Du and H.-H. Chen, "Security in wireless sensor networks," IEEE Wireless Communications, Vol.15, No.4, pp.66--66, 2008.
- J.C. Lee et al., "Key management issues in wireless sensor networks: current proposals and future developments," IEEE Wireless Communications, Vol.14, No.5, pp.76--84, 2007.

Wireless Ad Hoc and Sensor Networks CSE, IIT Kharagpur 25

So, here are the references. So, what we have seen so far are the different types of attacks that are possible on sensor networks. And we have also seen that there are different security protocols that have been proposed for sensor networks. We have first seen the spins protocol which is the one of the most popular sensor network security protocol that has been proposed. We have also seen the tiny sec as well as the leap protocol, but mind you that there are many more sensor network route security protocols that have been proposed and that exists in the literature, in these references you would be able to go through a few more of them.

So, actually I would suggest that you please go through some of these papers like the paper by Raymond and Midkiff which was published in the IEEE pervasive computing. It talks about the denial of service attacks and the different types of different types of DOS attacks that are possible of the under sensor networks, and the different solutions that have been proposed for it, but this paper is bit old it was published in 2008, since 2008 there are lot of other papers that have been proposed and a comprehensive summary of different types of security mechanisms and the different types of attacks and their counter solutions are available in the book by other than Mishra published by the Cambridge university place in 2014. It is titled principles of wireless sensor network the first reference in this slide.

So, with this we come to an end of the second part of the topic of sensor data security in sensor networks. And we have covered the security in sensor networks in 2 parts. First part was more focused on the security requirements and the second part more on the attacks and the solutions that have been proposed for sensor networks with this we covered the entire topic of security in sensor networks.

Thank you.