

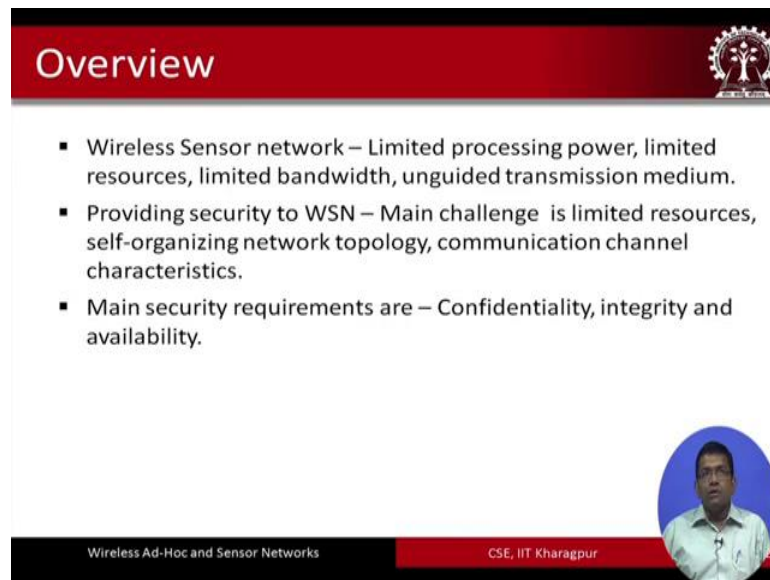
Wireless Ad Hoc and Sensor Networks
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture- 37
Security of Wireless Sensor Networks- Part-I

Security of wireless sensor networks; so, this particular topic has been segmented into 2. In the first part we are going to look at some of the requirements of security in sensor networks and what are the meanings of these requirements of security. And security first of all. So, this is the first part and the second they are after we are going to look into different attacks different types of attacks that are possible in sensor networks. And also very briefly about you know one of the possible solutions to each of them, but that we are not going to focus more.

We are going to focus more on what are the problems there are than the solutions because security as you can understand is a very big topic which is a vast topic with lot of different aspects and a search security is so much paramount and it is so much pass that there could be a separate course on security altogether even for wireless sensor network even for focusing on wireless sensor networks. Here could be a separate course. So, we just have to understand that what are the problems of security in wireless sensor networks and generally you know what are the different issues different types of attacks and what are the different types of solutions that are proposed for security in sensor networks.

(Refer Slide Time: 01:40)



The slide is titled "Overview" and features a red header bar with a logo on the right. The main content area is white and contains three bullet points. In the bottom right corner, there is a circular inset photo of a man in a light blue shirt. The footer consists of a black bar on the left with the text "Wireless Ad-Hoc and Sensor Networks" and a red bar on the right with the text "CSE, IIT Kharagpur".

Overview

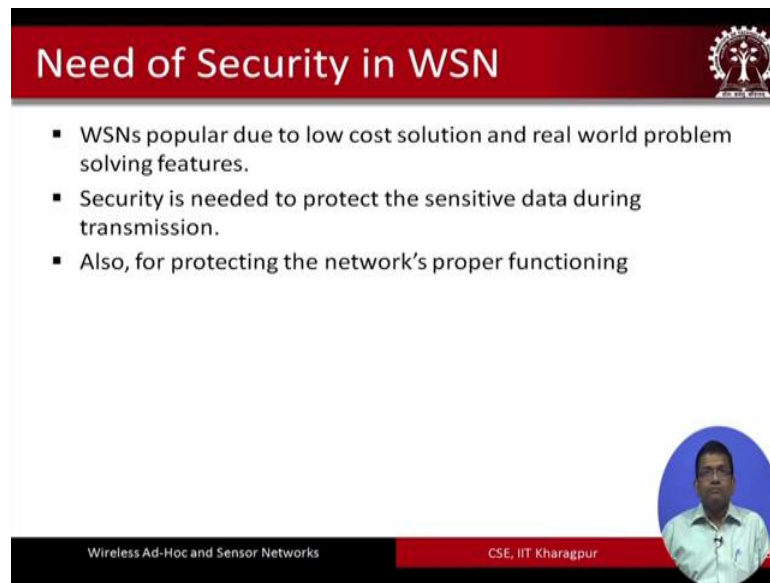
- Wireless Sensor network – Limited processing power, limited resources, limited bandwidth, unguided transmission medium.
- Providing security to WSN – Main challenge is limited resources, self-organizing network topology, communication channel characteristics.
- Main security requirements are – Confidentiality, integrity and availability.

Wireless Ad-Hoc and Sensor Networks

CSE, IIT Kharagpur

So, we have to understand couple of things. So, first of all what are the important security requirements. Requirements with respect to things like confidentiality integrity availability which are paramount in terms of requirements of security in any system including wireless sensor networks. This is number one number 2 is we also have to understand that when we are talking about security in sensor networks, that what are the what are the challenges that are going to arise when we want to establish security mechanisms in this networks right. So, we; that means, that we have to review we have to understand that what are the limitations what are the challenges of these sensor networks because of which implementation of these security requirements would be difficult. So, this is what we are going to cover in both the first and the second part of this topic of security sensor networks.

(Refer Slide Time: 02:39)



The slide features a red header with the title "Need of Security in WSN" and a small logo of a tree with a gear. Below the header, there is a bulleted list of three points. At the bottom right, there is a circular inset photo of a man in a light blue shirt. The footer contains the text "Wireless Ad-Hoc and Sensor Networks" and "CSE, IIT Kharagpur".

- WSNs popular due to low cost solution and real world problem solving features.
- Security is needed to protect the sensitive data during transmission.
- Also, for protecting the network's proper functioning

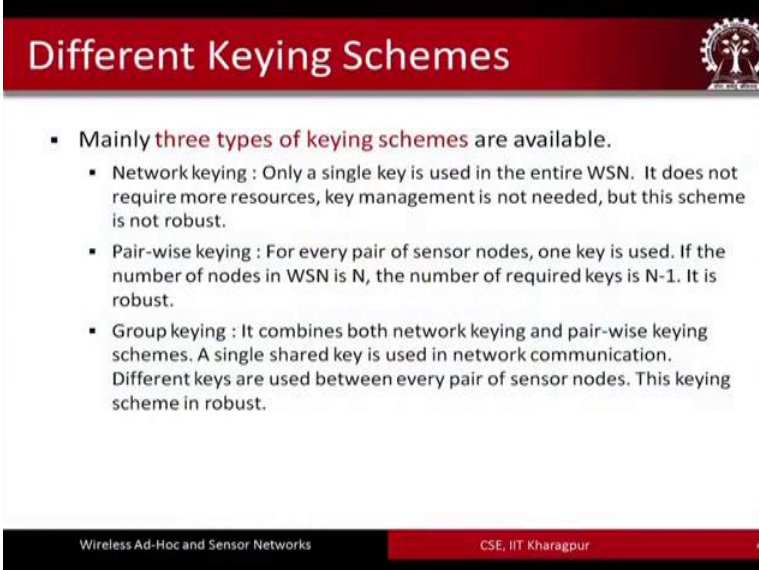
So, first of all you know we do not really have to emphasize once again that security is very important. So, we are talking about a network. And in any network as we know from our basic knowledge that you know networks are vulnerable to different types of attacks, bit wire network bit wireless even for wireless networks also even if we are talking about like Wi-Fi or cellular networks attacks of different types are possible right. So, this is very important. So, and when we are talking about wireless sensor networks, wireless sensor networks it is even more vulnerable. Because the sensor networks they are prone to different types of different types of attacks, because it is a wireless medium not only it is a wireless medium, but these nodes are very much resource constrained. Resource constraint with respect to computation resource constraint with respect to the memory. Limited memory that each of these nodes has plus energy consumption; that means, the they do not have much betterly with them and the solutions that you are going to propose for security in this networks they have to be very lightweight in all respects right.

So and at the same time these networks have to be protected even within this resource constraint sort of scenario these networks have to be protected, while proposing lightweight solutions that are perfect enough to protect these networks right. So that proper functioning of the network takes place and there is. So what kind of problems can arise in these networks. So, one thing is that the data that are sends by these different

sensor nodes. This data they can be either dropped maliciously or the data can be altered right.

So, the data that are sends by the different nodes you know when they are in transit when the data is in transit through the intermediate nodes to the intended sink node, the data can be altered, the data can be dropped in between maliciously that when some node which is attacking one the network in also maliciously it basically drops this information. The third thing is that the protocols and the devices means the nodes themselves, they can be compromised or the protocols they can be altered in the communication protocols they could be altered so that the intended functionality of these protocols are affected. So, these are the different types of problems that can arise in arising with respect to security in sensor networks. So, how do you come up with lightweight solutions in a resource constrained environment like this is the whole challenge of security in sensor networks.

(Refer Slide Time: 05:35)



Different Keying Schemes

- Mainly **three types of keying schemes** are available.
 - **Network keying** : Only a single key is used in the entire WSN. It does not require more resources, key management is not needed, but this scheme is not robust.
 - **Pair-wise keying** : For every pair of sensor nodes, one key is used. If the number of nodes in WSN is N , the number of required keys is $N-1$. It is robust.
 - **Group keying** : It combines both network keying and pair-wise keying schemes. A single shared key is used in network communication. Different keys are used between every pair of sensor nodes. This keying scheme is robust.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur 4

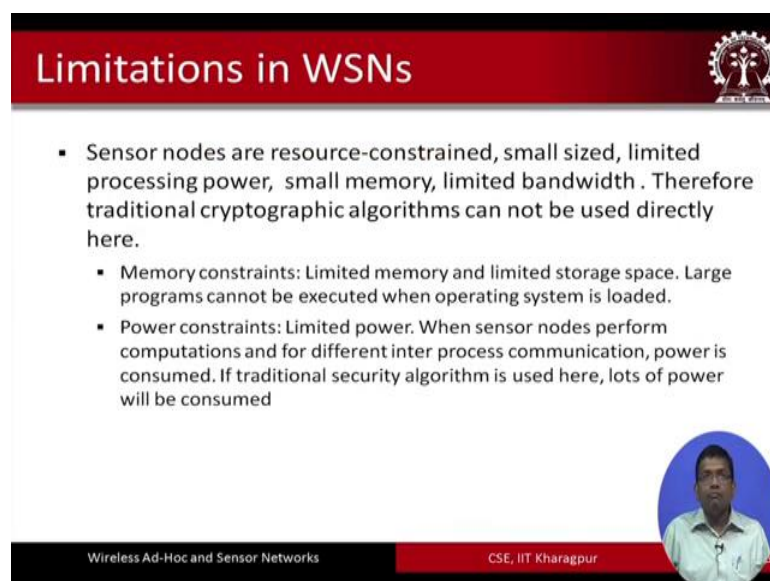
So when we talk about security mechanisms, cryptography based mechanisms come into the picture very easily. So, when we talk about cryptography, we have are dealing with keys. So, we know that in cryptography there are 2 types of cryptographic mechanisms one is called the symmetric key the other one is the asymmetric key. So irrespective of what type of key mechanism is being used. So, keys are very important. And there are 3 basically 3 types of key mechanisms that are available for sensor networks. One is the

network keying mechanism, where there is a single key that can be used for the entire sensor network for the entire network you have a single key.

So, basically you know one thing is that the good thing is that, because there is only a single key you do not this kind of implementation of this kind of networking mechanisms does not consume too much of resources. So, that is a good part and as such you know you do not even have to have keying key management based mechanisms that have been proposed for other types of networks. You do not have to have that, but in terms of robustness these are not very good. So, networking mechanisms are not very good. The second is the pair wise scheme and again as this name says that for every pair of sensor nodes a single key is used and maintained. So basically you know quite understandably that if the number of nodes in the network is N then the required number of keys is going to be N minus 1. And it is relatively robust compared to the networking. Because you know here for every pair of nodes you are using a different key. So, this is the pair wise key.

And the third is like a hybrid kind of it is called group keying. It combines the properties of both networking and pair wise keying mechanisms. So, a single shared key is used for the network communication and different keys are used for every pair of sensor nodes. So, it is a hybrid kind of approach you know using both. And this scheme is more robust compared to the previous ones.

(Refer Slide Time: 07:55)



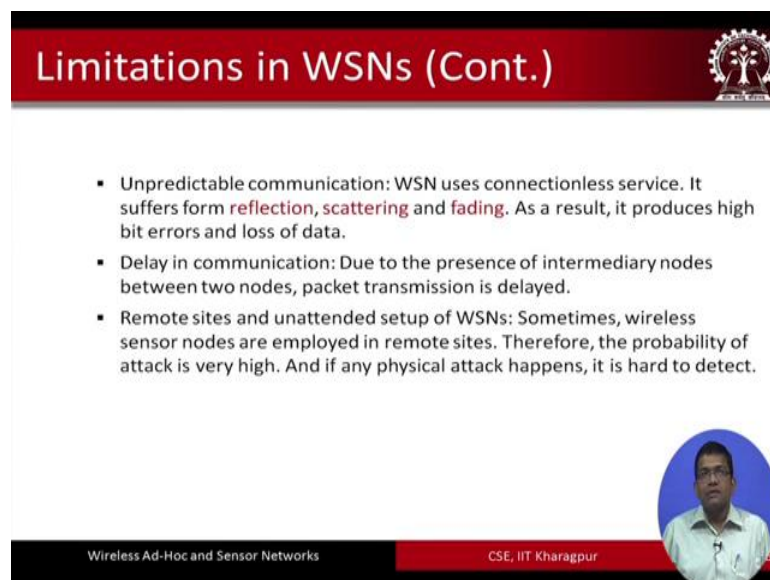
Limitations in WSNs

- Sensor nodes are resource-constrained, small sized, limited processing power, small memory, limited bandwidth. Therefore traditional cryptographic algorithms can not be used directly here.
 - Memory constraints: Limited memory and limited storage space. Large programs cannot be executed when operating system is loaded.
 - Power constraints: Limited power. When sensor nodes perform computations and for different inter process communication, power is consumed. If traditional security algorithm is used here, lots of power will be consumed

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur

Now, I think said before that there is wireless sensor networks basically have lot of limitations with respect to the memory, energy etcetera. So, first of all you know we are talking about in a typical sensor node we are talking about memory, which is just a few kilobytes just a few kilobytes, and you can understand that buffering becomes very difficult and if you are trying to use the traditional cryptographic mechanisms directly they cannot be used right. So, because you know these traditional cryptographic mechanisms, they are the memory hungry as well as power or energy hungry. They will consume they are computationally intensive because they are computationally intensive they are going to consume lot of energy right

(Refer Slide Time: 08:55)



The slide is titled "Limitations in WSNs (Cont.)" and features a red header with a logo on the right. The main content is a list of three bullet points. At the bottom right, there is a circular inset photo of a man in a white shirt. The footer contains the text "Wireless Ad-Hoc and Sensor Networks" and "CSE, IIT Kharagpur".

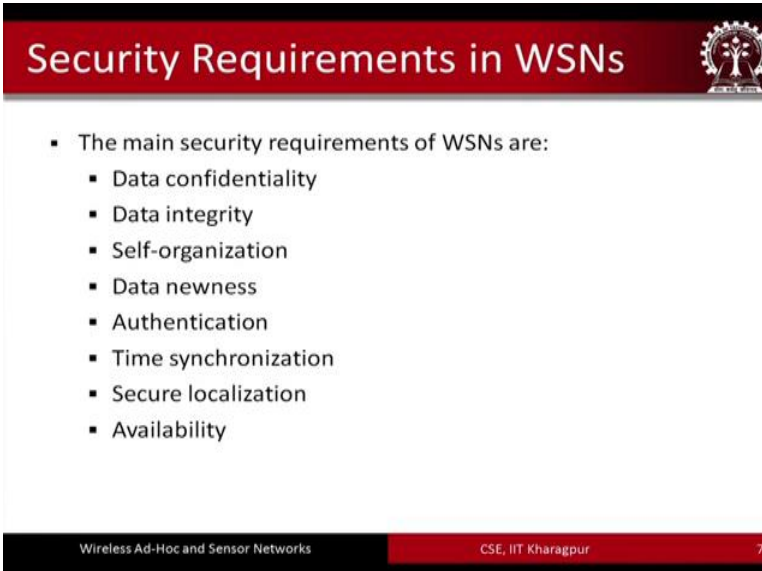
- Unpredictable communication: WSN uses connectionless service. It suffers from reflection, scattering and fading. As a result, it produces high bit errors and loss of data.
- Delay in communication: Due to the presence of intermediary nodes between two nodes, packet transmission is delayed.
- Remote sites and unattended setup of WSNs: Sometimes, wireless sensor nodes are employed in remote sites. Therefore, the probability of attack is very high. And if any physical attack happens, it is hard to detect.

So these are not very suitable for use in these resource constrained environments. Additionally, there are other limitations as well. Wireless sensor networks are more prone to different types of contradict ability unpredictable behavior such as reflection, scattering, fading etcetera which basically leads to huge data loss bit errors etcetera right. So, unpredictable communication. Delay in communication due to the presence of intermediate nodes between 2 nodes and because of this particular because it is a multi hop. So, you have you know between the source node and the destination node there are intermediate nodes and because of which the packet transmission gets delayed right. The third is the remote site and unattended setup of wireless sensor networks. So, the typically the nodes they are unattended, they are not they are not manned by anybody

and additionally these nodes they are deployed at remote sites for remote monitoring, remote continuous monitoring etcetera.

And the probability of attacks due to these basically increases even the physical attack can also happen; that means, the nodes physical can be compromised right. So, they can be removed they can be in a tempered etcetera. So, and because they are remotely deployed they are hard to detect you know this kind of tempering, and you know this kind of behavior where the nodes are physically compromised that would be hard to detect these networks.

(Refer Slide Time: 10:22)

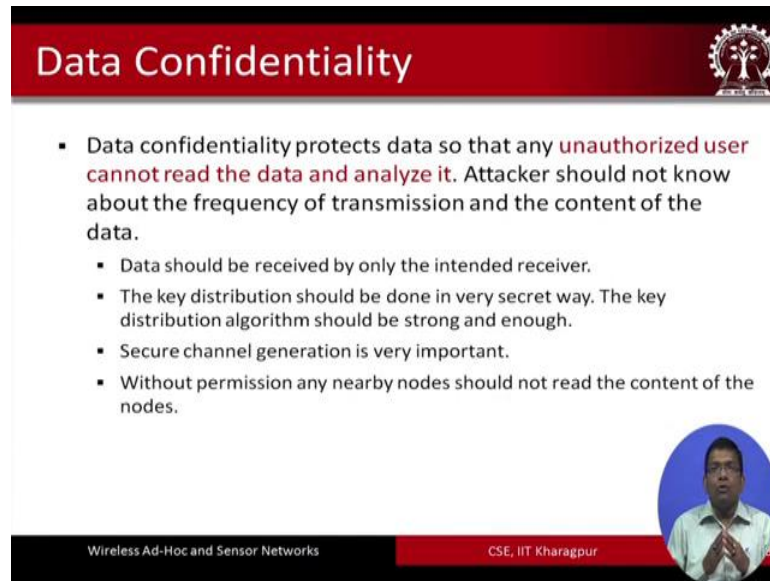


The slide features a red header with the title "Security Requirements in WSNs" and a small circular logo on the right. The main content is a bulleted list of security requirements. The footer contains the text "Wireless Ad-Hoc and Sensor Networks" on the left, "CSE, IIT Kharagpur" in the center, and the number "7" on the right.

- The main security requirements of WSNs are:
 - Data confidentiality
 - Data integrity
 - Self-organization
 - Data newness
 - Authentication
 - Time synchronization
 - Secure localization
 - Availability

Now I am going to now go through some of the security requirements in wireless sensor networks. So, these are the main requirements one is confidentiality integrity self organization newness of data authentication time synchronization secure localization and availability. So, briefly I am going to touch upon each of these requirements.

(Refer Slide Time: 10:45)



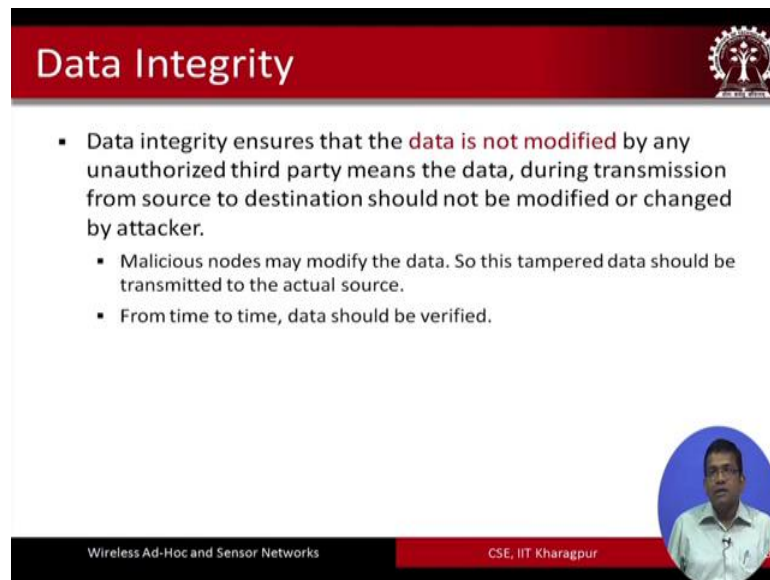
Data Confidentiality

- Data confidentiality protects data so that any **unauthorized user cannot read the data and analyze it**. Attacker should not know about the frequency of transmission and the content of the data.
 - Data should be received by only the intended receiver.
 - The key distribution should be done in very secret way. The key distribution algorithm should be strong and enough.
 - Secure channel generation is very important.
 - Without permission any nearby nodes should not read the content of the nodes.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur

So, when we are talking about confidentiality. So, confidentiality as we know a means that whoever is authorized for the data that entity should only get access to the data and others should not you know the data should be confidential and should not be accessible to any other entity who are not authorized for the data. So, the data should be received by only the intended receiver the key distribution should be done in a very secret way and the channel itself should be secured the channel those are which the data is sent it has to be secured that is very important and without the permission any nearby nodes should not read the content of the of the data that is being carried. So, without permission I mean nobody should no one else no other node should be able to get access to the data should be able to read the data and of course, not analyze the data.

(Refer Slide Time: 11:53)



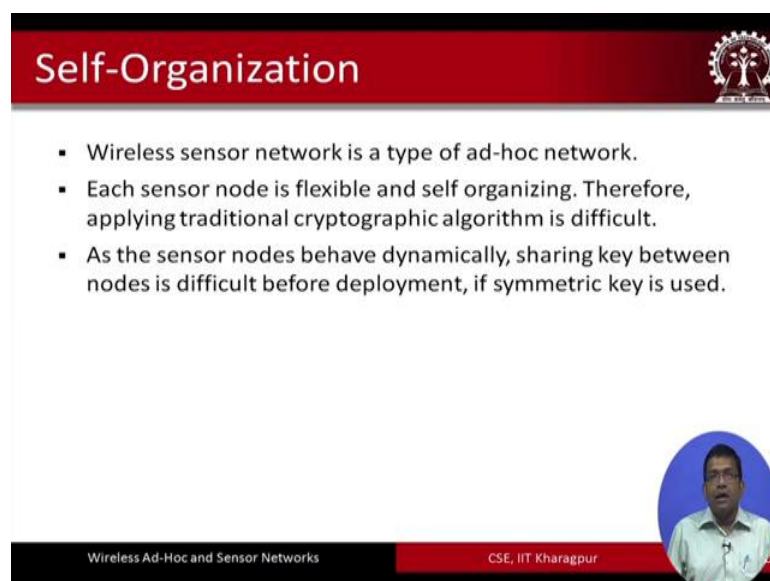
Data Integrity

- Data integrity ensures that the **data is not modified** by any unauthorized third party means the data, during transmission from source to destination should not be modified or changed by attacker.
 - Malicious nodes may modify the data. So this tampered data should be transmitted to the actual source.
 - From time to time, data should be verified.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur

So, that is data confidentiality the next one is data integrity. So, integrity again the dictionary meaning of it applies over here as well. So, the data that is obtained by the sensor nodes and is in transit over the network should not be modified by any third party by any means. So, the data is being transmitted the data you know the original data from the source to the intended destination node the base station etcetera. You know the integrity of the data should be maintained nobody should be able to modify the data that is in transit.

(Refer Slide Time: 12:34)



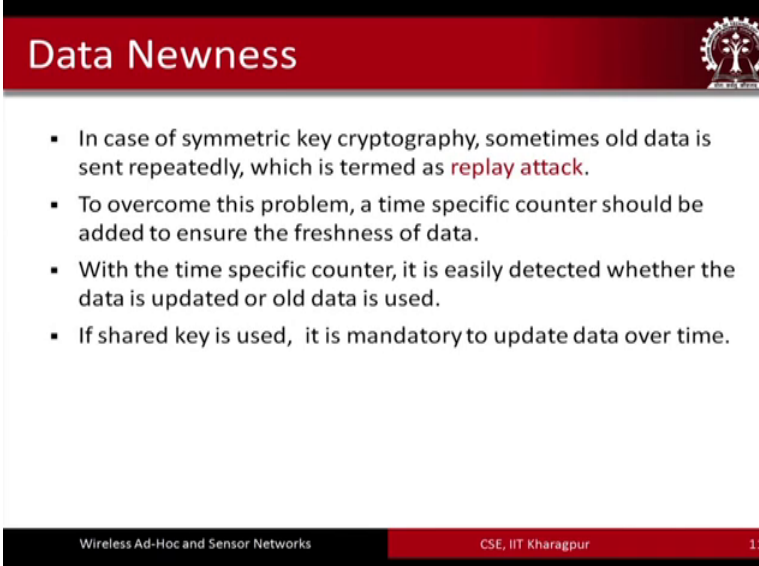
Self-Organization

- Wireless sensor network is a type of ad-hoc network.
- Each sensor node is flexible and self organizing. Therefore, applying traditional cryptographic algorithm is difficult.
- As the sensor nodes behave dynamically, sharing key between nodes is difficult before deployment, if symmetric key is used.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur

Third is self organization self organization in ad hoc network sensor networks is very important. So, you have we have a typically dynamic kind of topology and many things are dynamic by virtue of self organization because of which the application of the traditional cryptographic algorithms is difficult. So, traditional cryptographic algorithms like RSA etcetera. They assume that the overall topology remains fixed over time and did not change and whereas, in a self organizing network the topology in different ways the topology changes physical topology may also change, but due to the slip scheduling etcetera the logical topology the virtual topology can also change. So, because of which you know the application of traditional cryptographic mechanisms is difficult. So, you cannot use.

(Refer Slide Time: 13:29)



The slide features a red header with the title "Data Newness" and a logo on the right. The main content is a list of four bullet points. The footer contains the text "Wireless Ad-Hoc and Sensor Networks", "CSE, IIT Kharagpur", and the number "11".

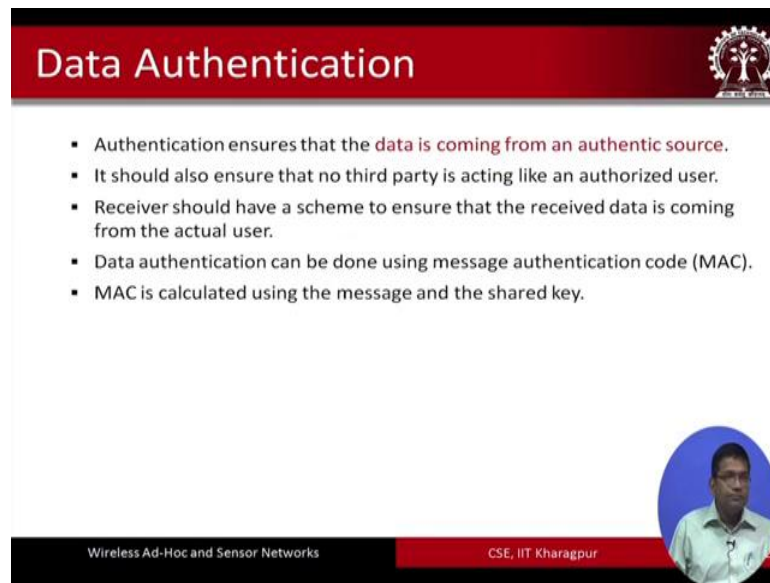
Data Newness

- In case of symmetric key cryptography, sometimes old data is sent repeatedly, which is termed as **replay attack**.
- To overcome this problem, a time specific counter should be added to ensure the freshness of data.
- With the time specific counter, it is easily detected whether the data is updated or old data is used.
- If shared key is used, it is mandatory to update data over time.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur 11

Data newness; that means, that the old data should not be sent repeatedly. So, basically you know if that is violated what we have is something called the replay attack. The replay attack as we will see later also basically the same old data you know periodically it is sent over and over again. So, to overcome this problem what could be done is to keep a timer time specific counter, which should be added to ensure the freshness of the data with the time specific counter it is easily detected whether the data is updated or old data is used.

(Refer Slide Time: 14:06)



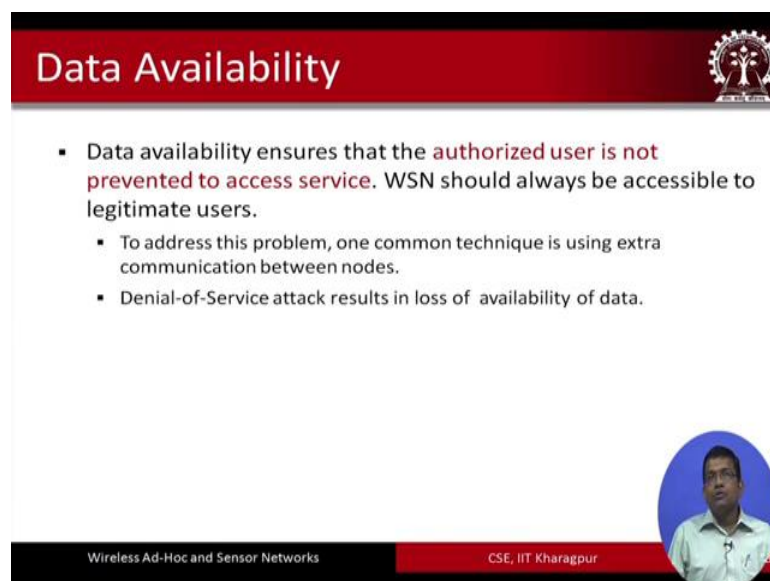
Data Authentication

- Authentication ensures that the **data is coming from an authentic source**.
- It should also ensure that no third party is acting like an authorized user.
- Receiver should have a scheme to ensure that the received data is coming from the actual user.
- Data authentication can be done using message authentication code (MAC).
- MAC is calculated using the message and the shared key.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur

Authentication data authentication. So, the data that is coming it should be from an authentic source some you know it should not happen that anybody can throw in pump in data into the network right. So, it should be coming from an authentic source. Otherwise what is going to happen is any malicious entity can come in and you know through it data into the network and that data is basically you know garbage data when it is a malicious data. So, it should not be used. So you know. So, authentication of the source is very important, authentication of the source and just to ensure that the data that is coming is also authentic.

(Refer Slide Time: 14:46)



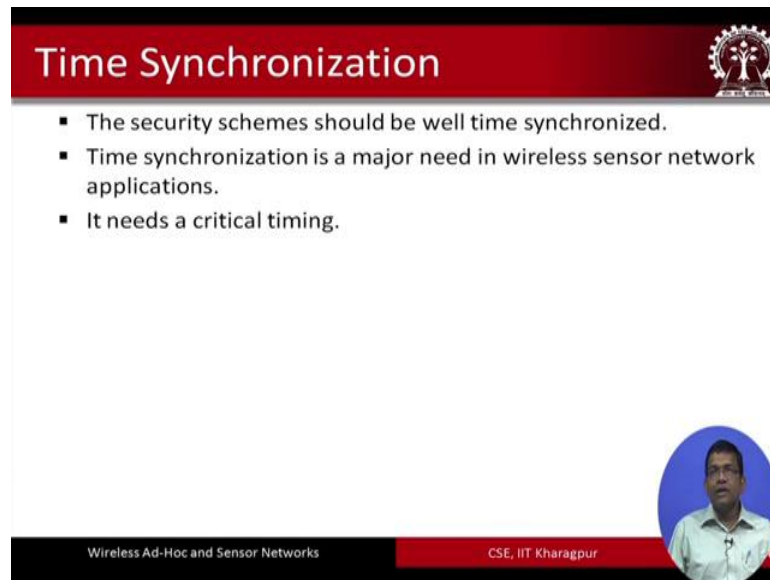
Data Availability

- Data availability ensures that the **authorized user is not prevented to access service**. WSN should always be accessible to legitimate users.
 - To address this problem, one common technique is using extra communication between nodes.
 - Denial-of-Service attack results in loss of availability of data.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur

Data availability basically you know it ensures that the authorized user is not prevented to access the service, authorized user is not prevented to access the service. So, sensor networks should always be accessible to the legitimate users.

(Refer Slide Time: 15:04)



The slide features a red header with the title "Time Synchronization" and a small logo on the right. Below the header, there are three bullet points. In the bottom right corner, there is a circular inset photo 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.

Time Synchronization

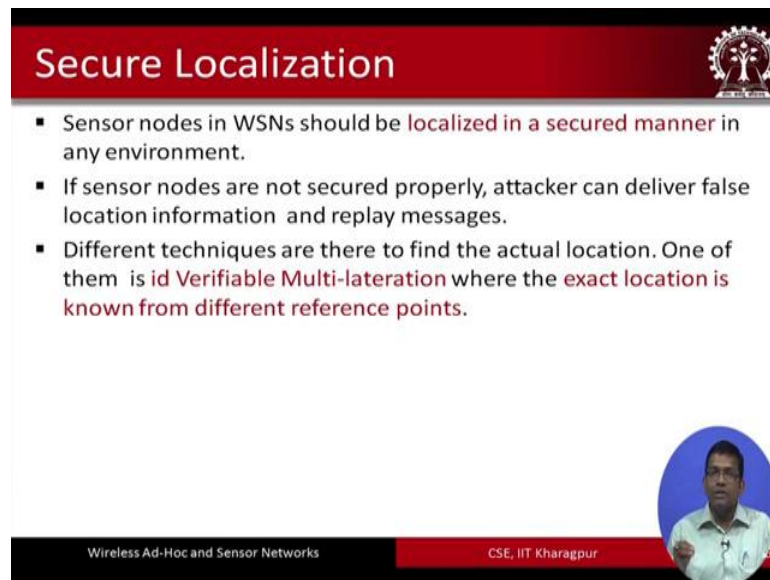
- The security schemes should be well time synchronized.
- Time synchronization is a major need in wireless sensor network applications.
- It needs a critical timing.

Wireless Ad-Hoc and Sensor Networks

CSE, IIT Kharagpur

Time synchronization is very important. So, you know as we can understand that. So, we have a distributed kind of environment the different entities which are participating in the security mechanisms this will be time synchronized. So this is a very critical aspect it needs you know. So, the different entities which are participating they have to be time synchronized in order for the entire processes or the different security mechanisms of the solutions that are deployed to run successfully.

(Refer Slide Time: 15:36)



Secure Localization

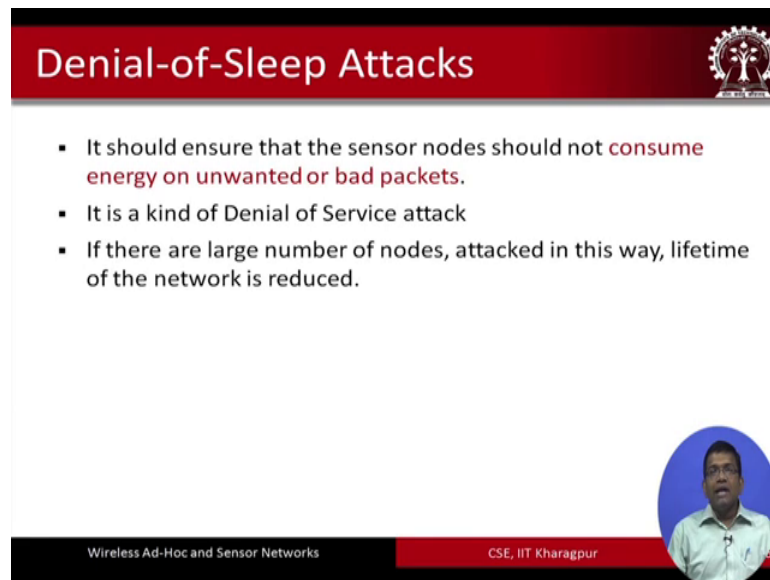
- Sensor nodes in WSNs should be **localized in a secured manner** in any environment.
- If sensor nodes are not secured properly, attacker can deliver false location information and replay messages.
- Different techniques are there to find the actual location. One of them is **id Verifiable Multi-lateration** where the **exact location is known from different reference points**.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur

Secured localization you see that localization means that understanding the locations of the different nodes getting that information. So, in sensor networks typically the data that is coming has to be geo tagged; that means, the geographic location of the data geographic location of the sensor nodes which are throwing in the data should also be emitted along with the data that is coming in otherwise the data has got no meaning.

Now the problem is that if that is compromised if that is compromised; that means, the actual location of the sensor node is not given along with the data maybe you know some other location is given or something like that that would lead to problems because you know. So, the correct location of the data has to be you know attended along with the data that is being same sent.


(Refer Slide Time: 16:33)



Denial-of-Sleep Attacks

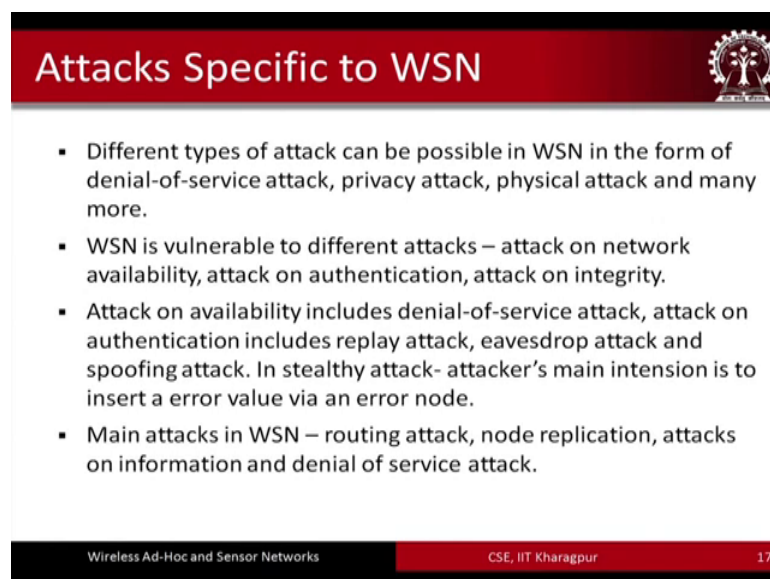
- It should ensure that the sensor nodes should not **consume energy on unwanted or bad packets**.
- It is a kind of Denial of Service attack
- If there are large number of nodes, attacked in this way, lifetime of the network is reduced.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur



Now, denial of sleep attacks is another typical aspect of wireless sensor network security in wireless sensor networks. So, basically what happens is this is the kind of denial of service attack where lot of unwanted or garbage packets could be sent into the network. So, these nodes they are always going to be kept busy and active and because of which they are not going to go to the sleep state and they are going to fast consume their limited resources the energy etcetera and that is one type of unwanted.

(Refer Slide Time: 17:15)



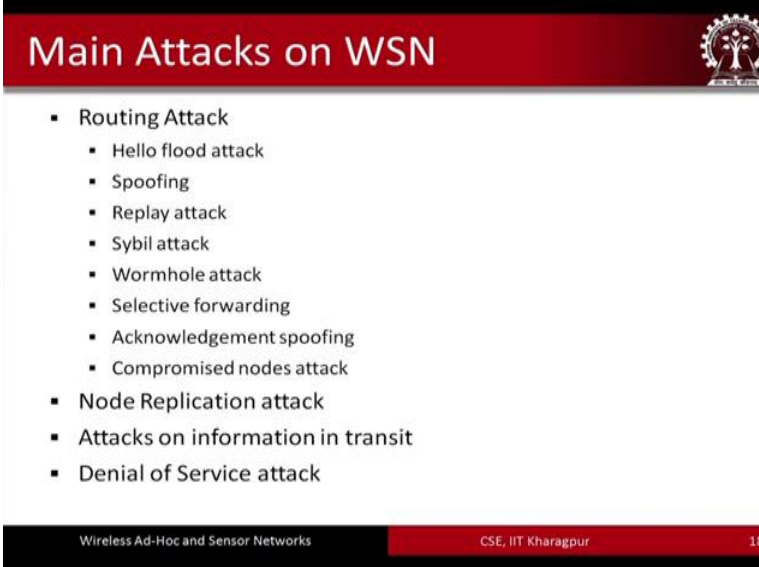
Attacks Specific to WSN

- Different types of attack can be possible in WSN in the form of denial-of-service attack, privacy attack, physical attack and many more.
- WSN is vulnerable to different attacks – attack on network availability, attack on authentication, attack on integrity.
- Attack on availability includes denial-of-service attack, attack on authentication includes replay attack, eavesdrop attack and spoofing attack. In stealthy attack- attacker's main intension is to insert a error value via an error node.
- Main attacks in WSN – routing attack, node replication, attacks on information and denial of service attack.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur 17

That is one type of an attack which is unwanted and there are different types of attacks that are specific to wireless sensor networks routing attack node replication attack attacks on information, and denial of service physical attacks are also possible, and attacks on authentication attacks or network availability attacks on integrity and there will like this actually there are large number of different types of attacks that are possible for wireless sensor network.

(Refer Slide Time: 17:41)



The slide is titled "Main Attacks on WSN" and features a red header with a logo on the right. The main content is a bulleted list of attack types. At the bottom, there is a black footer with white text and a red footer with white text.

- Routing Attack
 - Hello flood attack
 - Spoofing
 - Replay attack
 - Sybil attack
 - Wormhole attack
 - Selective forwarding
 - Acknowledgement spoofing
 - Compromised nodes attack
- Node Replication attack
- Attacks on information in transit
- Denial of Service attack

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur 18

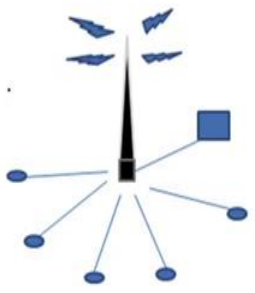
And we are now going to go through some of the main attacks on these networks when we are talking about routing attack there are few which are quite popular in the sensor network community. One is called the hello flood attack the second is the spoofing attack replay attack, Sybil attack, wormhole attack, selective forwarding acknowledgement spoofing compromised nodes attack. So, this is these are called the routing attacks.

Then we have the node replication attacks on information that is in transit and we have denial of service attacks. So, these are the different types of attacks that are possible different categories of attacks that are possible on any wireless sensor network.

(Refer Slide Time: 18:24)

Hello Flood Attack

- Attacker employs a high power transmitter which sends 'hello' packets constantly.
- The nodes which receives these 'hello' packets, assume that the received packets come from neighboring node.
- The nodes start communicating with the attacker.
- Attacker gains control over the network



The diagram illustrates a Hello Flood Attack. A central black tower with a signal antenna is labeled 'Hello flood attack'. It is surrounded by several blue circular nodes. Lines connect the tower to each node, representing the transmission of 'hello' packets. The nodes are arranged in a circle around the tower, and the lines represent the communication links between the attacker and the nodes.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur 19

Hello flood attack is like this. So, what we have is basically a high power transmitter like this you know, it is a high power transmitter which basically periodically got periodically when it is basically successively it will send the hello packets at a very high power and the intermediate nodes. Sorry the nodes which are in the close with the close proximity, then these nodes we are going to receive the hello packets which assume that basically these nodes are going to assume that, if these are coming from a legitimate neighboring node. And these nodes they start communicating with the attacker instead of the actual base station. So, you know it is coming from a you know. So, this particular attacker gives like a strong power legitimate neighbor 2 of these nodes and these nodes they are fulfilled in the process. And they would start communicating with the attacker thinking that it is a legitimate node. And this is my by doing this the attacker basically gains control over the entire network.

(Refer Slide Time: 19:29)

Spoofing Attack

- In spoofing attack, **message is altered** during transmission.
- Receiver receives inaccurate information.
- Routing action becomes different, data has to travel long distance.
- Consumes power of wireless sensor network.
- One common solution to tackle this spoofing attack is to apply different integrity checking mechanisms like message authentication code (MAC)

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur 20

Spoofing attack. So, in spoofing attack the message itself is altered during transmission the receiver receives the inaccurate information and the routing action becomes different and the data has to travel long distance because of this. And because of this particular thing unnecessary consumption of energy is going to take place in the entire network like. So, this is called the spoofing attack.

(Refer Slide Time: 19:55)

Replay Attack

- In Replay attack, same old message is sent repeatedly over the wireless sensor network.
- The bandwidth of the sensor network degrades.
- To overcome this attack timestamp or nonce is used with encryption algorithm to identify the old message.
- Timestamp is more preferred as it requires lesser number of messages compared to nonce.

Replay attack: Attacker intercepts the message, and retransmits it in future

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur 21

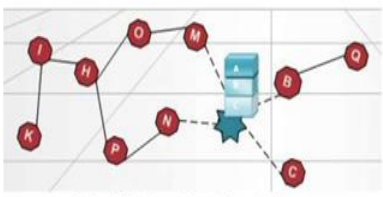
Now replay attack in replay attack as we can see that let us say that we have the source node and the destination node and this attacker will come in in between it inter intercepts

the message and retransmit it in the future. So, what it will do this attacker will come in between these 2 nodes and it will get access to this message that is that has been sent it will intercept it, and it will it will retransmit the data successively in the future. So, this is called the replay attack. And that basically is will consume the limited bandwidth of these networks unnecessarily because you know no new data is being sent and unnecessarily the bandwidth of the network is going to be consumed, and that basically brings the gradually that is going to bring the network town in the in the short term.

(Refer Slide Time: 20:55)

Sybil Attack

- Single malicious node behaves like multiple nodes.
- This malicious node sends several fake message.
- WSNs vulnerable to this attack, as sensor nodes are deployed in a very unstructured manner
- One solution is key registration system



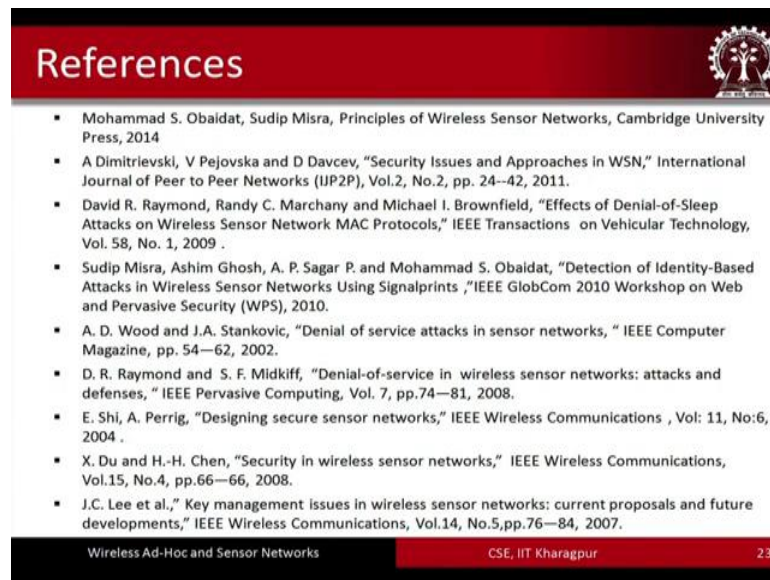
Dimitrievski, Popovska and Davcević, International Journal of Peer to Peer Networks, 2011

Sybil attack. A single malicious node behaves like multiple nodes.

Wireless Ad-Hoc and Sensor Networks CSE, IIT Kharagpur 22

Sybil attack. So, in Sybil attack basically it is sort of like faking a single a single basically a single sensor node will be like fixed as to have multiple identities. So basically a single malicious node behaves like multiple nodes essentially multiple nodes. So, in this particular case these malicious nodes they sent several fake messages and the sensor networks they are vulnerable to this attack as the sensor nodes are deployed in very on a unstructured manner. So, Sybil attack is quite common consequently in these networks.

(Refer Slide Time: 21:37)



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 23

So, here is a few types of different types of routing attacks that I have mentioned. So, far there are few more that I am going to cover in the next part and here are the references whatever has been covered. So, far you know it was many of them are quite interesting. So, what would be encouraged to go through these go through go through these references that will improve the understanding of security issues in in sensor networks.

Thank you.