Wireless Ad Hoc and Sensor Networks

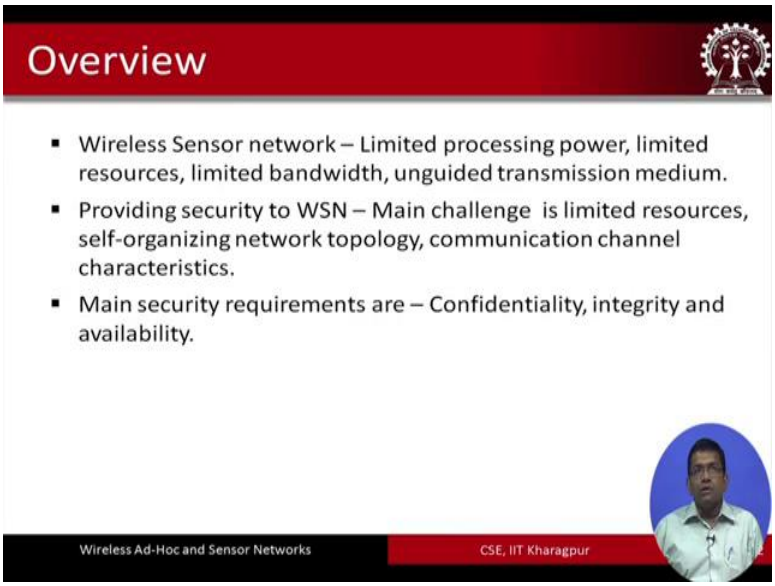
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

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.

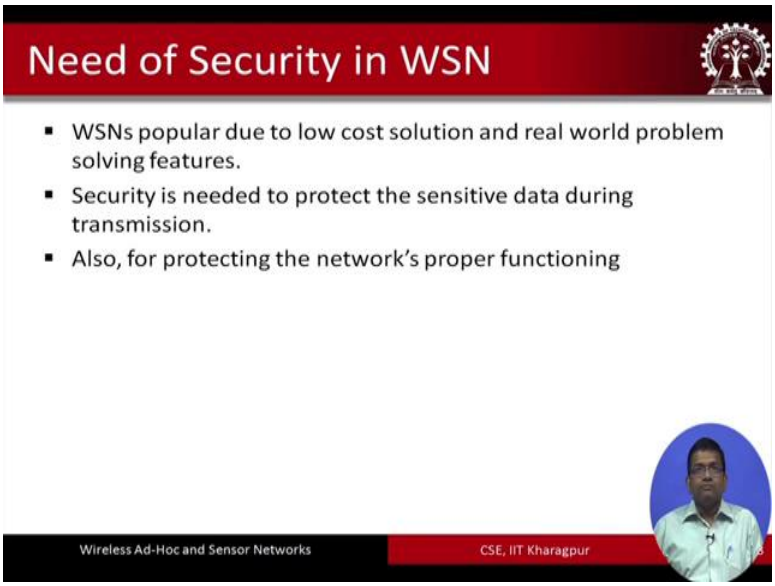
We are going to focus more on what are the problems there are than the solutions because security as you can understand is a very big topic which is a vast topic with lot of different aspects and a search security is so much paramount and it is so much pass that there could be a separate course on security 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)



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)



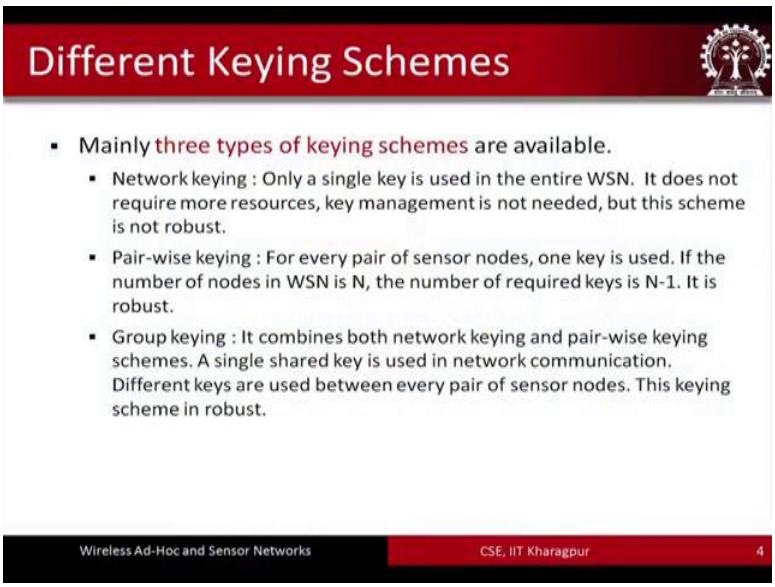
So, first of all you know we do not really have to emphasize once again that security is very important. So, we are talking about a network. And in any network as we know from our basic knowledge that you know networks are vulnerable to different types of attacks, bit wire network bit wireless even for 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)



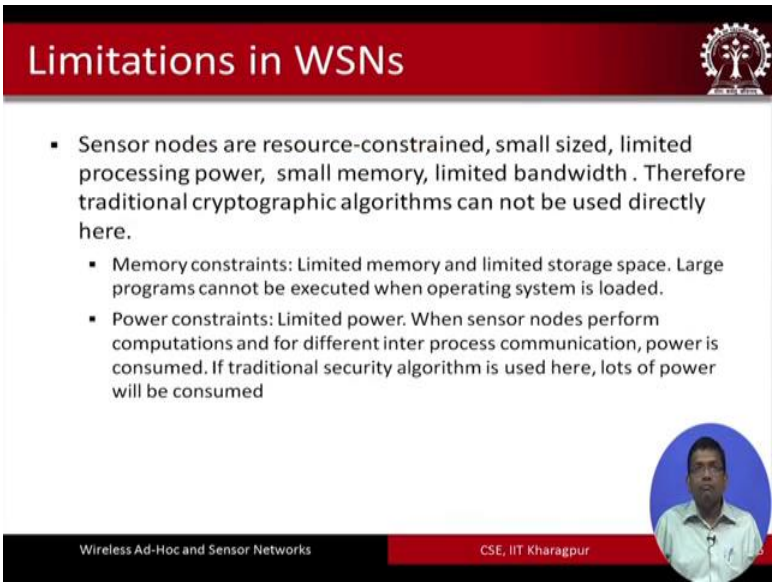
So when we talk about security mechanisms, cryptography based mechanisms come into the picture very easily. So, when we talk about cryptography, we have are dealing with keys. So, we know that in cryptography there are 2 types of cryptographic mechanisms one is called the symmetric key the other one 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.

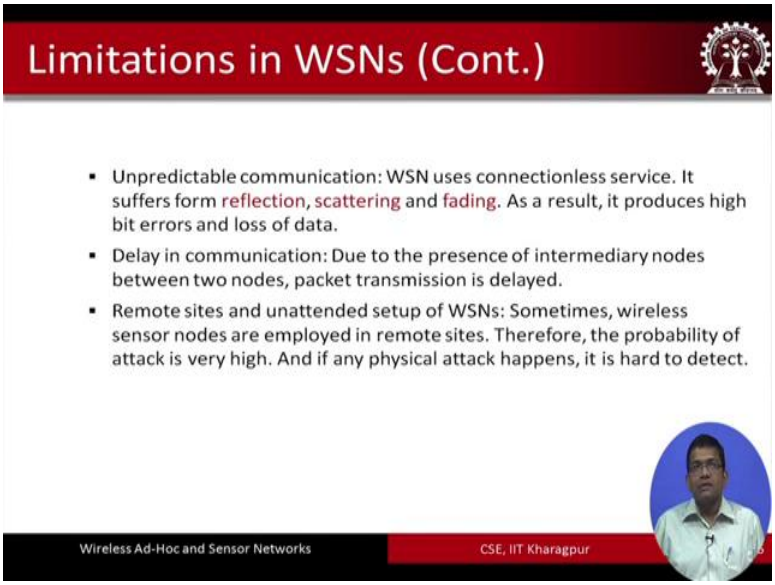
And the third is like a hybrid kind of it is called group keying. It combines the properties of both networking and pair wise keying mechanisms. So, a single shared key is used for the network communication and different keys are used for every pair of sensor nodes. So, it is a hybrid kind of approach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

(Refer Slide Time: 07:55)



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)

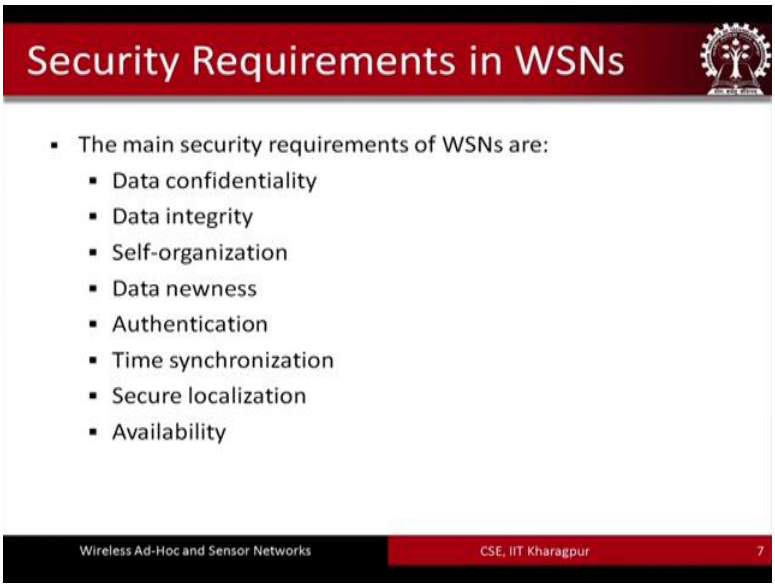


So these are not very suitable for use in these resource constrained environments. Additionally, there are other limitations as well. Wireless sensor networks are more prone to different types of contradict ability unpredictable behavior such as reflection, scattering, fading etcetera which basically 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.

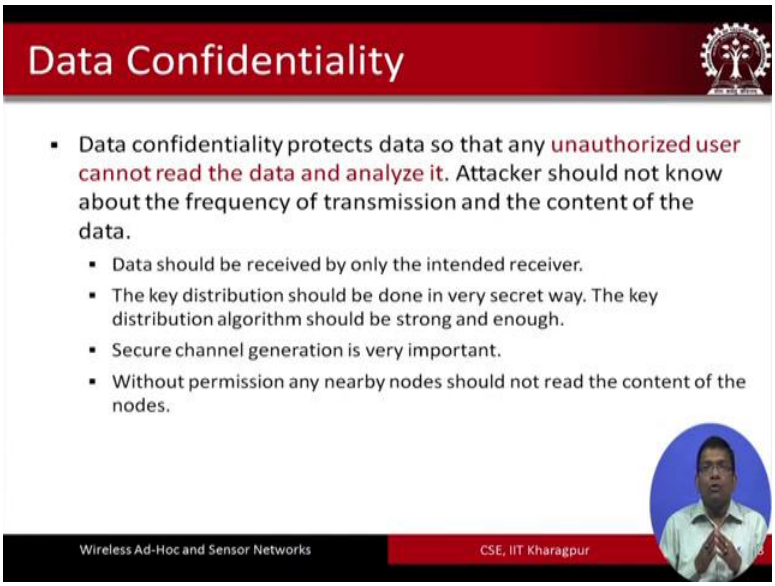
And the probability of attacks due to these basically increases even the physical attack can also happen; that means, the nodes physical can be compromised right. So, they can be removed they can be in a tempered etcetera. So, and because they are remotely deployed they are hard to detect you know this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



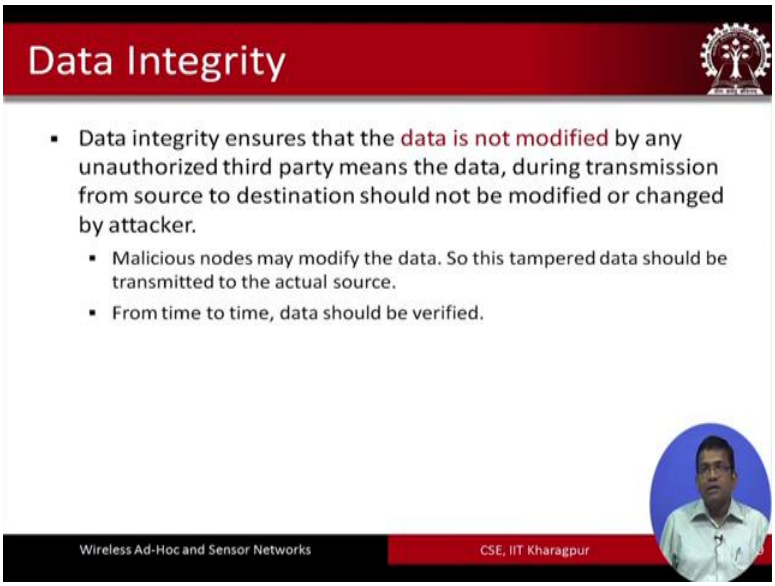
Now I am going to now go through some of the security requirements in wireless sensor networks. So, these are the main requirements one is confidentiality integrity self organization newness of data authentication time synchronization secure localization and availability. So, briefly I am going to touch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

(Refer Slide Time: 10:45)



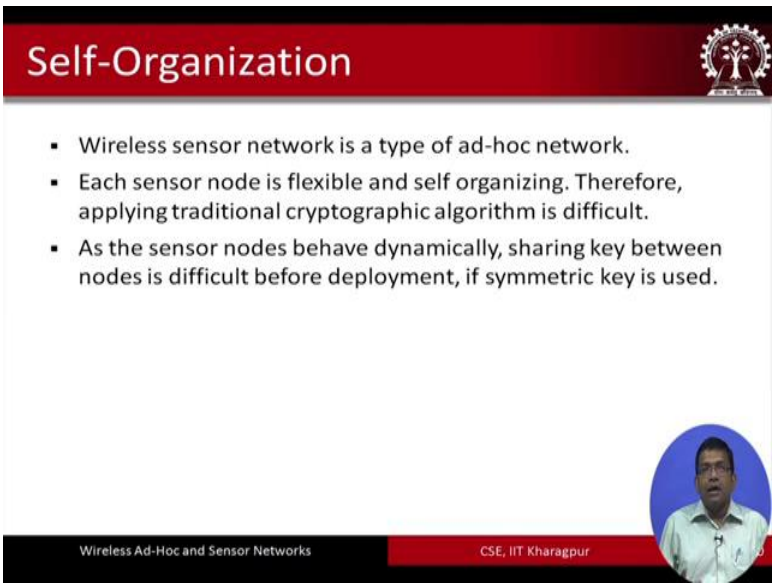
So, when we are talking about confidentiality. So, confidentiality as we know a means that whoever is authorized for the data that entity should only get access to the data and others should not you know the data should be confidential and should not be accessible to any other entity who are not authorized 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)



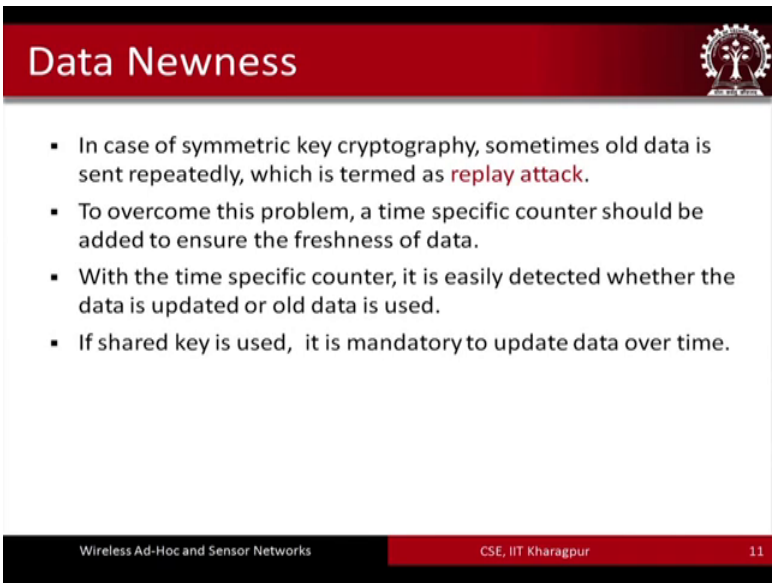
So, that is data confidentiality the next one is data integrity. So, integrity again the dictionary meaning of it applies over here as well. So, the data that is obtained by the sensor nodes and is in transit over the network should not be modified by any third party by any means. So, the data is being 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)



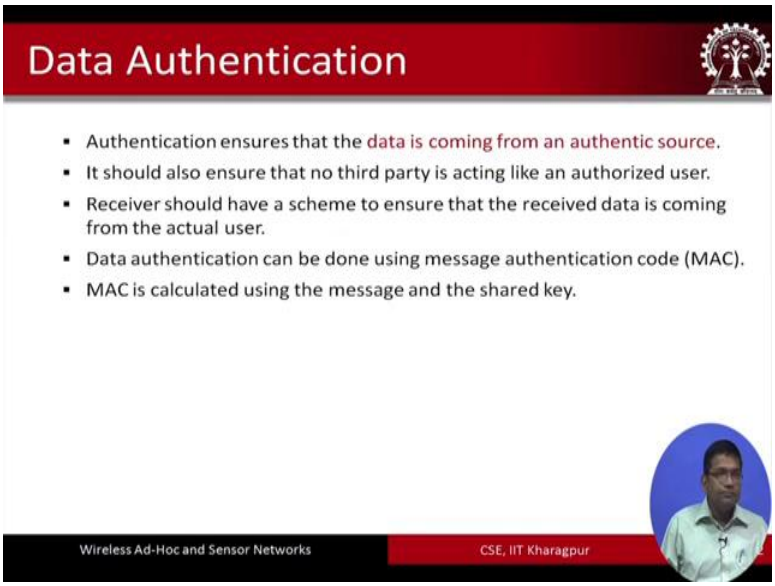
Third is self organization self organization in ad hoc network sensor networks is very important. So, you have we have a typically dynamic kind of topology and many things are dynamic by virtue of self organization because of which the application of the traditional cryptographic algorithms is difficult. 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)



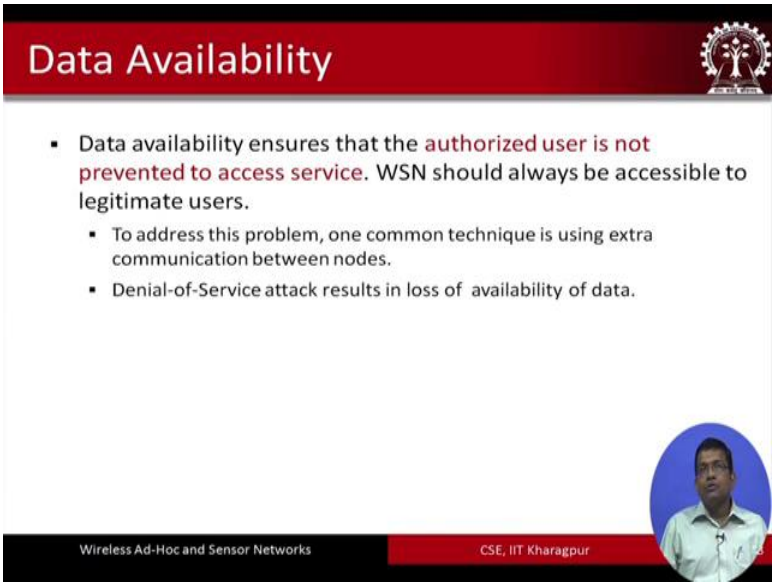
Data newness; that means, that the old data should not be sent repeatedly. So, basically you know if that is violated what we have is something called the replay attack. The replay attack as we will see later also basically the same old data you know periodically it is sent over and over again. So, to 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)



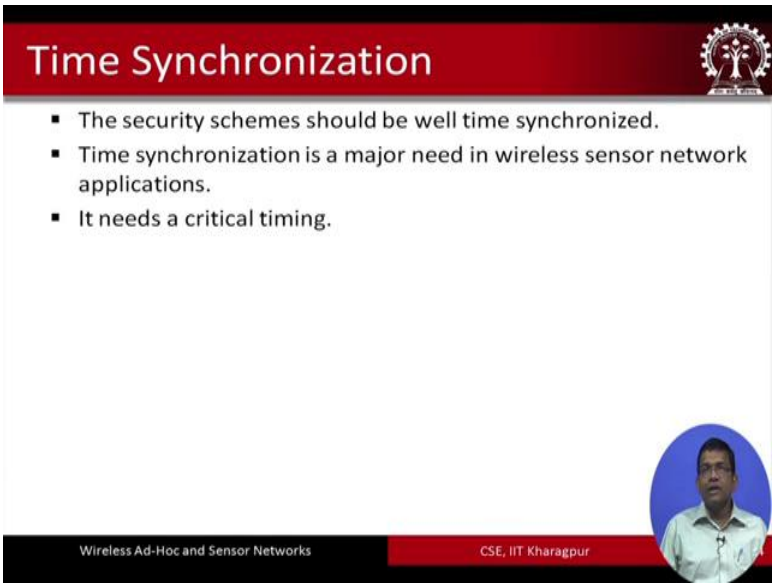
Authentication data authentication. So, the data that is coming it should be from an authentic source some you know it should not happen that anybody can throw in pump in data into the network right. So, it should be coming from an authentic source. Otherwise what is going to happen is any malicious 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)



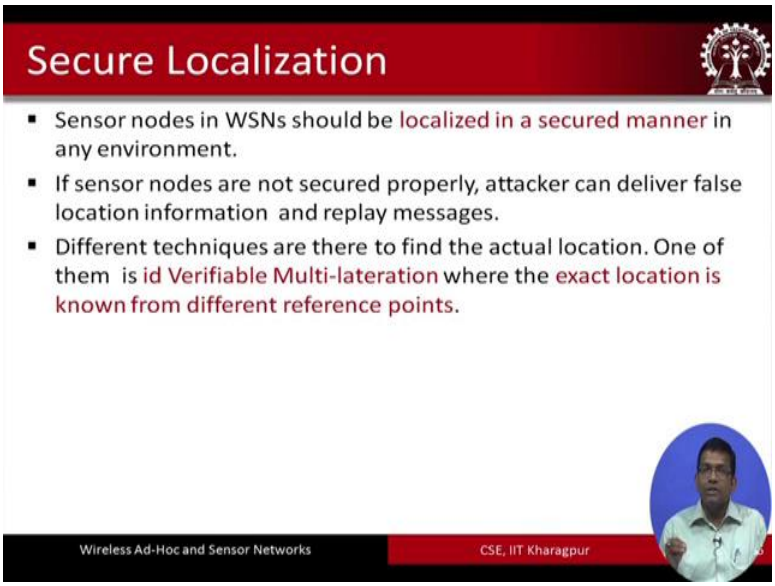
Data availability basically you know it ensures that the authorized user is not prevented to access the service, authorized user is not prevented to access the service. So, sensor networks should always be accessible to the legitimate users.

(Refer Slide Time: 15:04)



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.

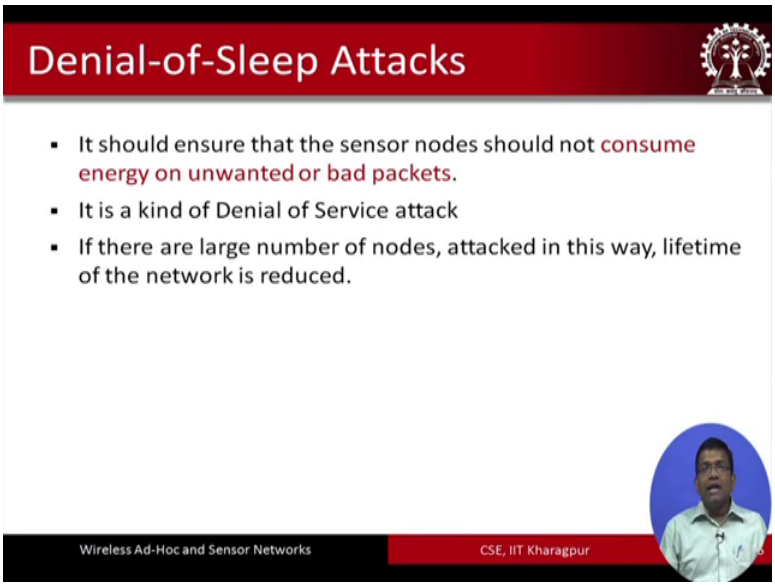
(Refer Slide Time: 15:36)



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 date 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.

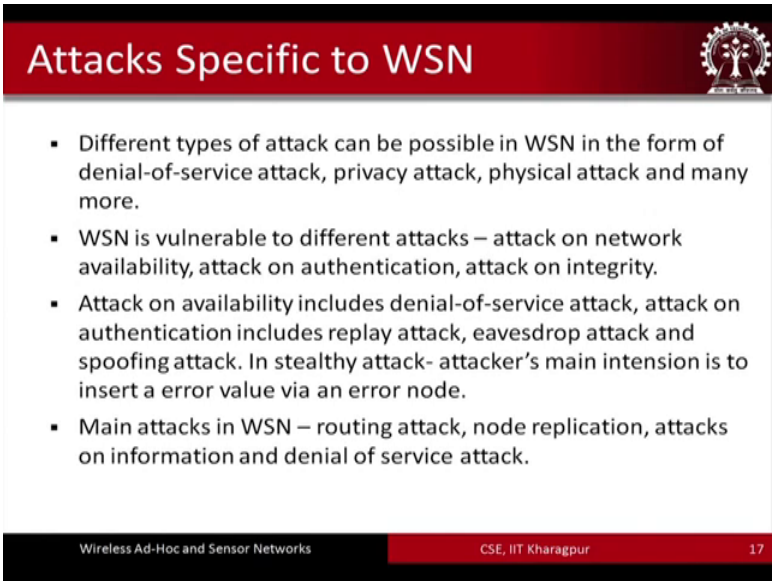
Now the problem is that if that is compromised if that is compromised; that means, the actual location of the sensor node is not given along with the data maybe you know some other location is given or something like that that would lead to problems because you know. So, the correct location of the data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

(Refer Slide Time: 16:33)



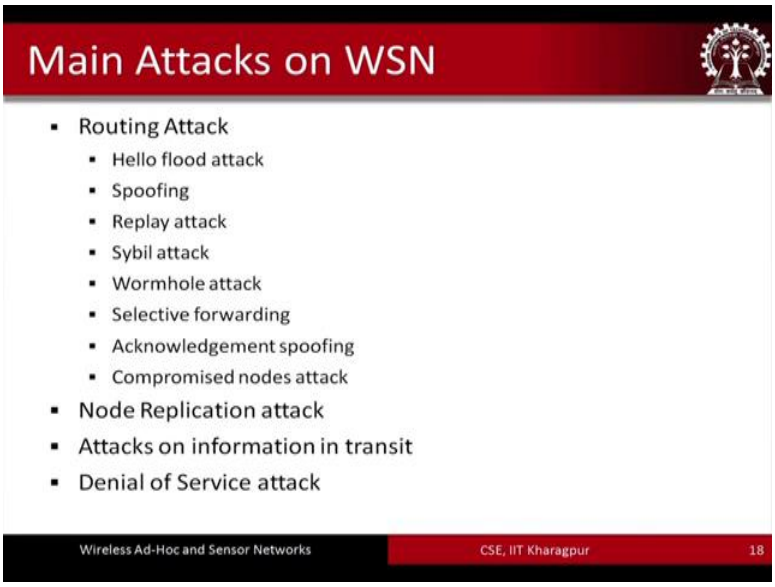
Now, denial of sleep attacks is another typical aspect of wireless sensor network security in wireless sensor networks. So, basically what happens is this is the kind of denial of service attack where lot of unwanted or garbage packets could be sent into the network. So, these nodes they are always going 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)



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.

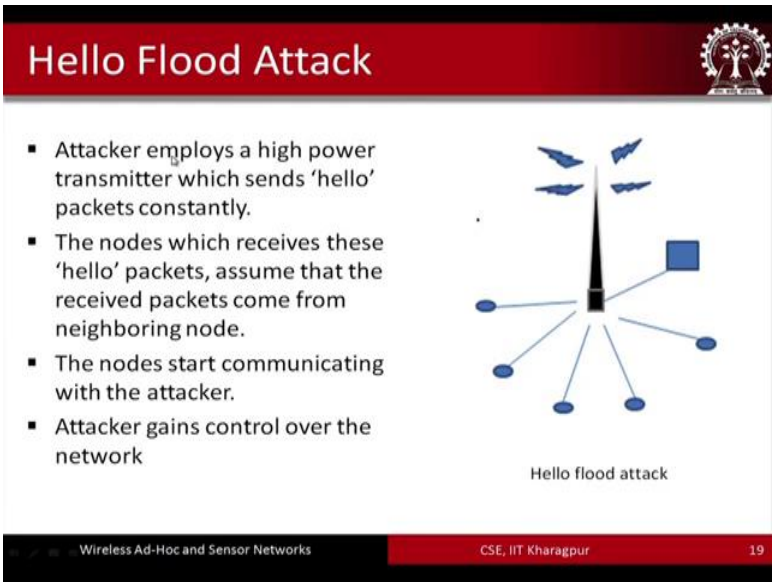
(Refer Slide Time: 17:41)



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.

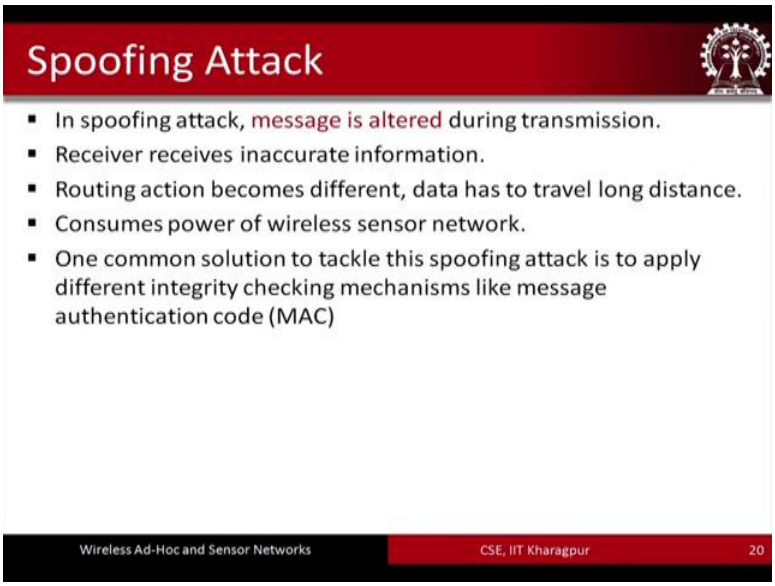
Then we have the node replication attacks on information that is in transit and we have denial of service attacks. So, these are the different types of attacks that are possible different categories of attacks that are possible on any wireless sensor network.

(Refer Slide Time: 18:24)



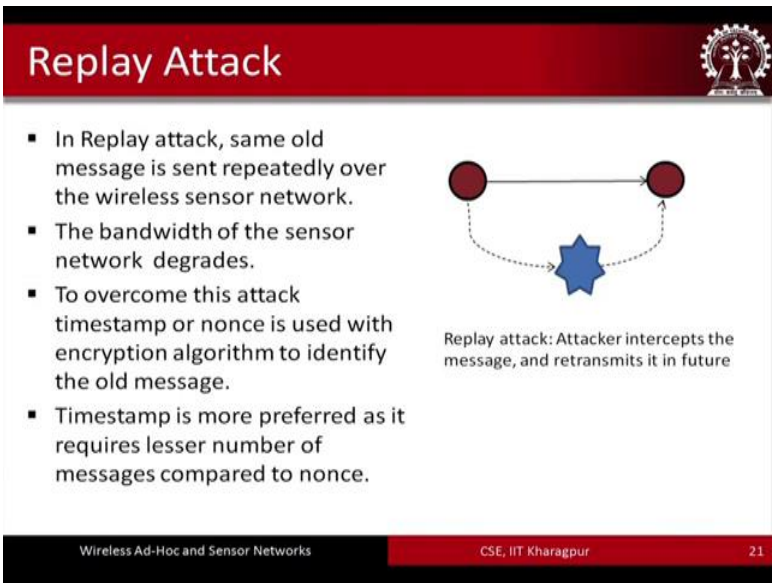
Hello flood attack is like this. So, what we have is basically a high power transmitter like this you know, it is a high power transmitter which basically periodically got periodically when it is basically successively it will send the hello packets at a very high power and the intermediate nodes. Sorry 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 fulled 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. 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.

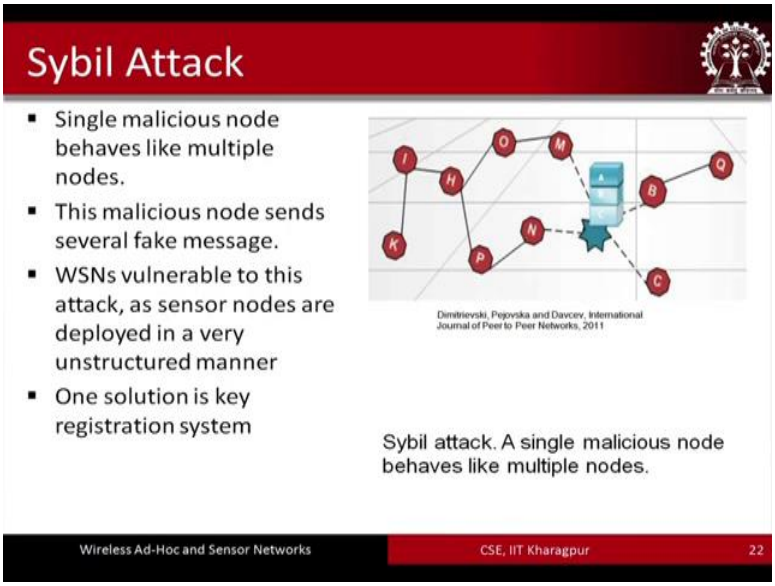
(Refer Slide Time: 19:55)



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

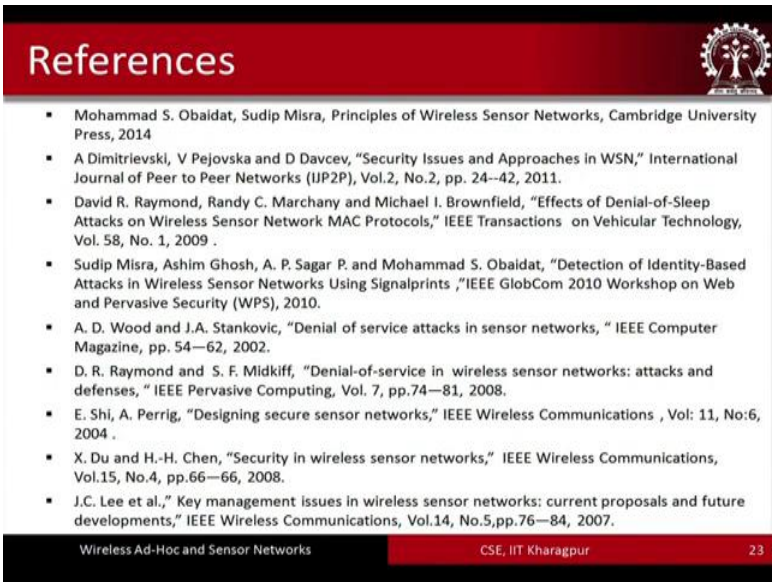
the message and retransmit is it in the future. So, what it will do this attacker will come in between these 2 nodes and it will get access to this message that is that has been sent it will intercept it, and it will it will retransmit the data successively in the future. So, this is called the replay 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. 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)



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.