4.6 Possible Solutions for Jamming

- Jamming in wireless networks is defined as the disruption of existing wireless communications by decreasing the signal-to-noise ratio at receiver sides through the transmission of interfering wireless signals.
- Jamming can be done at different levels, from hindering transmission to distorting packets in legitimate communications.
- Jamming makes use of intentional radio interferences to harm wireless communications by keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupted signal received at receivers. Jamming mostly targets attacks at the physical layer but sometimes cross- layer attacks are possible too.

4.6 Types of Jammers

- Jammers are malicious wireless nodes planted by an attacker to cause intentional interference in a wireless network. Depending upon the attack strategy, a jammer can either have the same or different capabilities from legitimate nodes in the network which they are attacking.
- The jamming effect of a jammer depends on its radio transmitter power, location and influence on the network or the targeted node. A jammer may jams a network in various ways to make the jamming as effective as possible. Basically, a jammer can be either **Proactive** and **Reactive**

Proactive jammer

- Proactive jammer transmits jamming (interfering) signals whether or not there is data communication in a network. It sends packets or random bits on the channel it is operating on, putting all the others nodes on that channel in non-operating modes. However, it does not switch channels and operates on only one channel until its energy is exhausted. There are three basic types of proactive jammers: constant, deceptive and random
- **Constant jammer,** emits continuous, random bits without following the CSMA protocol. A constant jammer prevents legitimate nodes from communicating with each other by causing the wireless media to be constantly busy. This type of attack is energy inefficient and easy to detect but is very easy to launch and can damage network communications.
- **Deceptive jammer,** sends a constant stream of bytes into the network to make it look like legitimate traffic.
- **Random jammer,** intermittently transmits either random bits or regular packets into networks. It continuously switches between two states: sleep phase and jamming phase. It sleeps for a certain time of period and then becomes active for jamming before returning back to a sleep state.

Reactive Jammer

- Reactive jammer starts jamming only when it observes a network activity occurs on a certain channel. As a result, a reactive jammer targets on compromising the reception of a message. It can disrupt both small and large sized packets. Since it has to constantly

monitor the network, reactive jammer is less energy efficient than random jammer. However, it is much more difficult to detect a reactive jammer than a proactive jammer because the Packet Delivery Ratio (PDR) cannot be determined accurately in practice. There are two different ways to implement a reactivejammer

- **Reactive RTS/CTS jammer**, jams the network when it senses a request-to-send (RTS) message is being transmitted from a sender. It starts jamming the channel as soon as the RTS is sent. In this way, the receiver will not send back clear-to-send (CTS) reply because the RTS packet sent from a sender is distorted. Then, the sender will not send data because it believes the receiver is busy with another on-going transmission.
- **Reactive Data/ACK jammer**, jams the network by corrupting the transmissions of data or acknowledgement (ACK) packets. This type of jammer can corrupt data packets, or it waits until the data packets reach the receiver and then corrupts the ACK packets. The corruptions of both data packets and ACK messages will lead to re- transmissions at the sender end.

4.6.1 Countermeasures for Proactive Jammer

- In proactive jamming, the jammer chokes the bandwidth so that a transmitter is unable to transmit. Therefore, carrier-sensing thresholds can be used to detect such type of jammers. When jamming is detected, nodes in the network can map the jammed area and re-route traffic, switch channel, or perform spatial retreat to counteract this jamming act.

4.6.2 Countermeasures for Reactive Jammer

- Reactive Jamming detection using BER. It is used to detect jamming using the bit error rate (BER) for reactive jammers that keep the received signal strength (RSS) low while introducing disruption in a packet.
- By looking at the RSS of each bit during the reception, it identifies the cause of bit errors for individual packet using predetermined knowledge, error correcting codes (ECC), or wired node chain systems. If the error is due to weak signal, the RSS should be low. .
- If the RSS value is high for a bit error, there are external interference or jamming. Assuming nodes can assess the expected local interference, the sequential jamming probability test calculates the marginal likelihood of errors due to 10 unintentional collisions. If this value is less than the log of the ratio of targeted probability for a missed alarm to the targeted probability, then there is jamming and an alarm is raised.
- If the marginal likelihood is less than the ratio, there is no jamming and the sequence is reset. There is also a possibility that no conclusion is made until there are more conclusive evidences for jamming.

4.7 Tampering Attack and its Countermeasures

- An attacker can damage or replace sensor and computation hardware and the program codes or remove sensitive materials like cryptographic keys to allow unrestricted access to higher levels of communication (Figure4.1). Thereby these tampering nodes interfere in the physical access of sensor nodes.

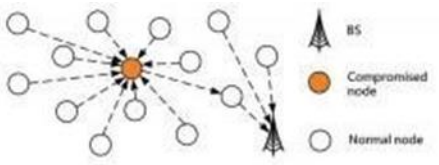

Figure 4.1 Tampering Attack

Countermeasures

- Some attacks in the physical layer are quite hard to cope with. For example, after sensors are deployed in the field, it is difficult or infeasible to prevent every single sensor from device tampering. Therefore, although there are some mechanisms that attempt to reduce the occurrences of attacks, more of them focus on protecting information from divulgence.

Access Restriction

- Obviously, restricting adversaries from physically accessing or getting close to sensors is effective on tampering attacks. It is good to have such restrictions if we can, but unfortunately, they are either difficult or infeasible in most cases. Therefore, we usually have to fall back on another type of restrictions: communication media access restriction.
- A few techniques exist nowadays that prevent attackers from accessing the wireless medium in use, including sleeping/hibernating and spread spectrum communication.
- This technique uses either analog schemes where the frequency variation is continuous, or digital schemes (e.g. frequency hopping) where the frequency variation is abrupt.
- By this way, attackers cannot easily locate the communication channel, and are thus restrained from attacking. The spread spectrum communications are not yet feasible for WSNs that are usually constrained in resources. Directional antenna is another technique for access restriction. By confining the directions of the signal propagation, it reduces the chances of adversaries accessing the communication channel.

Encryption

- In general, cryptography is the all-purpose solution to achieve security goals in WSNs. To protect data confidentiality, cryptography is indispensable.
- Cryptography can be applied to the data stored on sensors. Once data are encrypted, even if the sensors are captured, it is difficult for the adversaries to obtain useful information. A more costly encryption can yield higher strength, but it also drains the limited precious energy faster and needs more memory. More often, cryptography is applied to the data in transmission.
- There are basically two categories of cryptographic mechanisms: asymmetric and symmetric. In asymmetric mechanisms (e.g. RSA), the keys used for encryption and decryption are different, allowing for easier key distribution. It usually requires a third trusted party called Certificate Authority (CA) to distribute and check certificates so that the identity of the users using a certain key can be verified. However, due to the lack of a priori trust relationship and infrastructure support, it is infeasible to have CAs in WSNs.
- Furthermore, asymmetric cryptography usually consumes more resources such as

computation and memory.

- In comparison, symmetric mechanisms are more economical in terms of resource consumption. As long as two nodes share a key, they can use this key to encrypt and decrypt data and securely communicate with each other.