4.4 Network Security Attacks

- Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, WSNs have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

- For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Attackers may device different types of security attacks to make the WSN system unstable.

4.4.1 Based On the Capability of the Attacker Outsider versus insider (node compromise) attacks

- Outside attacks are defined as attacks from nodes, which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.

Passive versus Active attacks

- Passive attacks include eavesdropping on or monitoring packets exchanged within a WSN; active attacks involve some modifications of the data steam or the creation of a false stream.

Mote-class versus laptop-class attacks

- In mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities to the network nodes; in laptop-class attacks, an adversary can use more powerful devices (e.g., a laptop) to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes.

4.4.2 Attacks on Information in Transit

- In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be attacked to provide wrong information to the base stations or sinks. The attacks are:

  - **Interruption:** Communication link in sensor networks becomes lost or unavailable. This operation threatens service availability. The main purpose is to launch denial-of service (DoS) attacks. From the layer-specific perspective, this is aimed at all layers.

  - **Interception:** Sensor network has been compromised by an adversary where the attacker gains unauthorized access to sensor node or data in it. Example of this type of attacks is node capture attacks. This threatens message confidentiality. The main purpose is to eavesdrop on the information carried in the messages.

- **Modification:** Unauthorized party not only accesses the data but also tampers with it. This threatens message integrity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer, because of the richer semantics of these layers.

- **Fabrication:** An adversary injects false data and compromises the trustworthiness of information. This threatens message authenticity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This operation can also facilitate DOS attacks, by flooding the network.

- **Replaying existing messages:** This operation threatens message freshness. The main purpose of this operation is to confuse or mislead the parties involved in the communication protocol that is not time- aware.

4.4.3 Host Based Vs Network Based

4.4.3.1 Host-based attacks: It is further broken down in to User compromise: This involves compromising the users of a WSN, e.g. by cheating the users into revealing information such as passwords or keys about the sensor nodes. Hardware compromise: This involves tampering with the hardware to extract the program code, data and keys stored within a sensor node. The attacker might also attempt to load its program in the compromised node. Software compromise: This involves breaking the software running on the sensor nodes. Chances are the operating system and/or the applications running in a sensor node are vulnerable to popular exploits such as buffer overflows.

4.4.3.2Network-based attacks: It has two orthogonal perspectives layer-specific compromises, and protocol-specific compromises. This includes all the attacks on information in transit. Apart from that it also includes Deviating from protocol: When the attacker is, or becomes an insider of the network, and the attacker'spurpose is not to threaten the service availability, message confidentiality, integrity and authenticity of the network, but to gain an unfair advantage for itself in the usage of the network, the attacker manifests selfish behaviours, behaviours that deviate from the intended functioning of the protocol.

4.4 Layer wise Attacks in Wireless Sensor Networks

- This section discusses about the WSN layer wise attack.

4.4.3 Physical Layer Attacks

4.5.1.1 Jamming

- This is one of the Denial of Service Attacks in which the adversary attempts to disrupt the operation of the network by broadcasting a high-energy signal.

- Jamming attacks in WSNs, classifying them as constant (corrupts packets as they are transmitted), deceptive (sends a constant stream of bytes into the network to make it look like legitimate traffic), random (randomly alternates between sleep and jamming to save energy), and reactive (transmits a jam signal when it senses traffic).

- To defense against this attack, use spread-spectrum techniques for radio communication.

Handling jamming over the MAC layer requires Admission Control Mechanisms.

4.5.1.2 Radio Interference

- Here, adversary either produces large amounts of interference intermittently or persistently. To handle this issue, use of symmetric key algorithms in which the disclosure of the keys is delayed by some time interval.

4.5.1.3 Tampering or Destruction

- Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node.
- One defense to this attack involves tamper-proofing the node's physical package.
- Self-Destruction (tamper-proofing packages) – whenever somebody accesses the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information.

4.1.1 Data Link Layer Attacks

4.5.2.1 Continuous Channel Access (Exhaustion)

- A malicious node disrupts the Media Access Control protocol, by continuously requesting or transmitting over the channel. This eventually leads a starvation for other nodes in the network with respect to channel access.
- One of the countermeasures to such an attack is Rate Limiting to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions.
- A second technique is to use time division multiplexing where each node is allotted a time slot in which it can transmit.

4.5.2.2 Collision

- This is very much similar to the continuous channel attack. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid. A typical defense against collisions is the use of error-correcting codes.

4.5.2.3 Unfairness

- Repeated application of these exhaustion or collision based MAC layer attacks or an abusive use of cooperative MAC layer priority mechanisms, can lead into unfairness.
- This kind of attack is a partial DOS attack, but results in marginal performance degradation.
- One major defensive measure against such attacks is the usage of small frames, so that any individual node seizes the channel for a smaller duration only.

4.5.2.4 Interrogation

- Exploits the two-way request-to-send/clear-to-send (RTS/CTS) handshake that many MAC protocols use to mitigate the hidden-node problem.
- An attacker can exhaust a node's resources by repeatedly sending RTS messages to elicit CTS responses from a targeted neighbour node.
- To put a defense against such type of attacks a node can limit itself in accepting connections from same identity or use Anti replay protection and strong link-layer authentication.

4.5.2.5 Sybil Attack

- In this attack, a single node presents multiple identities to all other nodes in the WSN. This may mislead other nodes, and hence routes believed to be disjoint with respect to node can have the same adversary node.
- A countermeasure to Sybil Attack is by using a unique shared symmetric key for each node with the base station.

4.1.2 Network Layer Attacks

4.5.3.1 Sinkhole Attack

- Sinkhole attacks normally occur when compromised node send fake routing information to other nodes in the network with aim of attracting as many traffic as possible.

4.5.3.2 Hello Flood

- This attack exploits Hello packets that are required in many protocols to announce nodes to their neighbors. A node receiving such packets may assume that it is in radio range of the sender.
- A laptop class adversary can send this kind of packet to all sensor nodes in the network so that they believe the compromised node belongs to their neighbors. This causes a large number of nodes sending packets to this imaginary neighbour and thus into oblivion. Authentication is the key solution to such attacks. Such attacks can easily be avoided by verify bi-directionality of a link before taking action based on the information received over that link.

4.5.3.3 Node Capture

- Node capture attack is a serious attack through which an intruder can performs various operations on the network and can easily compromise the entire network. It is one of the hazardous attack in WSNs.
- A single node capture is sufficient for an attacker to take over the entire network.

4.5.3.4 Selective Forwarding/ Black Hole Attack

- In Black Hole attack, a malicious node falsely advertises good paths (e.g., shortest path or most stable path) to the destination node during the path-finding process (in on- demand

routing protocols) or in the route update messages (in table-driven routing protocols). The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node concerned. Malicious or attacking nodes can however refuse to route certain messages and drop them. If they drop all the packets through them, then it is called a Black Hole Attack.

- However if they selectively forward the packets, then it is called selective forwarding.
- To overcome this, Multi path routing can be used in combination with random selection of paths to destination, or braided paths can be used which represent paths which have no common link or which do not have two consecutive common nodes, or use implicit acknowledgments, which ensure that packets are forwarded as they were sent.

4.5.3.5 Wormhole Attacks

- An adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. This is usually done with the coordination of two adversary nodes, where the nodes try to understate their distance from each other, by broadcasting packets along an out-of-bound channel available only to the attacker.
- To overcome this, the traffic is routed to the base station along a path, which is always geographically shortest or use very tight time synchronization among the nodes, which is infeasible in practical environments.

4.5.3.6 Spoofed, Altered, or Replayed Routing Information

- The most direct attack against a routing protocol in any network is to target therouting information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency.
- A countermeasure against spoofing and alteration is to append a message authentication code (MAC) after the message. Efficient encryption and authentication techniques can defend spoofing attacks.

4.5.3.7 Misdirection

- This is a more active attack in which a malicious node present in the routing path can send the packets in wrong direction through which the destination is unreachable. In place of sending the packets in correct direction the attacker misdirects those and that too towards one node and thus this node may be victimized.

4.5.3.8 Homing

- In a homing attack, the attacker looks at network traffic to deduce the geographic location of critical nodes, such as cluster heads or neighbors of the base station. The attacker can then physically disable these nodes. This leads to another type of black hole attack.

4.1.3 Transport layer Attacks

4.5.4.1 Flooding

- Sometime, the malicious node can cause immense traffic of useless messages on the network. This is known as the flooding. Sometimes, malicious nodes replay some actual broadcast messages, and hence generating useless traffic on the network. This can cause congestion, and may eventually lead to the exhaustion of complete nodes. This is a form of Denial of Service attack.

4.5.4.2 De-synchronization Attacks

- In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence, these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information.

4.1.4 Application layer Attacks

4.5.5.1 Overwhelm Attack

- An attacker might attempt to overwhelm network nodes with sensor stimuli, causing the network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.

4.5.5.2 Path-based DOS Attack

- It involves injecting spurious or replayed packets into the network at leaf nodes. This attack can starve the network of legitimate traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station.

4.5.5.3 Deluge (reprogram) Attack

- Network programming system let you remotely reprogram nodes in deployed networks. If the reprogramming process isn't secure, an intruder can hijack this process and take control of large portions of a network. It can use authentication streams to secure the reprogramming process.