4.1 Introduction: Security in Wireless Sensor Networks

- WSN is a special type of network. The sensor networks, based on an inherently broadcast wireless medium, are vulnerable to a variety of attacks.
- Security is of prime importance in sensor networks because the absence of central authority, random deployment of nodes in the network and nodes assume a large amount of trust among themselves during data aggregation and event detection.
- From a set of sensor nodes in a given locality, only one final aggregated message may be sent to the BS, so it is necessary to ensure that communication links are secure for data exchange.
- Cryptographic solutions based on symmetric or public key cryptography are not suitable for sensor networks, due to the high processing requirements of the algorithms. So, need special type of protocol to ensure the security in sensor networks.

4.2 Network Security Requirements

- The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehaviour of nodes.
- The most important security requirements in WSN are listed below:
  - **Data Confidentiality**
  - **Authentication**
  - **Data Integrity**
  - **Data Freshness**
  - **Availability**
  - **Self-Organization**
  - **Time synchronization**
  - **Source Localization**
  - **Scalability**

Data Confidentiality

- Data Confidentiality requirement is required to ensure that sensitive information is well protected and not revealed to unauthorized third parties.
- The confidentiality objective helps to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication.

- By eavesdropping, the adversary could overhear critical information such as sensing data and routing information. Based on the sensitivity of the data stolen, an adversary may cause severe damage since he can use the sensing data for many illegal purposes

i.e. sabotage, blackmail.

- Furthermore, by stealing routing information the adversary could introduce his own malicious nodes into the network in an attempt to overhear the entire communication.

- If we consider eavesdropping to be a network level threat, then a local level threat could be a compromised node that an adversary has in his possession. Compromised nodes are a big threat to confidentiality objective since the adversary could steal critical data stored on nodes such as cryptographic keys that are used to encrypt the communication.

Authentication

- It ensures that the communicating node is the one that it claims to be. An adversary can not only modify data packets but also can change a packet stream by injecting fabricated packets.

- It is, therefore, essential for a receiver to have a mechanism to verify that the received packets have indeed come from the actual sender node.

- In case of communication between two nodes, data authentication can be achieved through a message authentication code (MAC) computed from the shared secret key.

Data Integrity

- The mechanism should ensure that no message can be altered by an entity as it traverses from the sender to the recipient.

Data Freshness

- It implies that the data is recent and ensures that no adversary can replay old messages.

- This requirement is especially important when the WSN nodes use shared-keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN.

- A nonce or time-specific counter may be added to each packet to check the freshness of the packet.

Availability

- Availability ensures that services and information can be accessed at the time that they are required.

- In sensor networks, there are many risks that could result in loss of availability such as

sensor node capturing and denial of service attacks.

- Lack of availability may affect the operation of many critical real-time applications like those in the healthcare sector that require a 24/7 operation that could even result in the loss of life.
- Therefore, it is critical to ensure resilience to attacks targeting the availability of the system and find ways to fill in the gap created by the capturing or disablement of a specific node by assigning its duties to some other nodes in the network.

Self-Organization

- In WSN no fixed infrastructure exists, hence, every node is independent having properties of adaptation to the different situations and maintains self-organizing and self-healing properties. This is a great challenge for security in WSN.

Time synchronization

- Most of the applications in sensor networks require time synchronization. Any security mechanism for WSN should also be time-synchronized. A collaborative WSN may require synchronization among a group of sensors.

Source Localization

- For data transmission some applications use location information of the sink node. It is important to give security to the location information.
- Non-secured data can be controlled by the malicious node by sending false signal strengths or replaying signals.

Scalability

- Hundreds of thousands of nodes are deployed in a network carrying out distributed operations. Because of this explosive proliferation of sensor nodes, scalability is becoming an important requirement in WSN.
- WSN must be scalable to provide capacity for additional nodes. New nodes inser tion and old nodes removal should be easy with no bad impact over the network operations.

4.3 Issues and Challenges in Security Provisioning

- A strong routing protocol can only protect the network from various malicious activities. Designing a strong security routing protocol for wireless sensor network is a very challenging task.
- WSN must have the richest set of different protocols to carryout application requirements; a WSN protocol must handle a hostile environment.
- Routing protocol should provide a high throughput, and a decrease packet loss ratio.

Routing algorithm should handle mobility and dynamic changing behavior in WSNs.

- Unreliable wireless media can drop packets; routing protocols should prevent packet loss. Designing a new routing protocol for WSN should consider the following security and privacy issues.

  - **Node Mobility**
  - **Coverage Problem**
  - **Shared Broadcast Radio Channel**
  - **Insecure Operational Environment**
  - **Lack of Central Authority**
  - **Lack of Association**
  - **Limited Resource Availability**
  - **Physical Vulnerability**
  - **Quality of Service**
  - **Programming Wireless Sensor Networks**

Node Mobility

- The mobility sink node is used to collect data from all sensors. A static sink node collects data from all sensors without changing its constant position. A mobile sink node has its own effects on the network, e.g., performance and dynamic change behavior. Routing protocols must provide better connectivity, an efficient energy consumption, a controlled flooding mechanism, etc.

Coverage Problem

- Coverage is an important performance metric in WSNs; it reflects how well the environment is monitored. The surrounding vicinity should be monitored all times to collect data; a dead node cannot forward any packets; consequently, it degrades network services.

Shared Broadcast Radio Channel

- Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in wireless sensor networks is broadcast in nature and is shared by all nodes in the network.

- Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

Insecure Operational Environment

- The operating environments where wireless sensor networks are used may not always be secure.
- One important application of such networks is in battlefields. In such applications, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

Lack of Central Authority

- In wired networks and infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points (such as routers, base stations, and access points) and implement security mechanisms at such points. Since wireless networks do not have any such central points, these mechanisms cannot be applied in wireless sensor networks.

Lack of Association

- Since these networks are dynamic in nature, a node can join or leave the network at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join into the network quite easily and carry out his/her attacks.

Limited Resource Availability

- Resources such as bandwidth, battery power, and computational power are scarce in wireless sensor networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

Physical vulnerability

- Nodes in these networks are usually compact and hand-held in nature. They could get damaged easily and are also vulnerable to theft.

Quality of Service

- QoS is the function of its application. The proper congestion control provides better QoS. In WSNs, there is a minimum chance of congestion outside the base station area. Congestion near the base station results into: channel occupancy, buffer overflow, packet collision, channel contention, high data rate, and minimum node's life.
- For better services, minimum congestion in the network is necessary. Congestion avoidance ensures high throughput, better link utilization, minimum delay, energy efficiency, and minimum data rate error. Control packets are used to prevent congestion.

Programming Wireless Sensor Networks

- Programming a large network of highly resource-constraint devices that are self-

organized and globally consistent, with a robust behavior and a dynamically changing environment, is a big challenge.

➢