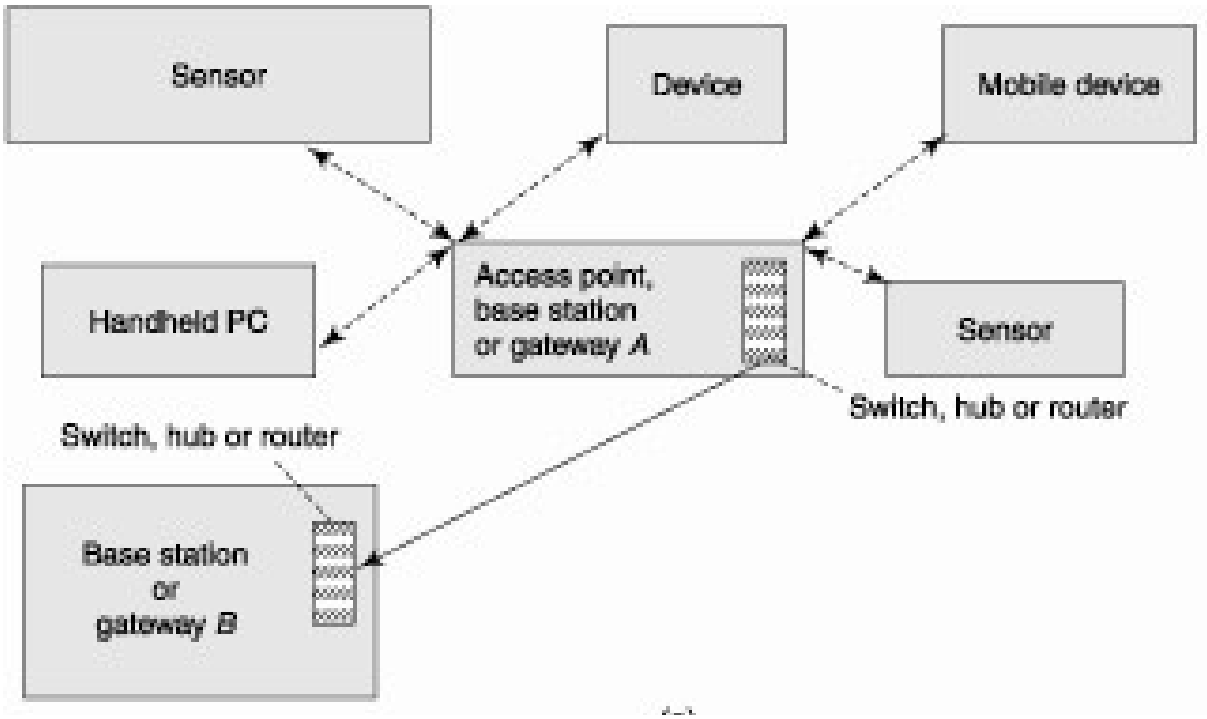
UNIT-4

Fixed infrastructure network:

- Switches, hubs, or routers locations fixed
- Networking using switches, hubs, routers, access-points, base stations, or gateways networked.
- To connect to and access the network a mobile device or wireless sensor has to be moved in the vicinity (connectivity range) of an access-point
- Example─ a cellular network



- Each mobile device or sensor connects to an access-point, base station, or gateway with a switch, hub, or router *A*

A Switch in fixed infrastructure

- Provides connectivity between the two, a hub functions as a central switching exchange
- **A router in fixed infrastructure**
- Provide two or more paths to route a message or packet so that the available path can be used at an instant
- They function as the nodes of the network

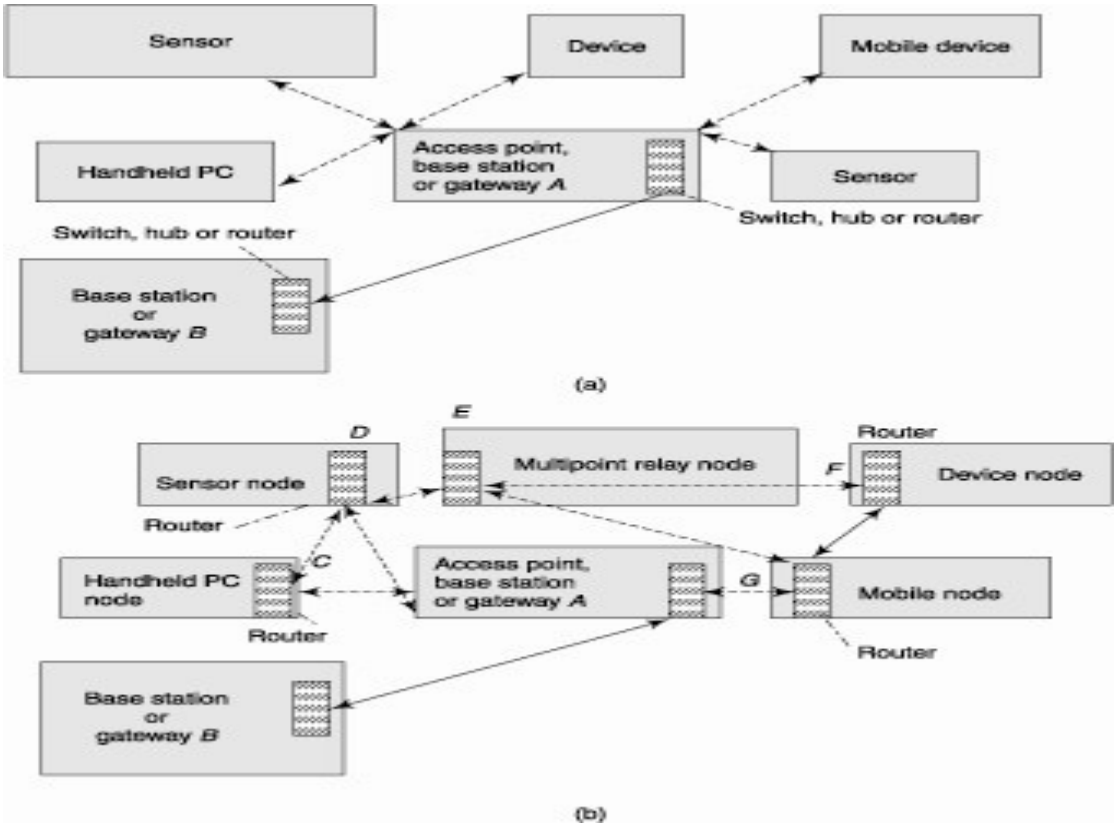
- A mobile device or sensor has to acquire an access-point or node of the fixed infrastructure network before being able to connect to another

Problem with fixed infrastructure network:

- Disconnection from the network and thus unable to communicate through the network when a wireless sensor or mobile device moves out of the range of access-point, base station, or gateway having the switch or router
- Even though there may be another wireless device in its vicinity connected to network
- Network not usable in operations like disaster relief

Mobile ad-hoc network (MANET)

- A network in which the locations of the switches, hubs, or routers can be mobile
- The number of routers available at an instant can increase or decrease, and the available routing paths can change
- The mobile devices or wireless sensors as well as the access-points can have switches or routers
- **Mobile ad-hoc network (MANET) architecture**



- **MANET Organization** :
- The ad-hoc network formed by the nodes *A*, *C*, *D*, *E*, *F*, and *G*.

- Change if *D* and *E* move away from each other such that they reach out of the range of wireless coverage
- Two new ad-hoc networks will then be formed by (i) *A*, *C*, and *D* and (ii) *A*, *G*, *F*, and *E*
- The devices on two networks can still connect to each other through the common node *A*
- Each mobile device or sensor functions as a node with a switch or router
- An important characteristic of ad-hoc network architecture is that its organization can change due to movement of a device or sensor
- In other words, the ad-hoc networks are self-organizing
- The routes available to the mobile devices or wireless sensors can thus change at any time
- Depend on presence and locations of other wireless devices in their vicinity (connectivity range)
- **MANET organization** Depends upon the location of the nodes, their connectivity, their service discovery capability, and their ability to search and route messages using nearest node or nearby nodes

MANET Properties:

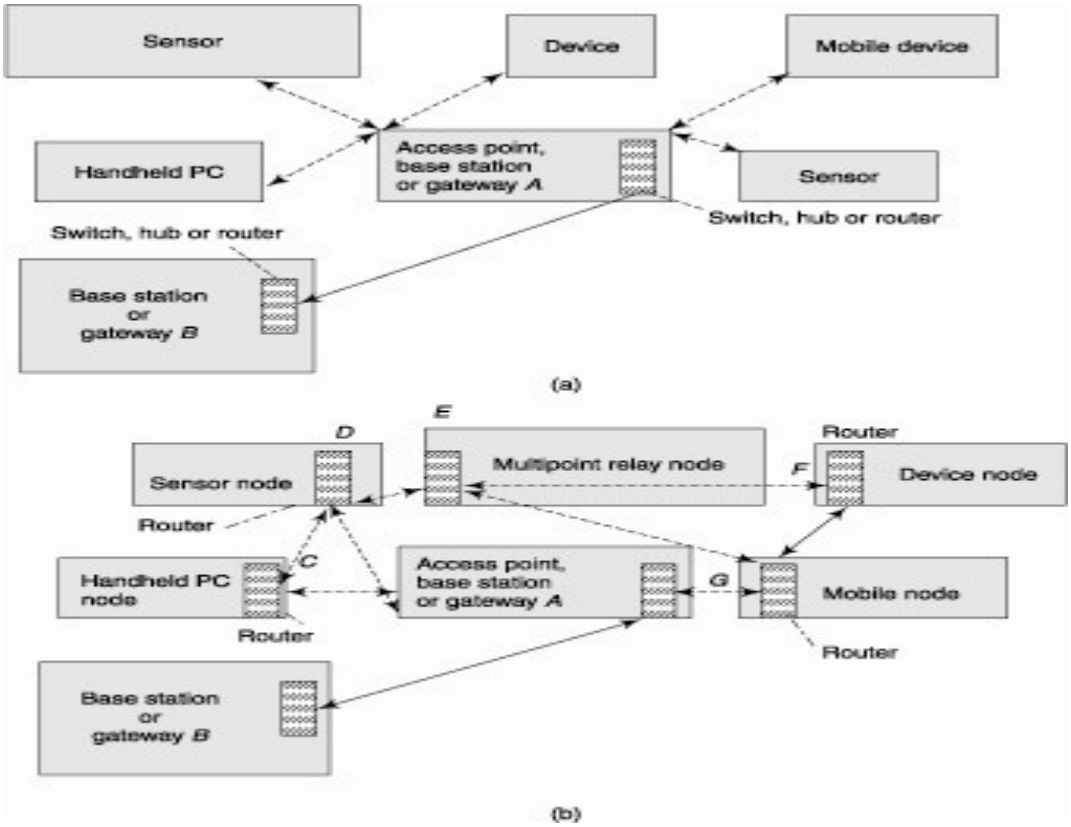
- **Neighbour discovery—** One of the important characteristics of a MANET node
- **Data routing abilities —** data can be routed from a source node to a neighbouring node
- Flexible network architecture and variable routing paths — to provide communication in case of the limited wireless connectivity range and resource constraints .
- **Flexibility—** enables fast establishment of networks
- When a new network is to be established, the only requirement is to provide a new set of nodes with limited wireless communication range
- A node has limited capability, that is, it can connect only to the nodes which are nearby and thus consumes limited power
- **Computations decentralization**– independent computational, switching (or routing), and communication capabilities
- **Limited wireless connectivity range**– require that a node should move in the vicinity of at least one nearby node within the wireless communication range, else the node should be provided with the access-point of wired communication.
- **Weak connectivity** and remote server latency
- Unreliable links to base station or gateway – failure of an intermediate node results in greater latency in communicating with the remote server
- **Resource constraints**– Limited bandwidth available between two intermediate nodes

- Node may have limited power and thus computations need to be energy-efficient
- No need of access-point
- Only selected access-points provided for connection to other networks or other MANETs
- Need to solve exposed or hidden terminal problem
- **Diversity in nodes**– iPods, palm handheld computers, Smartphones, PCs, smart labels, smart sensors, and automobile-embedded systems
- **Protocol diversity**– Nodes can use different protocols, for example, IrDA, Bluetooth, ZigBee, 802.11, GSM, or TCP/IP
- Data caching, saving, and aggregation at node

Spectrum:

- An access-point-based network
- Large number devices connects to a centralized server
- The bandwidth requirement too high
- N devices using FDMA in duplex transmission, then the required bandwidth will be 2 $\times$ N $\times f_{bw0}$, where f_{bw0} is the bandwidth allotted to one device for sending a packet to its access-point.
- **Bandwidth fixed infrastructure network**
- **Access-point** using TDMA and SDMA communication, the bandwidth (spectrum) requirement is reduced
- **Spectrum requirement at Nodes in MANET**
- Each MANET node has much smaller frequency spectrum requirements than that for a node in a fixed infrastructure network.
- A node itself ─ a router for all the packets coming from or going to the other nodes
- Node *D* at a given instant─ Can get incoming packets from *E*, *F*, *G*, and *A* and can send packets to *C* and *A* or vice versa
- Nodes are themselves mobile
- Therefore, bandwidth available to any node at any instant is variable
- MANET enables spectrum reuse
- Each wireless link provides a limited bandwidth
- MANET communication is multi-hop

- When node *D* transmits to *G*, it is through the three hops—(i) *D*—*E*, (ii) *E*—*F*, and (iii) *F*—*G*.
- Optimized to have signal strength just sufficient to carry the signal up to single hop
- Hops can therefore occur simultaneously using the same frequency band
-



Mobile Ad-hoc Network (MANET) Applications:

1. **Content Distribution and Synchronization:**

- Enterprise— A number of Bluetooth-enabled mobile handheld devices, PCs, laptops, and WiFi access-points
- MANET used for content-distribution, PIM, other information dissemination, information fusion, and file sharing in the enterprise

2. **MANET nodes in multicast tree topology**

- Disseminate data packets and form a multicasting network
- Clusters of the nodes used to give a multicast tree topology in a MANET

3. **Mesh Networking and Mobile Service Provider Network**

- Mesh-based mobile networks offer highly dynamic autonomous topology segments for the robust IP-compliant data services within the mobile wireless communication networks

- Inexpensive alternatives or improvement to infrastructure-based cellular CDMA or GSM mobile service provider

4. **Mesh Network**

- A multicast tree network differs from mesh as it provides only a single path between a sender and a receiver
- Mesh network many paths.

Mobile Ad-hoc Network (MANET) Security

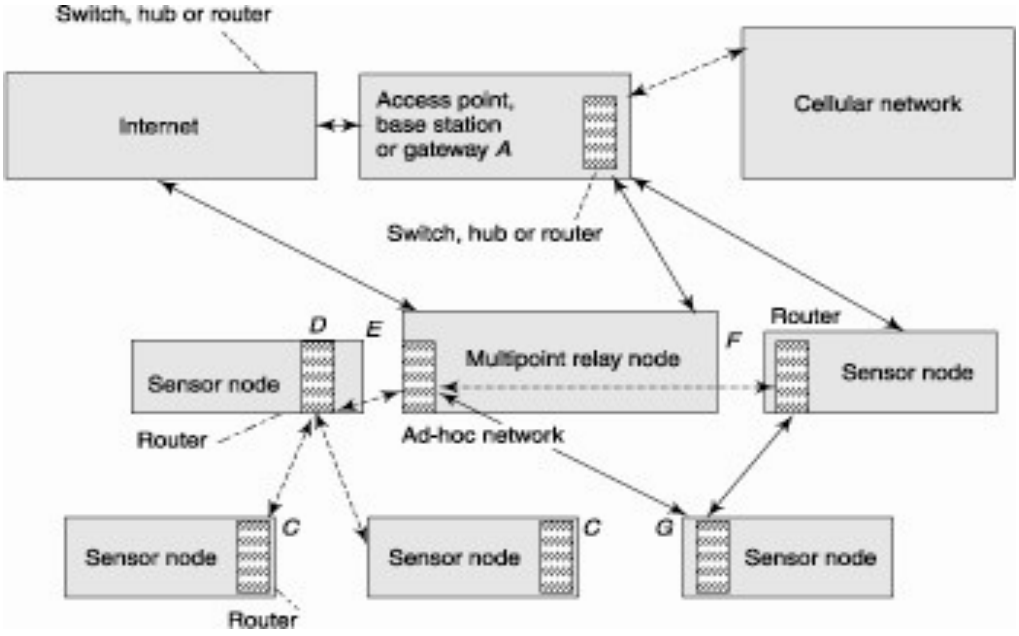
- **Confidentiality:** Only destined user must be able to read data
- Encryption of the data before transmission and deciphering it at the user end for ensuring confidentiality
- **Integrity:** Data integrity needs to be maintained or else the user receives a manipulated message
- System integrity needs to be maintained or else system can issue the message to wrong node
- **Pre-keying:** In order to decipher the encrypted messages, a key for deciphering is first exchanged between transmitter and receiver
- If a private key is used, key exchanges over wireless systems increase the risk of key trapping
- **Increased threat of eaves-dropping:**
- The probability that a MANET or sensor node transmits unsolicited messages while moving in the wireless region of two nodes is increased in ad-hoc networks
- Each node attempts to identify itself with a new node moving in its vicinity and during that process eavesdropping occurs
- **Availability:**
- Denial of service attack
- A source blocking the availability of data at the user end
- For example, the packets sent can be prevented from reaching the destination by some intermediate router misdirecting them due to the attack
- **Resource constraint:**
- Continuously irrelevant messages– exhaustion of device-memory due to caching and hoarding irrelevant data from the attacker

- Such an attack if occurs in between routers in the network, it seriously affects the whole network
- **Detection Power loss:**
- A mobile device may not detect the signals and therefore get data or message due to attack by jamming signals
- A solution is Frequency hopping of the modulation signal which has high background noise
- **Reconfiguration:**
- An attack can be on network configuration (e.g., manipulation of routing table)
- Network reconfiguration at different periods prevents such attacks
- **Spoofing (Impersonating address):**
- A node can impersonate an address in a mobile ad hoc network
- A common node to several paths can lead to choking of all routes

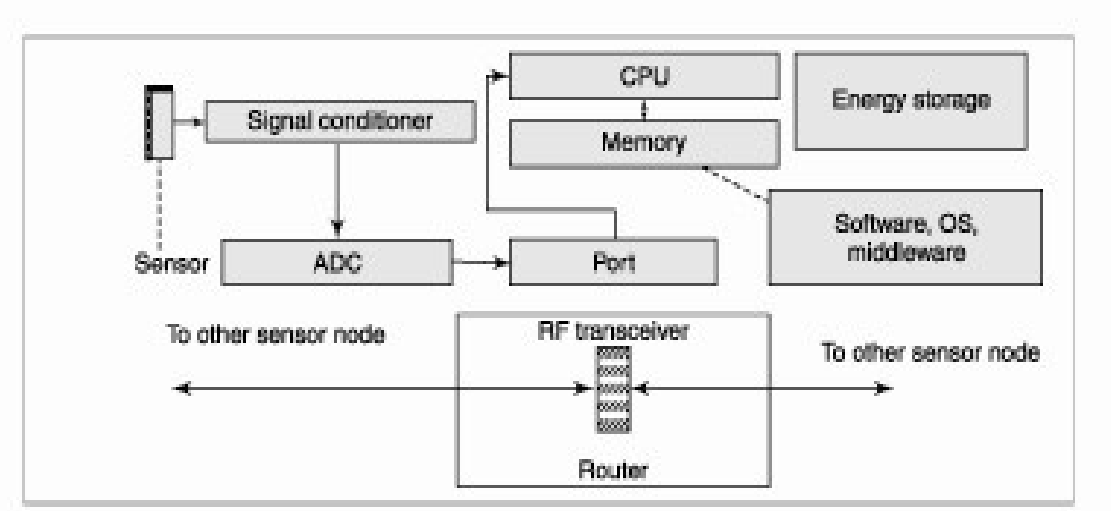
Wireless Sensor Networks

MANET Sensor nodes:

- Sophisticated hardware, software and features
- Each node has an analog sensor with signal conditioner circuit
- Sensing can be of the light level, temperature, location shift, time stamps of GPS satellites , vibration, pressure, weather data, noise levels, traffic density, and nearby passing vehicles



- The smart sensors have computational, communication, and networking capabilities but are constrained by their small size, limited energy availability, and limited memory
- Since greater computational speed needs greater energy, these sensors operate at limited computational speed
- Moreover, these have limited bandwidth



A smart wireless sensor architecture:

- Consists of an RF transceiver for communication, a *microcontroller* [CPU, memory, and ADC (analog-to-digital converter)], and an *energy source* or a power supply
- A charge pump traps the charge from the radiations (for example, from WiFi transceiver or an access-point)
- Alternatively, an energy-harvesting module can be used to trap solar radiation and store the energy
- The *RF transceiver* enables a node to receive data packets from nearby nodes and route these to next hop of the packet
- A wireless sensor node disseminates information to the network, central computer, or controller

• **Data Dissemination after Aggregation**

• Aggregation refers to the process of joining together present and previously received data packets after removing redundant or duplicate data

• **Data Dissemination after Compaction**

• Compacting means making information short without changing the meaning or context, for example, transmitting only the incremental data so that short information sent

• **Data Dissemination after Fusion**

• Fusion means formatting the information received in parts through various data packets and several types of data (or data from several sources), removing redundancy in the received data, and presenting the formatted information created from the information parts in cases when the individual records are not required and/or are not retrievable later

•