Mobile Ad-hoc Network

Dr. Tuhina Samanta

Introduction

- Mobile Adhoc Network (MANET) :-
  - Collection of wireless mobile hosts forming a temporary network,
  - No centralized administration or standard support services
- In MANETs the routers themselves may be mobile as against a mobile system which has mobile hosts and fixed routers.

Characteristics

- MANETs have no underlying information infrastructure
- Is Multihop in nature
- Every node in network acts as a router
- Nodes are free to move arbitrarily, and topology of network may be considered dynamic.

Characteristics (Contd.)

- Disadvantages :-
  1. Wireless connectivity constraints bandwidth and capacity of network.
  2. Fading, congestion, noise & interference.
  3. Limited power supply, dependence on batteries.
  4. Limited physical security as nodes are more vulnerable to eavesdropping, DOS attacks.

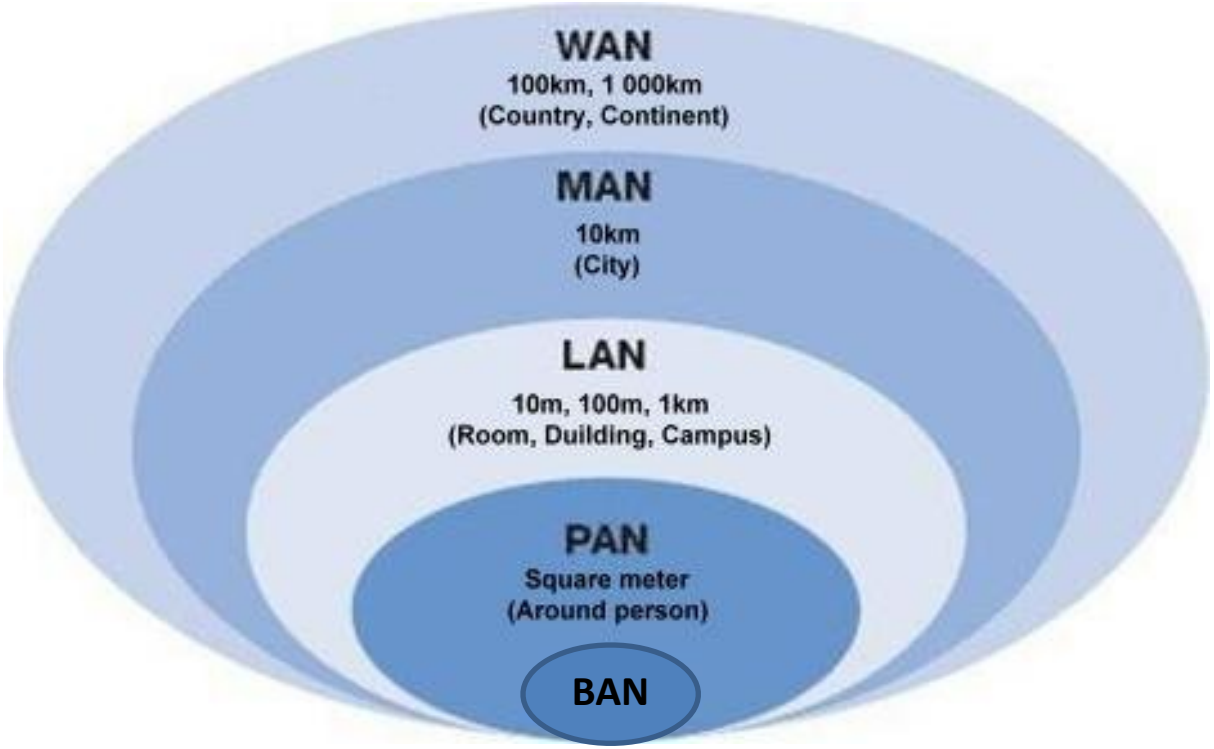
Characteristics (Contd.)

- Advantages of MANETs :-
  1. Deployment is easy and speedy.
  2. Since there is no dependence on infrastructure, network is robust and low cost.
  3. MANETs form the basis of all pervasive and ubiquitous computing.

Characteristics (Contd.)

- Applications :-
  1. In PAN using cell phones, laptops, wearable computers as they can be easily deployed.
  2. In military systems, they can be deployed on soldiers and tanks.
  3. In intelligent transport systems for providing vehicle-to-vehicle communication.
  4. Similarly in search and rescue systems, policing, fire fighting.

Classification



Categories of Ad hoc networks

Classification (contd.)

- Ad Hoc networks may be classified into three categories :-
  1. Body Area Network :
     - Can be correlated with a wearable computer, components of which are distributed on the body and BAN provides connectivity between these devices.
     - Communicating range of BAN corresponds to human body range, i.e., 1-2 meters.
     - Requirements :-
       - ability to interconnect heterogeneous devices like mobile phones, microphones, displays etc.
       - capability of auto configuration and service integration.
       - ability to connect to other MANETs for communication.

Classification (contd.)

2. Personal Area Network :
   - Network in the environment around a person. Connects mobile devices carried by users to other mobile and stationary devices.
   - Its communication range is up to 10 meters.
   - Wireless PAN makes use of 2.4 – 2.484 GHz ISM band.
   - Spread spectrum is employed at physical layer to reduce interference and utilize bandwidth properly.

Classification (contd.)

3. Wireless Local Area Network :
   - Offer greater flexibility than wired LANs.
   - Communication range is of a single building or a cluster of buildings in the range of 100-500 meters.
   - Two different approaches for implementation of LANs –
     - **Infrastructure based architecture :-**
       - » Existence of a centralized controller for each cell, often referred to as an Access Point, which itself is connected to a wired network.
     - **Ad hoc networking approach :-**
       - » Network is formed by the set of stations within the range of each other. These stations dynamically configure themselves to set up a temporary network.
       - » No fixed controller required, but one is elected from among the stations participating in the communication.

Technologies for MANETs

- Currently two main standards exist for ad hoc networks with respect to MAC and physical layers :-
  1. IEEE 802.11 :
     a. It's a standard for wireless LAN.
     b. It specifies MAC and physical layers for WLANs.
     c. Basic access methods in IEEE 802.11 MAC protocol -
        - Distribution Coordination Function (DCF) which is a CSMA/ CA MAC protocol.
        - Point Coordination Function (PCF) which operates using a polling mechanism, where a point coordinator provides transmission rights to a single station at a time.

Routing in MANETs

- MANET routing protocols expected to satisfy the following essential principles :-
  - Tolerance of unexpected network faults (e.g.. device and link failures).
  - Resilience to increasing traffic loads.
  - Minimal energy consumption (especially for small clients).

Requirements for Routing protocols

- Routing in MANETs is very different from that in wired networks because of their unique nature.
- Multiple access schemes can not be used because of the hidden and exposed terminal problems.
  Requirements of routing protocols for MANETs are :
  1. Should operate in a distributed manner, be multi-hop and loop free for best results.
  2. Causes of formation of routing loops is that nodes choose their next hops in a completely distributed manner based on information that could be stale and incorrect.

Requirements for Routing protocols

3. Should operate in a demand based or proactive mode because of the possibility of rapid changes in topology.
4. Should be scalable because the MANET size may increase to thousands of nodes.
5. Should have a provision for ‘sleep’ period because nodes may not be in operating state always.
6. Should support unidirectional links because transmission in both directions may not be same or possible.

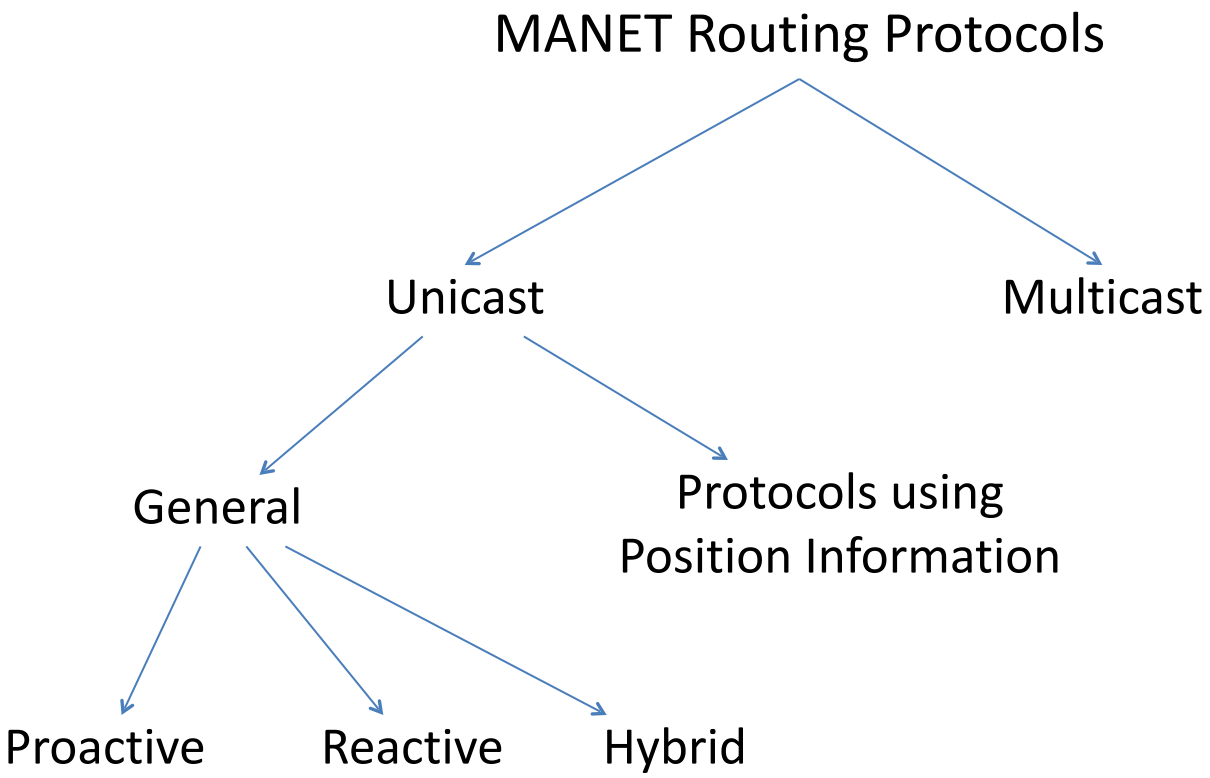
Requirements for Routing protocols

7. Should provide a security mechanism because any one could simply connect to the ad hoc network.
8. Besides above qualitative requirements it should satisfy some quantitative measures like:
   (a) route acquisition time,
   (b) end-to-end data throughput and delay,
   (c) percentage of out of order delivery,
   (d) efficiency and overheads of data transmission.

Requirements for Routing protocols

9. Further 2 basic parts to routing protocols :
   - Route discovery :
     - Is required to be done frequently because node mobility is high. To communicate with another node first a route to that node should be determined by initiating a route discovery procedure, using some kind of flooding.
   - Route maintenance :
     - For same reason as above and also because route changes can occur because of noise, interference, link breakage etc.
     - Using hop by hop acknowledgements route information is maintained at nodes affected by link failures.

Classification of Routing Protocols



Classification of Routing Protocols

- Proactive protocols:
  1. Also called table driven routing protocols.
  2. Calculate all possible paths in the network independently of their use.
  3. Advantage :
     - When a packet needs to be forwarded, path is already known and can be used immediately.

Classification of Routing Protocols

- Reactive protocols :
  1. Also called source initiated on demand routing protocols ; are those that invoke route determination procedure only on demand.
  2. If data traffic is not generated by nodes, then routing activity is totally absent.
- Hybrid protocols :
  - It merges the features of proactive and reactive protocols.

Proactive Routing Protocols

- Destination Sequenced Distance Vector (DSDV):-
  1. Most popular proactive routing protocol.
  2. Based on classical Bellman-Ford Distance Vector routing algorithm.
  3. Improvements made to Bellman-Ford algorithm include freedom from loops in routing tables.
  4. There are 4 distinct phases of DSDV protocol as discussed next.

DSDV Routing Protocols

1. Route Advertisement :
    1. Every mobile node in the network maintains a routing table containing all the possible destinations within the network and the number of hops to each destination.
    2. Each entry is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, and also avoid the formation of routing loops.
    3. These routing tables are broadcast to its current neighbours periodically.

DSDV Routing Protocols

2. Routing table entry structure :
   - The data broadcast by each mobile node contains the new sequence number and the following information for each new route:
     1. The destination address;
     2. The number of hops required to reach the destination;
     3. The sequence number of the information received regarding that destination, and stamped by the destination

DSDV Routing Protocol

3. Responding to topology changes :
    1. To maintain consistency of routing tables in a dynamically varying topology, updates are transmitted by a mobile node to each of its neighbour periodically.
    2. Updates may also be transmitted immediately when significant new information is available.

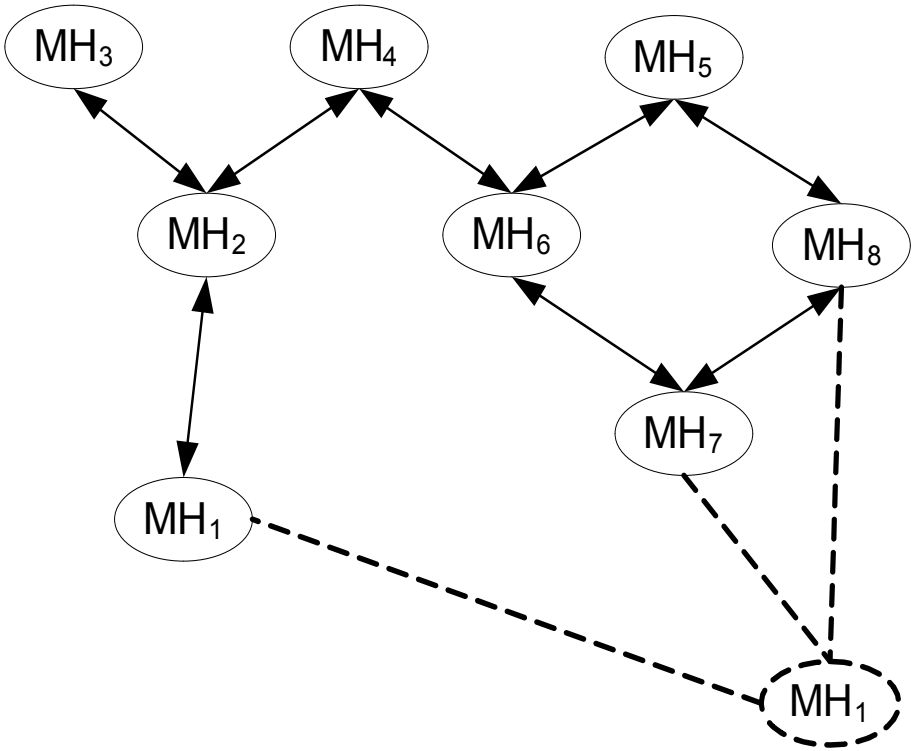
DSDV Routing Protocol

4. Route selection criteria :
    1. On receiving new routing information through an incremental packet, a mobile host compares it to that already available from previous packets. A route with more recent sequence number is used.
    2. Routes with older sequence numbers are discarded.
    3. A route with same sequence number to an existing route is chosen if it has a better metric, say cost, and existing route is discarded or stored as less preferable.

Proactive Routing Protocol

- Example :
  - Consider the ad hoc network shown in figure below.

MH_1 moves to a new location (shown by dotted lines).



- Table below shows a possible structure of the forwarding table at MH_4. It contains four fields :
  1. address of each destination in network.
  2. next hop to it.
  3. cost to it.
  4. sequence number of packet and its creator.

Structure of MH_4 routing table

Destination	Next hop	Metric	Sequence number
MH_1	MH_2	2	$S400\_MH_1$
MH_2	MH_2	1	$S120\_MH_2$
MH_3	MH_2	2	$S500\_MH_3$
MH_4	MH_4	0	$S700\_MH_4$
MH_5	MH_6	2	$S390\_MH_5$
MH_6	MH_6	1	$S070\_MH_6$
MH_7	MH_6	2	$S120\_MH_7$
MH_8	MH_6	3	$S040\_MH_8$

- A typical advertised route table for MH_4.

Destination	Metric	Sequence number
MH_1	2	$S400\_MH_1$
MH_2	1	$S120\_MH_2$
MH_3	2	$S500\_MH_3$
MH_4	0	$S700\_MH_4$
MH_5	2	$S390\_MH_5$
MH_6	1	$S070\_MH_6$
MH_7	2	$S120\_MH_7$
MH_8	3	$S040\_MH_8$

- When MH1 moves near MH8 and MH7, it starts an incremental routing information update and broadcasts it to MH6, which in turn sends an immediate update for MH1. MH1 upon receiving this information broadcasts it at intervals until the next full incremental dump.

Destination	Next hop	Metric	Sequence number
MH_1	MH_6	3	$S500\_MH_1$
MH_2	MH_2	1	$S230\_MH_2$
MH_3	MH_2	2	$S670\_MH_3$
MH_4	MH_4	0	$S820\_MH_4$
MH_5	MH_6	2	$S510\_MH_5$
MH_6	MH_6	1	$S180\_MH_6$
MH_7	MH_6	2	$S230\_MH_7$
MH_8	MH_6	3	$S170\_MH_8$

Updated Route Table at MH_4

Destination	Metric	Sequence number
MH_4	0	$S820\_MH_4$
MH_1	3	$S500\_MH_1$
MH_2	1	$S230\_MH_2$
MH_3	2	$S670\_MH_3$
MH_5	2	$S510\_MH_5$
MH_6	1	$S180\_MH_6$
MH_7	2	$S230\_MH_7$
MH_8	3	$S170\_MH_8$

Updated MH_4 advertised table

- Information for MH4 comes first, since it is the one doing the advertisement. Information for MH1 comes next because it is the only one which has significant route changes that affect it.

Reactive Routing Protocols

- Maintain information about only active routes. Routes are created when desired by source node. Hence the protocols also called on-demand routing protocols.
- Advantages :
  - Low network bandwidth overhead as no periodic routing advertisement messages are sent.
  - Battery power is conserved on mobile hosts (host can put itself on standby or sleep mode as it does not has to send or receive advertisements).
- Disadvantages :
  - High latency since a route discovery procedure is needed before transmission.
  - A separate route maintenance procedure is also necessary to adapt to link state changes.
- Examples:
  - Dynamic Source Routing (DSR), Adaptive on Demand Vector (ADOV), Temporarily Ordered Routing Algorithm (TORA).

Dynamic Source Routing

- Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which to forward a packet
- Sender explicitly lists this route in the packet's header, identifying each forwarding 'hop' by the address of the next node to which to transmit the packet on its way to the destination host.

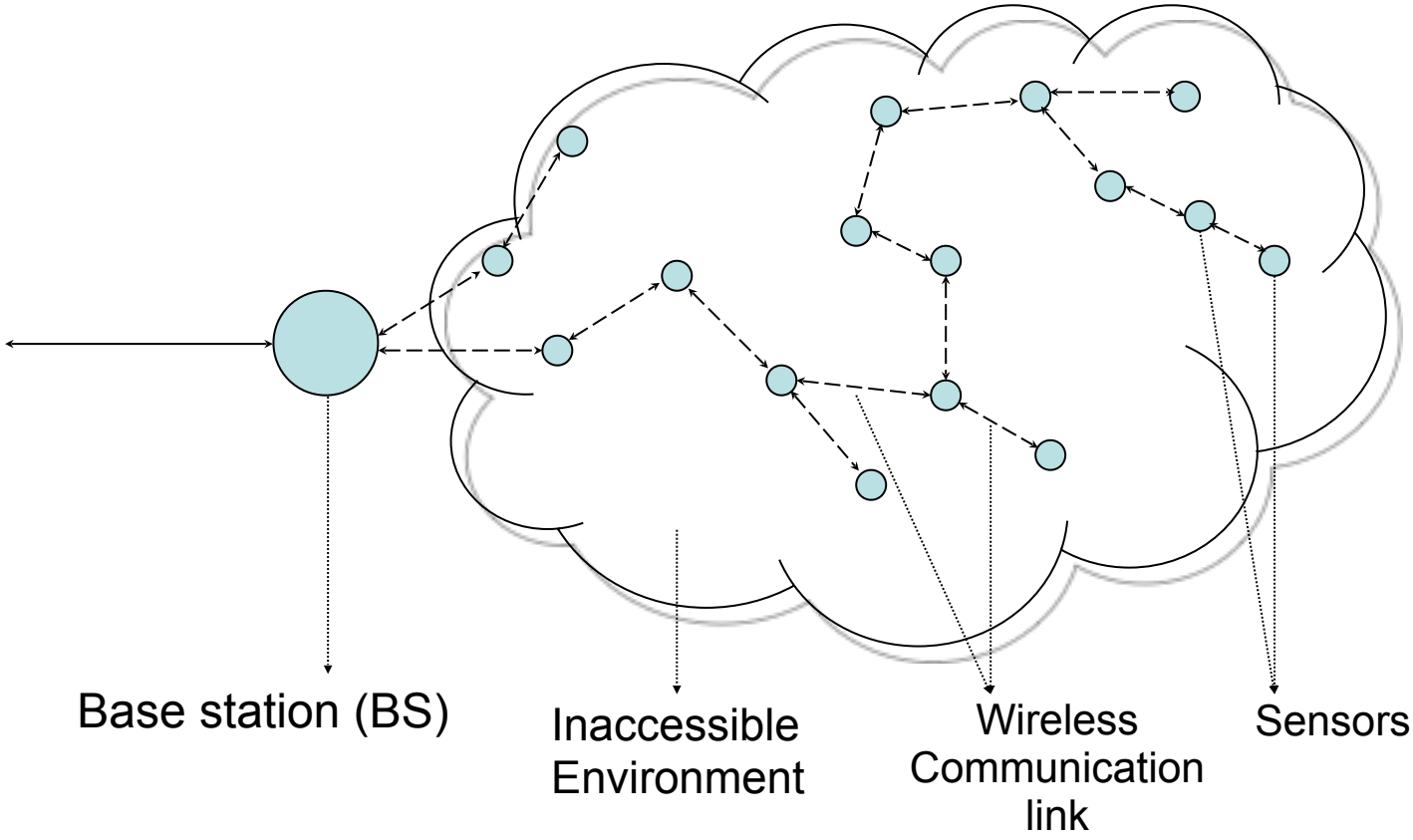
Dynamic Source Routing

- Each router maintains a **route cache** and check the route to the destination if a host sends a packet
- If a route is not found in the cache, **route discovery** (dynamic) is performed by the host node
- If a node moves out of the transmission range, the route is no longer used to reach the destination. This is called **route maintenance**

WIRELESS SENSOR NETWORKS

- Wireless sensors are compact devices that integrate communication, computation and micro-electrical mechanical (MEMS) devices into a single chip.
- A large number of sensors can be spread across a geographical area and networked in many applications that require unattended operations, hence producing a Wireless Sensor Network (WSN).
- The power of wireless sensor networks lies in the ability to deploy large numbers of such tiny sensor nodes. While the capability of any single device is minimal, the composition of hundreds of devices offers a significant opportunity for parallel, accurate and reliable data acquisition.

- The term, **‘ubiquitous** or **pervasive computing’** to denote the kind of computing where computers become so small and so omnipresent that they fade into the background.
- Unlike traditional wireless devices, wireless sensor nodes do not communicate directly with a base station, but rather operate in a peer-to-peer manner. The base station is usually a high computing device, which aggregates data from multiple sensor nodes and processes it.
- All nodes in the network do not necessarily communicate at any particular time, and each node can only communicate with a few nearby nodes. Therefore, data collected by individual nodes is routed between the thousands of tiny sensor nodes in a multi-hop fashion until they reach the base station.



- The figure is a typical wireless sensor network connected to the Internet through a base station and transit network. The network has a routing protocol to control the routing of data messages between nodes. The routing protocol also attempts to get messages to the base station in an energy-efficient manner. Thus sensor nodes act as routers as well as data originators

Applications of Wireless Sensor Networks:

1. Military applications
2. Environmental applications
3. Medical applications
4. Industrial applications
5. Urban applications

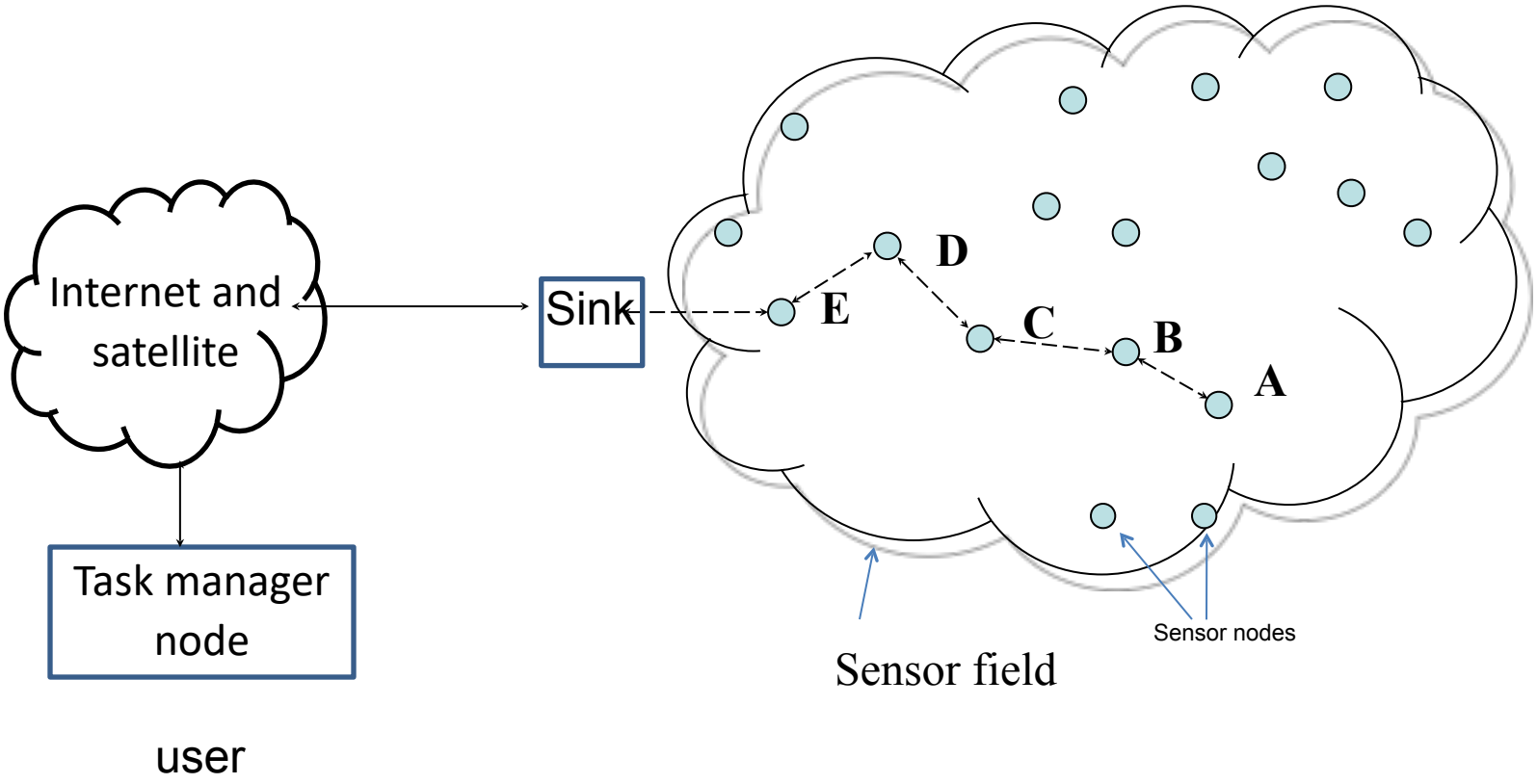
Differences with Mobile Ad hoc Networks

1. The number of sensor nodes in a sensor network is much more than that in an ad hoc network.
2. Sensor nodes are generally static and cooperate together to transfer the sensed data.
3. In mobile ad hoc networks, the number of nodes is much less but their mobility is very high.
4. Sensor nodes mainly use the broadcast communication paradigm, whereas most ad hoc networks are based on point-to point communication.
5. Another difference between the two is that sensor nodes have a much lower power consumption requirement, of the order of 0.75 mW.

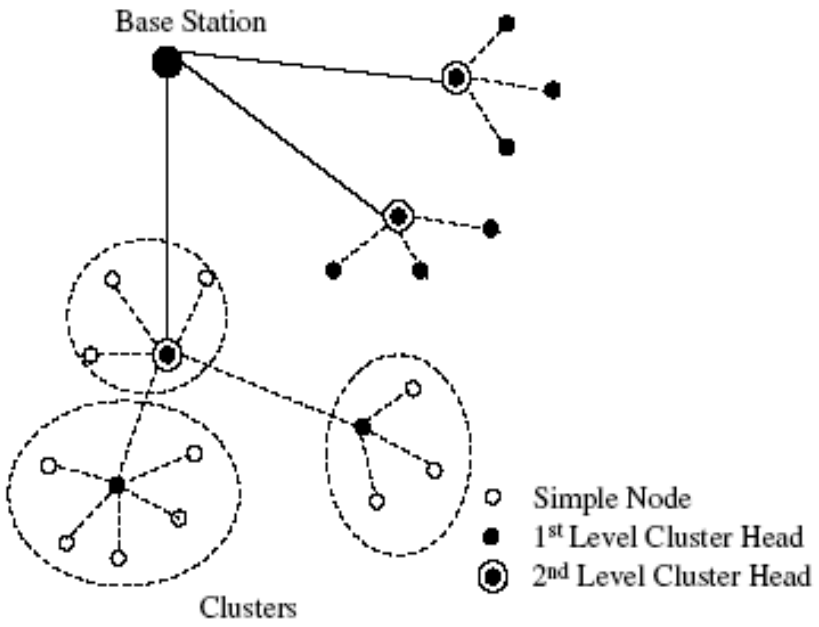
Design Issues

- Low power consumption
- Low cost
- Security
- Data throughput

WSN Architecture

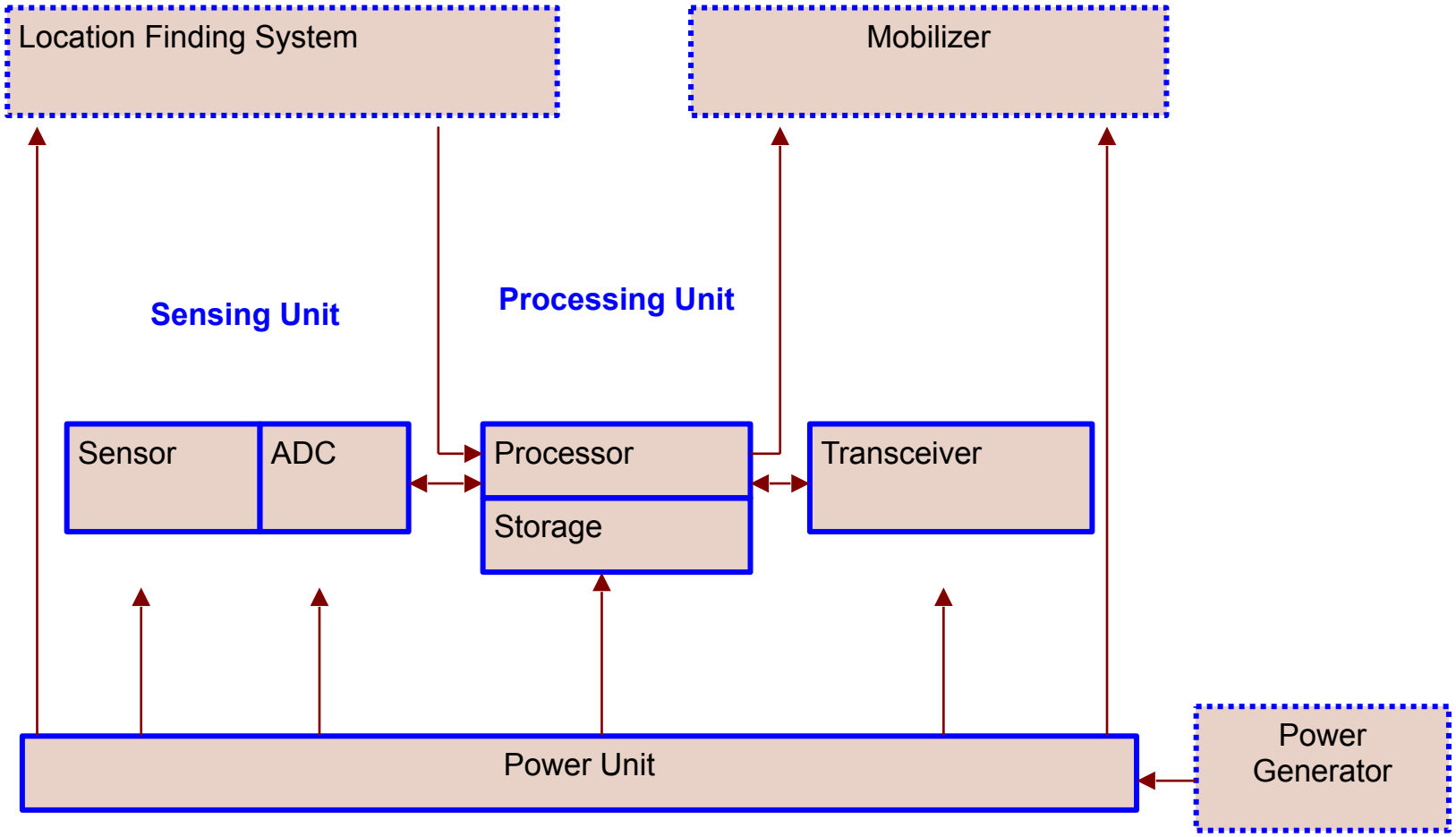


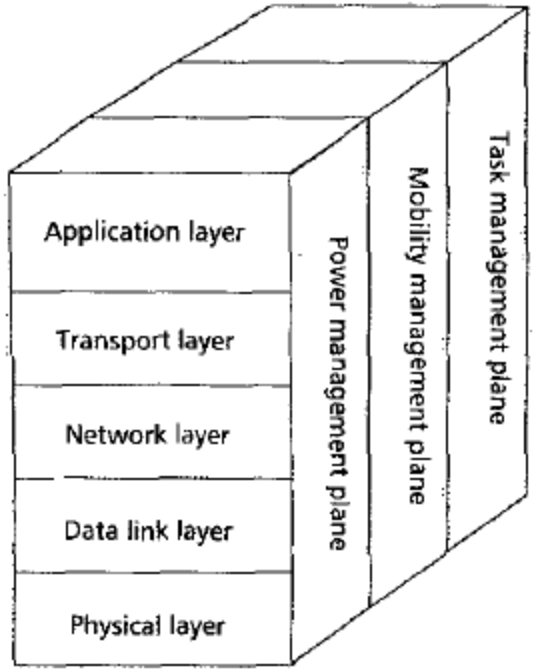
General architecture of a wireless sensor network



Cluster-based hierarchical architecture of WSNs

Sensor hardware components:





WSN Communications Architecture

- The **Power management plane** manages how a sensor node uses its power across all layers, since power efficiency is an essential constraint in WSNs.
- The **Task management plane** balances and schedules the sensing tasks given to a specific region, since not all sensor nodes in that region are required to perform the sensing task at the same time.

Routing protocols for WSN :

Routing protocols have been classified into three categories.

1. **Data centric protocols:**

- Data-centric protocols are query-based and depend on the naming of desired data, which helps in eliminating many redundant transmissions
- The sink sends queries to certain regions and waits for data from the sensors located in these regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data.

The following routing protocols can be considered to belong to this category.

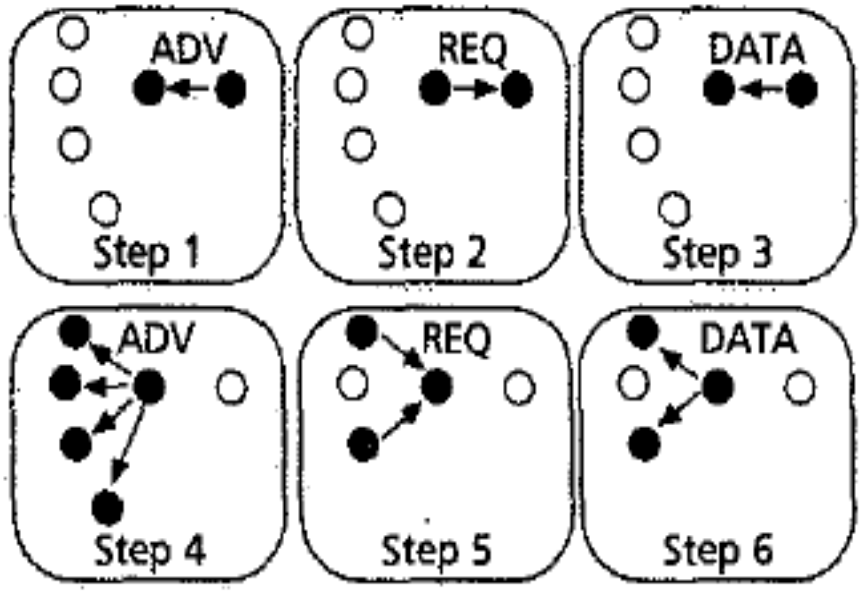
- Flooding and Gossiping
- Sensor Protocols for Information via Negotiation (SPIN)

Flooding and Gossiping:

- Flooding and gossiping are two classical mechanisms to relay data in sensor networks without the need for any routing algorithms and topology maintenance.
- Gossiping is a slightly enhanced version of flooding, where the receiving node sends the packet to a randomly selected neighbor, which picks another random neighbor to forward the packet to and so on.
- Flooding has several drawbacks.
  - **implosion** caused by duplicated messages sent to same node
  - **overlap** caused when two nodes sensing the same region send similar packets to the same neighbor
  - **resource blindness** by consuming large amount of energy without consideration for the energy constraints .
- Gossiping avoids the problem of implosion by just selecting a random node to send the packet rather than broadcasting. However, this causes delays in the propagation of data through the nodes.

Sensor Protocols for Information via Negotiation (SPIN):

- SPIN can be used to efficiently disseminate information in a wireless sensor network. Conventional data dissemination approaches like flooding and gossiping waste valuable communication and energy resources sending redundant information throughout the network.
- SPIN has three types of messages, ADV (Advertisement), REQ (Request) and DATA.



SPIN Protocol

Hierarchical protocols:

- A single-tier network can cause the gateway to overload with the increase in number of sensors. Such overload might cause latency in communication and inadequate tracking of events.
- To allow the system to cope with additional load and to be able to cover a large wider physical area without degrading service, clustering has been pursued in some routing approaches.
- The main aim of hierarchical routing is to efficiently maintain the energy consumption of sensor nodes by using multi-hop communication within a particular cluster. By performing data aggregation and fusion, the number of transmitted messages to the sink decreases.

Hierarchical routing approaches:

- Low Energy Adaptive Clustering Hierarchy (LEACH)
- PEGASIS
- TEEN and APTEEN

Location-based protocols:

- Location information can be utilized in routing data in an energy efficient way. For instance, if the region to be sensed is known, using the location of sensors, the query can be diffused only to that particular region. This will eliminate the number of transmission significantly.

- Some of these protocols, which were designed primarily for mobile ad hoc networks, consider the mobility of nodes during the design but are also applicable to sensor networks where there is less or no mobility.

  - Geographic Adaptive Fidelity or GAF
  - Minimum Energy Communication Network or MECN
  - Small Minimum Energy Communication Network or SMECN

Thank You