EC8702 - Ad hoc and Wireless Sensor Networks

AD HOC NETWORKS – INTRODUCTION AND ROUTING PROTOCOLS

Mr.M.Kamarajan,AP/ECE/MSAJCE

UNIT I AD HOC NETWORKS – INTRODUCTION AND ROUTING PROTOCOLS 9

Elements of Ad hoc Wireless Networks, Issues in Ad hoc wireless networks, Example commercial applications of Ad hoc networking, Ad hoc wireless Internet, Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks, Classifications of Routing Protocols, Table Driven Routing Protocols - Destination Sequenced Distance Vector (DSDV), On–Demand Routing protocols –Ad hoc On–Demand Distance Vector Routing (AODV).

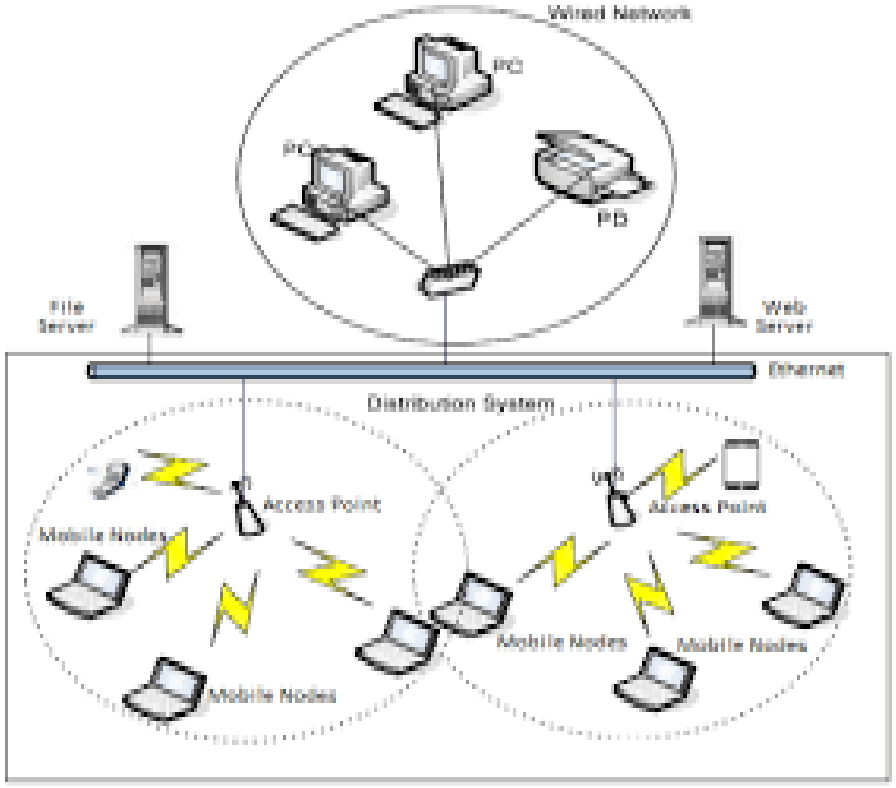
Presentation Outline – Lecturer 1

- Introduction
- Fundamentals of Wireless Communication Technology
- The Electromagnetic Spectrum
- Radio Propagation Mechanism
- Characteristics of the Wireless Channel
- Ad hoc Wireless networks
- Cellular and Ad Hoc Wireless Networks
- Features and Applications of Ad hoc Wireless networks

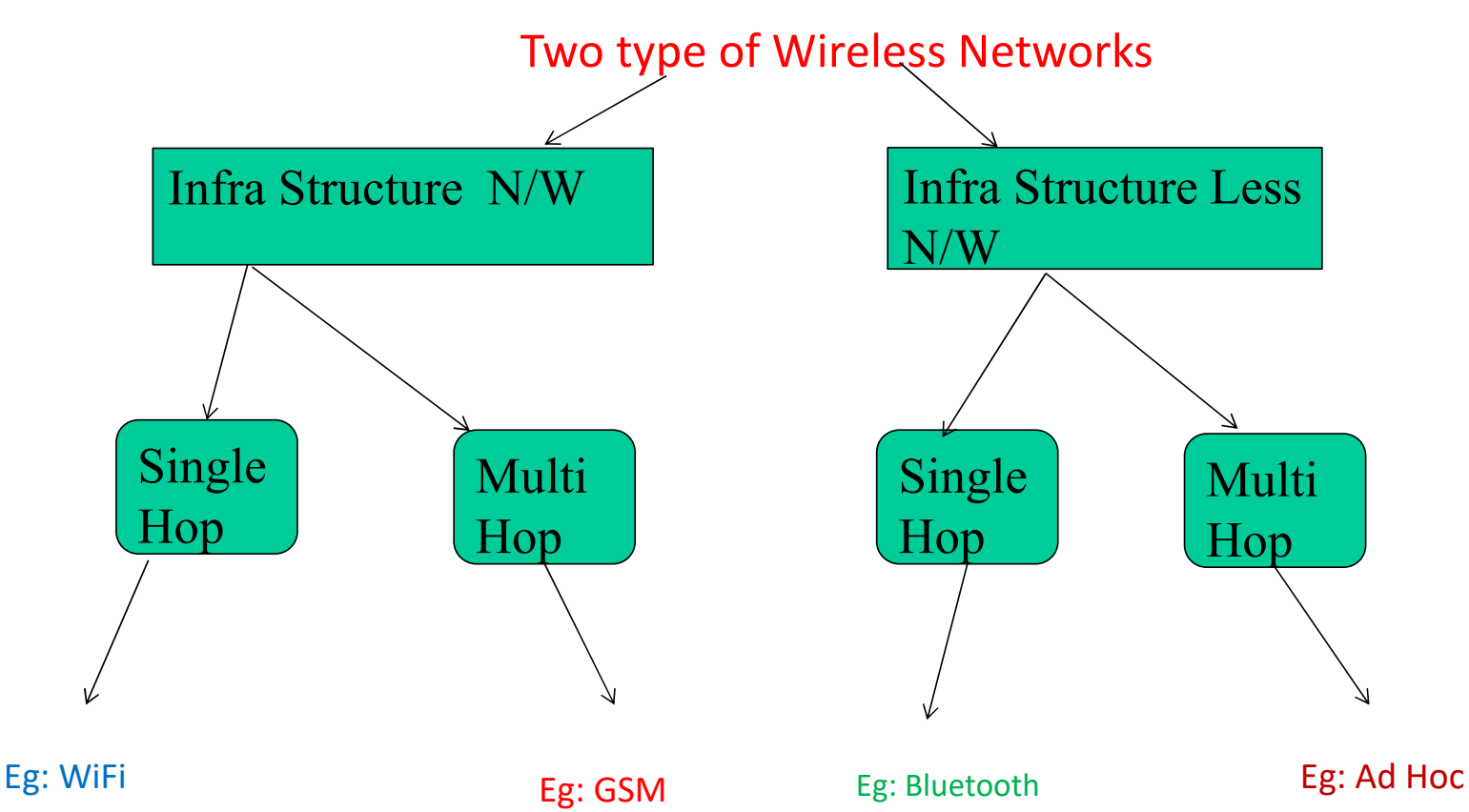
Introduction

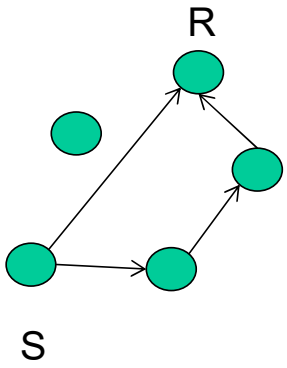
- Wireless Networking – refers to any kind of networking that does not involve cables
- Wireless telecommunications networks are implemented and administered using a transmission system called radio waves
- Implementation takes place at the physical level (layer) of the network structure
- It is a computer network that uses wireless data connections between network nodes

Wired Networking



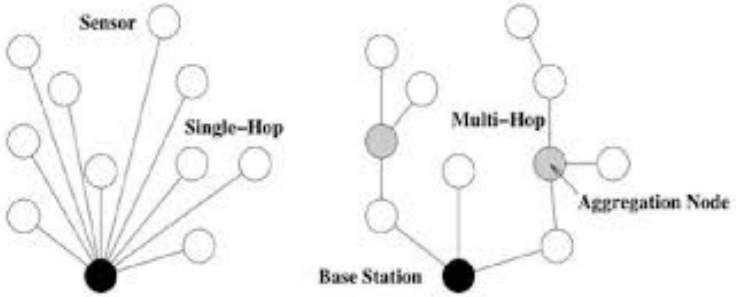
Note: Before starting Ad hoc , You should know Basic Idea about wireless networks, Wireless Networks?, Types of Wireless Networks, How the networks communicating, What type of communication they can be established….
(Without knowing the basic things you can not able to understand Ad Hoc

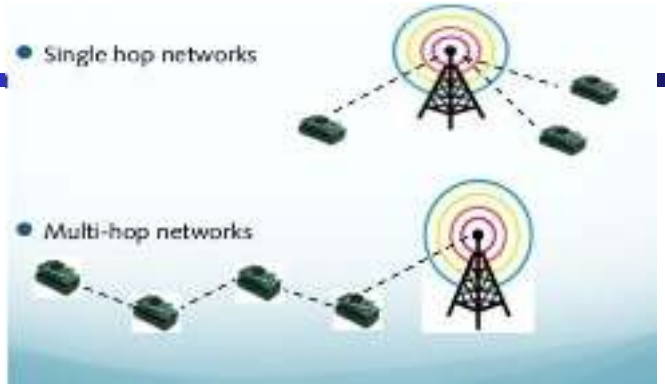


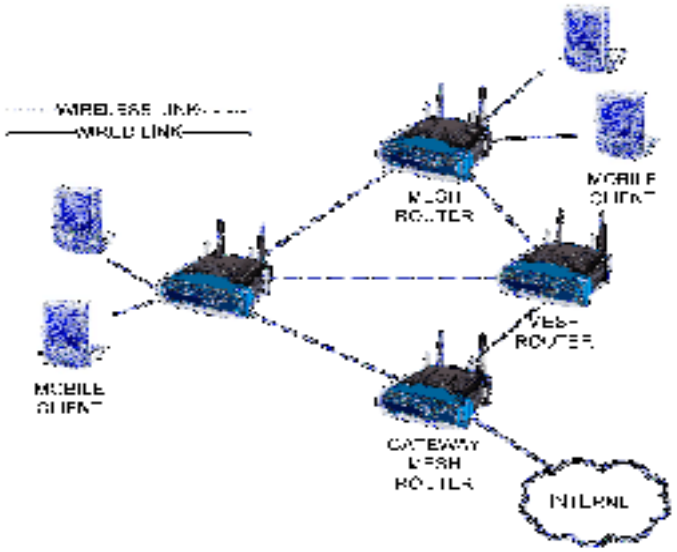


Single and Multi Hop

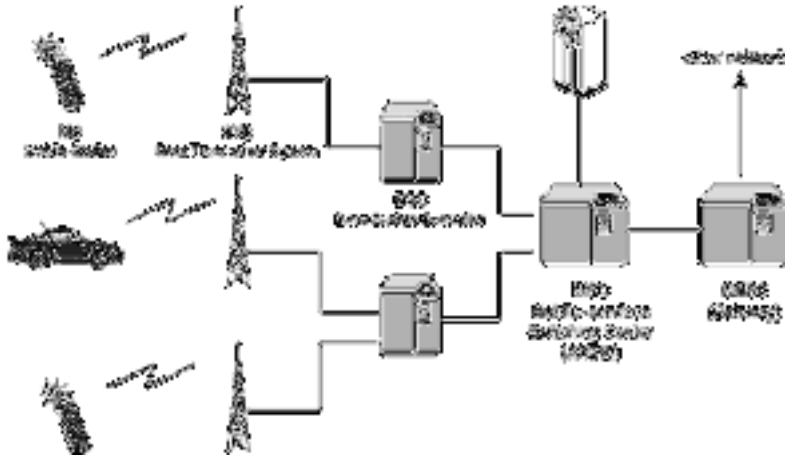
Infrastructure Wireless N/W







Single Hop- WiFi- Through Router communication is made



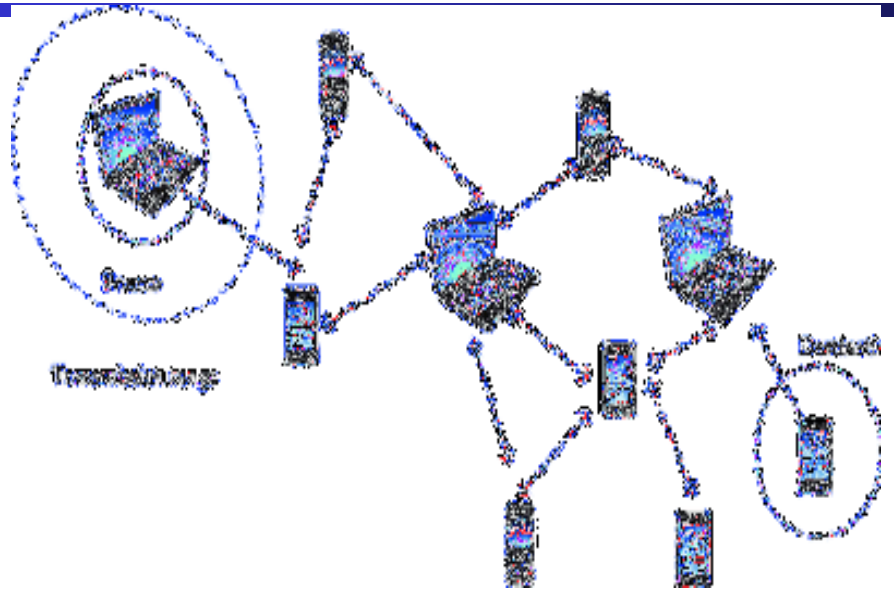
Multi Hop : Eg- GSM

Infrastructure Wireless Network

- **Network infrastructure** is the hardware and software resources of an entire **network**
- That enable **network** connectivity, communication, operations and management of an enterprise **network**. It provides the communication path and services between users, processes, applications, services and external **networks**/the internet. Connected to the wired LAN
- The Wireless Access point used to extend the Coverage area of LAN network and to connect wirelessly
- Computers both in wired and wireless environment can connect with each other

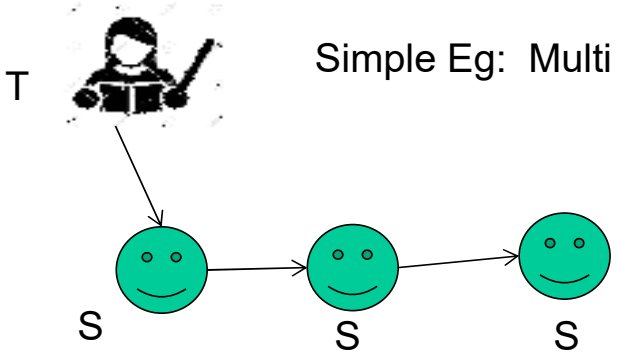
Infrastructure Less Wire Less Network

Mobile Ad Hoc



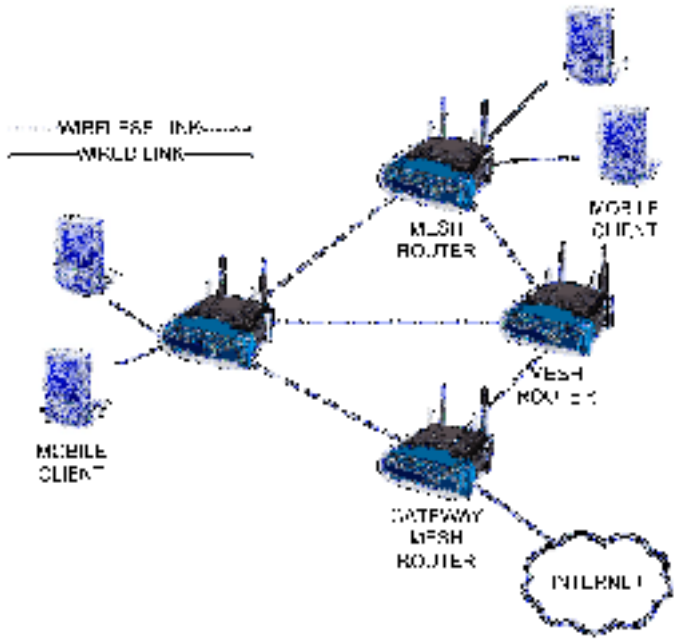
- No Router required
- No Additional component is (Infrastructure) required
- Just enable Bluetooth, make a connection and file transfer is made

- Single hop, No any intermediate is required

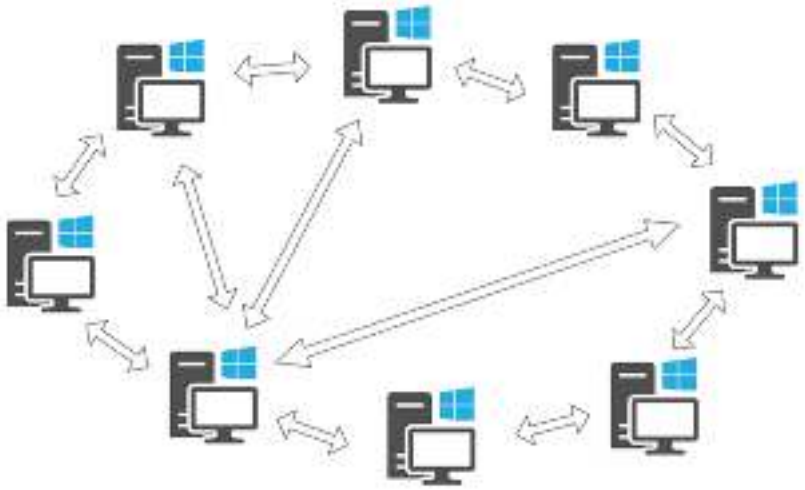


Simple Eg: Multi Hop

Wireless Network



Infrastructure based wireless network(WiFi)



Ad hoc wireless network (Multi hop-Infra Less N/W

Electromagnetic Spectrum and Its allocation – May 2018

3) Describe about the electromagnetic spectrum and its frequency bands with its uses. (8)

Wireless communication is based on the principle of broadcast and reception of electromagnetic waves. These waves can be characterized by their frequency (f) or their wavelength (λ).

Frequency is the number of cycles (oscillations) per second of the wave and is measured in Hertz (Hz) wavelength is the distance between two consecutive maxima or minima in the wave.

The speed of propagation of these waves (c) varies from medium to medium,

$C = \lambda * f$

where c is the speed of light ($3 \times 108 m/s$), f is the frequency of the wave in Hz, and λ is its wavelength in meters.

.

A pictographic view of the electromagnetic spectrum is given in Figure 1

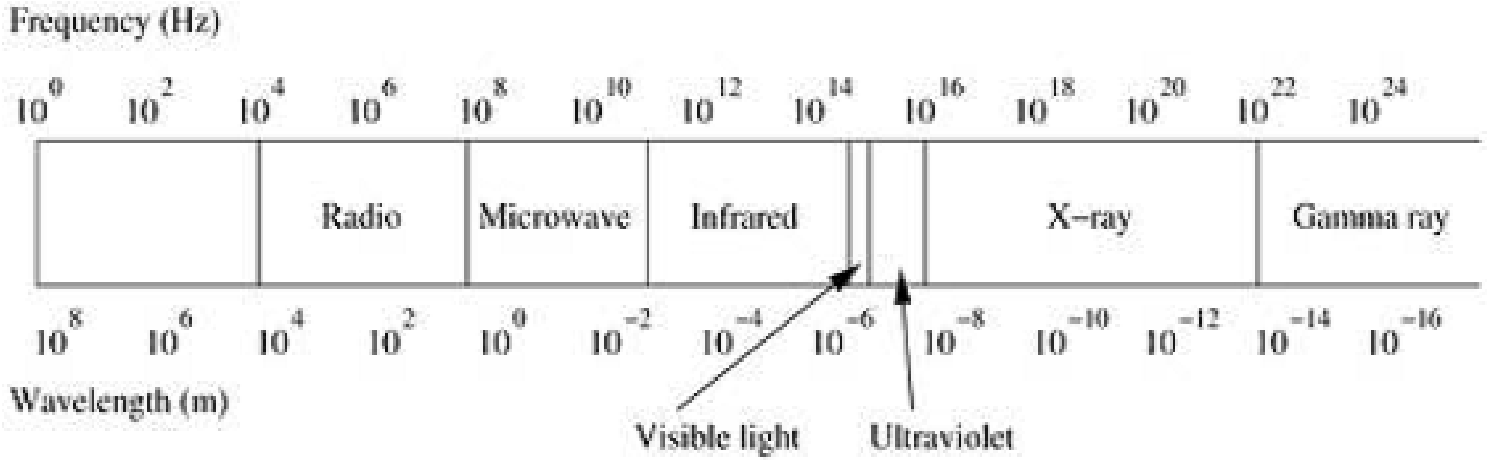


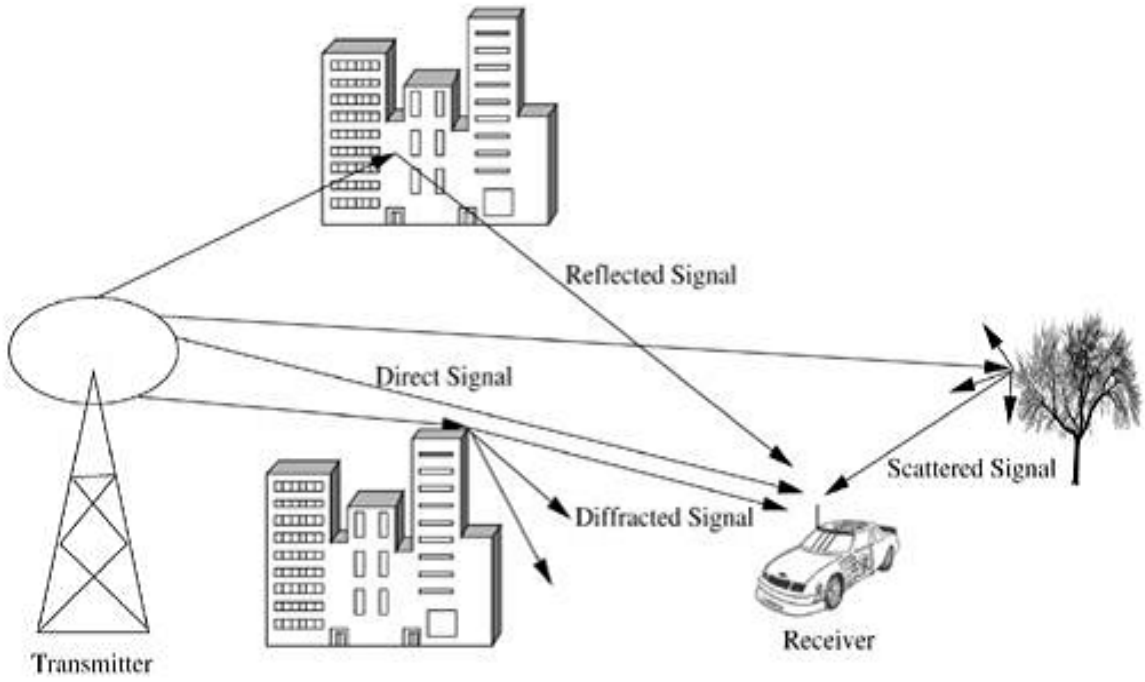
Figure 1.1. The electromagnetic spectrum

Table 1.1 shows the various frequency bands in the electromagnetic spectrum as defined by the International Telecommunications Union (ITU).

Band Name	Frequency	Wavelength	Applications
Extremely Low Frequency (ELF)	30 to 300 Hz	10,000 to 1,000 Km	Powerline frequencies
Voice Frequency (VF)	300 to 3,000 Hz	1,000 to 100 Km	Telephone communications
Very Low Frequency (VLF)	3 to 30 KHz	100 to 10 Km	Marine communications
Low Frequency (LF)	30 to 300 KHz	10 to 1 Km	Marine communications
Medium Frequency (MF)	300 to 3,000 KHz	1,000 to 100 m*	AM broadcasting
High Frequency (HF)	3 to 30 MHz	100 to 10 m	Long-distance aircraft/ship communications
Very High Frequency (VHF)	30 to 300 MHz	10 to 1 m	FM broadcasting
Ultra High Frequency (UHF)	300 to 3,000 MHz	100 to 10 cm	Cellular telephone
Super High Frequency (SHF)	3 to 30 GHz	10 to 1 cm	Satellite communications, microwave links
Extremely High Frequency (EHF)	30 to 300 GHz	10 to 1 mm	Wireless local loop
Infrared	300 GHz to 400 THz	1 mm to 770 nm	Consumer electronics
Visible Light	400 THz to 900 THz	770 nm to 330 nm	Optical communications

* Throughout this book, the unit *m* refers to meter(s).

Radio Propagation Mechanism (Multipath) –Nov 2016, May 2017. May2018, May2019



List the three radio waves propagation mechanisms.

Propagation Mechanism

- **Free-space propagation**
- **Reflection**
- **Diffraction**
- **Scattering**

If these IOs have a *smooth* surface, waves are *reflected* and a part of the energy penetrates the IO (*transmission*).

If the surfaces are *rough*, the waves are diffusely *scattered*.

Finally, waves can also be *diffracted* at the edges of the IOs

RADIO PROPAGATION MECHANISMS

Radio waves generally experience the following three propagation mechanisms:

- **Reflection:**

When the propagating radio wave hits an object which is very large compared to its wavelength (such as the surface of the Earth, or tall buildings), the wave gets reflected by that object. Reflection causes a phase shift of 180 degrees between the incident and the reflected rays.

- **Diffraction:**

This propagation effect is undergone by a wave when it hits an impenetrable object. The wave bends at the edges of the object, thereby propagating in different directions. This phenomenon is termed as diffraction. The dimensions of the object causing diffraction are comparable to the wavelength of the wave being diffracted. The bending causes the wave to reach places behind the object which generally cannot be reached by the line-of-sight transmission. The amount of diffraction is frequency-dependent, with the lower frequency waves diffracting more.

- Scattering:

When the wave travels through a medium, which contains many objects with dimensions small when compared to its wavelength, scattering occurs. The wave gets scattered into several weaker outgoing signals. In practice, objects such as street signs, lamp posts, and foliage cause scattering.

CHARACTERISTICS OF THE WIRELESS CHANNEL- May 2017, Nov 2018,May 2018, May 2019

i) Explain about the characteristics of the wireless channel.

- Path Loss
- Fading
- Interference
- Doppler Shift
- Transmission Rate Constraints

Path Loss

- Path loss can be expressed as the ratio of the power of the transmitted signal to the power of the same signal received by the receiver, on a given path. It is a function of the propagation distance.

Path loss is dependent on a number of factors such as the radio frequency used and the nature of the terrain. Since several of these factors (in particular, the terrain) cannot be the same everywhere, a single model may not be enough.

So, several models are required to describe the variety of transmission environments.

1.Free Space Propagation Model

in which there is a direct-path signal between the transmitter and the receiver, with no atmospheric attenuation or multipath components.

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2$$

The relationship between the transmitted power Pt and the received power Pr is given b

2.Two Ray Model

The signal reaches the receiver through two paths, one a line-of sight path, and the other the path through which the reflected (or refracted, or scattered) wave is received. According to the two-path model, the received power is given by

$$P_r = P_t G_t G_r \left(\frac{h_t h_r}{d^2}\right)^2$$

Fading

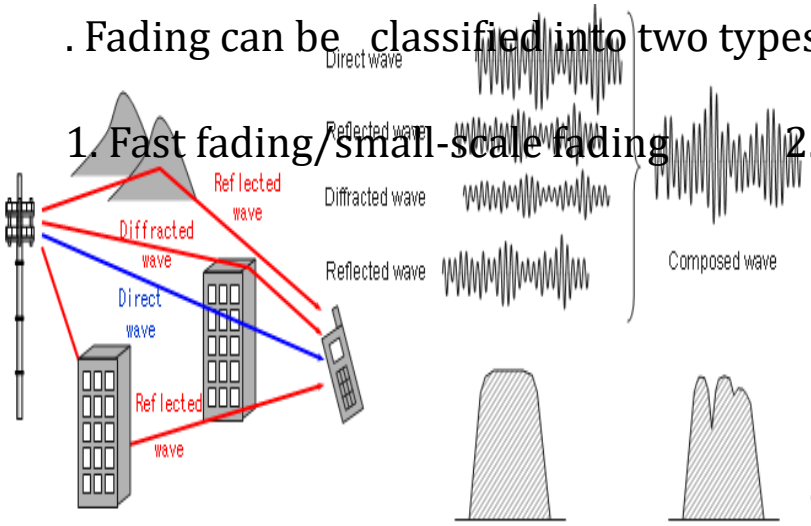
What is Fading?

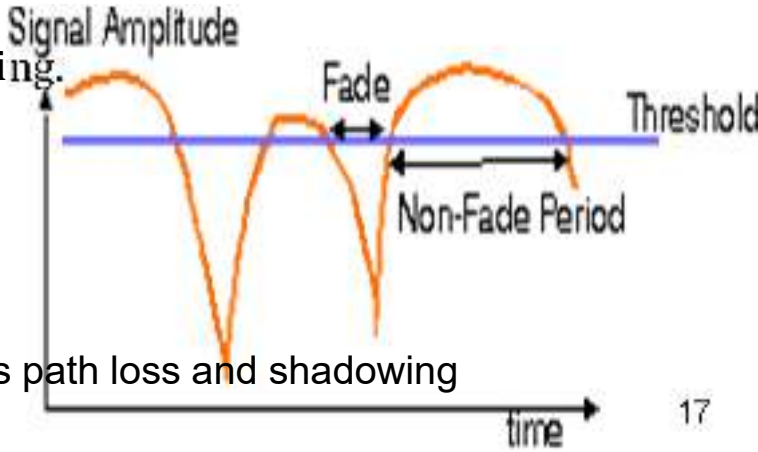
Fading refers to the fluctuations in signal strength when received at the receiver

Fading depends on various factors, In fixed scenario, fading depends on atmospheric conditions such as rainfall, lightening etc. In mobile scenario, fading depends on obstacles over the path which are varying with respect to time. These obstacles create complex transmission effects to the transmitted signal.

. Fading can be classified into two types:

1. Fast fading/small-scale fading 2. Slow fading/large-scale fading.





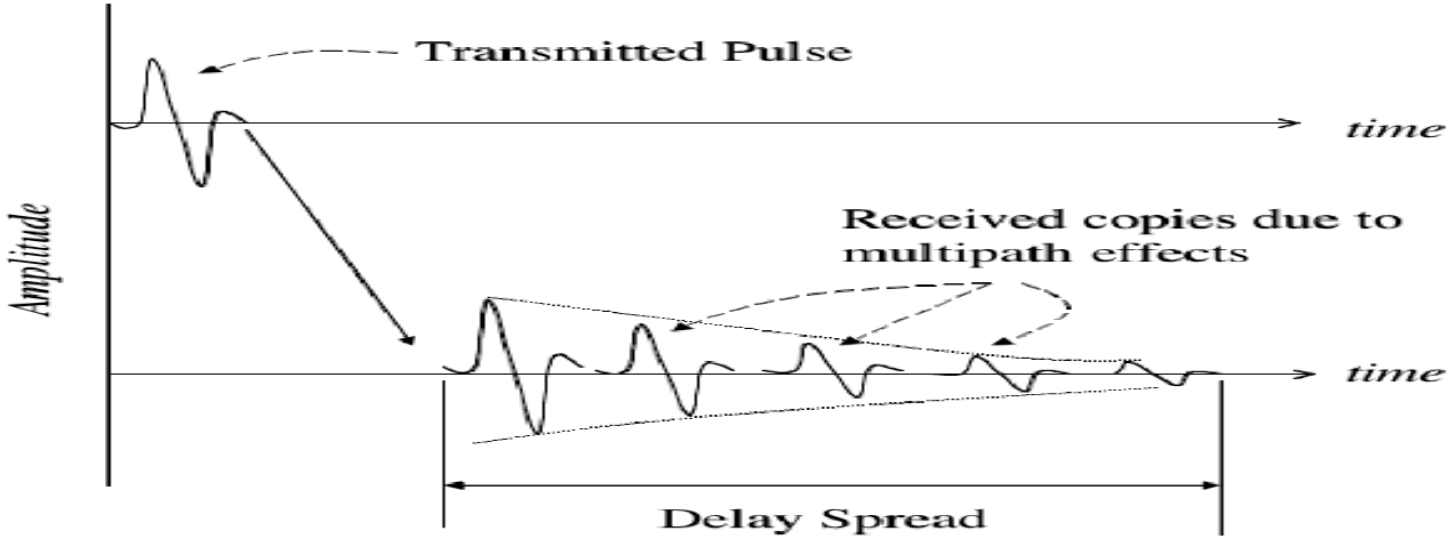
Large Scale Fading: It includes path loss and shadowing effects.

Delay Spread

The time between the reception of the first version of the signal and the last echoed signal is called delay spread.

The multipath propagation of the transmitted signal, which causes fast fading.

The multipath propagation of the transmitted signal, which causes fast fading, The multiple signal paths may sometimes add constructively or sometimes destructively at the receiver, causing a variation in the power level of the received signal.



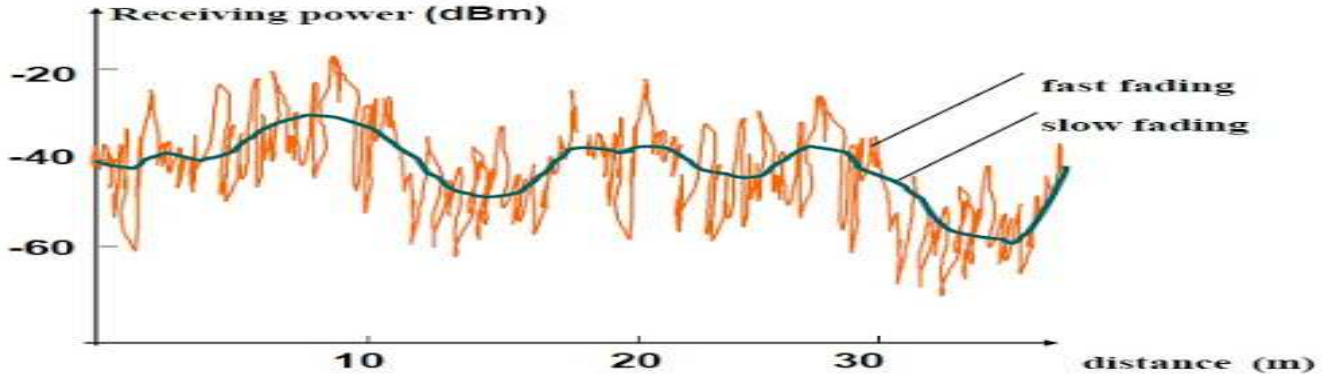
Fast fading refers to the rapid fluctuations in the amplitude(Strength) over short distance or short time period, phase, or multipath delays of the received signal, due to the interference between multiple versions (copies) of the same transmitted signal arriving at the receiver at slightly different times

Slow fading occurs when objects that partially absorb the transmissions lie between the transmitter and receiver.

Slow fading is so called because the duration of the fade may last for multiple seconds or minutes.

Slow fading may occur when the receiver is inside a building and the radio wave must pass through the walls of a building, or when the receiver is temporarily shielded from the transmitter by a building.

Slow fading is also referred to as shadow fading since the objects that cause the fade, which may be large buildings or other structures, block the direct transmission path from the transmitter to the receiver.



Fading Types(Based on Doppler Spread)

Fast Fading

- High Doppler spread
- Coherence time < Symbol period
- Channel variations faster than baseband signal variations

Slow Fading

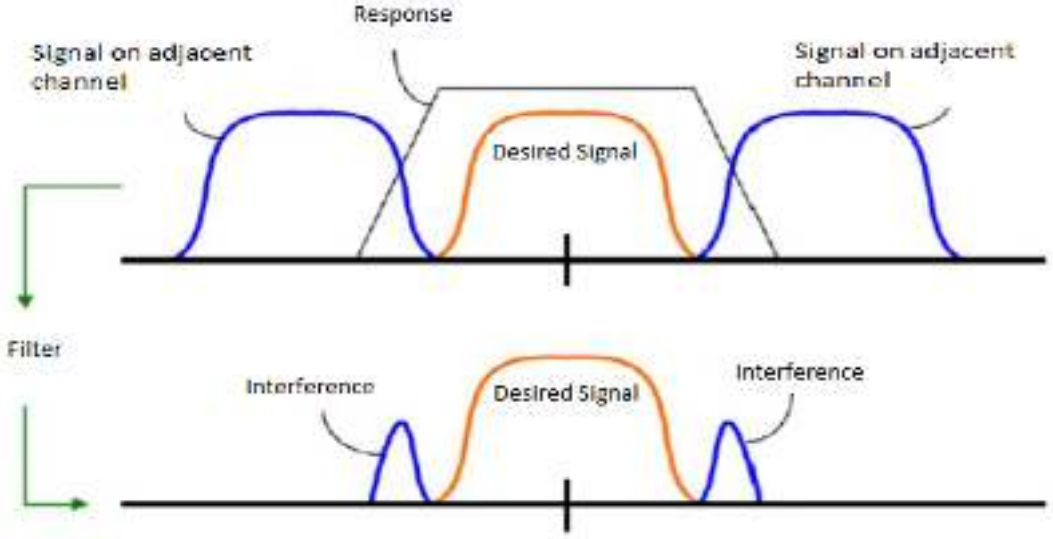
- Low Doppler spread
- Coherence time > Symbol period
- Channel variations slower than baseband signal variations

Interference

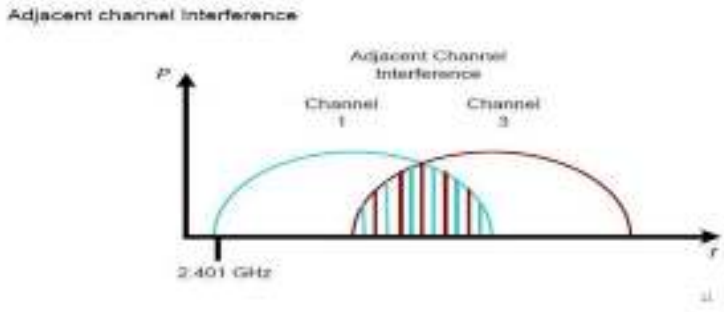
Wireless transmissions have to counter interference from a wide variety of sources. Two main forms of interference are

1. Adjacent channel interference

It case, signals in nearby frequencies have component outside their allocated ranges. These components may interfere with on-going transmissions in the adjacent frequencies. It can be avoided by carefully introducing guard bands2 between the allocated frequency ranges.



Adjacent-channel interference (ACI) :This type of interference occurs when the information on the adjacent channel seeps into pass band of the channel being transmitted, due to which performance of the main channel is degraded.



Co-Channel Interference

- **Conception:** the interference among the signals of co-channel cells is called co-channel interference.
- **Result from :** Frequency reuse
- **Reduction method:** co-channel cells must physically be spaced at a minimum interval to ensure adequate isolation of transmissions.

Adjacent Channel Interference

- **Conception:** The signal interference from the frequency adjacent to that of the signal used is called adjacent channel interference.
- **Reduction method:** accurate filtering and channel allocation (maximizing channel intervals of the cell). Interval of frequency reuse inter-cell interference, such as C/I, C/A

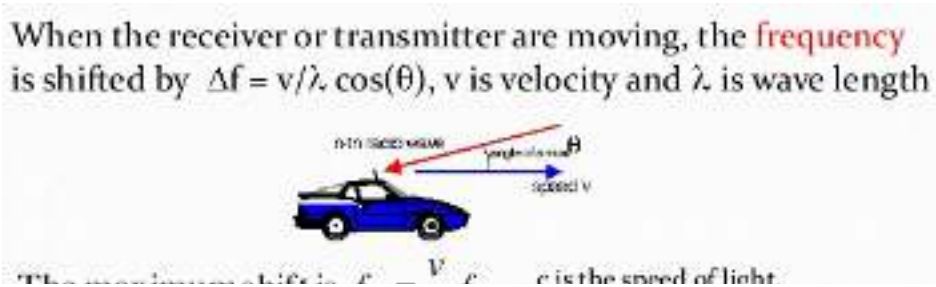
Doppler Shift

The Doppler shift is defined as the change/shift in the frequency of the received signal when the transmitter and the receiver are mobile with respect to each other. If they are moving toward each other, then the frequency of the received signal will be higher than that of the transmitted signal, and if they are moving away from each other, the frequency of the signal at the receiver will be lower than that at the transmitter.

The Doppler shift fd is given by

$$f_d = \frac{v}{\lambda}$$

where v is the relative velocity between the transmitter and receiver, and λ is the wavelength of the signal.



Transmission Rate Constraints

- Two important constraints that determine the maximum rate of data transmission on a channel are Nyquist's theorem and Shannon's theorem.
- **Nyquist's Theorem**
  - The signalling speed of a transmitted signal denotes the number of times per second the signal changes its value/voltage. The number of changes per second is measured in terms of *baud*.
  - The baud rate is not the same as the bit rate/data rate of the signal since each signal value may be used to convey multiple bits.
  - . The*Nyquist theorem* gives the maximum data rate possible on a channel. If B is the bandwidth of the channel (in Hz) and L is the number of discrete signal levels/voltage values used, then the maximum channel capacity C according to the Nyquist theorem is given by

    $$C = 2 \times B \times log_2 L \qquad \text{bits/sec}$$

- **Shannon's Theorem**
  - Noise level in the channel is represented by the SNR. It is the ratio of signal power (S) to noise power (N), specified in decibels, that is, $SNR = 10\ log10(S/N)$.
  - Shannon was his theorem on the maximum data rate possible on a noisy channel. According to *Shannon's theorem,* the maximum data rate C is given by

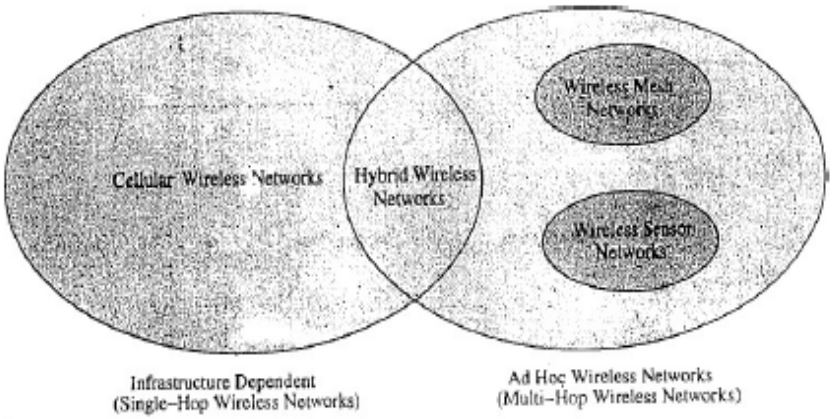
    $$C = B \times log_2(1 + (S/N)) \qquad \text{bits/sec}$$

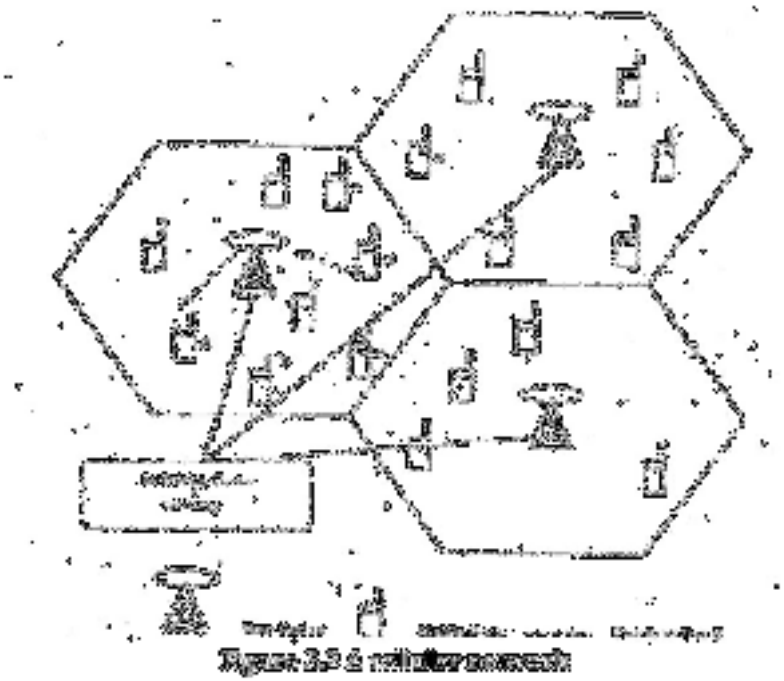
    where B is the bandwidth of the channel (in Hz).

Ad hoc wireless network

- ***Ad hoc*** is a word that originally comes from Latin and **means** “for this” or "for this situation.
- Multi hop wireless network
- The wireless hosts in ad hoc networks, communicate with each other without the existing of a fixed infrastructure
- Decentralized control
- A mobile ad-hoc network can be connected to other fixed networks or to the Internet.
- Most of the Ad-Hoc networks operates in ISM band
- Peer to Peer communication
- Additional feature described in IEEE 802.11 as independent basic service set (IBSS)
- Packed switched network

CELLULAR AND AD HOC WIRELESS NETWORKS





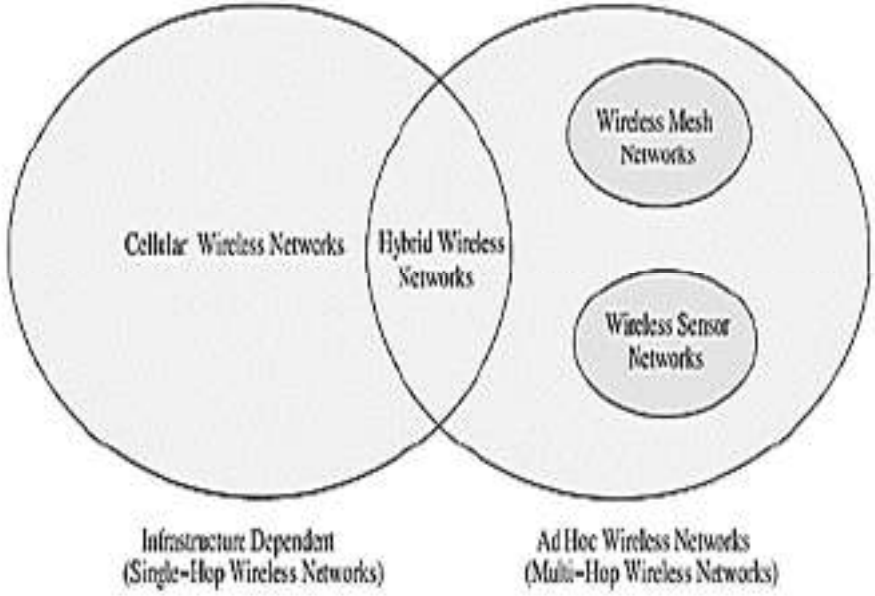
The current cellular wireless networks are classified as the infrastructure dependent network. The path setup for a call between two nodes, say, node C to E, is completed through base station as illustrated in figure below

Network Topology

- Infrastructure Based wireless network
  - numerous portable transceivers communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations
- Ad hoc wireless network
  - ***Mesh networks*** :

    fully connected network
  - ***Sensor networks*** :

    Sensors are connected via wireless to allow large scale collection of sensor data.



Ad Hoc Network

Adhoc wireless networks are defined as a category of wireless network that utilize multi-hop radio replaying and are capable of operating without the support of any fixed infrastructure.

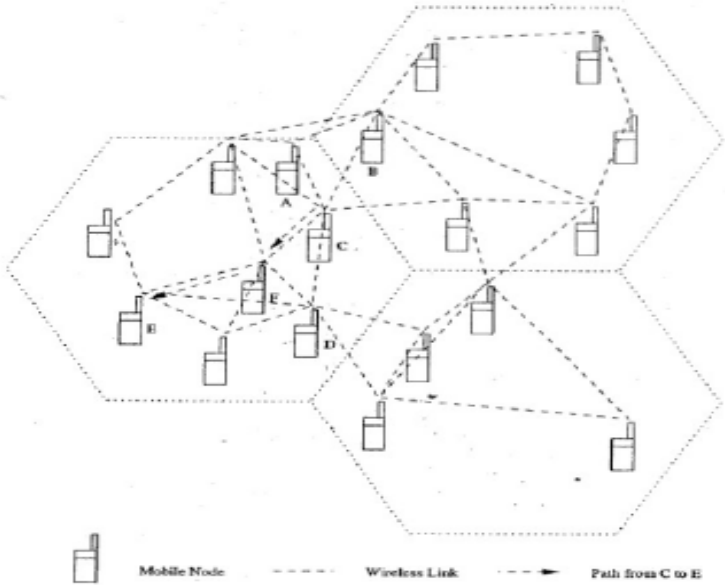


Figure 5.3: An ad hoc wireless network

Absence of any central co-ordinator or base station makes the routing complex.
Adhoc wireless network topology for the cellular network shown in above figure is illustrated below.

The path setup for a call between 2 nodes, say, node C to E , is completed through the intermediate mobile node F.
Wireless mesh network and Wireless sensor networks are specific examples of adhoc wireless networks.

The presence of base station simplifies routing and resource management in a cellular network.

But in adhoc networks, routing and resource management are done in a distributed manner in which all nodes co-ordinate to enable communication among them.

Cellular Networks	Ad Hoc Wireless Networks
Fixed infrastructure-based	Infrastructure-less
Single-hop wireless links	Multi-hop wireless links
Guaranteed bandwidth (designed for voice traffic)	Shared radio channel (more suitable for best-effort data traffic)
Centralized routing	Distributed routing
Circuit-switched (evolving toward packet switching)	Packet-switched (evolving toward emulation of circuit switching)
Seamless connectivity (low call drops during handoffs)	Frequent path breaks due to mobility
High cost and time of deployment	Quick and cost-effective deployment
Reuse of frequency spectrum through geographical channel reuse	Dynamic frequency reuse based on carrier sense mechanism
Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
Application domains include mainly civilian and commercial sectors	Application domains include battlefields, emergency search and rescue operations, and collaborative computing
High cost of network maintenance (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network
Mobile hosts are of relatively low complexity	Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capability)
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
Widely deployed and currently in the third generation of evolution	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

Cellular network Vs Ad hoc wireless network

Cellular network

- ❑ Communication through base station (BS)
- ❑ Single-hop
- ❑ Centralized management at BS
- ❑ Long-term communication
- ❑ Seamless connectivity
- ❑ Homogeneous devices
- ❑ Maintenance cost is high

Ad hoc wireless network

- ❑ Peer-to-peer communication
- ❑ Multi-hop, relay
- ❑ Distributed management
- ❑ Short-term, on-the-fly
- ❑ Frequent breakup in link
- ❑ Heterogeneous devices
- ❑ Self Organizing , maintenance properties are within the network

Benefits of wireless ad-hoc networks

- Ad hoc networks do not require access points
- Provide a low-cost way of direct client-to-client communication
- Ad-hoc networks are easy to configure and offer an effective way to communicate with devices nearby
- Used efficiently under the condition when running cable is not feasible.
- Ad-hoc networks are often secured to protect against attacks.
- An ad-hoc network linking a small number of devices might be better than a regular network with more users connected.
- Self organizing

Disadvantages of ad hoc wireless networks

- Devices in an ad-hoc network cannot disable Service Set Identifier(SSID) broadcasting
- Attackers can find and connect to an ad hoc device if they are within signal range
- Wireless ad-hoc networks cannot bridge wired LANs or to the internet without installing a special-purpose network gateway.
- Devices can only use the internet if one of them is connected to and sharing it with the others
- Ad-hoc mode requires more system resources as the physical network layout changes as devices are moved around
- Limited wireless bandwidth
- Frequent reconfiguration of network

Major Issues in Ad hoc wireless networks

- Medium access scheme
- Routing
- Multicasting
- Transport layer protocol
- Pricing scheme
- Quality of service provisioning
- Self-organization
- Security
- Energy management
- Addressing and service discovery
- Scalability
- Deployment considerations

1. Medium Access Scheme

The primary responsibility of a Medium Access Control (MAC) protocol in adhoc wireless networks is the distributed arbitration for the shared channel for transmission of packets. The major issues to be considered in designing a MAC protocol for adhoc wireless networks are as follows:

- ***Distributed Operation:***
  - The ad hoc wireless networks need to operate in environments where no centralized coordination is possible.
  - The MAC protocol design should be fully distributed involving minimum control overhead.
- ***Synchronization:***
  - The MAC protocol design should take into account the requirement of time synchronization.
  - Synchronization is mandatory for TDMA-based systems for management of transmission and reception slots.
- ***Hidden Terminals:***
  - Hidden terminals are nodes that are hidden(or not reachable) from the sender of a data transmission session, but are reachable to the receiver of the session.

- ***Exposed terminals:***
  - Exposed terminals, the nodes that are in the transmission range of the sender of an on – going session, are prevented from making a transmission.
- ***Throughput:***
  - The MAC protocol employed in adhoc wireless networks should attempt to maximize the throughput of the system.
  - The important considerations for throughput enhancement are
    - Minimizing the occurrence of collisions.
    - Maximizing channel utilization and
    - Minimizing control overhead.
- ***Access delay:***
  - The average delay that any packet experiences to get transmitted. The MAC protocol should attempt to minimize the delay.
- ***Fairness:***
  - Fairness refers to the ability of the MAC protocol to provide an equal share or weighted share of the bandwidth to all competing nodes. Fairness can be either *node-based* or *flow-based.*
- ***Real-time Traffic support*:**
  - In a contention-based channel access environment, without any central coordination, with limited bandwidth, and with location-dependent contention, supporting time- sensitive traffic such as voice, video, and real-time data requires explicit support from the MAC protocol.

- ***Resource reservation*:**
  - The provisioning of QoS defined by parameters such as bandwidth, delay, and jitter requires reservation of resources such as *bandwidth, buffer space*, and *processing power*.
- ***Ability to measure resource availability:***
  - In order to handle the resources such as bandwidth efficiently and perform call admission control based on their availability, the MAC protocol should be able to provide an estimation of resource availability at every node. This can also be used for making *cogestion control decisions*.
- ***Capability for power control:***
  - The transmission power control reduces the energy consumption at the nodes, causes a decrease in interference at neighboring nodes, and increases frequency reuse.
- ***Adaptive rate control:***
  - This refers to the variation in the data bit rate achieved over a channel.
  - A MAC protocol that has adaptive rate control can make use of a high data rate when the sender and receiver are nearby & adaptively reduce the data rate as they move away from each other.
- ***Use of directional antennas:***
  - This has many advantages that include increased spectrum reuse, Reduction in interference and Reduced power consumption.

2. Routing

The responsibilities of a routing protocol include exchanging the route information; finding a feasible path to a destination. The major challenges that a routing protocol faces are as follows:

- ***Mobility :***
  - The Mobility of nodes results in frequent path breaks, packet collisions, transient loops, stale routing information, and difficulty in resource reservation.
- ***Bandwidth constraint :***
  - Since the channel is shared by all nodes in the broadcast region, the bandwidth available per wireless link depends on the number of nodes & traffic they handle.
- ***Error-prone and shared channel :***
  - The Bit Error Rate (BER) in a wireless channel is very high [10-5 to 10 -3] compared to that in its wired counterparts [10-12 to 10-9].
  - Consideration of the state of the wireless link, signal-to-noise ratio, and path loss for routing in ad hoc wireless networks can improve the efficiency of the routing protocol.
- ***Location-dependent contention :***
  - The load on the wireless channel varies with the number of nodes present in a given geographical region.
  - This makes the contention for the channel high when the number of nodes increases.
  - The high contention for the channel results in a high number of collisions & a subsequent wastage of bandwidth.
- ***Other resource constraints :***

The constraints on resources such as computing power, battery power, and buffer storage also limit the capability of a routing protocol. The major requirements of a routing protocol in adhoc wireless networks are the following.

1. Minimum route acquisition delay
2. Quick route reconfiguration
3. Loop-free routing
4. Distributed routing approach
5. Minimum control overhead
6. Scalability
7. Provisioning of QoS
8. Support for time-sensitive traffic:
9. Security and privacy

3. Multicasting:

It plays important role in emergency search & rescue operations & in military communication. Use of single link connectivity among the nodes in a multicast group results in a tree-shaped multicast routing topology. Such a tree-shaped topology provides high multicast efficiency, with low packet delivery ratio due to the frequency tree breaks. The major issues in designing multicast routing protocols are as follows:

- ***Robustness :***
  - The multicast routing protocol must be able to recover & reconfigure quickly from potential mobility- induced link breaks thus making it suitable for use in high dynamic environments.

- ***Efficiency :***
  - A multicast protocol should make a minimum number of transmissions to deliver a data packet to all the group members.

- ***Control overhead :***
  - The scarce bandwidth availability in ad hoc wireless networks demands minimal control overhead for the multicast session.

- ***Quality of Service :***
  - QoS support is essential in multicast routing because, in most cases, the data transferred in a multicast session is time-sensitive.

- ***Efficient group management :***
  - Group management refers to the process of accepting multicast session members and maintaining the connectivity among them until the session expires.

- ***Scalability :***
  - The multicast routing protocol should be able to scale for a network with a large number of node

- ***Security :***
  - Authentication of session members and prevention of non-members from gaining unauthorized information play a major role in military communications.

4. Transport Layer Protocol

The main objectives of the transport layer protocols include:

Setting up & maintaining end-to-end connections, Reliable end-to-end delivery of packets, Flow control & Congestion control.

- Examples of some transport layers protocols are,

a. UDP (User Datagram Protocol) :

It is an unreliable connectionless transport layer protocol. It neither performs flow control & congestion control. It do not take into account the current network status such as congestion at the intermediate links, the rate of collision, or other similar factors affecting the network throughput.

b. TCP (Transmission Control Protocol):

It is a reliable connection-oriented transport layer protocol. It performs flow control & congestion control. Here performance degradation arises due to frequent path breaks, presence of stale routing information, high channel error rate, and frequent network partitions.

5. Pricing Scheme

- Assume that an optimal route from node A to node B passes through node C, & node C is not powered on.
- Then node A will have to set up a costlier & non-optimal route to B.
- The non-optimal path consumes more resources & affects the throughput of the system.
- As the intermediate nodes in a path that relay the data packets expend their resources such as battery charge & computing power, they should be properly compensated.
- Hence, pricing schemes that incorporate service compensation or service reimbursement are required.

6. Quality of Service Provisioning (QoS)

- QoS is the performance level of services offered by a service provider or a network to the user.
- QoS provisioning often requires ,Negotiation between host & the network.
- Resource reservation schemes.
- Priority scheduling &
- Call admission control.

- ***QoS parameters :***

Applications	Corresponding QoS parameter
1. Multimedia application	- 1. Bandwidth & Delay
2. Military application	- 2.Security & Reliability
3. Defense application	- 3.Finding trustworthy intermediate hosts & routing
4. Emergency search and rescue operations	- 4 .Availability
5. Hybrid wireless network	- 5.Maximum available link life, delay, bandwidth & channel utilization.

7. Self-Organization

- One very important property that an ad hoc wireless network should exhibit is organizing & maintaining the network by itself.

- The major activities that an ad hoc wireless network is required to perform for self-organization are, Neighbour discovery, Topology organization & Topology reorganization (updating topology information)

8. Security

Security is an important issue in ad hoc wireless network as the information can be hacked. Attacks against network are of 2 types :

I. *Passive attack* → Made by malicious node to obtain information transacted in the network without disrupting the operation.

II. *Active attack* → They disrupt the operation of network.

Further active attacks are of 2 types :

1. *External attack*: The active attacks that are executed by nodes outside the network.
2. *Internal attack:* The active attacks that are performed by nodes belonging to the same network.

The major security threats that exist in ad hoc wireless networks are as follows :

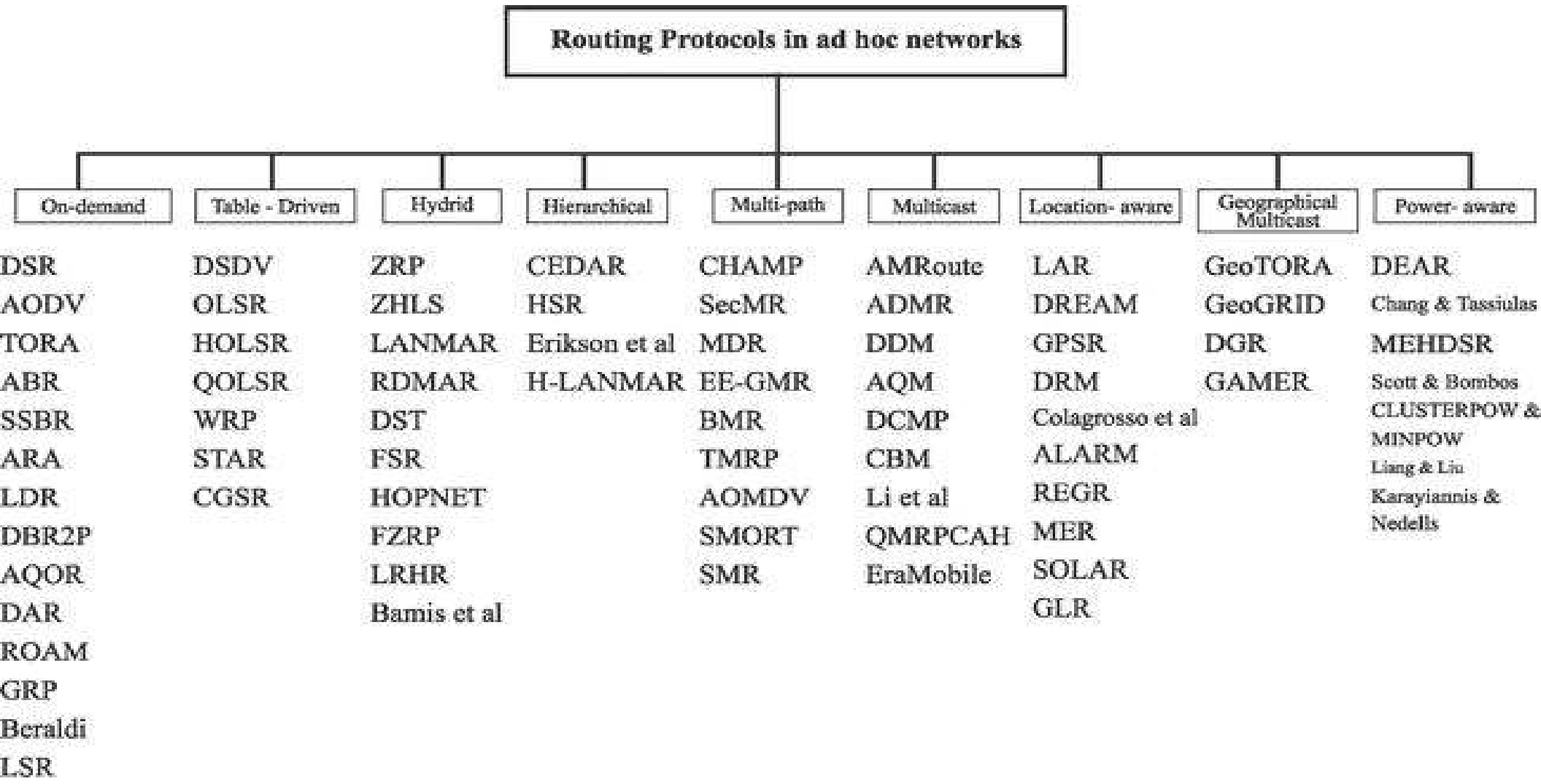
- ***Denial of service***
  - ➢ The attack affected by making the network resource unavailable for service to other nodes, either by consuming the bandwidth or by overloading the system.

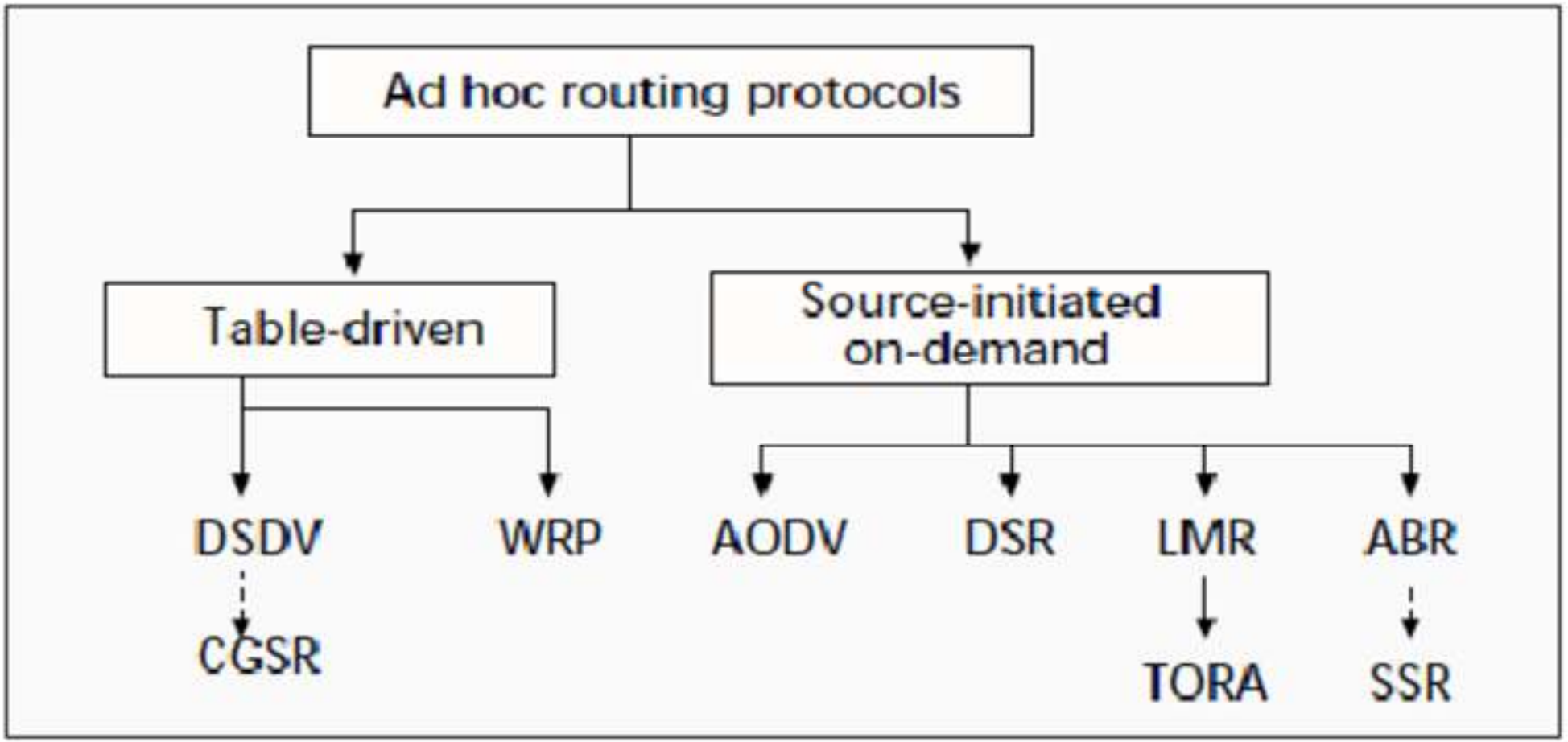
Types of ad-hoc wireless networks

- **Mobile Ad hoc NEtwork** (MANET)
  - involves mobile devices communicating directly with one another
  - a network of wireless mobile devices without an infrastructure
  - self-organizing and self-configuring
  - sometimes referred to as an "on-the-fly" or "spontaneous network."
- **Internet-based Mobile Ad hoc NEtworks** (iMANETs)
  - support internet protocols, such as TCP/IP and UDP
  - iMANET employs a network-layer routing protocol to connect mobile nodes
  - set up distributed routes automatically

Types of ad-hoc wireless networks…

- **Smartphone Ad hoc NEtworks** (SPANs)
  - employ existing hardware, such as Wi-Fi and Bluetooth
  - software (protocols) used in smartphones to create peer-to-peer (P2P) networks
  - does not rely on cellular carrier networks, wireless access points or traditional network infrastructure.
  - support multihop communication
- **Vehicular Ad hoc Network** (VANET)
  - communication between vehicles and roadside equipment
  - consists of groups of moving or stationary vehicles connected by a wireless network


Routing Protocols in ad hoc networks
On-demand
Table - Driven
Hydrid
Hierarchical
Multi-path
Multicast
Location- aware
Geographical Multicast
Power- aware
DSR
AODV
TORA
ABR
SSBR
ARA
LDR
DBR2P
AQOR
DAR
ROAM
GRP
Beraldi
LSR
DSDV
OLSR
HOLSR
QOLSR
WRP
STAR
CGSR
ZRP
ZHLS
LANMAR
RDMAR
DST
FSR
HOPNET
FZRP
LRHR
Bamis et al
CEDAR
HSR
Erikson et al
H-LANMAR
CHAMP
SecMR
MDR
EE-GMR
BMR
TMRP
AOMDV
SMORT
SMR
AMRoute
ADMR
DDM
AQM
DCMP
CBM
Li et al
QMRPCAH
EraMobile
LAR
DREAM
GPSR
DRM
Colagrosso et al
ALARM
REGR
MER
SOLAR
GLR
GeoTORA
GeoGRID
DGR
GAMER
DEAR
Chang & Tassiulas
MEHDSR
Scott & Bombos
CLUSTERPOW & MINPOW
Liang & Liu
Karayiannis & Nedells


Ad hoc routing protocols
Table-driven
Source-initiated on-demand
DSDV
WRP
AODV
DSR
LMR
ABR
CGSR
TORA
SSR

Issues in Designing Routing Protocol for Ad hoc network

- Mobility
- Distributed operation
- Synchronization
- Hidden terminal
- Access delay
- Fairness
- Resource reservation
- Capability of power control

Classification of routing protocols

***Routing protocols for ad-hoc wireless networks can be classified based on*:**

- routing information update mechanism:

  Proactive, Reactive, Hybrid
- usage of temporal information (e.g. cached routes):

  Past temporal , Future temporal
- usage of topology information:

  Flat, Hierarchical
- usage of specific resources :

  Power-aware routing

  Geographical information assisted routing

Desired Characteristics of routing protocol

- Fault tolerant Distributed routing , thus reduced control over head
- Adaptive to frequent topology changes
- Route computation and maintenance must involve a minimum number of
- Nodes and minimum connection setup time is desired.
- It must be localized, as global state maintenance involves a huge state
- propagation control overhead.
- It must be loop-free and free from stale routes.

Desired Characteristics of routing protocol …

- The number of packet collisions must be kept to a minimum by limiting
- the number of broadcasts made by each node.
- Quick convergence towards optimal route
- optimal use of bandwidth, computing power, memory, and battery power.
- Every node in the network should try to store stable local topology only
- information regarding the
- Good Quality of Service and to offer support for time-sensitive traffic.

Routing Protocols

- **Proactive protocols**
  - Table Driven protocol
  - Traditional distributed shortest path protocols
  - Maintain routes between every host pair at all times
  - Based on periodic updates; High routing overhead
  - Example: DSDV (destination sequenced distance vector)

- **Reactive protocols**
  - Determine route if and when needed
  - Source initiates route discovery
  - Network topology information is not maintained
  - Example: DSR (dynamic source routing)
    Ad hoc On–demand Distance Vector Routing (AODV)

Routing Protocols

- **Hybrid protocols**
  - Adaptive
  - Combination of proactive and reactive
  - Example : ZRP (zone routing protocol)

- **Hierarchical protocols**
  - choice of proactive and of reactive routing depends on the hierarchic level in which a node resides
  - hierarchy could be based on geographical information or it could be based on hop distance
  - Cluster Based Routing Protocol

Challenges of routing protocols in ad hoc networks

- **Movement of nodes:**
  - Path breaks
  - Partitioning of a network
  - Inability to use protocols developed for fixed network
- **Bandwidth is a scarce resource:**
  - Inability to have full information about topology
  - Control overhead must be minimized
- **Shared broadcast radio channel:**
  - Nodes compete for sending packets
  - Collisions
- **Erroneous transmission medium:**
  - Loss of routing packets

Table driven protocols

- maintain the global topology information in the form of tables at every node
- tables are updated frequently in order to maintain consistent and accurate network state information.
- ***Common advantages and shortcoming of these protocols***:
  - low delay of route setup process: all routes are immediately available;
  - high bandwidth requirements: updates due to link loss leads to high control overhead;
  - low scalability: control overhead is proportional to the number of nodes;
  - high storage requirements: whole table must be in memory.

Examples

- destination sequenced distance vector routing protocol (DSDV);
- wireless routing protocol (WRP); cluster head gateway routing protocol (CGCR).
- source-tree adaptive routing protocol (STAR);

Destination Sequenced Distance Vector (DSDV) routing protocol

- Destination-Sequenced Distance Vector (DSDV) routing protocol is a pro-active, table-driven routing protocol for MANETs
- Developed by Charles E. Perkins and Pravin Bhagwat in 1994
- Enhancement of the Bellman-Ford algorithm where each node maintains:
  - the shortest path to destination
  - the first node on this shortest path
- It uses the hop count as metric in route selection
- routes to all destinations are readily available at every node at all times
- Routing Tables are also exchanged when significant changes in local topology are observed by a node
- No Loop in routing
- Count to infinity problem is avoided

Destination Sequenced Distance Vector (DSDV) routing protocol

- Updating of routing table can be of two types:
  - ***incremental updates***:

    take place when a node does not observe significant changes in a local topology
  - ***full dumps***:

    take place when significant changes of local topology are observed;
- The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology
- Every node has a single entry in the routing table. The entry will have information about the node's IP address, last known sequence number and the hop count to reach that node
- the next hop neighbor to reach the destination node, the timestamp of the last update received for that node is also available at the node

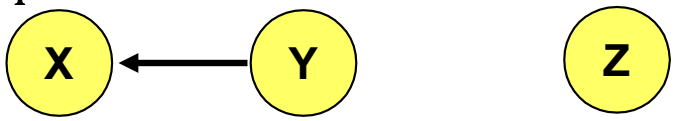
Destination Sequenced Distance Vector (DSDV) routing protocol…

The reconfiguration of path (used for ongoing data transfer) is done as follows:

- the end node of the broken link sends a table update message with:
  - broken link's weight assigned to ***infinity***
  - sequence number greater than the stored sequence number for that destination
- each node re-sends this message to its neighbors to propagate the broken link to the network
- even sequence number is generated by end node, odd by all other nodes
- Note: single link break leads to the propagation of routing table updates through the whole network

Destination Sequenced Distance Vector (DSDV) routing protocol example

- When X receives information from Y about a route to Z
- Let destination sequence number for Z at X be S(X), S(Y) is sent from Y



- If S(X) > S(Y), then X ignores the routing information received from Y
- If S(X) = S(Y), and cost of going through Y is smaller than the route known to X, then X sets Y as the next hop to Z
- If S(X) < S(Y), then X sets Y as the next hop to Z, and S(X) is updated to equal S(Y)

DSDV Table

- Sequence number originated from destination. Ensures loop freeness.
- Install Time when entry was made (used to delete stale entries from table)
- Stable Data Pointer to a table holding information on how stable a route is. Used to damp fluctuations in network.

Destination	Next hop	Metric	Sequence No.	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	3	C-588	001200	Ptr_C
D	B	4	D-312	001200	Ptr_D

Route Advertisements in DSDV

- ***Advertise to each neighbor own routing information***
  - Destination Address
  - Metric = Number of Hops to Destination
  - Destination Sequence Number

∞

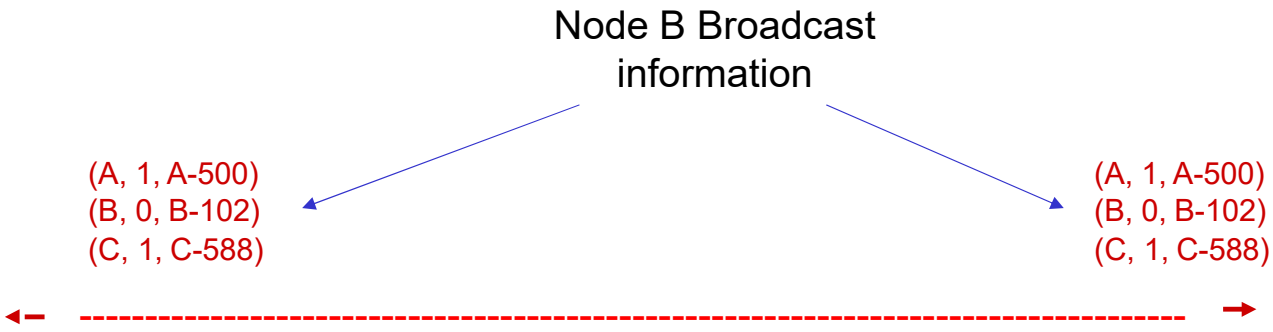
- ***Rules to set sequence number information***
  - On each advertisement increase own destination sequence number (use only even numbers)
  - If a node is no more reachable (timeout) increase sequence number of this node by 1 (odd sequence number) and set metric = ∞

Route Selection in DSDV

❑ ***Update information is compared to own routing table***

- Select route with higher destination sequence number
- Ensure to use always newest information from destination
- Select the route with better metric when sequence numbers are equal

Route Advertisement in DSDV



Node A

Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	2	C-588

Node B

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-100
C	C	1	C-588

Node C

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-100
C	C	0	C-588

Route Advertisement in DSDV

Node A

Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-102
C	B	2	C-588

Node B

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-102
C	C	1	C-588

Node C

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-588

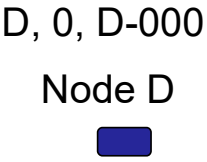
Respond to Topology Changes in DSDV

- **Immediate advertisements**
  - Information on new Routes, broken Links, metric change is immediately propagated to neighbors

- **Full/Incremental Update:**
  - ***Full Update***: Send all routing information from own table
  - ***Incremental Update***: Send only entries that has changed , make it fit into one single packet

New Node addition using DSDV

- Node D broadcast for first time and Send Sequence number D-000
- Node C insert entry for D with sequence number D-000 ,immediately broadcast own table



Node A

Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Node B

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Node C

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-590
D	D	1	D-000

New Node addition using DSDV…

Node A

Dest.	Next	Hop	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Node B

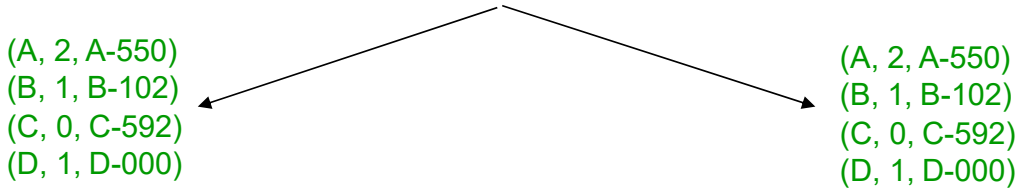
Dest.	Next	Hop	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Node C

Dest.	Next	Hop	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-592
D	D	1	D-000

Node D

Dest.	Next	Hop	Seq.
A	C	3	A-550
B	C	2	B-104
C	C	1	C-592
D	D	0	D-000



New Node addition using DSDV…

Dest.	Next	Hop	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Hop	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-592
D	C	2	D-000

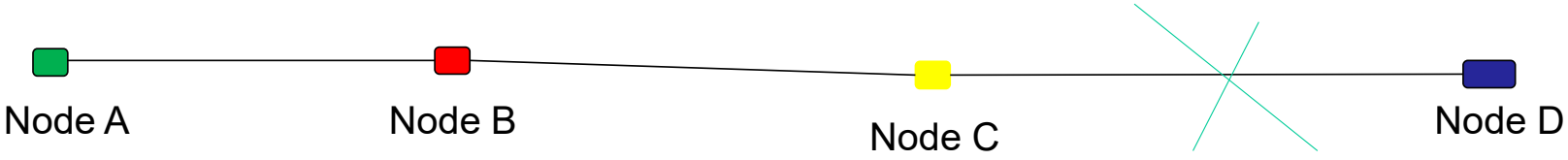
Dest.	Next	Hop	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-592
D	D	1	D-000

Dest.	Next	Hop	Seq.
A	C	3	A-550
B	C	2	B-104
C	C	1	C-592
D	D	0	D-000

(A, 2, A-550)
(B, 1, B-102)
(C, 0, C-592)
(D, 1, D-000)

(A, 2, A-550)
(B, 1, B-102)
(C, 0, C-592)
(D, 1, D-000)

Link Break in ad hoc network



Dest.	Next	Hop	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590
D	B	3	D-100

Dest.	Next	Hop	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-592
D	C	2	D-100

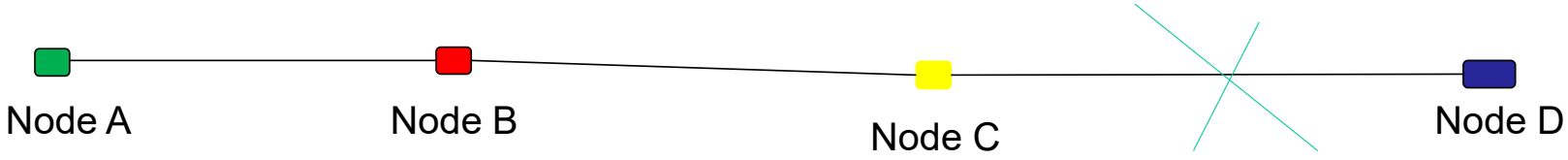
Dest.	Next	Hop	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-592
D	D	∞	D-101

Dest.	Next	Hop	Seq.
A	C	3	A-550
B	C	2	B-104
C	C	1	C-592
D	D	0	D-101

- B does its broadcast thus no impact on C
- C has higher sequence number for destination D
- No loop , no count to infinity on link break

(A, 2, A-550)
(B, 1, B-102)
(C, 0, C-592)
(D ∞, D-101)

Immediate Advertisement in ad hoc network



Dest.	Next	Hop	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590
D	D	∞	D-101

Dest.	Next	Hop	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-592
D	C	∞	D-101

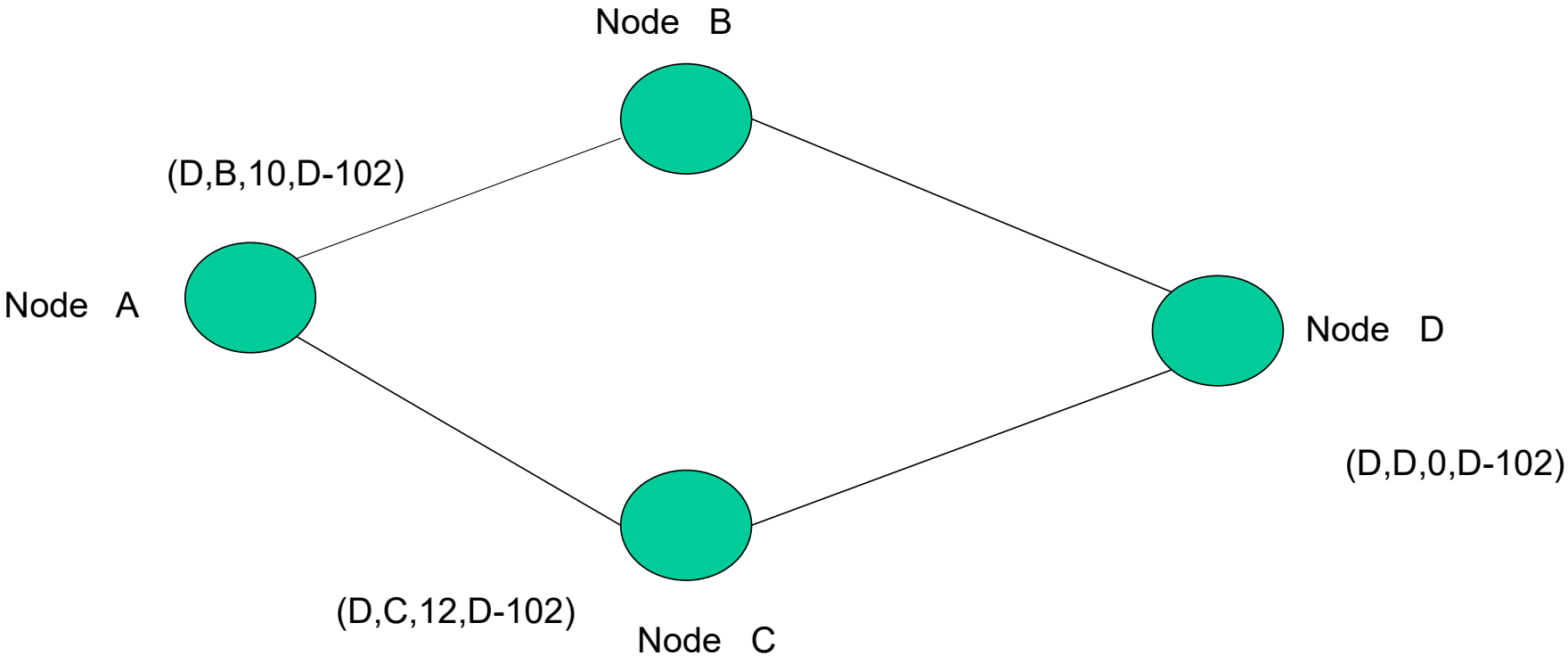
Dest.	Next	Hop	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-592
D	D	∞	D-101

Dest.	Next	Hop	Seq.
A	C	3	A-550
B	C	2	B-104
C	C	1	C-592
D	D	0	D-101

- Node C detects the link break with node D
- Immediate propagation of information to node B, the from node B to node A
- Disconnected node sequence number is changed to odd number

Fluctuations in DSDV

- ***Fluctuations*** occurs when every time node does its broadcast and lead to unnecessary route advertisements in the network



On demand routing protocol

- The route is discovered only when it is required/needed.
- Process of route discovery occurs by flooding the route request packets throughout the mobile network.
  - **Route Discovery:**
    This phase determines the most optimal path for the transmission of data packets between the source and the destination mobile nodes
  - **Route Maintenance:**
    This phase performs the maintenance work of the route as the topology in the mobile ad-hoc network is dynamic in nature

Reactive Routing – Source initiated

- Source floods the network with a *Route Request* packet when a route is not available to the required destination
- Flood is propagated outwards from the source
- Pure flooding = every node transmits the request only once
- Destination send the *Route reply* to *Route Request*
- Reply uses reversed path of *Route Request*
- sets up the forward path

Advantages & disadvantages of Reactive routing protocol

Advantages:

- eliminate periodic updates
- adaptive to network dynamics

Disadvantages:

- high flood-search overhead with mobility,
- distributed traffic
- high route acquisition latency

Ad-Hoc On Demand Vector Routing protocol (AODV)

- Reactive or On-demand routing protocol
- In AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission
- AODV supports multicasting and unicasting within a uniform framework
- Each route has a lifetime after which the route expires if it is not used
- AODV maintains only one route between a source-destination pair
- Routing table size is minimized by only including next hop information, not the entire route to a destination node.
- Sequence numbers for both destination and source are used.
- Managing the sequence number is the key to efficient routing and route maintenance

Basic Message set of AODV

- Route Request : “I need a route”
- Route Response : “Route advertisement”
- Route Error : “Withdraw route”
- hello : “ Link status monitoring”

Fields of Routing Table in AODV

- Destination IP address
- Destination Sequence Number
- Valid Destination Sequence Number Flag
- Other state and routing flags
- Network Interface
- Hop Count (needed to reach destination)
- Next Hop
- Lifetime (route expiration or deletion time)

Route Establishment in AODV

- Uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination.
- A node updates its path information only if the DestSeqNum of the current packet received is ***greater*** than the last DestSeqNum stored at the node.
- A *RouteRequest* consist of following fields:

  source identifier (SrcID),

  destination identifier(DestID),

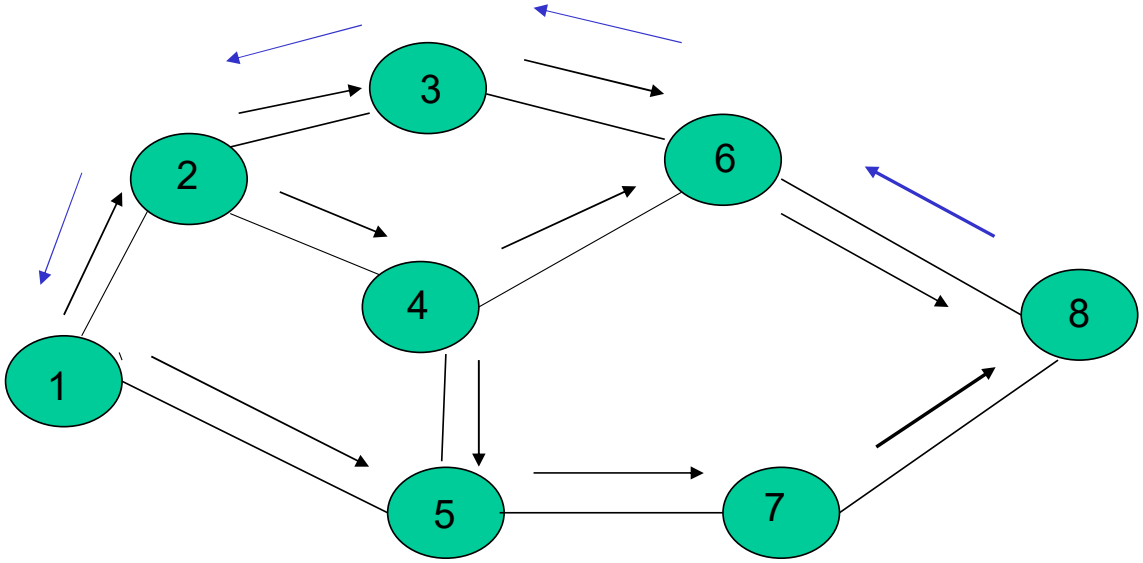
  source sequence number (SrcSeqNum)

  destination sequence number (DestSeqNum)

  broadcast identifier (BcastID),

  time to live (TTL)

Route Establishment in AODV…



RouteRequest

RouteReply

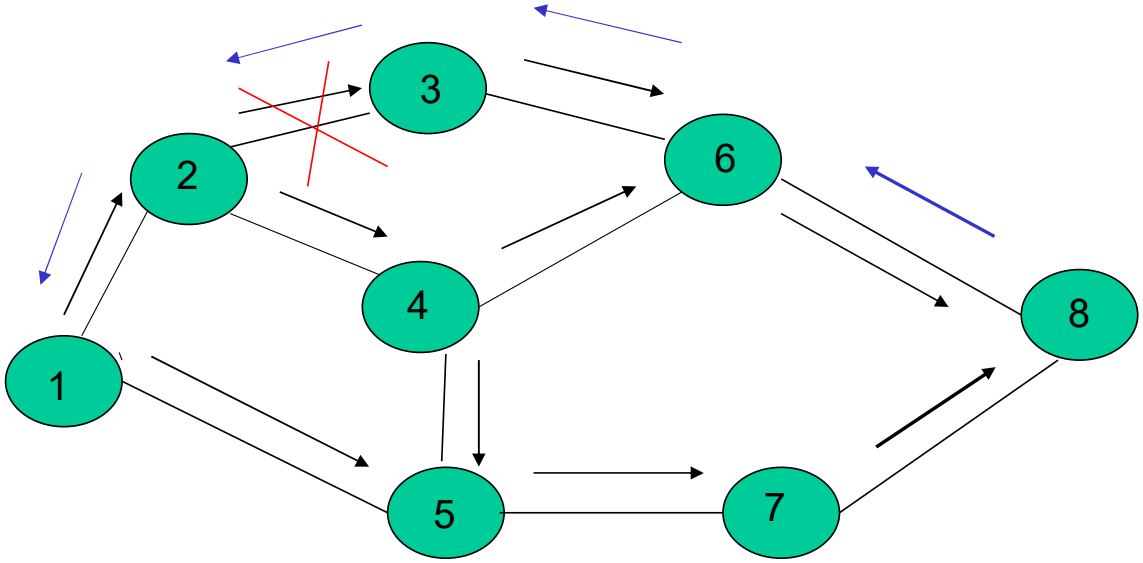
Network link

Node No.	1	2	3	4	5	6	7	8
DestSeqNum	4	10	6	3	2`	8	3	12

Route Maintenance in AODV

- BcastID-SrcID pair, indicates the multiple occurrence of RouteRequest then the duplicate copies are discarded
- If a ***path break*** is detected at an intermediate node, the node informs the end nodes by sending an unsolicited *RouteReply* with the ***hop count*** set as ∞.
- When a path breaks, between any two nodes both the nodes initiate *RouteError* messages to inform their end nodes about the link break
- The end nodes delete the corresponding entries from their tables. The source node reinitiates the pathfinding process with the new BcastID

Route Maintenance in AODV



RouteRequest

RouteReply

Network link

Node No.	1	2	3	4	5	6	7	8
DestSeqNum	4	10	6	3	2`	8	3	10

Advantages & Disadvantages of AODV

Advantages

- routes are established on demand and destination sequence numbers are used to find the latest route to the destination
- The connection setup delay is less

Disadvantages

- intermediate nodes can lead to inconsistent routes if the source sequence number is very old
- multiple *RouteReply* packets in response to a single *RouteRequest* packet can lead to heavy control overhead.
- periodic *beacon*ing leads to unnecessary bandwidth consumption.

Reference

C. Siva Ram Murthy and B. S. Manoj, ―Ad Hoc Wireless Networks Architectures and Protocols‖, Prentice Hall, PTR, 2004.

Thank You

EC8702- SENSOR NETWORKS - INTRODUCTION & ARCHITECTURE

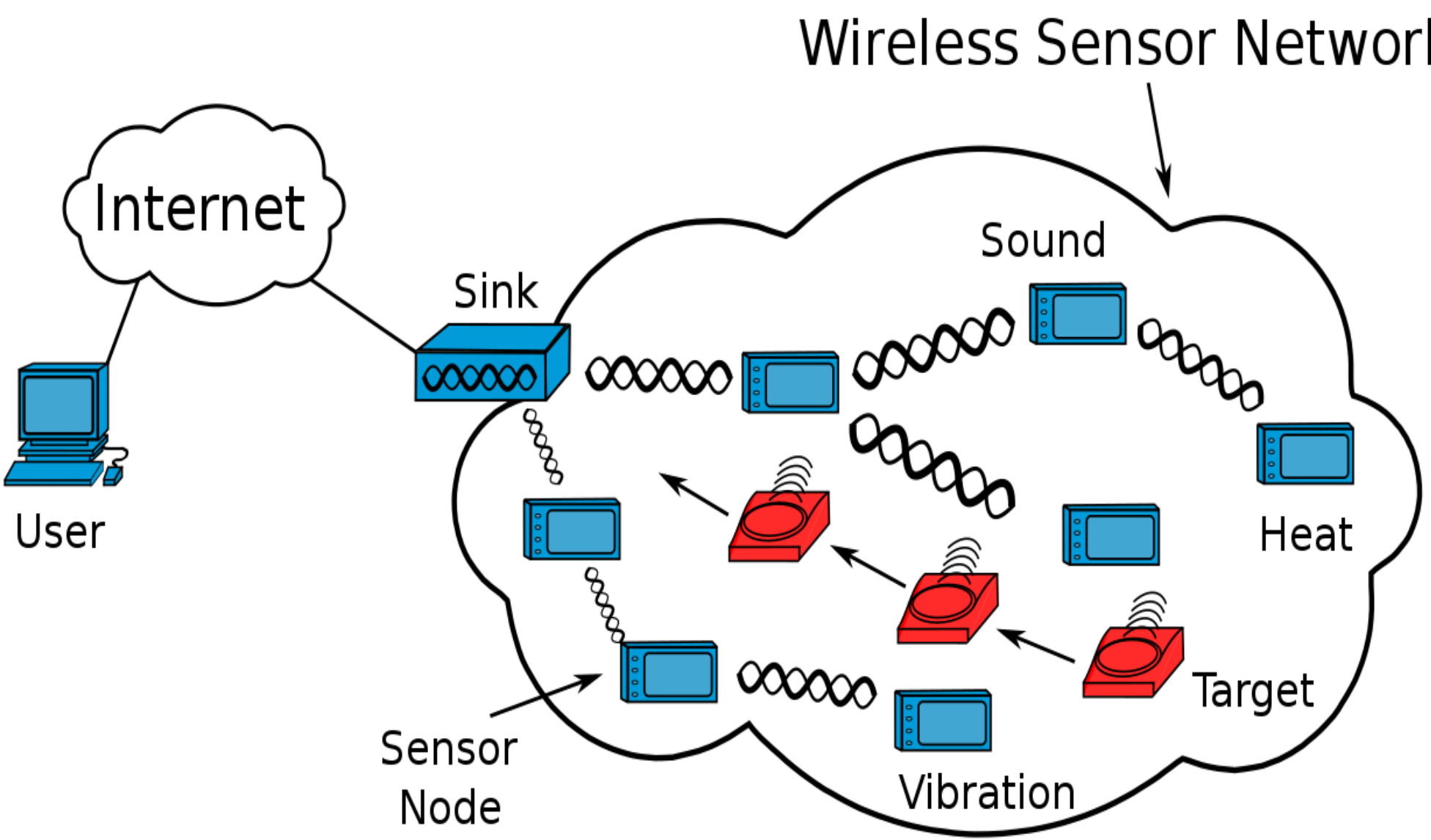
Mr.M.Kamarajan,
AP/ECE/MSAJCE

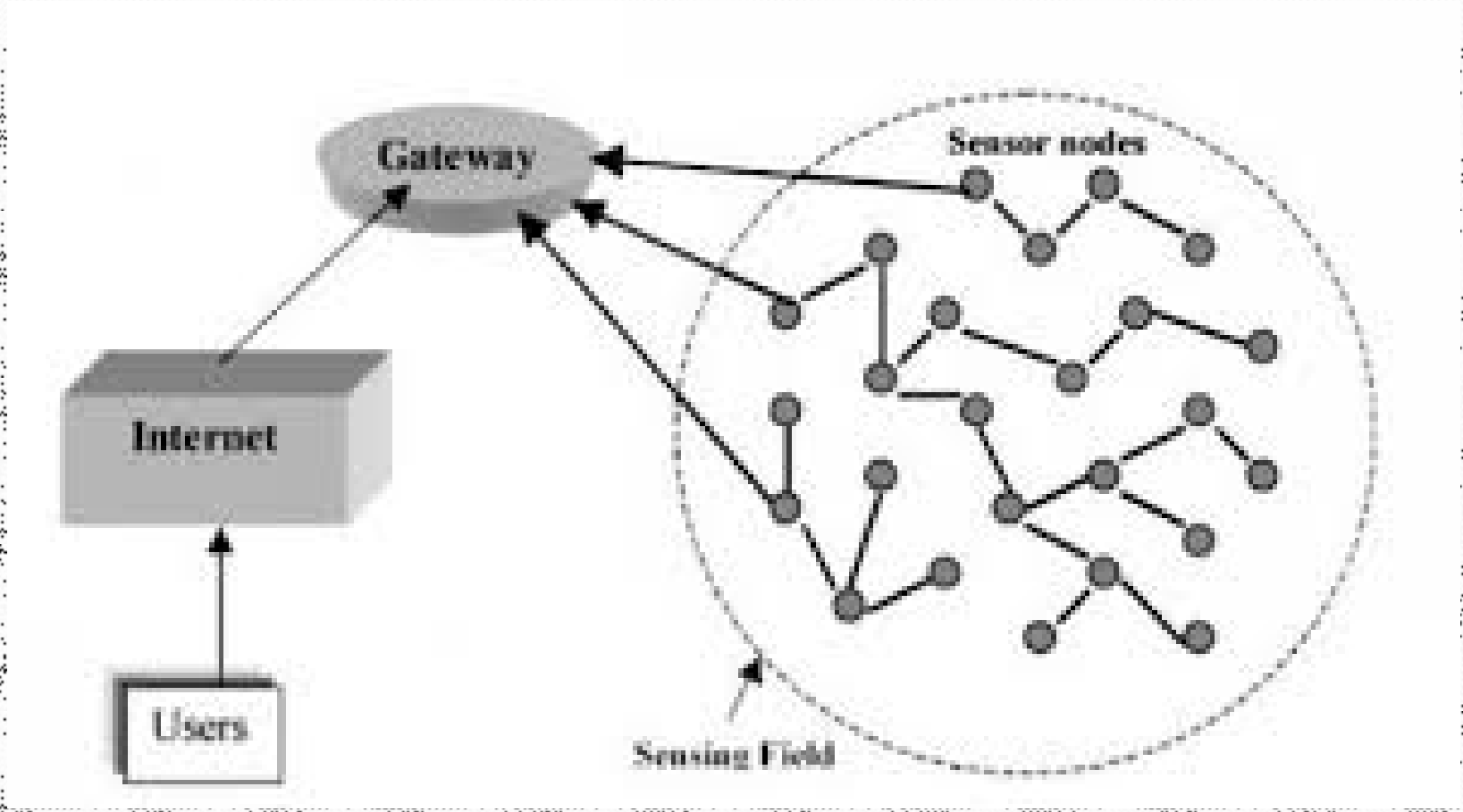
What is WSN?

Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location

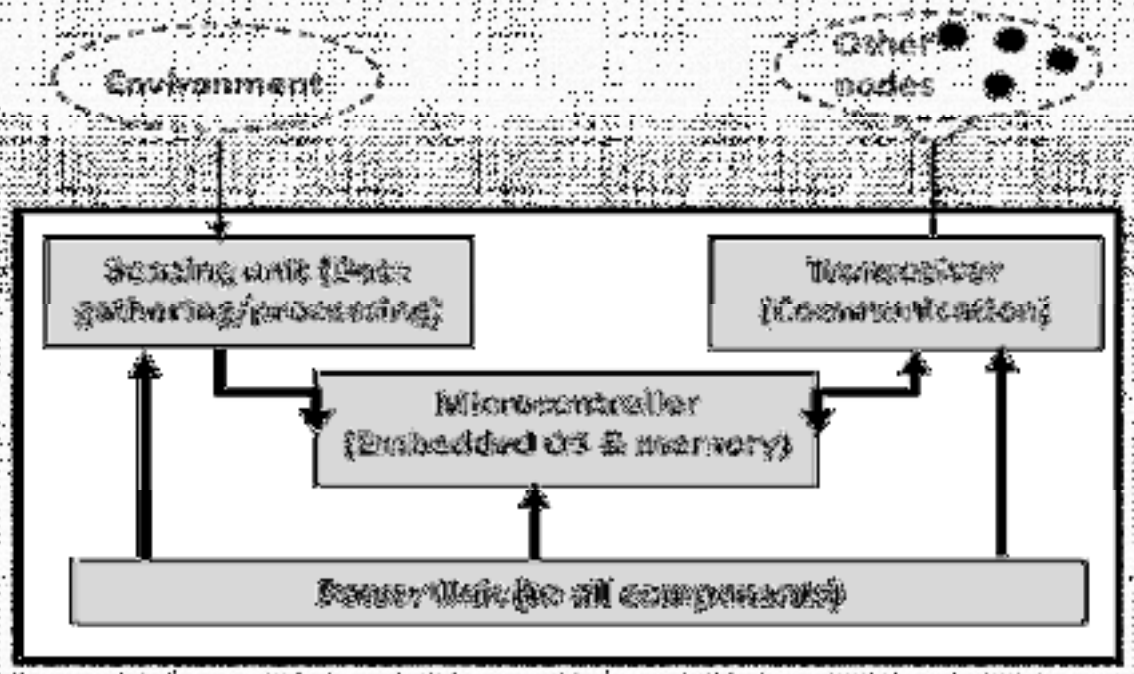
These are similar to wireless ad hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. WSNs are spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc\

WSN is a wireless network that consists of base stations and numbers of nodes (wireless sensors). These networks are used to monitor physical or environmental conditions like sound, pressure, temperature, and co-operatively pass data through the network to the main location


Wireless Sensor Network
Internet
Sink
User
Sound
Heat
Target
Vibration
Sensor
Node


Gateway
Sensor nodes
Internet
Users
Sensing Field

WSN **Sensors** are equipped with sensing, limited computation, and wireless communication capabilities



Comparison with ad hoc networks

Wireless sensor networks mainly use **broadcast** communication while ad hoc networks use **point-to-point** communication.

Unlike ad hoc networks wireless sensor networks are **limited by sensors** limited power, energy and computational capability.

Sensor nodes may **not have global ID** because of the large amount of overhead and large number of sensors.

ACTUATORS

1. **Passive, omni-directional sensors:**
   - Measure a physical quantity without actually manipulating the environment by active probing
   - No notion of "direction" involved in these measurements and may be self powered

   Eg: thermometer, light sensors, vibration, microphones, humidity, mechanical stress or tension in materials, chemical sensors sensitive, smoke detectors, air pressure, etc
2. **Passive, narrow-beam sensors:**
   - Are passive
   - Have a well-defined notion of direction of measurement.
   - Eg: Camera
3. **Active sensors:**
   - Actively probes the environment
   - Eg: a sonar or radar sensor or some types of seismic sensors

- **Actuators:**
  - Are as diverse as sensors
  - Usually are controlled by sensors and in turn trigger some function or device

WSNs Applications

- WSNs have many advantages over traditional networking techniques.

- They have an ever-increasing number of applications, such as infrastructure protection and security, surveillance, health-care, environment monitoring, food safety, intelligent transportation, and smart energy.

WSNs Applications

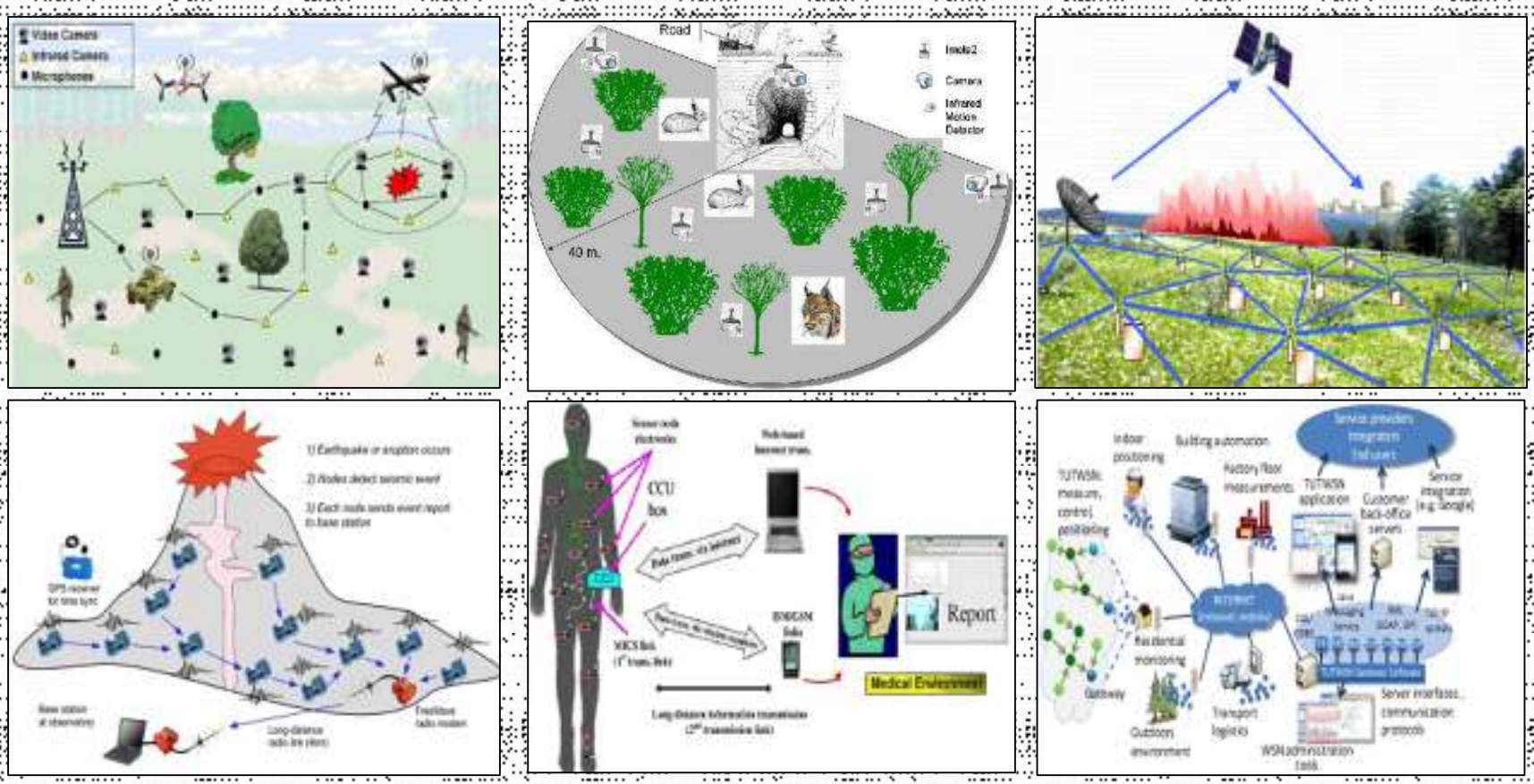


Figure : WSNs Applications

Applications of Wireless Sensor networks

The applications can be divided in three categories:

1. Monitoring of objects.
2. Monitoring of an area.
3. Monitoring of both area and objects.

Monitoring Area

- Environmental and Habitat Monitoring
- Precision Agriculture
- Indoor Climate Control
- Military Surveillance
- Treaty Verification
- Intelligent Alarms

Characteristics of Wireless Sensor Networks

Wireless Sensor Networks mainly consists of **sensors.**
Sensors are -

- low power
- limited memory
- energy constrained due to their small size.

Wireless networks can also be deployed in **extreme environmental** conditions and may be prone to enemy attacks.

Although deployed in an ad hoc manner they need to be **self organized** and **self healing** and can face constant reconfiguration.

CHALLENGES FOR WSNs

(i) Characteristic requirements

- TYPE OF SERVICE
- QUALITY OF SERVICE
- FAULT TOLERANCE:
- LIFE TIME:
- SCALIBILITY:
- WIDE RANGE OF DENSITIES
- PROGRAMMABILITY
- MAINTAINABILITY

(ii) Required mechanisms

- Multihop wireless communication
- Energy-efficient operation
- Auto-configuration
- Collaboration and in-network processing
- Data centric
- Locality
- Exploit trade-offs

CHALLENGES FOR WSNs

- **TYPE OF SERVICE:** Provide meaningful information and actions about a given task, hence new paradigms of using such a network are required.
- **QUALITY OF SERVICE:** Packet delivery ratio is an insufficient. Adapted concepts like reliable detection of events or the approximation of quality is important.
- **FAULT TOLERANCE:** Nodes should be damage and failure tolerant.
- **LIFE TIME:** WSN nodes rely on a limited supply of energy(batteries). Replacing these energy sources in the field is not practical, hence life time of WSN becomes important figure of merit.

The lifetime of a network also has direct trade-offs against quality of service: investing more energy can increase quality but decrease lifetime. Concepts to harmonize these trade-offs are required.

CHALLENGES FOR WSNs

SCALIBILITY: Protocols used must be able to support large no. of nodes, the employed architectures and protocols must be able scale to these numbers.

- **WIDE RANGE OF DENSITIES:**

Density of network: No. of nodes per unit area– the *density of the network* – can vary considerably. & it vary with applications. Density can vary over time and space because nodes fail or move; the density also does not have to homogeneous in the entire network and the network should adapt to such variations.

- **PROGRAMMABILITY:** Nodes should be programmable, and their programming must be changeable during operation when new tasks become important. So it should be flexibility on changing tasks

- **MAINTAINABILITY:** Environment of a WSN and the WSN itself change, the system has to adapt. Has to maintain itself; able to interact with external maintenance mechanisms.

CHALLENGES FOR WSNs

Required mechanisms

To realize these requirements, innovative mechanisms for a communication network have to be found, as well as new architectures, and protocol concepts

- **Multihop wireless communication**
- **Energy-efficient operation**
- **Auto-configuration**
- **Collaboration and in-network processing**
- **Data centric**
- **Locality**
- **Exploit trade-offs**

Design Challenges

Heterogeneity

The devices deployed maybe of various types and need to collaborate with each other.

Distributed Processing

The algorithms need to be centralized as the processing is carried out on different nodes.

Low Bandwidth Communication

The data should be transferred efficiently between sensors

Continued..

Large Scale Coordination

The sensors need to coordinate with each other to produce required results.

Utilization of Sensors

The sensors should be utilized in a ways that produce the maximum performance and use less energy.

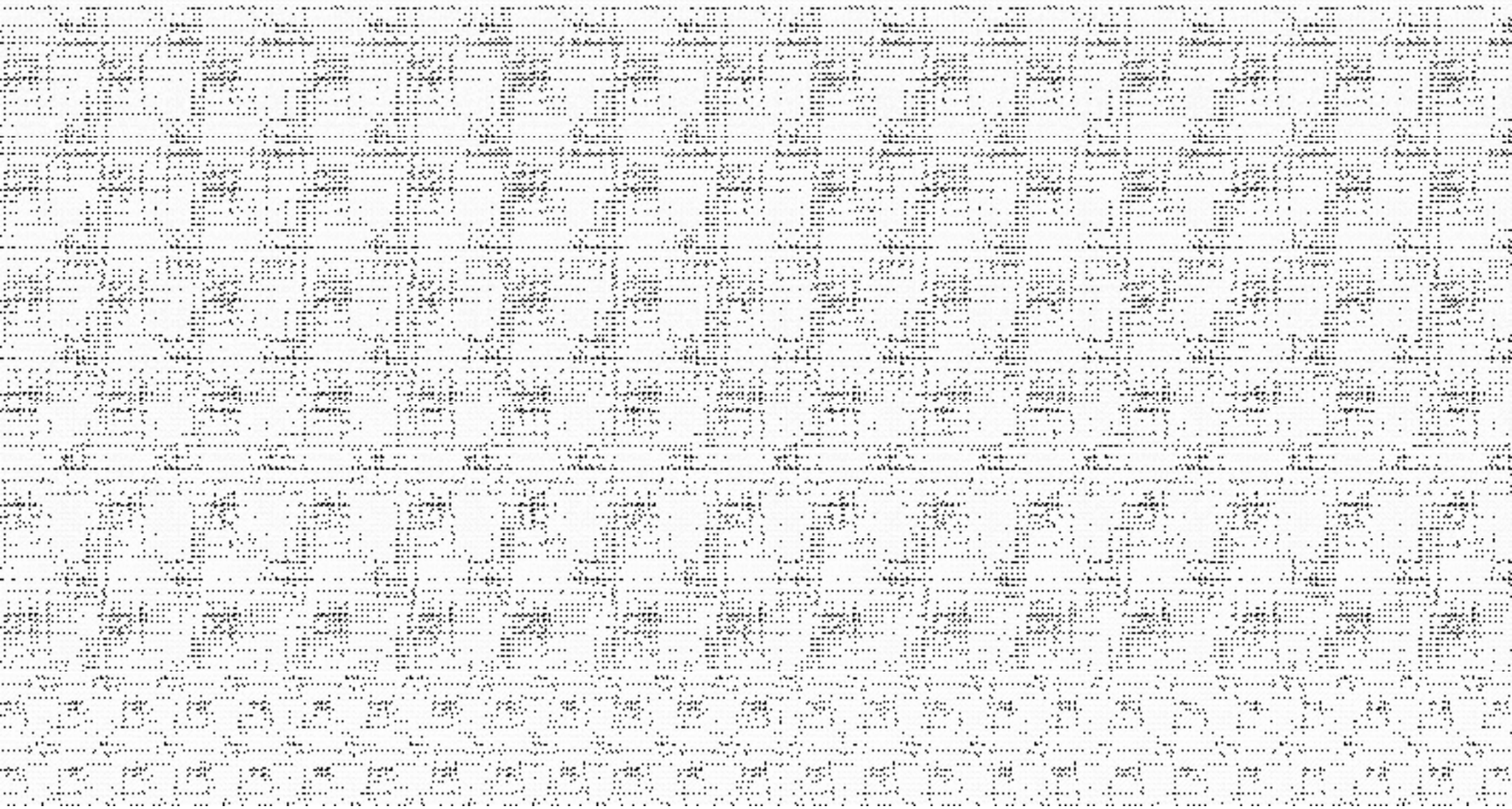
Real Time Computation

The computation should be done quickly as new data is always being generated.

Operational Challenges of Wireless Sensor Networks

- Energy Efficiency
- Limited storage and computation
- Low bandwidth and high error rates
- Errors are common
  - Wireless communication
  - Noisy measurements
  - Node failure are expected
- Scalability to a large number of sensor nodes
- Survivability in harsh environments
- Experiments are time- and space-intensive

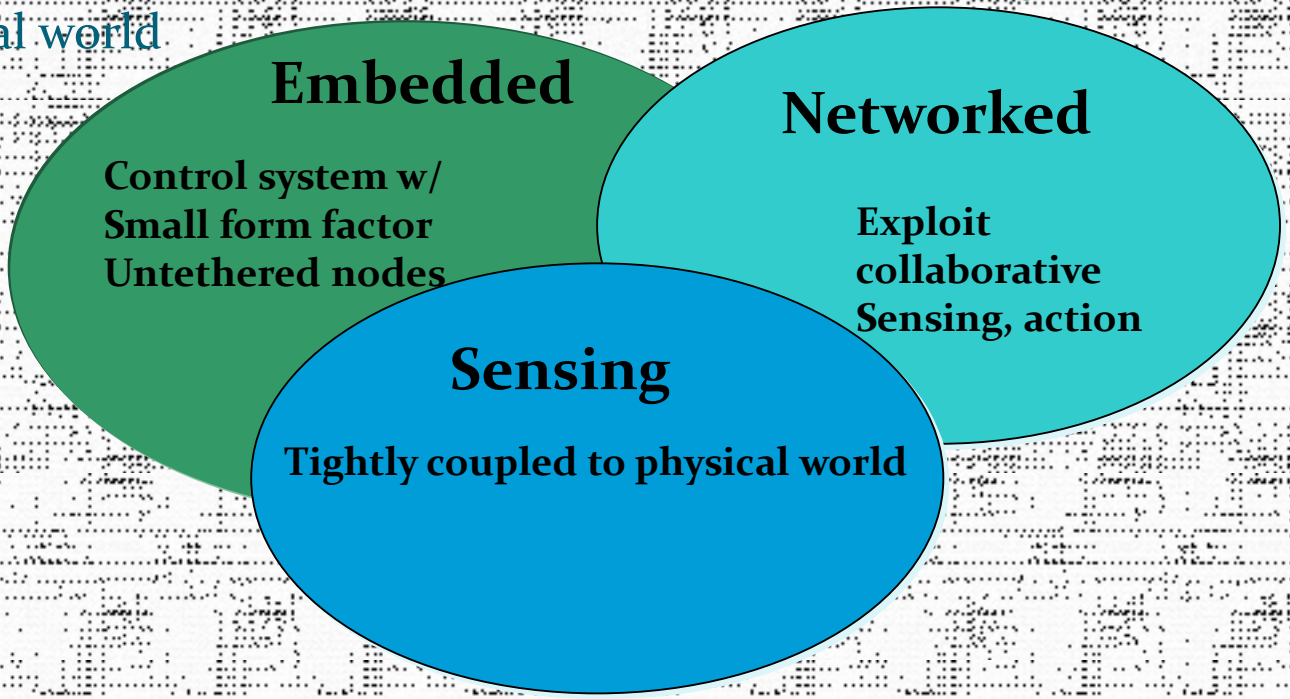
Difference Between MANET and WSN (Book page No 10)



Enabling Technologies (Book Page No 16)

Embed numerous distributed devices to monitor and interact with physical world

Network devices to coordinate and perform higher-level tasks



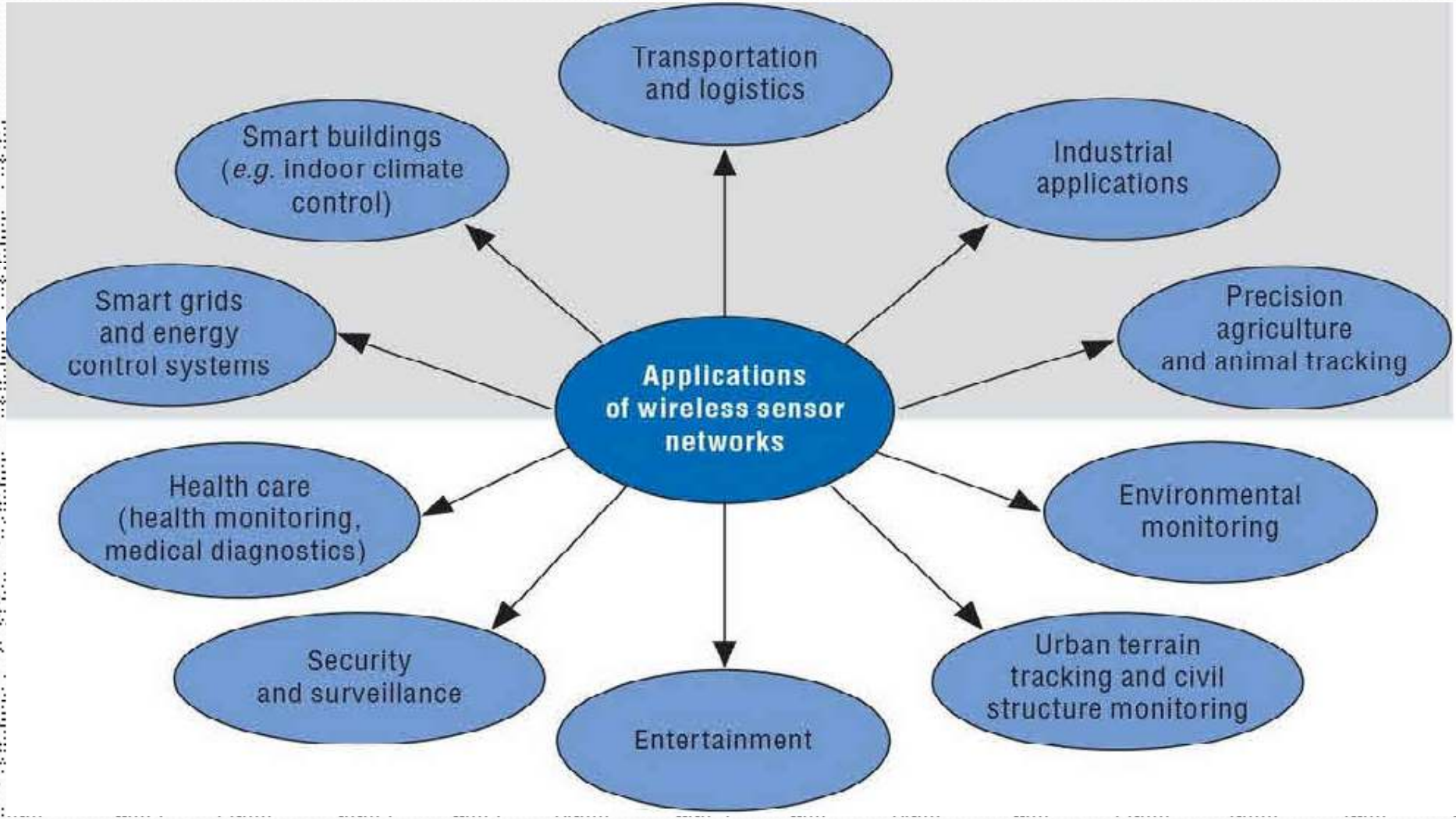
Exploit spatially and temporally dense, in situ, sensing and actuation

ENABLING TECHNOLOGIES FOR WSNs

1) Miniaturization of hardware
2) Reduced chip size & improved efficiency accompanied by reduced cost
3) The actual sensing element

These 3 parts have to be accompanied by power supply. This requires, depending on application, high capacity batteries that last for long times, that is, have only a negligible self-discharge rate, and that can efficiently provide small amounts of current

A sensor node has a device *energy scavenging.*


Transportation and logistics
Smart buildings (*e.g.* indoor climate control)
Industrial applications
Smart grids and energy control systems
Precision agriculture and animal tracking
Applications of wireless sensor networks
Health care (health monitoring, medical diagnostics)
Environmental monitoring
Security and surveillance
Urban terrain tracking and civil structure monitoring
Entertainment

Application Examples

- **DISASTER RELIEF APPLICATIONS**: Wildfire, sensors produce a "temperature map" of the area.
- **ENVIRONMENT CONTROL AND BIODIVERSITY MAPPING:** Chemical pollutants, surveillance of the marine ground floor and survey on no. of plant and animal species that live in a particular habitat.
- **INTELLIGENT BUILDINGS:** monitoring of temperature, airflow, humidity and other physical parameters in a building - reduce energy consumption. Also mechanical stress levels of buildings.

Application Examples

- **MACHINE SURVEILLANCE & PREVENTIVE MAINTANANCE:** Sensor nodes are fixed at difficult-to-reach areas of machinery to detect vibration patterns.
- **FACILITY MANAGEMENT:** Detection of intruders, tracking vehicle's position, scanning chemical leakage in chemical plants.
- **PRECISION AGRICULTURE:** Fertilizing by placing humidity/soil composition sensors into fields. Also pest control, livestock breeding can be improved.

Application Examples

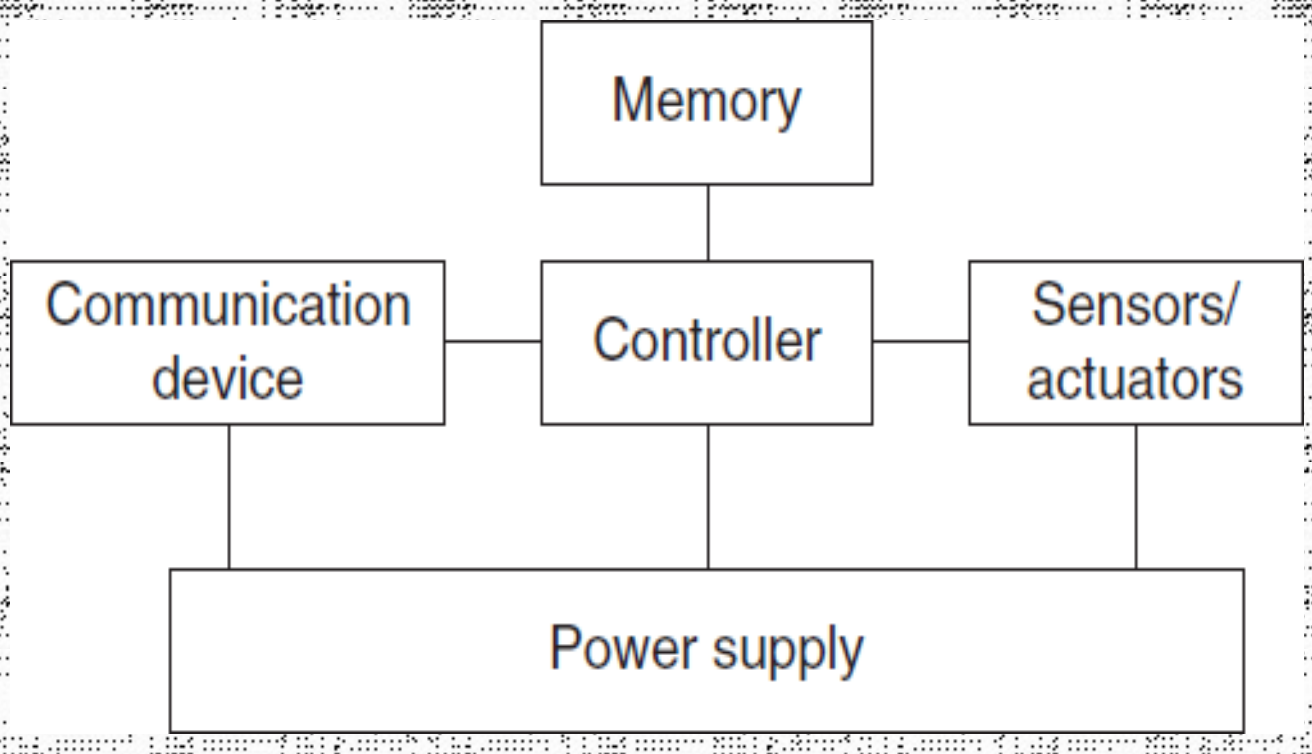
- **MEDICINE & HEALTH CARE:** Long-term surveillance of patients and automatic drug administration. Also used in patient-doctor tracking system.
- **LOGISTICS:** Used for simple tracking of goods during transportation or to facilitate inventory tracking in stores and warehouses.
- **TELEMATICS:** Used to gather information about traffic conditions at a higher resolution(intelligent roadside)

Single-Node Architecture

Hardware Components

- Sensor node hardware overview
- Controller(Microcontrollers versus microprocessors, FPGAs, and ASICs)
- Memory
- Communication device
- Sensors and actuators
- Power supply of sensor nodes

Sensor Node Hardware Components



Five main components of basic sensor node

Controller A controller to process all the relevant data, capable of executing arbitrary code.

Memory Some memory to store programs and intermediate data; usually, different types of memory are used for programs and data.

Sensors and actuators The actual interface to the physical world: devices that can observe or control physical parameters of the environment.

Communication Turning nodes into a network requires a device for sending and receiving information over a wireless channel

Power supply As usually no tethered power supply is available, some form of batteries are necessary to provide energy. Sometimes, some form of recharging by obtaining energy from the environment is available as well (e.g. solar cells).

CONTROLLER

- Collects data from the sensors, processes the data, decides when and where to send it, receives data from other sensor nodes, and decides on the actuator's behaviour.
- Executes various programs, ranging from time-critical signal processing and communication protocols to application programs.
- Microcontrollers, microprocessors, FPGAs, and ASICs can be used as controllers

CONTROLLER

- **Microcontroller:**
  - Flexible in connecting with other devices (like sensors)
  - Instruction set amenable to time-critical signal processing
  - Low power consumption
  - Built in memory
  - Freely programmable
  - Can reduce power consumption by going to sleep state
  - No memory management unit, hence reduced memory functionality.
- **Digital Signal Processors (DSP):**
  - Specialized programmable processors
  - Highly useful in signal processing applications
  - In WSN DSP can be used to process data coming from a simple analog, wireless communication device to extract a digital data stream.
  - But in WSN signal processing functions are not overly complicated.

CONTROLLER

- **Field-Programmable Gate Arrays (FPGAs)**
  - Can be easily reprogrammed to changing environment
  - Consumes more time and energy compared to μC
  - **Application Specific Integrated Circuits (ASICs)**
  - Specialized processor.
  - Trade off between flexibility and energy efficiency & performance.
  - A microcontroller requires software development, ASICs provide the same functionality in hardware, resulting in potentially more costly hardware development.
- Hence microcontrollers are more suitable for WSNs
- Eg. Microcontrollers: Intel StrongARM, Texas Instruments MSP 430 and Atmel ATmega

MEMORY

- **Random Access Memory (RAM):**
  - Store intermediate sensor readings, packets from other nodes
  - Comparatively faster
  - Volatile in nature
- **Read-only Memory (ROM) or Electrically Erasable Programmable Read-only Memory (EEPROM):**
  - Store program code
- **Flash Memory:**
  - Allows data to be erased or written in blocks instead of only a byte at a time
  - Serve as intermediate storage of data in case RAM is insufficient or when the power supply of RAM should be shut down for some time
  - Longer delay and more consumption of energy

COMMUNICATION DEVICE

- Used to exchange data between individualnodes.

- **Choice of transmission medium**
  - There are different mediums for wireless communication. Usual choice includes are,
    - Radio frequencies
    - Optical communication
    - Ultrasound
    - Magnetic inductance- used very specific cases
  - **RF-based Communication :**
    - Most suitable for WSN applications; since it provides
      - Relatively long range and high data rates
        - Acceptable error rates at reasonable energy expenditure and
        - No line of sight between sender and receiver required
    - Frequencies used: between about 433 MHz and 2.4 GHz

COMMUNICATION DEVICE

- **TRANSCEIVERS:**

For actual communication, both a transmitter and a receiver are required in a sensor node. The essential task is to convert a bit stream coming from a microcontroller (or a sequence of bytes or frames) and convert them to and from radio waves

- Device capable of doing both transmission and reception.
- But usually, only half duplex operation is realized.
- **Transceiver tasks and characteristics**

1.Service to upper layer:

- Offer certain services to the upper layers, most notably to the Medium Access Control (MAC) layer.

The service is mostly packet oriented. sometimes, a transceiver only provides a **byte interface or even only a bit interface to the** microcontroller

In any case, the transceiver must provide an interface that somehow allows the MAC layer to initiate frame transmissions and to hand over the packet from, say, the main memory of the sensor node into the transceiver (or a byte or a bit stream, with additional processing required on the microcontroller).

2. Power consumption and energy efficiency:

Energy efficiency is the energy required to transmit and receive a single bit.

- Transceivers should be switchable between different states
  (Eg. Idle, sleep and active).

COMMUNICATION DEVICE

3.Carrier frequency and multiple channels

- Transceivers are available for different carrier frequencies.

Some provides several carrier frequencies (“channels”). for example, for certain MAC protocols (FDMA or multichannel CSMA/ ALOHA techniques

4.State change times and energy:

- Transceiver can operate in different modes: sending or receiving, use different channels, or be in different power-safe states.
- Important figures of merit are the time and the energy required to change between two states.

5.Data rates:

The gross data rateis determined by carrier frequency and used bandwidth together with modulation and coding. Typical values are a few tens of kilobits per second – considerably less than in broadband wireless communication, but usually sufficient for WSNs. Different data rates can be achieved, for example, by using different modulations or changing the symbol rate

6.Modulations

COMMUNICATION DEVICE

- Transceivers can support one or several of on/off-keying (ASK, FSK etc.)

7.Coding: Some transceivers allow various coding schemes to be selected.

Transmission power control - Some transceivers can directly provide control over the transmission power to be used; some require some external circuitry for that purpose. Maximum output power is usually determined by regulations.

9.Noise figure: The **noise figure NF of an element is defined as the ratio of the Signal-to-Noise** Ratio (SNR) ratio SNR*I at the input of the element to the SNR ratio SNRO at the element's* output:

$$NF = SNR_I / SNR_O$$

It describes the degradation of SNR due to the element's operation and is typically given in dB: $NF\ dB = SNR_I\ dB - SNR_O\ dB$

10.Gain:

- Ratio of the output signal power to the input signal power
- Expressed in dB

COMMUNICATION DEVICE

11. Power efficiency

- **Efficiency of radio front end:** Ratio of the radiated power to the overall power consumed by the front end.
- **Efficiency of power amplifier:** Ratio of the output signal's power to the power consumed by the overall power amplifier.

12. Receiver sensitivity (given in dBm):

- The minimum signal power at the receiver needed to achieve a prescribed E_b/N_0 or a prescribed bit/packet error rate.

13. Out of band emission:

- The inverse to adjacent channel suppression is the out of band emission of a transmitter.

14. **Range:**

- It is considered in absence of interference
- It depends on:
  - the transmission power
  - the antenna characteristics
  - the attenuation caused by the environment
  - the used carrier frequency
  - the modulation/coding scheme that is used
  - the bit error rate that one is willing to accept at the receiver
  - the quality of the receiver- sensitivity.

15. **Frequency stability:**

- Variation of center frequencies when environmental conditions of oscillators like temperature or pressure varies. In extreme cases, poor frequency stability can break down communication links

COMMUNICATION DEVICE

16. Blocking performance:

- Achieved bit error rate in the presence of an interferer.

17. Carrier sense and RSSI:

- To sense whether the wireless channel, the carrier, is busy (another node is transmitting).
- **RSSI** (Received Signal Strength Indicator): The signal strength at which an incoming data packet has been received.

18. Voltage range:

Transceivers should operate reliably over a range of supply voltages.

Otherwise, inefficient voltage stabilization circuitry is required.

Transceiver Design Considerations

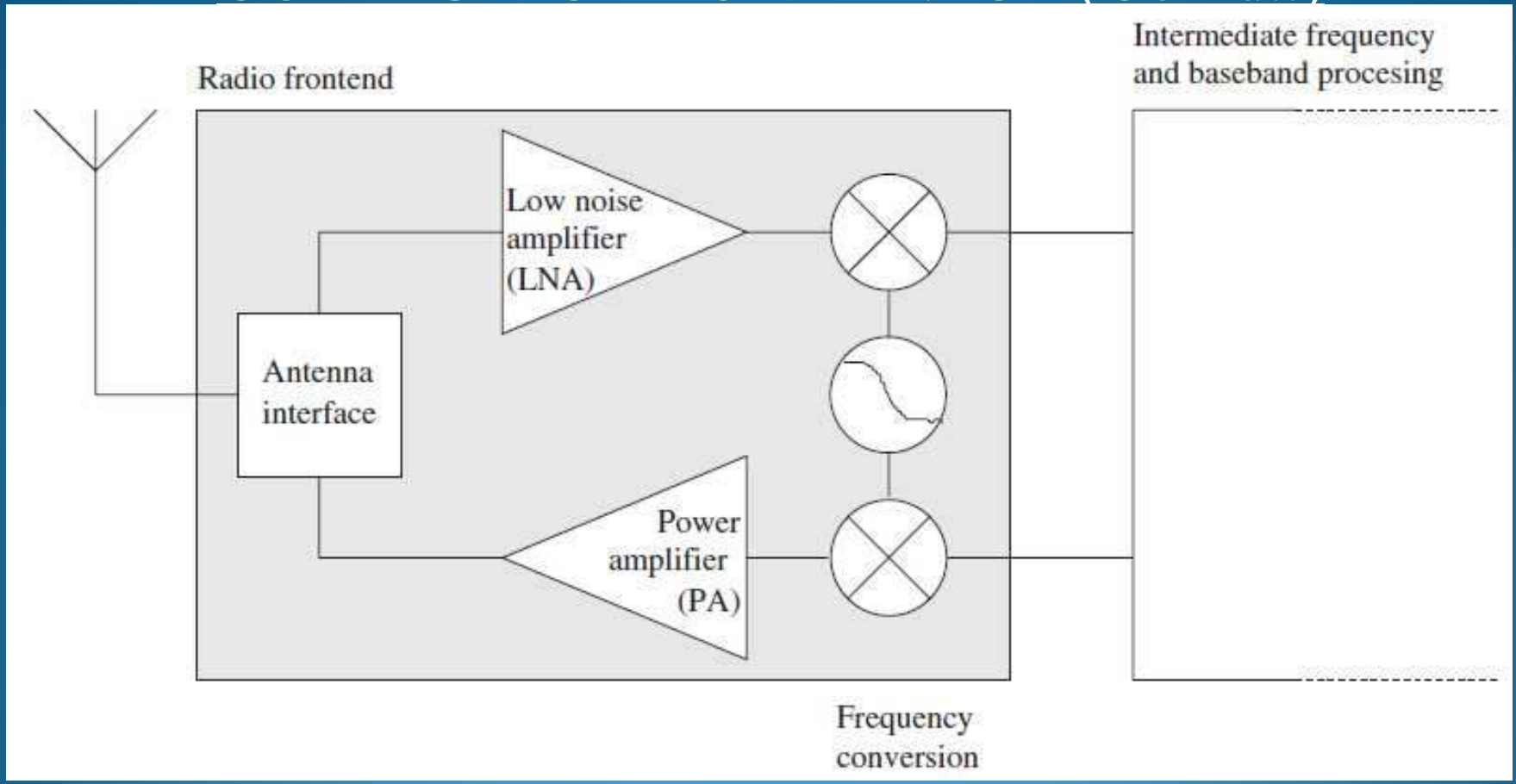
- **Transceiver structure:**
- **Radio frequency front end:** Analog signal processing in the actual radio frequency band. whears
- **Baseband processor:** signal processing in the digital domain and communicates with a sensor node's processor or other digital circuitry

RF front end: The **RF front end performs analog signal processing in the actual radio frequency band, for** example in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band;

- Power Amplifier (PA): accepts up-converted signals from the IF or baseband part and amplifies them for transmission over the antenna.
- Low Noise Amplifier (LNA): amplifies incoming signals without significantly reducing SNR. Always active and can consume a significant fraction of transceiver's energy.
- Local oscillators or voltage-controlled oscillators and mixers: used for frequency conversion from the RF spectrum to intermediate frequencies or to the baseband

RF front end

COMMUNICATION DEVICE (Contd..)



Transceiver Operational States

Many transceivers can distinguish four operational states

- **Mostly four states:**

1. **Transmit :** The transmit part of the transceiver is active and the antenna radiates energy.
2. **Receive :** The receive part is active
3. **Idle:** Transceiver is ready to receive but is not currently receiving anything. In this state, many parts of the receive circuitry are active, and others can be switched off.
4. **Sleep :** Significant parts of the transceiver are switched off. sleep states differ in the amount of circuitry switched off and in the associated recovery times and startup energy

Advanced Radio Concepts

1. Wakeup radio :

– **Wakeup receivers:** receiver specialized to notify an incoming packet, upon such an event, the main receiver can be turned on and perform the actual reception of the packet.

Their only purpose is to wake up the main receiver without needing (a significant amount of) power to do state a target power consumption of less than 1 µW.

2. Spread-spectrum transceivers:

– **Simple transceiver like ASK,FSK has limited performance**

– High performance transceivers with reduced interference

– Complex hardware and high cost.

2. Ultrawideband communication:

– Very large bandwidth is used to directly transmit digital sequence as very short impulses which occupy few Hertz up to the range of several GHz

– Sender and receiver has to be synchronized.

– Overlapping with conventional radio system can occur

– Small transmitting power is needed.

– Very high data rate can be realized over a short distance

– can easily penetrate obstacles such as doors.

– UWB transmitters are simpler where as receivers are more complex

Non Radio Frequency Wireless Communication

1. Optical

- Optical links can be used between sensor nodes for communication
- Very small energy per bit required for both generating and detecting optical light
- Communication can take place concurrently with only negligible interference.
- Communicating peers need to have a line of sight connection
- Strongly influenced by weather conditions

2. Ultrasound

- Used where Radio or optical waves can not penetrate the surrounding medium
- Travels relatively long distances at comparably low power.
- Used for surveillance of marine ground floor erosion
- Used as a secondary means of communication with a different propagation speed

Examples of radio transceivers RFM TR1000 family, Hardware accelerators (Mica motes), Chipcon CC1000 and CC2420 family, Infineon TDA 525x family, Ember EM2420 RF transceiver, LMX3162, Conexant RDSSS9M

IEEE 802.15.4/Ember EM2420 RF transceiver

National Semiconductor LMX3162

Sensors and actuators

Passive, omnidirectional sensors

Passive, narrow-beam sensors

Active sensors

Power supply of sensor nodes

Traditional batteries

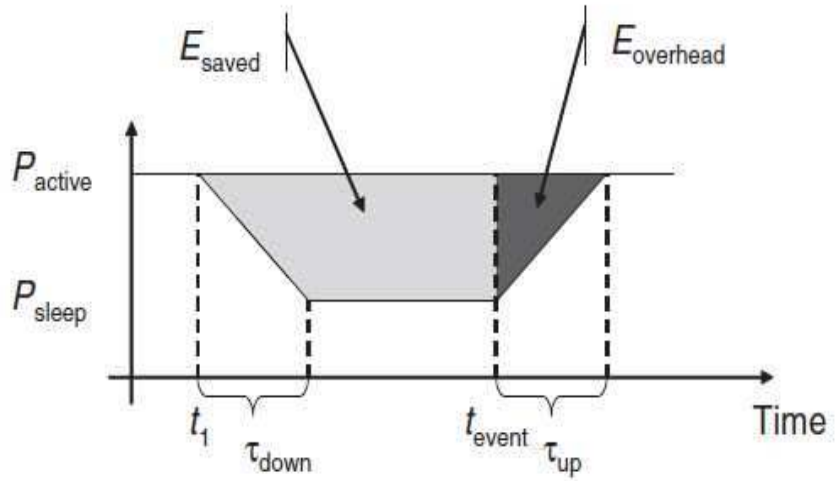
The power source of a sensor node is a battery, either nonrechargeable ("primary batteries") or, if an energy scavenging device is present on the node, also rechargeable ("secondary batteries").

Capacity, Capacity under load. Self-discharge, Efficient recharging

Energy Consumption of Sensor Nodes

Main consumers: controller, radio front ends, memory, and depending on type, the sensors.

- **Energy savings and overheads for sleep mo**



- t_1 : Time at which the decision whether or not a component is to be put into sleep mode should be taken to reduce power consumption from P_{active} to P_{sleep}.
- t_{event} : Time at which next event occurs
- Total energy wasted by idling at active time: $E_{active} = P_{active}(t_{event} - t_1)$
- T_{down}: Time taken by the node to reach sleep mode from active mode

Energy Consumption of Sensor Nodes

- Average power consumption during τ_{down} : $(P_{active} + P_{sleep})/2$.
- Energy consumed until t_{event} : P_{sleep}
- Energy required in sleep mode = $\tau_{down}(P_{active} + P_{sleep})/2 + (t_{event} - t_1 - \tau_{down})P_{sleep}$
- Energy required in active mode : $(t_{event} - t_1)P_{active}$
- energy saved in sleep mode:
  $E_{saved} = (t_{event} - t_1)P_{active} - (\tau_{down}(P_{active} + P_{sleep})/2 + (t_{event} - t_1 - \tau_{down})P_{sleep})$.
- Energy consumed for turning the node active from sleep mode: $E_{overhead} = \tau_{up}(P_{active} + P_{sleep})/2$
- Switching to sleep mode is beneficial only if $E_{overhead} < E_{saved}$ or, equivalently, if the time to the next event is sufficiently large:

$$(t_{event} - t_1) > \frac{1}{2}\left(\tau_{down} + \frac{P_{active} + P_{sleep}}{P_{active} - P_{sleep}}\tau_{up}\right)$$

Energy Consumption of Sensor Nodes

- **Microcontroller energy consumption**
- Embedded controllers commonly implement the concept of multiple operational states
- **Examples:**

1. Intel Strong ARM

– Provides three sleepmodes:

1. Normal mode: All parts of the processor are fully powered. Power consumption is up to400 mW.
2. Idle mode: Clocks to the CPU are stopped; clocks that pertain to peripherals are active. Any interrupt will cause return to normal mode. Power consumption is up to 100 mW.
3. Sleep mode: Only the real-time clock remains active. Wakeup occurs after a timer interrupt and takes up to 160ms. Power consumption is up to 50 µW.

Energy Consumption of Sensor Nodes

2. Texas Instruments MSP 430

- One Fully operational mode: consumes about 1.2 mW
- There are four sleep modes.
  - LPM4 ,deepest sleep mode :Consumes 0.3 μW. Only the controller is woken up by external interrupts.
  - LPM3, next higher mode: A clock is used for scheduled wake ups. Consumes about 6 μW.

3. Atmel ATmega

- The Atmel ATmega 128L has six different modes of power consumption.
- Power consumption varies between 6 mW and 15 mW in idle and active modes and is about 75 μW in power-down modes.

Energy Consumption of Sensor Nodes

- **Dynamic voltage scaling**
- Another technique that is used for saving power is to use a continuous notion of functionality/power adaptation by adapting the speed with which a controller operates instead of using different operational states.
- The supply voltage can be reduced at lower clock rates still guaranteeing correct operation.

Memory:

- On-chip memory of a microcontroller and FLASH memory consumes lesser energy; hence more appropriate for WSNs.

Radio transceivers

- Has two important tasks: transmitting and receiving data between a pair of nodes.
- Can operate in different modes

Energy Consumption of Sensor Nodes

A radio transceiver has essentially two tasks: transmitting and receiving data between a pair of nodes. To accommodate the necessary low total energy consumption, the transceivers should be turned off most of the time and only be activated when necessary – they work at a low **duty cycle. But this incurs additional complexity, time and power overhead that has** to be taken into account.

Radio transceivers

models for the energy consumption per bit for both sending and receiving

Modeling energy consumption during transmission

Energy consumed by a transmitter is due to two sources due to RF signal generation, which mostly depends on chosen modulation and target distance and henceon the transmission power *Ptx, that is, the power radiated by the antenna.*

A second part is due to electronic components necessary for frequency synthesis, frequency conversion, filters, and so on

For discussion, let us assume that the desired transmission power *Ptx is known*

Ptx is a function of system aspects like energy per bit over noise *Eb/No, the bandwidth efficiency ηBW, the distance d and the path loss coefficient* γ.

The transmitted power is generated by the amplifier of a transmitter. Its own power consumption *Pamp depends on its architecture, but for most of them, their consumed power depends on the power* they are to generate.

$$P_{\text{amp}} = \alpha_{\text{amp}} + \beta_{\text{amp}} P_{\text{tx}}. \tag{2.4}$$

where α_{amp} and β_{amp} are constants depending on process technology and amplifier architecture [559].

As an example, MIN and CHANDRAKASAN [563] report, for the μAMPS-1 nodes, $\alpha_{\text{amp}} = 174\,\text{mW}$ and $\beta_{\text{amp}} = 5.0$. Accordingly, the **efficiency of the power amplifier** η_{PA} for $P_{\text{tx}} = 0\,\text{dBm} = 1\,\text{mW}$ radiated power is given by

$$\eta_{\text{PA}} = \frac{P_{\text{tx}}}{P_{\text{amp}}} = \frac{1\,\text{mW}}{174\,\text{mW} + 5.0 \cdot 1\,\text{mW}} \approx 0.55\,\%.$$

In addition to the amplifier, other circuitry has to be powered up during transmission as well, for example, baseband processors. This power is referred to as *PtxElec*

.

The energy to transmit a packet *n-bits long (including all headers) then depends on how long it* takes to send the packet, determined by the nominal bit rate *R and the coding rate Rcode, and on* the total consumed power during transmission.

If, in addition, the transceiver has to be turned on before transmission, startup costs also are incurred (mostly to allow voltage-controlled oscillators and phase-locked loops to settle). Equation (2.5) summarizes these effects.

$$E_{tx}(n, R_{code}, P_{amp}) = T_{start}P_{start} + \frac{n}{RR_{code}}(P_{txElec} + P_{amp}). \quad (2.5)$$

To elucidate, the energy *Ercvd required to receive a packet has a startup component TstartPstart* similar to the transmission case when the receiver had been turned off (startup times are considered equal for transmission and receiving here); it also has a component that is proportional to the packet time *n RRcode*

During this time of actual reception, receiver circuitry has to be powered up, requiring a (more or less constant) power of *PrxElec – for example, to drive the LNA in the RF front* end.

$$E_{rcvd} = T_{start}P_{start} + \frac{n}{RR_{code}}P_{rxElec} + nE_{decBit}.$$

Relationship between computation and communication

What is the relation in energy consumption between sending data and computing?

Again, details about this relationship heavily depend on the particular hardware in use,

Network Architecture

Sensor network scenarios
Optimization goals and figures of merit
Design principles for WSNs
Service interfaces of WSNs
Gateway concepts

In wireless **sensor** networks (WSNs), **all** the data collected by the **sensor nodes** are forwarded to a **sink node**. Therefore, the placement of the **sink node** has a great impact on the energy consumption and lifetime of WSNs. **Sink nodes** are used to collect and pre-process data which gathered from regular **sensor nodes**.

- The **sink** is the common destination of all data collected by nodes in the network in case of convergecast data profile. The **sink** can be a gateway between the **WSN** and other king of networks.

- ink nodes are used to collect and pre-process data which gathered from regular sensor nodes.

- In Wireless Sensor Networks (WSN) the energy consumption and life times of sensors are an important issue. The data collected by respective cluster's nodes will be transmitted to the elected cluster heads. The cluster heads then will send all collected data to the Sink Node or Base Station. The data received by base station will be sent to data processing center. That is the reason Sink Node is called the gateway between the sensor nodes and data processing center.
- the sink node is used to collect data from different sensor nodes

Basic scenarios: Wireless Sensor Networks

- Sensor network scenarios

Sources: A source is any entity in the network that can provide information, that is, typically a sensor node; it could also be an actuator node that provides feedback about an operation.(Any entity that provides data/measurements)

- ***Sinks***: the entity where information is required

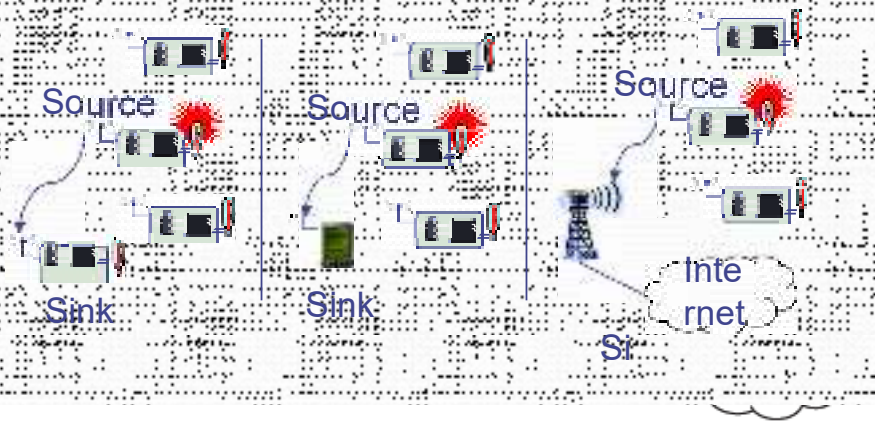
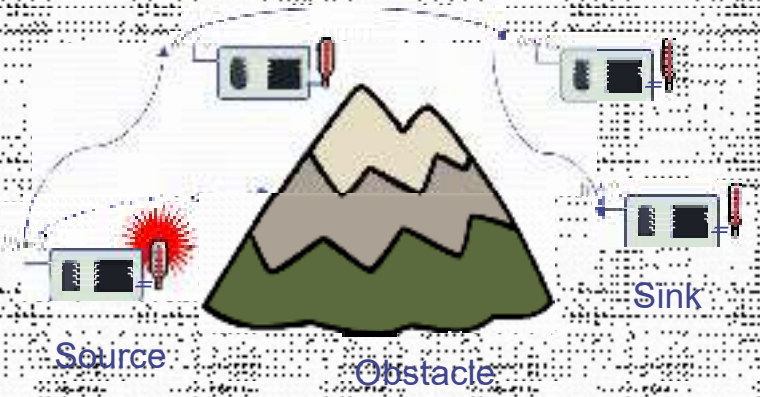


Figure 3.1 Three types of sinks in a very simple, single-hop sensor network

- Applications: Usually, machine to machine, often limited amounts of data

Single-hop vs. multi-hop networks

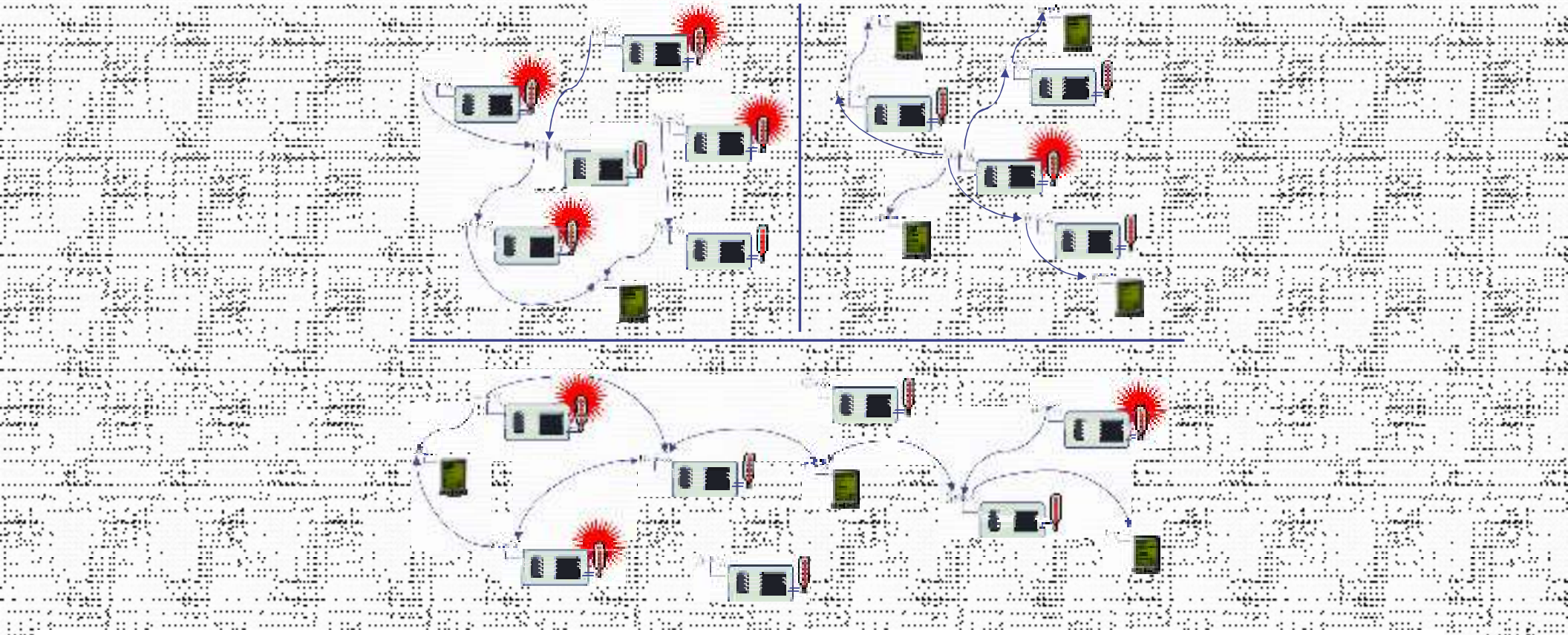
the simple, direct communication between source and sink is not always possible, specifically in WSNs, which are intended to cover a lot of ground (e.g. in environmental or agriculture applications) or that operate in difficult radio environments with strong attenuation (e.g. in buildings).



Energy efficiency with multi-hopping?

To overcome such limited distances, an obvious way out is to use relay stations, with the data packets taking multi hops from the source to the sink. This concept of multihop networks in figureis particularly attractive for WSNs as the sensor nodes themselves can act as such relay nodes, foregoing the need for additional equipment

WSN: Multiple sinks, multiple sources



3.1.3 Multiple sinks and sources

So far, only networks with a single source and a single sink have been illustrated. In many cases, there are multiple sources and/or multiple sinks present. In the most challenging case, multiple sources should send information to multiple sinks, where either all or some of the information has to reach all or some of the sinks. Figure 3.3 illustrates these combinations.

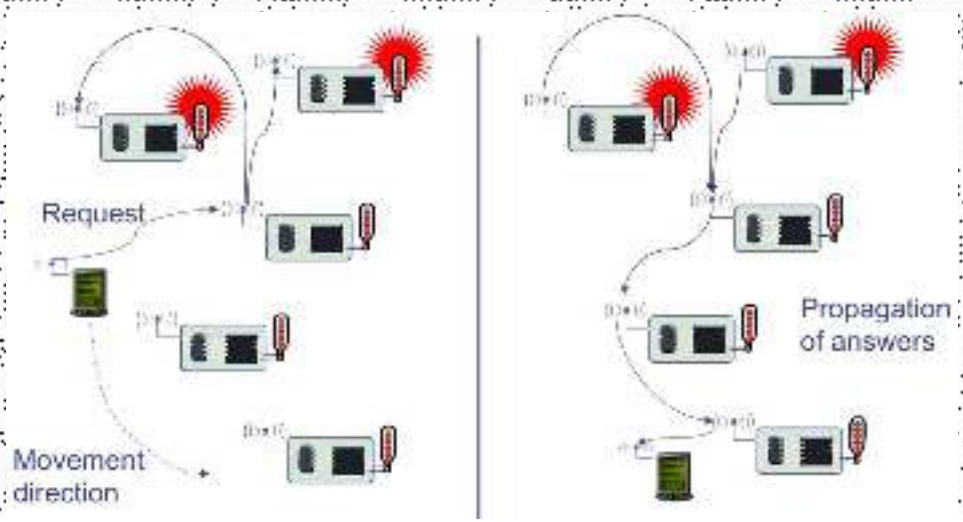
Different sources of mobility

WSN Node mobility

The wireless sensor nodes themselves can be mobile. In the face of node mobility, the network has to reorganize itself frequently enough to be able to function correctly.

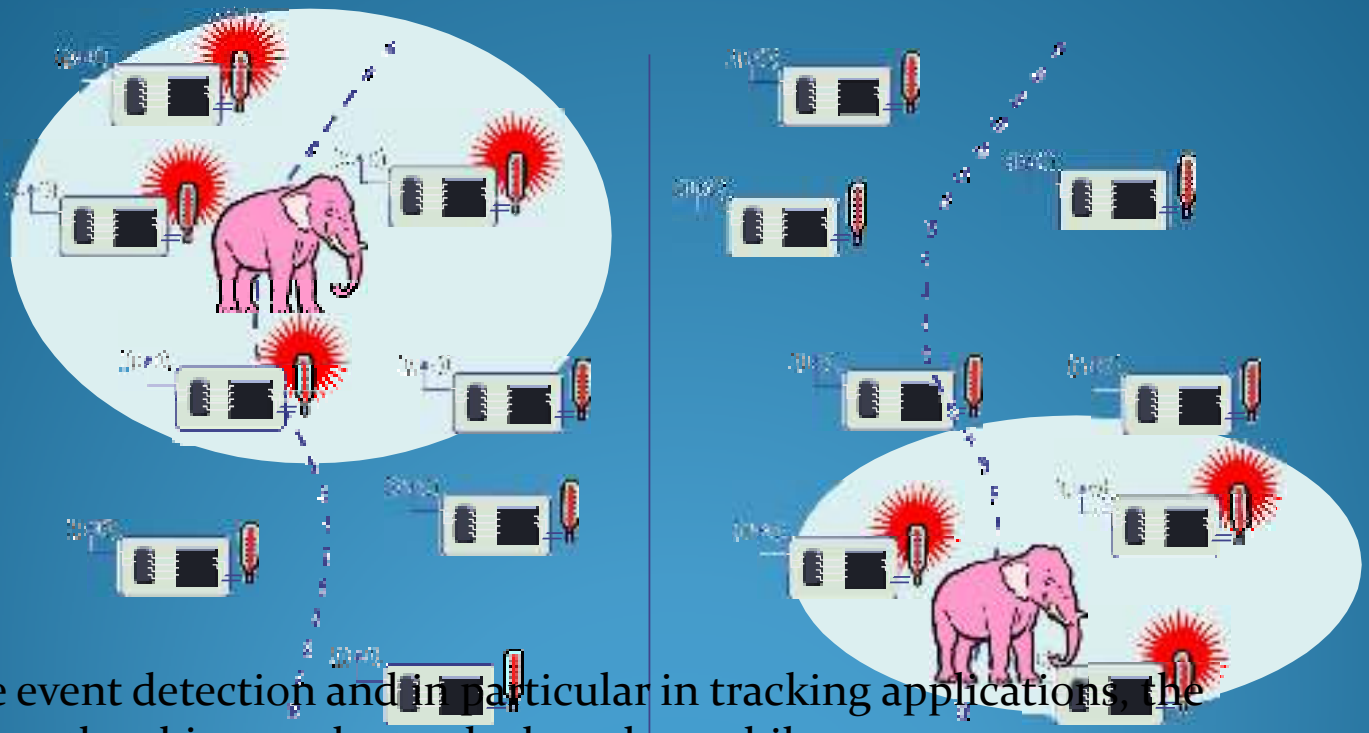
- A node participating as source/sink (or destination) or a relay node might move around
- Deliberately, self-propelled or by external force; targeted or at random
- Happens in both WSN and MANET

WSN Sink mobility=The information sinks can be mobile (Figure 3.4). While this can be a special case of node mobility, the important aspect is the mobility of an information sink that is not partof the sensor network, for example, a human user requested information via a PDA whil walking in an intelligent building.



Different sources of mobility

WSN Event mobility



In applications like event detection and in particular in tracking applications, the cause of the events or the objects to be tracked can be mobile.
In such scenarios, it is (usually) important that the observed event is covered by a sufficient number of sensors at all time. Hence, sensors will wake up around the object, engaged in higher activity to observe the present object, and then go back to sleep

Optimization goals and figures of merit

- **Quality of service**

QoS can be regarded as a low-level, networking-device-observable attribute – bandwidth, delay, jitter, packet loss rate – or as a high-level, user-observable, so-called subjective attribute like the perceived quality of a voice communication or a video transmission. high-level QoS attributes in WSN highly depend on the application. Some generic possibilities are:

- **Event detection/reporting probability:**
  - The probability that an event that actually occurred is not detected/not reported to an information sink that is interested in such an event
  - Eg: Not reporting a fire alarm to a surveillance station
- **Event classification error:** Events are not only to be detected but also to be classified, the error in classification must be small.
- **Event detection delay:** The delay between detecting an event and reporting it to any/all interested sinks
- **Missing reports:** In applications that require periodic reporting, the probability of undelivered reports should be small.

Optimization goals and figures of merit

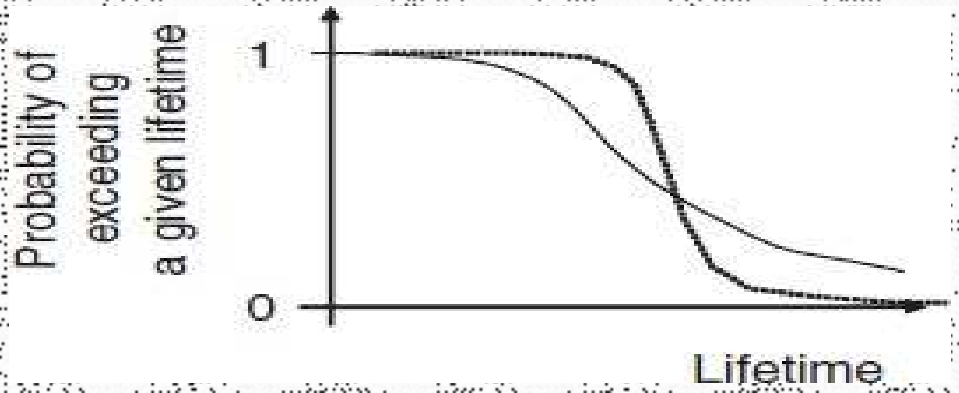
- **Approximation accuracy:**
  - The Tracking applications mustaverage/max absolute or relative error with respect to the actual function that occurs in function approximation applications
  - E.g. approximating the temperature as a function of location for a given area
- **Tracking accuracy:**
  - not miss an object to be tracked.
  - The reported position should be as close to the real position as possible, and the error should be small.
- **Energy efficiency**
- **Energy per correctly received bit:** Average energy spent, counting all sources of energy consumption at all possible intermediate hops, to transport one bit of information from the source to the destination

Optimization goals and figures of merit

- **Energy per reported (unique) event:** The same event is sometimes reported from various sources; this metric is usually normalized to unique event.
- **Delay/energy trade-offs:** Trade-off exists between delay and energy overhead
- **Network lifetime:** The time for which the network is operational / the time during which it is able to fulfill its tasks. Possible definitions are:
  - **Time to first node death:** Time at which the first node in the network run out of energy or fail and stop operating
  - **Network half-life:** Time at which 50% of the nodes have run out of energy and stopped operating.
  - **Time to partition:** Time at which the first partition of the network into two (or more) disconnected parts occur

Optimization goals and figures of merit

- **Time to loss of coverage:** The time when for the first time any spot in the deployment region is no longer covered by any node's observations.
- **Time to failure of first event notification:** Time at which a node or a part of the network fails to deliver an event



Two probability curves of a node exceeding a given lifetime – the dotted curve trades off better minimal lifetime against reduced maximum lifetime

Optimization goals and figures of merit

Scalability

Ability to maintain performance characteristics irrespective of the size of the network

Robustness

WSN should not fail just because a limited number of nodes run out of energy, or because their environment changes and break up existing radio links between two nodes

These failures have to be compensated, for example, by finding other routes.

Text Book & References

- Text Book

- Holger Karl ,Andreas willig, ―Protocol and Architecture for Wireless Sensor Networks‖, John wiley publication, Jan 2006.

- References

1. Feng Zhao, Leonidas Guibas, ―Wireless Sensor Networks: an information processing approach‖, Elsevier publication, 2004.
2. Charles E. Perkins, ―Ad Hoc Networking‖, Addison Wesley, 2000.
3. I.F. Akyildiz, W. Su, Sankarasubramaniam, E. Cayirci, ―Wireless sensor networks: a survey‖, computer networks, Elsevier, 2002, 394 - 422.

THANK YOU

ypes of WSNs (Wireless Sensor Networks)

Terrestrial WSNs.

Underground WSNs.

Underwater WSNs.

Multimedia WSNs.

Mobile WSNs.