

# **CS 442**

## **Wireless Sensor Network**

<b>Syllabus</b>	<b>CS 442</b>	<b>Wireless Sensor Network</b>	<b>L</b>	<b>T</b>	<b>P</b>	<b>C</b>
		<b>B.Tech (CSE)   Eighth Semester (Elective)</b>	<b>3</b>	<b>1</b>	<b>0</b>	<b>4</b>
<b>Lecture Plan</b>	<b>Unit-1</b>	<b>Introduction:</b> Introduction to wireless sensor network. Definitions, Challenges, Application requirements, Protocol Stack, Special features, Difference with other kinds of networks, issues and research problems.				
<b>Marks distrib.</b>	<b>Unit-2</b>	<b>Wireless fundamentals,</b> Antennas, propagation, and path loss, Digital radio communication, RF spectrum, modulation, 2-ray model, others.				
<b>Books &amp; Ref.</b>	<b>Unit-3</b>	Low power PAN, LAN Standards, IEEE 802.11, 802.15, 802.15.4 and Zigbee.				
	<b>Unit-4</b>	<b>Medium Access:</b> Medium access problem related to sensor network, Aloha, CSMA, Slotted Aloha, RTS/CTS, ACKs, TRAMA, SMAC and other WSN MAC protocols, Energy management.				
	<b>Unit-5</b>	<b>Network layer / Routing:</b> Adhoc network routing, Data centric routing, Hierarchical routing protocols, Geographical routing, Location based routing.				
	<b>Unit-6</b>	<b>Localization:</b> Localization challenges, needs, and state of the art solutions. Localization, range free and range based localization.				
	<b>Unit-7</b>	<b>Application:</b> Application specific network design and deployment, mobile sensor network, Linear and grid based networks, Network infrastructure management and control.				

**Syllabus**

Unit-1	<b>Introduction:</b> Introduction to wireless sensor network. Definitions, Challenges, Application requirements, Protocol Stack, Special features, Difference with other kinds of networks, issues and research problems.
Unit-2	<b>Wireless fundamentals:</b> Antennas, propagation, and path loss, Digital radio communication, RF spectrum, modulation, 2-ray model, others.
Unit-3	Low power PAN, LAN Standards, IEEE 802.11, 802.15, 802.15.4 and Zigbee.
Books & Ref.	

**Lecture Plan****Marks distrib.****Books & Ref.****Mid sem exam**

Unit-4	<b>Medium Access:</b> Medium access problem related to sensor network, Aloha, CSMA, Slotted Aloha, RTS/CTS, ACKs, TRAMA, SMAC and other WSN MAC protocols, Energy management.
Unit-5	<b>Network layer / Routing:</b> Adhoc network routing, Data centric routing, Hierarchical routing protocols, Geographical routing, Location based routing.
Unit-6	<b>Localization:</b> Localization challenges, needs, and state of the art solutions. Localization, range free and range based localization.
Unit-7	<b>Application:</b> Application specific network design and deployment, mobile sensor network, Linear and grid based networks, Network infrastructure management and control.

**End sem exam****Syllabus**

<b>Mid sem</b>	<b>: 30</b>
<b>End sem</b>	<b>: 50</b>
<b>Sessional</b>	<b>: 20</b>
<hr/>	
<b>Total</b>	<b>: 100</b>

**Lecture Plan****Marks distrib.****Books & Ref.****Sessional (20):-**

**Minor test : 10**

**Class Performance\* : 10**

\* From Assignments, TP, Attendance

**Syllabus****Books:**

1. Kazem Sohraby, Daniel Minoli, Taieb Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications*, Wiley-Interscience
2. Feng Zhao, Leonidas Guibas, *Wireless Sensor Networks: An Information Processing Approach*, Morgan Kaufmann Publishers
3. (Ed) Pradeep Kumar Singh, Bharat K. Bhargava, Marcin Paprzycki, Narottam Chand Kaushal, Wei-Chiang Hong, *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, Springer
4. William Stallings, *Wireless Communications & Networks*, Pearson Pub
5. T.S. Rappaport, *Wireless Communications: Principles and Practice*, Pearson Education India

**Lecture Plan****Marks distrib.****Books & Ref.****References:**

Recent papers

**Unit 1:**

**Introduction:** Introduction to wireless sensor network. Definitions, Challenges, Application requirements, Protocol Stack, Special features, Difference with other kinds of networks, issues and research problems.

# **Unit 1**

## **Introduction**

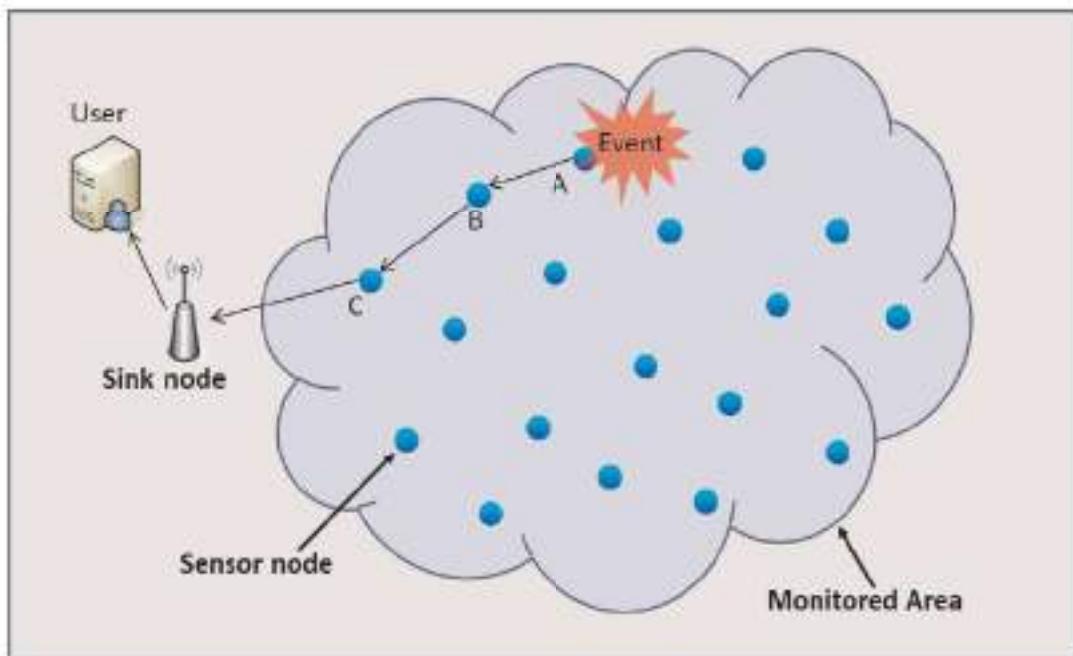
# Introduction

A **sensor network** is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it.

- Random deployment (mostly)
- Cooperative capabilities

7

## WSN architecture



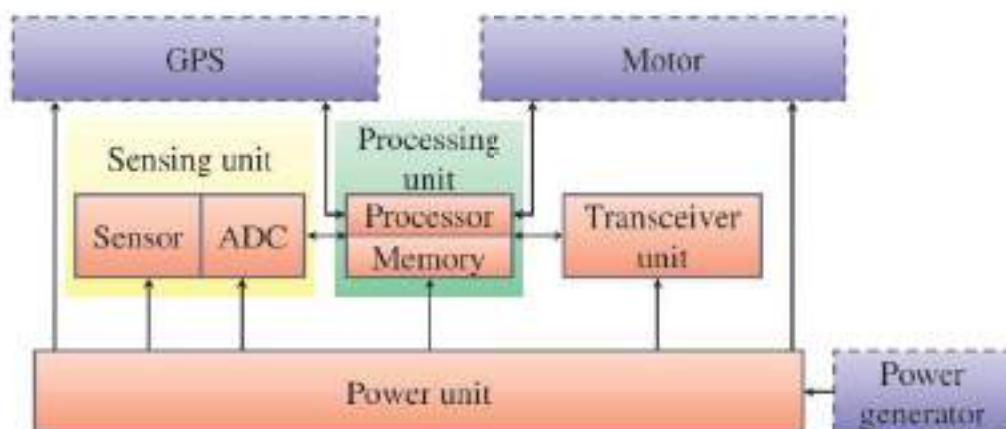
# Wireless Sensor Networks (WSNs)

- ▶ Sensor Network = a few **sink nodes** and a huge number of **sensor nodes**
- ▶ Sink node:
  - ▶ A control center where user can retrieve data gathered from sensor networks
  - ▶ Static/Mobile

9

## Sensor Node

- ▶ Sensor node:
  - ✓ Sensing unit
  - ✓ Processing unit
  - ✓ Transceiver unit
  - ✓ Power unit
  - ✓ Additional units



# Sensor Elements

---



Ultrasonic Sensor



Temperature/Humidity Sensor



GPS Receiver Module



Tri-Axis Accelerometer Module



Color Sensor



PIR Sensor

11

# Sensor Elements

---



Compass Module



Hall-Effect Sensor



Gyroscope Module



Pressure Sensor



Humidity Sensor



Piezo Film Vibra Tab Mass



QTI Sensor



Sound Impact Sensor

12

## Static Sensors (example)

---

- ▶ MICA2
- ▶ The first commercial product
- ▶ Applications
  - ▶ Security, Surveillance and Force Protection
  - ▶ Environmental Monitoring
  - ▶ Large Scale Wireless Networks (1000+)
  - ▶ Distributed Computing Platform



13

## Static Sensors (example)

---

- ▶ MICA2DOT
- ▶ Applications
  - ▶ Temperature and Environmental Monitoring
  - ▶ Remote Data Logging
  - ▶ Smart Badges, Wearable Computing



14

## Static Sensors (example)

---

- ▶ MICAz (Zigbee)
- ▶ Applications
  - ▶ Indoor Building Monitoring and Security
  - ▶ Acoustic, Video, Vibration and Other High Speed Sensor Data
  - ▶ Large Scale Sensing Networks(1000+ Points)



15

## Static Sensors (example)

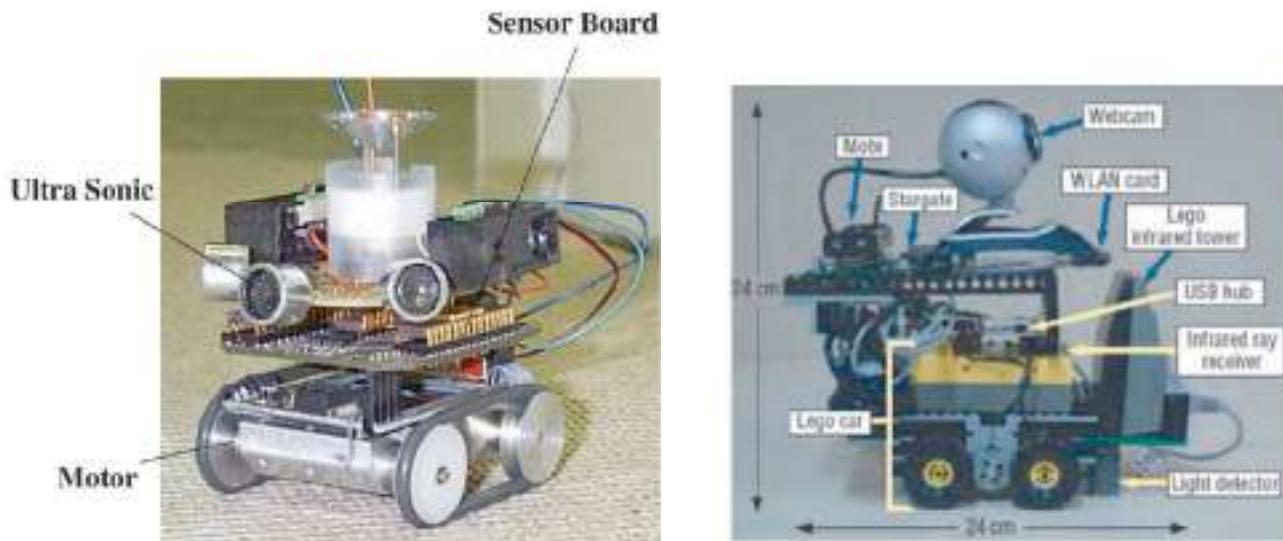
---

- ▶ TELOS B
- ▶ Applications
  - ▶ Platform for low power research development
  - ▶ Wireless sensor network experimentation



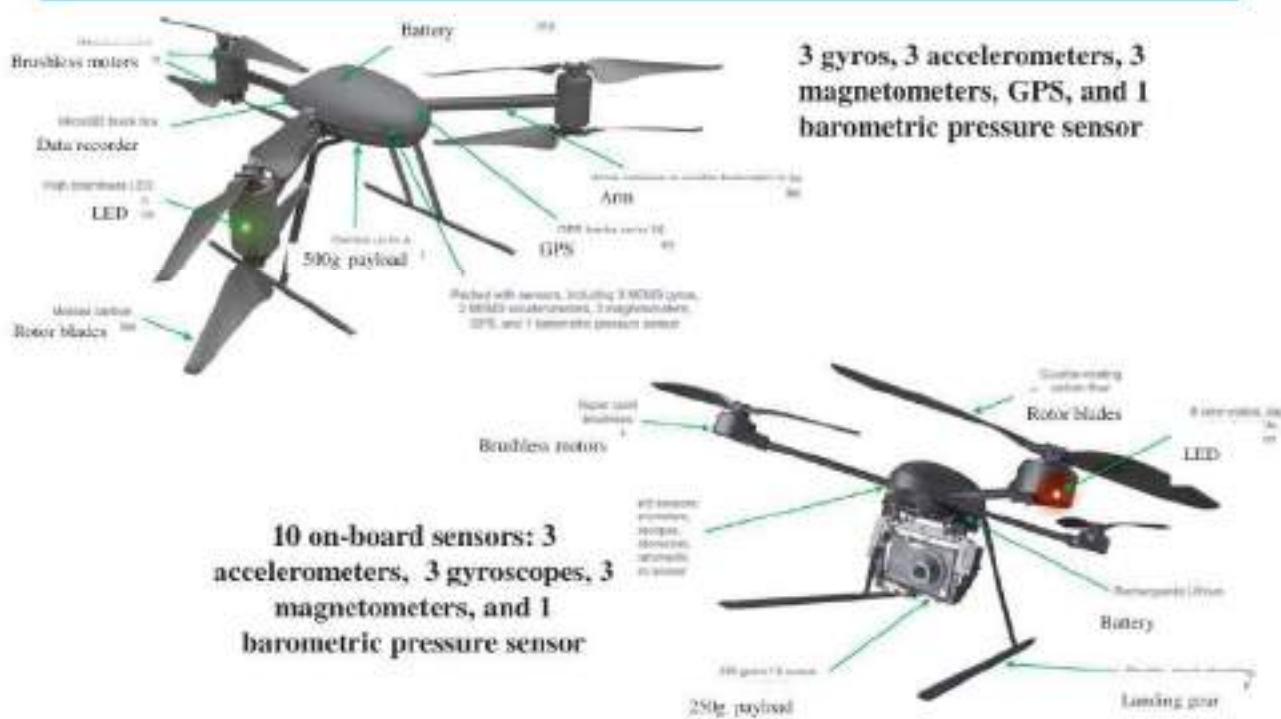
16

# Mobile Sensor : Typical



17

# Mobile Sensor : Typical



18

# Sensor Node Software Platforms

- AutoSec
  - Bertha
  - BTnut Nut/OS
  - COMiS
  - Contiki
  - CORMOS
  - COUGAR
  - DSWare
  - eCos
  - Enviro-Track
  - EYESOS
  - Global Sensor Networks; GSN
  - Impala
  - jWebDust
  - LiteOS
  - MagnetOS
  - MANTIS
  - MiLAN
  - Netwiser
  - OCTAVEX
  - SenOS
  - SensorWare
  - SINA
  - SOS
  - **TinyDB**
  - TinyGALS
  - **TinyOS**
  - t-Kernel
  - VIP Bridge
- Programming languages**
- c@t (Computation at a point in space (@) Time )
  - DCL (Distributed Compositional Language)
  - galsC
  - **nesC**
  - **Proto-threads**
  - SNACK
  - SQTL

19



## Applications of Sensor networks

# Applications of WSNs

---

- ▶ Entertainment Applications
- ▶ Security Applications
- ▶ Environment and Ecology
- ▶ Health Care
- ▶ Smart Home
- ▶ Agricultural Applications
- ▶ Industrial Applications
- ▶ Military Applications
- ▶ Art Applications

21



## Applications of sensor networks

---

### Military applications

- Monitoring friendly forces, equipment and ammunition
- Battlefield surveillance
- Battle damage assessment
- Nuclear, biological and chemical attack detection



## Applications of sensor networks

---

### Environmental applications

- Forest fire detection
- Biocomplexity mapping of the environment
- Flood detection
- Precision agriculture

23



## Applications of sensor networks

---

### Health applications

- Tele-monitoring of human physiological data
- Tracking and monitoring patients and doctors inside a hospital
- Drug administration in hospitals

24



## Applications of sensor networks

### Home and other commercial applications

- Home automation and Smart environment
- Interactive museums
- Managing inventory control
- Vehicle tracking and detection
- Detecting and monitoring car thefts

25

## Entertainment Applications

### ► Wii (Nintendo - Game Player )

- One main feature of the Wii Remote is its motion sensing capability, which allows the user to interact with and manipulate items on screen via gesture recognition.
- Motion Sensor (Orientation Sensor + G-Sensor ) and Infrared Sensor



# Entertainment Applications

## ▶ Wii Vitality Sensor

- ▶ The device will sense the user's pulse and a number of other signals transmitted by Human's bodies.



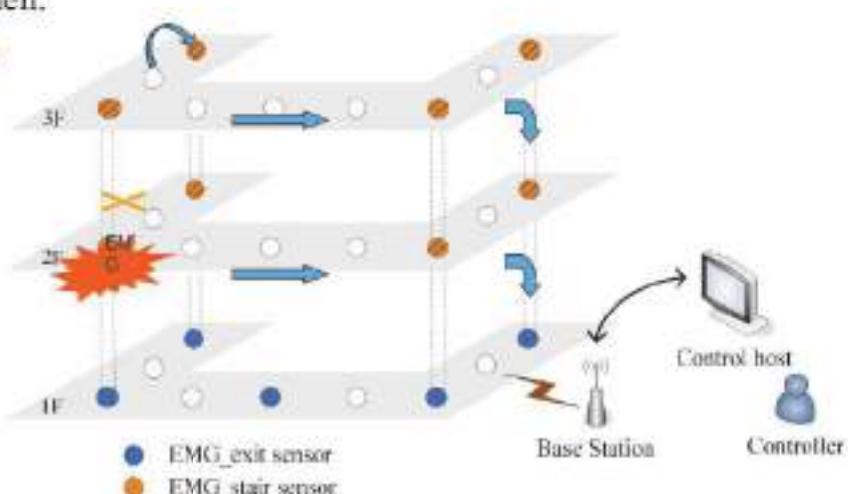
27

# Security Applications

## ▶ Disaster Relief and Guiding System

- ▶ Constructs the escape system with the Wireless Sensor Networks
  - ▶ Detects the high temperature area.
  - ▶ Guide to the evacuation exit.
  - ▶ Report to firemen.

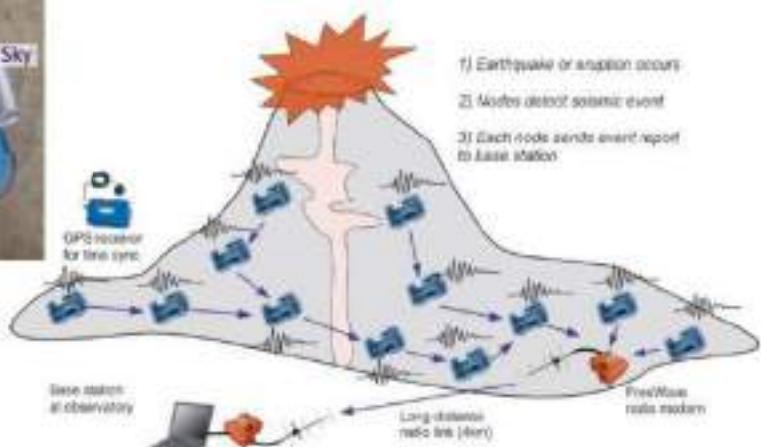
## ▶ Temperature Sensors



28

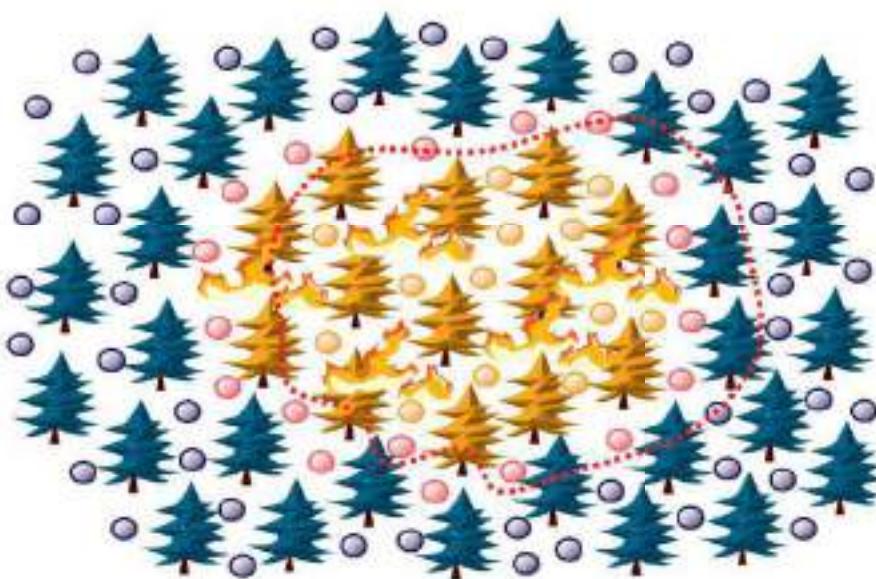
# Security Applications

- ▶ Volcanic eruption
  - ▶ Effective early warning systems
  - ▶ Using **Seismic Sensors** to detect seismic event when eruption occurs.



29

# Security Applications : Threat Detection



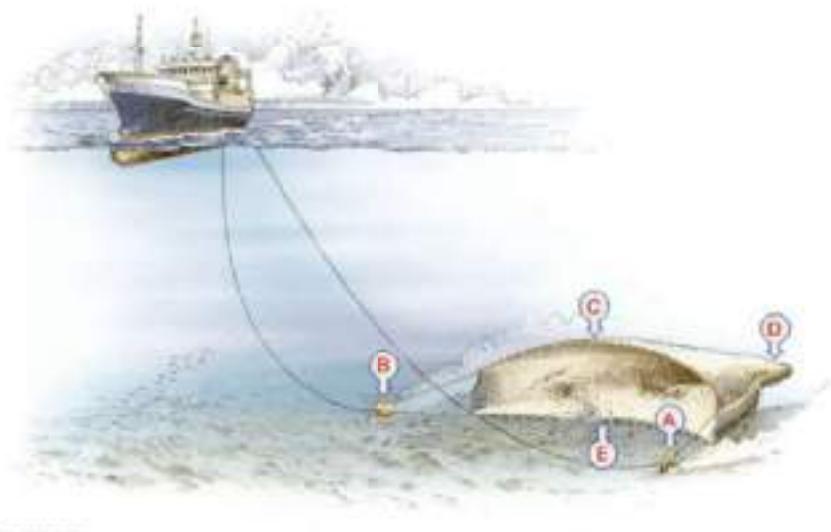
30

# Environment and Ecology

---

## ► Underwater Sensor Network

- ▶ To detect shoal, marine life, etc.
- ▶ Sonar Sensor



31

# Environment and Ecology

---

## ► Debris Flow Monitoring of Wireless Sensor Network System

- ▶ Humidity Sensor, Temperature Sensor, Pressure Sensor, Optical Sensor

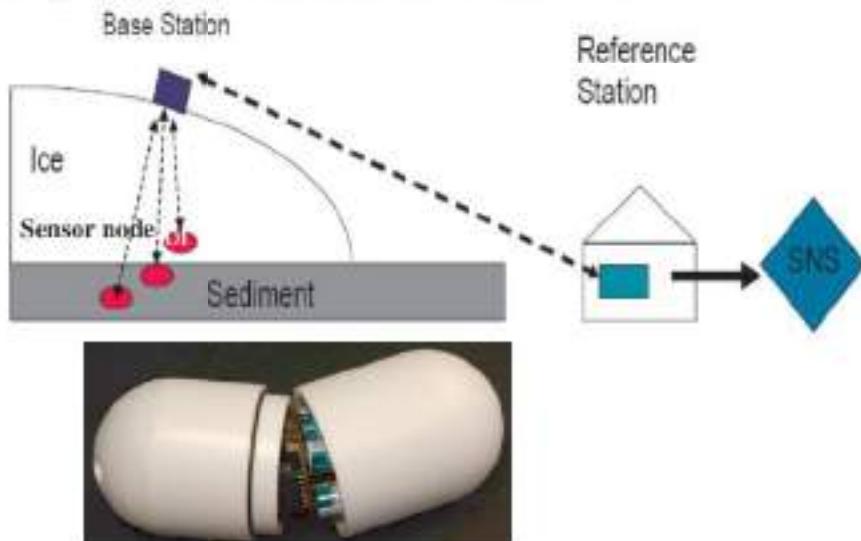


32

# Environment and Ecology

## ► The GlacsWeb Architecture

- to **detect the movement of the glacier**, then the sensor sending a message to the system to monitor the glacier.
- Pressure Sensor, Temperature Sensor and Orientation Sensor**



33

# Environment and Ecology

## ► Habitat Monitoring on Great Duck Island

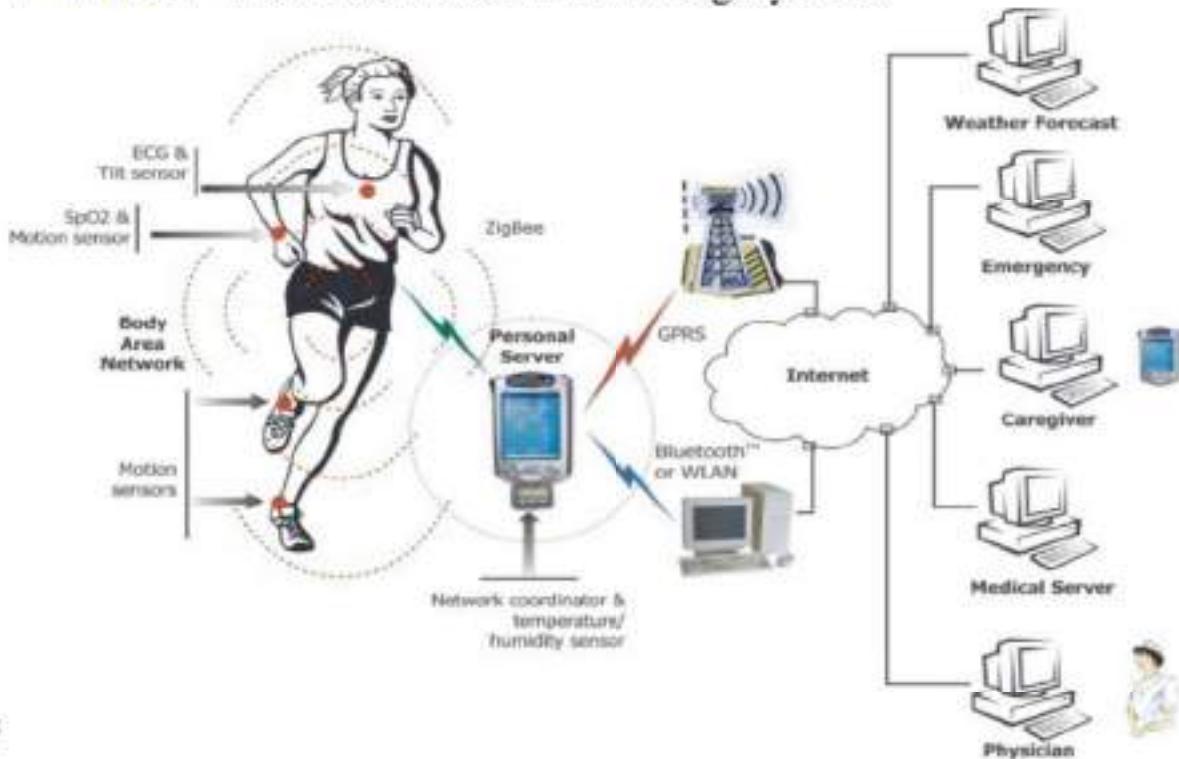
- Wireless sensor networks monitor the microclimates in and around nesting burrow used by the Leach's Storm Petrel
- Temperature, humidity, barometric pressure, mid-range infrared, and image**



34

# Health Care

## ► WHMS - Wearable Health Monitoring Systems



35

# Smart Home

## ► Aegis - Smart Home

- Sensor Model : Orientation Sensor, G-Sensor, Infrared Sensor and Gas Sensor



36

# Agricultural Applications

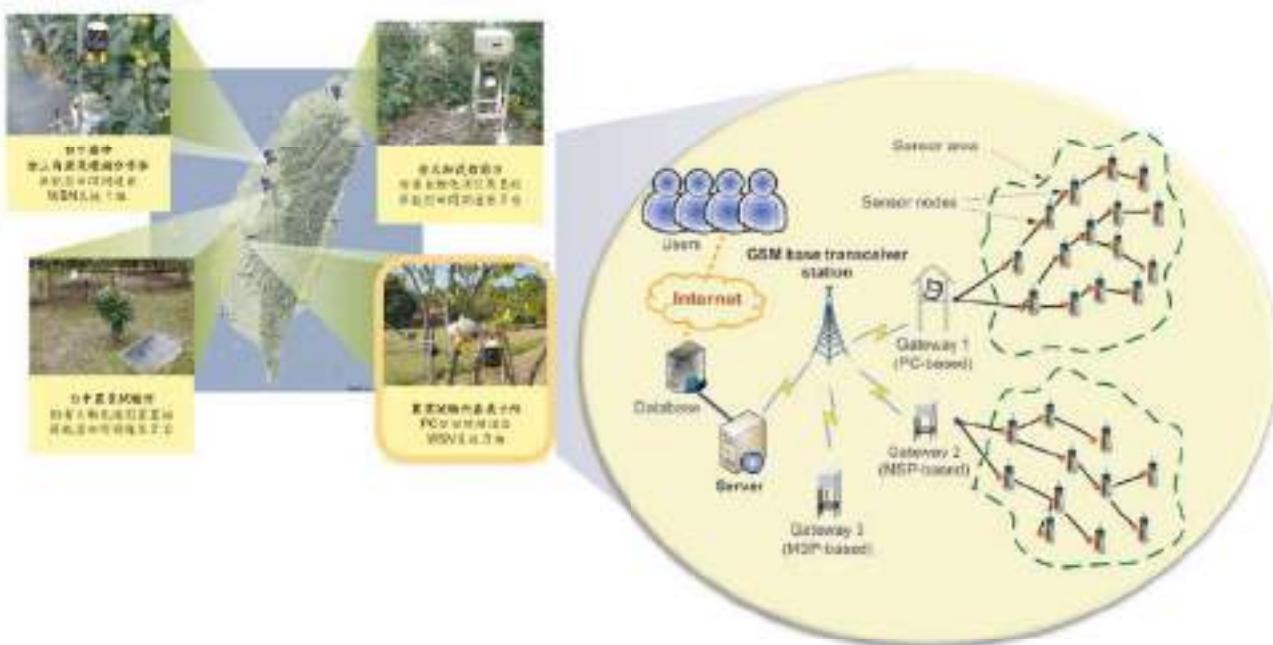
- ▶ The oriental fruit fly Ecological Monitoring and Early Warning System
  - ▶ Sensor Model : Octopus II with Humidity Sensor, Temperature Sensor, Pressure Sensor and Optical Sensor



37

# Agricultural Applications

- ▶ Application of WSN technology in the oriental fruit fly ecological monitoring



38

# Agricultural Applications

---

## ► The wine making

- ▶ The ice-wine which must be an exact temperature for a certain amount of time before it is harvested in order to qualify
- ▶ To find out that the temperature is actually not quite cold enough yet. So all the workers are sent home and paid for three hours of work. If wireless sensors were used instead perhaps some money and time could be saved.
- ▶ **Humidity Sensor, Temperature Sensor**



39

# Industrial Applications

---

## ► LCD plants

- ▶ To prevent shaking of the glass substrate during processing
- ▶ Improve the productivity (increase 5%)
- ▶ **Seismic Sensors, Displacement Sensors**



# Industrial Applications

## ▶ Smart Parking

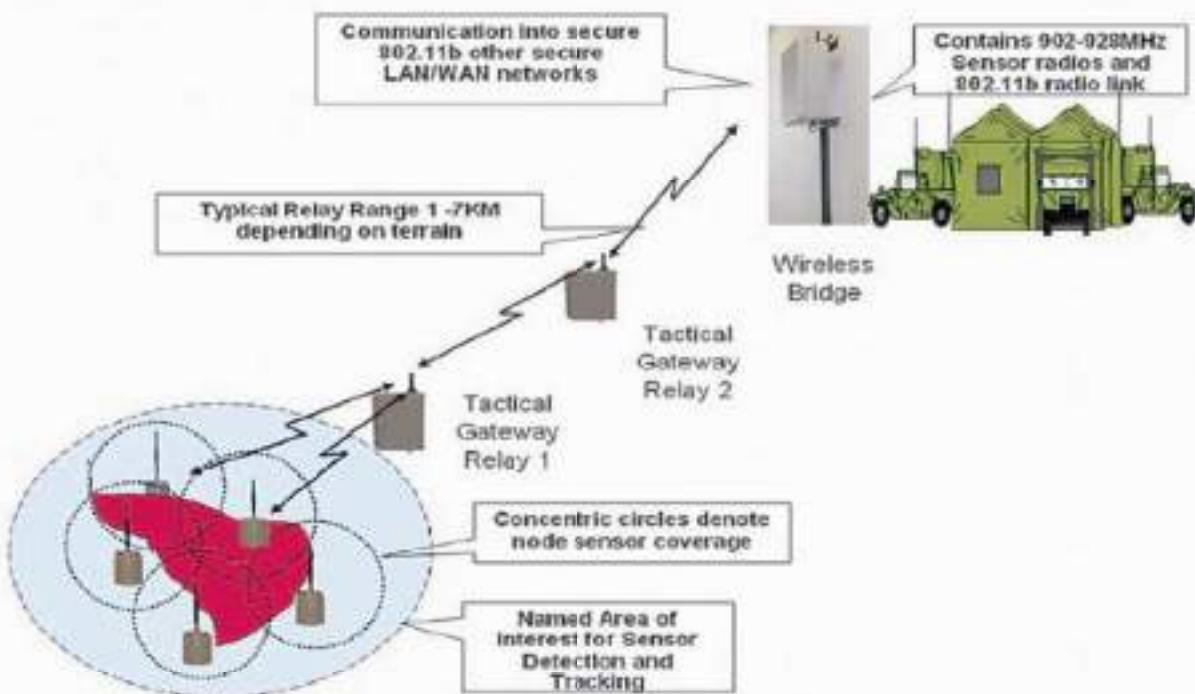
- ▶ Drivers will be alerted to empty parking places either by displays on street signs, or by looking at maps on screens of their smart phones.
- ▶ They able to pay for parking by cell phone, and add to the parking meter from their phones without returning to the car.



41

# Military Applications

- ▶ Unattended ground sensor network for area force protection.



42

# Military Applications

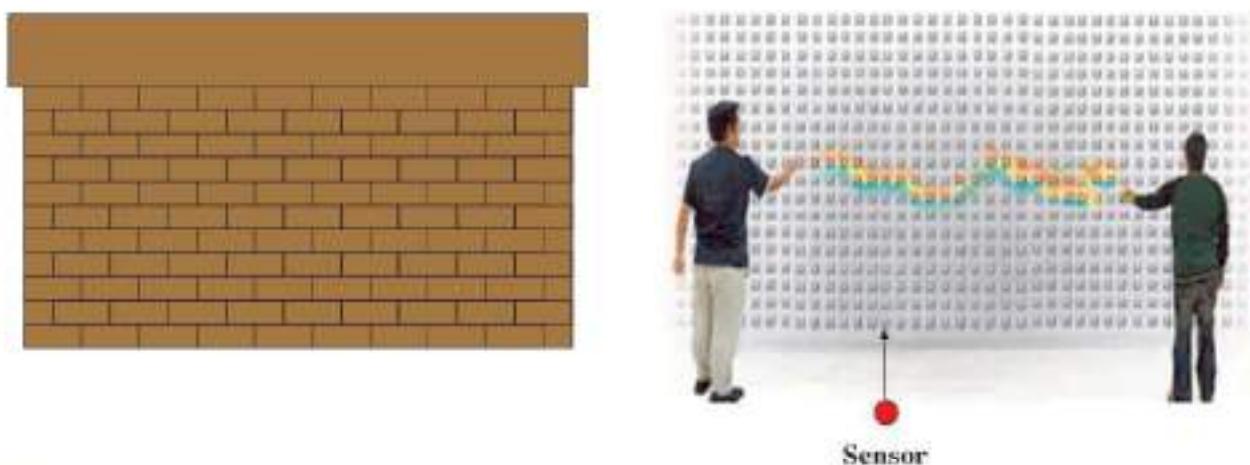
- ▶ Mobile Sensor in the military
  - The **robotic weapons** now playing greater roles on the battlefield.



43

# Art Applications - Interactive Art

- ▶ WSN in Interactive Wall
  - ▶ Deploy the sensor in the wall to sense the data and show the image or text at the wall (LEDs).
  - ▶ **Humidity Sensor, Temperature Sensor, Optical Sensor, Ultrasonic Sensor**



44



## Difference of WSN with other networks

### Sensor networks VS ad hoc networks:

- The number of nodes in a sensor network can be several **orders of magnitude** higher than the nodes in an ad hoc network.
- Sensor nodes are **densely deployed**.
- Sensor nodes are **limited in power, computational capacities and memory**.
- Sensor nodes are **prone to failures**.
- The **topology** of a sensor network changes frequently.
- Sensor nodes **mainly use broadcast**, most ad hoc networks are based on p2p.
- Sensor nodes **may not have global ID**.



## Difference of WSN with other networks

### Sensor networks VS ad hoc networks:

- The number of nodes in a sensor network can be several **orders of magnitude** higher than the nodes in an ad hoc network.
- Sensor nodes are **densely deployed**.
- Sensor nodes are **limited in power, computational capacities and memory**.
- Sensor nodes are **prone to failures**.
- The **topology** of a sensor network changes frequently.
- Sensor nodes **mainly use broadcast**, most ad hoc networks are based on p2p.
- Sensor nodes **may not have global ID**.

45



## Factors influencing sensor network design

- Fault Tolerance
- Scalability
- Hardware Constraints
- Sensor Network Topology
- Environment
- Transmission Media
- Power Consumption

46



## Factors influencing sensor network design

### Fault tolerance

- Fault tolerance is the **ability to sustain** sensor network functionalities without any interruption due to sensor node failures.
- The fault tolerance level depends on the application of the sensor networks.

42



## Factors influencing sensor network design

### Scalability

- Scalability measures the **density of the sensor nodes**.
- Density =  $\mu(R) = (N\pi R^2)/A$   
R – Radio Transmission Range

43

## Factors influencing sensor network design

### Production costs

- The cost of a single node is very important to justify the overall cost of the networks.
- The cost of a sensor node is a very challenging issue given the amount of functionalities with a price of much less than a dollar.

47

## Factors influencing sensor network design

### Hardware constraints

In a node : Everything is limited / constrained

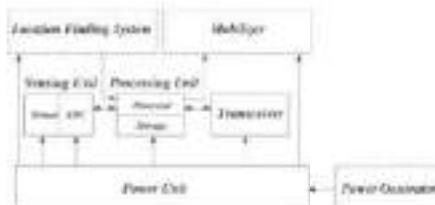


Fig. 1. The components of a sensor node.

51



## Factors influencing sensor network design

### Sensor network topology

- Pre-deployment and deployment phase
- Post-deployment phase
- Re-deployment of additional nodes phase

53



## Factors influencing sensor network design

### Target Environment / Design is application specific

- Busy intersections
- Interior of a large machinery
- Bottom of an ocean
- Surface of an ocean during a tornado
- Biologically or chemically contaminated field
- Battlefield beyond the enemy lines
- Home or a large building
- Large warehouse
- Animals
- Fast moving vehicles
- Drain or river moving with current.

53



## Factors influencing sensor network design

### Transmission media

In a multihop sensor network, communicating nodes are linked by a wireless medium.

To enable global operation, the chosen transmission medium must be available worldwide.

- Radio
- Infrared
- optical media

53



## Factors influencing sensor network design

### Power Consumption

- Sensing
- Communication
- Data processing

54



## Communication architecture of sensor networks

55



## Communication architecture of sensor networks

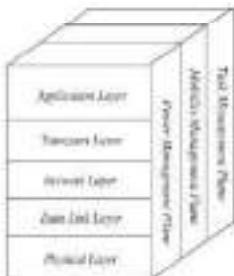


Fig. 5: The sensor network protocol stack

- Combine power and routing awareness
- Integrates data with networking protocols
- Communicates power-efficiently through the wireless medium
- Promotes cooperative efforts among sensor nodes.

56



## Communication architecture of sensor networks

### Physical layer:

Address the needs of simple but robust modulation, transmission, and receiving techniques.

- frequency selection
- carrier frequency generation
- signal detection and propagation
- signal modulation and data encryption.

62



## Communication architecture of sensor networks

### ▪ Propagation Effects

Minimum output power  
Signal attenuation wrt distance in order of  $(d^n)$ ,  $2 \leq n \leq 4$   
Ground reflect – in Multihop dense sensor network

- Power Efficiency Modulation Scheme  
M-ary Modulation scheme  
Ultra wideband (impulse radio)

58



## Communication architecture of sensor networks

### Open research issues

- Modulation schemes
- Strategies to overcome signal propagation effects
- Hardware design: transceiver

13



## Communication architecture of sensor networks

### Data link layer:

Responsible for the multiplexing of data stream, data frame detection, the medium access and error control.

- Medium Access Control
- Power Saving Modes of Operation
- Error Control

14



## Communication architecture of sensor networks

### Medium access control

- Creation of the network infrastructure
- Fairly and efficiently share communication resources between sensor nodes
- Existing MAC protocols (Cellular System, Bluetooth and mobile ad hoc network)

63



## Communication architecture of sensor networks

### MAC for Sensor Networks

- Self-organizing medium access control for sensor networks and Eaves-drop-and-register Algorithm
- CSMA-Based Medium Access
- Hybrid TDMA/PDMA-Based

MAC protocol	Channel access mode	Sensor network specifics	Power consumption
SBACCT and EDR [118]	Fixed allocation of discrete time-slots at fixed frequency	Implementation of large available bandwidth compared to sensor data rate	Random node age during setup and learning nodes off while idle
Hybrid TDMA/TDMA [90]	Controlled frequency over time division	Optimum number of channels is essential for minimum node energy	Hardware-based approach for system energy minimization
CSMA-based [91]	Continuous channel random access	Application phase shift and pretransmit delay	Constant listening time for energy efficiency

63



## Communication architecture of sensor networks

### Power Saving Modes of Operation

- Sensor nodes communicate using **short data packets**
- The **shorter** the packets, the **more** dominance of startup energy
- Operation in a power saving mode is energy efficient only if the **time spent** in that mode is **greater than a certain threshold**.

63



## Communication architecture of sensor networks

### Error Control

- Error control modes in Communication Networks (additional retransmission energy cost)  
Forward Error Correction (FEC)  
Automatic repeat request (ARQ)
- Simple error control codes with low-complexity encoding and decoding might present the best solutions for sensor networks.

64



## Communication architecture of sensor networks

### Open research issues

- MAC for static/mobile sensor networks
- Determination of lower bounds on the energy required for sensor network self-organization
- Error control coding schemes,
- Power saving modes of operation

63



## Communication architecture of sensor networks

### Network layer:

- Power efficiency is always an important consideration.
- Sensor networks are mostly data centric.
- Data aggregation is useful only when it does not hinder the collaborative effort of the sensor nodes.
- An ideal sensor network has attribute-based addressing and location awareness.
- Energy Efficient Routes

64



## Communication architecture of sensor networks

### Network layer:

- **Power efficiency** is always an important consideration.
- Sensor networks are mostly **data centric**.
- **Data aggregation** is useful only when it does not hinder the collaborative effort of the sensor nodes.
- An ideal sensor network has **attribute-based addressing** and **location awareness**.
- **Energy Efficient Routes**

66



## Communication architecture of sensor networks

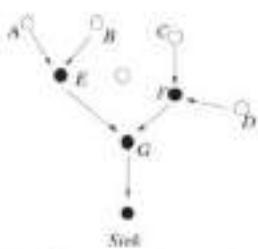
### Data centric operation : Interest Dissemination

- Sinks broadcast the interest
- Sensor nodes broadcast the advertisements
- Attribute-based naming
  - *"The areas where the temperature is over 70°F"*
  - *"The temperature read by a certain node"*

67

# Communication architecture of sensor networks

## Data aggregation



- Solve implosion and overlap Problem
- Aggregation based on same attribute of phenomenon
- Specifics (the locations of reporting sensor nodes) should not be left out

Fig. 5. Example of data aggregation.

68

# Communication architecture of sensor networks

## Several Network Layer Schemes for Sensor Networks

Network layer scheme	Description
SMECN [18]	Creates a subgraph of the sensor network that contains the minimum energy path
Flooding	Broadcasts data to all neighbor nodes regardless if they receive it before or not
Gossiping [19]	Sends data to one randomly selected neighbor
SPIN [15]	Sends data to sensor nodes only if they are interested; has three types of messages (i.e., ADV, REQ, and DATA)
SAR [13]	Creates multiple trees where the root of each tree is one hop neighbor from the sink; selects a tree for data to be routed back to the sink according to the energy resources and additive QoS metric
LEACH [16]	Forms clusters to minimize energy dissipation
Directed diffusion [5]	Sets up gradients for data to flow from source to sink during interest dissemination

69



## Communication architecture of sensor networks

### Open research issues

- New **energy efficient protocols** need to be developed to address higher topology changes and higher scalability.
- New internetworking schemes should be developed to allow easy **communication between the sensor networks and external networks**.

70



## Communication architecture of sensor networks

### Transport layer:

- This layer is especially needed when the system is planned to be accessed through Internet or other external networks.
- TCP/UDP type protocols meet most requirements (not based on global addressing).
- **Little attempt thus far** to propose a scheme or to discuss the issues related to the transport layer of a sensor network in literature.

71



## Communication architecture of sensor networks

### Open research issues

- Because acknowledgments are too costly, new schemes that split the end-to-end communication probably at the sinks may be needed.

72



## Communication architecture of sensor networks

### Application layer:

Management protocol makes the hardware and software of the lower layers transparent to the sensor network management applications.

- Sensor management protocol (SMP)
- Task assignment and data advertisement protocol (TADAP)
- Sensor query and data dissemination protocol (SQDDP)

73



## Communication architecture of sensor networks

### Sensor management protocol (SMP)

- Introducing the **rules** related to data aggregation, attribute-based naming, and clustering to the sensor nodes
- Exchanging **data related to the location**
- **Finding algorithms**
- **Time synchronization** of the sensor nodes
- **Moving sensor nodes**
- Turning sensor nodes on and off
- **Querying** the sensor network configuration and the status of nodes, and **reconfiguring** the sensor network
- **Authentication**, key distribution, and security in data communications

74

## Other Application specific Design Issues

- ▶ Deployment
- ▶ Localization
- ▶ Communications
- ▶ Data Gathering
- ▶ Coverage
- ▶ Tracking
- ▶ Navigation
- ▶ Underwater Issues
- ▶ Visual Sensor Networks

# Deployment

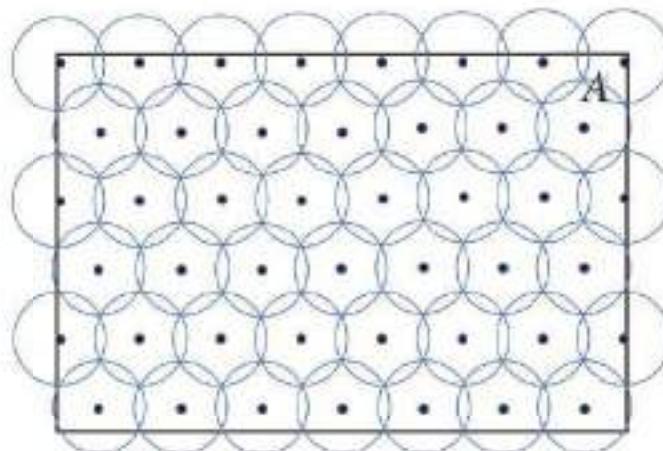
---

## ► WSN deployment

- Full coverage (monitoring quality)
- Minimal number of sensor nodes (cost)

## ► Existing deployment schemes

- Random deployment
- Regular deployment
- Gaussian deployment



76

# Deployment

---

## ► Random Deployment

- Coverage hole
- A large number of sensor nodes (hardware cost)

## ► Mobile Sensors

- Mobility overcomes hole problem
- Hardware cost

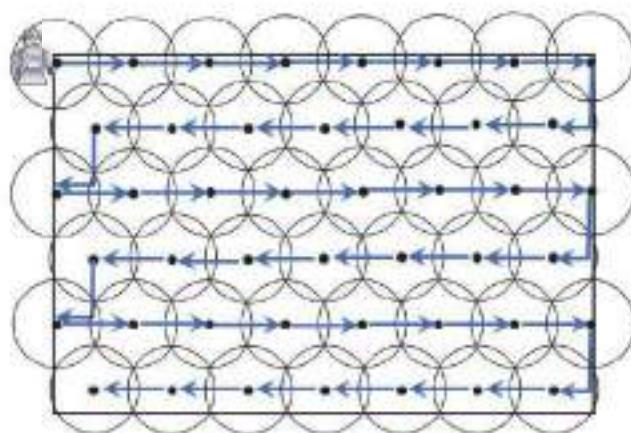
77

# Deployment

---

## ► Robot Deployment

- Regularly deploy static sensor nodes
- Easy to obtain full coverage by using minimal number of static sensors
  - Low hardware cost
  - Easy and simple



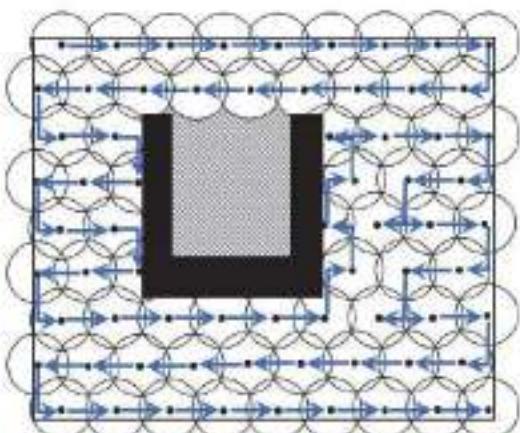
78

# Deployment

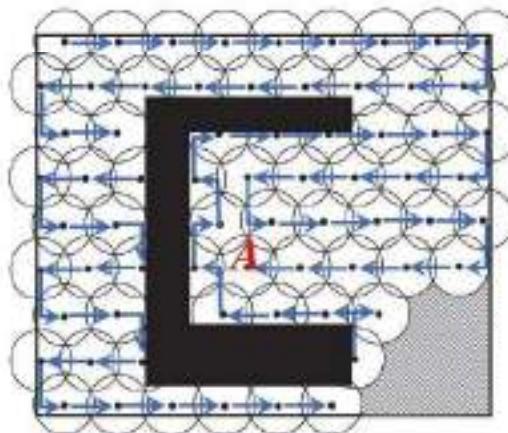
---

## ► Challenges

- There have obstacles in the monitor region.



Hole Problem



Dead-End Problem

79

# **Communications**

---

- ▶ The communication of the WSN
  - ▶ Network Layer Protocol
    - ▶ Multi-casting
    - ▶ Uni-casting
  - ▶ MAC Scheduling
    - ▶ Sleep-Wakeup
    - ▶ Contention
- ▶ Challenges
  - ▶ How to find the shortest path from event point to sink ?
  - ▶ How to balance the lifetime of all the sensors?

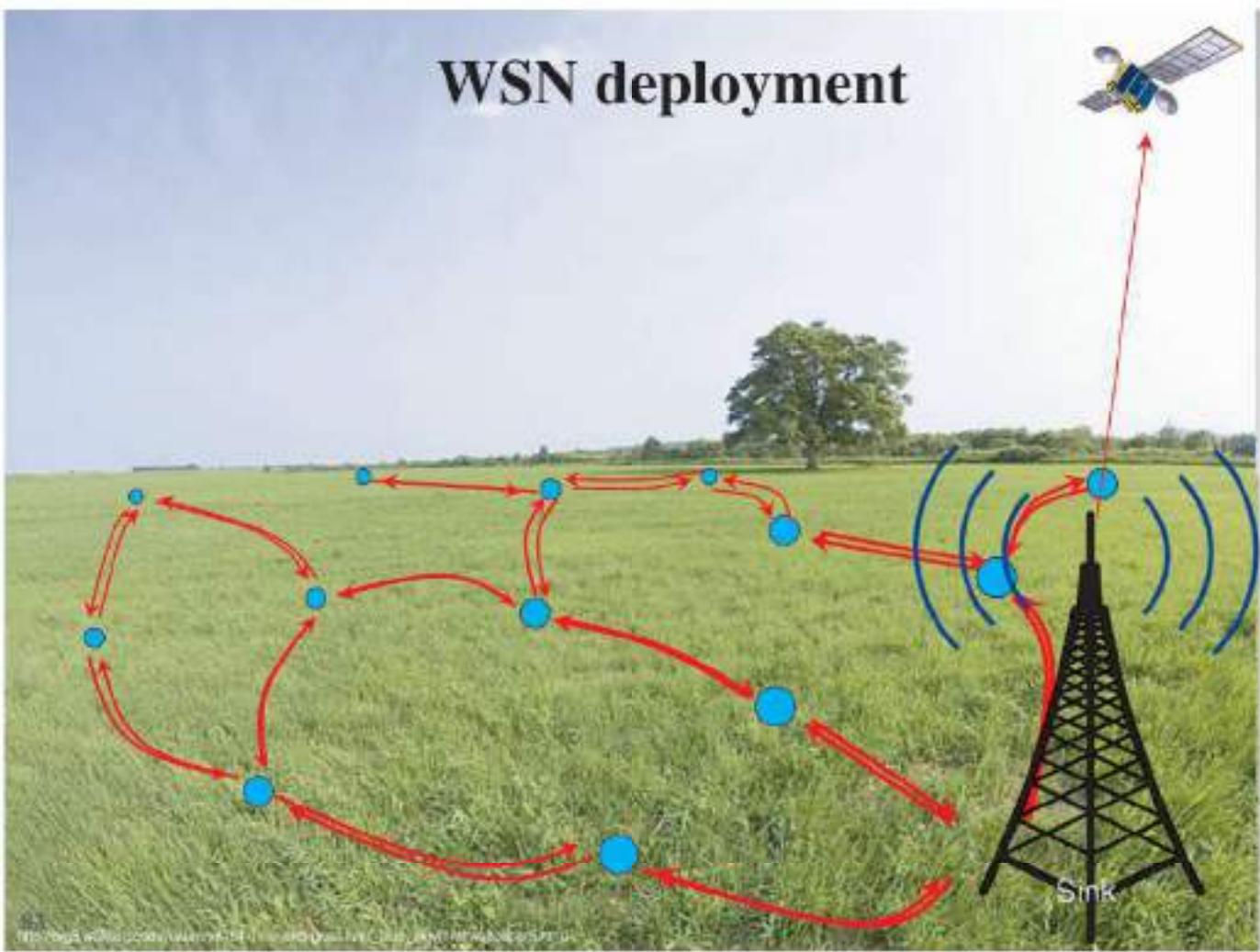
80

# **Communications : QUERY pattern**

---

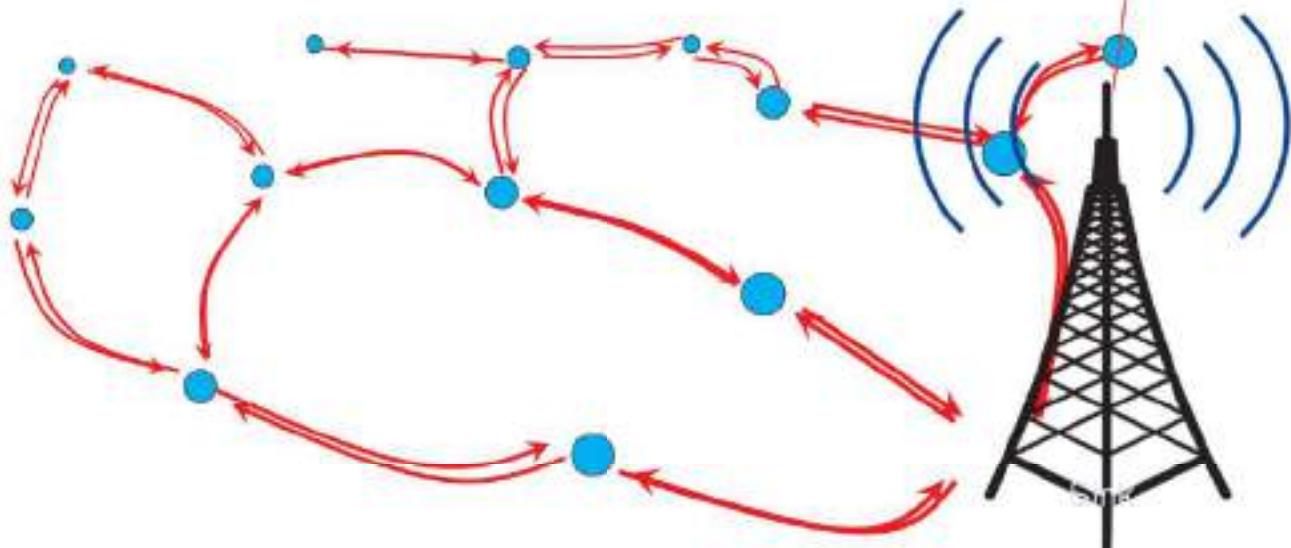
- ▶ Query pattern of the WSN
  - ▶ Periodic
  - ▶ Event driven

81



# Periodic Query

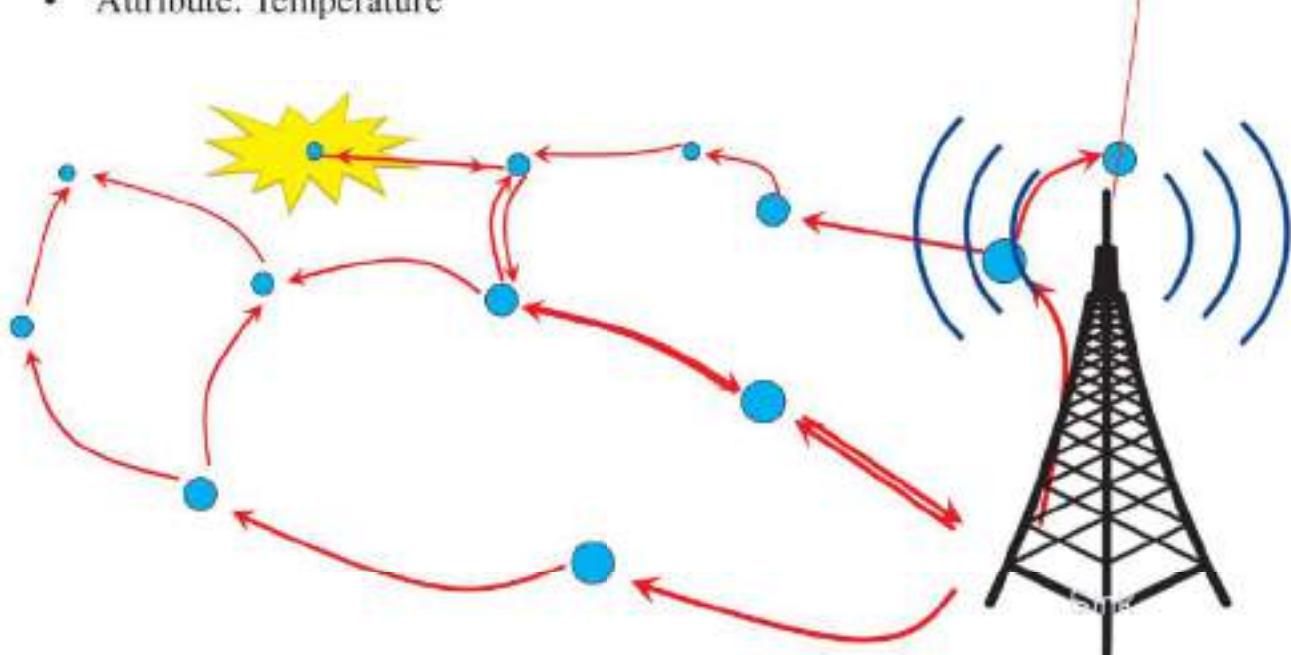
- 
1. Request using flooding
    - Frequency: 1/10 min
    - Duration: 24hr
    - Attribute: Temperature
  2. Report using multi-hop and tree structure
  3. **Report**



84

# Event Driven

- 
1. Request using flooding
    - Frequency: 1/10 min
    - Duration: 24hr
    - Attribute: Temperature
  2. Event happen
  3. **Report**

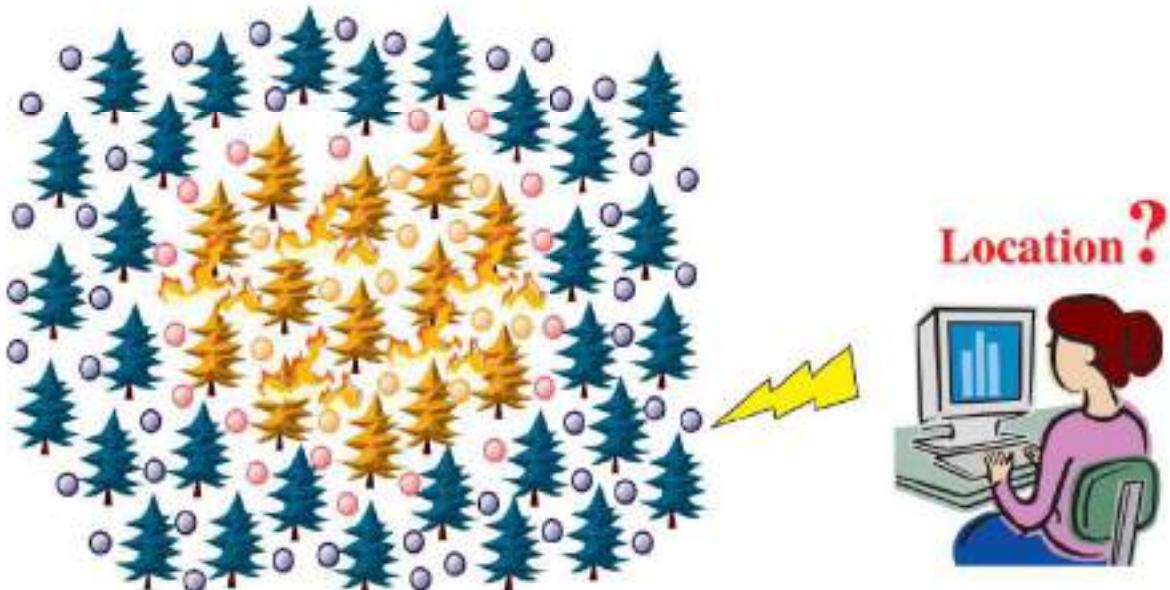


85

# Localization

---

- ▶ The techniques used to identify the position of each sensor node are central to such location-aware operations.



86

# Localization

---

- ▶ The techniques used to identify the position of each sensor node are central to such location-aware operations.
- ▶ Challenges
  - ▶ Accuracy vs. Complexity/Cost
  - ▶ Availability and Feasibility of accurate location systems.  
(e.g. GPS is not available indoor)

87

# Data Gathering

---

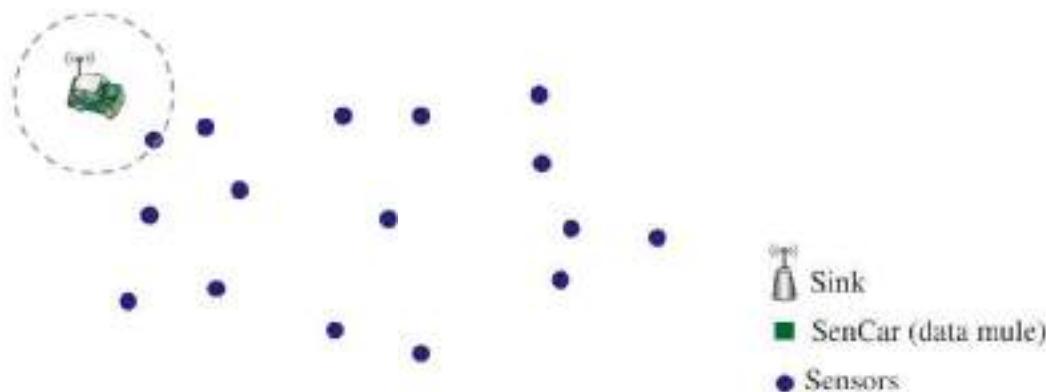
- ▶ Recent years have witnessed a surge of interest in **efficient data gathering** schemes in WSNs.
  - ▶ Routing protocol
  - ▶ Distributed data compression
  - ▶ Efficient transmission schedule
  - ▶ Hierarchical infrastructure (Cluster based networks)
  
- ▶ Mobile sensor data gathering
  - ▶ Data MULEs (Data collector)

88

# Data Gathering

---

- ▶ **Mobile sensor data gathering**
  - ▶ Radically solves the non-uniformity of energy consumption among sensors.
  - ▶ The mobile data collector works well not only in a fully connected network, but also in a disconnected network.

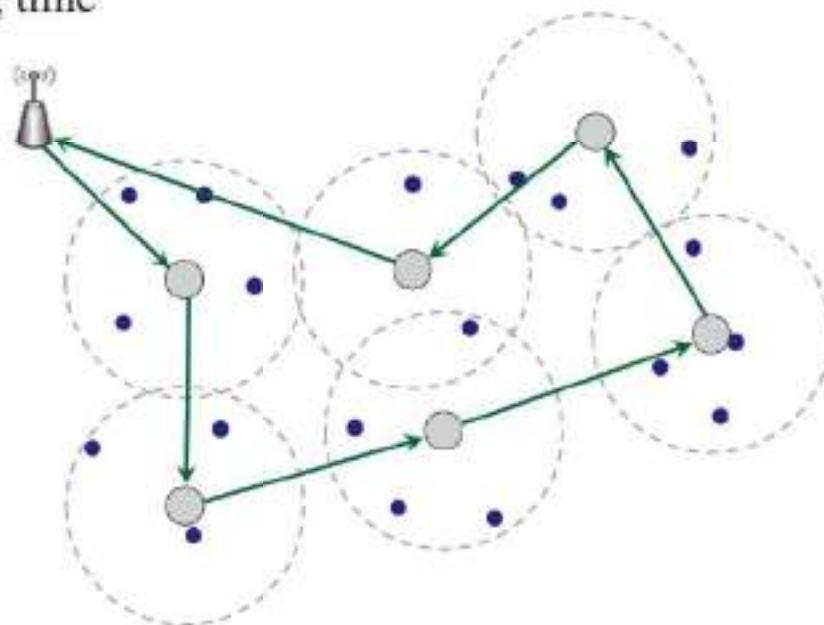


89

## Data Gathering

---

- ▶ The total time of a data gathering tour mainly consists of
  - ▶ Data uploading time
  - ▶ Moving time



90

## Data Gathering

---

- ▶ Challenges
  - ▶ How to select the position of polling point to increase the efficiency of data gathering?
  - ▶ How to combine mobile data gathering with routing technique to reduce the total time of a data gathering ?

91

# Coverage

---

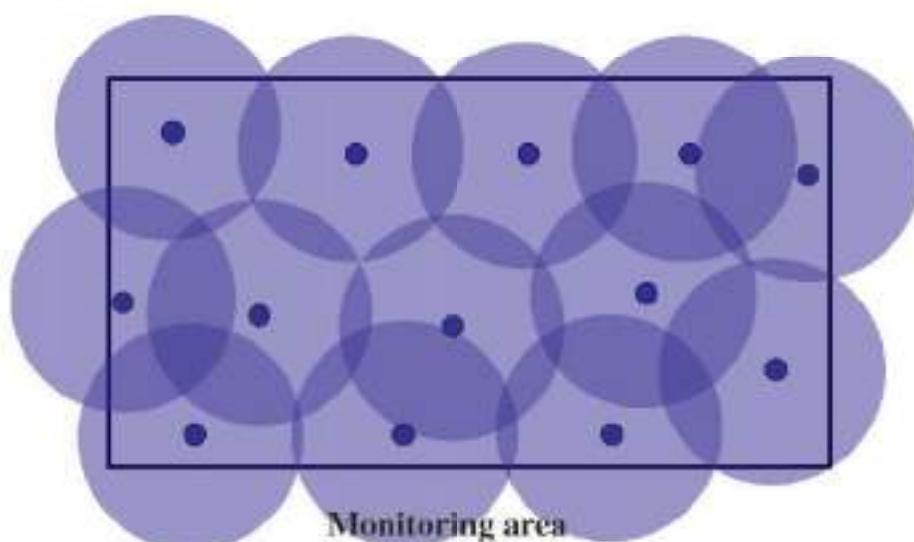
- ▶ Coverage is one of the fundamental problems in Wireless Sensor Networks (WSNs).
  
- ▶ The Coverage of the WSNs
  - ▶ Area coverage
  - ▶ Target coverage
  - ▶ Barrier coverage

92

## Area Coverage

---

- ▶ Two kind of covering sensor for solving problem
  - ▶ Static sensor
  - ▶ Mobile sensor



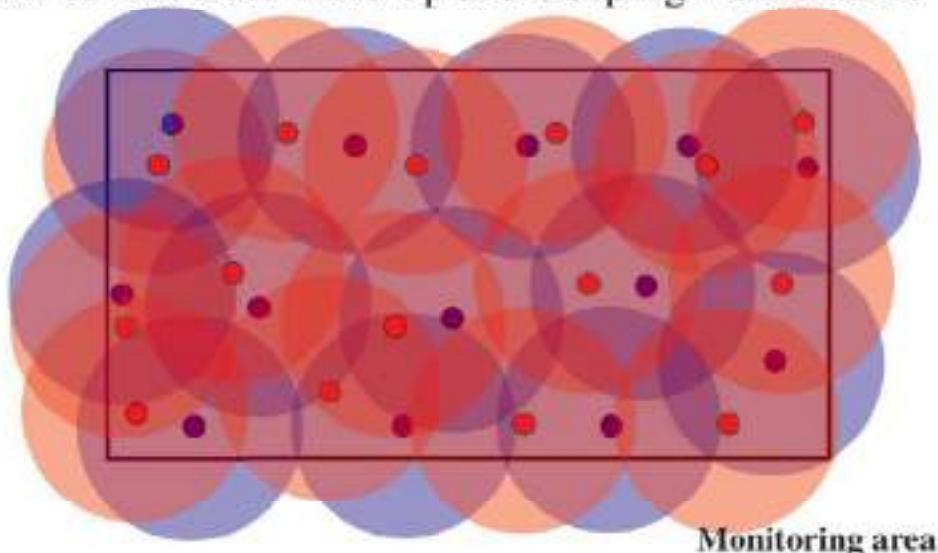
93

# Area Coverage

---

## ► Static sensor

- ▶ How to cover all of the interested area by minimum sensors?
- ▶ How to modulate wake-up and sleeping mechanism?



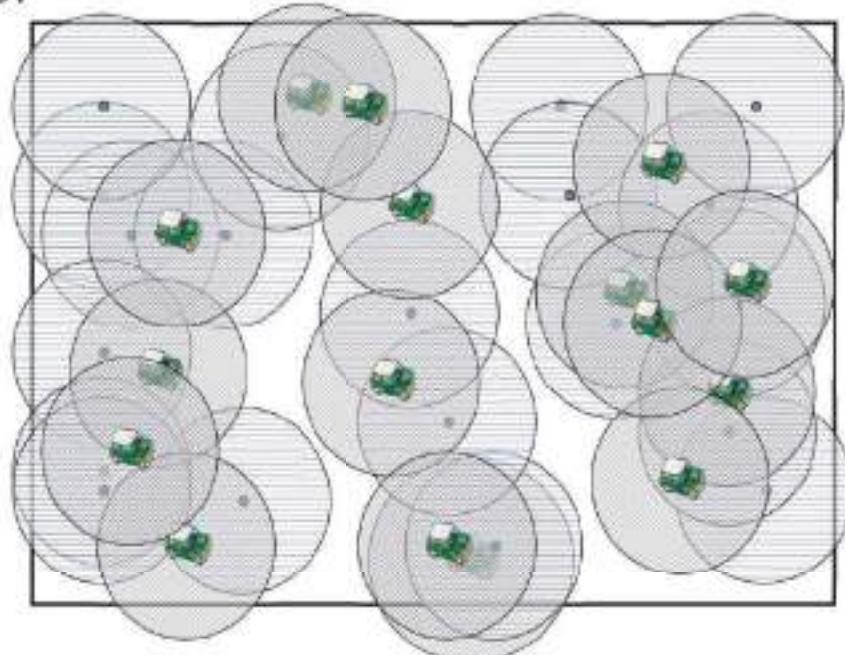
94

# Area Coverage

---

## ► Mobile sensor

- ▶ How to select the minimum mobile sensors to cover all of the hole?



95

# Barrier Coverage



96

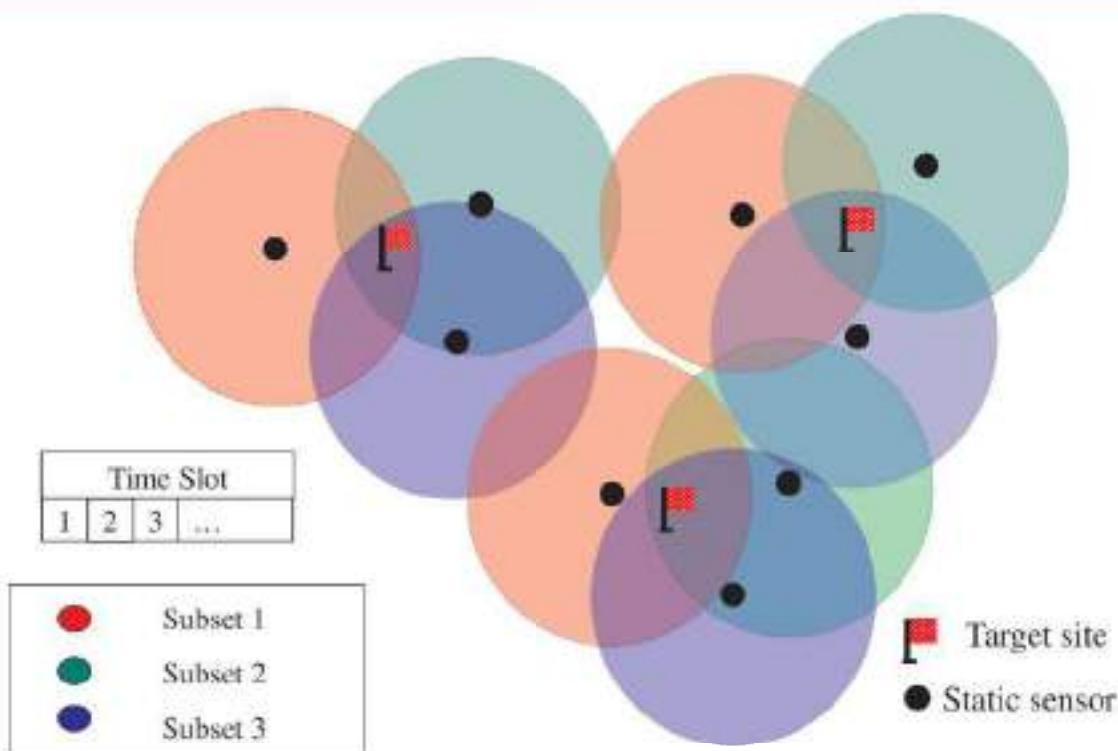
# Barrier Coverage

- ▶ Challenges
  - ▶ How to establish  $k$ -barrier coverage by minimizing sensors number?
  - ▶ How to extend lifetime as long as possible?

97

# Target Coverage

---



98

# Target Coverage

---

- ▶ Challenges
  - ▶ Connectivity.
  - ▶ How to modulate wake-up and sleeping mechanism?
  - ▶ How to cover more targets by the minimum sensors?

99

# Target Tracking

---

- ▶ Object tracking is an important issue of wireless sensor networks.

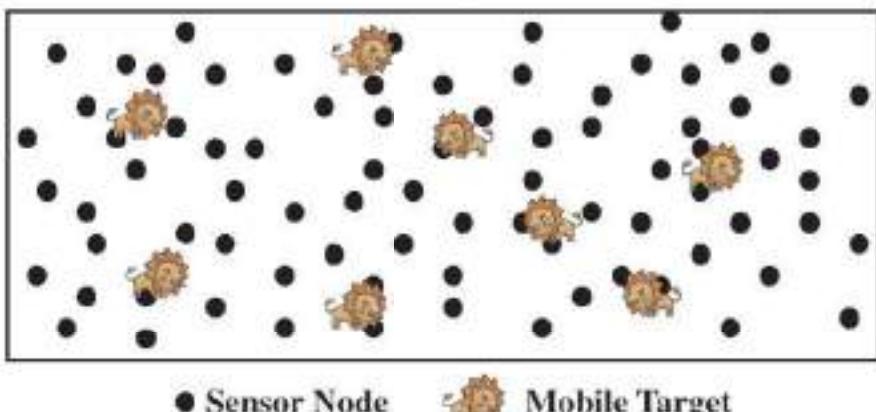


100

## Tracking

---

- ▶ Challenges
  - ▶ Improve tracking accuracy
  - ▶ How can we track the target according to tracking quality that users require?
    - ▶ Minimize of sensor nodes
    - ▶ Long network life time
  - ▶ How to track more than one target at the same time?

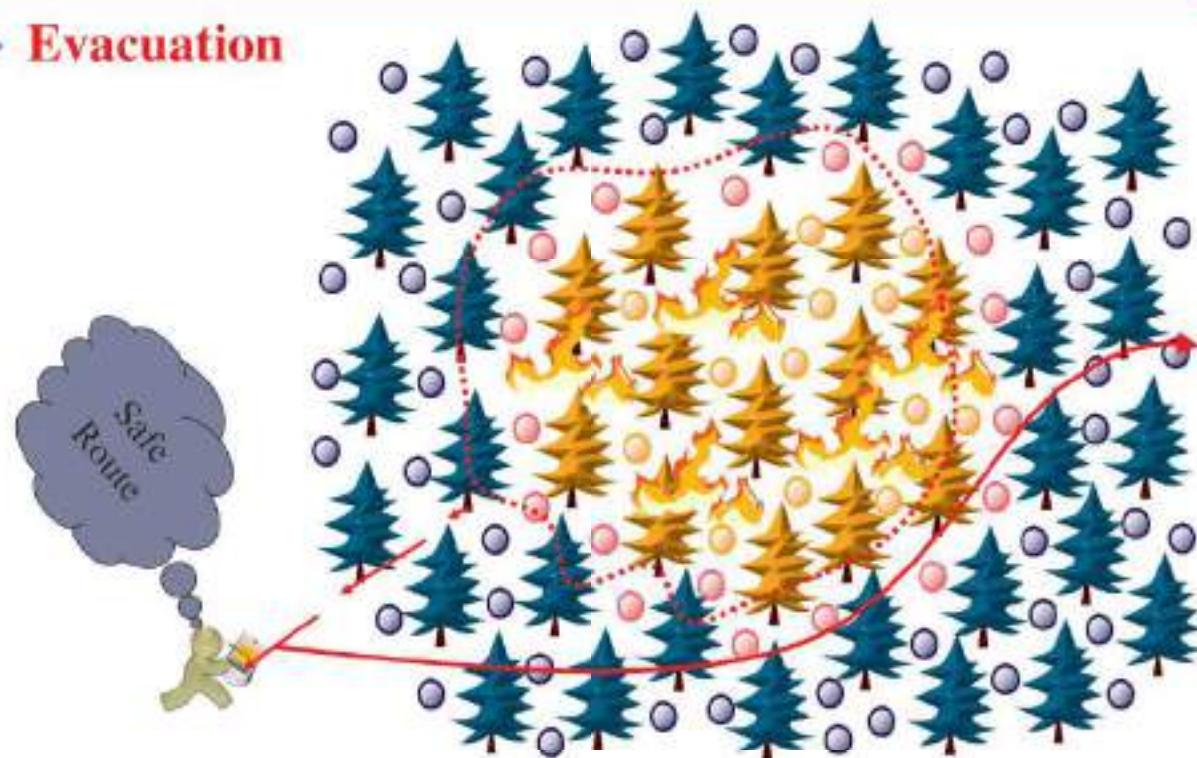


101

# Navigation

---

## ► Evacuation



102

# Navigation

---

## ► Problem & Challenges

- Evacuation of disaster
  - When the disaster occur, how to decide a security route and guide the users keep away from dangerous region by WSN?
- Target tracking & guiding
  - How to predict the trajectory of moving targets and guide the users to catch up with targets by WSN?

103

# Underwater WSNs

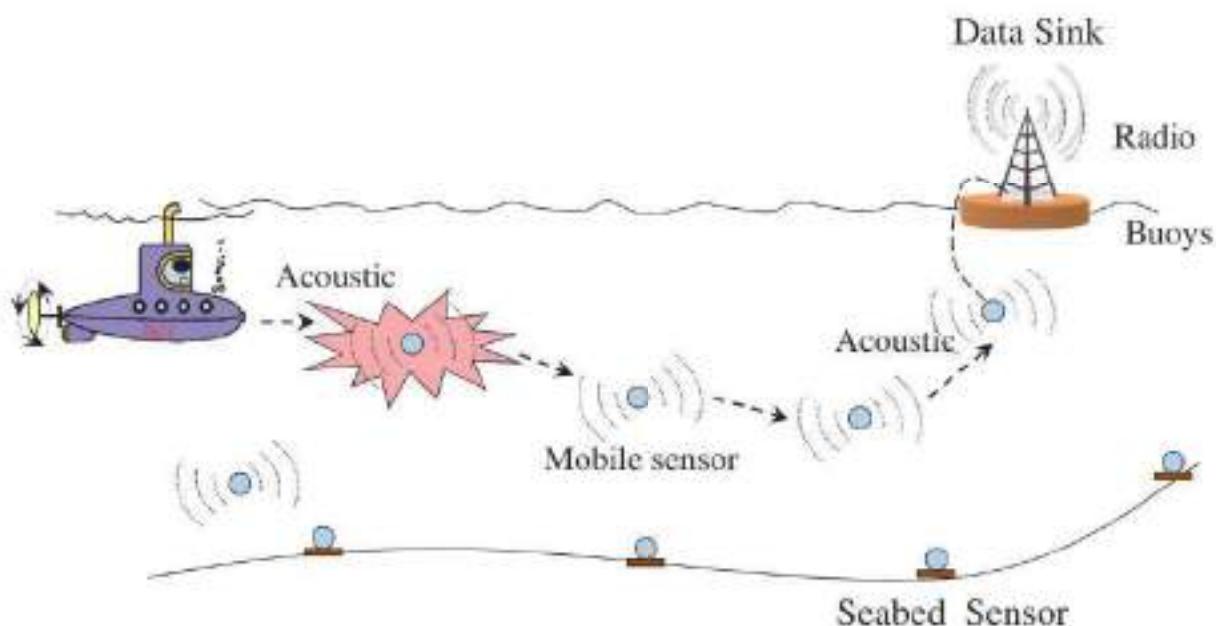
---

- ▶ Growing interest in monitoring the marine environment.
  - ▶ scientific exploration
  - ▶ commercial exploitation
  - ▶ coastline protection
  - ▶ Security surveillance

104

# Underwater WSNs

---



105

## **Challenges : Underwater WSNs**

---

- ▶ **Challenges posed by Acoustic Channel**

- ▶ Impact of Ocean Current
- ▶ Acoustic Wave Propagation
- ▶ Low Propagation Speed
- ▶ High and Variable Propagation Delay
- ▶ High Bit Error Rates
- ▶ Limited Bandwidth
- ▶ Low Battery Power
- ▶ Localization Problem

106

## **Challenges : Underwater WSNs**

---

- ▶ **Problems Associated with MAC Protocol of UWSNs**

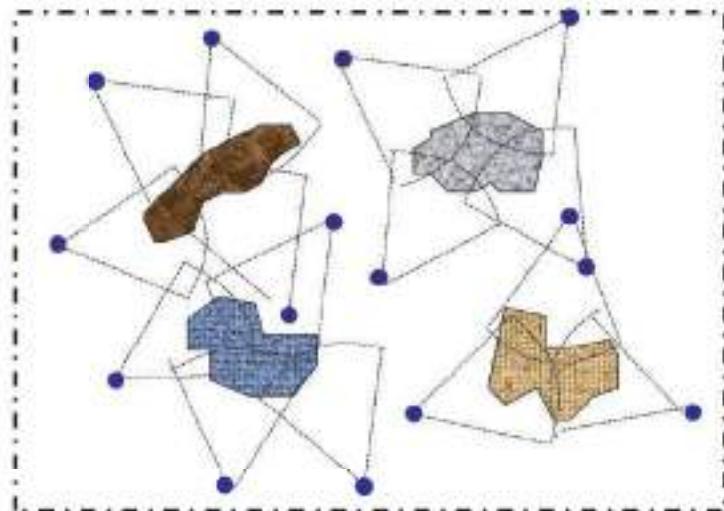
- ▶ Network Topology and Deployment in UWSN
- ▶ Energy Consumption
- ▶ Synchronization
- ▶ Hidden Node and Exposed Node Problem
- ▶ High Delay Associated in Handshaking
- ▶ Power Waste in Collision

107

# Visual Sensor Networks

---

- ▶ Assume that the **shape of monitor region** is known.
- ▶ How to deploy camera sensor
  - ▶ minimum number of camera nodes
  - ▶ **1-coverage , 2-coverage , or k-coverage**

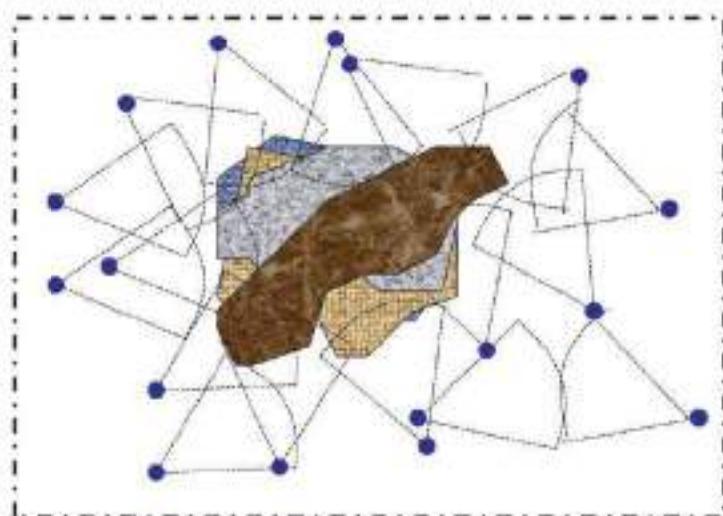


108

# Visual Sensor Networks

---

- ▶ Random deployment of camera sensors
- ▶ To monitor the dynamic changes of the shape of monitor region
- ▶ Camera sensor
  - ▶ Mobility & Rotation
  - ▶ Mobility & Non-rotation
  - ▶ Non-mobility & Rotation
  - ▶ Non-mobility & Non-rotation



109

# Visual Sensor Networks

---

- ▶ Challenges
  - ▶ How to cover the monitoring area
    - ▶ by minimum number of camera nodes
    - ▶ by minimum moving distance of camera nodes
    - ▶ by minimum rotation angle of camera nodes
  - ▶ Find maximum number of sets of camera nodes
    - ▶ Schedule each set of camera nodes to sleep or wake up
  - ▶ Achieve 1-coverage, or 2-coverage, or k-coverage

110

## Recommend Reading

---

- ▶ See in Google drive following PDF:

**WSNbook (Karl) :- Chapter 1, 2**

**Paper: WSN – a Survey**

- ▶ **Next – Unit 2 (Wireless network fundamentals)**

111

# **CS 442 Unit 1 - Recommended Reading**

---

- ▶ See in Google drive following PDF:

**Class slides**

**Paper: Wireless sensor networks: a survey (By IF Akyildiz et al)**

**Karl's book: Chap 1,2**

- ▶ Next – Unit 2 (Wireless network fundamentals)

## Wireless sensor networks: a survey

I.F. Akyildiz, W. Su\*, Y. Sankarasubramaniam, E. Cayirci

*Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA*

Received 12 December 2001; accepted 20 December 2001

---

### Abstract

This paper describes the concept of sensor networks which has been made viable by the convergence of micro-electro-mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored. Open research issues for the realization of sensor networks are also discussed. © 2002 Published by Elsevier Science B.V.

**Keywords:** Wireless sensor networks; Ad hoc networks; Application layer; Transport layer; Networking layer; Routing; Data link layer; Medium access control; Error control; Physical layer; Power aware protocols

---

### 1. Introduction

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Sensor networks represent a significant improve-

ment over traditional sensors, which are deployed in the following two ways [39]:

- Sensors can be positioned far from the actual *phenomenon*, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required.
- Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused.

A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it.

\* Corresponding author. Tel.: +1-404-894-5141; fax: +1-404-894-7883.

E-mail addresses: [ian@ece.gatech.edu](mailto:ian@ece.gatech.edu) (I.F. Akyildiz), [weil-ian@ece.gatech.edu](mailto:weil-ian@ece.gatech.edu) (W. Su), [yogi@ece.gatech.edu](mailto:yogi@ece.gatech.edu) (Y. Sankarasubramaniam), [erdal@ece.gatech.edu](mailto:erdal@ece.gatech.edu) (E. Cayirci).

The position of sensor nodes need not be engineered or pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

The above described features ensure a wide range of applications for sensor networks. Some of the application areas are health, military, and security. For example, the physiological data about a patient can be monitored remotely by a doctor. While this is more convenient for the patient, it also allows the doctor to better understand the patient's current condition. Sensor networks can also be used to detect foreign chemical agents in the air and the water. They can help to identify the type, concentration, and location of pollutants. In essence, sensor networks will provide the end user with intelligence and a better understanding of the environment. We envision that, in future, wireless sensor networks will be an integral part of our lives, more so than the present-day personal computers.

Realization of these and other sensor network applications require wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad hoc networks [65] are outlined below:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.

- Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

Since large number of sensor nodes are densely deployed, neighbor nodes may be very close to each other. Hence, multihop communication in sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the transmission power levels can be kept low, which is highly desired in covert operations. Multihop communication can also effectively overcome some of the signal propagation effects experienced in long-distance wireless communication.

One of the most important constraints on sensor nodes is the low power consumption requirement. Sensor nodes carry limited, generally irreplaceable, power sources. Therefore, while traditional networks aim to achieve high quality of service (QoS) provisions, sensor network protocols must focus primarily on power conservation. They must have inbuilt trade-off mechanisms that give the end user the option of prolonging network lifetime at the cost of lower throughput or higher transmission delay.

Many researchers are currently engaged in developing schemes that fulfill these requirements. In this paper, we present a survey of protocols and algorithms proposed thus far for sensor networks. Our aim is to provide a better understanding of the current research issues in this field. We also attempt an investigation into pertaining design constraints and outline the use of certain tools to meet the design objectives.

The remainder of the paper is organized as follows: In Section 2, we present some potential sensor network applications which show the usefulness of sensor networks. In Section 3, we discuss the factors that influence the sensor network design. We provide a detailed investigation of current proposals in this area in Section 4. We conclude our paper in Section 5.

## 2. Sensor networks applications

Sensor networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions that include the following [23]:

- temperature,
- humidity,
- vehicular movement,
- lightning condition,
- pressure,
- soil makeup,
- noise levels,
- the presence or absence of certain kinds of objects,
- mechanical stress levels on attached objects, and
- the current characteristics such as speed, direction, and size of an object.

Sensor nodes can be used for continuous sensing, event detection, event ID, location sensing, and local control of actuators. The concept of micro-sensing and wireless connection of these nodes promise many new application areas. We categorize the applications into military, environment, health, home and other commercial areas. It is possible to expand this classification with more categories such as space exploration, chemical processing and disaster relief.

### 2.1. Military applications

Wireless sensor networks can be an integral part of military *command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting* (C4ISRT) systems. The rapid deployment, self-organization and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military C4ISRT. Since sensor networks are based on the dense deployment of disposable and low-cost sensor nodes, destruction of some nodes by hostile actions does not affect a military operation as much as the destruction of a traditional sensor, which makes sensor networks concept a better approach for battlefields. Some of the military

applications of sensor networks are monitoring friendly forces, equipment and ammunition; battlefield surveillance; reconnaissance of opposing forces and terrain; targeting; battle damage assessment; and nuclear, biological and chemical (NBC) attack detection and reconnaissance.

*Monitoring friendly forces, equipment and ammunition:* Leaders and commanders can constantly monitor the status of friendly troops, the condition and the availability of the equipment and the ammunition in a battlefield by the use of sensor networks. Every troop, vehicle, equipment and critical ammunition can be attached with small sensors that report the status. These reports are gathered in sink nodes and sent to the troop leaders. The data can also be forwarded to the upper levels of the command hierarchy while being aggregated with the data from other units at each level.

*Battlefield surveillance:* Critical terrains, approach routes, paths and straits can be rapidly covered with sensor networks and closely watched for the activities of the opposing forces. As the operations evolve and new operational plans are prepared, new sensor networks can be deployed anytime for battlefield surveillance.

*Reconnaissance of opposing forces and terrain:* Sensor networks can be deployed in critical terrains, and some valuable, detailed, and timely intelligence about the opposing forces and terrain can be gathered within minutes before the opposing forces can intercept them.

*Targeting:* Sensor networks can be incorporated into guidance systems of the intelligent ammunition.

*Battle damage assessment:* Just before or after attacks, sensor networks can be deployed in the target area to gather the battle damage assessment data.

*Nuclear, biological and chemical attack detection and reconnaissance:* In chemical and biological warfare, being close to ground zero is important for timely and accurate detection of the agents. Sensor networks deployed in the friendly region and used as a chemical or biological warning system can provide the friendly forces with critical reaction time, which drops casualties drastically. We can also use sensor networks for detailed

reconnaissance after an NBC attack is detected. For instance, we can make a nuclear reconnaissance without exposing a recce team to nuclear radiation.

## 2.2. Environmental applications

Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that affect crops and livestock; irrigation; macroinstruments for large-scale Earth monitoring and planetary exploration; chemical/biological detection; precision agriculture; biological, Earth, and environmental monitoring in marine, soil, and atmospheric contexts; forest fire detection; meteorological or geophysical research; flood detection; bio-complexity mapping of the environment; and pollution study [2,6–8,10,11,14, 31,35,39,40,42,61,81,88,89].

*Forest fire detection:* Since sensor nodes may be strategically, randomly, and densely deployed in a forest, sensor nodes can relay the exact origin of the fire to the end users before the fire is spread uncontrollable. Millions of sensor nodes can be deployed and integrated using radio frequencies/optical systems. Also, they may be equipped with effective power scavenging methods [12], such as solar cells, because the sensors may be left unattended for months and even years. The sensor nodes will collaborate with each other to perform distributed sensing and overcome obstacles, such as trees and rocks, that block wired sensors' line of sight.

*Biocomplexity mapping of the environment* [11]: A biocomplexity mapping of the environment requires sophisticated approaches to integrate information across temporal and spatial scales [26,87]. The advances of technology in the remote sensing and automated data collection have enabled higher spatial, spectral, and temporal resolution at a geometrically declining cost per unit area [15]. Along with these advances, the sensor nodes also have the ability to connect with the Internet, which allows remote users to control, monitor and observe the biocomplexity of the environment.

Although satellite and airborne sensors are useful in observing large biodiversity, e.g., spatial complexity of dominant plant species, they are not fine grain enough to observe small size biodiversity, which makes up most of the biodiversity in an ecosystem [43]. As a result, there is a need for ground level deployment of wireless sensor nodes to observe the biocomplexity [29,30]. One example of biocomplexity mapping of the environment is done at the James Reserve in Southern California [11]. Three monitoring grids with each having 25–100 sensor nodes will be implemented for fixed view multimedia and environmental sensor data loggers.

*Flood detection* [7]: An example of a flood detection is the ALERT system [90] deployed in the US. Several types of sensors deployed in the ALERT system are rainfall, water level and weather sensors. These sensors supply information to the centralized database system in a pre-defined way. Research projects, such as the COUGAR Device Database Project at Cornell University [7] and the DataSpace project at Rutgers [38], are investigating distributed approaches in interacting with sensor nodes in the sensor field to provide snapshot and long-running queries.

*Precision Agriculture:* Some of the benefits is the ability to monitor the pesticides level in the drinking water, the level of soil erosion, and the level of air pollution in realtime.

## 2.3. Health applications

Some of the health applications for sensor networks are providing interfaces for the disabled; integrated patient monitoring; diagnostics; drug administration in hospitals; monitoring the movements and internal processes of insects or other small animals; telemonitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital [8,42,60,71,88].

*Telemonitoring of human physiological data:* The physiological data collected by the sensor networks can be stored for a long period of time [41], and can be used for medical exploration [62]. The installed sensor networks can also monitor and detect elderly people's behavior, e.g., a fall [9,16]. These small sensor nodes allow the subject a

greater freedom of movement and allow doctors to identify pre-defined symptoms earlier [56]. Also, they facilitate a higher quality of life for the subjects compared to the treatment centers [5]. A “Health Smart Home” is designed in the Faculty of Medicine in Grenoble—France to validate the feasibility of such system [60].

*Tracking and monitoring doctors and patients inside a hospital:* Each patient has small and light weight sensor nodes attached to them. Each sensor node has its specific task. For example, one sensor node may be detecting the heart rate while another is detecting the blood pressure. Doctors may also carry a sensor node, which allows other doctors to locate them within the hospital.

*Drug administration in hospitals:* If sensor nodes can be attached to medications, the chance of getting and prescribing the wrong medication to patients can be minimized. Because, patients will have sensor nodes that identify their allergies and required medications. Computerized systems as described in [78] have shown that they can help minimize adverse drug events.

#### 2.4. Home applications

*Home automation:* As technology advances, smart sensor nodes and actuators can be buried in appliances, such as vacuum cleaners, micro-wave ovens, refrigerators, and VCRs [67]. These sensor nodes inside the domestic devices can interact with each other and with the external network via the Internet or Satellite. They allow end users to manage home devices locally and remotely more easily.

*Smart environment:* The design of smart environment can have two different perspectives, i.e., human-centered and technology-centered [1]. For human-centered, a smart environment has to adapt to the needs of the end users in terms of input/output capabilities. For technology-centered, new hardware technologies, networking solutions, and middleware services have to be developed. A scenario of how sensor nodes can be used to create a smart environment is described in [36]. The sensor nodes can be embedded into furniture and appliances, and they can communicate with each other

and the room server. The room server can also communicate with other room servers to learn about the services they offered, e.g., printing, scanning, and faxing. These room servers and sensor nodes can be integrated with existing embedded devices to become self-organizing, self-regulated, and adaptive systems based on control theory models as described in [36]. Another example of smart environment is the “Residential Laboratory” at Georgia Institute of Technology [21]. The computing and sensing in this environment has to be reliable, persistent, and transparent.

#### 2.5. Other commercial applications

Some of the commercial applications are monitoring material fatigue; building virtual keyboards; managing inventory; monitoring product quality; constructing smart office spaces; environmental control in office buildings; robot control and guidance in automatic manufacturing environments; interactive toys; interactive museums; factory process control and automation; monitoring disaster area; smart structures with sensor nodes embedded inside; machine diagnosis; transportation; factory instrumentation; local control of actuators; detecting and monitoring car thefts; vehicle tracking and detection; and instrumentation of semiconductor processing chambers, rotating machinery, wind tunnels, and anechoic chambers [2,8,14,23,24,42,63,69–71,77,88].

*Environmental control in office buildings:* The air conditioning and heat of most buildings are centrally controlled. Therefore, the temperature inside a room can vary by few degrees; one side might be warmer than the other because there is only one control in the room and the air flow from the central system is not evenly distributed. A distributed wireless sensor network system can be installed to control the air flow and temperature in different parts of the room. It is estimated that such distributed technology can reduce energy consumption by two quadrillion British Thermal Units (BTUs) in the US, which amounts to saving of \$55 billion per year and reducing 35 million metric tons of carbon emissions [71].

*Interactive museums:* In the future, children will be able to interact with objects in museums to learn more about them. These objects will be able to respond to their touch and speech. Also, children can participate in real time cause-and-effect experiments, which can teach them about science and environment. In addition, the wireless sensor networks can provide paging and localization inside the museum. An example of such museums is the San Francisco Exploratorium that features a combination of data measurements and cause-and-effect experiments [71].

*Detecting and monitoring car thefts:* Sensor nodes are being deployed to detect and identify threats within a geographic region and report these threats to remote end users by the Internet for analysis [69].

*Managing inventory control:* Each item in a warehouse may have a sensor node attached. The end users can find out the exact location of the item and tally the number of items in the same category. If the end users want to insert new inventories, all the users need to do is to attach the appropriate sensor nodes to the inventories. The end users can track and locate where the inventories are at all times.

*Vehicle tracking and detection:* There are two approaches as described in [77] to track and detect the vehicle: first, the line of bearing of the vehicle is determined locally within the clusters and then it is forwarded to the base station, and second, the raw data collected by the sensor nodes are forwarded to the base station to determine the location of the vehicle.

### 3. Factors influencing sensor network design

A sensor network design is influenced by many factors, which include *fault tolerance; scalability; production costs; operating environment; sensor network topology; hardware constraints; transmission media; and power consumption*. These factors are addressed by many researchers as surveyed in this paper. However, none of these studies has a full integrated view of all factors that are driving the design of sensor networks and sensor nodes. These factors are important because they serve as a

guideline to design a protocol or an algorithm for sensor networks. In addition, these influencing factors can be used to compare different schemes.

#### 3.1. Fault tolerance

Some sensor nodes may fail or be blocked due to lack of power, have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures [37,55,75]. The reliability  $R_k(t)$  or fault tolerance of a sensor node is modelled in [37] using the Poisson distribution to capture the probability of not having a failure within the time interval  $(0, t)$ :

$$R_k(t) = \exp(-\lambda_k t) \quad (1)$$

where  $\lambda_k$  and  $t$  are the failure rate of sensor node  $k$  and the time period, respectively.

Note that protocols and algorithms may be designed to address the level of fault tolerance required by the sensor networks. If the environment where the sensor nodes are deployed has little interference, then the protocols can be more relaxed. For example, if sensor nodes are being deployed in a house to keep track of humidity and temperature levels, the fault tolerance requirement may be low since this kind of sensor networks is not easily damaged or interfered by environmental noise. On the other hand, if sensor nodes are being deployed in a battlefield for surveillance and detection, then the fault tolerance has to be high because the sensed data are critical and sensor nodes can be destroyed by hostile actions. As a result, the fault tolerance level depends on the application of the sensor networks, and the schemes must be developed with this in mind.

#### 3.2. Scalability

The number of sensor nodes deployed in studying a phenomenon may be in the order of hundreds or thousands. Depending on the application, the number may reach an extreme value of millions. The new schemes must be able to work

with this number of nodes. They must also utilize the high density nature of the sensor networks. The density can range from few sensor nodes to few hundred sensor nodes in a region, which can be less than 10 m in diameter [14]. The density can be calculated according to [8] as

$$\mu(R) = (N\pi R^2)/A \quad (2)$$

where  $N$  is the number of scattered sensor nodes in region  $A$ ; and  $R$ , the radio transmission range. Basically,  $\mu(R)$  gives the number of nodes within the transmission radius of each node in region  $A$ .

In addition, the number of nodes in a region can be used to indicate the node density. The node density depends on the application in which the sensor nodes are deployed. For machine diagnosis application, the node density is around 300 sensor nodes in a  $5 \times 5 \text{ m}^2$  region, and the density for the vehicle tracking application is around 10 sensor nodes per region [77]. In general, the density can be as high as 20 sensor nodes/ $\text{m}^3$  [77]. A home may contain around two dozens of home appliances containing sensor nodes [67], but this number will grow if sensor nodes are embedded into furniture and other miscellaneous items. For habitat monitoring application, the number of sensor nodes ranges from 25 to 100 per region [11]. The density will be extremely high when a person normally containing hundreds of sensor nodes, which are embedded in eye glasses, clothing, shoes, watch, jewelry, and human body, is sitting inside a stadium watching a basketball, football, or baseball game.

### 3.3. Production costs

Since the sensor networks consist of a large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the networks. If the cost of the network is more expensive than deploying traditional sensors, then the sensor network is not cost-justified. As a result, the cost of each sensor node has to be kept low. The state-of-the-art technology allows a Bluetooth radio system to be less than 10\$ [71]. Also, the price of a PicoNode is targeted to be less than 1\$ [70]. The cost of a sensor node should be much less than 1\$ in order for the sensor network to be

feasible [70]. The cost of a Bluetooth radio, which is known to be a low-cost device, is even 10 times more expensive than the targeted price for a sensor node. Note that a sensor node also has some additional units such as sensing and processing units as described in Section 3.4. In addition, it may be equipped with a location finding system, mobilizer, or power generator depending on the applications of the sensor networks. As a result, the cost of a sensor node is a very challenging issue given the amount of functionalities with a price of much less than a dollar.

### 3.4. Hardware constraints

A sensor node is made up of four basic components as shown in Fig. 1: a *sensing unit*, a *processing unit*, a *transceiver unit* and a *power unit*. They may also have application dependent additional components such as a *location finding system*, a *power generator* and a *mobilizer*. Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units may be supported by a power scavenging unit such as solar cells. There are also other subunits, which are application dependent.

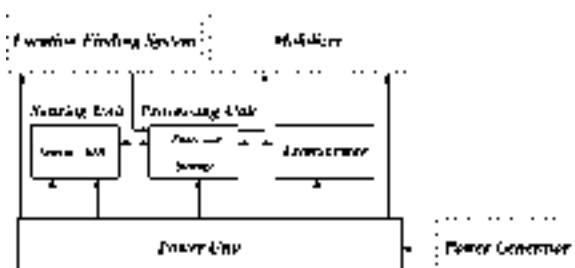


Fig. 1. The components of a sensor node.

Most of the sensor network routing techniques and sensing tasks require the knowledge of location with high accuracy. Thus, it is common that a sensor node has a location finding system. A mobilizer may sometimes be needed to move sensor nodes when it is required to carry out the assigned tasks.

All of these subunits may need to fit into a matchbox-sized module [39]. The required size may be smaller than even a cubic centimeter [69] which is light enough to remain suspended in the air. Apart from the size, there are also some other stringent constraints for sensor nodes. These nodes must [42]

- consume extremely low power,
- operate in high volumetric densities,
- have low production cost and be dispensable,
- be autonomous and operate unattended,
- be adaptive to the environment.

Since the sensor nodes are often inaccessible, the lifetime of a sensor network depends on the lifetime of the power resources of the nodes. Power is also a scarce resource due to the size limitations. For instance, the total stored energy in a *smart dust mote* is on the order of 1 J [69]. For wireless integrated network sensors (WINS) [86], the total average system supply currents must be less than 30  $\mu$ A to provide long operating life. WINS nodes are powered from typical lithium (Li) coin cells (2.5 cm in diameter and 1 cm in thickness) [86]. It is possible to extend the lifetime of the sensor networks by energy scavenging [71], which means extracting energy from the environment. Solar cells is an example for the techniques used for energy scavenging.

The transceiver unit of sensor nodes may be a passive or active optical device as in smart dust motes [69] or a radio frequency (RF) device. RF communications require modulation, band pass, filtering, demodulation and multiplexing circuitry, which make them more complex and expensive. Also, the path loss of the transmitted signal between two sensor nodes may be as high as the fourth order exponent of the distance between them, because the antennas of the sensor nodes are close to the ground [69]. Nevertheless, RF com-

munication is preferred in most of the ongoing sensor network research projects, because the packets conveyed in sensor networks are small, data rates are low (i.e., generally less than 1 Hz) [71], and the frequency re-use is high due to short communication distances. These characteristics also make it possible to use low duty cycle radio electronics for sensor networks. However, designing energy efficient and low duty cycle radio circuits is still technically challenging, and current commercial radio technologies such as those used in Bluetooth is not efficient enough for sensor networks because turning them on and off consumes much energy [77].

Though the higher computational powers are being made available in smaller and smaller processors, processing and memory units of sensor nodes are still scarce resources. For instance, the processing unit of a smart dust mote prototype is a 4 MHz Atmel AVR 8535 micro-controller with 8 KB instruction flash memory, 512 bytes RAM and 512 bytes EEPROM [66]. TinyOS operating system is used on this processor, which has 3500 bytes OS code space and 4500 bytes available code space. The processing unit of another sensor node prototype, namely  $\mu$ AMPS wireless sensor node, has a 59–206 MHz SA-1110 micro-processor [77]. A multithreaded  $\mu$ -OS operating system is run on  $\mu$ AMPS wireless sensor nodes.

Most of the sensing tasks require the knowledge of position. Since sensor nodes are generally deployed randomly and run unattended, they need to corporate with a location finding system. Location finding systems are also required by many of the proposed sensor network routing protocols as explained in Section 4. It is often assumed that each sensor node will have a global positioning system (GPS) unit that has at least 5 m accuracy [48]. In [74] it is argued that equipping all sensor nodes with a GPS is not viable for sensor networks. An alternative approach where a limited number of nodes use GPS and help the other nodes to find out their locations terrestrially as proposed in [74].

### 3.5. Sensor network topology

Sheer numbers of inaccessible and unattended sensor nodes, which are prone to frequent failures,

make topology maintenance a challenging task. Hundreds to several thousands of nodes are deployed throughout the sensor field. They are deployed within tens of feet of each other [39]. The node densities may be as high as 20 nodes/m<sup>3</sup> [77]. Deploying high number of nodes densely requires careful handling of topology maintenance. We examine issues related to topology maintenance and change in three phases:

### *3.5.1. Pre-deployment and deployment phase*

Sensor nodes can be either thrown in mass or placed one by one in the sensor field. They can be deployed by

- dropping from a plane,
- delivering in an artillery shell, rocket or missile,
- throwing by a catapult (from a ship board, etc.),
- placing in factory, and
- placing one by one either by a human or a robot.

Although the sheer number of sensors and their unattended deployment usually preclude placing them according to a carefully engineered deployment plan, the schemes for initial deployment must

- reduce the installation cost,
- eliminate the need for any pre-organization and pre-planning,
- increase the flexibility of arrangement, and
- promote self-organization and fault tolerance.

### *3.5.2. Post-deployment phase*

After deployment, topology changes are due to change in sensor nodes' [39,50]

- position,
- reachability (due to jamming, noise, moving obstacles, etc.),
- available energy,
- malfunctioning, and
- task details.

Sensor nodes may be statically deployed. However, device failure is a regular or common

event due to energy depletion or destruction. It is also possible to have sensor networks with highly mobile nodes. Besides, sensor nodes and the network experience varying task dynamics, and they may be a target for deliberate jamming. Therefore, sensor network topologies are prone to frequent changes after deployment.

### *3.5.3. Re-deployment of additional nodes phase*

Additional sensor nodes can be re-deployed at any time to replace the malfunctioning nodes or due to changes in task dynamics. Addition of new nodes poses a need to re-organize the network. Coping with frequent topology changes in an ad hoc network that has myriads of nodes and very stringent power consumption constraints requires special routing protocols. This issue is examined in detail in Section 4.

## *3.6. Environment*

Sensor nodes are densely deployed either very close or directly inside the phenomenon to be observed. Therefore, they usually work unattended in remote geographic areas. They may be working

- in busy intersections,
- in the interior of a large machinery,
- at the bottom of an ocean,
- inside a twister,
- on the surface of an ocean during a tornado,
- in a biologically or chemically contaminated field,
- in a battlefield beyond the enemy lines,
- in a home or a large building,
- in a large warehouse,
- attached to animals,
- attached to fast moving vehicles, and
- in a drain or river moving with current.

This list gives us an idea about under which conditions sensor nodes are expected to work. They work under high pressure in the bottom of an ocean, in harsh environments such as a debris or a battlefield, under extreme heat and cold such as in the nozzle of an aircraft engine or in arctic regions, and in an extremely noisy environment such as under intentional jamming.

### 3.7. Transmission media

In a multihop sensor network, communicating nodes are linked by a wireless medium. These links can be formed by radio, infrared or optical media. To enable global operation of these networks, the chosen transmission medium must be available worldwide.

One option for radio links is the use of industrial, scientific and medical (ISM) bands, which offer license-free communication in most countries. The International Table of Frequency Allocations, contained in Article S5 of the Radio Regulations (Volume 1), specifies some frequency bands that may be made available for ISM applications. They are listed in Table 1.

Some of these frequency bands are already being used for communication in cordless phone systems and wireless local area networks (WLANs). For sensor networks, a small-sized, low-cost, ultralow power transceiver is required. According to [68], certain hardware constraints and the trade-off between antenna efficiency and power consumption limit the choice of a carrier frequency for such transceivers to the ultrahigh frequency range. They also propose the use of the 433 MHz ISM band in Europe and the 915 MHz ISM band in North America. The transceiver design issues in these two bands are addressed in [25,51]. The main advantages of using the ISM bands are the free radio, huge spectrum allocation and global availability. They are not bound to a particular standard, thereby giving more freedom for the implementa-

tion of power saving strategies in sensor networks. On the other hand, there are various rules and constraints, like power limitations and harmful interference from existing applications. These frequency bands are also referred to as unregulated frequencies.

Much of the current hardware for sensor nodes is based upon RF circuit design. The μAMPS wireless sensor node, described in [77], uses a Bluetooth-compatible 2.4 GHz transceiver with an integrated frequency synthesizer. The low-power sensor device described in [93], uses a single channel RF transceiver operating at 916 MHz. The WINS architecture [69] also uses radio links for communication.

Another possible mode of internode communication in sensor networks is by infrared. Infrared communication is license-free and robust to interference from electrical devices. Infrared based transceivers are cheaper and easier to build. Many of today's laptops, PDAs and mobile phones offer an infrared data association interface. The main drawback though, is the requirement of a line of sight between sender and receiver. This makes infrared a reluctant choice for transmission medium in the sensor network scenario.

An interesting development is that of the smart dust mote [42], which is an autonomous sensing, computing and communication system that uses optical medium for transmission. Two transmission schemes, passive transmission using a corner-cube retroreflector (CCR), and active communication using a laser diode and steerable mirrors, are examined in [88]. In the former, the mote does not require an onboard light source. A configuration of three mirrors (CCR) is used to communicate a digital high or low. The latter uses an onboard laser diode and an active-steered laser communication system to send a tightly collimated light beam toward the intended receiver.

The unusual application requirements of sensor networks make the choice of transmission media more challenging. For instance, marine applications may require the use of the aqueous transmission medium. Here, one would like to use long-wavelength radiation that can penetrate the water surface. In hospitable terrain or battlefield applications might encounter error prone channels

Table 1  
Frequency bands available for ISM applications

Frequency band	Center frequency
6765–6795 kHz	6780 kHz
13,553–13,567 kHz	13,560 kHz
26,957–27,283 kHz	27,120 kHz
40.66–40.70 MHz	40.68 MHz
433.05–434.79 MHz	433.92 MHz
902–928 MHz	915 MHz
2400–2500 MHz	2450 MHz
5725–5875 MHz	5800 MHz
24–24.25 GHz	24.125 GHz
61–61.5 GHz	61.25 GHz
122–123 GHz	122.5 GHz
244–246 GHz	245 GHz

and greater interference. Moreover, a sensor antenna might not have the height and radiation power of those in other wireless devices. Hence, the choice of transmission medium must be supported by robust coding and modulation schemes that efficiently model these vastly different channel characteristics.

### 3.8. Power consumption

The wireless sensor node, being a micro-electronic device, can only be equipped with a limited power source (<0.5 Ah, 1.2 V). In some application scenarios, replenishment of power resources might be impossible. Sensor node lifetime, therefore, shows a strong dependence on battery lifetime. In a multihop ad hoc sensor network, each node plays the dual role of data originator and data router. The malfunctioning of few nodes can cause significant topological changes and might require re-routing of packets and re-organization of the network. Hence, power conservation and power management take on additional importance. It is for these reasons that researchers are currently focusing on the design of power-aware protocols and algorithms for sensor networks.

In other mobile and ad hoc networks, power consumption has been an important design factor, but not the primary consideration, simply because power resources can be replaced by the user. The emphasis is more on QoS provisioning than the power efficiency. In sensor networks though, power efficiency is an important performance metric, directly influencing the network lifetime. Application specific protocols can be designed by appropriately trading off other performance metrics such as delay and throughput with power efficiency.

The main task of a sensor node in a sensor field is to detect events, perform quick local data processing, and then transmit the data. Power consumption can hence be divided into three domains: *sensing*, *communication*, and *data processing*.

The sensing unit and its components were introduced in Section 3.4. Sensing power varies with the nature of applications. Sporadic sensing might consume lesser power than constant event monitoring. The complexity of event detection also plays a crucial role in determining energy expen-

diture. Higher ambient noise levels might cause significant corruption and increase detection complexity. Power consumption in data communication and processing are discussed in detail in the following subsections.

#### 3.8.1. Communication

Of the three domains, a sensor node expends maximum energy in data communication. This involves both data transmission and reception. It can be shown that for short-range communication with low radiation power ( $\sim 0$  dbm), transmission and reception energy costs are nearly the same. Mixers, frequency synthesizers, voltage control oscillators, phase locked loops (PLL) and power amplifiers, all consume valuable power in the transceiver circuitry. It is important that in this computation we not only consider the active power but also the start-up power consumption in the transceiver circuitry. The start-up time, being of the order of hundreds of micro-seconds, makes the start-up power non-negligible. This high value for the start-up time can be attributed to the lock time of the PLL. As the transmission packet size is reduced, the start-up power consumption starts to dominate the active power consumption. As a result, it is inefficient in turning the transceiver ON and OFF, because a large amount of power is spent in turning the transceiver back ON each time.

In [77], the authors present a formulation for the radio power consumption ( $P_c$ ) as

$$P_c = N_T [P_T(T_{on} + T_{st}) + P_{out}(T_{on})] + N_R [P_R(R_{on} + R_{st})] \quad (3)$$

where  $P_{T/R}$  is the power consumed by the transmitter/receiver;  $P_{out}$ , the output power of the transmitter;  $T/R_{on}$ , the transmitter/receiver on time;  $T/R_{st}$ , the transmitter/receiver start-up time and  $N_{T/R}$ , the number of times transmitter/receiver is switched on per unit time, which depends on the task and medium access control (MAC) scheme used.  $T_{on}$  can further be rewritten as  $L/R$ , where  $L$  is the packet size and  $R$ , the data rate. Today's state-of-the-art low power radio transceiver has typical  $P_T$  and  $P_R$  values around 20 dbm and  $P_{out}$  close to 0 dbm [59]. Note that PicoRadio aims at a  $P_c$  value of  $-20$  dbm.

The design of a small-sized, low-cost, ultralow power transceiver is discussed in [68]. A direct-conversion architecture is proposed for the transceiver circuitry. Based on their results, the authors present a power budget and estimate the power consumption to be at least an order of magnitude less than the values given above for  $P_T$  and  $P_R$  values.

### 3.8.2. Data processing

Energy expenditure in data processing is much less compared to data communication. The example described in [69], effectively illustrates this disparity. Assuming Rayleigh fading and fourth power distance loss, the energy cost of transmitting 1 KB a distance of 100 m is approximately the same as that for executing 3 million instructions by a 100 million instructions per second (MIPS)/W processor. Hence, local data processing is crucial in minimizing power consumption in a multihop sensor network.

A sensor node must therefore have built-in computational abilities and be capable of interacting with its surroundings. Further limitations of cost and size lead us to the choice of complementary metal oxide semiconductor (CMOS) technology for the micro-processor. Unfortunately, this has inbuilt limitations on energy efficiency. A CMOS transistor pair draws power everytime it is switched. This switching power is proportional to the switching frequency, device capacitance (which further depends on the area) and square of the voltage swing. Reducing the supply voltage is hence an effective means of lowering power consumption in the active state. Dynamic voltage scaling, explored in [52,64], aims to adapt processor power supply and operating frequency to match workloads. When a micro-processor handles time-varying computational load, simply reducing the operating frequency during periods of reduced activity results in a linear decrease in power consumption, but reducing the operating voltage gives us quadratic gains. On the other hand, this compromises on peak performance of the processor. Significant energy gains can be obtained by recognizing that peak performance is not always desired and therefore, the processor's operating voltage and frequency can be dynamically

adapted to instantaneous processing requirements. In [80], the authors propose a workload prediction scheme based on adaptive filtering of the past workload profile and analyze several filtering schemes. Other low power CPU organization strategies are discussed in [28,49,91].

The power consumption in data processing ( $P_p$ ) can be formulated as follows:

$$P_p = CV_{dd}^2 f + V_{dd} I_0 e^{V_{dd}/n'V_T} \quad (4)$$

where  $C$  is the total switching capacitance;  $V_{dd}$ , the voltage swing and  $f$ , the switching frequency. The second term indicates the power loss due to leakage currents [80]. The lowering of threshold voltage to satisfy performance requirements results in high subthreshold leakage currents. Coupled with the low duty cycle operation of the micro-processor in a sensor node, the associated power loss becomes significant [77].

It is to be noted that there may be some additional circuitry for data encoding and decoding. Application specific integrated circuits may also be used in some cases. In all these scenarios, the design of sensor network algorithms and protocols are influenced by the corresponding power expenditures, in addition to those that have been discussed.

## 4. Sensor networks communication architecture

The sensor nodes are usually scattered in a *sensor field* as shown in Fig. 2. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the *sink* and the end users. Data are routed back to the end user by a multihop infrastructureless architecture through the sink as shown in Fig. 2. The sink may communicate with the *task manager node* via Internet or Satellite.

The protocol stack used by the sink and all sensor nodes is given in Fig. 3. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes. The protocol stack consists of the *application layer*, *transport layer*, *network layer*, *data link layer*,



Fig. 2. Sensor nodes scattered in a sensor field.

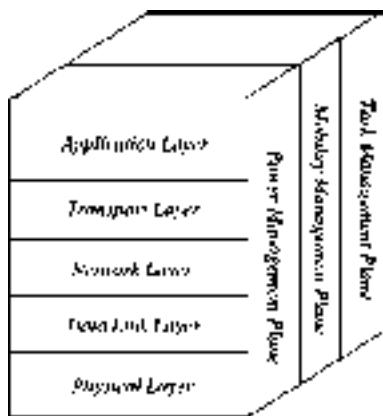


Fig. 3. The sensor networks protocol stack.

*physical layer, power management plane, mobility management plane, and task management plane.* Depending on the sensing tasks, different types of application software can be built and used on the application layer. The transport layer helps to maintain the flow of data if the sensor networks application requires it. The network layer takes care of routing the data supplied by the transport layer. Since the environment is noisy and sensor nodes can be mobile, the MAC protocol must be power aware and able to minimize collision with neighbors' broadcast. The physical layer addresses the needs of a simple but robust modulation, transmission and receiving techniques. In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes. These planes help the sensor nodes coordinate the sensing task and lower the overall power consumption.

The power management plane manages how a sensor node uses its power. For example, the sensor node may turn off its receiver after receiving a message from one of its neighbors. This is to avoid getting duplicated messages. Also, when the power level of the sensor node is low, the sensor node broadcasts to its neighbors that it is low in power and cannot participate in routing messages. The remaining power is reserved for sensing. The mobility management plane detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who are their neighbor sensor nodes. By knowing who are the neighbor sensor nodes, the sensor nodes can balance their power and task usage. The task management plane balances and schedules the sensing tasks given to a specific region. Not all sensor nodes in that region are required to perform the sensing task at the same time. As a result, some sensor nodes perform the task more than the others depending on their power level. These management planes are needed, so that sensor nodes can work together in a power efficient way, route data in a mobile sensor network, and share resources between sensor nodes. Without them, each sensor node will just work individually. From the whole sensor network standpoint, it is more efficient if sensor nodes can collaborate with each other, so the lifetime of the sensor networks can be prolonged. Before we discuss the need for the protocol layers and management planes in sensor networks, we map three existing work [42,69,77] to the protocol stack as shown in Fig. 3.

The so-called WINS is developed in [69], where a distributed network and Internet access is provided to the sensor nodes, controls, and processors. Since the sensor nodes are in large number, the WINS networks take advantage of this short distance between sensor nodes to provide multi hop communication and minimize power consumption. The way in which data is routed back to the user in the WINS networks follows the architecture specified in Fig. 2. The sensor node, i.e., a WINS node, detects the environmental data, and the data is routed hop by hop through the WINS nodes until it reaches the sink, i.e., a WINS gateway. So the WINS nodes are sensor nodes A, B, C,

D, and E according to the architecture in Fig. 2. The WINS gateway communicates with the user through conventional network services, such as the Internet. The protocol stack of a WINS network consists of the application layer, network layer, MAC layer, and physical layer. Also, it is explicitly pointed out in [69] that a low-power protocol suite that addresses the constraints of the sensor networks should be developed.

The smart dust motes [42], i.e., sensor nodes, may be attached to objects or even float in the air because of their small size and light weight. They use MEMS technology for optical communication and sensing. These motes may contain solar cells to collect energy during the day, and they require a line of sight to communicate optically with the base station transceiver or other motes. Comparing the smart dust communication architecture with the one in Fig. 2, the smart dust mote, i.e., the sensor node, typically communicates directly with the base station transceiver, i.e., sink. A peer-to-peer communication is also possible, but there are possible collision problems in medium access due to “hidden nodes”. The protocol layers in which the smart dust motes incorporate are application layer, MAC layer, and the physical layer.

Another approach to design protocols and algorithms for sensor networks is driven by the requirements of the physical layer [77]. The protocols and algorithms should be developed according to the choice of physical layer components, such as the type of micro-processors, and the type of receivers. This bottom-up approach of the  $\mu$ AMPS wireless sensor node also addresses the importance of the application layer, network layer, MAC layer, and physical layer as illustrated in Fig. 3 to be tightly integrated with the sensor node's hardware. The  $\mu$ AMPS wireless sensor node also communicates with the user according to the architecture specified in Fig. 2. Different schemes, such as time division multiple access (TDMA) versus frequency division multiple access (FDMA) and binary modulation versus  $M$ -ary modulation are compared in [77]. This bottom-up approach points out that sensor network algorithms have to be aware of the hardware and able to use special features of the micro-processors and transceivers to minimize the sensor node's power consumption. This may

push toward a custom solution for different types of sensor node design. Different types of sensor nodes deployed also lead to different types of sensor networks. This may also lead to different types of collaborative algorithms.

#### 4.1. Application layer

To the best of our knowledge, although many application areas for sensor networks are defined and proposed, potential application layer protocols for sensor networks remains a largely unexplored region. In this survey, we examine three possible application layer protocols, i.e., sensor management protocol (SMP), task assignment and data advertisement protocol (TADAP), and sensor query and data dissemination protocol (SQDDP), needed for sensor networks based on the proposed schemes related to the other layers and sensor network application areas. All of these application layer protocols are open research issues.

##### 4.1.1. Sensor management protocol

Designing an application layer management protocol has several advantages. Sensor networks have many different application areas, and accessing them through networks such as Internet is aimed in some current projects [69]. An application layer management protocol makes the hardware and softwares of the lower layers transparent to the sensor network management applications.

System administrators interact with sensor networks by using SMP. Unlike many other networks, sensor networks consist of nodes that do not have global IDs, and they are usually infrastructureless. Therefore, SMP needs to access the nodes by using attribute-based naming and location-based addressing, which are explained in detail in Section 4.3.

SMP is a management protocol that provides the software operations needed to perform the following administrative tasks:

- introducing the rules related to data aggregation, attribute-based naming and clustering to the sensor nodes,
- exchanging data related to the location finding algorithms,

- time synchronization of the sensor nodes,
- moving sensor nodes,
- turning sensor nodes on and off,
- querying the sensor network configuration and the status of nodes, and re-configuring the sensor network, and
- authentication, key distribution and security in data communications.

The descriptions of some of these tasks are given in [20,23,66,74,75].

#### 4.1.2. Task assignment and data advertisement protocol

Another important operation in the sensor networks is interest dissemination. Users send their interest to a sensor node, a subset of the nodes or whole network. This interest may be about a certain attribute of the phenomenon or a triggering event. Another approach is the advertisement of available data in which the sensor nodes advertise the available data to the users, and the users query the data which they are interested in. An application layer protocol that provides the user software with efficient interfaces for interest dissemination is useful for lower layer operations, such as routing as explained in Section 4.3.

#### 4.1.3. Sensor query and data dissemination protocol

SQDDP provides user applications with interfaces to issue queries, respond to queries and collect incoming replies. Note that these queries are generally not issued to particular nodes. Instead, attribute-based or location-based naming is preferred. For instance, “the locations of the nodes that sense temperature higher than 70 °F” is an attribute-based query. Similarly, “temperatures read by the nodes in region A” is an example for location-based naming.

Sensor query and tasking language (SQLT) [75] is proposed as an application that provides even a larger set of services. SQLT supports three types of events, which are defined by keywords *receive*, *every*, and *expire*. Receive keyword defines events generated by a sensor node when the sensor node receives a message; every keyword defines events occurred periodically due to a timer time-out; and expire keyword defines the events occurred when a

timer is expired. If a sensor node receives a message that is intended for it and contains a script, the sensor node then executes the script. Although SQLT is proposed, different types of SQDDP can be developed for various applications. The use of SQDDPs may be unique to each application.

#### 4.1.4. Open research issues

Although SQLT is proposed, there are still other application layer protocols need to be developed to provide a greater level of services. As mentioned before, the SMP allows software to perform administrative tasks such as moving sensor nodes and time synchronization of the nodes. Research developments should also focus on the TADAP and SQDDP as described in Sections 4.1.2 and 4.1.3.

### 4.2. Transport layer

The need for transport layer is pointed out in the literature [69,71]. This layer is especially needed when the system is planned to be accessed through Internet or other external networks. However, to the best of our knowledge there has not been any attempt thus far to propose a scheme or to discuss the issues related to the transport layer of a sensor network in literature. TCP with its current transmission window mechanisms does match to the extreme characteristics of the sensor network environment. An approach such as TCP splitting [4] may be needed to make sensor networks interact with other networks such as Internet. In this approach, TCP connections are ended at sink nodes, and a special transport layer protocol can handle the communications between the sink node and sensor nodes. As a result, the communication between the user and the sink node is by UDP or TCP via the Internet or Satellite; on the other hand, the communication between the sink and sensor nodes may be purely by UDP type protocols, because each sensor node has limited memory.

Unlike protocols such as TCP, the end-to-end communication schemes in sensor networks are not based on global addressing. These schemes must consider that attribute-based naming is used to indicate the destinations of the data packets.

The attributed-based naming is described in Section 4.3. The factors such as power consumption and scalability, and the characteristics like data-centric routing makes sensor networks need different handling in transport layer. Thus, these requirements stress the need for new types of transport layer protocols.

#### 4.2.1. Open research issues

The development of transport layer protocols is a challenging effort because the sensor nodes are influenced by the factors explained in Section 3, especially the hardware constraints such as the limited power and memory. As a result, each sensor node cannot store large amount of data like a server in the Internet, and acknowledgements are too costly for sensor networks. Therefore, new schemes that split the end-to-end communication probably at the sinks may be needed where UDP type protocols are used in the sensor network and traditional TCP/UDP protocols in the Internet or Satellite network.

#### 4.3. Network layer

Sensor nodes are scattered densely in a field either close to or inside the phenomenon as shown in Fig. 2. As discussed in Section 1, special multihop wireless routing protocols between the sensor nodes and the sink node are needed. The ad hoc routing techniques already proposed in the literature [65] do not usually fit the requirements of the sensor networks due to the reasons explained in Section 1. The networking layer of sensor networks is usually designed according to the following principles:

- Power efficiency is always an important consideration.
- Sensor networks are mostly data centric.
- Data aggregation is useful only when it does not hinder the collaborative effort of the sensor nodes.
- An ideal sensor network has attribute-based addressing and location awareness.

One of the following approaches can be used to select an energy efficient route. We use Fig. 4 to

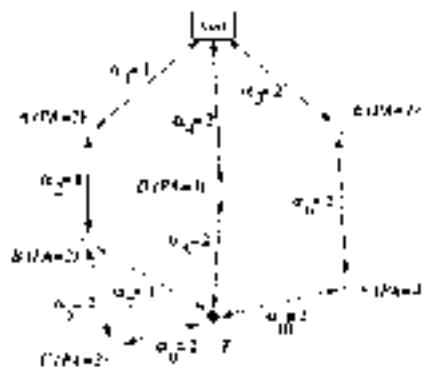


Fig. 4. The power efficiency of the routes.

describe each of these approaches, where node T is the source node that senses the phenomena. It has the following four possible routes to communicate with the sink:

- *Route 1*: Sink-A-B-T, total PA = 4, total  $\alpha = 3$ ,
- *Route 2*: Sink-A-B-C-T, total PA = 6, total  $\alpha = 6$ ,
- *Route 3*: Sink-D-T, total PA = 3, total  $\alpha = 4$ ,
- *Route 4*: Sink-E-F-T, total PA = 5, total  $\alpha = 6$ ,

where PA is the available power and  $\alpha_i$ , the energy required to transmit a data packet through the related link.

- *Maximum available power (PA) route*: The route that has maximum total available power is preferred. The total PA is calculated by summing the PAs of each node along the route. Based on this approach, Route 2 is selected in Fig. 4. However, Route 2 includes the nodes in Route 1 and an extra node. Therefore, although it has a higher total PA, it is not a power efficient one. As a result, it is important not to consider the routes derived by extending the routes that can connect the sensor to the sink as an alternative route. Eliminating Route 2, we select Route 4 as our power efficient route when we use maximum PA scheme.
- *Minimum energy (ME) route*: The route that consumes ME to transmit the data packets between the sink and the sensor node is the ME route. As shown in Fig. 4, Route 1 is the ME route.

- *Minimum hop (MH) route:* The route that makes the MH to reach the sink is preferred. Route 3 in Fig. 4 is the most efficient route based on this scheme. Note that the ME scheme selects the same route as the MH when the same amount of energy, i.e., all  $\alpha$  are the same, is used on every link. Therefore, when nodes broadcast with same power level without any power control, MH is then equivalent to ME.
- *Maximum minimum PA node route:* The route along which the minimum PA is larger than the minimum PAs of the other routes is preferred. In Fig. 4, Route 3 is the most efficient and Route 1 is the second efficient paths. This scheme precludes the risk of using up a sensor node with low PA much earlier than the others because they are on a route with nodes which has very high PAs.

Another important issue is that routing may be based on data centric. In data-centric routing, the interest dissemination is performed to assign the sensing tasks to the sensor nodes. There are two approaches used for interest dissemination: sinks broadcast the interest [39], and sensor nodes broadcast an advertisement for the available data [35] and wait for a request from the interested sinks.

The data-centric routing requires attribute-based naming [20,22,54,75]. For attribute-based naming, the users are more interested in querying an attribute of the phenomenon, rather than querying an individual node. For instance, “the areas where the temperature is over 70 °F” is a more common query than “the temperature read by a certain node”. The attribute-based naming is used to carry out queries by using the attributes of the phenomenon. The attribute-based naming also makes broadcasting, attribute-based multicasting, geo-casting and any-casting important for sensor networks.

The data aggregation is a technique used to solve the implosion and overlap problems in data-centric routing [35]. In this technique, a sensor network is usually perceived as a reverse multicast tree as shown in Fig. 5 where the sink asks the sensor nodes to report the ambient condition of the phenomena. Data coming from multiple sensor nodes are aggregated as if they are about the same

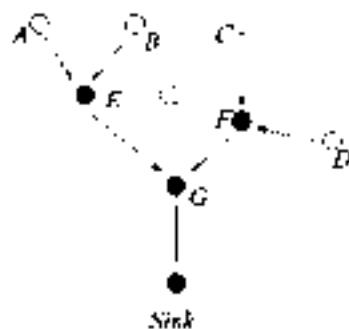


Fig. 5. Example of data aggregation.

attribute of the phenomenon when they reach the same routing node on the way back to the sink. For example, sensor node E aggregates the data from sensor nodes A and B while sensor node F aggregates the data from sensor nodes C and D as shown in Fig. 5. Data aggregation can be perceived as a set of automated methods of combining the data that comes from many sensor nodes into a set of meaningful information [34]. With this respect, data aggregation is known as data fusion [35]. Also, care must be taken when aggregating data, because the specifics of the data, e.g., the locations of reporting sensor nodes, should not be left out. Such specifics may be needed by certain applications.

One other important function of the network layer is to provide internetworking with external networks such as other sensor networks, command and control systems and the Internet. In one scenario, the sink nodes can be used as a gateway to other networks. While another scenario is creating a backbone by connecting sink nodes together and making this backbone access other networks via a gateway.

To provide insight into current research on the networking layer, we discuss different schemes proposed for the sensor networks for the rest of this section.

*Small minimum energy communication network (SMECN):* A protocol is developed in [73], which computes an energy efficient subnetwork, namely the MECN, when a communication network is given. A new algorithm called SMECN is proposed by [48] to also provide such a subnetwork.

The subnetwork, i.e., subgraph, constructed by SMECN is smaller than the one that is constructed by MECN if the broadcast region is circular around a broadcaster for a given power setting. The subgraph  $G$  of the graph  $G'$ , which represents the sensor network, minimizes the energy usage satisfying the following conditions: the number of edges in  $G$  is less than in  $G'$  while containing all nodes in  $G'$ ; if two nodes,  $u$  and  $v$ , are connected in graph  $G'$ , they are also connected in subgraph  $G$ ; the energy required to transmit data from node  $u$  to all its neighbors in subgraph  $G$  is less than the energy required to transmit to all its neighbors in graph  $G'$ . The SMECN also follows the ME property, which MECN uses to construct the subnetwork. The ME property is such that there exists a ME path in subgraph  $G$  between node  $u$  and  $v$  for every pair  $(u, v)$  of nodes that are connected in  $G'$ .

The power required to transmit data between node  $u$  and  $v$  is modelled as  $p(u, v) = td(u, v)^n$ , where  $t$  is a constant;  $d(u, v)$ , the distance between node  $u$  and  $v$ ; and  $n \geq 2$ , the path-loss exponent experienced by radio transmission. Also, the power needed to receive data is  $c$ . Since  $p(u, v)$  increases by  $n$ th power of the distance between node  $u$  and  $v$ , it may take less power to relay data than directly transmit data between node  $u$  and  $v$ . The path between node  $u$  (i.e.,  $u_0$ ) and  $v$  (i.e.,  $u_k$ ) is represented by  $r$ , where  $r = (u_0, u_1, \dots, u_k)$  in the subgraph  $G = (V, E)$  is an ordered list of nodes such that the pair  $(u_i, u_{i+1}) \in E$ . Also, the length of  $r$  is  $k$ . The total power consumption between node  $u_0$  and  $u_k$  is

$$C(r) = \sum_{i=0}^{k-1} (p(u_i, u_{i+1}) + c) \quad (5)$$

where  $p(u_i, u_{i+1})$  is the power required to transmit data between node  $u_i$ , and  $u_{i+1}$ ; and  $c$ , the power required to receive data. A path  $r$  is a ME path from  $u_0$  to  $u_k$  if  $C(r) \leq C(r')$  for all paths  $r'$  between node  $u_0$  and  $u_k$  in  $G'$ . As a result, a subgraph  $G$  has the ME property if for all  $(u, v) \in V$ , there exists a path  $r$  in  $G$ , which is a ME path in  $G'$  between node  $u$  and  $v$ .

*Flooding:* Flooding is an old technique that can also be used for routing in sensor networks. In

flooding, each node receiving a data or management packet repeats it by broadcasting, unless a maximum number of hops for the packet is reached or the destination of the packet is the node itself. Flooding is a reactive technique, and it does not require costly topology maintenance and complex route discovery algorithms. However, it has several deficiencies such as [35]:

- *Implosion:* Implosion is a situation where duplicated messages are sent to the same node. For example, if sensor node A has  $N$  neighbor sensor nodes that are also the neighbors of sensor node B, the sensor node B receives  $N$  copies of the message sent by sensor node A.
- *Overlap:* If two nodes share the same observing region, both of them may sense the same stimuli at the same time. As a result, neighbor nodes receive duplicated messages.
- *Resource blindness:* The flooding protocol does not take into account of the available energy resources. An energy resource aware protocol must take into account the amount of energy available to them at all time.

*Gossiping:* A derivation of flooding is gossiping [32] in which nodes do not broadcast but send the incoming packets to a randomly selected neighbor. A sensor node randomly selects one of its neighbors to send the data. Once the neighbor node receives the data, it selects randomly another sensor node. Although this approach avoid the implosion problem by just having one copy of a message at any node, it takes long time to propagate the message to all sensor nodes.

*Sensor protocols for information via negotiation (SPIN):* A family of adaptive protocols called SPIN [35] is designed to address the deficiencies of classic flooding by negotiation and resource adaptation. The SPIN family of protocols are designed based on two basic ideas: sensor nodes operate more efficiently and conserve energy by sending data that describe the sensor data instead of sending the whole data, e.g., image, and sensor nodes must monitor the changes in their energy resources.

SPIN has three types of messages, i.e., ADV, REQ, and DATA. Before sending a DATA

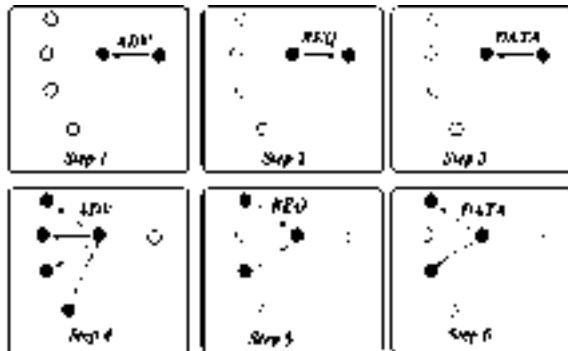


Fig. 6. The SPIN protocol [35].

message, the sensor broadcasts an ADV message containing a descriptor, i.e., meta-data, of the DATA as shown in Step 1 of Fig. 6. If a neighbor is interested in the data, it sends a REQ message for the DATA and DATA is sent to this neighbor sensor node as shown in Steps 2 and 3 of Fig. 6, respectively. The neighbor sensor node then repeats this process as illustrated in Steps 4, 5, and 6 of Fig. 6. As a result, the sensor nodes in the entire sensor network, which are interested in the data, will get a copy.

Note that SPIN is based on data-centric routing [35] where the sensor nodes broadcast an advertisement for the available data and wait for a request from interested sinks.

*Sequential assignment routing (SAR):* In [83], a set of algorithms, which perform organization, management and mobility management operations in sensor networks, are proposed. Self-organizing MAC for sensor networks (SMACS) is a distributed protocol that enables a collection of sensor nodes to discover their neighbors and establish transmission/reception schedules without the need for a central management system. The eavesdrop and register (EAR) algorithm is designed to support seamless interconnection of the mobile nodes. The EAR algorithm is based on the invitation messages and on the registration of stationary nodes by the mobile nodes. The SAR algorithm creates multiple trees where the root of each tree is an one hop neighbor from the sink. Each tree grows outward from the sink while avoiding nodes with very low QoS (i.e., low throughput/high de-

lay) and energy reserves. At the end of this procedure, most nodes belong to multiple trees. This allows a sensor node to choose a tree to relay its information back to the sink. There are two parameters associated with each path, i.e., a tree, back to the sink:

- *Energy resources:* The energy resources is estimated by the number of packets, which the sensor node can send, if the sensor node has exclusive use of the path.
- *Additive QoS metric:* A high additive QoS metric means low QoS.

The SAR algorithm selects the path based on the energy resources and additive QoS metric of each path, and the packet's priority level. As a result, each sensor node selects its path to route the data back to the sink.

Also, two more algorithms called single winner election and multiwinner election handle the necessary signaling and data transfer tasks in local cooperative information processing.

*Low-energy adaptive clustering hierarchy (LEACH):* LEACH is a clustering-based protocol that minimizes energy dissipation in sensor networks [34]. The purpose of LEACH is to randomly select sensor nodes as cluster-heads, so the high-energy dissipation in communicating with the base station is spread to all sensor nodes in the sensor network. The operation of LEACH is separated into two phases, the set-up phase and the steady phase. The duration of the steady phase is longer than the duration of the set-up phase in order to minimize the overhead.

During the set-up phase, a sensor node chooses a random number between 0 and 1. If this random number is less than the threshold  $T(n)$ , the sensor node is a cluster-head.  $T(n)$  is calculated as

$$T(n) = \begin{cases} \frac{P}{1 - P[r \bmod(1/P)]} & \text{if } n \in G, \\ 0 & \text{otherwise,} \end{cases}$$

where  $P$  is the desired percentage to become a cluster-head;  $r$ , the current round; and  $G$ , the set of nodes that have not being selected as a cluster-head in the last  $1/P$  rounds. After the cluster-heads are selected, the cluster-heads advertise to all

sensor nodes in the network that they are the new cluster-heads. Once the sensor nodes receive the advertisement, they determine the cluster that they want to belong based on the signal strength of the advertisement from the cluster-heads to the sensor nodes. The sensor nodes inform the appropriate cluster-heads that they will be a member of the cluster. Afterwards, the cluster-heads assign the time on which the sensor nodes can send data to the cluster-heads based on a TDMA approach.

During the steady phase, the sensor nodes can begin sensing and transmitting data to the cluster-heads. The cluster-heads also aggregate data from the nodes in their cluster before sending these data to the base station. After a certain period of time spent on the steady phase, the network goes into the set-up phase again and entering into another round of selecting the cluster-heads.

**Directed diffusion:** The directed diffusion data dissemination paradigm is proposed in [39] where the sink sends out interest, which is a task description, to all sensors as shown in Fig. 7(a). The task descriptors are named by assigning attribute-value pairs that describe the task. Each sensor node then stores the interest entry in its cache. The interest entry contains a timestamp field and several gradient fields. As the interest is propagated throughout the sensor network, the gradients from the source back to the sink are set up as shown in Fig. 7(b). When the source has data for the interest, the source sends the data along the interest's

gradient path as shown in Fig. 7(c). The interest and data propagation and aggregation are determined locally. Also, the sink must refresh and reinforce the interest when it starts to receive data from the source. Note that the directed diffusion is based on data-centric routing where the sink broadcasts the interest.

#### 4.3.1. Open research issues

An overview of the protocols proposed for sensor networks is given in Table 2. These protocols need to be improved or new protocols need to be developed to address higher topology changes and higher scalability. Also, new internetworking schemes should be developed to allow easy communication between the sensor networks and external networks, e.g., Internet.

#### 4.4. Data link layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network. In the following two subsections, we discuss some of the medium access and error control strategies for sensor networks.

##### 4.4.1. Medium access control

The MAC protocol in a wireless multihop self-organizing sensor network must achieve two goals. The first is the creation of the network infrastructure. Since thousands of sensor nodes are densely scattered in a sensor field, the MAC scheme must establish communication links for data transfer. This forms the basic infrastructure needed for wireless communication hop by hop and gives the sensor network self-organizing ability. The second objective is to fairly and efficiently share communication resources between sensor nodes. Traditional MAC schemes can all be categorized based on their resource sharing mechanisms. Table 3 provides an insight into the advantages and disadvantages, and application domains of these classes.

**Reasons why existing MAC protocols cannot be used:** It has been emphasized in earlier sections

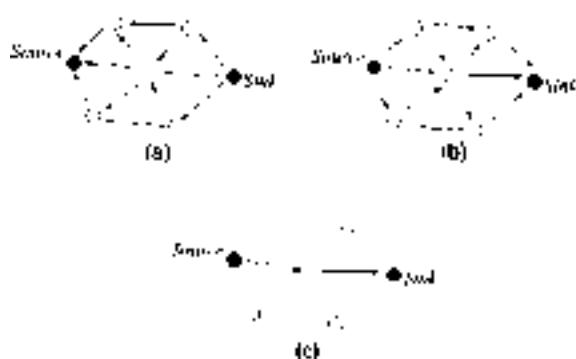


Fig. 7. An example of directed diffusion [39]: (a) propagate interest, (b) set up gradient and (c) send data.

**Table 2**  
An overview of network layer schemes

Network layer scheme	Description
SMECN [48]	Creates a subgraph of the sensor network that contains the ME path
Flooding	Broadcasts data to all neighbor nodes regardless if they receive it before or not
Gossiping [32]	Sends data to one randomly selected neighbor
SPIN [35]	Sends data to sensor nodes only if they are interested; has three types of messages, i.e., ADV, REQ, and DATA
SAR [83]	Creates multiple trees where the root of each tree is one hop neighbor from the sink; select a tree for data to be routed back to the sink according to the energy resources and additive QoS metric
LEACH [34]	Forms clusters to minimize energy dissipation
Directed diffusion [39]	Sets up gradients for data to flow from source to sink during interest dissemination

**Table 3**  
Categorization of MAC protocols

Category	Resource sharing mode	Application domain	Disadvantages
Dedicated assignment or fixed allocation	Pre-determined fixed allocation	Appropriate for continuous traffic and provides bounded delay	Inefficient for bursty traffic
Demand based	According to demand or user request	Useful for variable rate and multimedia traffic	Additional overhead and delay due to reservation process
Random access or contention based	Channel contention when transmission packets are available	Suitable for bursty traffic	Inefficient for delay-sensitive traffic

that novel protocols and algorithms are needed to effectively tackle the unique resource constraints and application requirements of sensor networks. To illustrate the impact of these constraints, let us take a closer look at MAC schemes in other wireless networks and analyze why they cannot be adopted into the sensor network scenario.

In a cellular system, the base stations form a wired backbone. A mobile node is only a single hop away from the nearest base station. This type of network is also referred to as infrastructure based in literature. The primary goal of the MAC protocol in such systems is the provision of high QoS and bandwidth efficiency. Power conservation assumes only secondary importance as base stations have unlimited power supply and the mobile user can replenish exhausted batteries in the handset. Hence, medium access is invariably inclined toward a dedicated resource assignment strategy. Such an access scheme is impractical for sensor networks as there is no central controlling agent like the base station. This makes network-wide synchronization a difficult proposition. Moreover, power efficiency

directly influences network lifetime in a sensor network and hence is of prime importance.

Bluetooth and the mobile ad hoc network (MANET) are probably the closest peers to the sensor networks. Bluetooth is an infrastructure-less short-range wireless system intended to replace the cable between electronic user terminals with RF links. The Bluetooth topology is a star network where a master node can have up to seven slave nodes wirelessly connected to it to form a piconet. Each piconet uses a centrally assigned TDMA schedule and frequency hopping pattern. Transmission power is typically around 20 dBm and the transmission range is of the order of tens of meters. The MAC protocol in a MANET has the task of forming the network infrastructure and maintaining it in the face of mobility. Hence, the primary goal is the provision of high QoS under mobile conditions. Although the nodes are portable battery-powered devices, they can be replaced by the user and hence, power consumption is only of secondary importance.

In contrast to these two systems, the sensor network may have a much larger number of nodes. The transmission power ( $\sim 0$  dBm) and radio range of a sensor node is much less than those of the Bluetooth or the MANET. Topology changes are more frequent in a sensor network and can be attributed both to node mobility and failure. The mobility rate can also be expected to be much lower than in the MANET. In essence, the primary importance of power conservation to prolong network lifetime in a sensor network means that none of the existing Bluetooth or MANET MAC protocols can be directly used.

*MAC for sensor networks:* It is evident from our previous discussions that the MAC protocol for sensor networks must have built-in power conservation, mobility management and failure recovery strategies. Though many schemes for medium access have been proposed for MANETs [85,94,95] the design of an efficient MAC scheme for the new regime of sensor networks is still an open research issue. Thus far, both *fixed allocation* and *random access* versions of medium access have been proposed [83,93]. *Demand-based* MAC schemes may be unsuitable for sensor networks due their large messaging overhead and link set-up delay. Power conservation is achieved by the use of power saving operation modes and by preferring time-outs to acknowledgements, wherever possible.

It has been reasoned in [69] that since radios must be turned off during idling for precious power savings, the MAC scheme should include a variant of TDMA. Such a medium access mechanism is presented in [83]. Further, contention-based channel access is deemed unsuitable due to their requirement to monitor the channel at all times. It must be noted however, that random medium access can also support power conservation, as in the IEEE 802.11 standard for WLANs, by turning off radios depending on the status of the net allocation vector. Constant listening times and adaptive rate control schemes can also help achieve energy efficiency in random access schemes for sensor networks [93]. Some of the proposed MAC protocols are discussed next.

*SMACS and the EAR algorithm:* The SMACS protocol [83] achieves network start-up and link-layer organization, and the EAR algorithm en-

ables seamless connection of mobile nodes in a sensor network. SMACS is a distributed infrastructure-building protocol which enables nodes to discover their neighbors and establish transmission/reception schedules for communication without the need for any local or global master nodes. In this protocol, the neighbor discovery and channel assignment phases are combined so that by the time nodes hear all their neighbors, they would have formed a connected network. A communication link consists of a pair of time slots operating at a randomly chosen, but fixed frequency (or frequency hopping sequence). This is a feasible option in sensor networks, since, as mentioned earlier in Section 3.7, the available bandwidth can be expected to be much higher than the maximum data rate for sensor nodes. Such a scheme avoids the necessity for network-wide synchronization, although communicating neighbors in a subnet need to be time synchronized. *Power conservation* is achieved by using a random wake-up schedule during the connection phase and by turning the radio off during idle time slots.

The EAR protocol [83] attempts to offer continuous service to the mobile nodes under both mobile and stationary conditions. Here, the mobile nodes assume full control of the connection process and also decide when to drop connections, thereby minimizing messaging overhead. The EAR is transparent to the SMACS, so that the SMACS is functional until the introduction of mobile nodes into the network. In this model, the network is assumed to be mainly static, i.e., any mobile node has a number of stationary nodes in its vicinity. A drawback of such a time-slot assignment scheme is the possibility that members already belonging to different subnets might never get connected.

*CSMA based medium access:* A CSMA based MAC scheme for sensor networks is presented in [93]. Traditional CSMA based schemes are deemed inappropriate as they all make the fundamental assumption of stochastically distributed traffic and tend to support independent point-to-point flows. On the contrary, the MAC protocol for sensor networks must be able to support variable, but highly correlated and dominantly periodic traffic. Any CSMA based medium access scheme has two important components, the *listening mechanism*

and the *backoff scheme*. As reported and based on simulations in [93], the constant listen periods are energy efficient and the introduction of random delay provides robustness against repeated collisions. Fixed window and binary exponential decrease backoff schemes are recommended to maintain proportional fairness in the network. A phase change at the application level is also advocated to get over any capturing effects. It is proposed in this work that the energy consumed per unit of successful communication can serve as a good indicator of *energy efficiency*.

An adaptive transmission rate control (ARC) scheme, that achieves medium access fairness by balancing the rates of originating and route-thru traffic is also discussed here. This ensures that nodes closer to the access point are not favored over those deep down into the network. The ARC controls the data origination rate of a node in order to allow the route-thru traffic to propagate. A progressive signalling mechanism is used to inform the nodes to lower their data originating rate. The ARC uses a linear increase and multiplicative decrease approach [57]. While the linear increase leads to more aggressive channel competition, the multiplicative decrease controls transmission failure penalty. Since dropping route-thru traffic is costlier, the associated penalty is lesser than that for originating data transmission failure. This ensures that route-thru traffic is preferred over the originating traffic.

The computational nature of this scheme makes it more energy efficient than handshaking and messaging schemes using the radio. The ARC also attempts to reduce the problem of hidden nodes in a multihop network by constantly tuning the

transmission rate and performing phase changes, so that periodic streams are less likely to repeatedly collide.

*Hybrid TDMA/FDMA based:* This centrally controlled MAC scheme is introduced in [77]. In this work, the effect of non-ideal physical layer electronics on the design of MAC protocols for sensor networks is investigated. The system is assumed to be made up of energy constrained sensor nodes that communicate to a single, nearby, high-powered base station (<10 m). Specifically, the machine monitoring application of sensor networks, with strict data latency requirements, is considered and a hybrid TDMA–FDMA medium access scheme is proposed. While a pure TDMA scheme dedicates the full bandwidth to a single sensor node, a pure FDMA scheme allocates minimum signal bandwidth per node. Despite the fact that a pure TDMA scheme minimizes the transmit on-time, it is not always preferred due to the associated time synchronization costs. An analytical formula is derived in [77] to find the optimum number of channels which gives the lowest system *power consumption*. This determines the hybrid TDMA–FDMA scheme to be used. The optimum number of channels is found to depend on the ratio of the power consumption of the transmitter to that of the receiver. If the transmitter consumes more power, a TDMA scheme is favored, while the scheme leans toward FDMA when the receiver consumes greater power.

To get a deeper insight into the salient features and effectiveness of MAC protocols for sensor networks, we present a qualitative overview in Table 4. It also serves as an indicator for comparative evaluation of some of the MAC schemes

Table 4  
Qualitative overview of MAC protocols for sensor networks

MAC protocol	Channel access mode	Sensor network specifics	Power conservation
SMACS and EAR [83]	Fixed allocation of duplex time slots at fixed frequency	Exploitation of large available bandwidth compared to sensor data rate	Random wake up during set-up and turning radio off while idle
Hybrid TDMA/FDMA [77]	Centralized frequency and time division	Optimum number of channels calculated for minimum system energy	Hardware based approach for system energy minimization
CSMA based [93]	Contention-based random access	Application phase shift and pre-transmit delay	Constant listening time for energy efficiency

proposed thus far in literature. The column titled *sensor network specifics* aims to illustrate the novel and important features in each of these schemes that enable their application in the sensor network domain. They present the deviations and differences from traditional MAC schemes, which by themselves would not be applicable. We also outline how each of these schemes achieves power efficiency.

#### 4.4.2. Power saving modes of operation

Regardless of which type of medium access scheme is used for sensor networks, it certainly must support the operation of power saving modes for the sensor node. The most obvious means of power conservation is to turn the transceiver off when it is not required. Though this power saving method seemingly provides significant energy gains, an important point that must not be overlooked is that sensor nodes communicate using short data packets. As explained in Section 3.8.1, the shorter the packets, the more the dominance of start-up energy. In fact, if we blindly turn the radio off during each idling slot, over a period of time, we might end up expending more energy than if the radio had been left on. As a result, operation in a power saving mode is energy efficient only if the time spent in that mode is greater than a certain threshold. There can be a number of such useful modes of operation for the wireless sensor node, depending on the number of states of the micro-processor, memory, A/D convertor and the transceiver. Each of these modes can be characterized by its power consumption and the latency overhead, which is the transition power to and from that mode. A dynamic power management scheme for wireless sensor networks is discussed in [80] where five power saving modes are proposed and intermode transition policies are investigated. The threshold time is found to depend on the transition times and the individual power consumption of the modes in question.

#### 4.4.3. Error control

Another important function of the data link layer is the error control of transmission data. Two important modes of error control in communica-

tion networks are the forward error correction (FEC) and automatic repeat request (ARQ). To the best of our knowledge, the application of ARQ schemes is thus far unexplored in the regime of sensor networks, though many adaptive and low-power versions are existent in literature for other mobile networks [44,97]. The usefulness of ARQ in sensor network applications is limited by the additional re-transmission cost and overhead. On the other hand, decoding complexity is greater in FEC, as error correction capabilities need to be built-in. Considering this, simple error control codes with low-complexity encoding and decoding might present the best solutions for sensor networks. In the design of such a scheme it is important to have good knowledge of the channel characteristics and implementation techniques. In the following subsection, we briefly review the motivation and basic design considerations for FEC, which in turn will help us understand the requirements for sensor networks.

**FEC:** Link reliability is an important parameter in the design of any wireless network, and more so in sensor networks, due to the unpredictable and harsh nature of channels encountered in various application scenarios. Some of the applications like mobile tracking and machine monitoring require high data precision. Channel bit error rate (BER) is a good indicator of link reliability. The BER can be shown to be directly proportional to the symbol rate  $R_s$  and inversely proportional to both the received SNR ( $E_s/N_0$ ) and the transmitter power level  $P_{out}$ . Let us assume that a coding scheme with rate  $R$  is used. If the data symbol transmission rate remains the same as that before coding, the total symbol transmission rate must increase to  $R_s/R$ . Also, if the transmission power is unchanged, the received energy per symbol decreases to  $RE_s$ . The BER measured at the decoder input, the raw BER, is hence greater than the BER without coding. This loss is overcome in the decoder by exploiting the redundancy and structure of the code to correct some of the transmission errors. In fact, a good choice of the error correcting code can result in several orders of magnitude reduction in BER and an overall gain. The *coding gain* is generally expressed in terms of the additional transmit power needed to obtain the

same BER without coding. A simple (15,11) Hamming code is found to reduce BER by almost  $10^3$  and ensures a coding gain of 1.5 dB for binary phase shift keying modulated data and additive white Gaussian noise model [92].

Reliable data communication can hence be provided either by increasing the output transmit power ( $P_{\text{out}}$ ) or the use of suitable FEC. Since a sensor node has limited power resources, the former option is not feasible. We hence turn to FEC. As we have seen, FEC can achieve significant reduction in the BER for any given value of  $P_{\text{out}}$ . However, we must take into account the *additional processing power that goes into encoding and decoding*. This processing power is drawn from the limited resources possessed by the node. This might be critical for sensor networks though it can be negligibly small in other wireless networks. If the associated processing power is greater than the coding gain, then the whole process in energy inefficiency and the system is better off without coding. On the other hand, FEC is a valuable asset in sensor networks, if the sum of the encoding and decoding processing powers is less than the transmission power savings. It is to be noted that all these computations and comparisons must be carried out for a given, in most cases application specific, BER.

Though adaptive FEC has received some attention in other wireless networks, it remains largely unexplored in sensor networks. The impact of adapting packet size and error control on energy efficiency in wireless systems is investigated in [47,58]. In [76], the authors examine this issue for sensor networks. They assume a frequency non-selective, slow Rayleigh fading channel and use convolutional codes for FEC. Based on their analysis, they conclude that the average energy consumption per useful bit shows an exponential increase with the constraint length of the code and is independent of the code rate. Moreover, they find that FEC is generally inefficient if the decoding is performed using a micro-processor and recommend an on-board dedicated Viterbi decoder. To the best of our knowledge, other coding schemes remain unexplored. Simple encoding techniques that enable easy decoding might present an energy efficient solution for sensor networks.

#### 4.4.4. Open research issues

Though some medium access schemes have been proposed for sensor networks, the area is still largely open to research. So is the mainly unexplored domain of error control in sensor networks. Key open research issues include:

- *MAC for mobile sensor networks*: The proposed SMACS and EAR [83] perform well only in a mainly static sensor networks. It is assumed in the connection schemes that a mobile node has many static nodes as neighbors. These algorithms must be improved to deal with more extensive mobility in the sensor nodes and targets. Mobility issues, carrier sensing, and backoff mechanisms for the CSMA based scheme also remain largely unexplored.
- *Determination of lower bounds on the energy required for sensor network self-organization*.
- *Error control coding schemes*: Error control is extremely important in some sensor network applications like mobile tracking and machine monitoring. Convolutional coding effects have been considered in [77]. The feasibility of other error control schemes in sensor networks needs to be explored.
- *Power saving modes of operation*: To prolong network lifetime, a sensor node must enter into periods of reduced activity when running low on battery power. The enumeration and transition management for these nodes is open to research. Some ideas are outlined in [80].

#### 4.5. Physical layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption. Frequency selection aspects have been dealt with in Section 3.7. Frequency generation and signal detection have more to do with the underlying hardware and transceiver design and hence are beyond the scope of our paper. In the following, we focus on signal propagation effects, power efficiency and modulation schemes for sensor networks.

It is well known that long-distance wireless communication can be expensive, both in terms

of energy and implementation complexity. While designing the physical layer for sensor networks, energy minimization assumes significant importance, over and above the decay, scattering, shadowing, reflection, diffraction, multipath and fading effects. In general, the minimum output power required to transmit a signal over a distance  $d$  is proportional to  $d^n$ , where  $2 \leq n < 4$ . The exponent  $n$  is closer to four for low-lying antennae and near-ground channels [72,82], as is typical in sensor network communication. This can be attributed to the partial signal cancellation by a ground-reflected ray. While trying to resolve these problems, it is important that the designer is aware of inbuilt diversities and exploits this to the fullest. For instance, multihop communication in a sensor network can effectively overcome shadowing and path-loss effects, if the node density is high enough. Similarly, while propagation losses and channel capacity limit data reliability, this very fact can be used for spatial frequency re-use. Energy efficient physical layer solutions are currently being pursued by researchers. Although some of these topics have been addressed in literature, it still remains a vastly unexplored domain of the wireless sensor networks. A discussion of some existing ideas follows.

The choice of a good modulation scheme is critical for reliable communication in a sensor network. Binary and  $M$ -ary modulation schemes are compared in [77]. While an  $M$ -ary scheme can reduce the transmit on-time by sending multiple bits per symbol, it results in complex circuitry and increased radio power consumption. These trade-off parameters are formulated in [76] and it is concluded that under start-up power dominant conditions, the binary modulation scheme is more energy efficient. Hence,  $M$ -ary modulation gains are significant only for low start-up power systems. A low-power direct-sequence spread-spectrum modem architecture for sensor networks is presented in [13]. This low-power architecture can be mapped to an ASIC technology to further improve efficiency.

Ultrawideband (UWB) or impulse radio (IR) has been used for baseband pulse radar and ranging systems and has recently drawn considerable interest for communication applications [18],

especially in indoor wireless networks [53]. UWB employs baseband transmission and thus, it requires no intermediate or radio carrier frequencies. Generally, pulse position modulation is used. The main advantage of UWB is its resilience to multipath [17,45,46]. Low transmission power and simple transceiver circuitry, make UWB an attractive candidate for sensor networks.

#### 4.5.1. Open research issues

The physical layer is a largely unexplored area in sensor networks. Open research issues range from power efficient transceiver design to modulation schemes. A few of these are given below

- *Modulation schemes:* Simple and low-power modulation schemes need to be developed for sensor networks. The modulation scheme can be either baseband, as in UWB, or passband.
- *Strategies to overcome signal propagation effects:* Signal propagation effects in sensor networks have been dealt with in Section 4.5.
- *Hardware design:* Tiny, low-power, low-cost transceiver, sensing and processing units need to be designed. Power efficient hardware management strategies are also essential.

## 5. Conclusion

The flexibility, fault tolerance, high sensing fidelity, low-cost and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required. Many researchers are currently engaged in developing the technologies needed for different layers of the sensor networks protocol stack as shown in Fig. 3. A list of current sensor networks

Table 5  
Current research projects

Project name	Research area	HTTP location
SensoNet [3]	Transport, network, data link and physical layers	<a href="http://www.ece.gatech.edu/research/labs/bwn/">http://www.ece.gatech.edu/research/labs/bwn/</a>
WINS [22,69]	Power control, mobility and task management planes	<a href="http://www.janet.ucla.edu/WINS/">http://www.janet.ucla.edu/WINS/</a>
SPIN [35]	Distributed network and Internet access to sensors, controls, and processors	
SPINS [66]	Data dissemination protocols	<a href="http://nms.lcs.mit.edu/projects/leach">http://nms.lcs.mit.edu/projects/leach</a>
SINA [75,84]	Security protocol	<a href="http://paris.cs.berkeley.edu/~perrig/projects.html">http://paris.cs.berkeley.edu/~perrig/projects.html</a>
$\mu$ AMPS [77]	Information networking architecture	<a href="http://www.eecis.udel.edu/~cshen/">http://www.eecis.udel.edu/~cshen/</a>
LEACH [34]	Framework for implementing adaptive energy-aware distributed microsensors	<a href="http://www-mtl.mit.edu/research/icsystems/uamps/">http://www-mtl.mit.edu/research/icsystems/uamps/</a>
Smart dust [42]	Cluster formation protocol	<a href="http://nms.lcs.mit.edu/projects/leach">http://nms.lcs.mit.edu/projects/leach</a>
	Laser communication from a cubic millimeter	<a href="http://robotics.eecs.berkeley.edu/~pister/SmartDust/">http://robotics.eecs.berkeley.edu/~pister/SmartDust/</a>
	Mote delivery	
	SubmicroWatt electronics	
	Power sources	
	MacroMotes (COTS Dust)	
SCADDS [8,11,20,22,23,27,33,39,96]	Scalable coordination architectures for deeply distributed and dynamic systems	<a href="http://www.isi.edu/scadds/">http://www.isi.edu/scadds/</a>
PicoRadio [70,71]	Develop a “system-on-chip” implementation of a PicoNode	<a href="http://bwrc.eecs.berkeley.edu/Research/Pico_Radio/PicoNode.htm">http://bwrc.eecs.berkeley.edu/Research/Pico_Radio/PicoNode.htm</a>
PACMAN [79]	Mathematical framework that incorporates key features of computing nodes and networking elements	<a href="http://pacman.usc.edu">http://pacman.usc.edu</a>
Dynamic sensor networks [19]	Routing and power aware sensor management Network services API	<a href="http://www.east.isi.edu/DIV10/dsn/">http://www.east.isi.edu/DIV10/dsn/</a>
Aware home [36]	Requisite technologies to create a home environment that can both perceive and assist its occupants	<a href="http://www.cc.gatech.edu/fce/ahri">http://www.cc.gatech.edu/fce/ahri</a>
COUGAR device database project [7]	Distributed query processing	<a href="http://www.cs.cornell.edu/database/cougar/index.htm">http://www.cs.cornell.edu/database/cougar/index.htm</a>
DataSpace [38]	Distributed query processing	<a href="http://www.cs.rutgers.edu/dataman">http://www.cs.rutgers.edu/dataman</a>

research projects is given in Table 5. Along with the current research projects, we encourage more insight into the problems and more development in solutions to the open research issues as described in this paper.

## References

- [1] G.D. Abowd, J.P.G. Sterbenz, Final report on the inter-agency workshop on research issues for smart environments, IEEE Personal Communications (October 2000) 36–40.
- [2] J. Agre, L. Clare, An integrated architecture for cooperative sensing networks, IEEE Computer Magazine (May 2000) 106–108.
- [3] I.F. Akyildiz, W. Su, A power aware enhanced routing (PAER) protocol for sensor networks, Georgia Tech Technical Report, January 2002, submitted for publication.
- [4] A. Bakre, B.R. Badrinath, I-TCP: indirect TCP for mobile hosts, Proceedings of the 15th International Conference on Distributed Computing Systems, Vancouver, BC, May 1995, pp. 136–143.
- [5] P. Bauer, M. Sichitiu, R. Istepanian, K. Premaratne, The mobile patient: wireless distributed sensor networks for patient monitoring and care, Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine, 2000, pp. 17–21.
- [6] M. Bhardwaj, T. Garnett, A.P. Chandrakasan, Upper bounds on the lifetime of sensor networks, IEEE International Conference on Communications ICC'01, Helsinki, Finland, June 2001.
- [7] P. Bonnet, J. Gehrke, P. Seshadri, Querying the physical world, IEEE Personal Communications (October 2000) 10–15.
- [8] N. Bulusu, D. Estrin, L. Girod, J. Heidemann, Scalable coordination for wireless sensor networks: self-configuring localization systems, International Symposium on Communication Theory and Applications (ISCTA 2001), Ambleside, UK, July 2001.
- [9] B.G. Celler et al., An instrumentation system for the remote monitoring of changes in functional health status of the elderly, International Conference IEEE-EMBS, New York, 1994, pp. 908–909.

- [10] A. Cerpa, D. Estrin, ASCENT: adaptive self-configuring sensor networks topologies, UCLA Computer Science Department Technical Report UCLA/CSDTR-01-0009, May 2001.
- [11] A. Cerpa, J. Elson, M. Hamilton, J. Zhao, Habitat monitoring: application driver for wireless communications technology, ACM SIGCOMM'2000, Costa Rica, April 2001.
- [12] A. Chandrakasan, R. Amirtharajah, S. Cho, J. Goodman, G. Konduri, J. Kulik, W. Rabiner, A. Wang, Design considerations for distributed micro-sensor systems, Proceedings of the IEEE 1999 Custom Integrated Circuits Conference, San Diego, CA, May 1999, pp. 279–286.
- [13] C. Chien, I. Elgorriaga, C. McConaghay, Low-power direct-sequence spread-spectrum modem architecture for distributed wireless sensor networks, ISLPED'01, Huntington Beach, California, August 2001.
- [14] S. Cho, A. Chandrakasan, Energy-efficient protocols for low duty cycle wireless microsensor, Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI Vol. 2 (2000), p. 10.
- [15] R. Colwell, Testimony of Dr. Rita Colwell, Director, National Science Foundation, Before the Basic Research Subcommittee, House Science Committee, Hearing on Remote Sensing as a Research and Management Tool, September 1998.
- [16] G. Coyle et al., Home telecare for the elderly, Journal of Telemedicine and Telecare 1 (1995) 183–184.
- [17] R.J. Cramer, M.Z. Win, R.A. Scholtz, Impulse radio multipath characteristics and diversity reception, IEEE International Conference on Communications ICC'98 Vol. 3 (1998), pp. 1650–1654.
- [18] J.M. Cramer, R.A. Scholtz, M.Z. Win, On the analysis of UWB communication channels, IEEE MILCOM'99, 1999, pp. 1191–1195.
- [19] DSN Team, Multilateration Poster, SensIT Workshop, St. Petersburg, FL, April 2001.
- [20] J. Elson, D. Estrin, Random, ephemeral transaction identifiers in dynamic sensor networks, Proceedings 21st International Conference on Distributed Computing Systems, Mesa, AZ, April 2001, pp. 459–468.
- [21] I.A. Essa, Ubiquitous sensing for smart and aware environments, IEEE Personal Communications (October 2000) 47–49.
- [22] D. Estrin, L. Girod, G. Pottie, M. Srivastava, Instrumenting the world with wireless sensor networks, International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2001), Salt Lake City, Utah, May 2001.
- [23] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Next century challenges: scalable coordination in sensor networks, ACM MobiCom'99, Washington, USA, 1999, pp. 263–270.
- [24] D. Estrin, R. Govindan, J. Heidemann, Embedding the Internet, Communication ACM 43 (2000) 38–41.
- [25] P. Favre et al., A 2V, 600  $\mu$ A, 1 GHz BiCMOS super regenerative receiver for ISM applications, IEEE Journal of Solid State Circuits 33 (1998) 2186–2196.
- [26] M. Gell-Mann, What is complexity? Complexity 1 (1), 1995.
- [27] L. Girod, D. Estrin, Robust range estimation using acoustic and multimodal sensing, Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2001), Maui, Hawaii, October 2001.
- [28] K. Govil, E. Chan, H. Wasserman, Comparing algorithms for dynamic speed-setting of a low-power CPU, Proceedings of ACM MobiCom'95, Berkeley, CA, November 1995, pp. 13–25.
- [29] M.P. Hamilton, M. Flaxman, Scientific data visualization and biological diversity: new tools for spatializing multi-media observations of species and ecosystems, Landscape and Urban Planning 21 (1992) 285–297.
- [30] M.P. Hamilton, Hummercams, robots, and the virtual reserve, Directors Notebook, February 6, 2000, available from <http://www.jamesreserve.edu/news.html>.
- [31] B. Halweil, Study finds modern farming is costly, World Watch 14 (1) (2001) 9–10.
- [32] S. Hedetniemi, A. Liestman, A survey of gossiping and broadcasting in communication networks, Networks 18 (4) (1988) 319–349.
- [33] J. Heidemann, F. Silva, C. Intanagonwiwat, Building efficient wireless sensor networks with low-level naming, Proceedings of the Symposium on Operating Systems Principles, Banff, Canada, 2001.
- [34] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, IEEE Proceedings of the Hawaii International Conference on System Sciences, January 2000, pp. 1–10.
- [35] W.R. Heinzelman, J. Kulik, H. Balakrishnan, Adaptive protocols for information dissemination in wireless sensor networks, Proceedings of the ACM MobiCom'99, Seattle, Washington, 1999, pp. 174–185.
- [36] C. Herring, S. Kaplan, Component-based software systems for smart environments, IEEE Personal Communications, October 2000, pp. 60–61.
- [37] G. Hoblos, M. Staroswiecki, A. Aitouche, Optimal design of fault tolerant sensor networks, IEEE International Conference on Control Applications, Anchorage, AK, September 2000, pp. 467–472.
- [38] T. Imielinski, S. Goel, DataSpace: querying and monitoring deeply networked collections in physical space, ACM International Workshop on Data Engineering for Wireless and Mobile Access MobiDE 1999, Seattle, Washington, 1999, pp. 44–51.
- [39] C. Intanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: a scalable and robust communication paradigm for sensor networks, Proceedings of the ACM MobiCom'00, Boston, MA, 2000, pp. 56–67.
- [40] C. Jaikaeo, C. Srisathapornphat, C. Shen, Diagnosis of sensor networks, IEEE International Conference on Communications ICC'01, Helsinki, Finland, June 2001.
- [41] P. Johnson et al., Remote continuous physiological monitoring in the home, Journal of Telemed Telecare 2 (2) (1996) 107–113.

- [42] J.M. Kahn, R.H. Katz, K.S.J. Pister, Next century challenges: mobile networking for smart dust, Proceedings of the ACM MobiCom'99, Washington, USA, 1999, pp. 271–278.
- [43] T.H. Keitt, D.L. Urban, B.T. Milne, Detecting critical scales in fragmented landscapes, *Conservation Ecology* 1 (1) (1997) 4. Available from <<http://www.consecolo.org/vol1/iss1/art4>>.
- [44] R. Kravets, K. Schwan, K. Calvert, Power-aware communication for mobile computers, Proceedings of Mo-MUC'99, San Diego, CA, November 1999, pp. 64–73.
- [45] H. Lee, B. Han, Y. Shin, S. Im, Multipath characteristics of impulse radio channels, IEEE Vehicular Technology Conference Proceedings, Tokyo, Vol. 3, 2000, pp. 2487–2491.
- [46] C.J. Le Martret, G.B. Giannakis, All-digital impulse radio for MUI/ISI-resilient multiuser communications over frequency-selective multipath channels, Proceedings of IEEE Military Communications Conference (MILCOM'00), Vol. 2, 2000, pp. 655–659.
- [47] P. Letteri, M.B. Srivastava, Adaptive frame length control for improving wireless link throughput, range and energy efficiency, Proceedings of IEEE INFOCOM'98, San Francisco, USA, March 1998, pp. 564–571.
- [48] L. Li, J.Y. Halpern, Minimum-energy mobile wireless networks revisited, IEEE International Conference on Communications ICC'01, Helsinki, Finland, June 2001.
- [49] J. Lorch, A. Smith, Reducing processor power consumption by improving processor time management in a single-user operating system, Proceedings of ACM MobiCom'96, 1996.
- [50] S. Meguerdichian, F. Koushanfar, G. Qu, M. Potkonjak, Exposure in wireless ad-hoc sensor networks, Proceedings of ACM MobiCom'01, Rome, Italy, 2001, pp. 139–150.
- [51] T. Melly, A. Porret, C.C. Enz, E.A. Vittoz, A 1.2 V, 430 MHz, 4dBm power amplifier and a 250  $\mu$ W Frontend, using a standard digital CMOS process, IEEE International Symposium on Low Power Electronics and Design Conference, San Diego, August 1999, pp. 233–237.
- [52] R. Min, T. Furrer, A. Chandrakasan, Dynamic voltage scaling techniques for distributed microsensor networks, Proceedings of ACM MobiCom'95, August 1995.
- [53] F.R. Mireles, R.A. Scholtz, Performance of equicorrelated ultra-wideband pulse-position-modulated signals in the indoor wireless impulse radio channel, IEEE Conference on Communications, Computers and Signal Processing, Vol. 2, 1997, pp. 640–644.
- [54] J. Mirkovic, G.P. Venkataramani, S. Lu, L. Zhang, A self-organizing approach to data forwarding in largescale sensor networks, IEEE International Conference on Communications ICC'01, Helsinki, Finland, June 2001.
- [55] D. Nadig, S.S. Iyengar, A new architecture for distributed sensor integration, Proceedings of IEEE Southeastcon'93, Charlotte, NC, April 1993.
- [56] Y.H. Nam et al., Development of remote diagnosis system integrating digital telemetry for medicine, International Conference IEEE-EMBS, Hong Kong, 1998, pp. 1170–1173.
- [57] T. Nandagopal, T. Kim, X. Gao, V. Bhargavan, Achieving MAC layer fairness in wireless packet networks, Proceedings of the ACM MobiCom'00, Boston, MA, 2000.
- [58] B. Narendran, J. Sienicki, S. Yajnik, P. Agrawal, Evaluation of an adaptive power and error control algorithm for wireless systems, IEEE International Conference on Communications ICC'97, Montreal, Canada, June 1997.
- [59] National Semiconductor Corporation, LMX3162 Single Chip Radio Transceiver, Evaluation Notes and Datasheet, March 2000.
- [60] N. Noury, T. Herve, V. Rialle, G. Virone, E. Mercier, G. Morey, A. Moro, T. Porcheron, Monitoring behavior in home using a smart fall sensor, IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology, October 2000, pp. 607–610.
- [61] With Glacier Park in Its Path, Fire Spreads to 40,000 Acres, New York Times, Vol. 150, Issue 51864, p. 24, 0p, 1 map, 4c, 9/2/2001.
- [62] M. Ogawa et al., Fully automated biosignal acquisition in daily routine through 1 month, International Conference on IEEE-EMBS, Hong Kong, 1998, pp. 1947–1950.
- [63] N. Priyantha, A. Chakraborty, H. Balakrishnan, The cricket location-support system, Proceedings of ACM MobiCom'00, August 2000, pp. 32–43.
- [64] T. Pering, T. Burd, R. Brodersen, The simulation and evaluation of dynamic voltage scaling algorithms, Proceedings of International Symposium on Low Power Electronics and Design ISLPED'98, August 1998, pp. 76–81.
- [65] C. Perkins, Ad Hoc Networks, Addison-Wesley, Reading, MA, 2000.
- [66] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, SPINS: security protocols for sensor networks, Proceedings of ACM MobiCom'01, Rome, Italy, 2001, pp. 189–199.
- [67] E.M. Petriu, N.D. Georganas, D.C. Petriu, D. Makrakis, V.Z. Groza, Sensor-based information appliances, IEEE Instrumentation and Measurement Magazine (December 2000) 31–35.
- [68] A. Porret, T. Melly, C.C. Enz, E.A. Vittoz, A low-power low-voltage transceiver architecture suitable for wireless distributed sensors network, IEEE International Symposium on Circuits and Systems'00, Geneva, Vol. 1, 2000, pp. 56–59.
- [69] G.J. Pottie, W.J. Kaiser, Wireless integrated network sensors, Communications of the ACM 43 (5) (2000) 551–558.
- [70] J. Rabaey, J. Ammer, J.L. da Silva Jr., D. Patel, PicoRadio: ad-hoc wireless networking of ubiquitous low-energy sensor/monitor nodes, Proceedings of the IEEE Computer Society Annual Workshop on VLSI (VLSI'00), Orlando, Florida, April 2000, pp. 9–12.
- [71] J.M. Rabaey, M.J. Ammer, J.L. da Silva Jr., D. Patel, S. Roundy, PicoRadio supports ad hoc ultra-low power

- wireless networking, IEEE Computer Magazine (2000) 42–48.
- [72] T. Rappaport, Wireless Communications: Principles and Practice, Prentice-Hall, Englewood Cliffs, NJ, 1996.
  - [73] V. Rodoplu, T.H. Meng, Minimum energy mobile wireless networks, IEEE Journal of Selected Areas in Communications 17 (8) (1999) 1333–1344.
  - [74] A. Savvides, C. Han, M. Srivastava, Dynamic fine-grained localization in ad-hoc networks of sensors, Proceedings of ACM MobiCom'01, Rome, Italy, July 2001, pp. 166–179.
  - [75] C. Shen, C. Srisathapornphat, C. Jaikaeo, Sensor information networking architecture and applications, IEEE Personal Communications, August 2001, pp. 52–59.
  - [76] E. Shih, B.H. Calhoun, S. Cho, A. Chandrakasan, Energy-efficient link layer for wireless microsensor networks, Proceedings IEEE Computer Society Workshop on VLSI 2001, Orlando, FL, April 2001, pp. 16–21.
  - [77] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, A. Chandrakasan, Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks, Proceedings of ACM MobiCom'01, Rome, Italy, July 2001, pp. 272–286.
  - [78] B. Sibbald, Use computerized systems to cut adverse drug events: report, CMAJ: Canadian Medical Association Journal 164 (13) (2001) 1878, 1/2p, 1c.
  - [79] S. Singh, M. Woo, C.S. Raghavendra, Power-aware routing in mobile ad hoc networks, Proceedings of ACM MobiCom'98, Dallas, Texas, 1998, pp. 181–190.
  - [80] A. Sinha, A. Chandrakasan, Dynamic power management in wireless sensor networks, IEEE Design and Test of Computers, March/April 2001.
  - [81] S. Slijepcevic, M. Potkonjak, Power efficient organization of wireless sensor networks, IEEE International Conference on Communications ICC'01, Helsinki, Finland, June 2001.
  - [82] K. Sohrabi, B. Manriquez, G. Pottie, Near-ground wideband channel measurements, IEEE Proceedings of Vehicular Technology Conference, New York, 1999.
  - [83] K. Sohrabi, J. Gao, V. Ailawadhi, G.J. Pottie, Protocols for self-organization of a wireless sensor network, IEEE Personal Communications, October 2000, pp. 16–27.
  - [84] C. Srisathapornphat, C. Jaikaeo, C. Shen, Sensor information networking architecture, International Workshop on Parallel Processing, September 2000, pp. 23–30.
  - [85] Y. Tseng, S. Wu, C. Lin, J. Sheu, A multi-channel MAC protocol with power control for multi-hop mobile ad hoc networks, IEEE International Conference on Distributed Computing Systems, Mesa, AZ, April 2001, pp. 419–424.
  - [86] S. Vardhan, M. Wilczynski, G. Pottie, W.J. Kaiser, Wireless integrated network sensors (WINS): distributed in situ sensing for mission and flight systems, IEEE Aerospace Conference, Vol. 7, 2000, pp. 459–463.
  - [87] B. Walker, W. Steffen, An overview of the implications of global change of natural and managed terrestrial ecosystems, Conservation Ecology 1 (2) (1997). Available from <<http://www.consecol.org/vol1/iss2/art2>>.
  - [88] B. Warneke, B. Liebowitz, K.S.J. Pister, Smart dust: communicating with a cubic-millimeter computer, IEEE Computer (January 2001) 2–9.
  - [89] <http://www.fao.org/sd/EIdirect/EIre0074.htm>.
  - [90] <http://www.alertsystems.org>.
  - [91] M. Weiser et al., Scheduling for reduced CPU energy, Proceedings of 1st USENIX Symposium on Operating System Design and Implementation, November 1994, pp. 13–23.
  - [92] S. Wicker, Error Control Coding for Digital Communication and Storage, Prentice-Hall, Englewood Cliffs, NJ, 1995.
  - [93] A. Woo, D. Culler, A transmission control scheme for media access in sensor networks, Proceedings of ACM MobiCom'01, Rome, Italy, July 2001, pp. 221–235.
  - [94] S. Wu, C. Lin, Y. Tseng, J. Sheu, A new multi channel MAC protocol with on-demand channel assignment for multihop mobile ad hoc networks, International Symposium on Parallel Architectures, Algorithms, and Networks, I-SPAN 2000, Dallas, 2000, pp. 232–237.
  - [95] S. Wu, Y. Tseng, J. Sheu, Intelligent medium access for mobile ad hoc networks with busy tones and power control, IEEE Journal on Selected Areas in Communications (September 2000) 1647–1657.
  - [96] Y. Xu, J. Heidemann, D. Estrin, Geography-informed energy conservation for ad hoc routing, Proceedings of ACM MobiCom'2001, Rome, Italy, July 2001.
  - [97] M. Zorzi, R. Rao, Error control and energy consumption in communications for nomadic computing, IEEE Transactions on Computers 46 (3) (1997) 279–289.

# **CS 442**

# **Wireless Sensor Network**

## **Unit 2**

### **Unit 2:**

Antennas, propagation, and path loss, Digital radio communication, RF spectrum, modulation, 2-ray model, others.

## **Unit 2**

## **Wireless fundamentals**

# Wireless networks

- Access computing/communication services, **on the move**
- Wireless WANs
  - Cellular Networks: GSM, GPRS, CDMA
  - Satellite Networks: Iridium
- Wireless LANs
  - WiFi Networks: 802.11
  - Personal Area Networks: Bluetooth
- Wireless MANs
  - WiMaX Networks: 802.16
  - Mesh Networks: Multi-hop WiFi
  - Adhoc Networks: useful when infrastructure not available

3

## Limitations

- Limitations of the **Wireless Network**
  - limited communication bandwidth
  - frequent disconnections
  - heterogeneity of fragmented networks
- Limitations Imposed by **Mobility**
  - route breakages
  - lack of mobility awareness by system/applications
- Limitations of the **Device**
  - short battery lifetime
  - limited capacities

4

# Mobile communication

## ■ Wireless vs. mobile Examples



stationary computer  
laptop in a hotel (portable)  
wireless LAN, WSN  
Personal Digital Assistant (PDA)

- Integration of wireless into existing fixed networks:
  - Local area networks: IEEE 802.11, HIPERLAN
  - Wide area networks: Cellular 3G, IEEE 802.16
  - Internet: Mobile IP extension

## Wireless v/s Wired networks

- **Regulations of frequencies**
  - Limited availability, coordination is required
  - useful frequencies are almost all occupied
- **Bandwidth and delays**
  - Low transmission rates
    - few Kbits/s to some Mbit/s.
  - Higher delays
    - several hundred milliseconds
  - Higher loss rates
    - susceptible to interference, e.g., engines, lightning
- **Always shared medium**
  - Lower security, simpler active attacking
  - radio interface accessible for everyone
  - secure access mechanisms important

# Wireless link characteristics

- *decreased signal strength*: radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources*: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- *multipath propagation*: radio signal reflects off objects ground, arriving at destination at slightly different times

.... make communication across (even a point to point) wireless link much more "difficult"

SNR: signal-to-noise ratio

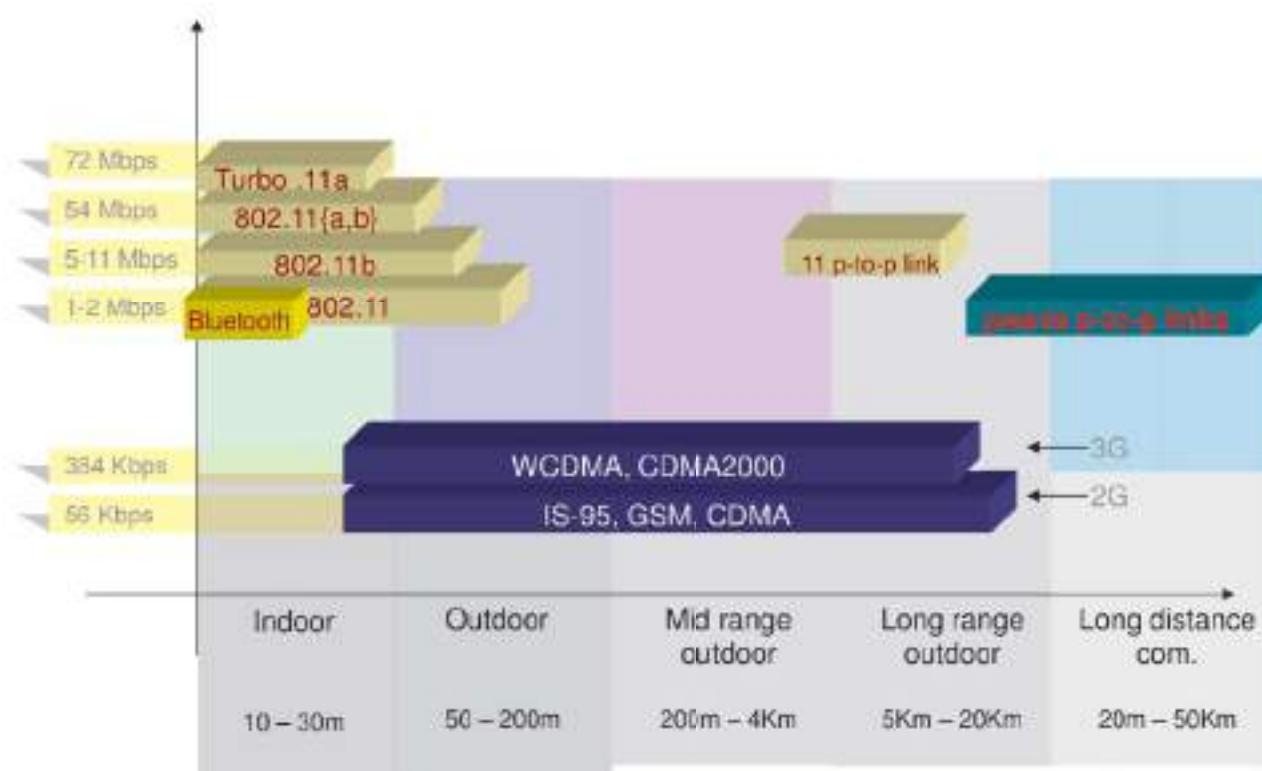
- larger SNR – easier to extract signal from noise (a "good thing")

## *SNR versus BER tradeoffs*

- *given physical layer*: increase power -> increase SNR->decrease BER
- *given SNR*: choose physical layer that meets BER requirement, giving highest throughput
  - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)

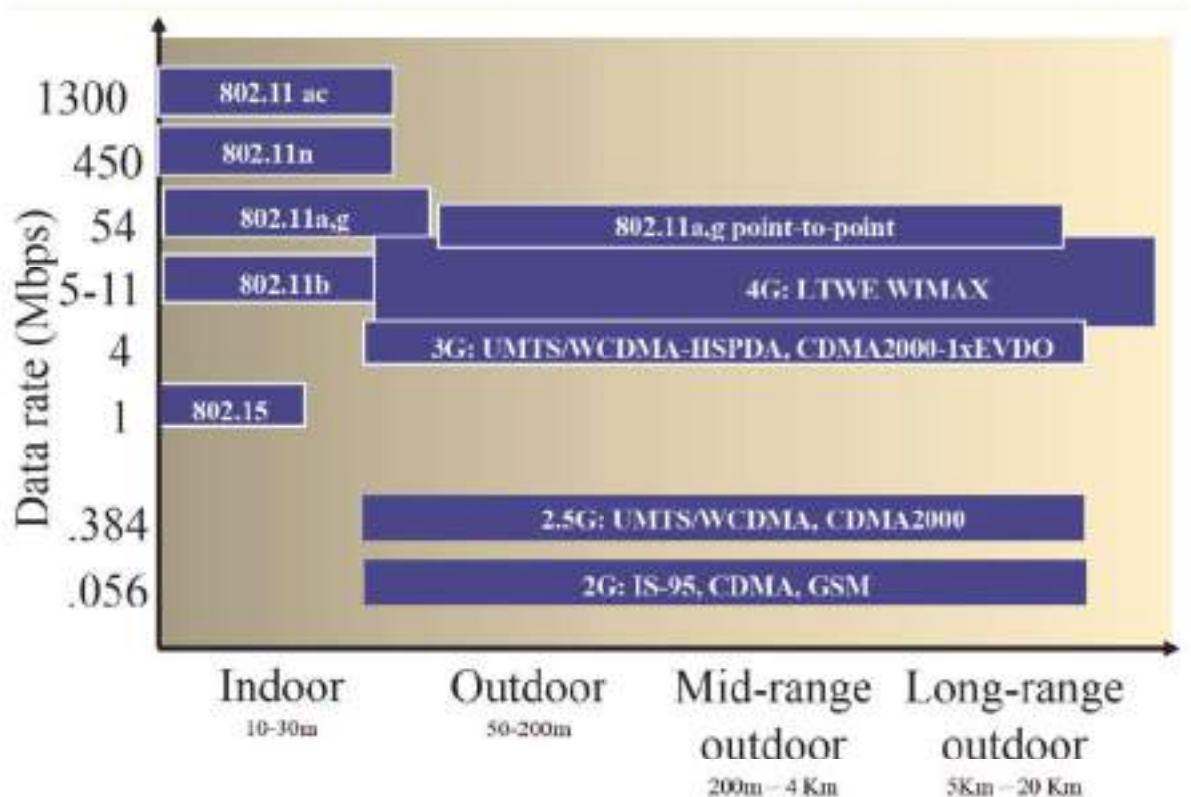
7

# Wireless Technology Landscape



8

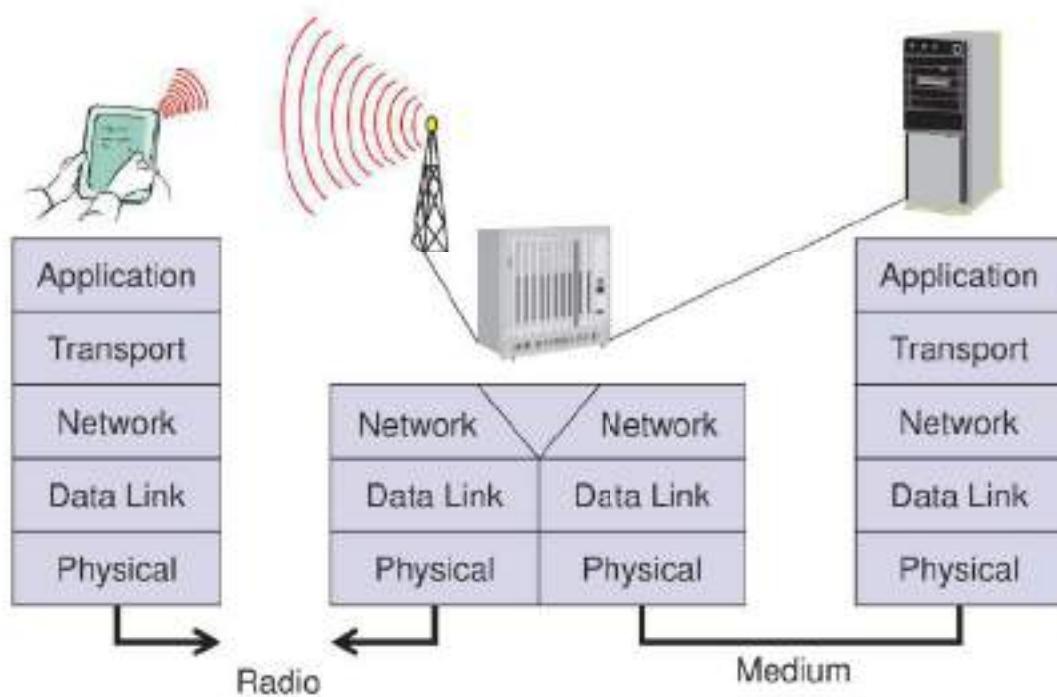
# Characteristics of selected WL link



9

## OSI reference Vs Wireless Networks

# Reference model



11

## Perspectives

- **Network designers:** Concerned with cost-effective design
  - Need to ensure that network resources are efficiently utilized and fairly allocated to different users.
- **Network users:** Concerned with application services
  - Need guarantees that each message sent will be delivered without error within a certain amount of time.
- **Network providers:** Concerned with system administration
  - Need mechanisms for security, management, fault-tolerance and accounting.

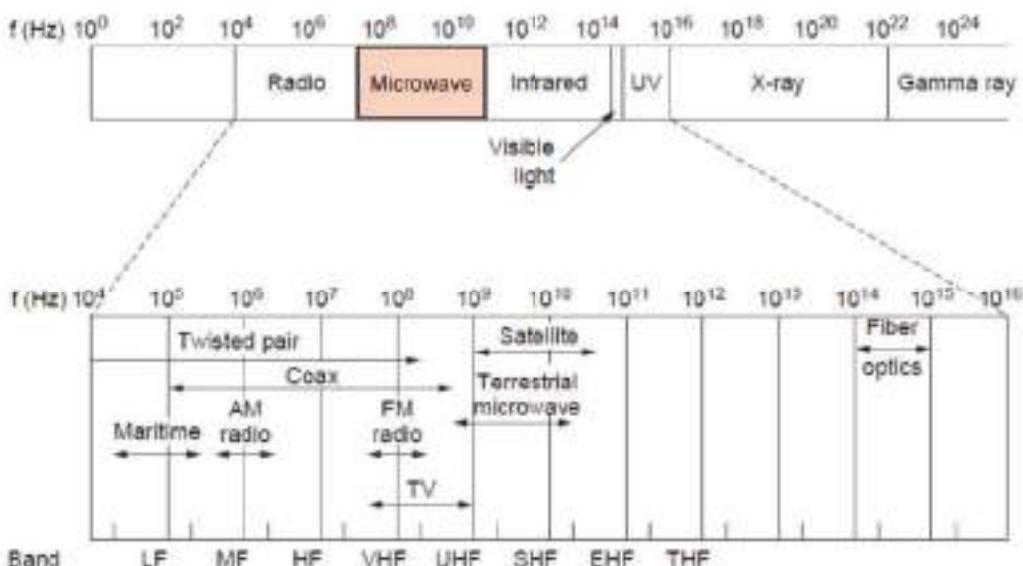
12

## RF Basics

### Factors affecting wireless system design

- Frequency allocations
  - What range to operate? May need licenses.
- Multiple access mechanism
  - How do users share the medium without interfering?
- Antennas and propagation
  - What distances? Possible channel errors introduced.
- Signals encoding
  - How to improve the data rate?
- Error correction
  - How to ensure that bandwidth is not wasted?

# RF Spectrum



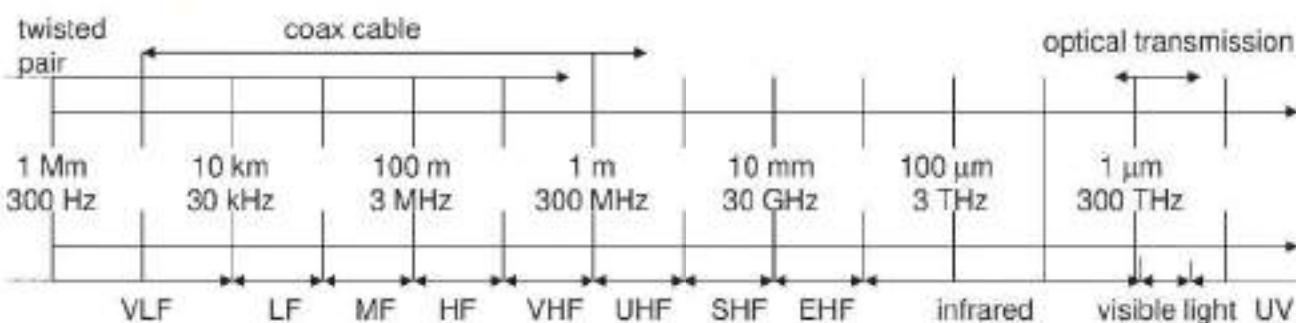
Different bands have different uses:

- Radio: wide-area broadcast; Infrared/Light: line-of-sight
- Microwave: LANs and 3G/4G/5G;

← Networking focus

15

## Frequencies for communication



- VLF = Very Low Frequency
- LF = Low Frequency
- MF = Medium Frequency
- HF = High Frequency
- VHF = Very High Frequency
- Frequency and wave length:  $\lambda = c/f$
- wave length  $\lambda$ , speed of light  $c \approx 3 \times 10^8$  m/s, frequency  $f$
- UHF = Ultra High Frequency
- SHF = Super High Frequency
- EHF = Extra High Frequency
- UV = Ultraviolet Light

16

# Wireless frequency allocation

- Radio frequencies range from 9KHz to 400GHZ (ITU)
- Microwave frequency range
  - 1 GHz to 40 GHz
  - Directional beams possible
  - Suitable for point-to-point transmission
  - Used for satellite communications
- Radio frequency range
  - 30 MHz to 1 GHz
  - Suitable for omnidirectional applications
- Infrared frequency range
  - Roughly,  $3 \times 10^{11}$  to  $2 \times 10^{14}$  Hz
  - Useful in local point-to-point multipoint applications within confined areas

17

## Frequencies for mobile communication

- VHF-/UHF-ranges for mobile radio
  - simple, small antenna for cars
  - deterministic propagation characteristics, reliable connections
- SHF and higher for directed radio links, satellite communication
  - small antenna, focusing
  - large bandwidth available
- Wireless LANs use frequencies in UHF to SHF spectrum
  - some systems planned up to EHF
  - limitations due to absorption by water and oxygen molecules (resonance frequencies)
    - weather dependent fading, signal loss caused by heavy rainfall etc.

18

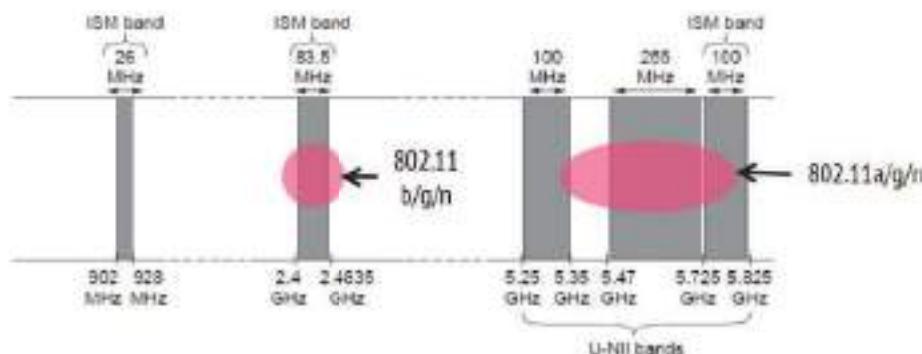
# Frequency regulations

- Frequencies from 9KHz to 300 MHZ in high demand (especially VHF: 30-300MHZ)
- Two unlicensed bands
  - Industrial, Science, and Medicine (ISM): 2.4 GHz
  - Unlicensed National Information Infrastructure (UNII): 5.2 GHz
- Different agencies license and regulate
  - [www.fcc.gov](http://www.fcc.gov) - US
  - [www.etsi.org](http://www.etsi.org) - Europe
  - [www.wpc.dot.gov.in](http://www.wpc.dot.gov.in) - India
  - [www.itu.org](http://www.itu.org) - International co-ordination
- Regional, national, and international issues
- Procedures for military, emergency, air traffic control, etc

19

## ISM band

- ISM: Industrial Scientific and Medical Radio band
- Free for use at low power; devices manage interference
- Widely used for networking; WiFi, Bluetooth, Zigbee, etc.

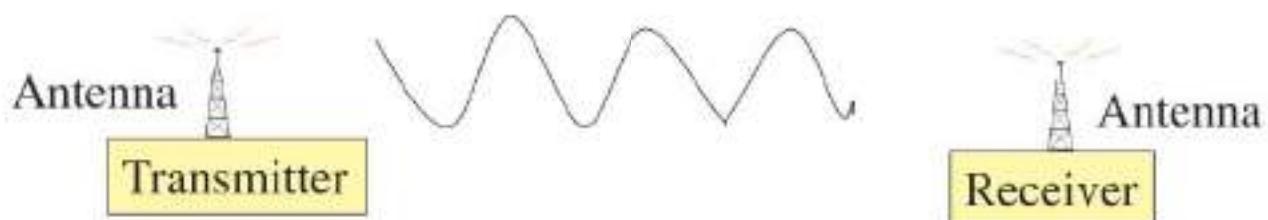


20

## Wireless transmission

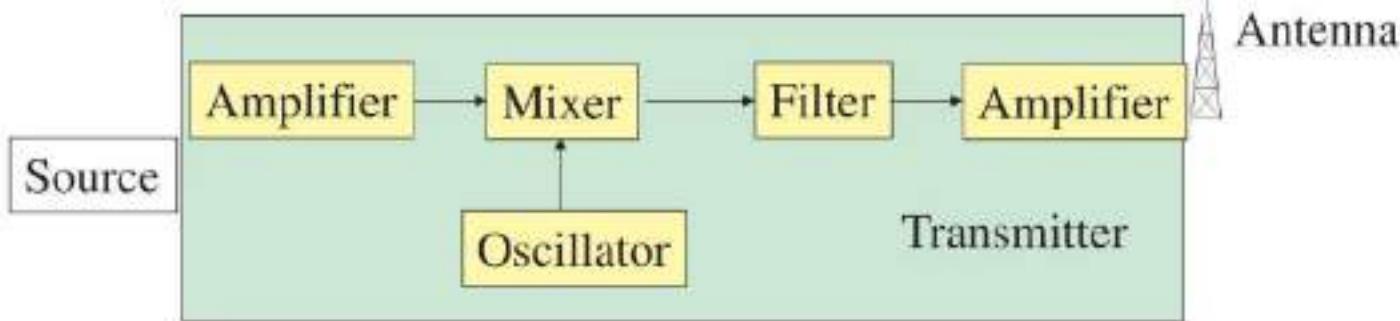
21

## Wireless transmission



- Wireless communication systems consist of:
  - Transmitters
  - Antennas: radiates electromagnetic energy into air
  - Receivers
- In some cases, transmitters and receivers are on same device, called transceivers.

# Transmitters



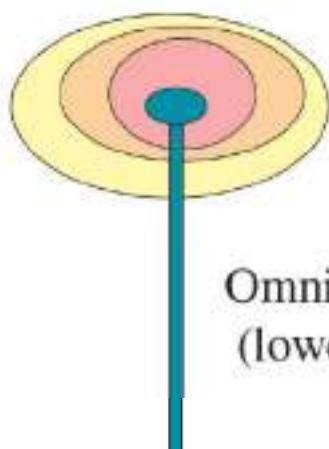
Suppose, to generate a signal that is sent at 900 MHz and the original source generates a signal at 300 MHz.

- Amplifier - strengthens the initial signal
- Oscillator - creates a carrier wave of 600 MHz
- Mixer - combines signal with oscillator and produces 900 MHz (also does modulation, etc)
- Filter - selects correct frequency
- Amplifier - Strengthens the signal before sending it

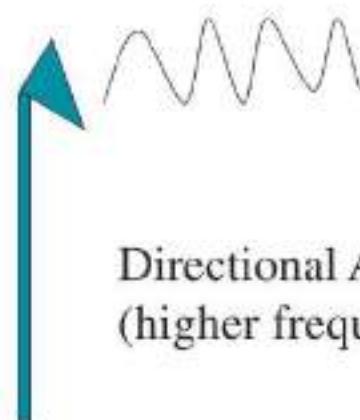
# Antennas

# Antennas

- An antenna is an electrical conductor or system of conductors to send/receive RF signals
  - Transmission - radiates electromagnetic energy into space
  - Reception - collects electromagnetic energy from space
- In two-way communication, the same antenna can be used for transmission and reception



Omnidirectional Antenna  
(lower frequency)

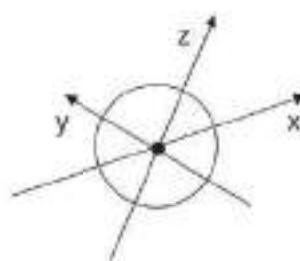
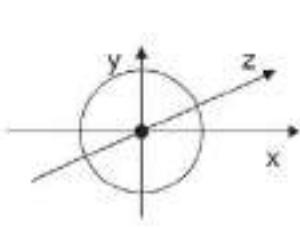


Directional Antenna  
(higher frequency)

25

## Antennas: isotropic radiator

- Radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission
- Isotropic radiator: equal radiation in all directions (three dimensional) - only a **theoretical reference antenna**
- Real antennas always have directive effects (vertically and/or horizontally)
- Radiation pattern: measurement of radiation around an antenna

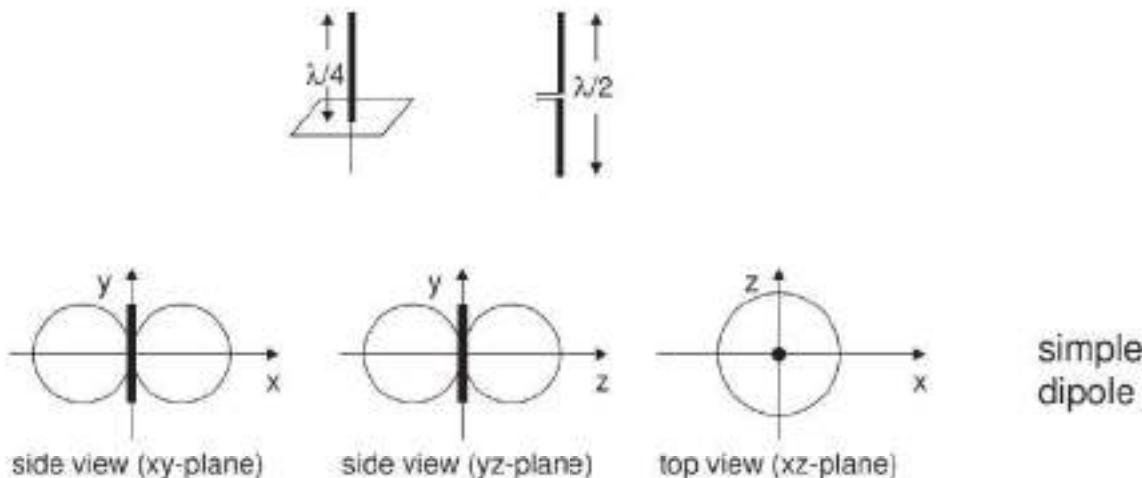


ideal  
isotropic  
radiator

26

# Antennas: simple dipoles

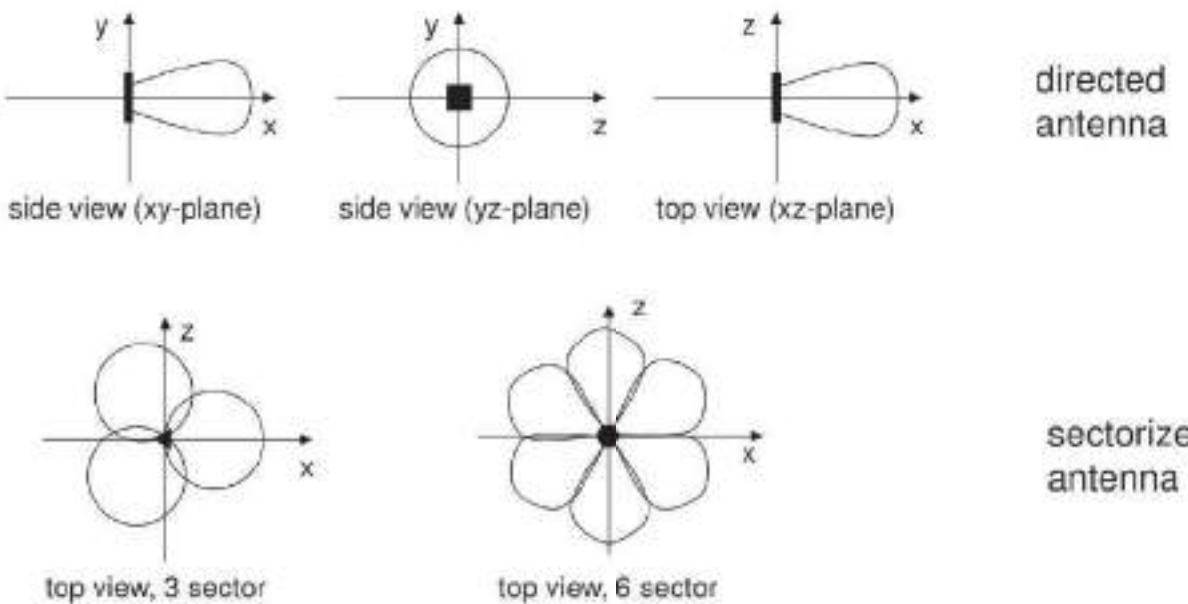
- Real antennas are not isotropic radiators
  - dipoles with lengths  $\lambda/4$  on car roofs or  $\lambda/2$  (Hertzian dipole)  
→ shape of antenna proportional to wavelength
- Gain: maximum power in the direction of the main lobe compared to the power of an isotropic radiator (with the same average power)



27

# Antennas: directed and sectorized

- Often used for microwave connections or base stations for mobile phones (e.g., radio coverage of a valley)

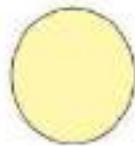


28

# Antenna models

## In **Omni Mode**:

- Nodes receive signals with gain  $G^o$



## In **Directional Mode**:

- Capable of beamforming in specified direction
- Directional Gain  $G^d$  ( $G^d > G^o$ )



29

## Directional communication

Received Power  $\propto$  (Transmit power)

\*(Tx Gain) \* (Rx Gain)

Directional gain is higher

Directional antennas useful for:

- Increase “range”, keeping transmit power constant
- Reduce transmit power, keeping range comparable with omni mode

30

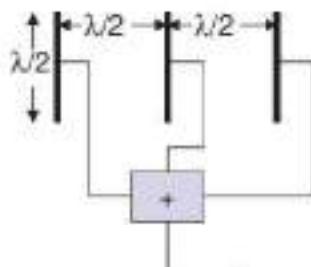
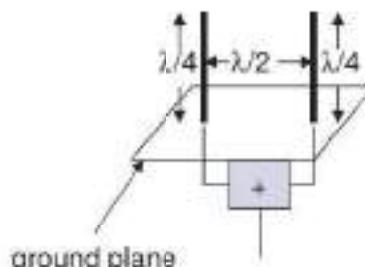
# Comparison of omni and directional

Issues	Omni	Directional
Spatial Reuse	Low	High
Connectivity	Low	High
Interference	Omni 	Directional 
Cost & Complexity	Low	High

31

## Antennas: diversity

- Grouping of 2 or more antennas
  - multi-element antenna arrays
- Antenna diversity
  - switched diversity, selection diversity
    - receiver chooses antenna with largest output
  - diversity combining
    - combine output power to produce gain
    - cophasing needed to avoid cancellation



32

# Signal Propagation Model

## Signals

- physical representation of data
- function of time and location
- signal parameters: parameters representing the value of data
- classification
  - continuous time/discrete time
  - continuous values/discrete values
  - analog signal = continuous time and continuous values
  - digital signal = discrete time and discrete values
- signal parameters of periodic signals:  
period  $T$ , frequency  $f=1/T$ , amplitude  $A$ , phase shift  $\phi$ 
  - sine wave as special periodic signal for a carrier:

$$s(t) = A_t \sin(2 \pi f_t t + \phi_t)$$

# Signal Propagation Model

CS 442 WSN Unit-2

## Signals

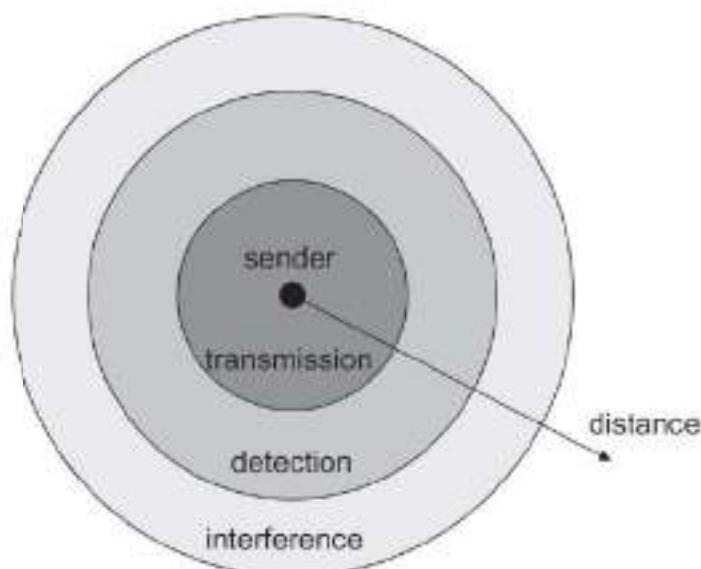
- physical representation of data
- function of time and location
- signal parameters: parameters representing the value of data
- classification
  - continuous time/discrete time
  - continuous values/discrete values
  - analog signal = continuous time and continuous values
  - digital signal = discrete time and discrete values
- signal parameters of periodic signals:  
period  $T$ , frequency  $f=1/T$ , amplitude  $A$ , phase shift  $\varphi$ 
  - sine wave as special periodic signal for a carrier:

$$s(t) = A_t \sin(2 \pi f_t t + \varphi_t)$$

CS 442 WSN Unit-2

# Signal propagation ranges

- Transmission range
  - communication possible
  - low error rate
- Detection range
  - detection of the signal possible
  - no communication possible
- Interference range
  - signal may not be detected
  - signal adds to the background noise



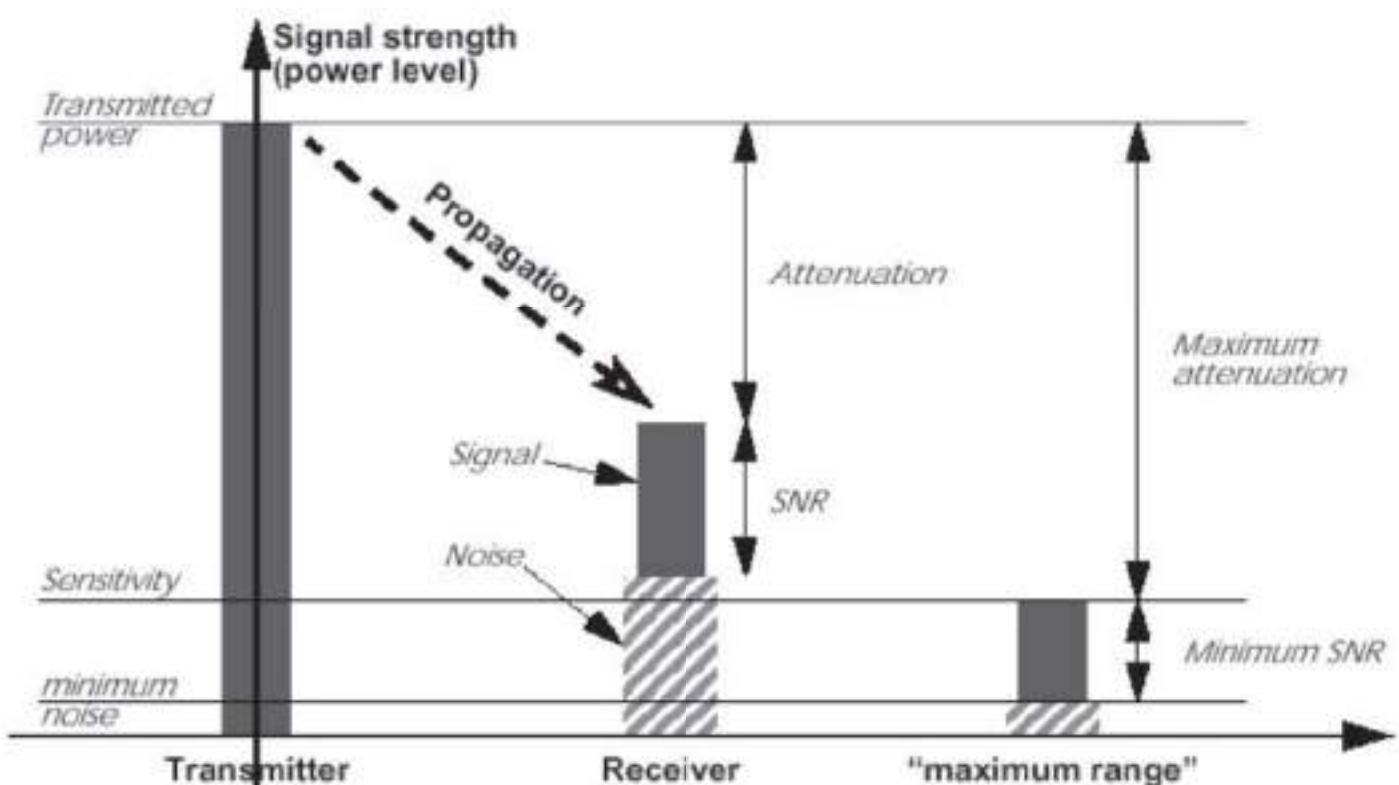
CS 442 WSN Unit-2

# Attenuation

- Strength of signal falls off with distance over transmission medium
- Attenuation factors for unguided media:
  - Received signal must have sufficient strength so that circuitry in the receiver can interpret the signal
  - Signal must maintain a level sufficiently higher than noise to be received without error
  - Attenuation is greater at higher frequencies, causing distortion
- Approach: amplifiers that strengthen higher frequencies

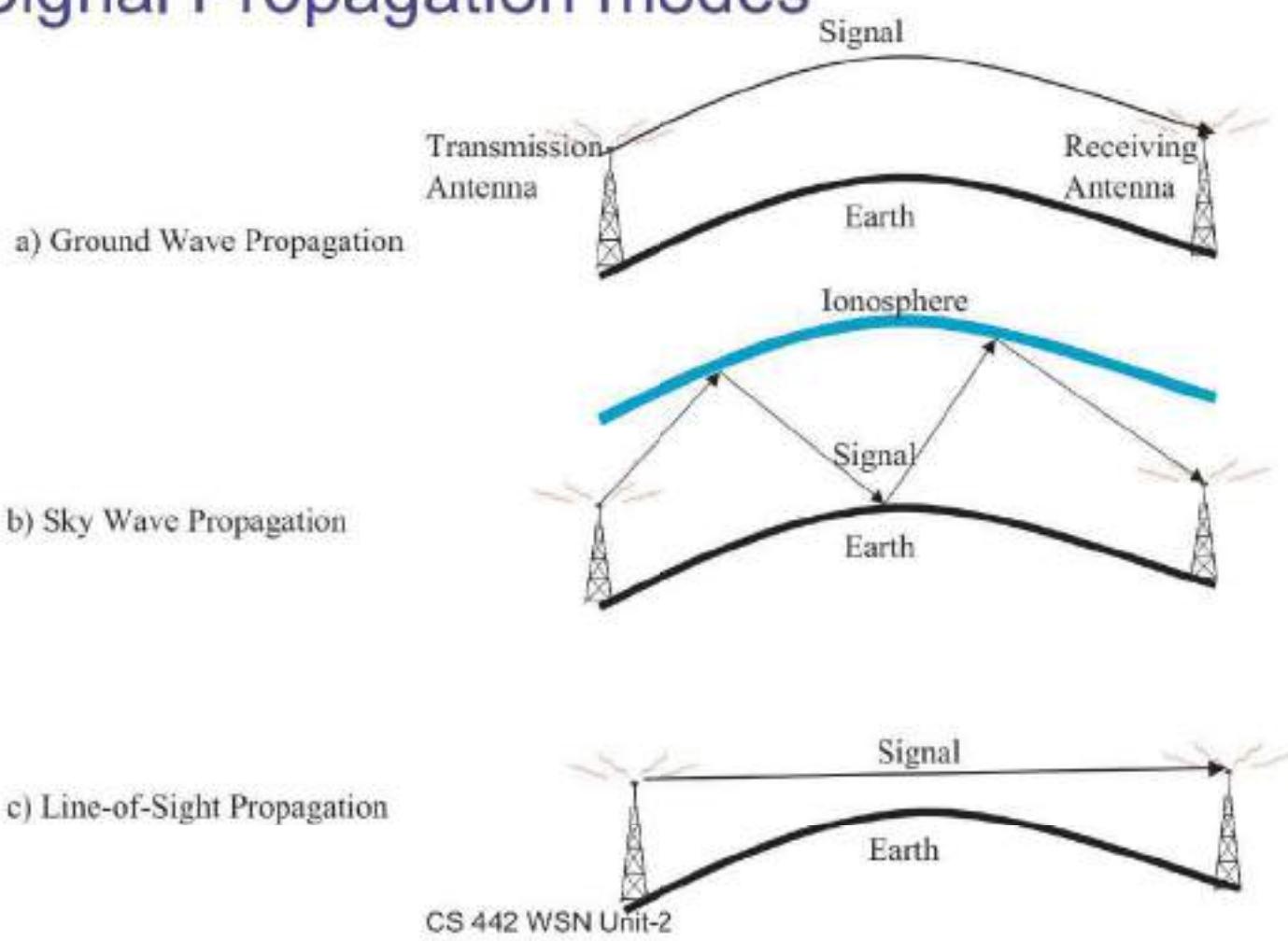
CS 442 WSN Unit-2

# Attenuation: Propagation & Range



CS 442 WSN Unit-2

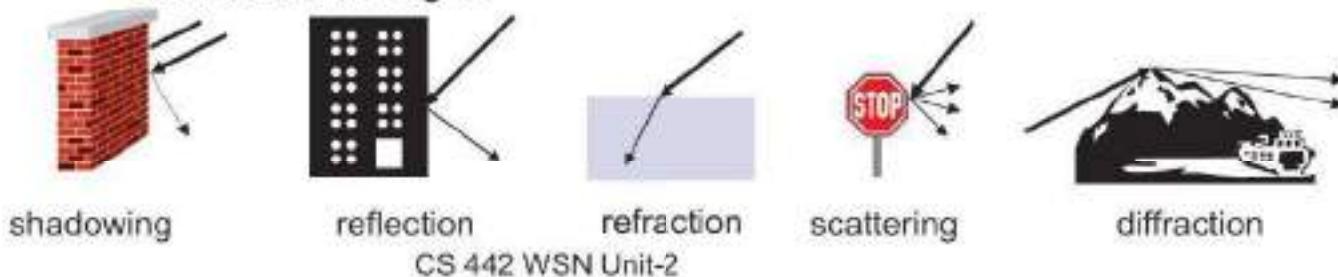
## Signal Propagation modes



CS 442 WSN Unit-2

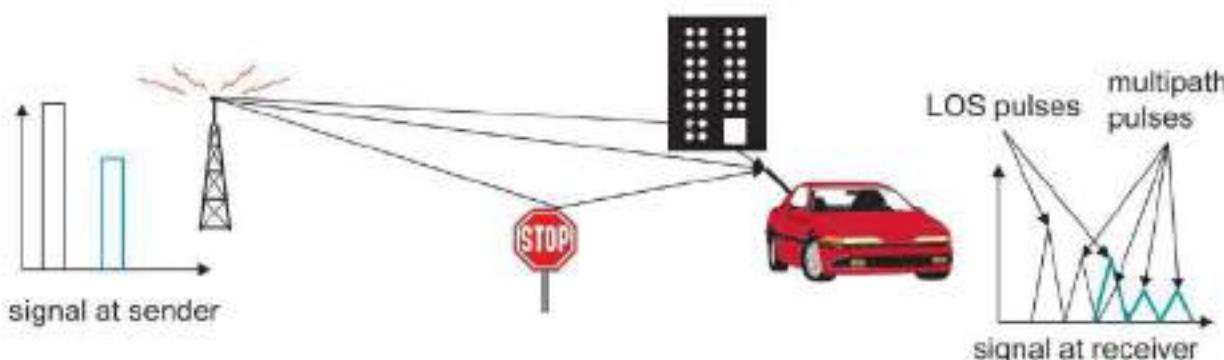
# Signal propagation

- Propagation in free space always like light (straight line)
- Receiving power proportional to  $1/d^2$   
( $d$  = distance between sender and receiver)
- Receiving power additionally influenced by
  - fading (frequency dependent)
  - shadowing
  - reflection at large obstacles
  - refraction depending on the density of a medium
  - scattering at small obstacles
  - diffraction at edges



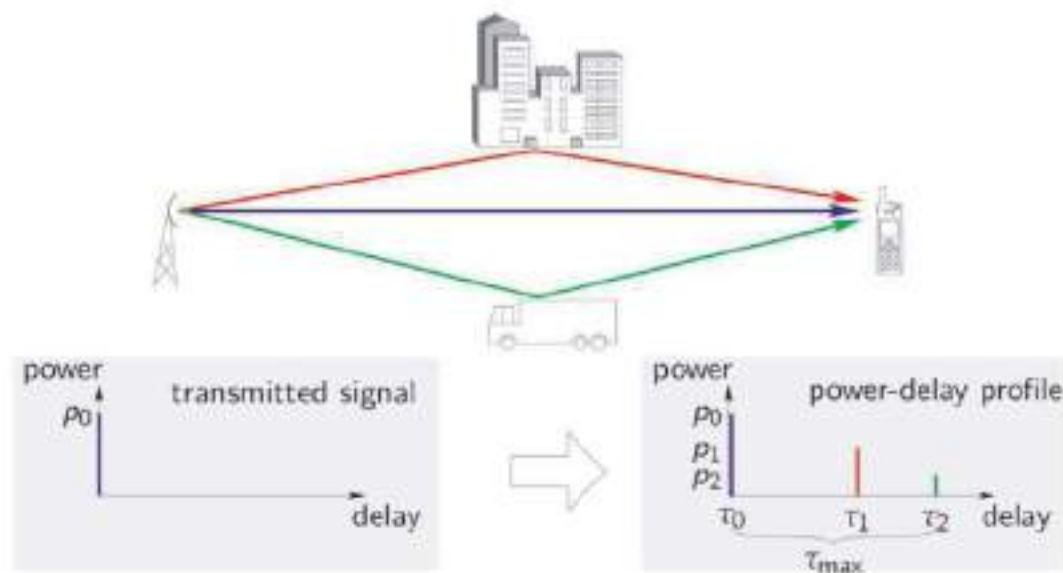
# Multipath propagation

- Signal can take many different paths between sender and receiver due to reflection, scattering, diffraction



- Time dispersion: signal is dispersed over time
- → interference with “neighbor” symbols, Inter Symbol Interference (ISI)
- The signal reaches a receiver directly and phase shifted
- → distorted signal depending on the phases of the different parts

# Multipath channel effect



CS 442 WSN  
Fall 2014

# Signal attenuation : Path loss

Free space loss, ideal isotropic antenna

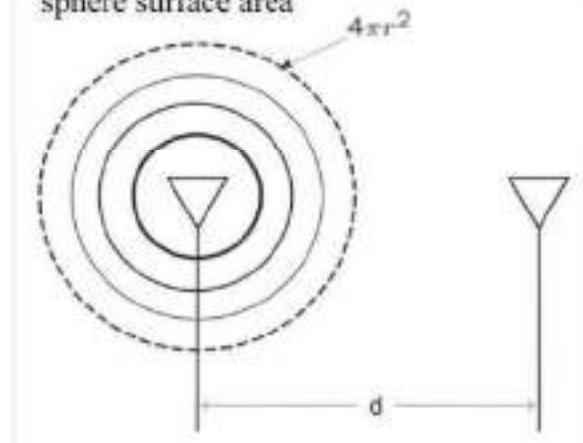
$$\frac{P_r}{P_t} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi f d)^2}{c^2}$$

- $P_t$  = signal power at transmitting antenna
  - $P_r$  = signal power at receiving antenna
  - $\lambda$  = carrier wavelength
  - $d$  = propagation distance between antennas
  - $c$  = speed of light ( $3 \times 10^8$  m/s)
- where  $d$  and  $\lambda$  are in the same units (e.g., meters)

With antenna gains

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

energy received at an antenna distance  $d$  away is inversely proportional to the sphere surface area

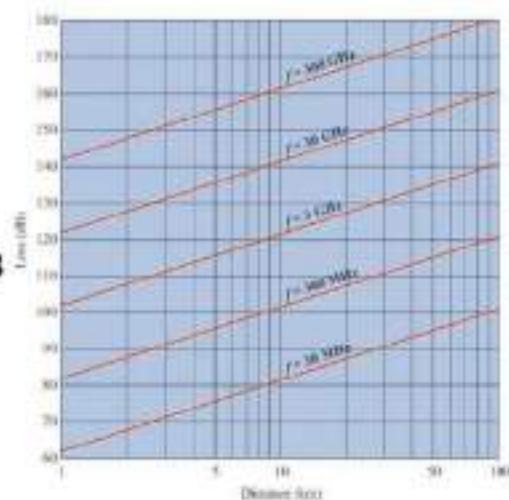


CS 442 WSN  
Fall 2014

## Free Path loss

- Free space loss equation can be recast:

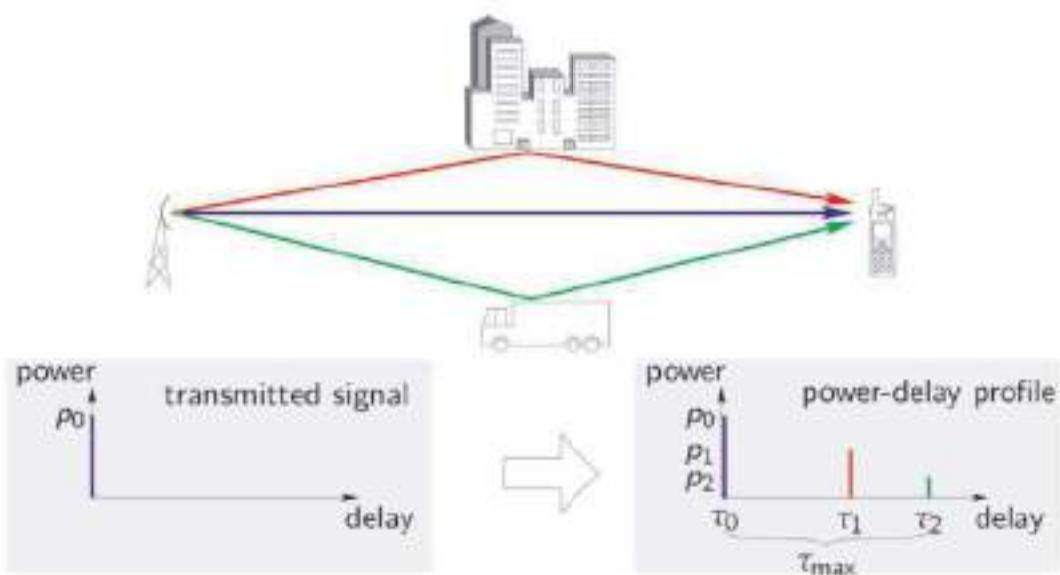
$$\begin{aligned}L_{dB} &= 10 \log \frac{P_t}{P_r} = 20 \log \left( \frac{4\pi d}{\lambda} \right) \\&= -20 \log(\lambda) + 20 \log(d) + 21.98 \text{ dB} \\&= 20 \log \left( \frac{4\pi f d}{c} \right) = 20 \log(f) + 20 \log(d) - 147.56 \text{ dB}\end{aligned}$$



CS 442 WSN

Figure 9

## Multipath channel effect

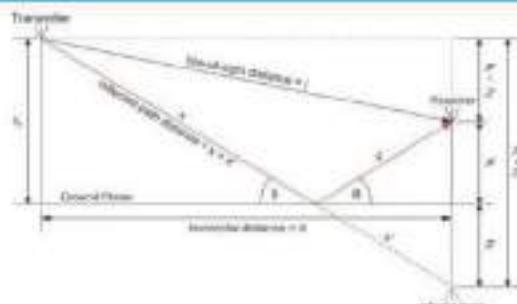


CS 442 WSN

Figure 10

## Path Loss : Two ray model

$$P_r = P_t \frac{G_t G_r h_t^2 h_r^2}{d^4}$$



### Empirical Pathloss Formula

$$P_r = P_t P_o \left( \frac{d_o}{d} \right)^\alpha$$

$\alpha$  = Pathloss exponent

$d_0$  = 1m

$P_0$  = Received power at  $d_0$

## Path Loss Exponents for Different Environments

Environment	Path Loss Exponent, $n$
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed cellular radio	3 to 5
In building line-of-sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

# Review: Five basic propagation mechanisms

---

1. **Free-space propagation**
2. **Transmission**
  - ▶ Through a medium
  - ▶ Refraction occurs at boundaries
3. **Reflections**
  - ▶ Waves impinge upon surfaces that are large compared to the signal wavelength
4. **Diffraction**
  - ▶ Secondary waves behind objects with sharp edges
5. **Scattering**
  - ▶ Interactions between small objects or rough surfaces

CS 442 WSN

Page 2

# Review: Models Derived from Empirical Measurements

---

- ▶ Need to design systems based on empirical data applied to a particular environment
  - ▶ To determine power levels, tower heights, height of mobile antennas
- ▶ Okumura developed a model, later refined by Hata
  - ▶ Detailed measurement and analysis of the Tokyo area
  - ▶ Among the best accuracy in a wide variety of situations
- ▶ Predicts path loss for typical environments
  - ▶ Urban
  - ▶ Small, medium sized city
  - ▶ Large city
  - ▶ Suburban
  - ▶ Rural

Environment	Path Loss Exponent, $\alpha$
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed cellular radio	3 to 5
In building line-of-sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

CS 442 WSN

Page 2

## Review: The Effects of Multipath Propagation

---

- ▶ Reflection, diffraction, and scattering
- ▶ Multiple copies of a signal may arrive at different phases
  - ▶ If phases add destructively, the signal level relative to noise declines, making detection more difficult
- ▶ Intersymbol interference (ISI)
  - ▶ One or more delayed copies of a pulse may arrive at the same time as the primary pulse for a subsequent bit
- ▶ Rapid signal fluctuations
  - ▶ Over a few centimeters

CS 442 WSN

Page 9

## Review : Attenuation, Fading

---

- ▶ Strength of signal falls off with distance over transmission medium
- ▶ Attenuation factors for unguided media:
  - ▶ Received signal must have sufficient strength so that circuitry in the receiver can interpret the signal
  - ▶ Signal must maintain a level sufficiently higher than noise to be received without error
  - ▶ Attenuation is greater at higher frequencies, causing distortion

CS 442 WSN

Page 9

## Fading...

---

- ▶ Large-scale fading
  - ▶ Signal variations over large distances
  - ▶ Path loss  $L_{dB}$  as we have seen already
  - ▶ Shadowing
  - ▶ Doppler spread
- ▶ Statistical variations
  - ▶ Rayleigh fading
  - ▶ Ricean fading

CS 442 WSN  
Fall 2010

## Shadowing

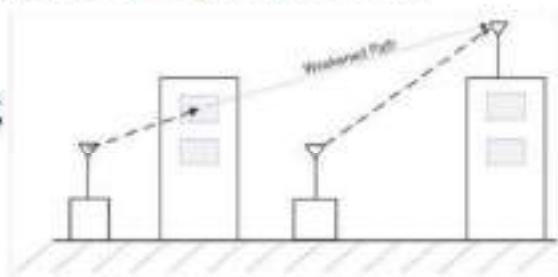
---

Trees and buildings may be located between the transmitter and the receiver and cause degradation in received signal strength

Shadowing is a random process

$$P_r = P_t P_a \chi \left( \frac{d_s}{d} \right)^\alpha$$

$$\chi = 10^{x/10}, \text{ where } x \sim N(0, \sigma_x^2)$$



CS 442 WSN  
Fall 2010

## Fading...

---

- ▶ Large-scale fading
  - ▶ Signal variations over large distances
  - ▶ Path loss  $L_{dB}$  as we have seen already
  - ▶ Shadowing
  - ▶ Doppler spread
- ▶ Statistical variations
  - ▶ Rayleigh fading
  - ▶ Ricean fading

CS 442 WSN  
Fall 2010

## Shadowing

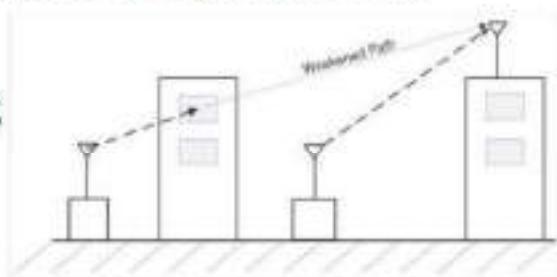
---

Trees and buildings may be located between the transmitter and the receiver and cause degradation in received signal strength

Shadowing is a random process

$$P_r = P_t P_a \chi \left( \frac{d_s}{d} \right)^\alpha$$

$$\chi = 10^{x/10}, \text{ where } x \sim N(0, \sigma_x^2)$$



CS 442 WSN  
Fall 2010

## Doppler spread

Doppler power spectrum is caused by *motion* between the transmitter and receiver

*Doppler power spectrum* gives the statistical power distribution of the channel versus frequency for a signal transmitted at one exact frequency

Doppler spread is

$$f_D = \frac{vf_c}{c} \quad \text{where } v \text{ is the maximum speed between the transmitter and the receiver, } f_c \text{ is the carrier frequency, and } c \text{ is the speed of light}$$

Doppler varies with  $f_c$ . If communication bandwidth  $B \ll f_c$ ,  $f_D$  can be treated as approximately constant.

The coherence time and Doppler spread are inversely related

$$T_c \approx \frac{1}{f_D}$$

## Fading types : Doppler spread

- ▶ **Doppler Spread**
  - ▶ Frequency fluctuations caused by movement
- ▶ **Coherence time  $T_c$**  characterizes Doppler shift
  - ▶ How long a channel remains the same
- ▶ Coherence time  $T_c \gg T_b$  bit time  $\rightarrow$  ***slow fading***
  - ▶ The channel does not change during the bit time
- ▶ Otherwise ***fast fading***
- ▶ **Example :  $T_c = 70$  ms, bit rate  $r_b = 100$  kbs**
  - ▶ Bit time  $T_b = 1/100 \times 10^3 = 10 \mu\text{s}$
  - ▶  $T_c \gg T_b$ ?  $70 \text{ ms} \gg 10 \mu\text{s}$ ?
  - ▶ True, so ***slow fading***

## Fading types : Multi path

---

- ▶ Multipath fading
  - ▶ Multiple signals arrive at the receiver
  - ▶ **Coherence bandwidth  $B_c$**  characterizes multipath
    - ▶ Bandwidth over which the channel response remains relatively constant
    - ▶ Related to delay spread, the spread in time of the arrivals of multipath signals
  - ▶ **Signal bandwidth  $B_s$  is proportional to the bit rate**
  - ▶ If  $B_c \gg B_s$ , then ***flat fading***
    - ▶ The signal bandwidth fits well within the channel bandwidth
  - ▶ Otherwise, ***frequency selective fading***
- ▶ Example:  $B_c = 150$  kHz, bit rate  $r_b = 100$  kbs
  - ▶ Assume signal bandwidth  $B_s \approx r_b$ ,  $B_s = 100$  kHz
  - ▶  $B_c \gg B_s$ ?  $150$  kHz  $\gg 100$  kHz?
  - ▶ Using a factor of 10 for “ $\gg$ ”,  $150$  kHz is not more than  $10 \times 100$  kHz
  - ▶ False, so *frequency selective fading*

CS 442 WSN

Page 2

## Noise

---

- ▶ Thermal Noise
- ▶ Intermodulation noise
- ▶ Crosstalk
- ▶ Impulse Noise

CS 442 WSN

Page 3

## Thermal Noise

---

- ▶ Thermal noise due to agitation of electrons
- ▶ Present in all electronic devices and transmission media
- ▶ Cannot be eliminated
- ▶ Function of temperature

## Noise contd.

---

- ▶ **Intermodulation noise** – occurs if signals with different frequencies share the same medium
  - ▶ Interference caused by a signal produced at a frequency that is the sum or difference of original frequencies
- ▶ **Crosstalk** – unwanted coupling between signal paths
- ▶ **Impulse noise** – irregular pulses or noise spikes
  - ▶ Short duration and of relatively high amplitude
  - ▶ Caused by external electromagnetic disturbances, or faults and flaws in the communications system

**\*\* Next**

---

CS 442 WSN Unit-2

# **CS 442**

## **Wireless Sensor Network**

### **Unit 2 – Contd.**

CS 442 WSN U2

#### **Unit 2:**

RF spectrum,

Antennas, propagation, and path loss, 2-ray model,

Digital radio communication,

modulation, others.

## **Unit 2**

### **Wireless fundamentals**

CS 442 WSN U2

# Examples of Analog and Digital Data

- Analog
  - Video
  - Audio
- Digital
  - Text
  - Integers

CS-442 WSN I/2

## Analog Signals

- A **continuously varying** electromagnetic wave that may be propagated over a variety of media, depending on frequency
- Examples of media:
  - Copper wire media (twisted pair and coaxial cable)
  - Fiber optic cable
  - Atmosphere or space propagation
- Analog signals **can propagate analog and digital data**

CS-442 WSN I/2

# Digital Signals

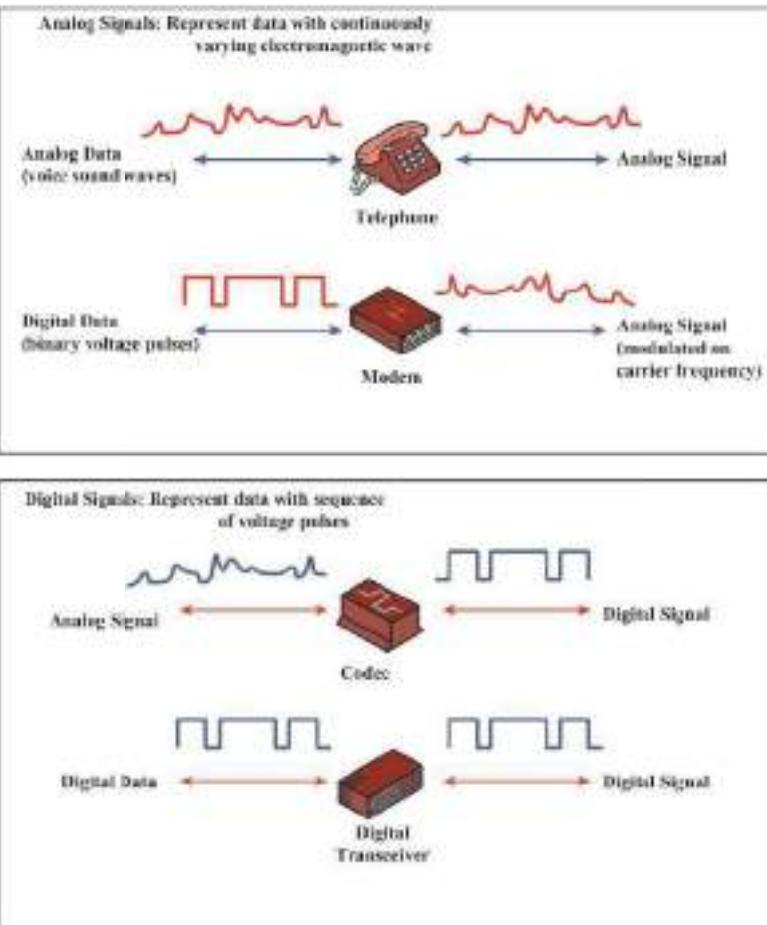
- A **sequence of voltage pulses** that may be transmitted over a copper wire medium
- Generally **cheaper than analog** signaling
- Less susceptible to noise interference
- **Suffer more from attenuation**
- Digital signals can propagate analog and digital data

CS-442 WSN L2

## Data and Signal Combinations

- Digital data, digital signal
  - Equipment for **encoding** is **less expensive** than digital-to-analog equipment
- Analog data, digital signal
  - Conversion **permits use of modern digital transmission** and switching equipment
- Digital data, analog signal
  - **Some transmission media will only propagate analog signals**
  - Examples include optical fiber and satellite
- Analog data, analog signal
  - Analog data **easily** converted to analog signal

CS-442 WSN L2



Analog and Digital Signaling of Analog and Digital Data

## Analog Transmission

- Transmit analog signals without regard to content
- **Attenuation limits length of transmission link**
- Cascaded amplifiers boost signal's energy for longer distances but cause distortion
  - Analog data can tolerate distortion
  - Introduces errors in digital data

# Digital Transmission

- Concerned with the content of the signal
- **Attenuation endangers integrity of data**
- Digital Signal
  - Repeaters achieve greater distance
  - Repeaters recover the signal and retransmit
- Analog signal carrying digital data
  - Retransmission device recovers the digital data from analog signal
  - Generates new, clean analog signal

CS-442 WSN I/2

# Channel Capacity

- **Impairments**, such as noise, limit data rate that can be achieved
- Channel Capacity – **the maximum rate** at which data can be transmitted over a given communication path, or channel, under given conditions

CS-442 WSN I/2

# Concepts : Channel Capacity

- **Data rate** - rate at which data can be communicated (bps)
- **Bandwidth** - the bandwidth of the transmitted signal as constrained by the transmitter and the nature of the transmission medium (Hertz)
- **Noise** - average level of noise over the communications path
- **Error rate** - rate at which errors occur
  - Error = transmit 1 and receive 0; transmit 0 and receive 1

CS-442 WSN I/2

# Frequency-Domain Concepts

- **Fundamental frequency** - when all frequency components of a signal are integer multiples of one frequency, it's referred to as the fundamental frequency
- **Spectrum** - range of frequencies that a signal contains
- **Absolute bandwidth** - width of the spectrum of a signal
- **Effective bandwidth** (or just bandwidth) - narrow band of frequencies that most of the signal's energy is contained in

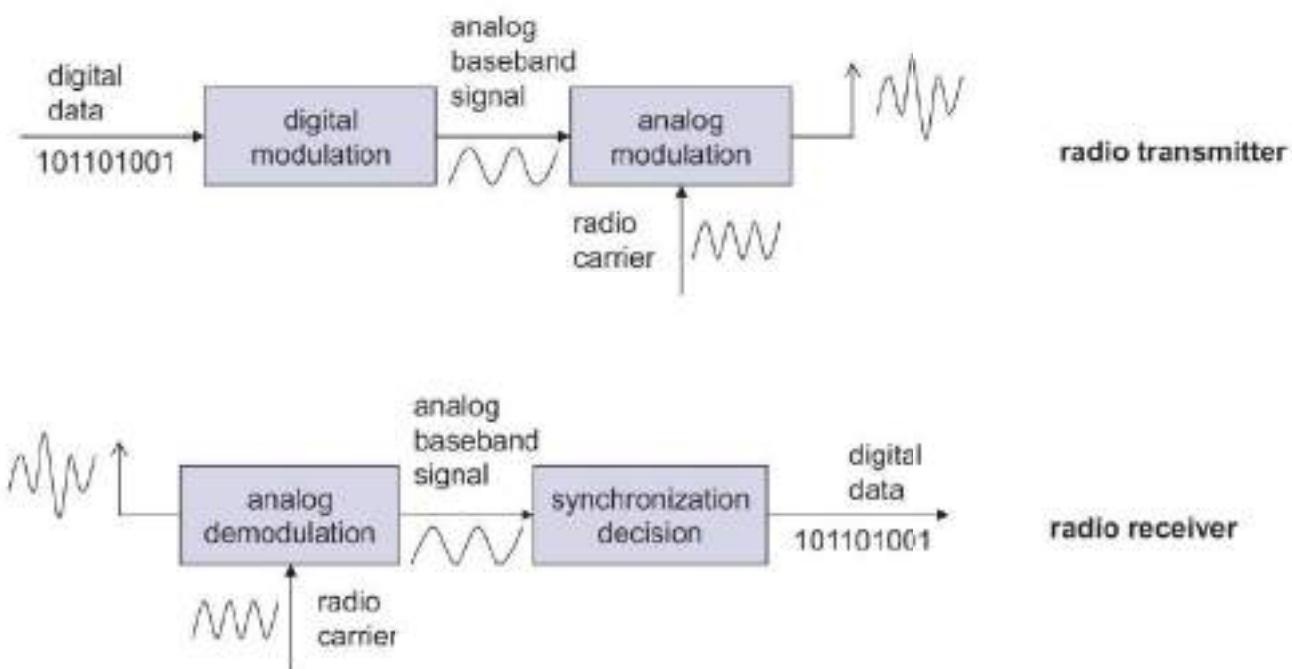
CS-442 WSN I/2

# Modulation

- Digital modulation
  - digital data is translated into an analog signal (baseband)
  - ASK, FSK, PSK
  - differences in spectral efficiency, power efficiency, robustness
- Analog modulation
  - shifts center frequency of baseband signal up to the radio carrier
- Motivation
  - smaller antennas (e.g.,  $\lambda/4$ )
  - Frequency Division Multiplexing
  - medium characteristics
- Basic schemes
  - Amplitude Modulation (AM)
  - Frequency Modulation (FM)
  - Phase Modulation (PM)

CS 442 WSN U2

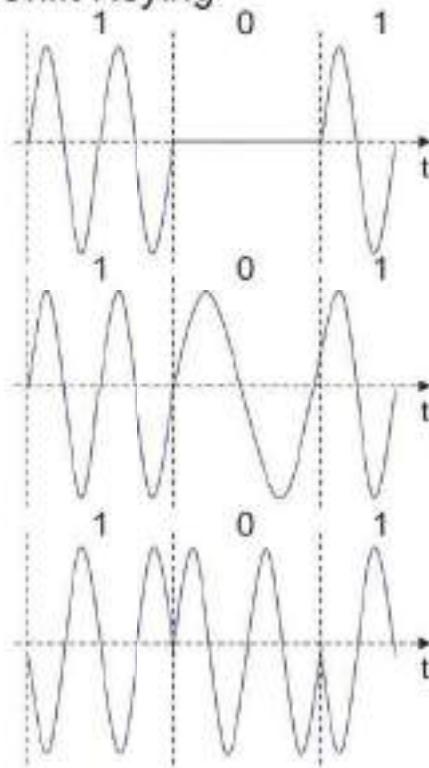
## Modulation and demodulation



CS 442 WSN U2

# Digital modulation

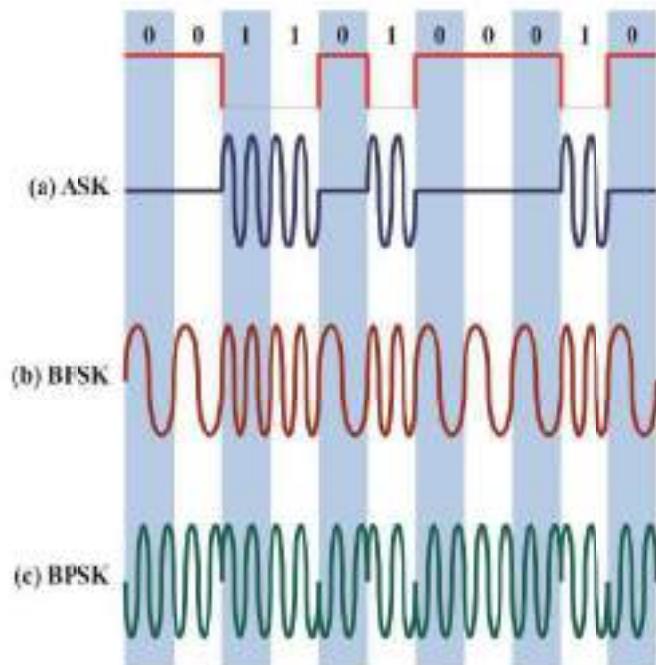
- Modulation of digital signals known as Shift Keying
- Amplitude Shift Keying (ASK):
  - very simple
  - low bandwidth requirements
  - very susceptible to interference
- Frequency Shift Keying (FSK):
  - needs larger bandwidth
- Phase Shift Keying (PSK):
  - more complex
  - robust against interference
- Many advanced variants



CS 442 WSN U2

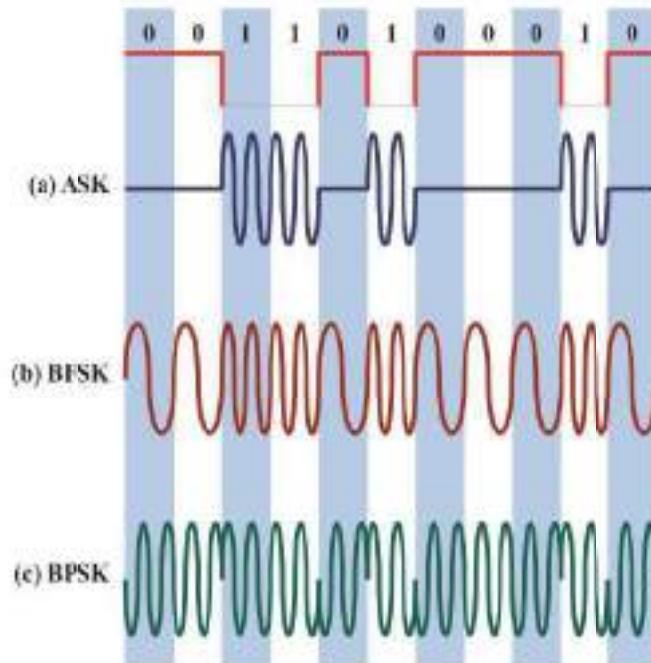
## Encoding Techniques

- Digital data to analog signal
  - Amplitude-shift keying (ASK)
    - Amplitude difference of carrier frequency
  - Frequency-shift keying (FSK)
    - Frequency difference near carrier frequency
  - Phase-shift keying (PSK)
    - Phase of carrier signal shifted



## Modulation of Analog Signals for Digital Data

CS-442 WSN I/2



## Modulation of Analog Signals for Digital Data

CS-442 WSN I/2

# Review : Signal

- Signal parameters of periodic signals:  
period  $T$ , frequency  $f=1/T$ , amplitude  $A$ , phase shift  $\varphi$ 
  - sine wave as special periodic signal for a carrier:

$$s(t) = A_t \sin(2 \pi f_t t + \varphi_t)$$

# Amplitude-Shift Keying

- One binary digit represented by presence of carrier, at constant amplitude
- Other binary digit represented by absence of carrier

$$s(t) = \begin{cases} A\cos(2\pi f_c t) & \text{binary 1} \\ 0 & \text{binary 0} \end{cases}$$

- where the carrier signal is  $A\cos(2\pi f_c t)$

CS-442 WSN I/2

# Amplitude-Shift Keying

- Susceptible to sudden gain changes
- Inefficient modulation technique
- Used to transmit digital data over optical fiber

CS-442 WSN I/2

## Binary Frequency-Shift Keying (BFSK)

- Two binary digits represented by two different frequencies near the carrier frequency

$$s(t) = \begin{cases} A \cos(2\pi f_1 t) & \text{binary 1} \\ A \cos(2\pi f_2 t) & \text{binary 0} \end{cases}$$

- where  $f_1$  and  $f_2$  are offset from carrier frequency  $f_c$  by equal but opposite amounts  $f_d$

CS-442 WSN I/2

## Binary Frequency-Shift Keying (BFSK)

- Less susceptible to error than ASK
- Used for high-frequency (3 to 30 MHz) radio transmission
- Can be used at higher frequencies on LANs that use coaxial cable

CS-442 WSN I/2

# Multiple Frequency-Shift Keying (MFSK)

- More than two frequencies are used
- More bandwidth efficient but more susceptible to error

$$s_i(t) = A \cos 2\pi f_i t \quad 1 \leq i \leq M$$

- $f_i = f_c + (2i - 1 - M)f_d$
- $f_c$  = the carrier frequency
- $f_d$  = the difference frequency
- $M$  = number of different signal elements =  $2^L$
- $L$  = number of bits per signal element

CS-442 WSN I/2

# Phase-Shift Keying (PSK)

- Two-level PSK (BPSK)
  - Uses two phases to represent binary digits

$$\begin{aligned} s(t) &= \begin{cases} A \cos(2\pi f_c t) & \text{binary 1} \\ A \cos(2\pi f_c t + \pi) & \text{binary 0} \end{cases} \\ &= \begin{cases} A \cos(2\pi f_c t) & \text{binary 1} \\ -A \cos(2\pi f_c t) & \text{binary 0} \end{cases} \end{aligned}$$

CS-442 WSN I/2

# Quadrature Phase-Shift Keying (PSK)

- Four-level PSK (QPSK)
  - Each element represents more than one bit

$$s(t) = \begin{cases} A \cos\left(2\pi f_c t + \frac{\pi}{4}\right) & 11 \\ A \cos\left(2\pi f_c t + \frac{3\pi}{4}\right) & 01 \\ A \cos\left(2\pi f_c t - \frac{3\pi}{4}\right) & 00 \\ A \cos\left(2\pi f_c t - \frac{\pi}{4}\right) & 10 \end{cases}$$

CS-442 WSN I/2

# Multiplexing

- Capacity of transmission medium usually exceeds capacity required for transmission of a single signal
- Multiplexing - carrying multiple signals on a single medium
  - More efficient use of transmission medium

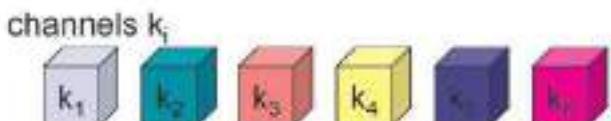
CS-442 WSN I/2



**Multiplexing**

## Multiplexing Mechanisms

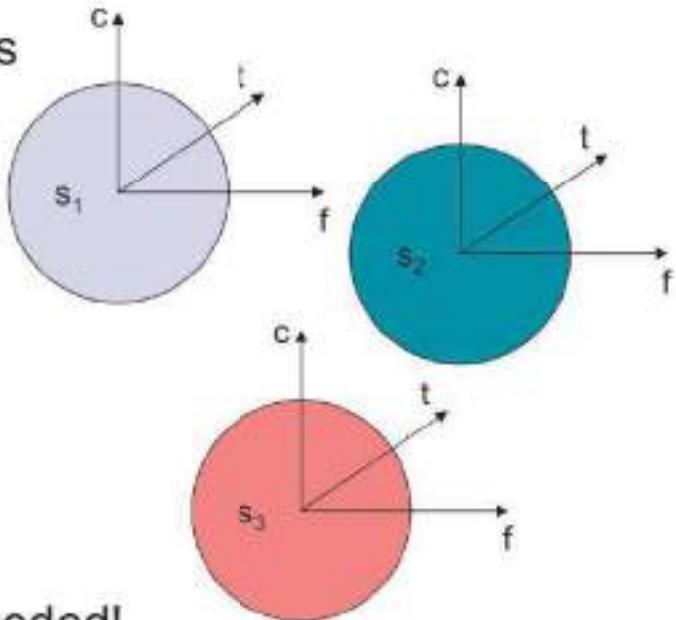
# Multiplexing



- Multiplexing in 4 dimensions

- space ( $s_i$ )
  - time ( $t$ )
  - frequency ( $f$ )
  - code ( $c$ )

- Goal: multiple use  
of a shared medium
- Important: guard spaces needed!



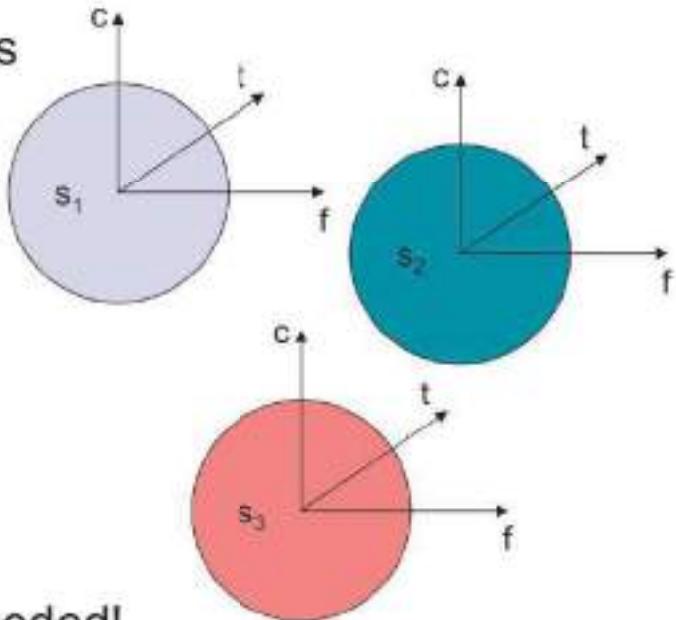
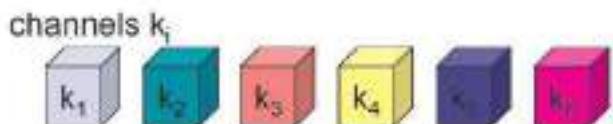
# Multiplexing

- Multiplexing in 4 dimensions

- space ( $s_i$ )
- time ( $t$ )
- frequency ( $f$ )
- code ( $c$ )

- Goal: multiple use of a shared medium

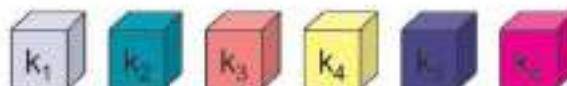
- Important: guard spaces needed!



CS 442 WSN U2

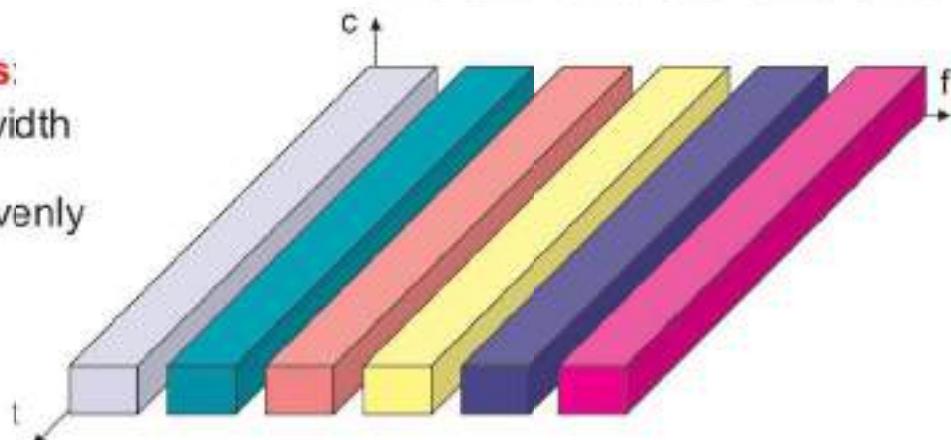
## Frequency multiplex

- Separation of the whole spectrum into smaller frequency bands
- A channel gets a certain band of the spectrum for the whole time
- Advantages:
  - no dynamic coordination necessary
  - works also for analog signals



- **Disadvantages:**

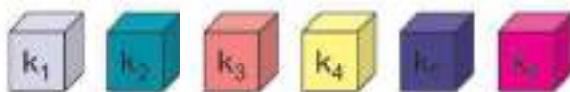
- waste of bandwidth if the traffic is distributed unevenly
- inflexible
- guard spaces



CS 442 WSN U2

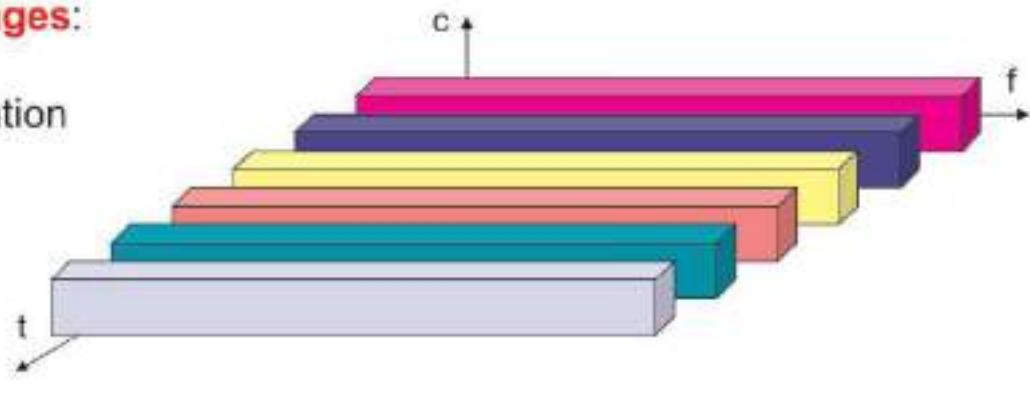
# Time multiplex

- A channel gets the whole spectrum for a certain amount of time
- **Advantages:**
- only one carrier in the medium at any time
- throughput high even for many users



- **Disadvantages:**

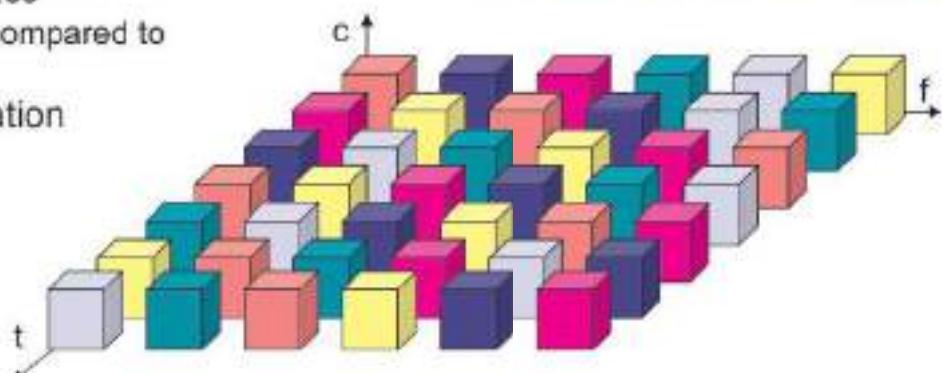
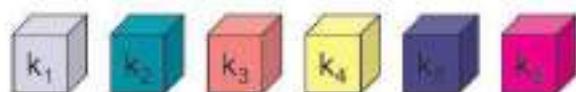
- precise synchronization necessary



CS 442 WSN U2

# Time and frequency multiplex

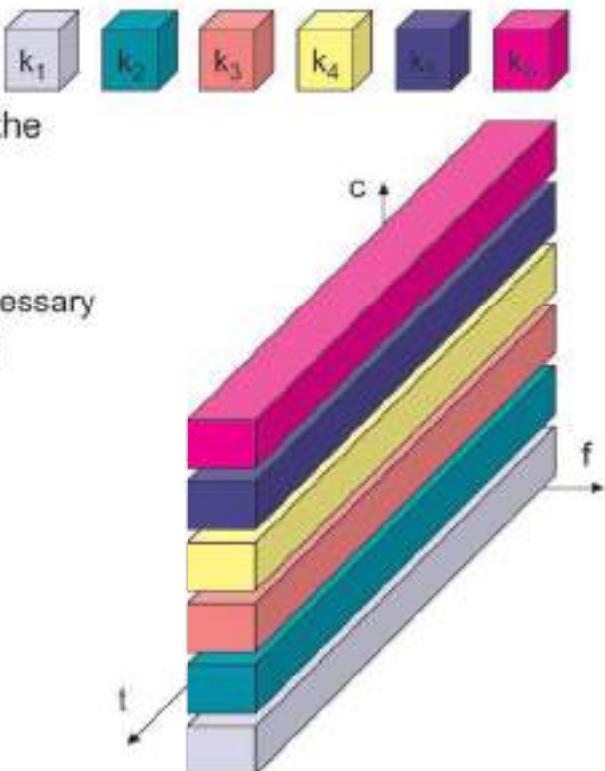
- Combination of both methods
- A channel gets a certain frequency band for a certain amount of time
- Example: GSM
- Advantages:
  - better protection against tapping
  - protection against frequency selective interference
  - higher data rates compared to code multiplex
- but: precise coordination required



CS 442 WSN U2

# Code multiplex

- Each channel has a unique code
- All channels use the same spectrum at the same time
- Advantages:
  - bandwidth efficient
  - no coordination and synchronization necessary
  - good protection against interference and tapping
- Disadvantages:
  - lower user data rates
  - more complex signal regeneration
- Implemented using spread spectrum technology



CS 442 WSN U2

## CDMA Example

- $D$  = rate of data signal
- Break each bit into  $k$  chips
  - Chips are a user-specific fixed pattern
- Chip data rate of new channel =  $kD$
- If  $k=6$  and code is a sequence of 1s and -1s
  - For a '1' bit, A sends code as chip pattern
    - $\langle c_1, c_2, c_3, c_4, c_5, c_6 \rangle$
  - For a '0' bit, A sends complement of code
    - $\langle -c_1, -c_2, -c_3, -c_4, -c_5, -c_6 \rangle$
- Receiver knows sender's code and performs electronic decode function
$$S_u(d) = d_1 \times c_1 + d_2 \times c_2 + d_3 \times c_3 + d_4 \times c_4 + d_5 \times c_5 + d_6 \times c_6$$
  - $\langle d_1, d_2, d_3, d_4, d_5, d_6 \rangle$  = received chip pattern
  - $\langle c_1, c_2, c_3, c_4, c_5, c_6 \rangle$  = sender's code

CS 442 WSN U2

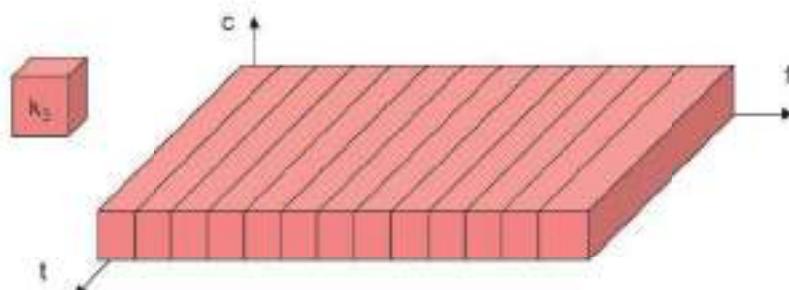
# CDMA Example

- User A code =  $\langle 1, -1, -1, 1, -1, 1 \rangle$ 
  - To send a 1 bit =  $\langle 1, -1, -1, 1, -1, 1 \rangle$
  - To send a 0 bit =  $\langle -1, 1, 1, -1, 1, -1 \rangle$
- User B code =  $\langle 1, 1, -1, -1, 1, 1 \rangle$ 
  - To send a 1 bit =  $\langle 1, 1, -1, -1, 1, 1 \rangle$
- Receiver receiving with A's code
  - (A's code)  $\times$  (received chip pattern)
    - User A '1' bit: 6  $\rightarrow$  1
    - User A '0' bit: -6  $\rightarrow$  0
    - User B '1' bit: 0  $\rightarrow$  unwanted signal ignored

CS 442 WSN U2

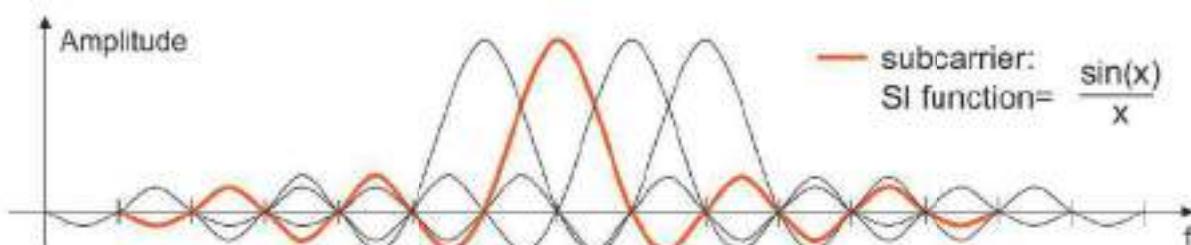
## OFDM (Orthogonal Frequency Division Multiplexing)

- Parallel data transmission on several orthogonal subcarriers with lower rate



Maximum of one subcarrier frequency appears exactly at a frequency where all other subcarriers equal zero

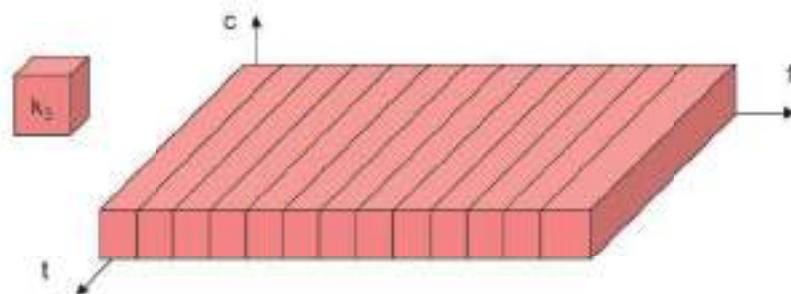
- superposition of frequencies in the same frequency range



CS 442 WSN U2

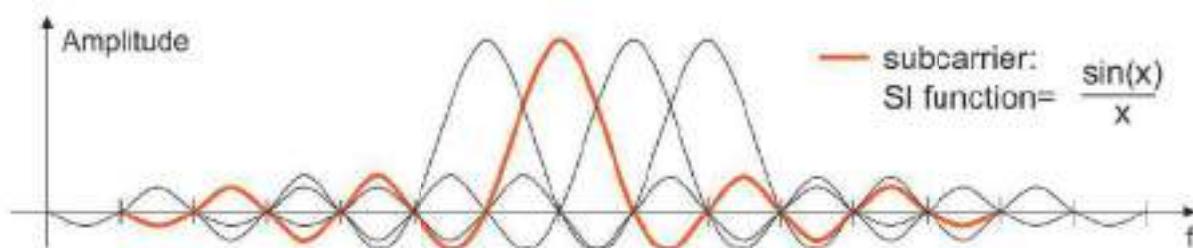
## OFDM (Orthogonal Frequency Division Multiplexing)

- Parallel data transmission on several orthogonal subcarriers with lower rate



Maximum of one subcarrier frequency appears exactly at a frequency where all other subcarriers equal zero

- superposition of frequencies in the same frequency range



CS 442 WSN U2

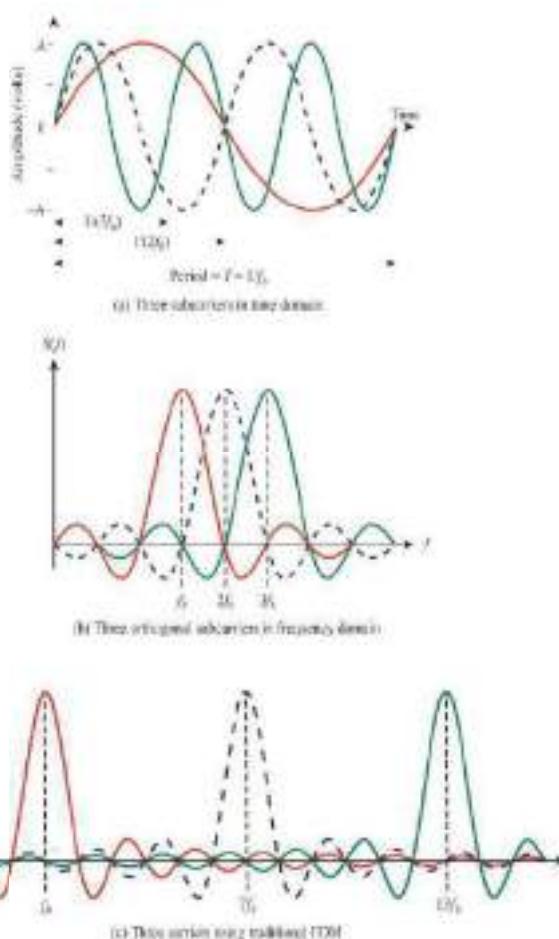
## OFDM

- Also called multicarrier modulation
- Start with a data stream of  $R$  bps
  - Could be sent with bandwidth  $Nf_b$
  - With bit duration  $1/R$
- OFDM splits into  $N$  parallel data streams
  - Called *subcarriers*
  - Each with bandwidth  $f_b$
  - And data rate  $R/N$  (bit time  $N/R$ )

# Orthogonality

- The spacing of the  $f_b$  frequencies allows tight packing of signals
  - Actually with overlap between the signals
  - Signals at spacing of  $f_b, 2f_b, 3f_b$ , etc.
- The choice of  $f_b$  is related to the bit rate to make the signals *orthogonal*
- Traditional FDM makes signals completely avoid frequency overlap
  - OFDM allows overlap which greatly increases capacity

CS-442 WSN L2



# Benefits of OFDM

- Frequency selective fading only affects some subcarriers
- More importantly, OFDM overcomes intersymbol interference (ISI)
  - ISI is caused by multipath signals arriving in later bits
  - OFDM bit times are much, much longer (by a factor of  $N$ )
    - ISI is dramatically reduced
  - OFDM's long bit times eliminate most of the ISI
  - OFDM also uses a *cyclic prefix* (CP) to overcome the residual ISI
    - Adds additional time to the OFDM symbol before the real data is sent
    - Called the *guard interval*
    - ISI diminishes before the data starts

CS-442 WSN I/2

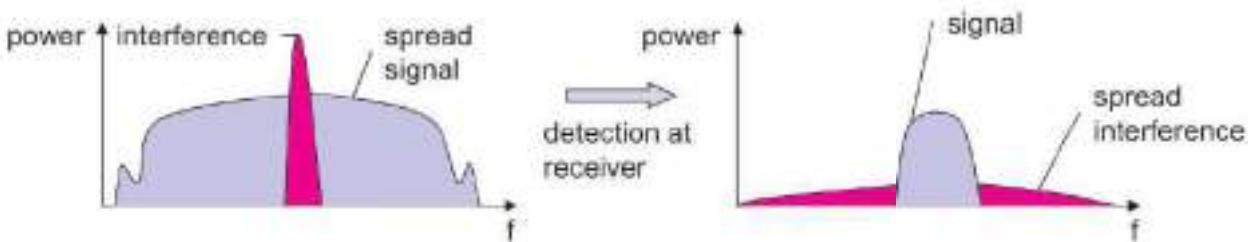
## OFDM applications

- OFDM created great expansion in wireless networks
  - Greater efficiency in bps/Hz
- Main air interface in the change from 3G to 4G
  - Also expanded 802.11 rates
- Critical technology for broadband wireless access
  - WiMAX
- Application
  - 802.11a, HiperLAN2, ADSL

CS-442 WSN I/2

# Spread spectrum

- Problem of radio transmission: frequency dependent fading can wipe out narrow band signals for duration of the interference
- Solution: spread the narrow band signal into a broad band signal using a special code - protection against narrow band interference



- Side effects:
  - coexistence of several signals without dynamic coordination
  - tap-proof
- Alternatives: Direct Sequence (DSSS), Frequency Hopping (FHSS)

CS 442 WSN U2

## Spread Spectrum technique

- Input is fed into a channel encoder
  - Produces analog signal with narrow bandwidth
- Signal is further modulated using sequence of digits
  - Spreading code or spreading sequence
  - Generated by pseudonoise, or pseudo-random number generator
- Effect of modulation is to increase bandwidth of signal to be transmitted

## ...Spread Spectrum technique

- On receiving end, digital sequence is used to demodulate the spread spectrum signal
- Signal is fed into a channel decoder to recover data

CS-442 WSN I/2

## Direct Sequence Spread Spectrum (DSSS)

- Each bit in original signal is represented by multiple bits in the transmitted signal
- Spreading code spreads signal across a wider frequency band
  - Spread is in direct proportion to number of bits used
- One technique combines digital information stream with the spreading code bit stream using exclusive-OR

CS-442 WSN I/2

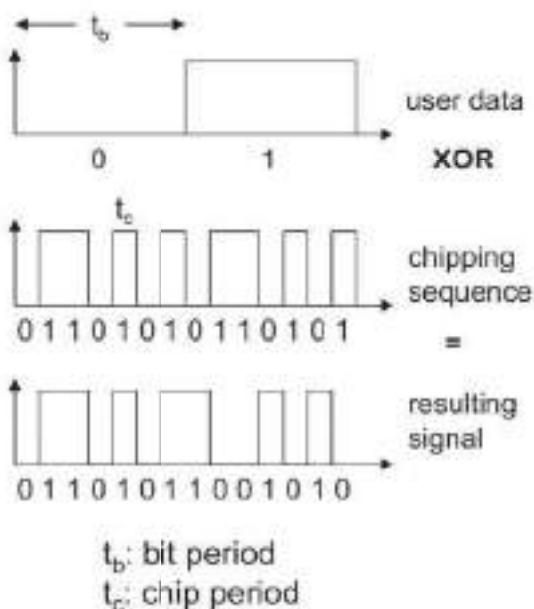
# DSSS : CDMA

- Basic Principles of CDMA
  - $D$  = rate of data signal
  - Break each bit into  $k$  chips
    - Chips are a user-specific fixed pattern
  - Chip data rate of new channel =  $kD$
- Each user encodes with a different spreading code

CS 442 WSN U2

## DSSS (Direct Sequence)

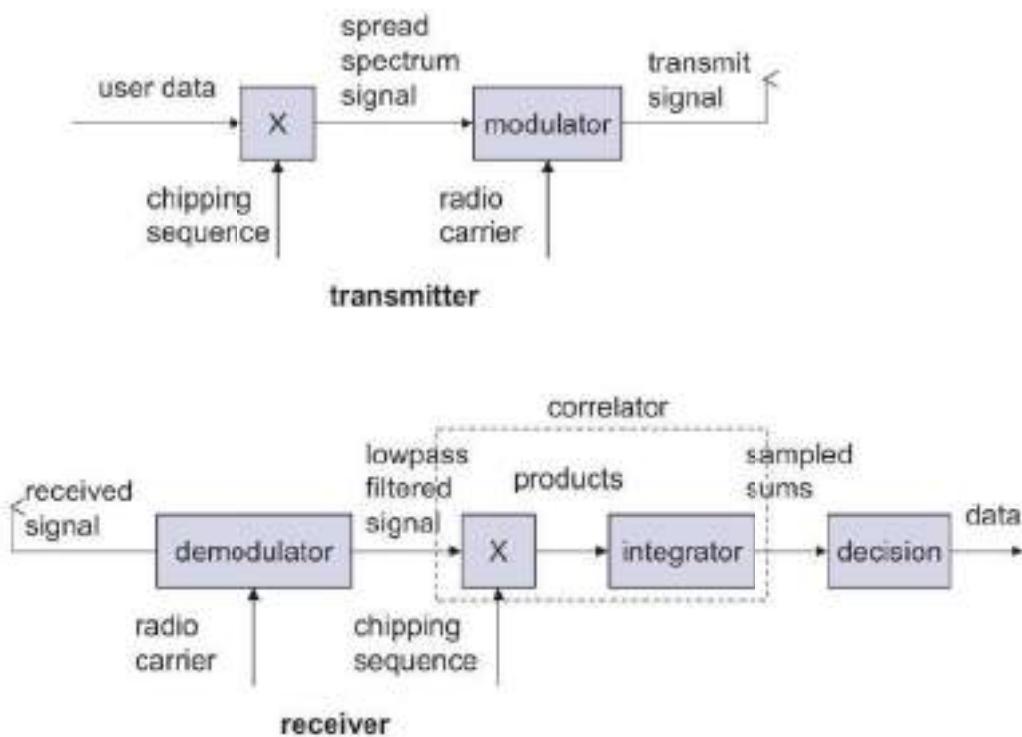
- XOR of the signal with pseudo-random number (chipping sequence)
  - many chips per bit (e.g., 128) result in higher bandwidth of the signal
- Advantages
  - reduces frequency selective fading
- Disadvantages
  - precise power control necessary



$t_b$ : bit period

$t_c$ : chip period

# DSSS Transmit/Receive



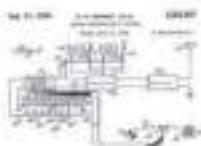
CS 442 WSN U2



CS 442 WSN U2

### The Mother Of Wireless Technology

Hedy Lamarr was more than a pretty face in Hollywood. Learn how this actress bucked convention and shaped our modern technology through her invention.



**INVENTION:**  
Frequency Hopping  
Spread Spectrum



**LEGACY:**  
WiFi, GPS, And Bluetooth



**HONORS:**

National Inventors Hall  
Of Fame Inductee 2014



CS 442 WSN U2

## Frequency hopping communication invented by actress Hedy Lamar

UNITED STATES PATENT OFFICE

2,292,287

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.

Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

This invention relates broadly to secret communication systems involving the use of carrier waves of different frequencies, and is especially useful in the remote control of dirigible craft.

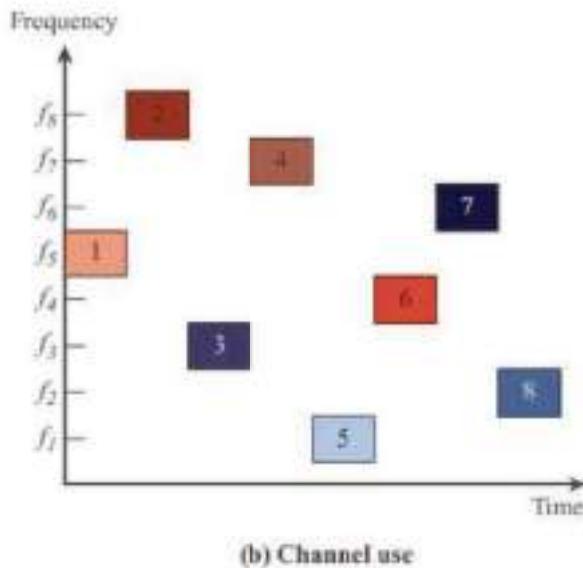
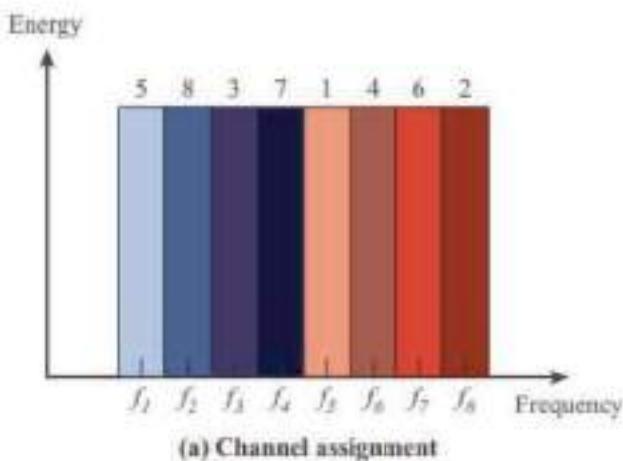
Fig. 2 is a schematic diagram of the apparatus at a receiving station;

Fig. 3 is a schematic diagram illustrating a starting circuit for starting the motors at the

# Frequency Hopping Spread Spectrum (FHSS)

- Signal is broadcast over seemingly random series of radio frequencies
- Signal hops from frequency to frequency at fixed intervals
- Channel sequence dictated by spreading code
- Receiver, hopping between frequencies in synchronization with transmitter, picks up message
- Advantages
  - Eavesdroppers hear only unintelligible blips
  - Attempts to jam signal on one frequency succeed only at knocking out a few bits

CS 442 WSN U2



Frequency Hopping Example

# Frequency Hoping Spread Spectrum (FHSS)

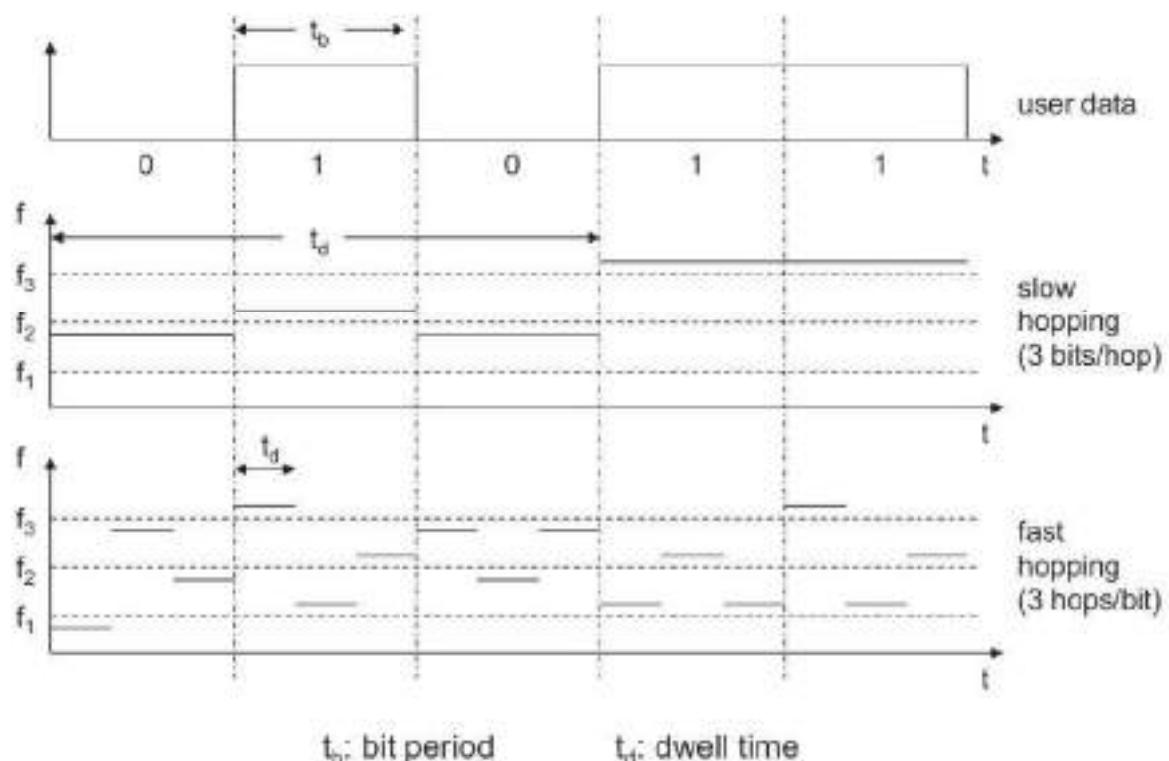
- Signal is broadcast over seemingly random series of radio frequencies
  - A number of channels allocated for the FH signal
  - Width of each channel corresponds to bandwidth of input signal
- Signal hops from frequency to frequency at fixed intervals
  - Transmitter operates in one channel at a time
  - Bits are transmitted using some encoding scheme
  - At each successive interval, a new carrier frequency is selected

CS 442 WSN U2

## Frequency Hopping

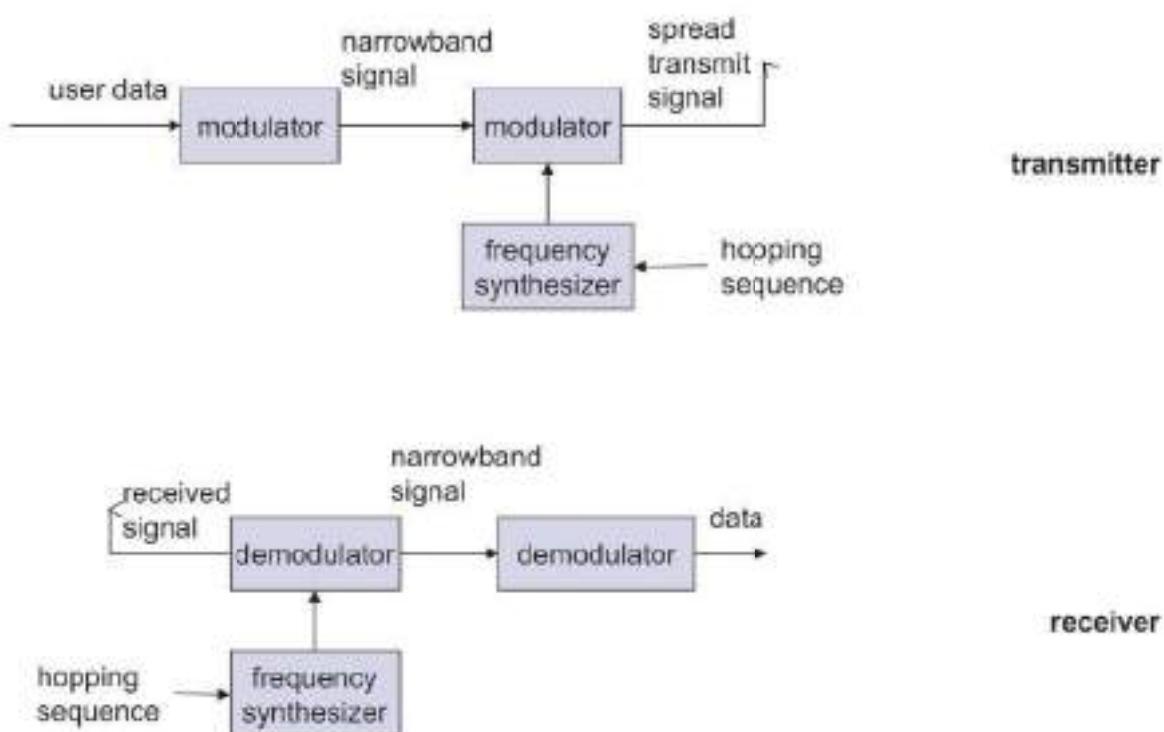
- Discrete changes of carrier frequency
  - sequence of frequency changes determined via pseudo random number sequence
- Two versions
  - Fast Hopping: several frequencies per user bit
  - Slow Hopping: several user bits per frequency
- Advantages
  - frequency selective fading and interference limited to short period
  - simple implementation
  - uses only small portion of spectrum at any time
- Disadvantages
  - not as robust as DSSS
  - simpler to detect

# Slow and Fast FHSS



CS 442 WSN U2

## FHSS Transmit/Receive



CS 442 WSN U2

# Channel correction Mechanisms

- Forward error correction (we see now)
- Adaptive equalization (We'll see shortly)
- Adaptive modulation and coding (We'll see shortly)
- Diversity techniques and MIMO (We'll see shortly)
- OFDM (We have seen)
- Spread spectrum techniques (We have seen)
- Bandwidth expansion (We'll see shortly)

# **CS 442**

# **Wireless Sensor Network**

## **Unit 3**

CS 442 WSN Unit-3

### **Unit 3:**

Low power PAN, LAN Standards, IEEE 802.11, 802.15, 802.15.4 and Zigbee.

## **Unit 3**

## **WLAN, WPAN standards**

# IEEE 802 Standards Working Groups

Number	Topic
★ 802.1	Overview and architecture of LANs
★ 802.2 ↓	Logical link control
★ 802.3 *	Ethernet
★ 802.4 ↓	Token bus (was briefly used in manufacturing plants)
★ 802.5	Token ring (IBM's entry into the LAN world)
★ 802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 ↑	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
★ ★ 802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
★ 802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

★ You have studied in Computer Network Course

★ We study in this course

## Interfaces, Protocols, Standards

- ▶ Interface
- ▶ Protocol
- ▶ Standards

# IEEE 802.11

CS 442 WSN Unit-3

## Wireless Local Area Networks

- The proliferation of laptop computers and other mobile devices (PDAs and cell phones) created an *obvious* application level demand for wireless local area networking.
- Companies jumped in, quickly developing *incompatible* wireless products in the 1990's.
- Industry decided to entrust standardization to IEEE committee that dealt with wired LANS – *namely, the IEEE 802 committee!!*

# Categories of Wireless Networks

- **Base Station** :: all communication through an **access point** {note hub topology}. Other nodes can be fixed or mobile.
- **Infrastructure Wireless** :: base station network is connected to the wired Internet.
- **Ad hoc Wireless** :: wireless nodes communicate directly with one another.
- **MANETs (Mobile Ad Hoc Networks)** :: ad hoc nodes are mobile.

7

## Wireless LANs

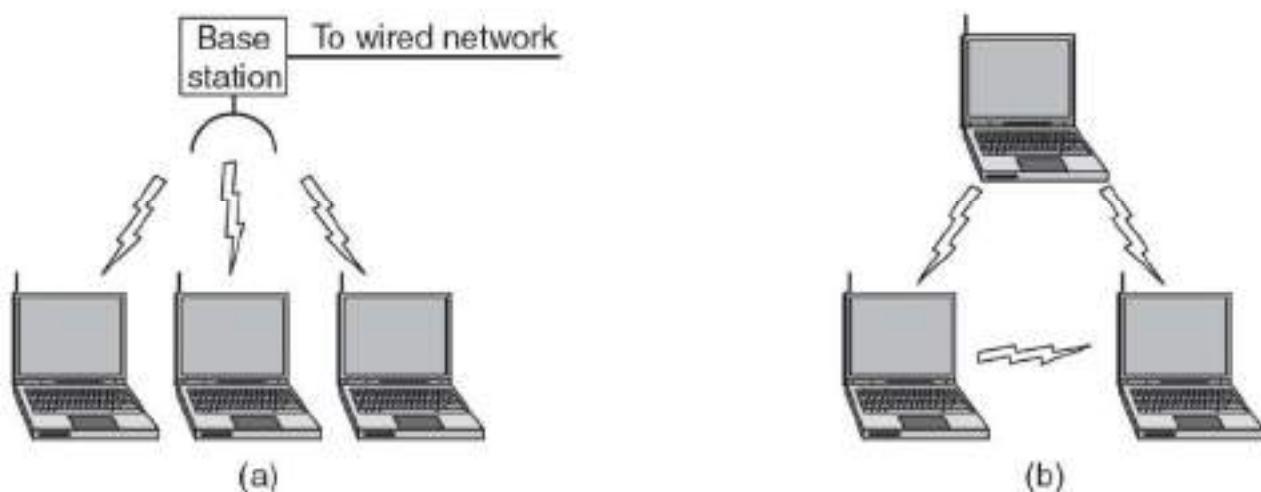
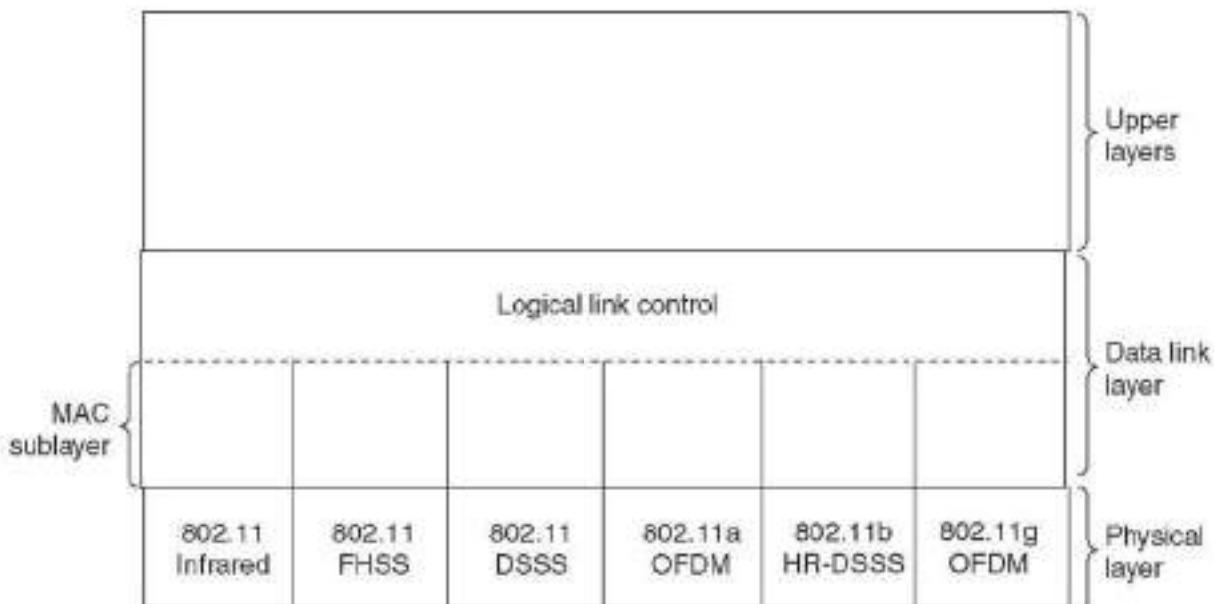


Figure 1-36.(a) Wireless networking with a base station. (b) Ad hoc networking.

8

# The 802.11 Protocol Stack



Part of the 802.11 protocol stack.

9

## 802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management
- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions

DLC	LLC	
PHY	MAC	MAC Management
	PLCP	PHY Management
	PMD	

Station Management

10

# The 802.11 Protocol Architecture

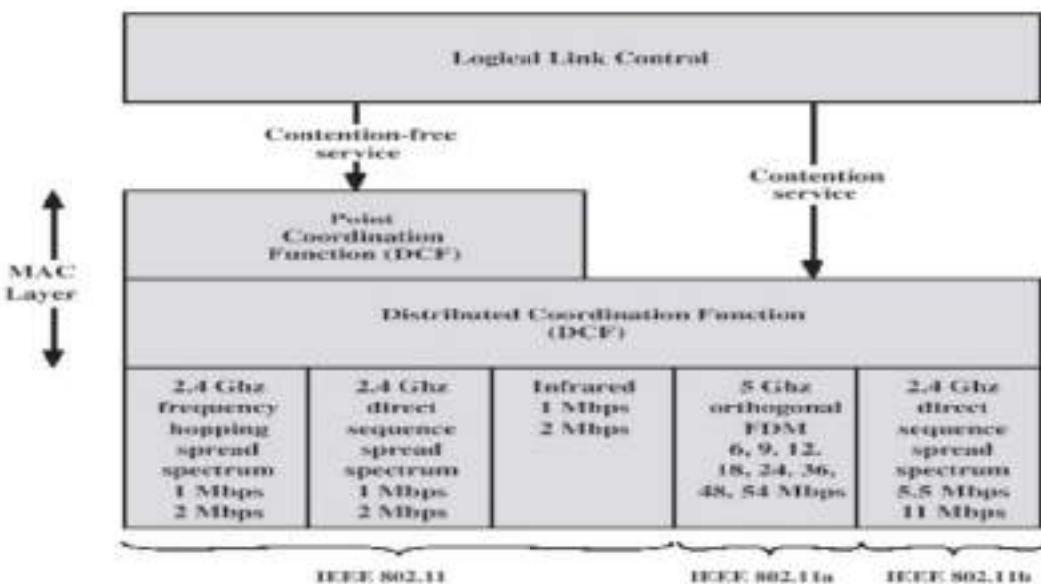
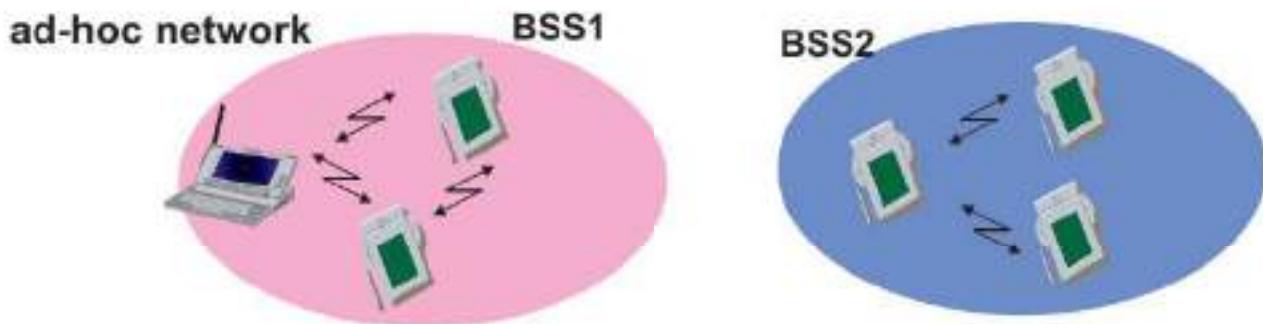


Figure 14.5 IEEE 802.11 Protocol Architecture

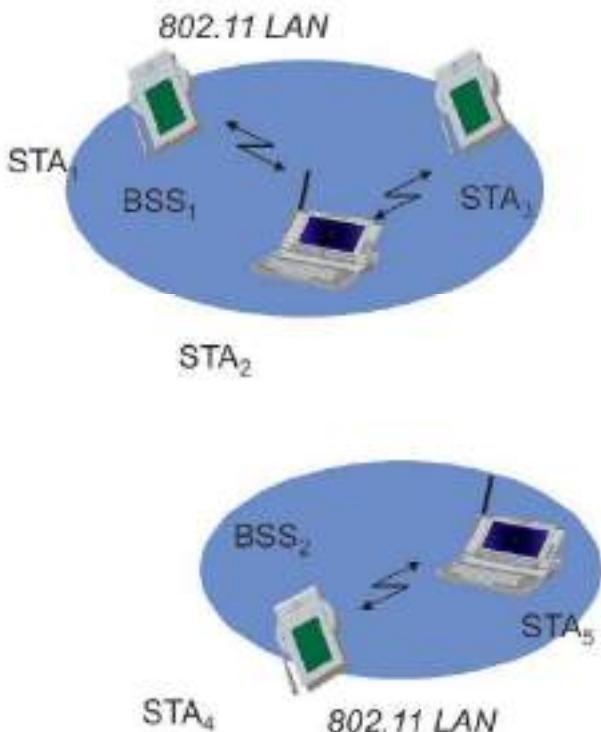
11

## Components of IEEE 802.11 architecture

- The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN
- The ovals can be thought of as the coverage area within which member stations can directly communicate
- The Independent BSS (IBSS) is the simplest LAN. It may consist of as few as two stations



# 802.11 - ad-hoc network (DCF)

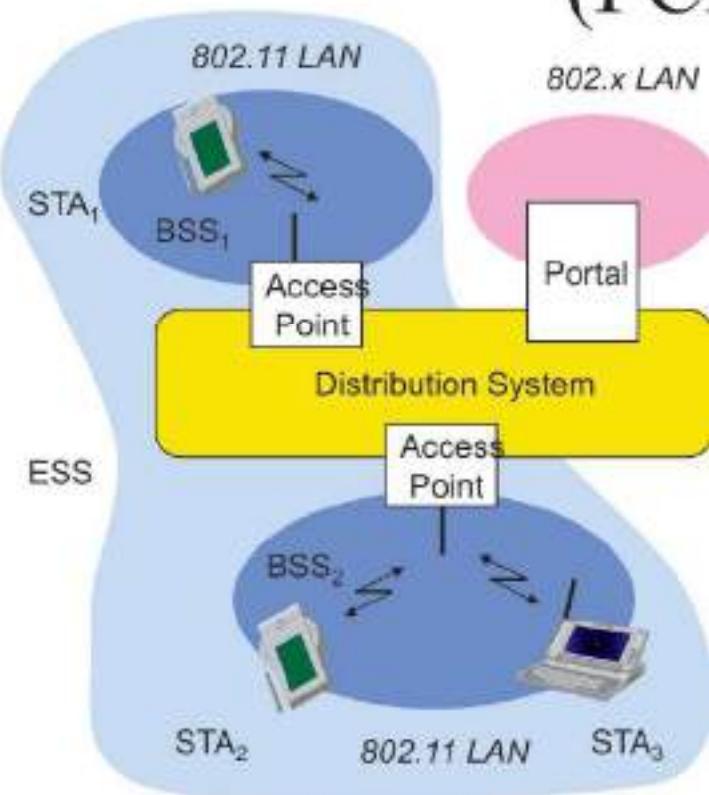


- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS): group of stations using the same radio frequency

13

# 802.11 - infrastructure network

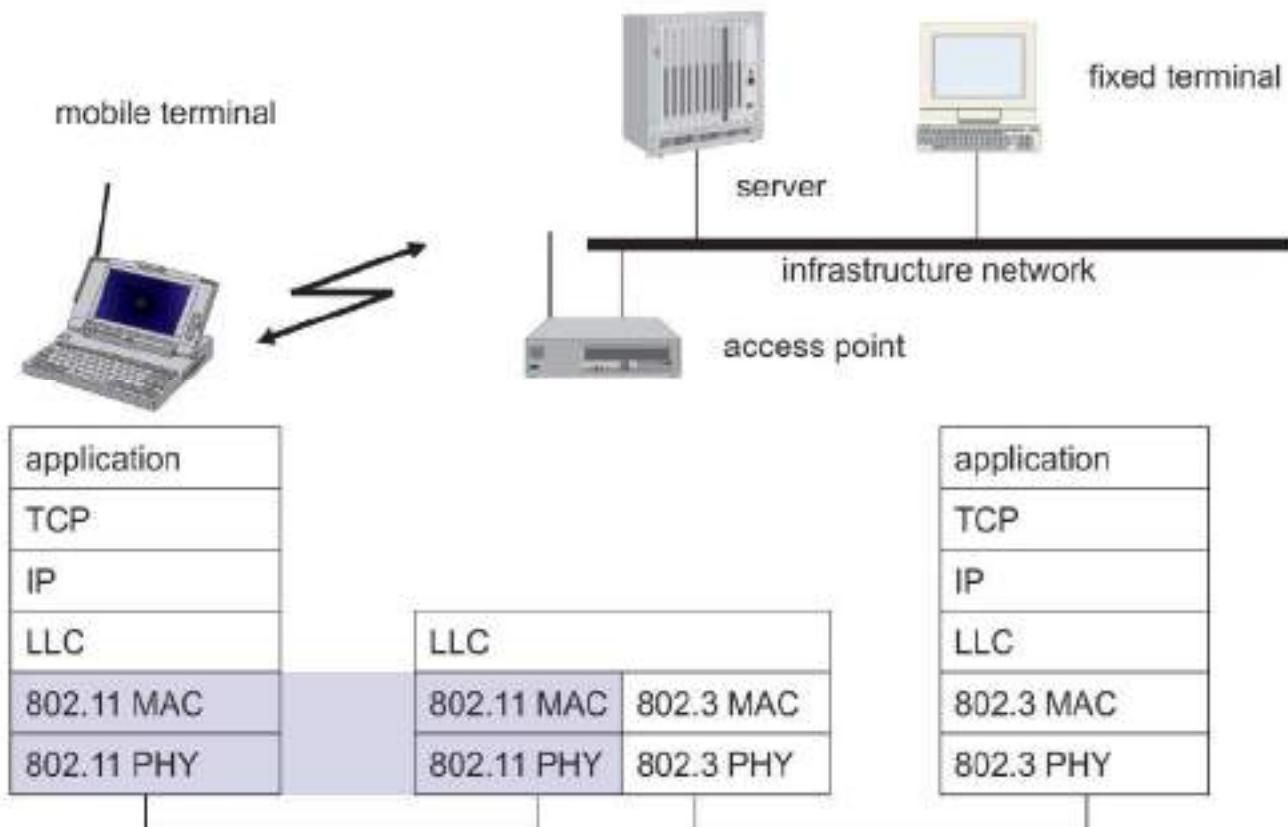
## (PCF)



- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

14

# 802.11- in the TCP/IP stack



## 802.11 Physical Layer

- Physical layer conforms to OSI (five options)
  - 1997: **802.11** infrared, FHSS, DHSS
  - 1999: **802.11a** OFDM and **802.11b** HR-DSSS
  - 2001: **802.11g** OFDM
- 802.11 Infrared**
  - Two capacities 1 Mbps or 2 Mbps.
  - Cannot penetrate walls.
- 802.11 FHSS (Frequency Hopping Spread Spectrum)**
  - 79 channels, each 1 MHz wide at low end of 2.4 GHz ISM band.
  - Same pseudo-random number generator used by all stations.
  - Dwell time: min. time on channel before hopping (400 msec).

# 802.11 Physical Layer

- **802.11 DSSS (Direct Sequence Spread Spectrum)**
  - Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA see Tanenbaum sec. 2.6.2).
  - Each bit transmitted as 11 chips (Barker seq.), PSK at 1Mbaud.
  - 1 or 2 Mbps.
- **802.11a OFDM (Orthogonal Frequency Divisional Multiplexing)**
  - Compatible with European HiperLan2.
  - 54Mbps in wider 5.5 GHz band → transmission range is limited.
  - Uses 52 FDM channels (48 for data; 4 for synchronization).
  - Encoding is complex ( PSM up to 18 Mbps and QAM above this capacity).
  - E.g., at 54Mbps 216 data bits encoded into into 288-bit symbols.
  - More difficulty penetrating walls.

17

# 802.11 Physical Layer

- **802.11b HR-DSSS (High Rate Direct Sequence Spread Spectrum)**
  - **11a and 11b shows a split in the standards committee.**
  - **11b** approved and hit the market before **11a**.
  - Up to 11 Mbps in 2.4 GHz band using 11 million chips/sec.
  - Note in this bandwidth all these protocols have to deal with interference from microwave ovens, cordless phones and garage door openers.
  - Range is 7 times greater than **11a**.
  - **11b and 11a are incompatible!!**

18

## 802.11 Physical Layer

- **802.11g OFDM(Orthogonal Frequency Division Multiplexing)**
  - Supports 54 Mbps.
  - Uses 2.4 GHz frequency for greater range.

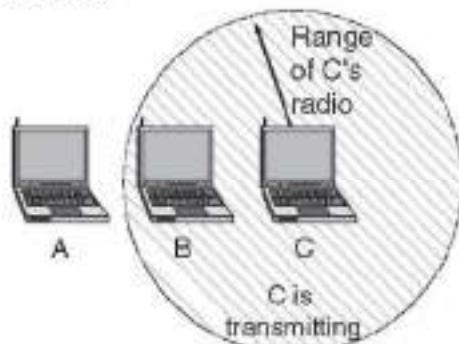
19

## 802.11 MAC Sublayer Protocol

- In 802.11 wireless LANs, “seizing channel” does not exist as in 802.3 wired Ethernet.
- Two additional problems:
  - Hidden Terminal Problem
  - Exposed Station Problem
- To deal with these two problems 802.11 supports two modes of operation **DCF (Distributed Coordination Function)** and **PCF (Point Coordination Function)**.
- **All implementations must support DCF, but PCF is optional.**

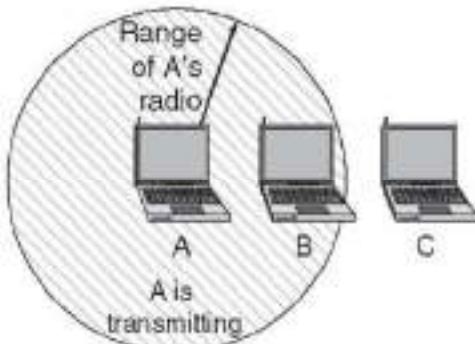
20

A wants to send to B  
but cannot hear that  
B is busy



(a)

B wants to send to C  
but mistakenly thinks  
the transmission will fail



(b)

(a) The hidden station problem. (b) The exposed station problem.

## The Hidden Terminal Problem

- Wireless stations have transmission ranges and not all stations are within radio range of each other.
- Simple CSMA will not work!
- C transmits to B.
- If A “*senses*” the channel, it will not hear C’s transmission and falsely conclude that A can begin a transmission to B.

# The Exposed Station Problem

- The inverse problem.
- B wants to send to C and listens to the channel.
- When B hears A's transmission, B falsely assumes that it cannot send to C.

## The Hidden Terminal Problem

- Wireless stations have transmission ranges and not all stations are within radio range of each other.
- Simple CSMA will not work!
- C transmits to B.
- If A “*senses*” the channel, it will not hear C’s transmission and falsely conclude that A can begin a transmission to B.

22

## The Exposed Station Problem

- The inverse problem.
- B wants to send to C and listens to the channel.
- When B hears A’s transmission, B falsely assumes that it cannot send to C.

23

## Distribute Coordination Function (DCF)

- Uses CSMA/ CA (CSMA with Collision Avoidance).
  - Uses both physical and *virtual* carrier sensing.
  - Two methods are supported:
    1. **based on MACAW with virtual carrier sensing**
    2. **1-persistent physical carrier sensing.**

24

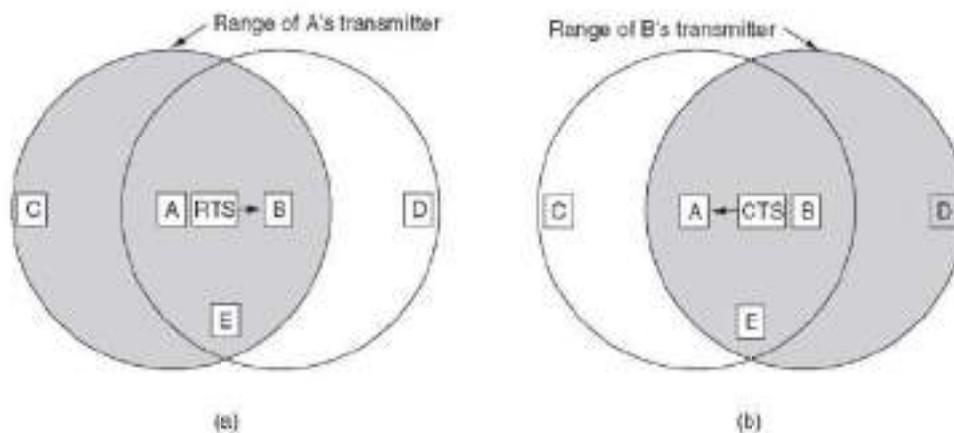
## Wireless LAN Protocols

- MACA protocol solved hidden, exposed terminal:
  - Send Ready-to-Send (*RTS*) and Clear-to-Send (*CTS*) first
  - RTS, CTS helps determine who else is in range or busy (Collision avoidance).
  - Can a collision still occur?

25

# Wireless LAN Protocols

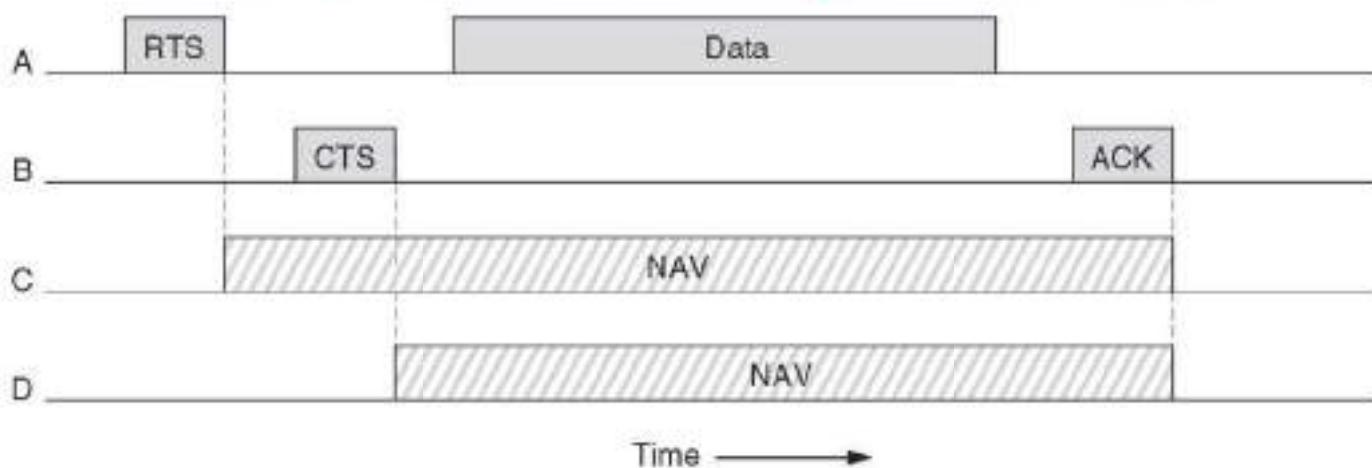
- MACAW added ACKs and CSMA (no RTS at same time)



(a) A sending an RTS to B.(b) B responding with a CTS to A.

26

## Virtual Channel Sensing in CSMA/CA

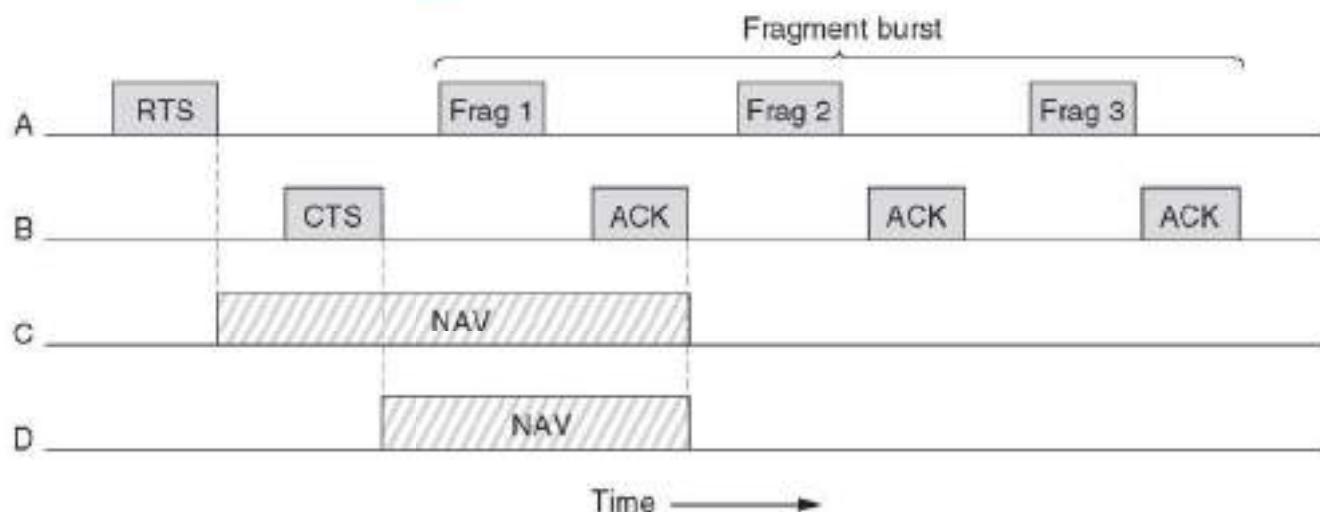


The use of virtual channel sensing using CSMA/CA.

- C (in range of A) receives the RTS and based on information in RTS creates a **virtual channel busy NAV**.
- D (in range of B) receives the CTS and creates a shorter NAV.

27

# Fragmentation in 802.11



- High wireless error rates → long packets have less probability of being successfully transmitted.
- Solution: MAC layer fragmentation with stop-and-wait protocol on the fragments.

28

## 1-Persistent Physical Carrier Sensing

- Station *senses* the channel when it wants to send.
- If idle, station transmits.
  - *Station does not sense channel while transmitting.*
- If the channel is busy, station defers until idle and then transmits.
- Upon collision, wait a *random time* using binary exponential backoff.

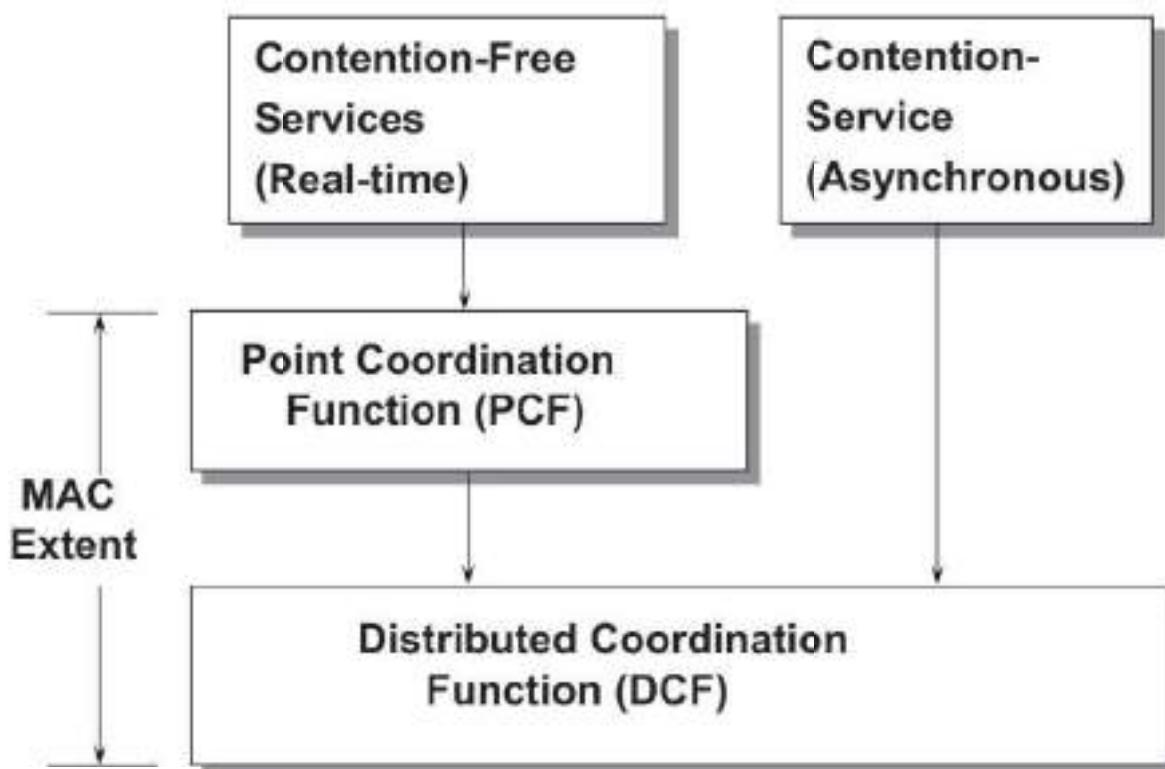
29

# Point Coordinated Function (PCF)

- PCF uses a base station to poll other stations to see if they have frames to send.
- No collisions occur.
- Base station sends ***beacon frame*** periodically.
- Base station can tell another station to ***sleep*** to save on batteries and base stations holds frames for sleeping station.

30

## 802.11 MAC Architecture

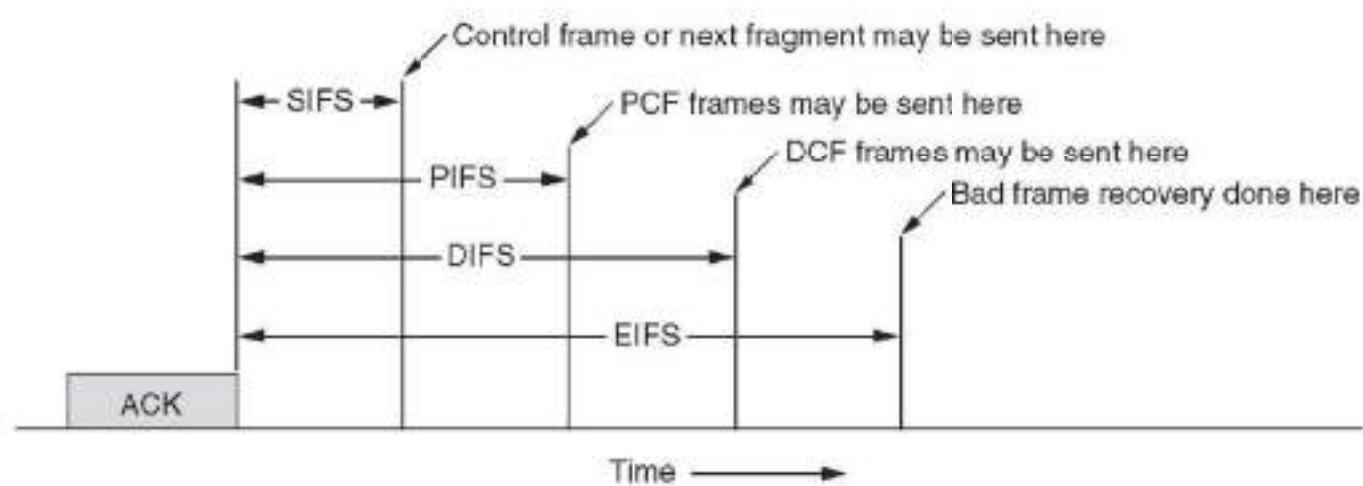


# DCF and PCF Co-Existence

- Distributed and centralized control can co-exist using InterFrame Spacing.
- SIFS (Short IFS) :: is the time waited between packets in an ongoing dialog (RTS,CTS,data, ACK, next frame)
- PIFS (PCF IFS) :: when no SIFS response, base station can issue beacon or poll.
- DIFS (DCF IFS) :: when no PIFS, any station can attempt to acquire the channel.
- EIFS (Extended IFS) :: lowest priority interval used to report bad or unknown frame.

32

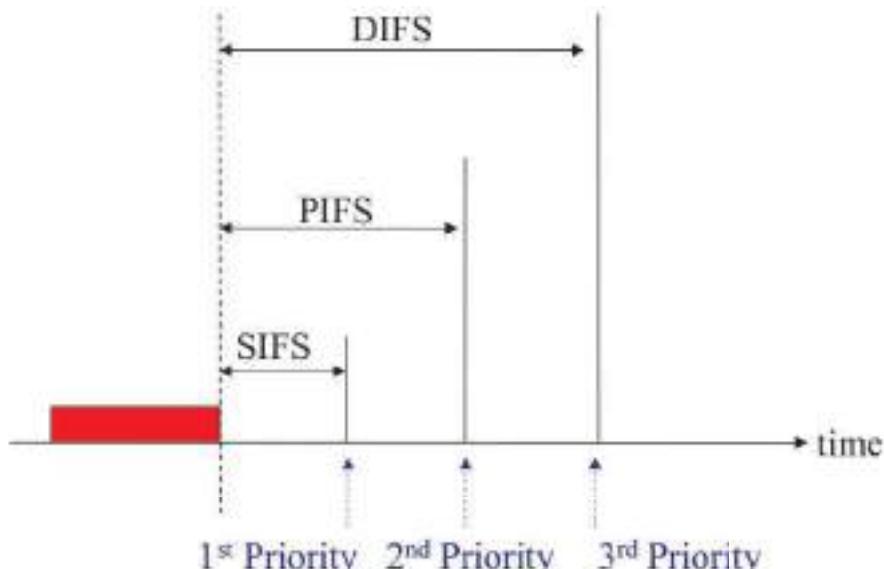
## Interframe Spacing in 802.11.



33

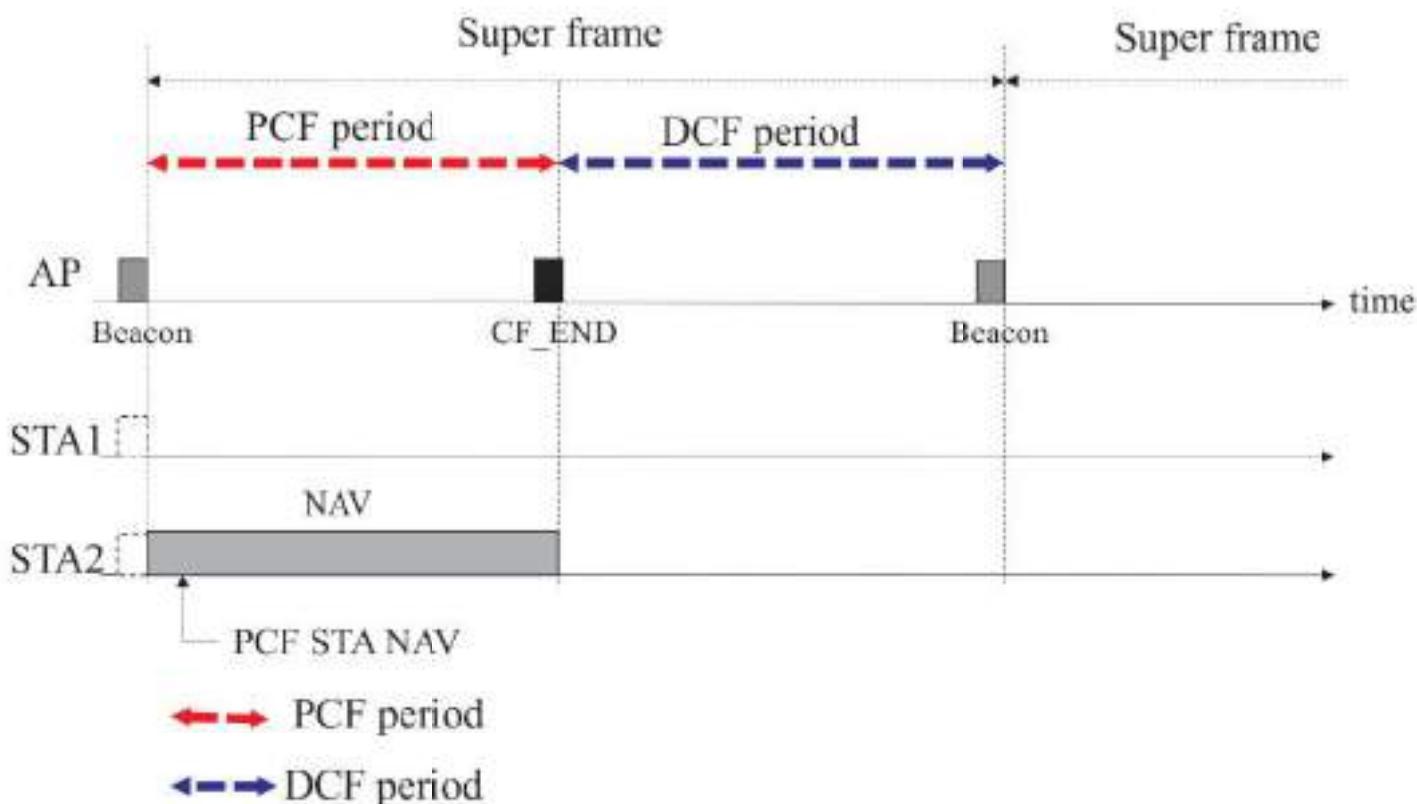
# Priority Scheme : DSSS example

- Goal : Let each frame has different priority
  - SIFS → PIFS → DIFS → EIFS
  - 802.11 DSSS – SIFS(10μs), PIFS(30μs), DIFS(50μs), EIFS(>50μs)



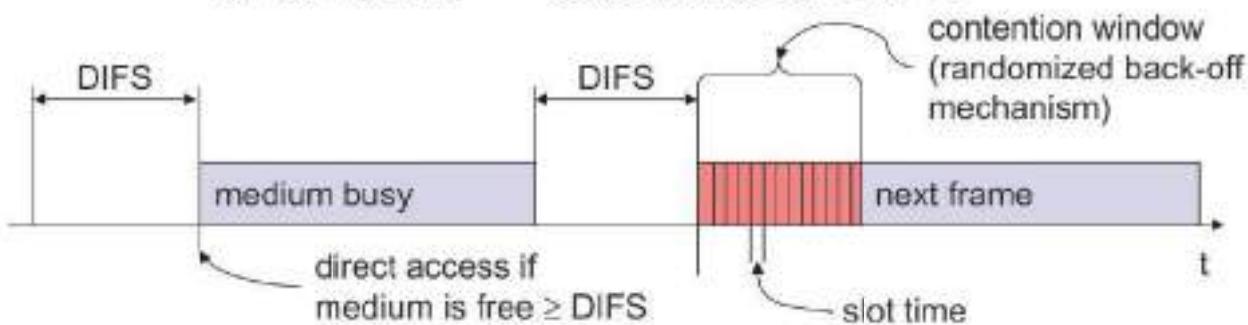
34

## 802.11 Superframe



35

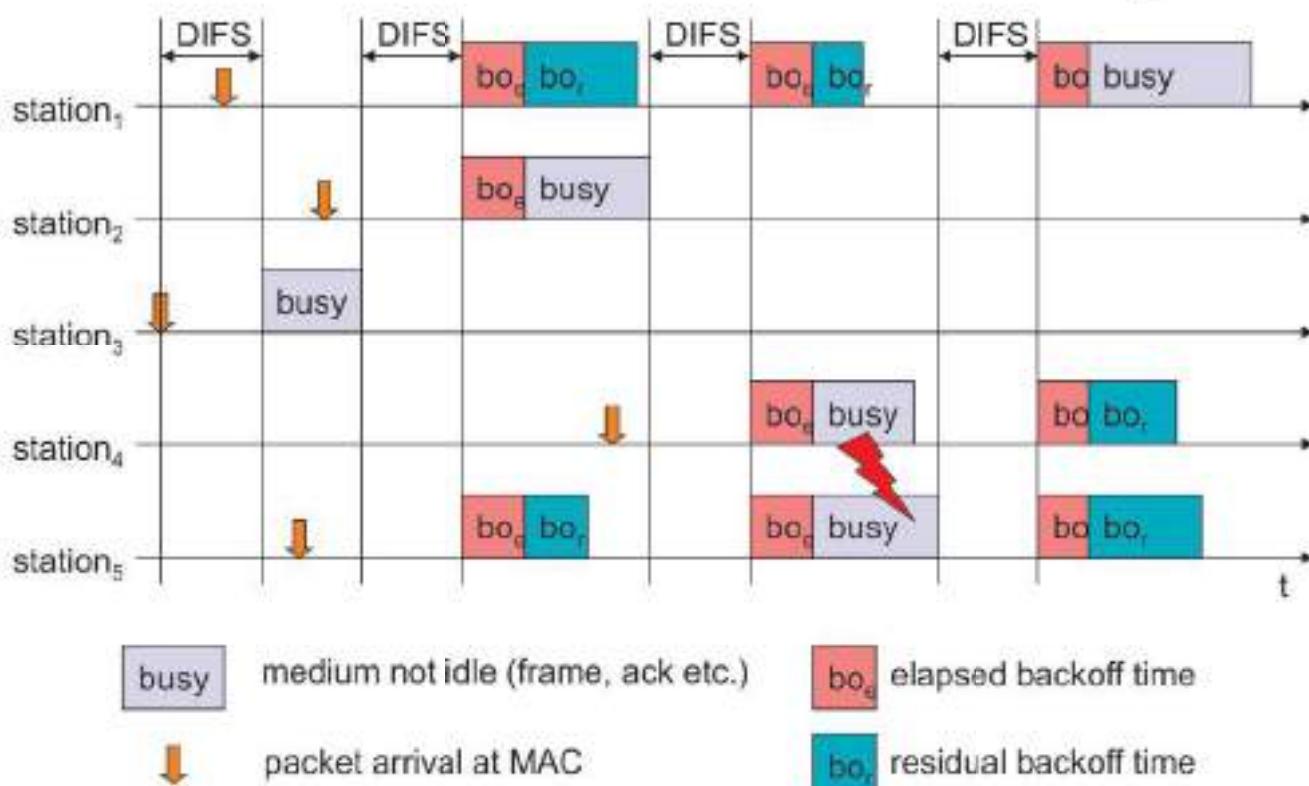
# 802.11 - CSMA/CA



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

36

## 802.11 –CSMA/CA example

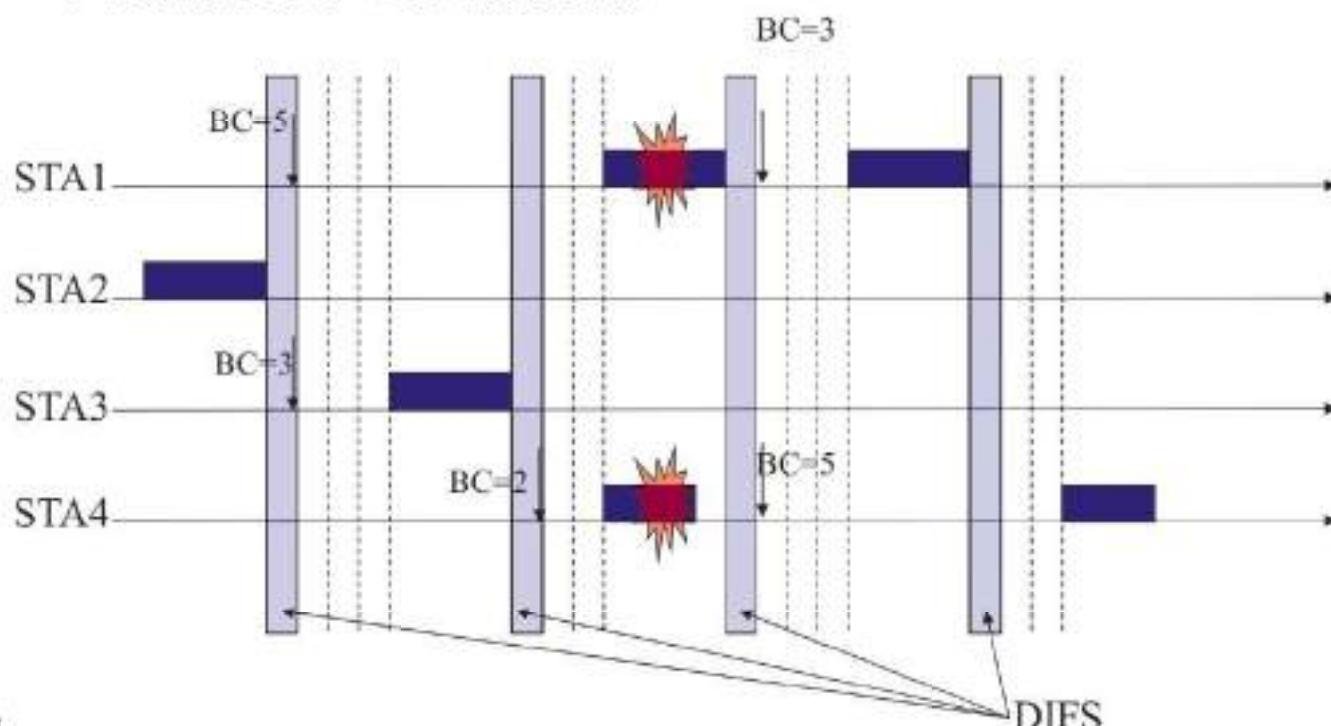


37

# Random backoff

## ➤ Backoff Counter :

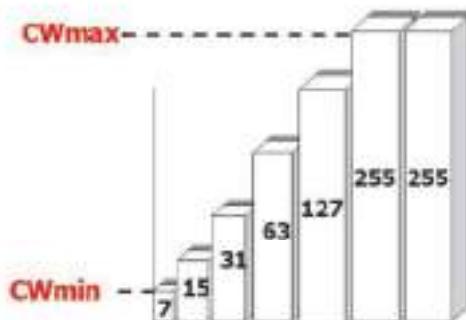
- when network busy → B.C. freeze
- network idle → B.C. decrease



38

## DCF: the Random Backoff Time

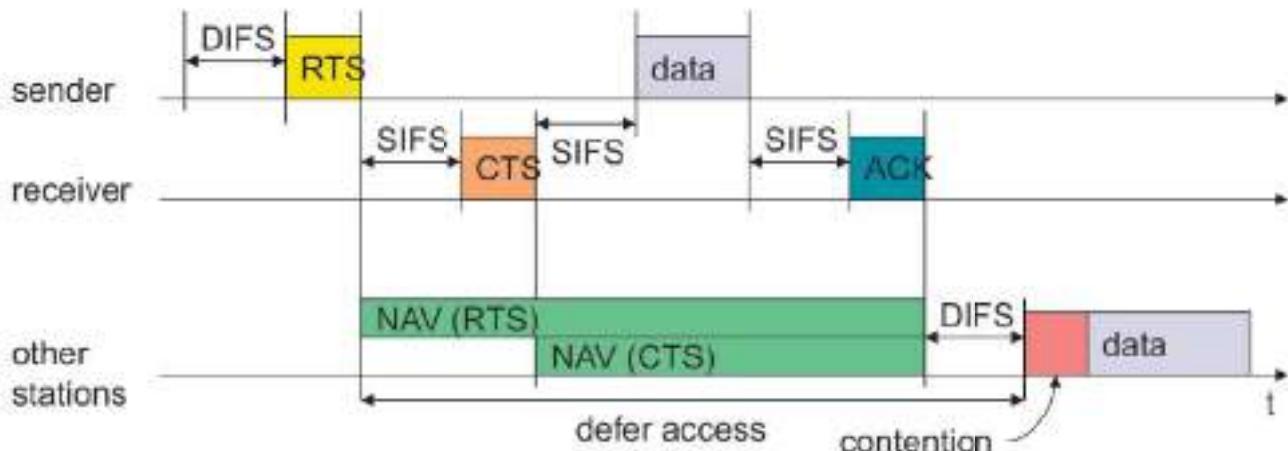
- Backoff time = CW\* Random() \* Slot time
- CW = starts at **CWmin** and doubles after each failure until reaching **CWmax** and remains there in all remaining retries
  - ✓ e.g., CWmin = 7, CWmax = 255
- Random() = (0,1)
- Slot Time = Transmitter turn-on delay +  
medium propagation delay +  
medium busy detect response time



39

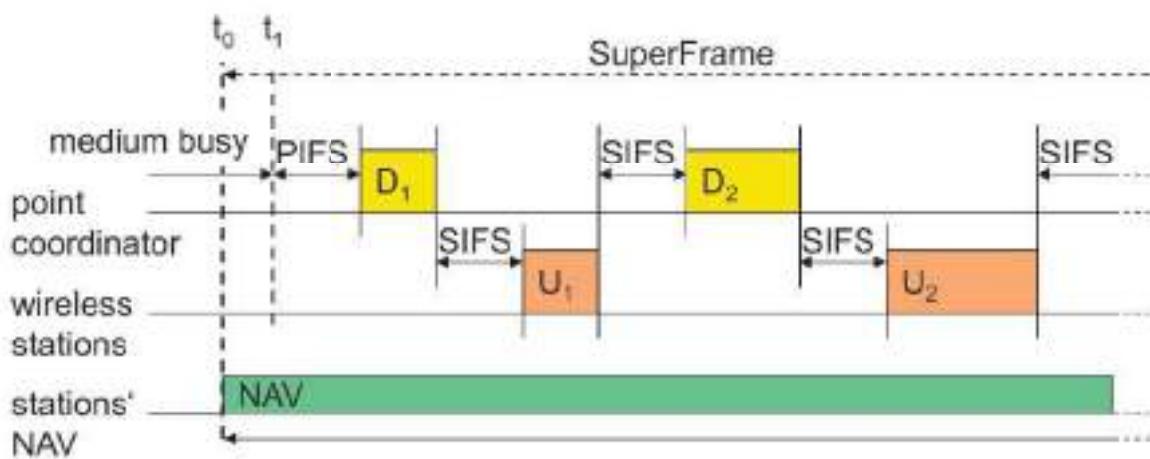
# 802.11 –RTS/CTS

- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



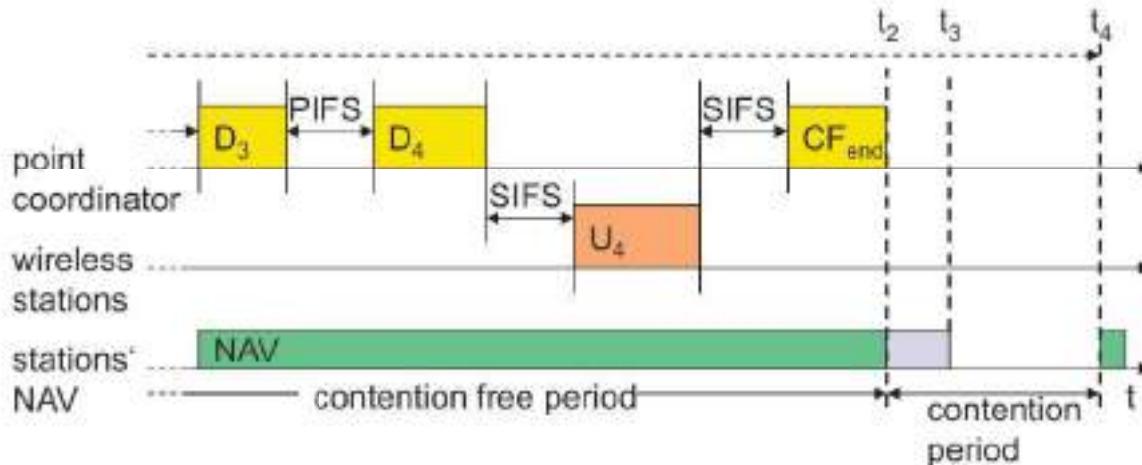
40

# 802.11 - PCF I



41

# 802.11 - PCF II



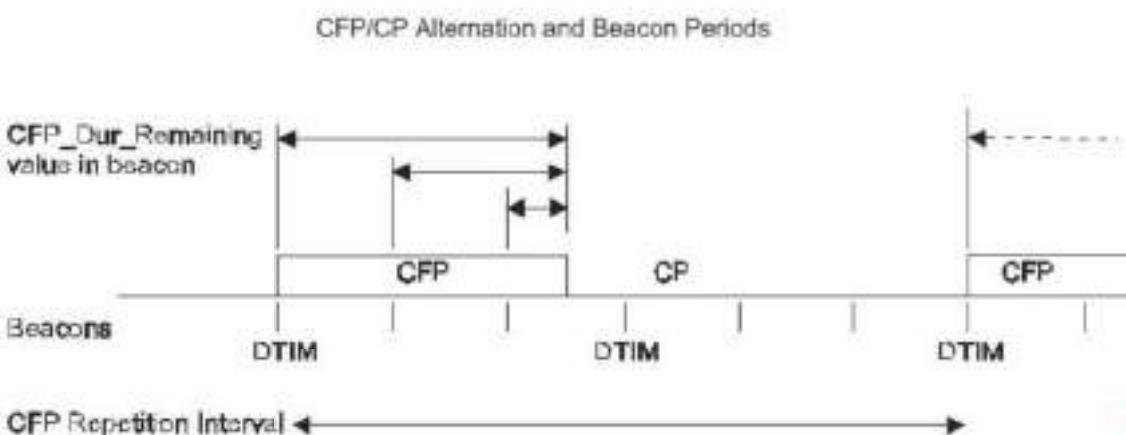
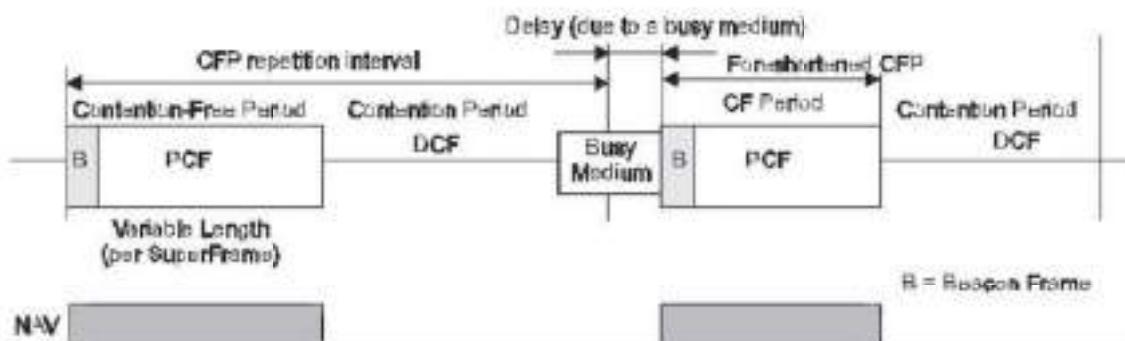
42

## 802.11 - MAC layer contd.

- **Traffic services**
  - Asynchronous Data Service (mandatory) – DCF
  - Time-Bounded Service (optional) - PCF
- **Access methods**
  - **DCF CSMA/CA (mandatory)**
    - collision avoidance via randomized back-off mechanism
    - ACK packet for acknowledgements (not for broadcasts)
  - **DCF w/ RTS/CTS (optional)**
    - avoids hidden terminal problem
  - **PCF (optional)**
    - access point polls terminals according to a list

43

# CFP structure and Timing



## 802.11 - MAC management

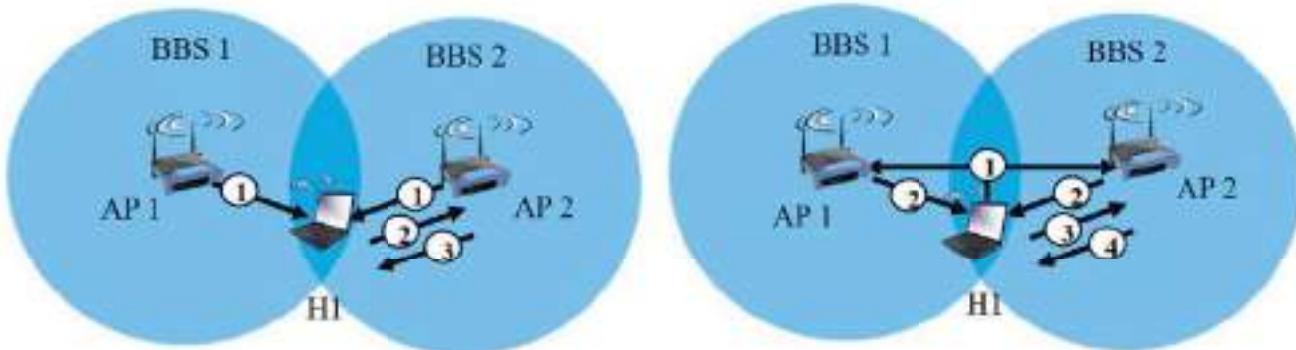
- **Synchronization**
  - try to find a LAN, try to stay within a LAN
  - timer etc.
- **Power management**
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- **Association/Reassociation**
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- **MIB - Management Information Base**
  - managing, read, write

# 802.11 - Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- **Host: must associate with an AP**
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

46

## 802.11 – Passive / Active scanning



### passive scanning:

- (1) beacon frames sent from APs
- (2) association Request frame sent: H1 to selected AP
- (3) association Response frame sent from selected AP to H1

### active scanning:

- (1) Probe Request frame broadcast from H1
- (2) Probe Response frames sent from APs
- (3) Association Request frame sent: H1 to selected AP
- (4) Association Response frame sent from selected AP to H1

47

# Power management

- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
- Infrastructure
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP
- Ad hoc
  - Ad hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP
    - collision of ATIMs possible (scalability?)

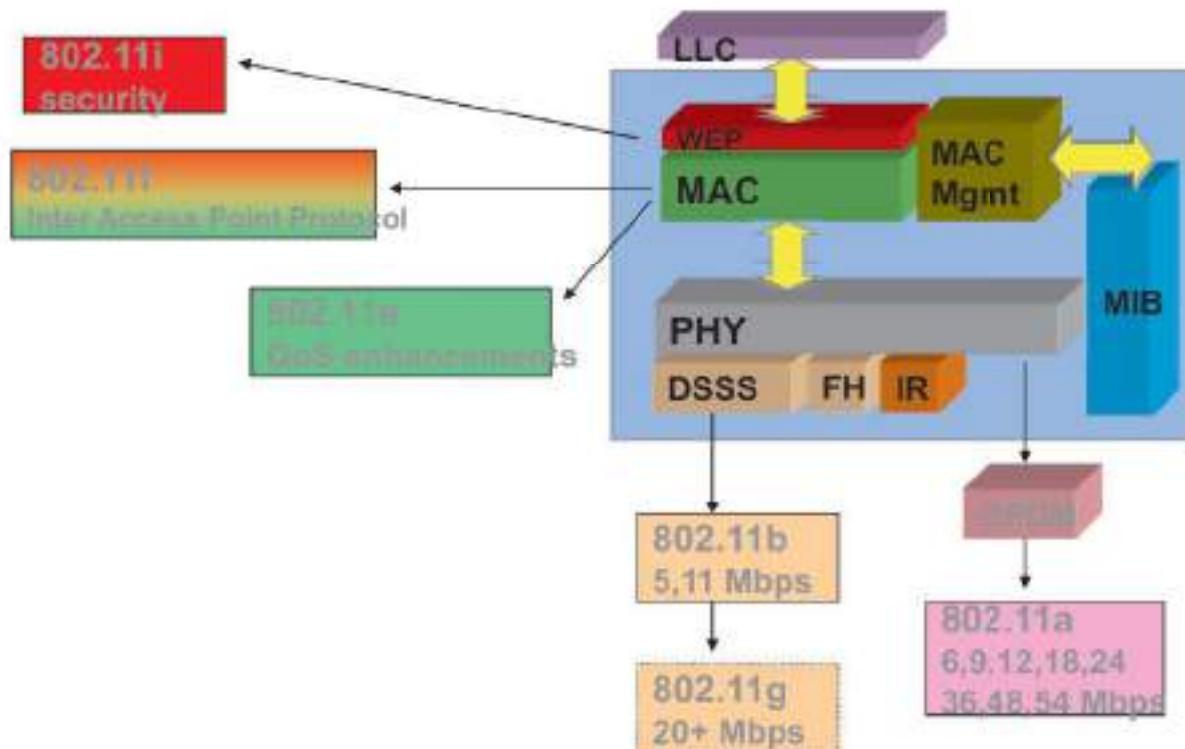
48

# 802.11 - Roaming

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals (passive) or send probes (active) into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources

49

# 802.11 variants



50

## IEEE 802.11abgn

- IEEE 802.11a
  - Makes use of 5-GHz band
  - Provides rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps
  - Uses orthogonal frequency division multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
  - Provides data rates of 5.5 and 11 Mbps
  - Complementary code keying (CCK) modulation scheme
- IEEE 802.11g
  - Mix of a & b on 2.4Ghz
- IEEE 802.11n
  - Multiple Input Multiple Output
- Higher rates are not achieved for free
  - There are assumptions about range, channel, power

51

# IEEE 802.11

## Packet formats

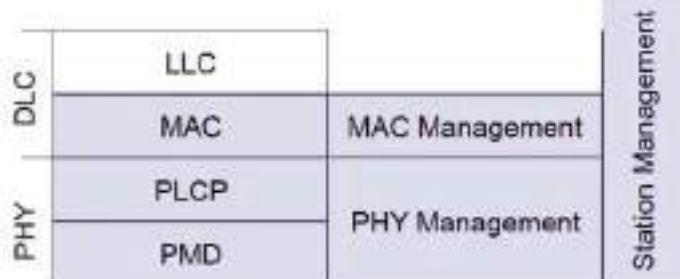
## Frame formats

52

Recall...

## 802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management
- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions



53

# FHSS PHY packet format

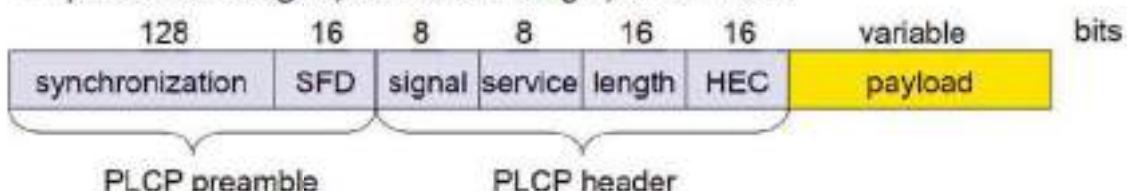
- Synchronization
  - synch with 010101... pattern
- SFD (Start Frame Delimiter)
  - 0000110010111101 start pattern
- PLW (PLCP\_PDU Length Word)
  - length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)
  - data rate of payload (1 or 2 Mbit/s)
- HEC (Header Error Check)
  - CRC with  $x^{16}+x^{12}+x^5+1$



54

# DSSS PHY packet format

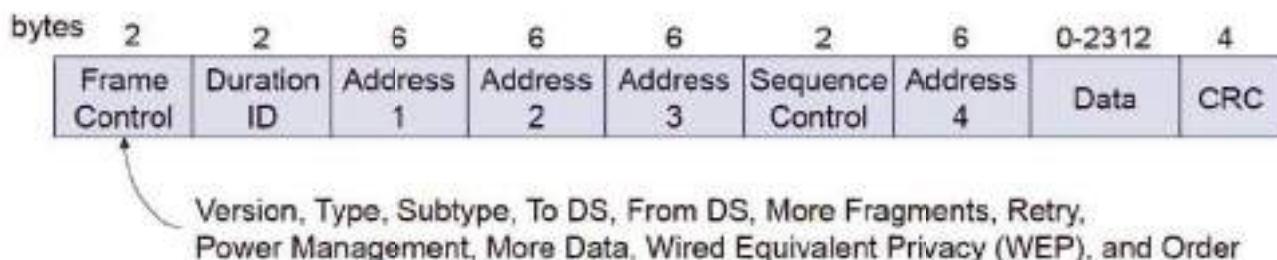
- Synchronization
  - synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter)
  - 1111001110100000
- Signal
  - data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service                      Length
  - future use, 00: 802.11 compliant               length of the payload
- HEC (Header Error Check)
  - protection of signal, service and length,  $x^{16}+x^{12}+x^5+1$



55

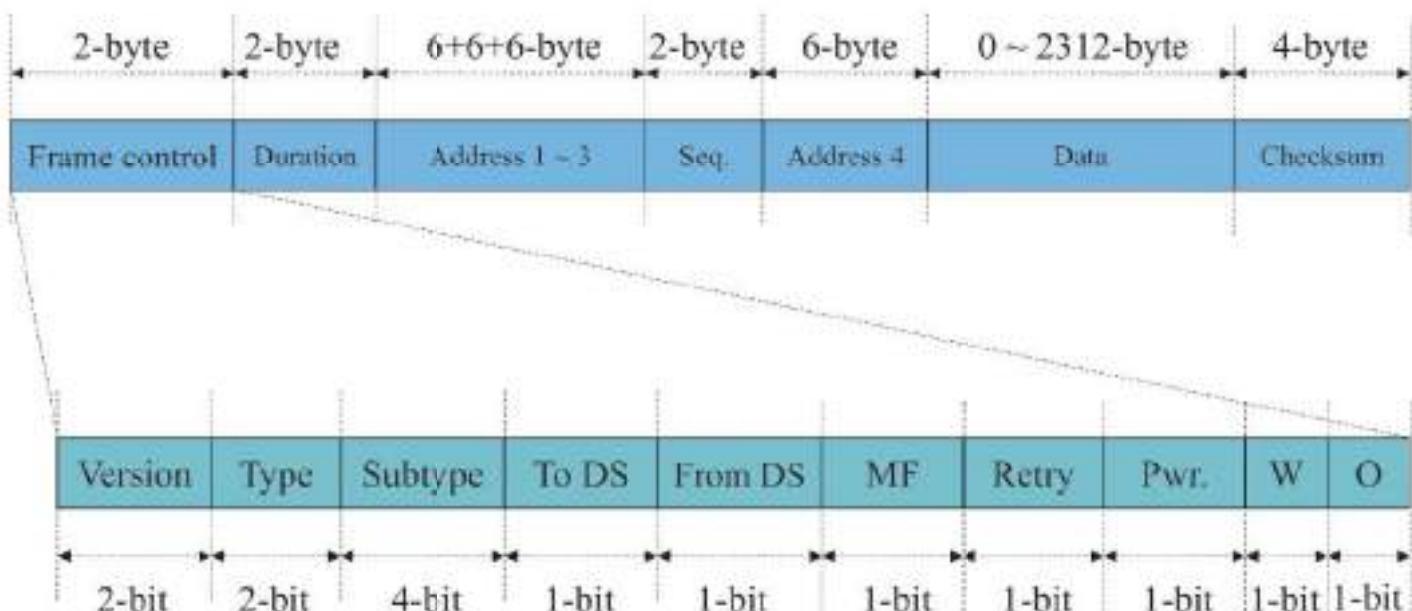
# 802.11 - Frame format

- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data

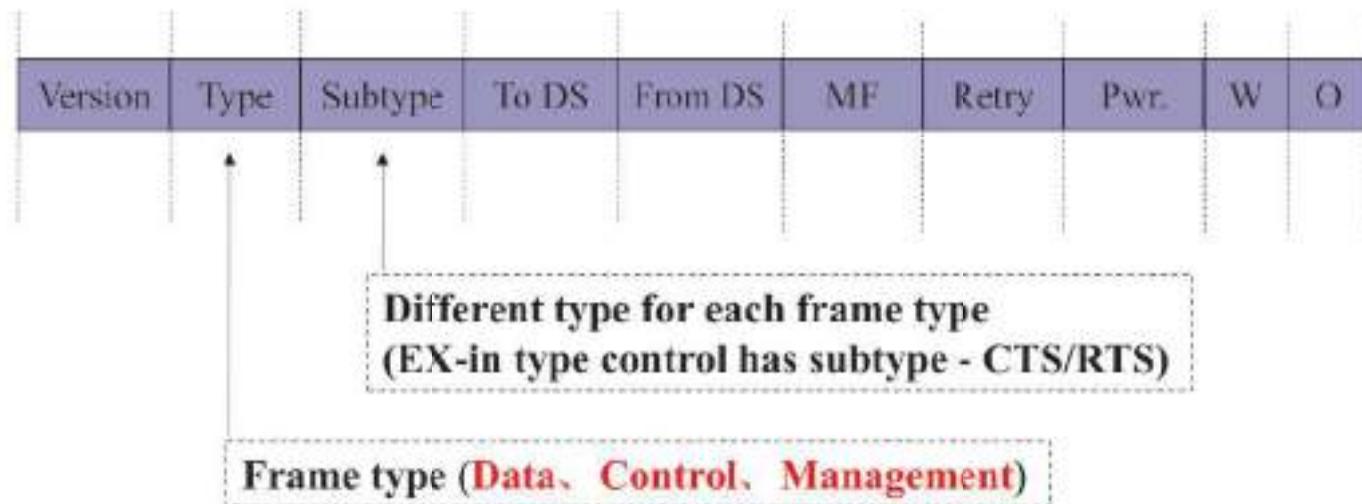


56

## 802.11 (Frame Structure)

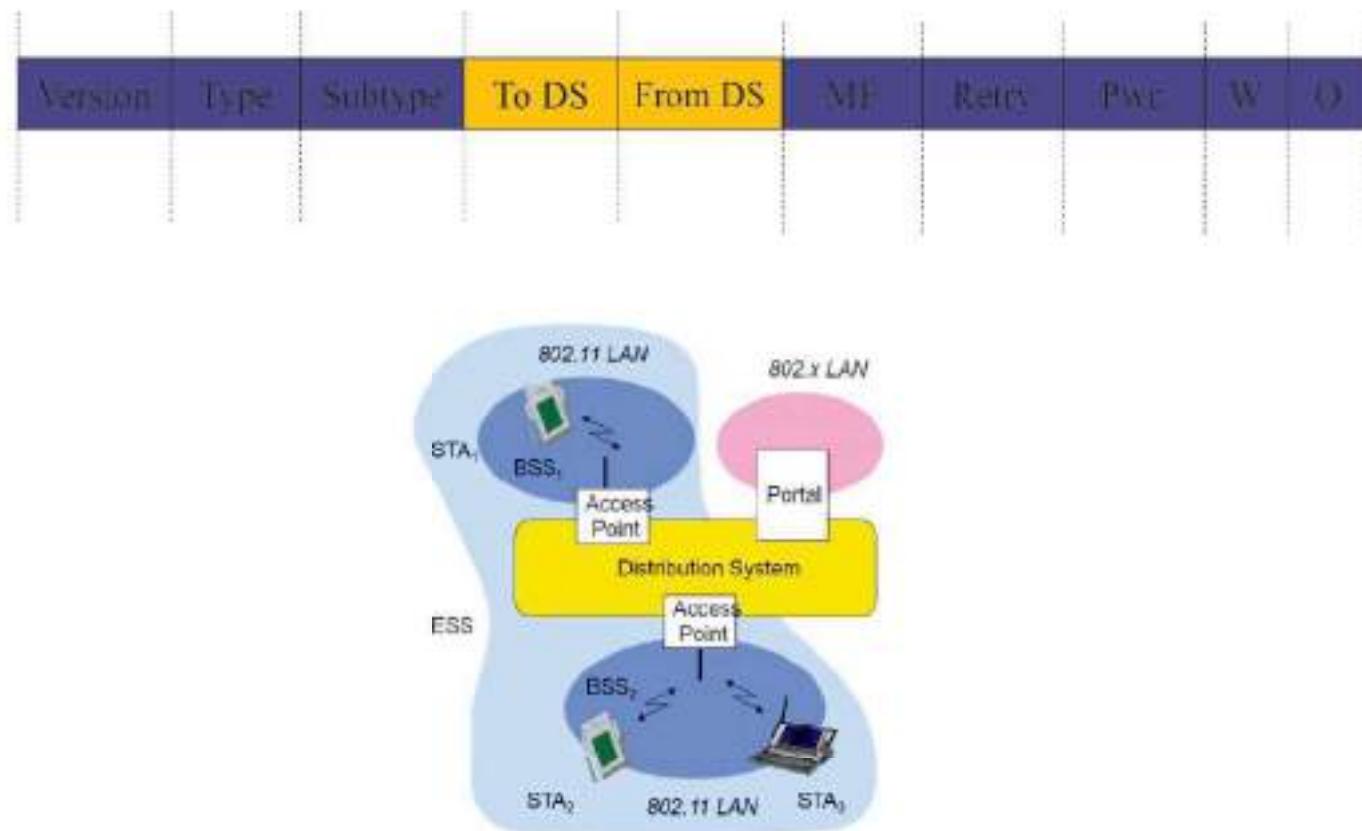


# 802.11 (Frame Structure)



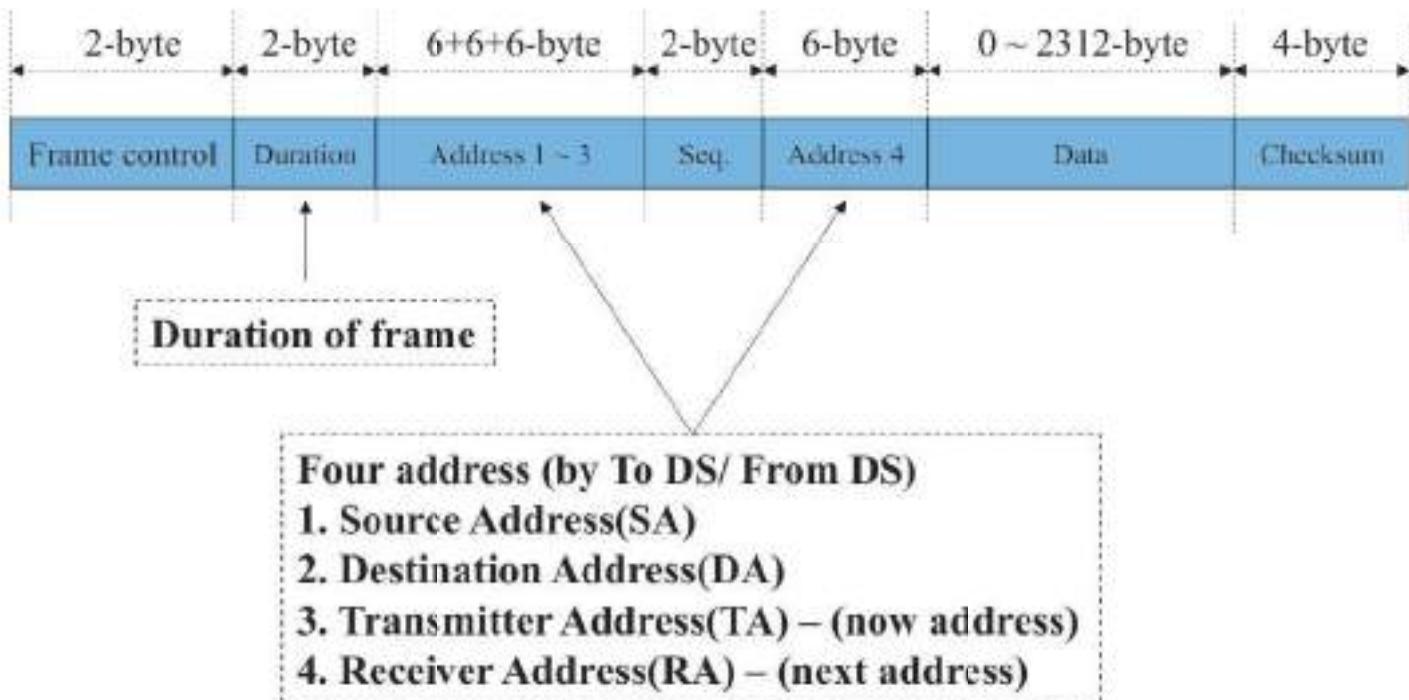
58

# 802.11 (Frame Structure)



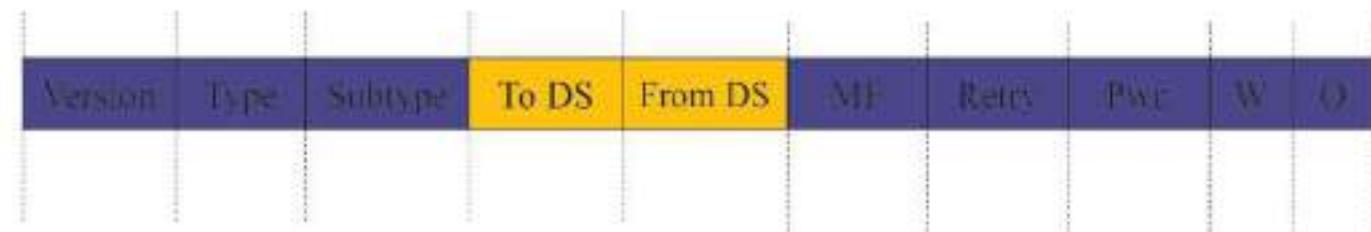
59

# 802.11 (Frame Structure)



60

# 802.11 (Frame Structure)

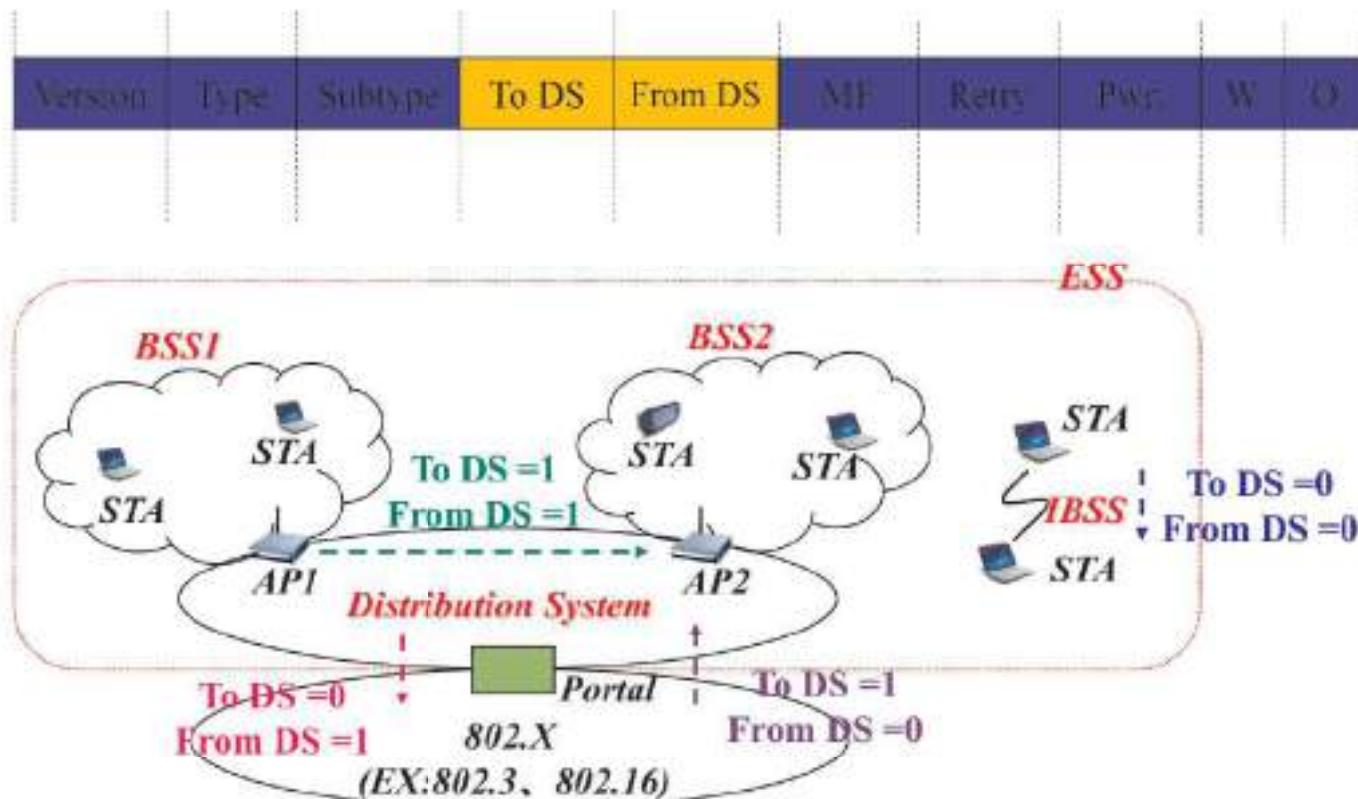


## MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network: from AP	0	1	DA	BSSID	SA	-
infrastructure network: to AP	1	0	BSSID	SA	DA	-
infrastructure network: within DS	1	1	RA	TA	DA	SA

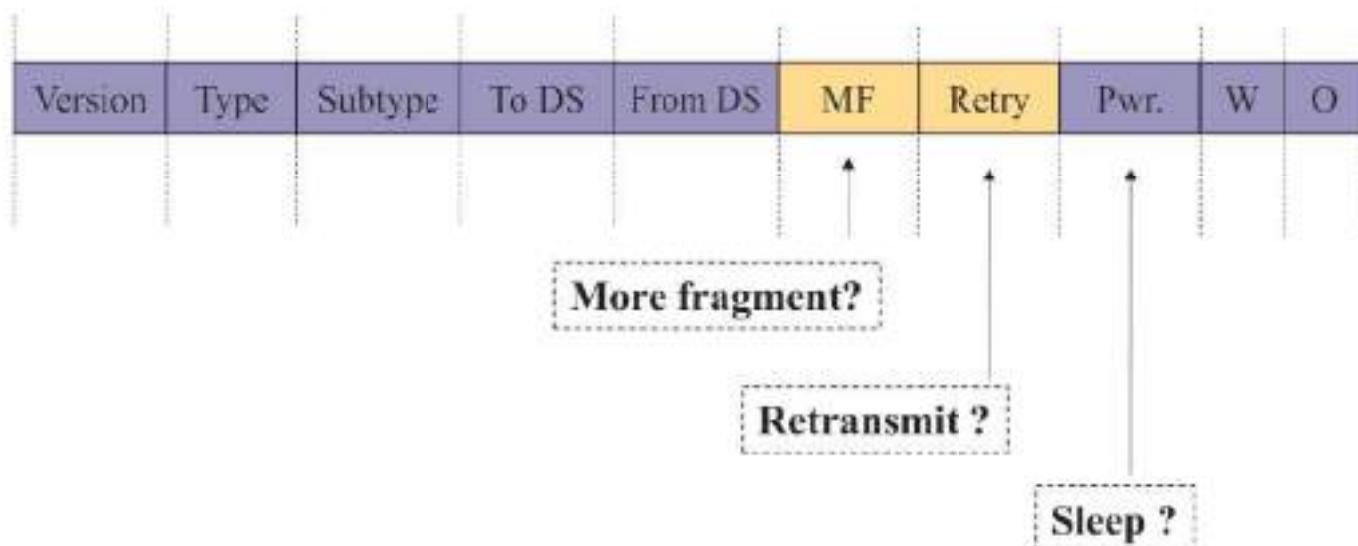
DS: Distribution System  
AP: Access Point  
DA: Destination Address (final recipient)  
SA: Source Address (initiator)  
BSSID: Basic Service Set Identifier  
RA: Receiver Address (immediate recipient)  
TA: Transmitter Address (immediate sender)

# 802.11 (Frame Structure)



62

# 802.11 (Frame Structure)



63

# Frame Types

- **Class 1 frames**

- Control Frames

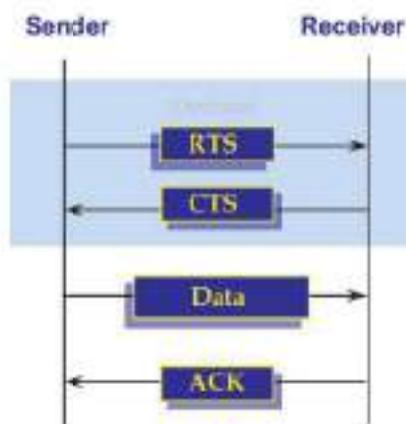
- (1) RTS
    - (2) CTS
    - (3) ACK
    - (4) CF-End+ACK
    - (5) CF-End

- Management Frames

- (1) Probe Request/Response
    - (2) Beacon
    - (3) Authentication
      - » Successful association enables Class 2 frames.
      - » Unsuccessful association leaves STA in State 1.
    - (4) Deauthentication
      - Return State 1.
    - (5) Announcement traffic indication message (ATIM)

- Data Frames

- (1) In IBSS, direct data frames only (FC control bits "To DS and from DS" both false)



64

# Frame Types

- **Class 2 Frames**

- Data Frames

- (1) Asynchronous data. Direct data frames only (FC control bits "To DS and from DS" both false)

- Management Frames

- (1) Association Request/Response
      - » Successful association enables Class 3 frames.
      - » Unsuccessful association leaves STA in State 2.
    - (2) Reassociation request/response
      - » Successful association enables Class 3 frames.
      - » Unsuccessful association leaves STA in State 2.
    - (3) Disassociation
      - Return State 2.

PS. When STA A receives a non-authenticated frame from STA B,  
STA A sends a deauthentication to STA B

65

# Frame Types

- **Class 3 Frames**
  - Data Frames
    - (1) Asynchronous data. Indirect data frames allowed (FC control bits "To DS and from DS" may be set to utilize DS Services)
  - Management Frames
    - (1) Deauthentication
      - » Return state 1
  - Control Frames
    - (1) PS-Poll

66

# Logical Service Interface

- The DS may not be identical to an existing wired LAN and **can be created from many different technologies** including current 802.x wired LANs.
- 802.11 does not constrain the DS to be either Data Link or Network Layer based. Nor constrain a DS to be either **centralized** or **distributed**.
- 802.11 specifies **services** instead of specific DS implementations. Two categories of services are defined: **Station Service (SS)** and **Distribution System Service (DSS)**.
- The complete set of 802.11 architectural services are:

1. Association	6. Authentication
2. Disassociation	7. Deauthentication
3. Reassociation	8. Privacy
4. Distribution	9. MSDU delivery
5. Integration	

SS: 6,7,8,9

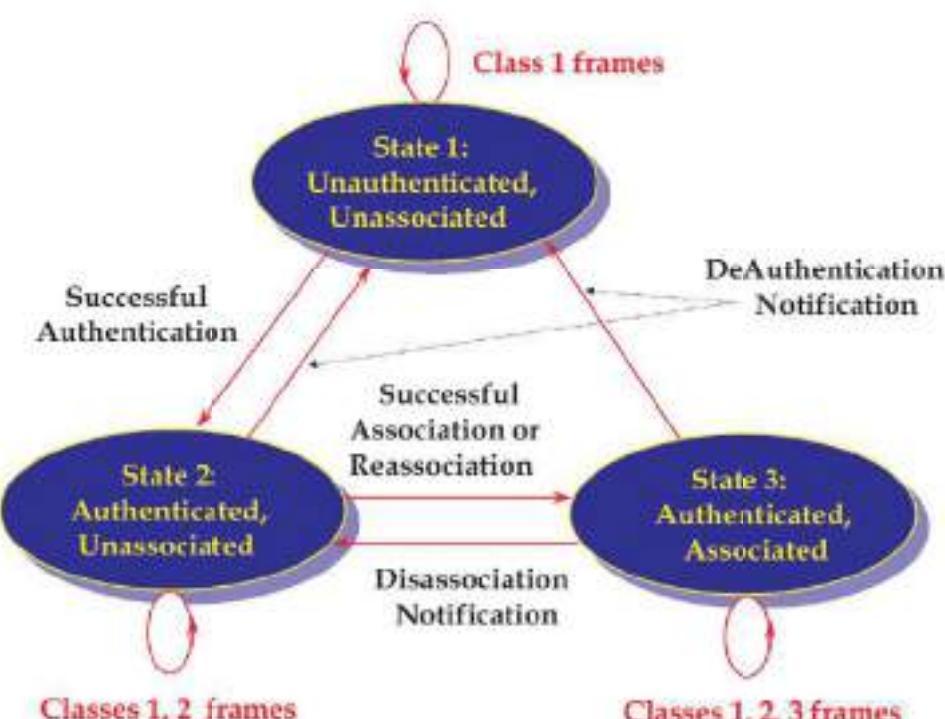
DSS: 1,2,3,4,5

67

## Relationship Between Services

- For a station, two state variables are required to keep track:
  - **Authentication State** : Unauthenticated and Authenticated
  - **Association State** : Unassociated and Associated
- Three station states are possible:
  - **State 1** : Initial start state, Unauthenticated, Unassociated.
  - **State 2** : Authenticated, not Associated.
  - **State 3** : Authenticated and Associated
- These states determine the 802.11 frame types (grouped into classes) which may be sent by a station.
  - State 1 : Only Class 1 frames are allowed.
  - State 2 : Either Class1 or Class 2 are allowed.
  - State 3 : All frames are allowed.

## Relationship Between State Variables and Services



Next

IEEE 802.15

70

71

# **CS 442**

## **Wireless Sensor Network**

### **Unit 3**

1

#### **Unit 3:**

Low power PAN, LAN Standards, IEEE 802.11,  
802.15, 802.15.4 and Zigbee.

.

### **Unit 3... contd.**

### **WLAN, WPAN standards**

2

## IEEE 802 Standards Working Groups

Number	Topic
★ 802.1	Overview and architecture of LANs
★ 802.2 ↓	Logical link control
★ 802.3 *	Ethernet
★ 802.4 ↓	Token bus (was briefly used in manufacturing plants)
★ 802.5	Token ring (IBM's entry into the LAN world)
★ 802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 ↑	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
★ ★ 802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
★ 802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

★ You have studied in Computer Network Course

★ We study in this course

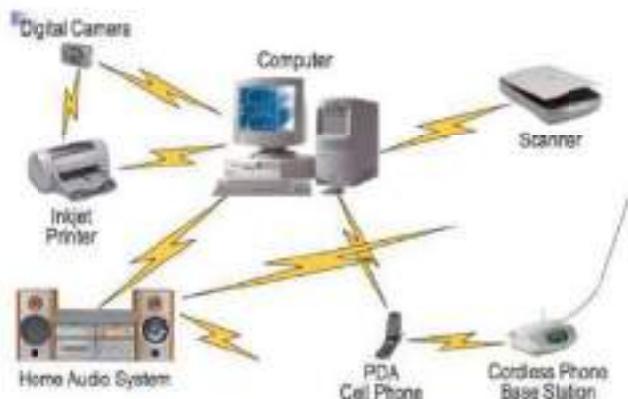
3

## WPAN Standards

## IEEE 802.15

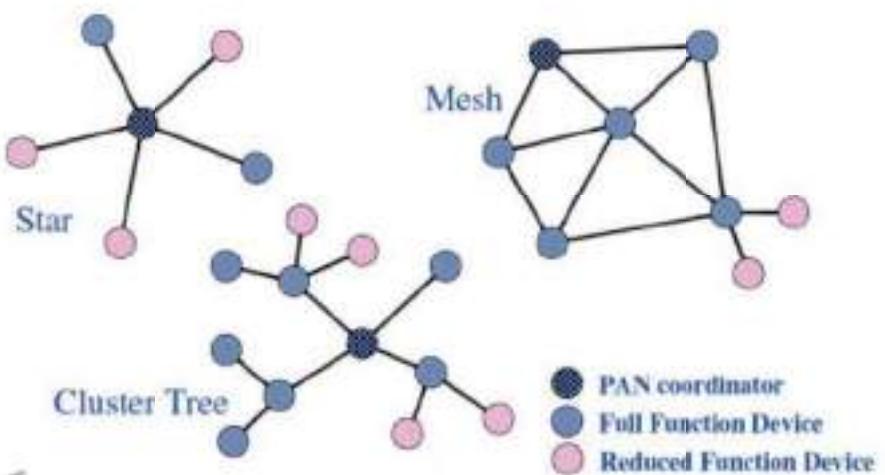
# Wireless Personal Area Networks

- Person centered short-range wireless connectivity



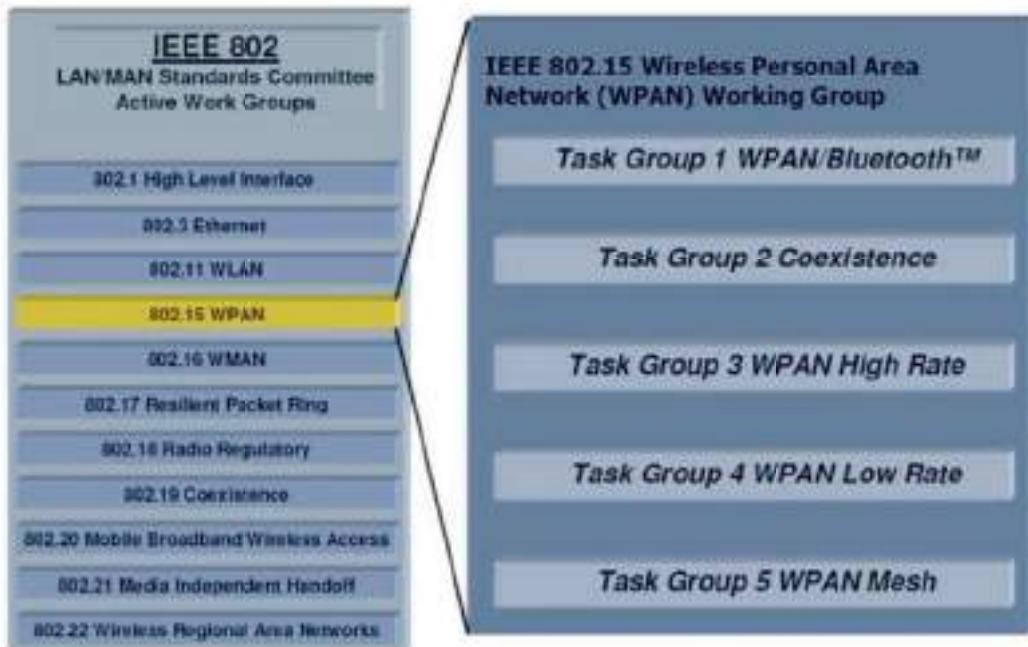
5

## WPAN Topologies



6

# IEEE 802.15 WPAN Working Group

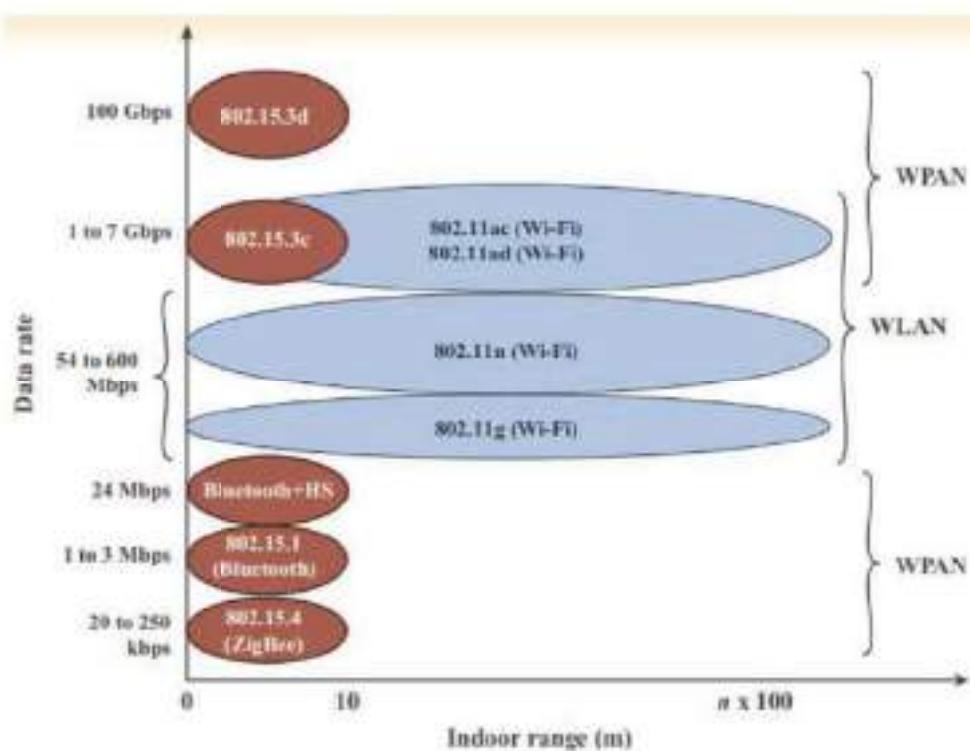


7

## IEEE 802.15 Protocol Architecture

Logical link control (LLC)			
802.15.1 Bluetooth MAC	802.15.3 MAC	802.15.4, 802.15.4e MAC	
802.15.1 2.4 GHz 1, 2, or 3 Mbps 24 Mbps HS	802.15.3c 60 GHz 1 to 6 Gbps	802.15.3d 60 GHz 100 Gbps	802.15.4, 802.15.4a 868/915 MHz, 2.4 GHz DSSS: 20, 40, 100, 250 kbps UWB: 110 kbps to 27 Mbps CSS: 250 kbps, 1 Mbps

8



9

## IEEE 802.15 WPAN Standards

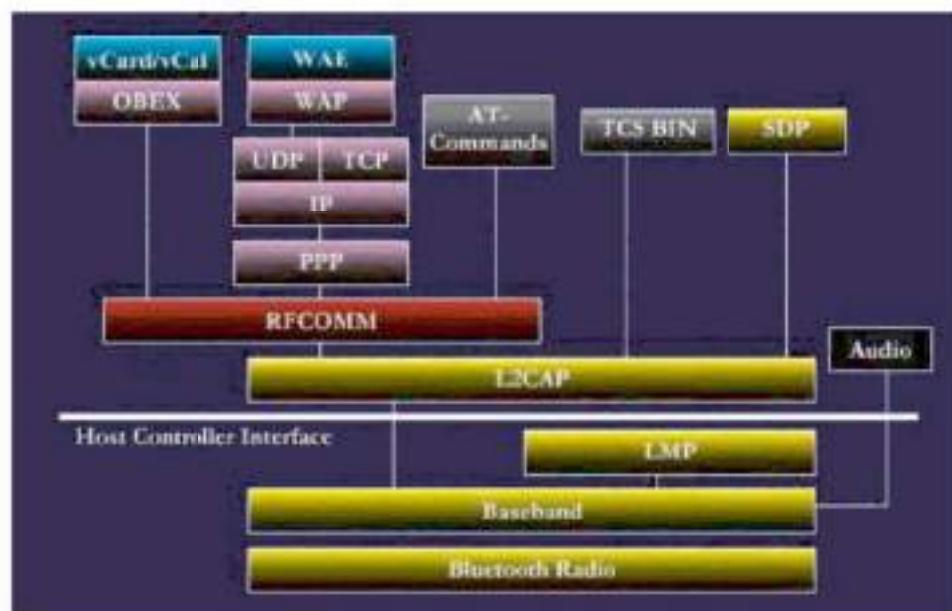
IEEE standard	Topic	Data throughput	Suitable applications	QoS needs
802.15.1	Bluetooth	1Mbps	Cell phones, Computers, Personal Digital Assistants (PDAs), Handheld Personal Computers (HPC's), printers, microphones, speakers, headsets, bar code readers, sensors, displays, pagers, and cellular & Personal Communications Service (PCS) phones	QoS suitable for voice applications
802.15.2	Coeexistence of Bluetooth and 802.11b	N/A	N/A	N/A
802.15.3	High-rate WPAN	>20Mbps	Low power, low cost solutions for portable consumer of digital imaging and multimedia applications	Very high QoS
802.15.4	Low-rate WPAN	<0.25 Mbps	Industrial, agricultural, vehicular, residential, medical applications, sensors and actuators with very low power consumption and low cost	Relaxed needs for data rate and QoS

# The Bluetooth Protocol standard (IEEE 802.15.1)

- Logically partitioned into 3 group
  - Transport protocol group
    - Radio layer
    - Baseband layer
    - Link manager layer
    - Logical link control
    - Adaptation layer
    - Host controller interface
  - Middleware protocol group
    - RFCOMM, SDP, IrDA
  - Application group
    - Application profiles

11

## Bluetooth Protocol Stack



12

# Bluetooth protocol stack

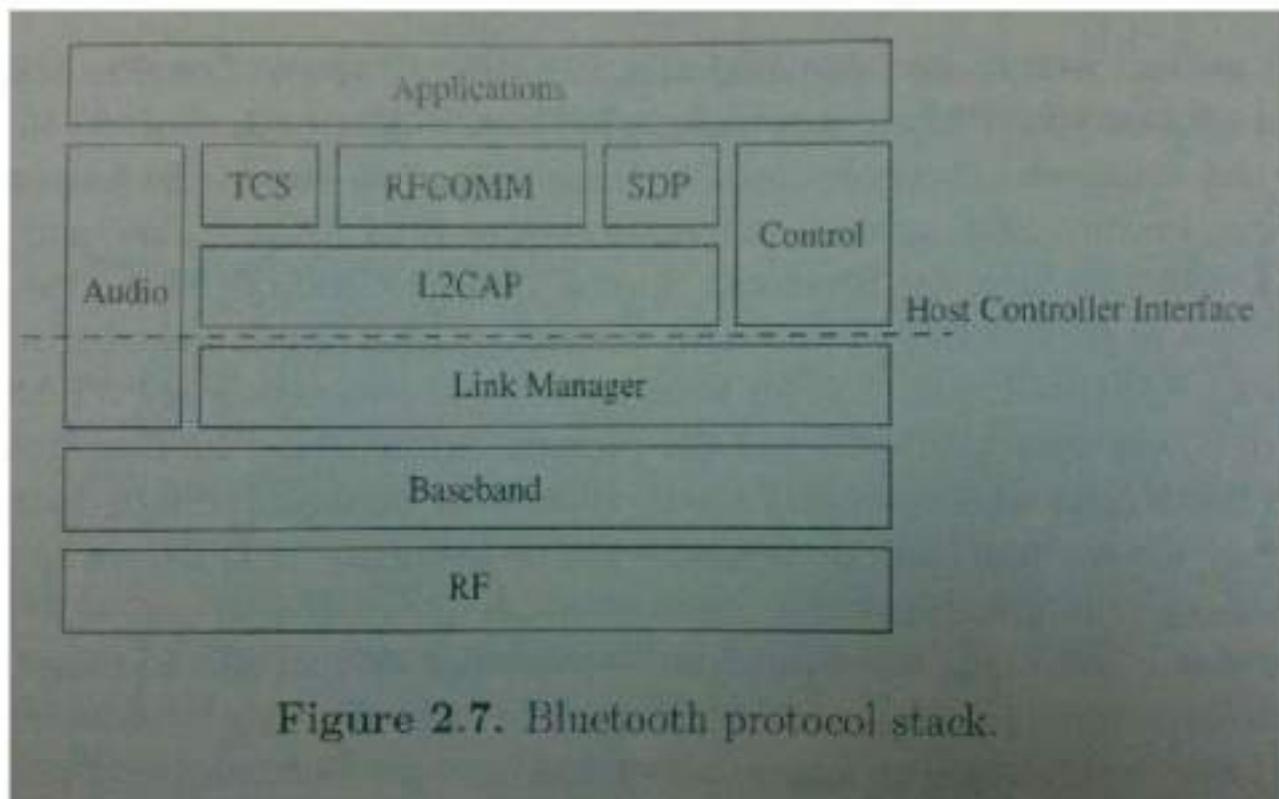


Figure 2.7. Bluetooth protocol stack.

13

## Bluetooth : Radio (Physical) Layer

- GFSK
- 64Kbps voice channels and asynchronous data channels with peak rate of 1Mbps
- Data channel: asymmetric or symmetric
- 79 channels, 79 hops
- Typical link range: up to 10 m, can be extended to 100m by increasing power

14

# Baseband Layer

## • Piconet (Fig 2.8)

- 48-bit address
- Master +
- up to 7 active slaves

15

## Piconet

- Master + up to 7 active slaves

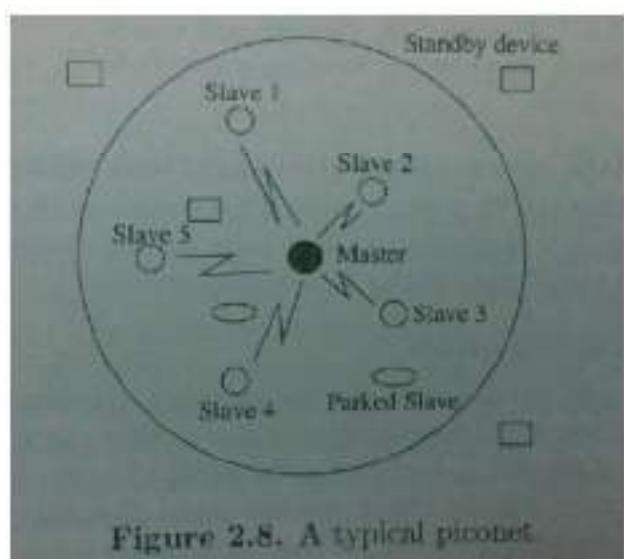
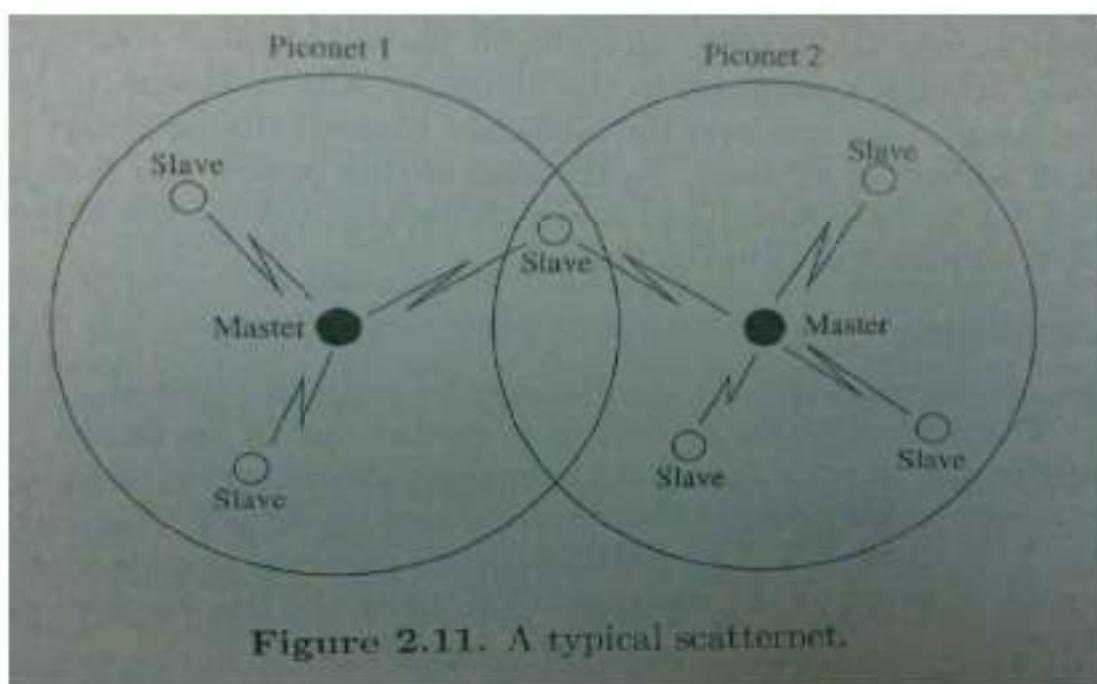


Figure 2.8. A typical piconet

# Scatternets

- Piconet may overlap both spatially and temporally
- Each piconet is characterized by a unique master and hop independently
- As more piconets added, more probability of collisions
- Device can participate in 2 or more piconets by time sharing (as a slave in several piconets, but as a master in only a single piconet)
- A group of piconets →scatternet (Fig2.11)

17



18

- Issues:
  - **Gateway nodes**: bound back-and-forth, hard to achieve full utilization
  - Timing may miss:

19

## Operational States

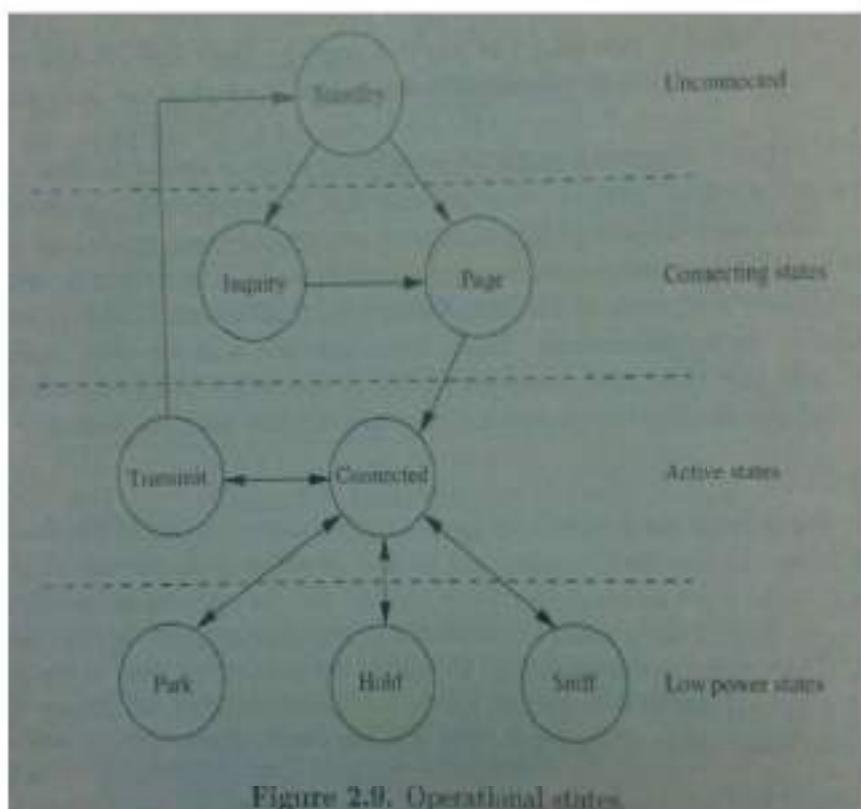


Figure 2.9. Operational states.

## Inquiry State

- A potential master sends inquiry packet on inquiry hop sequence of frequencies
- A slave periodically enter inquiry scan state and listen for inquiry packets
- When received, send response packet containing hopping sequence and device address

21

## Page State

- Master estimate slave's clock to determine hop sequence, and send page message
- Slaves listen in page scan mode. On receiving page message, slave enter page response sub-state, send page response containing its device access code (DAC)
- Master enter page response state (after receiving slave's response), inform slaves its clock and address for determining hopping sequence and synchronization

22

# Link Manager Protocol

- Power Management
  - **Active mode**: active slaves are polled by master
  - **Sniff mode**: master issues a command to slave to enter sniff mode
  - **Hold mode**: temporarily not support ACL packets, performing scanning, paging, inquiring, or attending another piconet
  - **Park mode**: slave gives up its active member address
- Security Management
- **Minimal QoS support** by allowing control over parameters such delay and jitter

23

## Bluetooth : Transmission over a channel

- ACL: asynchronous connectionless link
- SCO: synchronous connection oriented link

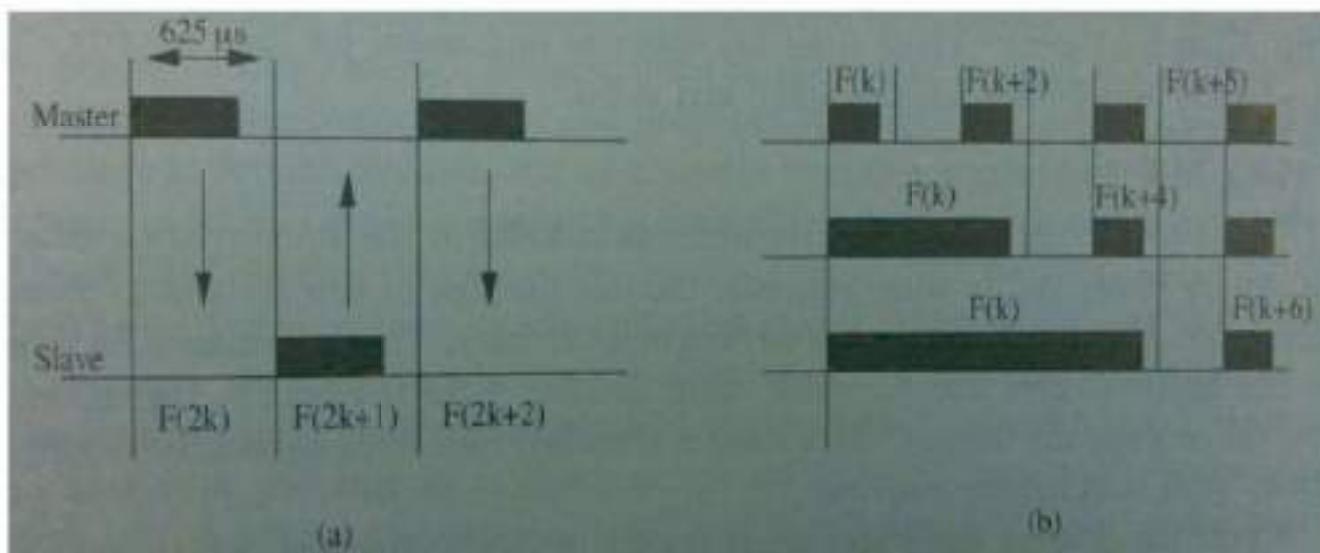


Figure 2.10. Transmission of packets over a channel.

24

## SCO Links vs. ACL Links

	Intended Traffic Type	Retransmission	Max # links between master and slave	Supported during hold mode	Switched connection type
ACL	Data	Yes	1	No	Packet
SCO	Time bounded info (Audio or Video)	No	3	Yes	Circuit

25

## Bluetooth Baseband Formats



(a) Packet format



### (b) Access code format



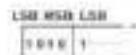
(c) Header format (prior to coding)



### Single-list packets



The preamble is a fixed zero-one pattern of four symbols used to facilitate dc compensation. The sequence is either 1010 or 0101, depending whether the LSB of the following sync word is 1 or 0, respectively.



presente - www.morci



presentable sync word

## Packet format

## Bluetooth Packet Fields

- Access code – used for timing synchronization, offset compensation, paging, and inquiry
- Header – used to identify packet type and carry protocol control information
- Payload – contains user voice or data and payload header, if present

27

## Profiles

- Over 40 different profiles are defined in Bluetooth documents
  - Only subsets of Bluetooth protocols are required
  - Reduces costs of specialized devices
- All Bluetooth nodes support the Generic Access Profile
- Profiles may depend on other profiles
  - Example: File Transfer Profile
    - Transfer of directories, files, documents, images, and streaming media formats
    - Depends on the Generic Object File Exchange, Serial Port, and Generic Access Profiles.
    - Interfaces with L2CAP and RFCOMM protocols

28

# Bluetooth Profiles

- Promote interoperability among many implementations of bluetooth protocol stack
- Provide a clear and transparent standard that can be used to implement a specific user end function
- 4 categories of profiles
  - Generic profiles
  - Telephony profiles
  - Networking profiles
  - Serial and object exchange profiles

29

Next..... LoWPAN

ZigBee

<http://www.zigbee.org>

30

## Next..... LoWPAN

ZigBee

<http://www.zigbee.org>

30

---

**Unit 3 (contd...)**

**IEEE 802.15.4**  
**&**  
**ZIGBEE**

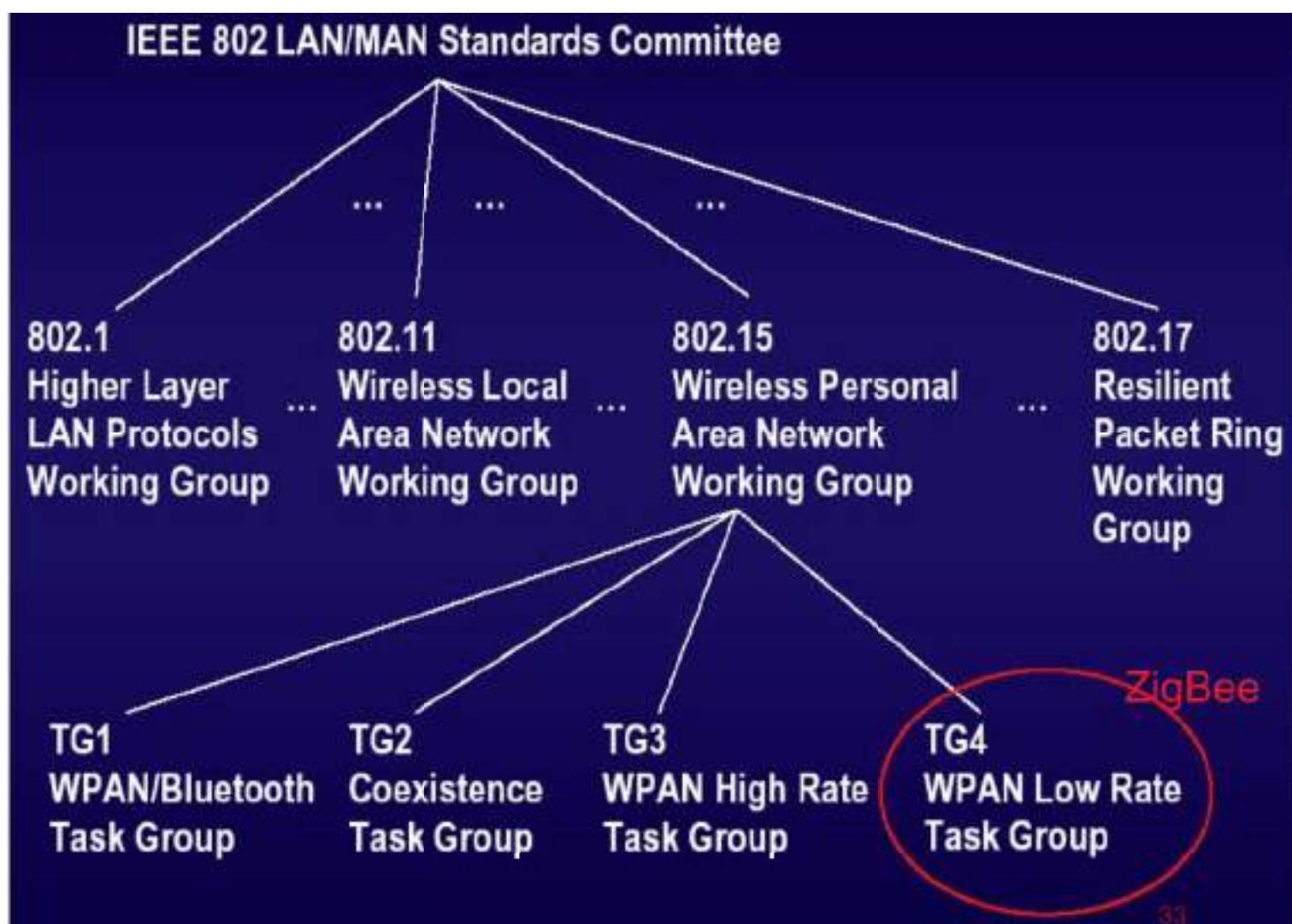
---

31

# Review : 802.15

- IEEE 802.15 is the 15th working group of the IEEE 802
- Specializes in Wireless PAN (Personal Area Network)
- It includes four task groups (numbered from 1 to 4)

32



33

- IEEE 802.15.4 - Standard released in May 2003 for LR-WPAN

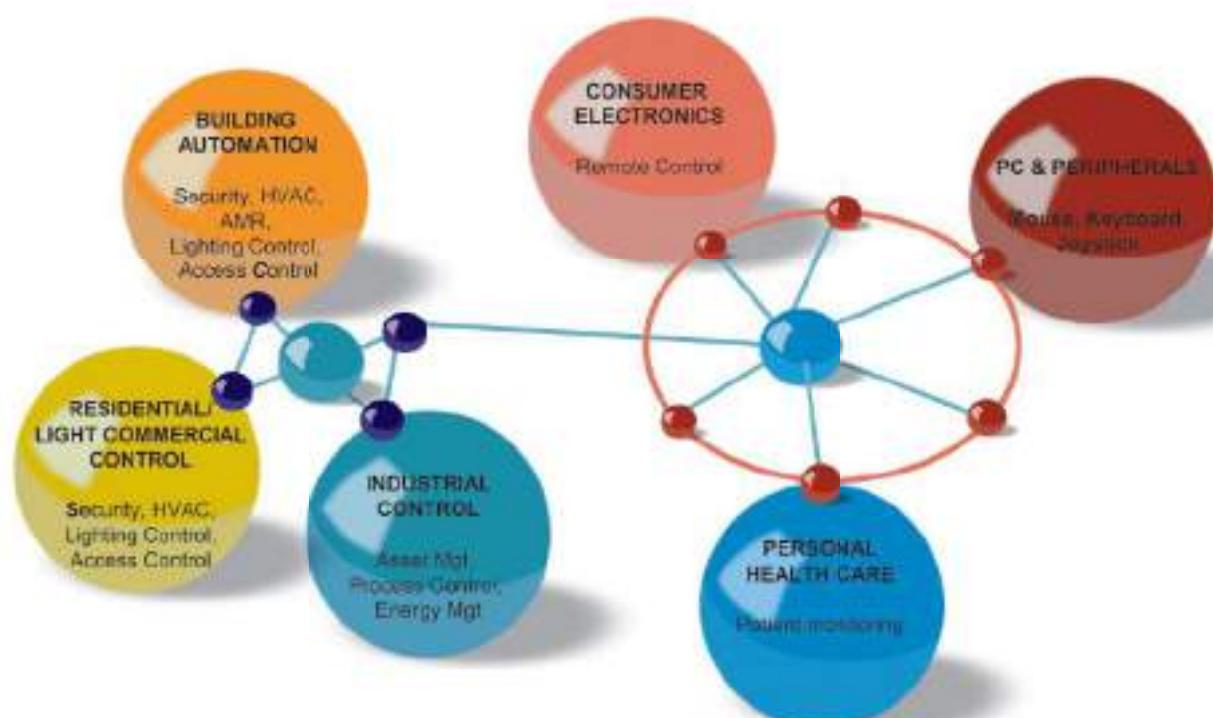
- Zigbee - set of high level communication protocols based upon the specification produced by 802.15.4

- The ZigBee Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard.

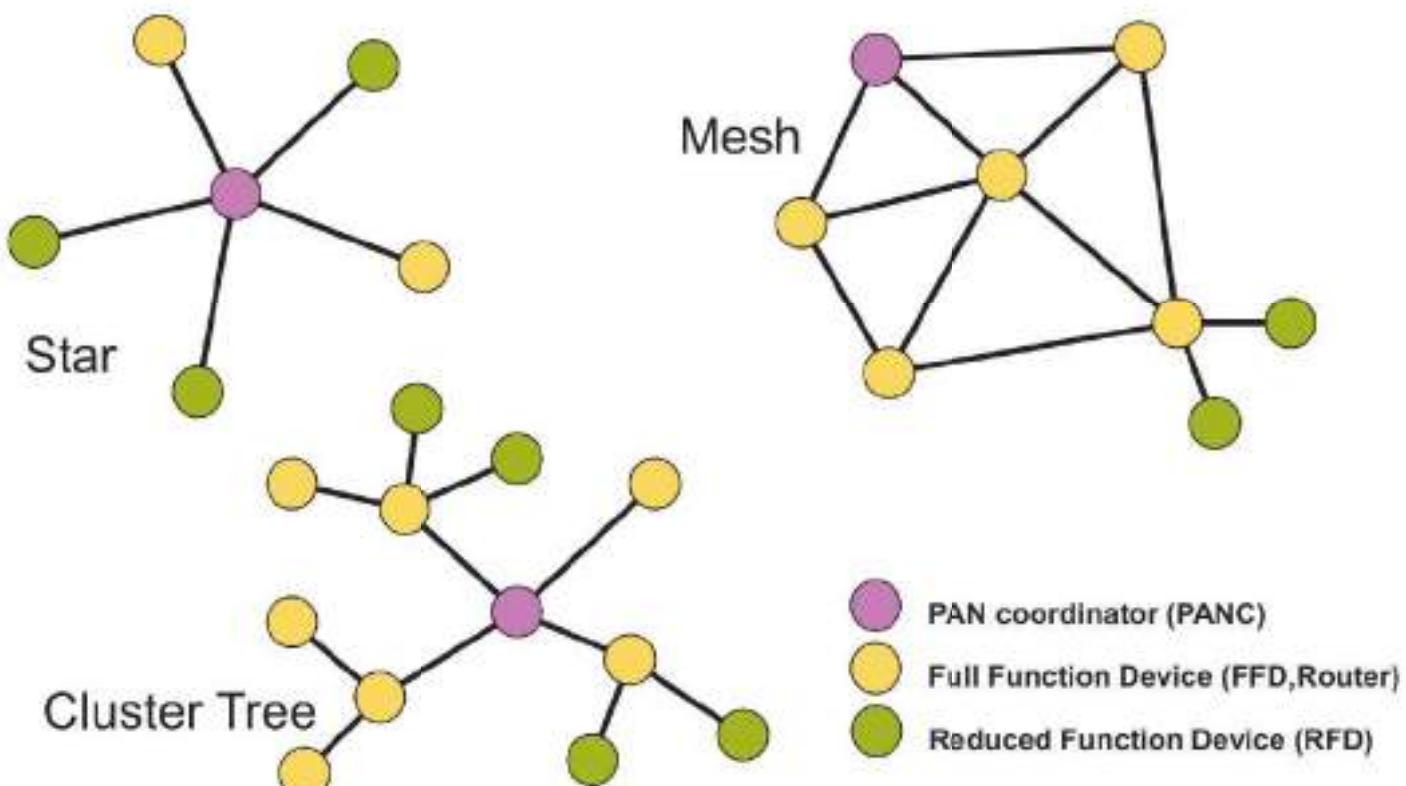


34

## ZigBee Wireless Markets and Applications

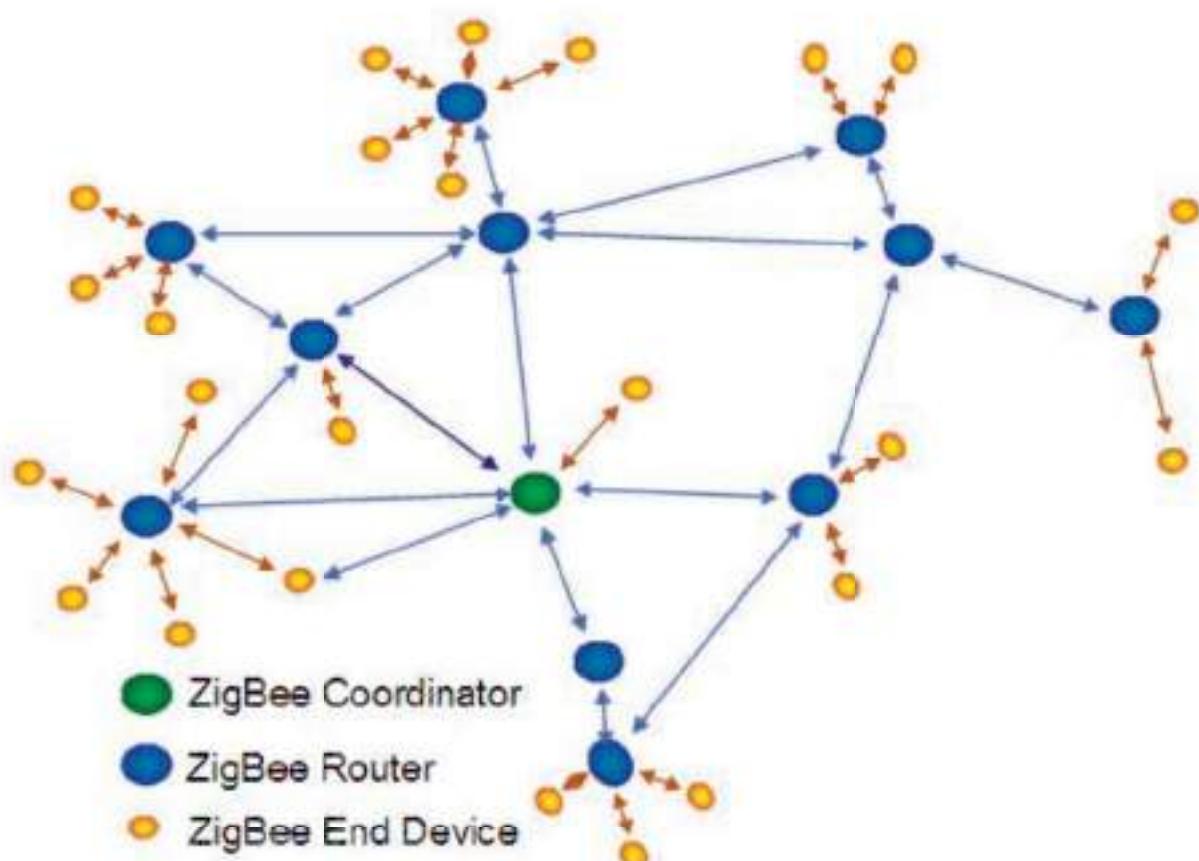


# Network Topology Models



36

## ZigBee is Mesh Networking



37

# ZigBee networking Basics

## Network Scan

*Device scans the 16 channels to determine the best channel to occupy.*

## Creating/Joining a PAN

*Device can create a network (coordinator) on a free channel or join an existing network*

## Device Discovery

*Device queries the network to discover the identity of devices on active channels*

## Service Discovery

*Device scans for supported services on devices within the network*

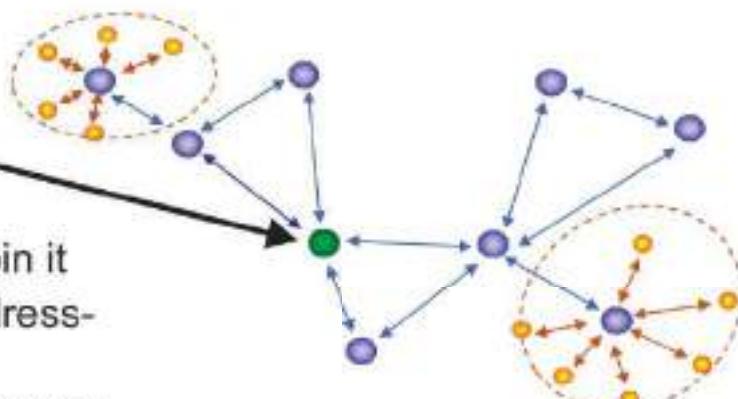
## Binding

*Devices communicate via command/control messaging*

38

## Network Pieces –PAN Coordinator

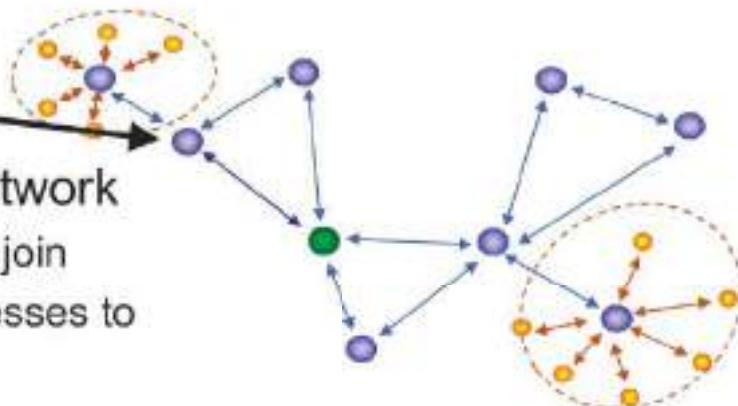
- PAN Coordinator
  - “owns” the network
    - Starts it
    - Allows other devices to join it
    - Provides binding and addressable services
    - Saves messages until they can be delivered
    - And more... could also have i/o capability
  - A “full-function device” – FFD
  - Mains powered



39

# Network Pieces - Router

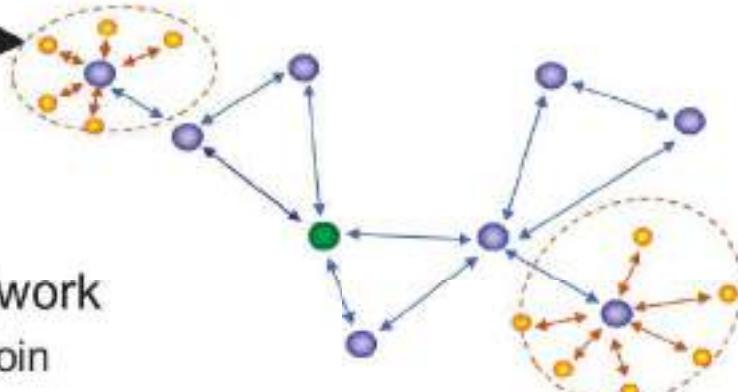
- Routers
  - Routes messages
  - Does not own or start network
    - Scans to find a network to join
    - Given a block of addresses to assign
- A “full-function device” – FFD
- Mains powered depending on topology
- Could also have i/o capability



40

# Network Pieces – End Device

- End Device
  - Communicates with a single device
  - Does not own or start network
    - Scans to find a network to join
  - Can be an FFD or RFD (reduced function device)
  - Usually battery powered



41

# Traffic types

- Periodic data
  - Application defined rate (e.g. **sensing temperature**)
- Intermittent data
  - Application/external stimulus defined rate (e.g. **light switch**)
- Repetitive low latency data
  - Allocation of time slots (e.g. **mouse**)

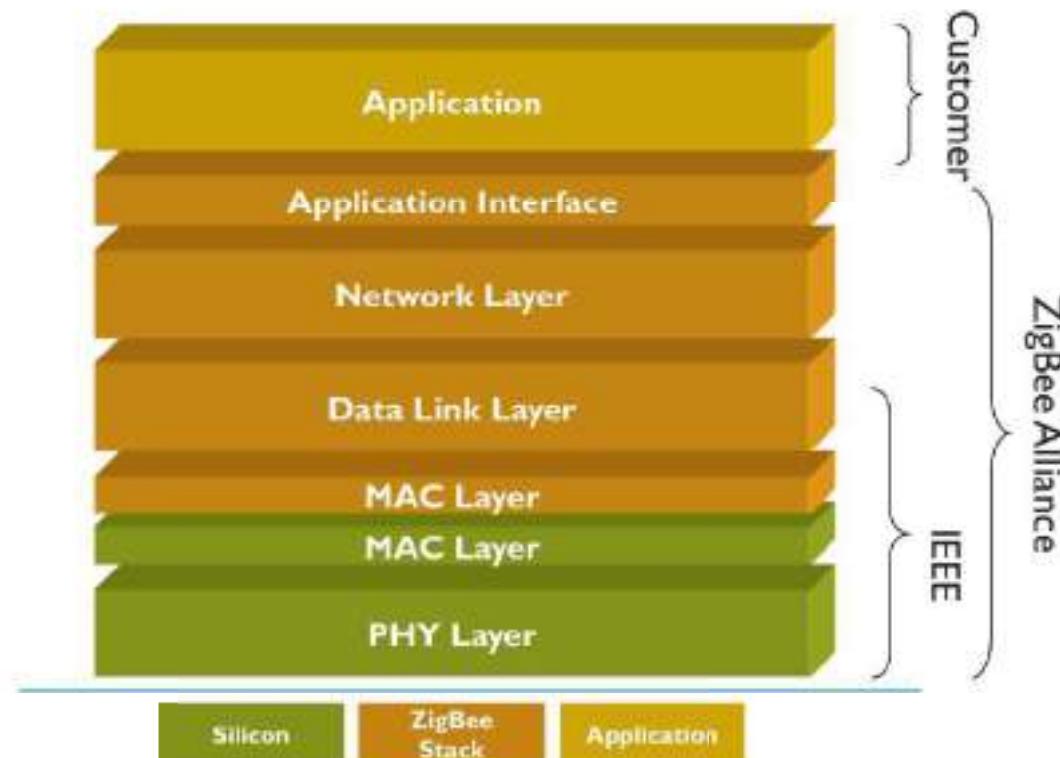
42

## IEEE 802.15.4



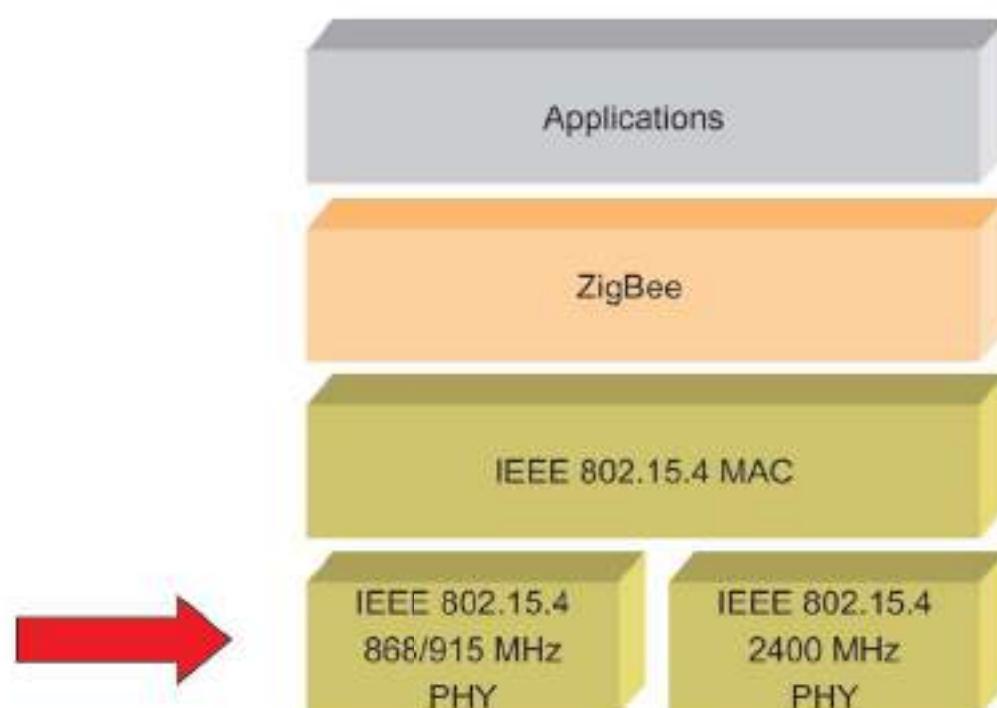
43

# ZigBee Alliance - IEEE - Customer Relationship



44

## 802.15.4 Architecture: Physical Layer



45

## **Physical Layer functionalities:**

- Activation and deactivation of the radio transceiver
- Energy detection within the current channel
- Link quality indication for received packets
- Clear channel assessment for CSMA-CA
- Channel frequency selection
- Data transmission and reception

## **ZigBee specifies two Physical media:**

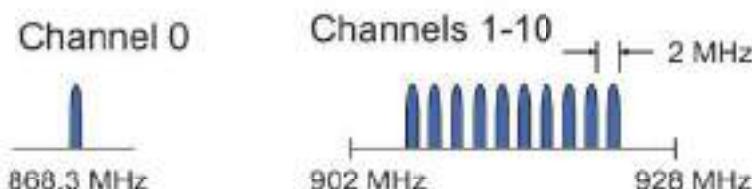
- 868 MHz/915 MHz direct sequence spread spectrum (DSSS) PHY (11 channels)
  - 1 channel (20Kb/s) in European 868MHz band
  - 10 channels (40Kb/s) in 915 (902-928)MHz ISM band
- 2450 MHz direct sequence spread spectrum (DSSS) PHY (16 channels)
  - 16 channels (250Kb/s) in 2.4GHz band

46

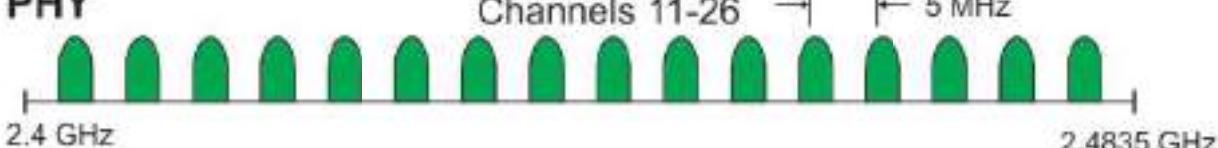
## **IEEE 802.15.4 Physical Layer**

- Operates in unlicensed ISM bands:

**868MHz/  
915MHz  
PHY**



**2.4 GHz  
PHY**

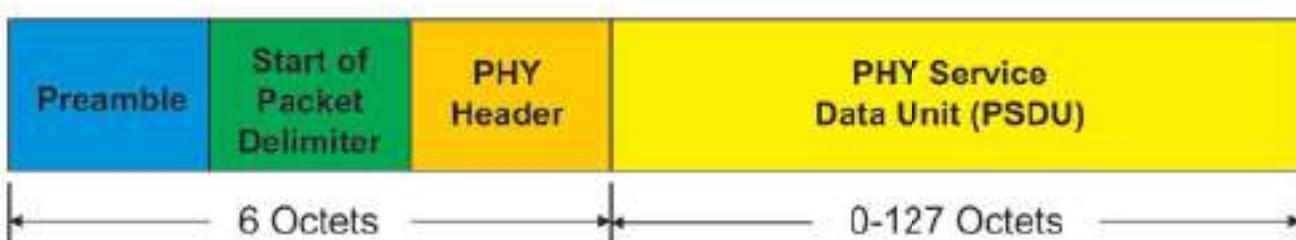


47

# IEEE 802.15.4 PHY Layer Packet Structure

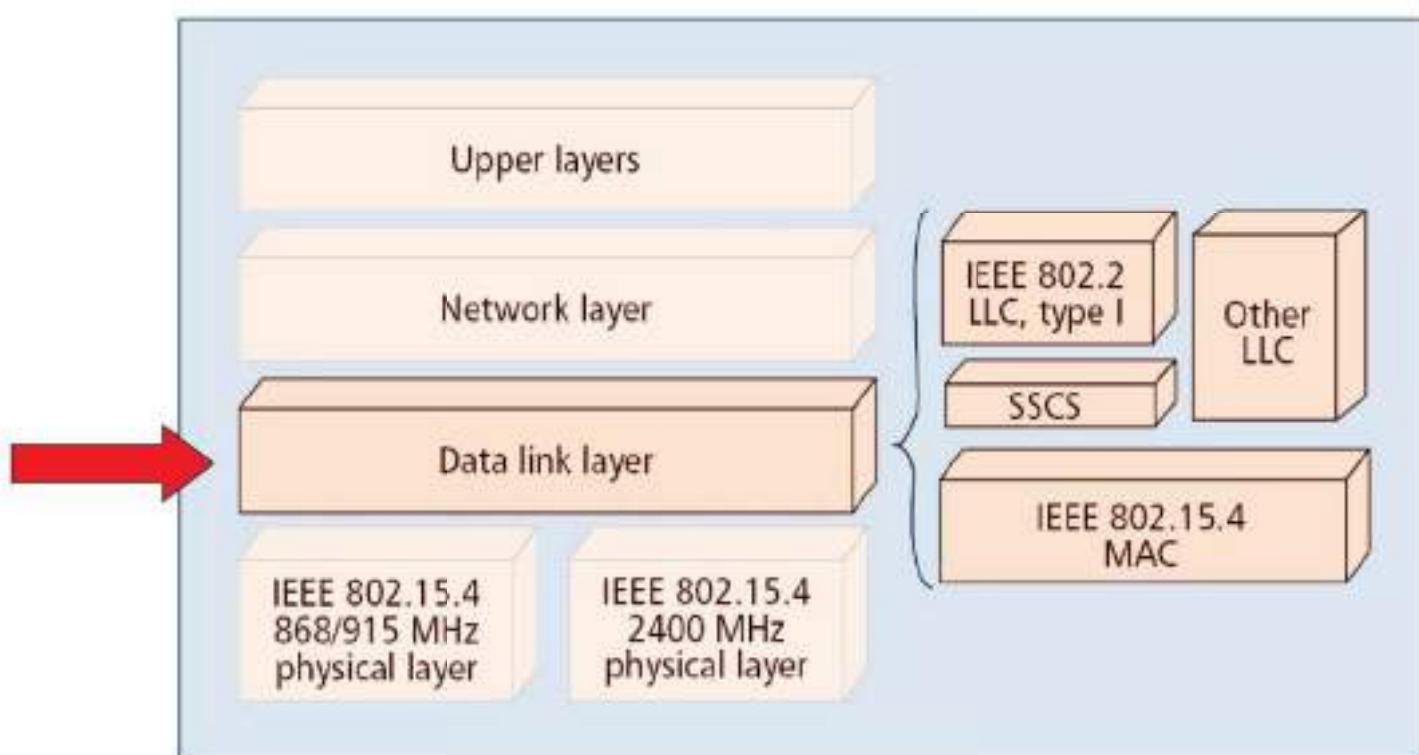
## PHY Packet Fields

- Preamble (32 bits) – synchronization
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field



48

## 802.15.4 Architecture: MAC layer



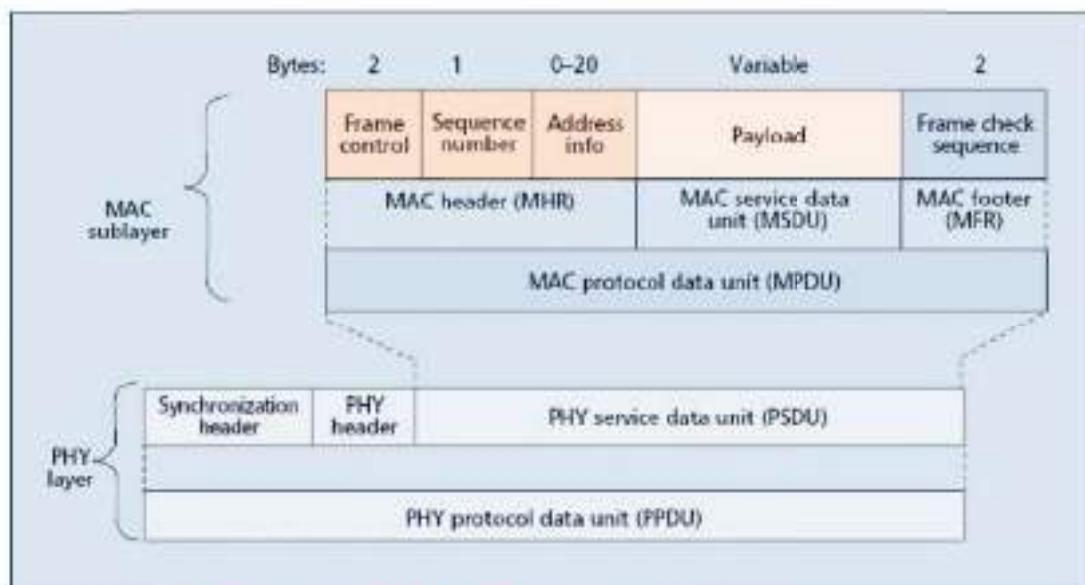
49

- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range operation
- Very low power consumption

Simple but flexible protocol !

50

## IEEE 802.15.4 MAC Overview General Frame Structure



### 4 Types of MAC Frames:

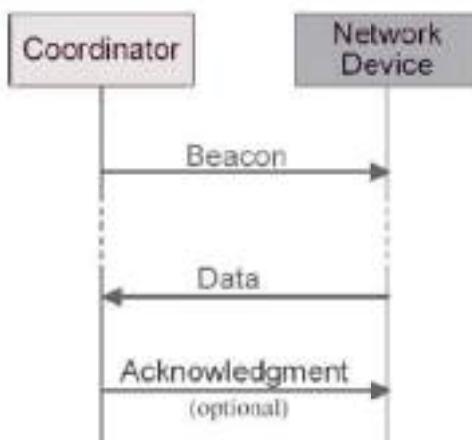
- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

51

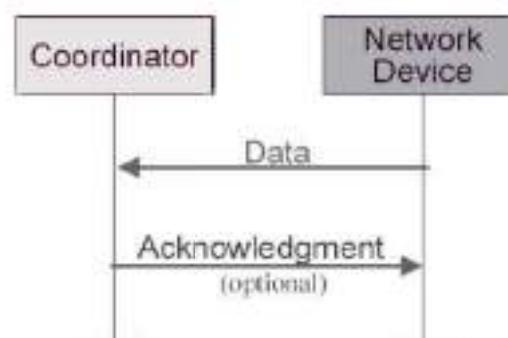
# Data Transfer Model

## Data transferred from device to coordinator

- In a beacon-enable network, device finds the beacon to synchronize to the super-frame structure. Then using slotted CSMA/CA to transmit its data.
- In a non beacon-enable network, device simply transmits its data using un-slotted CSMA/CA



Communication to a coordinator  
In a **beacon-enabled** network

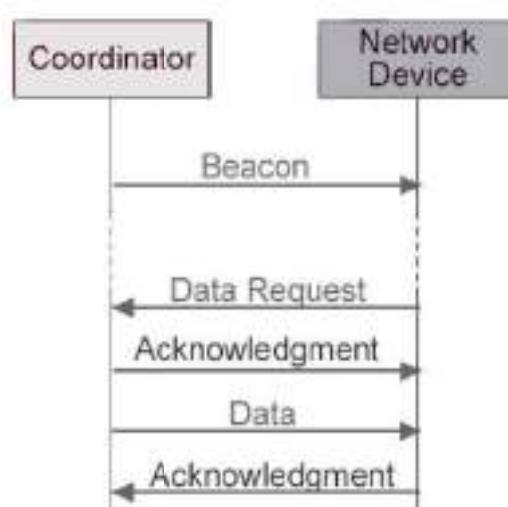


Communication to a coordinator  
In a **non beacon-enabled** network

52

# Data Transfer Model

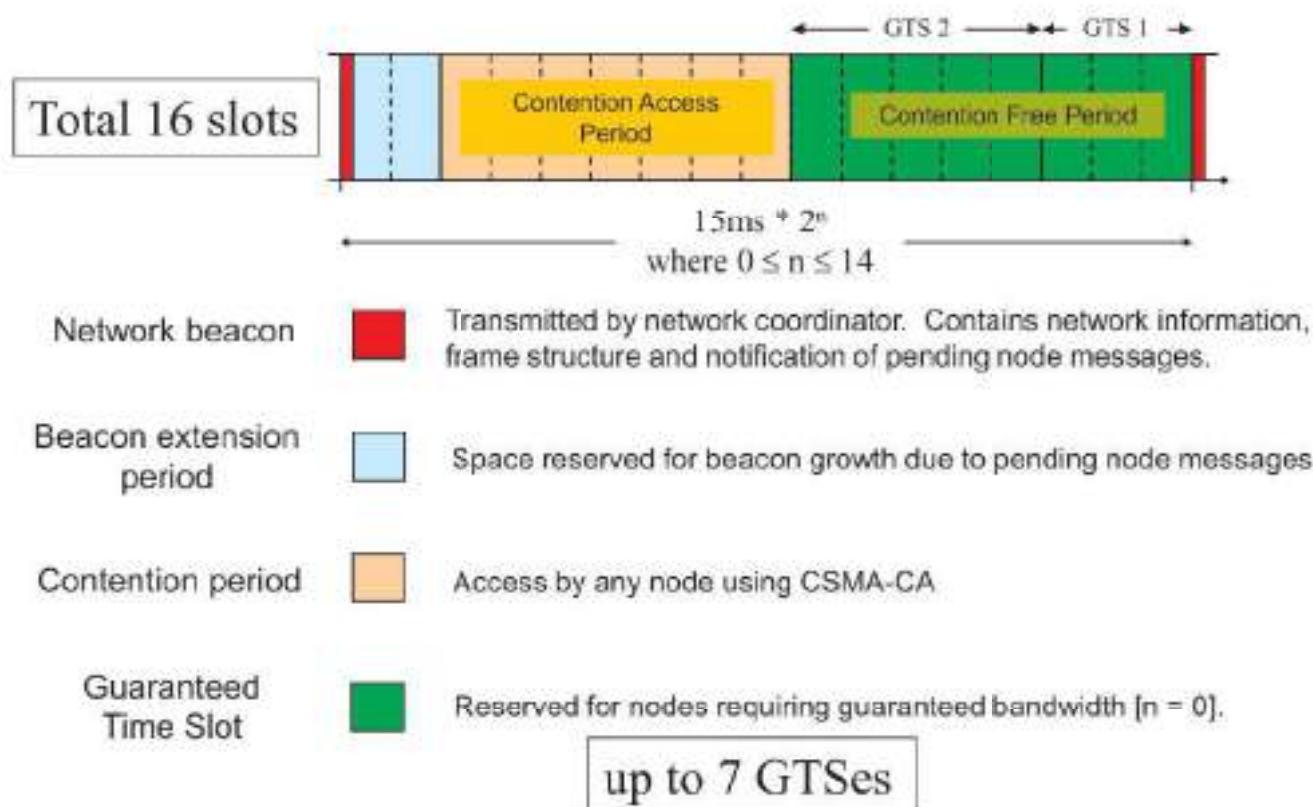
- **Data transferred from coordinator to device**
  - In a beacon-enable network, the coordinator indicates in the beacon that "**data is pending**."
  - Device periodically listens to the beacon and transmits a **MAC command request** using slotted CSMA/CA if necessary.



Communication from a coordinator  
In a **beacon-enabled** network

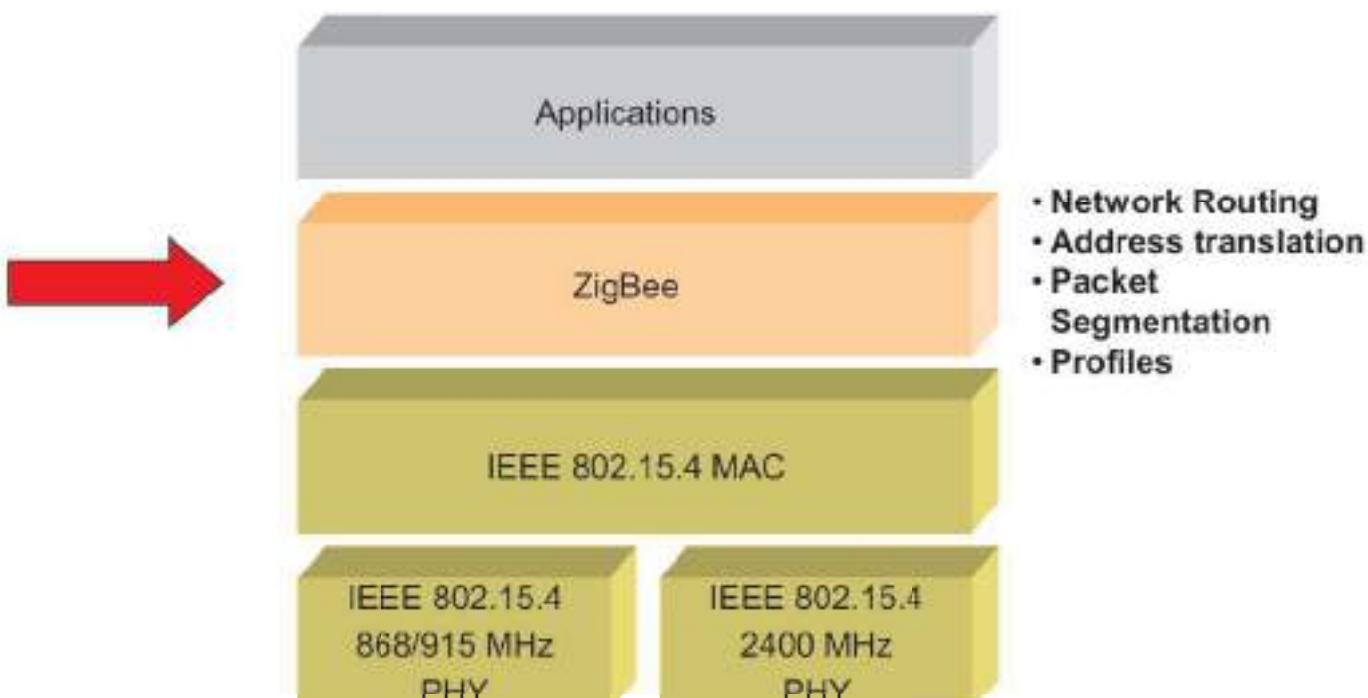
53

# Superframe: CSMA-CA + TDMA



54

## 802.15.4 + ZigBee



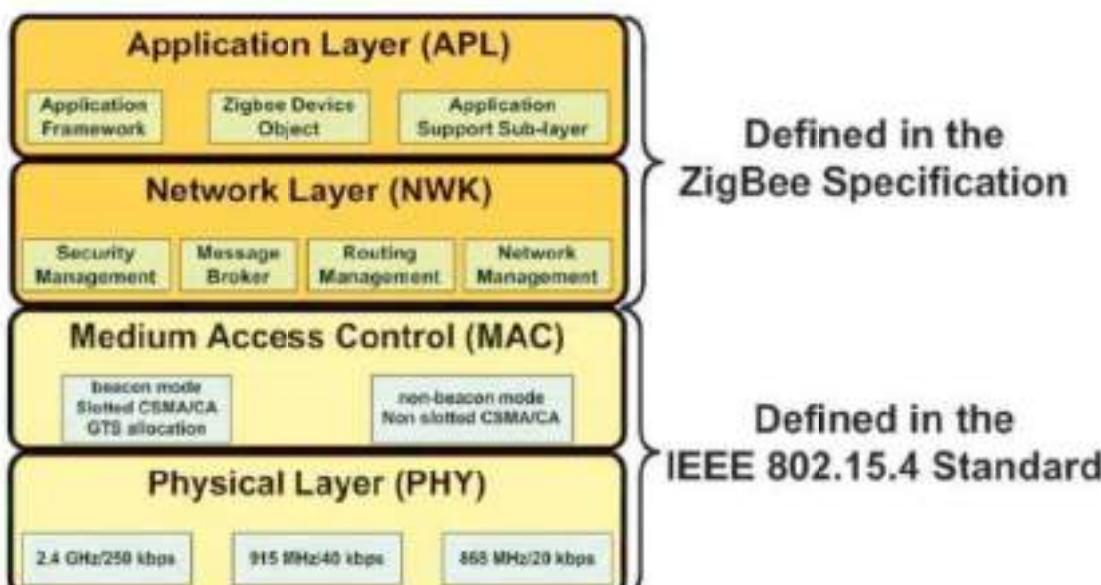
55

# ZigBee Stack Architecture :



56

## 802.15.4 + ZigBee



57

# Comparison with peer technologies!

Feature(s)	IEEE 802.11b	Bluetooth	ZigBee
Power Profile	Hours	Days	Years
Complexity	Very Complex	Complex	Simple
Nodes/Master	32	7	64000
Latency	Enumeration upto 3 seconds	Enumeration upto 10 seconds	Enumeration 30ms
Range	100 m	10m	70m-300m
Extendability	Roaming possible	No	YES
Data Rate	11Mbps	1Mbps	250Kbps
Security	Authentication Service Set ID (SSID)	64 bit, 128 bit	128 bit AES and Application Layer user defined

58

## ZigBee vs Bluetooth

**Bluetooth is Best      But ZigBee is Better**

For :

- Ad-hoc networks between capable devices
- Handsfree audio
- Screen graphics, pictures...
- File transfer

If :

- The Network is static
- Lots of devices
- Infrequently used
- Small Data Packets

59

# Air Interface:

**ZigBee**

**DSSS**

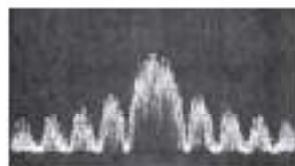
**11 chips/ symbol**

**62.5 K symbols/s**

**4 Bits/ symbol**

**Peak Information Rate**

**~128 Kbit/second**



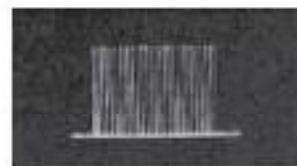
**Bluetooth**

**FHSS**

**1 M Symbol / second**

**Peak Information Rate**

**~720 Kbit/second**



60

## Timing Considerations

### ZigBee:

- New slave enumeration = 30ms typically
- Sleeping slave changing to active = 15ms typically
- Active slave channel access time = 15ms typically

### Bluetooth:

- New slave enumeration = >3s
- Sleeping slave changing to active = 3s typically
- Active slave channel access time = 2ms typically

**ZigBee protocol is optimized for timing critical applications**

61

# Power Considerations

## ZigBee

- 2+ years from 'normal' batteries
- Designed to optimise slave power requirements

## Bluetooth

- Power model as a mobile phone (regular charging)
- Designed to maximise ad-hoc functionality

Application example of a light switch with respect to latency and power consumption .....

62

## 802.15.4/ZigBee Products



Control4 Home Automation System  
<http://www.control4.com/products/components/complete.htm>



Eaton Home HeartBeat monitoring system  
[www.homeheartbeat.com](http://www.homeheartbeat.com)



Chip Sets

- Ember, <http://www.ember.com/index.html>
- ChipCon, <http://www.chipcon.com>
- Freescale, <http://www.freescale.com>



Software, Development Kits

- AirBee, <http://www.airbeewireless.com/products.php>
- Software Technologies Group, <http://www.stg.com/wireless/>



**Crossbow Technology**  
– Wireless Sensor Networks  
[www.xbow.com](http://www.xbow.com)

63

# SUMMARY:

---

- **IEEE 802.15.4 and ZigBee**

- Allows Designer to concentrate on end application
  - Silicon vendors and ZigBee Alliance take care of transceiver, RF channel and protocol, ZigBee "look and feel"
- Reliable and robust communications
  - PHY and MAC outperform all known non-standards-based products currently available
- Flexible network architectures
- Very long primary battery life (months to years to decades)
- Low system complexity. (Due to its architecture)

64

# References:

---

- IEEE 2003 version of 802.15.4 MAC & Phy standard
  - <http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf>
- ZigBee Specification
  - [http://www.zigbee.org/en/spec\\_download/download\\_request.asp](http://www.zigbee.org/en/spec_download/download_request.asp)
- 802.15.4 Tutorial
  - [http://grouper.ieee.org/groups/802/15/pub/2003/Jan03/03036r0P802-15\\_WG-802-15-4-TG4-Tutorial.ppt](http://grouper.ieee.org/groups/802/15/pub/2003/Jan03/03036r0P802-15_WG-802-15-4-TG4-Tutorial.ppt)
- ZigBee Technology: Wireless Control that Simply Works
  - <http://www.hometoys.com/htinews/oct03/articles/kinney/zigbee.htm>
- Home networking with Zigbee
  - <http://www.embedded.com//showArticle.jhtml?articleID=18902431>
  - [www.howstuffwork.com](http://www.howstuffwork.com)
  - <http://en.wikipedia.org/wiki/Zigbee>

□ [www.zigbee.org](http://www.zigbee.org)  
□ [www.xbow.com](http://www.xbow.com)

65

# **Next ... Unit 4**

## **WSN MAC**

# CS 442

## Wireless Sensor Network

### Unit 4

**Unit-4      Medium Access:** Medium access problem related to sensor network, Aloha, CSMA, Slotted Aloha, RTS/CTS, ACKs, TRAMA, SMAC and other WSN MAC protocols, Energy management.

CS 442 WSN Unit-4

## MAC / Requirements / Attributes

---

- ▶ **Basic task of MAC protocol**
  - ▶ Collision avoidance/minimization
- ▶ **Energy efficiency**
  - ▶ MAC layer controls radio. Radio often consume most energy
- ▶ **Scalability and adaptivity**
  - ▶ Nodes join, exit, rejoin, die, move to different location
  - ▶ Good MAC should accommodate such changes
- ▶ **Channel utilization**
  - ▶ Very important in cellular or wireless LAN
  - ▶ Often secondary in WSNs
- ▶ **Latency**
- ▶ **Throughput**
- ▶ **Fairness**
  - ▶ Important in traditional cellular/wireless LAN, less important in WSNs

## Medium Access Control (MAC) - Methods

---

- ▶ **One Approach (Be nice – share)**
  - ▶ Avoid interference by **scheduling** nodes on sub-channels
    - ▶ TDMA (Time-Division Multiple Access)
    - ▶ FDMA (Frequency-Division Multiple Access)
    - ▶ CDMA (Code-Division Multiple Access)
- ▶ **Another Approach (Compete/*contend*)**
  - ▶ Don't pre-allocate transmission, compete => probabilistic coordination
  - ▶ ALOHA (Transmit. Collision? Yes, discard packet, retransmit later)
  - ▶ Carrier Sense (IEEE 802.11)

3

## MAC : WSN requirements

---

- ▶ **For WSNs, most important attributes of a good MAC are**
  - ▶ Effective collision avoidance
  - ▶ Energy Efficiency
  - ▶ Scalability and adaptivity
- ▶ **Other attributes are normally secondary**
  - ▶ Fairness
  - ▶ Latency
  - ▶ Channel utilization

4

# Energy Efficiency in MAC Protocols

---

- › Motivation – Energy efficiency is very important in WSNs.
- › What causes energy waste from a MAC perspective?
  - › Collision
    - › Collided packets are discarded, retransmission require energy
    - › Not a big issue in scheduled (TDMA, CDMA, FDMA) MAC protocols, but an issue in contention MAC protocols.
  - › Idle listening
    - › Long distance (500 m or more) Tx energy consumption dominates, but in short-range communication Rx energy consumption can be close to Tx energy consumption
    - › MICA2 *idle:receiving:transmission* ratio at 1 mW is 1:1:1.41 @ 433 MHz and 1mW
    - › Can be a dominant factor in WSN energy consumption

5

# Energy Efficiency in Mac Protocols

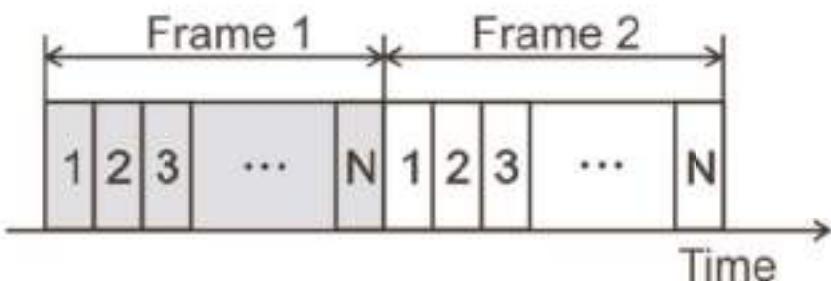
---

- › Overhearing
  - › When a node receives packets that are destined for another node
- › Control packet overhead
  - › Sending, receiving, listening, all consumes energy
- › Adaptation
  - › Reconfiguring when nodes join leave

6

# TDMA Overview

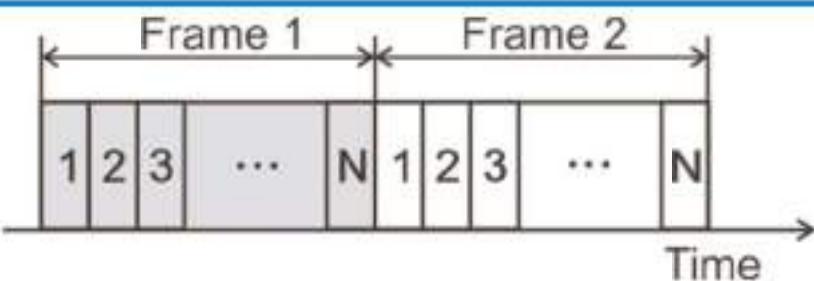
## Channel is divided into N slots (a frame)



- ▶ Each node gets a time slot
- ▶ It only transmits in its time slot
- ▶ It only need listen during its time slot
- ▶ Frame may be static – fix number of slots
- ▶ Frames may be dynamically adjusted
- ▶ Frequently used in cellular communications (i.e., GSM)

7

# TDMA for WSNs



## Often used in WSNs

- ▶ Typically, nodes communicate with base station
- ▶ Major advantage of TDMA – supports low-duty-cycle operations on nodes
  - ▶ Large frames
  - ▶ Nodes only have to listen in their time slot
- ▶ Low duty-cycle => low energy consumption

8

## TDMA Disadvantages for WSNs

---

- ▶ **Cluster paradigm (analogous to cell phones)**
- ▶ **One node is selected as the cluster head and acts as base station**
- ▶ **Nodes communicate only with head**
- ▶ **Direct peer-to-peer communication not energy efficient**
  - ▶ Nodes must listen on all time slots, reducing energy
- ▶ **Inter-cluster communication requires other MAC protocols**
- ▶ **Most important issue is limited scaling**
  - ▶ When a new nodes joins the base station must reallocate slots and adjusting the frame size
  - ▶ This can take time and energy to propagate

9

## Examples of Scheduled Protocols

---

- ▶ **Sohrabi & Pottie**
- ▶ **Low-Energy Adaptive Clustering Hierarchy (LEACH)**
  - ▶ Organize nodes into cluster hierarchies
  - ▶ TDMA within each cluster
  - ▶ Nodes only talk to node head
  - ▶ Position of head is rotated among nodes depending on remaining energy
  - ▶ Node then uses long-range/high-power communication to base
  - ▶ Nodes don't need to know global topology
  - ▶ Nodes don't need control information from base station

# Examples of Scheduled Protocols

---

## ► Bluetooth

- ▶ Designed for PAN, but attractive for WSNs
- ▶ Bluetooth organizes itself into clusters, piconets
- ▶ Frequency-hopping CDMA is used to handle inter-cluster interference
- ▶ Within cluster, TDMA MAC protocol
- ▶ Master-slave approach. Cluster head (master), other nodes are slaves.
- ▶ Master uses polling to decide which slave can transmit
- ▶ Only communication between master and one or more slaves are possible
- ▶ Maximum number of nodes in a cluster is 8

11

# Energy Conservation in Scheduled MAC Protocols

---

- ▶ Collision free
- ▶ No need for idle listening
- ▶ TDMA naturally support low-duty cycle operation

12

# Contention-Based MAC Protocols

---

- › Channel are not divided, but shared channel allocated on-demand
- › **Advantages**
  - › Scale easily across node density and load
  - › More flexible (no need to form clusters, hierarchies) peer-to-peer directly supported
  - › Don't require fine-grained synchronization as in TDMA
- › **Major disadvantage**
  - › Inefficient use of energy

13

## Review: Energy Efficiency in MAC Protocols

---

- › **What causes energy waste from a MAC perspective?**
  - › Collision
  - › Idle listening
  - › Overhearing
    - › When a node receives packets that are destined for another node
  - › Control packet overhead
    - › Sending, receiving, listening, all consumes energy
  - › Adaptation
    - › Reconfiguring when nodes join leave

14

## Examples of Contention MAC Protocols discussed

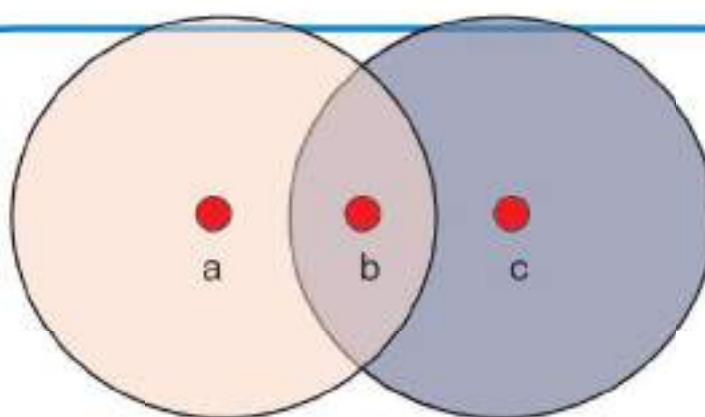
---

- ▶ ALOHA
- ▶ Slotted-ALOHA
- ▶ Carrier Sense Medium Access (CSMA)
  - ▶ Central idea – listen (carrier sense) before transmitting
- ▶ Variants
  - ▶ Non-persistent CSMA
    - ▶ If medium busy, wait random time and try again
  - ▶ 1-Persistent CSMA
    - ▶ If medium busy, keep listening and transmit when medium becomes free
  - ▶  $p$ -Persistent CSMA
    - ▶ If medium busy, transmit with probability  $(1-p)$ . If medium free transmit with probability  $p$ .

15

## Hidden Terminal Problem in CSMA

---



- ▶ Node a, b, and c can only hear their immediate neighbors
- ▶ When node a sends to b, c is unaware of a, its carrier sense indicates carrier free
- ▶ Node c starts transmitting
- ▶ Packets from a and c collide at b

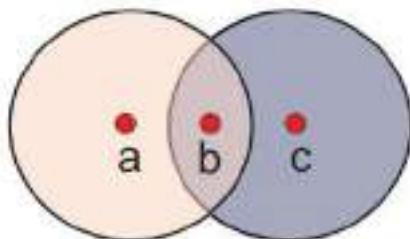
16

## CSMA/CA - Carrier Sense Collision Avoidance

---

- ▶ Establish a brief handshake between sender and receiver before sending data

- ▶ Sender sends Request-to-Send (RTS) packet to intended receiver
- ▶ Receiver replies with Clear-to-Send (CTS) packet
- ▶ Only then does transmitter send data



- ▶ RTS-CTS packets announce to neighbors
- ▶ Node c hears CTS packets from b to a, and does not transmit
- ▶ Does not eliminate collisions, but collisions are now mostly (brief) RST

17

## Variations

---

- ▶ MACA – RST and CTS packets indicate size on data so other nodes know how long to back off
- ▶ MACAW – adds an Acknowledge ACK packet
  - ▶ RTS-CTS-DATA-ACK
- ▶ IEEE 802.11
  - ▶ CSMA/CA, MACA, and MACAW => Distributed coordination function (DCF) + enhancements

18

# Energy Conservation in Contention Protocols

---

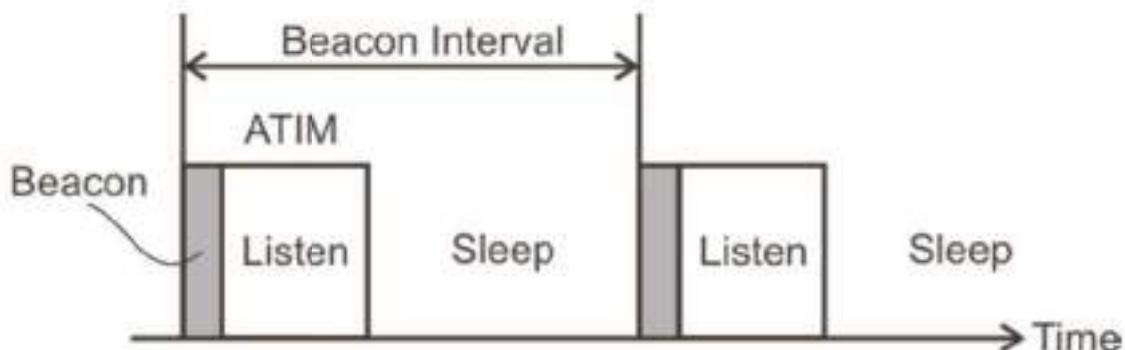
- › Basic idea, put radio to sleep with it is not used
- › This makes it difficult for nodes to communicate
- › Beacons
- › Coordinate sleeping (frames)

19

## Beacons (IEEE 802.11 & Piconet)

---

- › One node periodically broadcast beacon (all participate)
- › Beacon synchronizes all nodes
- › After each beacon, ad hoc traffic indication message (ATIM).
- › All nodes are awake during ATIM
- › Then CSMA



- › Assumption: all nodes can hear each other. Generalizing to multi-hop is not easy

20

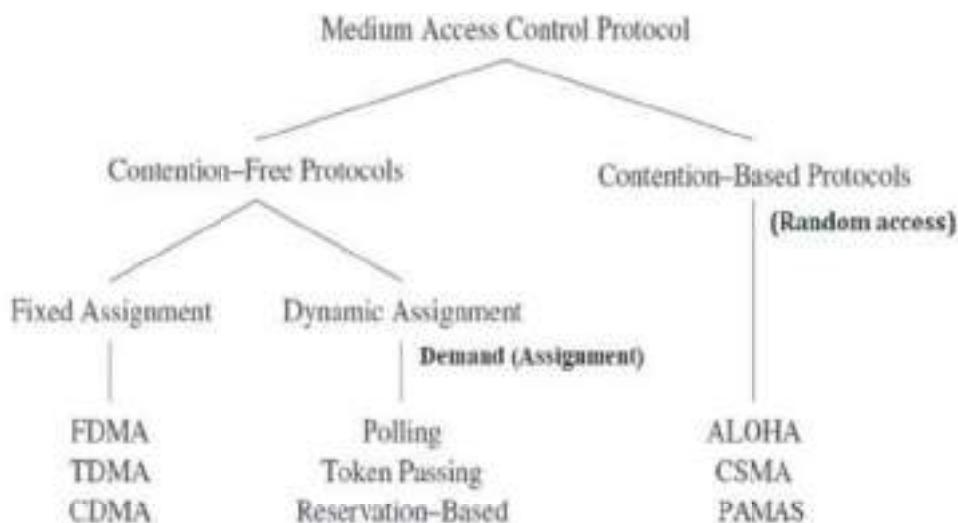
# WSN MAC Protocols

---

## Important classes of MAC protocols

A huge number of (wireless) MAC protocols have been devised during the last thirty years. They can be roughly classified into the following classes:

- Fixed assignment protocols,
- Demand assignment protocols,
- Random access protocols.



CS 442 WSN Unit-4

## PAMAS protocol (Power Aware Multi-access with Signaling)

---

- The PAMAS protocol is originally designed for ad hoc networks.
- It provides a detailed overhearing avoidance mechanism while it does not consider the idle listening problem.
- The protocol combines the busy-tone solution and RTS/CTS handshake.
- Uses two channels: a **data channel** and a **control channel**.
- All the signaling packets (RTS, CTS, busy tones) are transmitted on the control channel, while the data channel is reserved for data packets.
- PAMAS conserves battery power by selectively powering off nodes that are not actively transmitting or receiving packets.

## PAMAS protocol (Power Aware Multi-access with Signaling)

---

### Initiating a data transfer

- A PAMAS device sends an RTS message over the control channel to the receiver.
- Receiver responds with CTS if it does not detect activity on the data channel and has not overheard other recent RTS or CTS messages.
- If the source does not receive a CTS within a specific timeout interval, it will attempt to transmit again after a back-off time (exponential back-off algorithm).
- Otherwise, it begins data transmission and the receiver node issues a busy tone over the control channel (whose length is greater than twice the length of CTS).

23

## PAMAS protocol (Power Aware Multi-access with Signaling)

---

- Every node in a PAMAS network independently decides when to power off its transceiver.
- Specifically, a node decides to turn off its transceiver whenever one of two conditions holds:
  - a neighbor begins a transmission and the node has no frames to transmit.
  - a neighbor transmits a frame to another neighbor, even if the node has frames to transmit.
- A node can easily detect either condition by
  - Overhearing its neighbor's transmissions (condition 1) or
  - Overhearing its neighbor's busy tone (condition 2).
- A node can identify how long to power down its transceiver by embedding the size or expected transmission duration into messages

24

# PAMAS protocol and Channel Probing

---

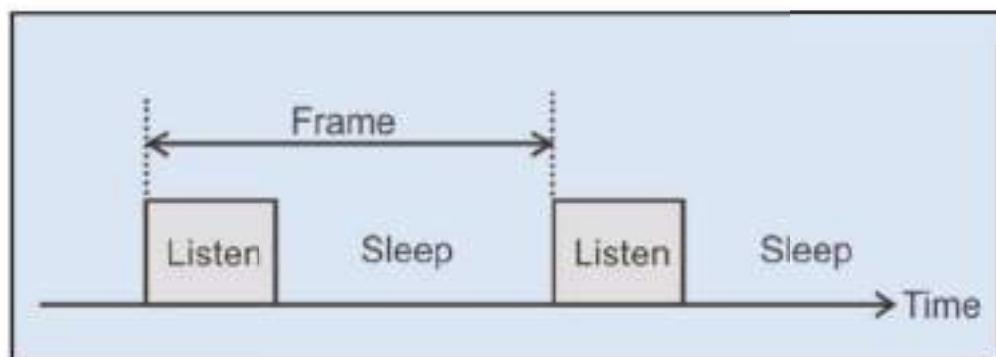
- ▶ Two channels
  - ▶ Data
  - ▶ Control
- ▶ Upon wakeup, probe control channel for activity related to destination node
  - ▶ Neighbor answer probe? Yes, go back to sleep
- ▶ Probing eliminated interference with transmission in data channel
- ▶ More complex to implement (two channels)
- ▶ PAMAS does not reduce idle listening.

25

## S-MAC

---

- ▶ Specifically designed for WSN
- ▶ Reduces energy from all major sources
  - ▶ Idle listening, collision, overhearing and control overhead
- ▶ Course-grained sleep/wakeup cycle

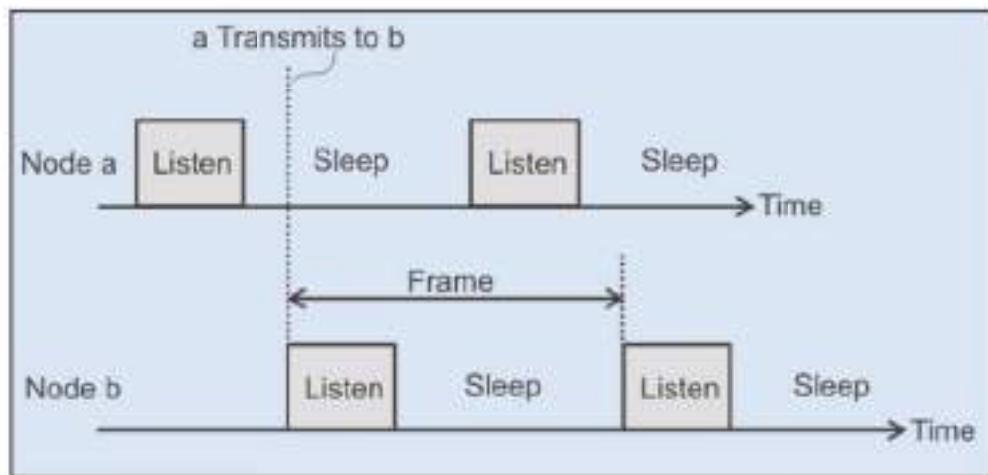


- ▶ Each node has its own wakeup-listen (communicate), sleep schedule
- ▶ Schedules are shared with neighbors

26

## S-MAC Scheduling

- › All nodes choose their own schedules
- › Share schedules with neighbors
- › Node then schedule transmissions during listen times of neighbors



- › If a wants to send to b, it just waits for b's listen cycle to start

27

## S-MAC Scheduling

- › Nodes periodically broadcast SYNC packets to synchronize clocks
- › S-MAC encourages neighbors to adopt identical schedules
  - › When it configures itself, a node listens for a synchronization period, and adopts the first schedule it hears
  - › Nodes periodically does *neighbor discovery*, by listening for an entire frame
- › 1-10% Duty cycle

28

## S-MAC Data Transmission

---

- Contention happens only during listen interval
- S-MAC puts a duration field in *each packet* (some other protocols have it only at the start)
  - Nodes that don't have medium access, know how long to sleep even if they try to gain medium access in the middle of an ongoing conversation
- Application-Level Message Passing
  - Only one RTS and CTS for all fragments
  - Each fragment has ACK (which also contains duration)
  - Reserves medium
  - Burst mode
  - Aids in-network processing in WSNs
- Variation Adaptive Listening
  - Rather than wait until the next scheduled listen interval, nodes wake up immediately after RTS-CTS-DATA-ACK

29

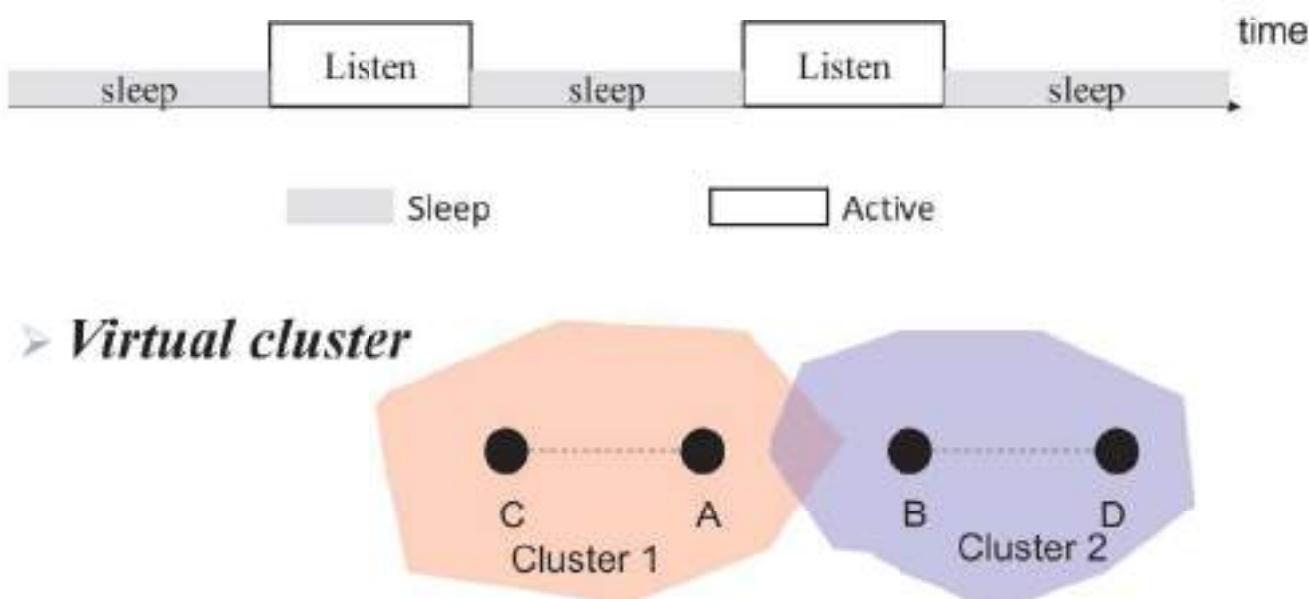
## S-MAC

---

- Designed for reduce energy consumption and support self-configuration
- To reduce energy consumption in listening to an idle channel, nodes *periodically sleep*
- Neighboring nodes form *virtual clusters* to auto-synchronize on sleep schedules
- S-MAC applies *message passing* to reduce contention latency for sensor-network applications

## S-MAC : Virtual cluster

- Locally managed synchronizations periodic sleep-listen schedules



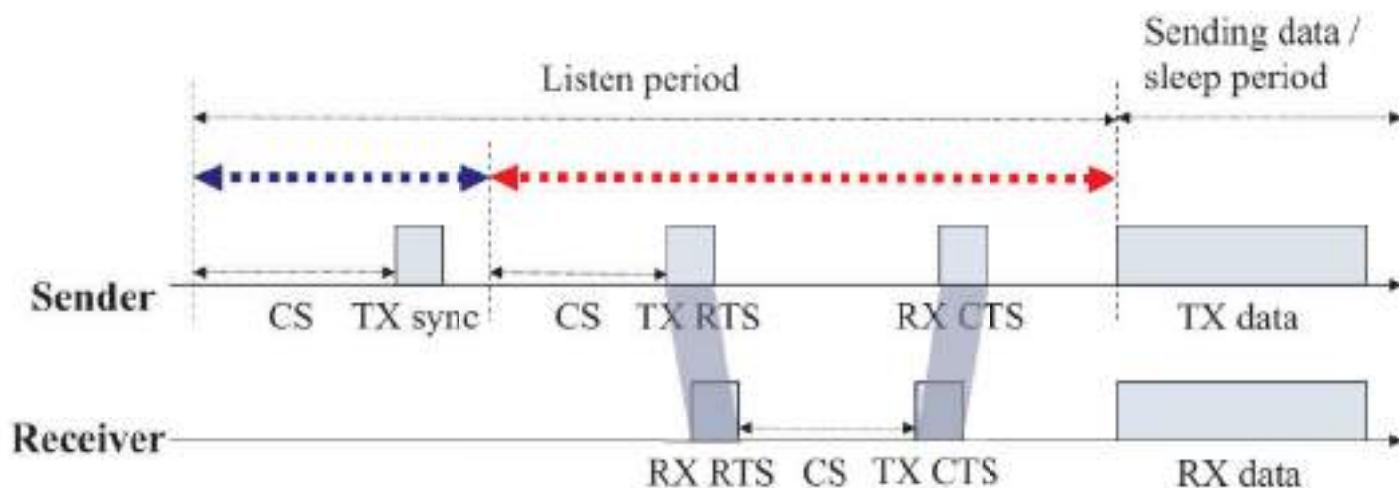
## S-MAC

- Every node should wakeup in Listen period

↳ Synchronization period

↳ Control period (RTS/CTS)

※ Node use CSMA before sending any packet



# S-MAC

---

## ➤ Adaptive-Listening

- Node who overhears its neighbor's transmissions (ideally only RTS or CTS) **wake up** for a short period of time at the **end of the data transmission**.
- If the node is the next-hop node => remain active after data transmission, prepare to forwarding its neighbor's message.
- If the node does not receive anything during the adaptive listening => go back to sleep.

## S-MAC-Summary

---

### ➤ Locally time synchronization between neighbors

### ➤ Power saving method:

- Fixed wakeup/sleep interval

### ➤ Transmit Characteristic:

- Contention transmission through CSMA

## S-MAC-Summary

---

### ➤ Advantage

- Idle listening is reduced by sleep schedules
- Time synchronization overhead may be prevented by sleep schedule announcements

### ➤ Disadvantage

- Adaptive listening incurs overhearing or idle listening
- Sleep and listen periods are predefined and constant

## S-MAC Pros and Cons

---

### ➤ Cons

- Relatively Complex (especially since CSMA is often touted as being simple...)
- Increased Latency

### ➤ Pros

- Periodic sleep provides excellent energy performance at light loads
- Adaptive listen adjusts to traffic to achieve same performance as no-sleep at heavy load

## S-MAC-Summary

---

### ➤ Advantage

- Idle listening is reduced by sleep schedules
- Time synchronization overhead may be prevented by sleep schedule announcements

### ➤ Disadvantage

- Adaptive listening incurs overhearing or idle listening
- Sleep and listen periods are predefined and constant

## S-MAC Pros and Cons

---

### ➤ Cons

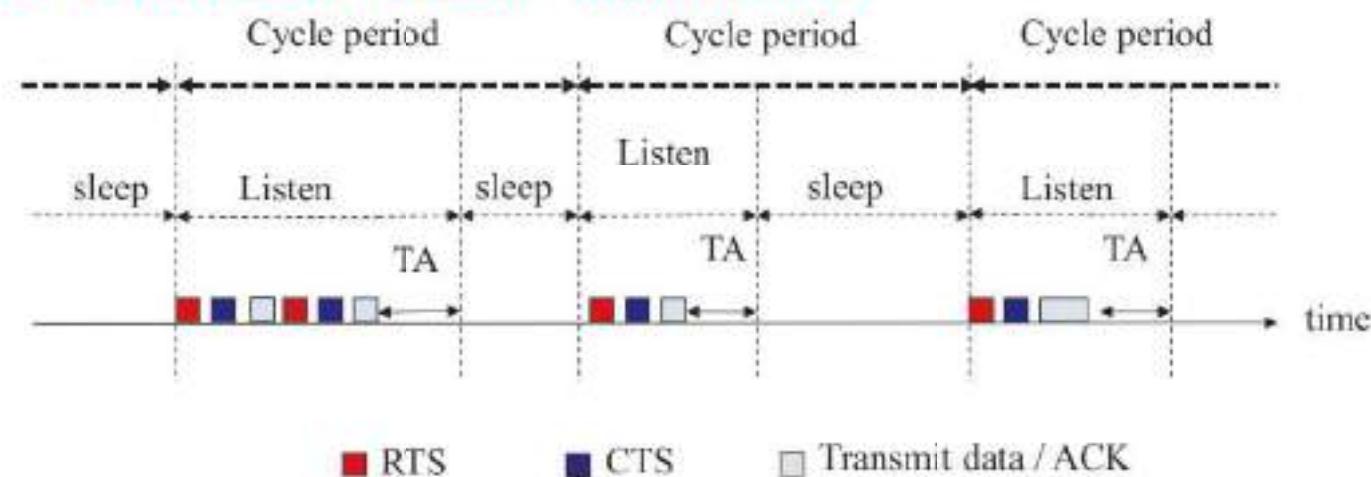
- Relatively Complex (especially since CSMA is often touted as being simple...)
- Increased Latency

### ➤ Pros

- Periodic sleep provides excellent energy performance at light loads
- Adaptive listen adjusts to traffic to achieve same performance as no-sleep at heavy load

## Timeout T-MAC

- Improvement of S-MAC
- T-MAC have variable “Listen Period”



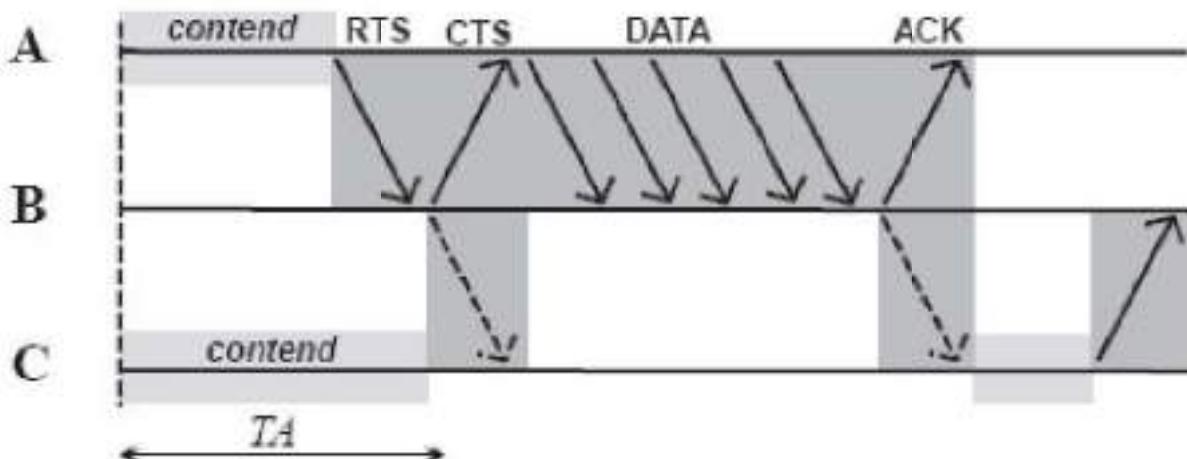
- The listen period ends when no activation event has occurred for a time threshold  $TA$

## Timeout T-MAC

- Improve the idle listening problem of the fixed duty cycle solution, such like S-MAC
- T-MAC protocol is to reduce idle listening by transmitting all messages in *bursts of variable* length, and sleeping between bursts
- An *adaptive duty cycle* in a novel way: by dynamically ending the active part of it

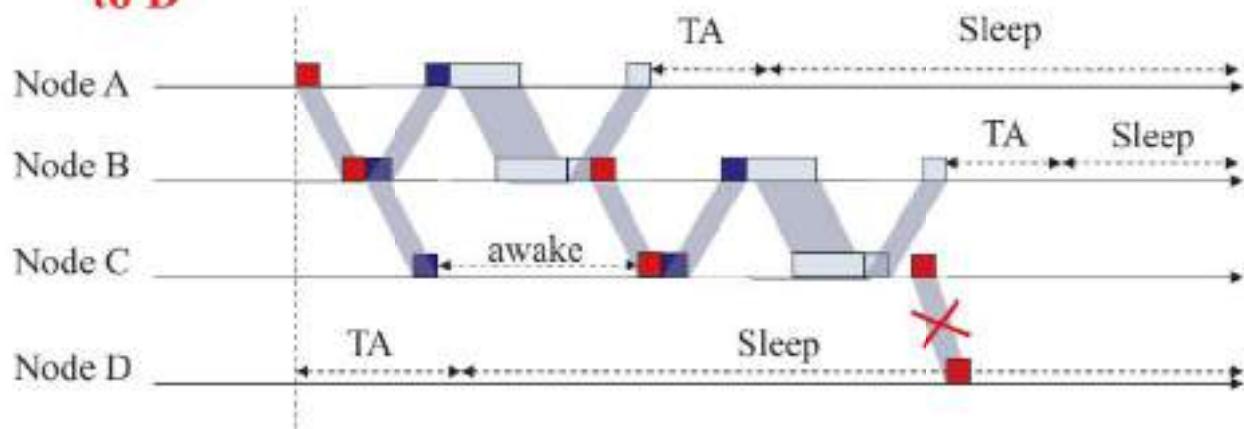
# Timeout T-MAC

$$TA = 1.5 (T_{contention\ interval} + T_{RTS} + T_{RTS2CTS})$$



# Timeout T-MAC

- The data forwarding problem
  - Early sleeping problem, consider the case that A sends data to D



When node D go sleeping before C forward data, the data transmission process may delay to next cycle.

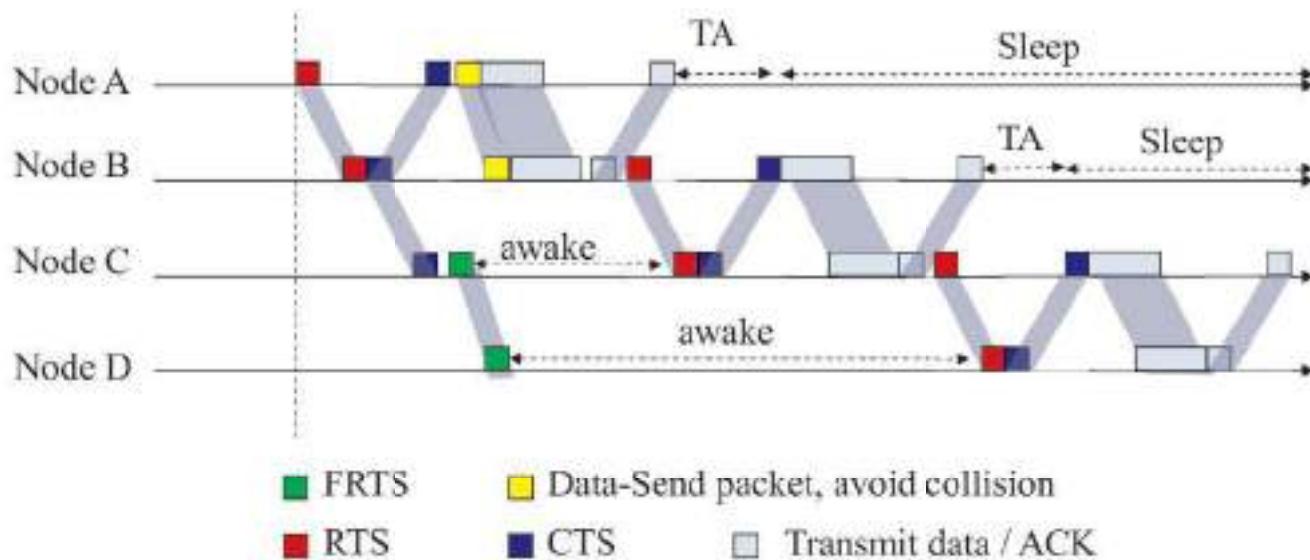
■ RTS

■ CTS

■ Transmit data / ACK

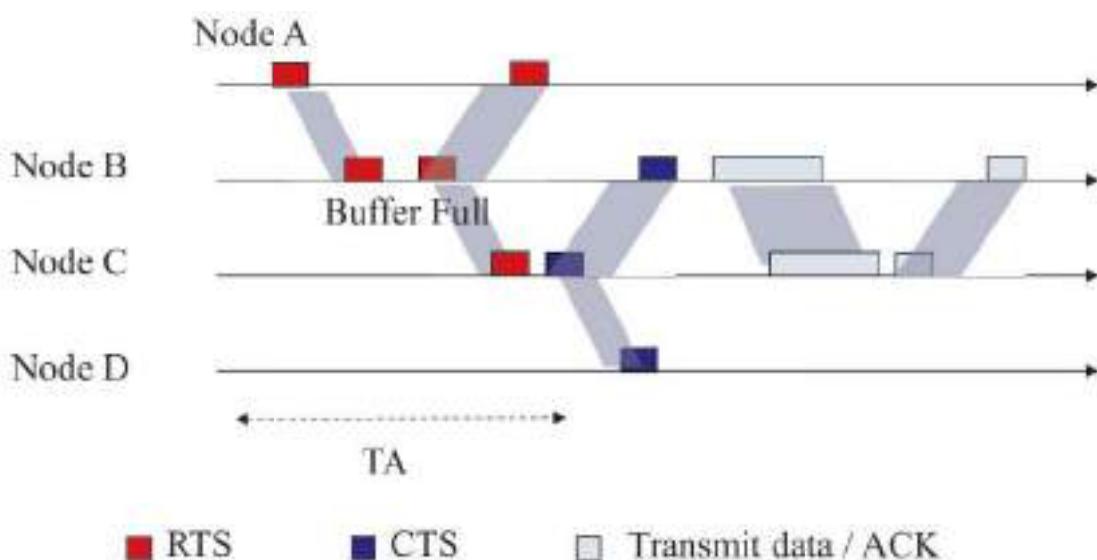
## Timeout T-MAC

- Solution of early sleeping problem
  - Future request-to-send (FRTS)
  - Forwarding node uses FRTS awake next hop node and destination node



## Timeout T-MAC

- Taking priority on full buffers
  - When a node's transmit/routing buffers are almost full, it may prefer sending than receiving



## **Timeout T-MAC-Summary**

---

- Locally time synchronization between neighbors
- Power saving method:
  - Dynamic wakeup/sleep interval
- Transmit Characteristic:
  - Contention transmission through CSMA

## **Timeout T-MAC**

---

- Advantage
  - Enhance the poor results of the S-MAC protocol under variable traffic loads
- Disadvantage
  - Early sleeping problem
  - Higher latency than S-MAC

## B-MAC

---

- **B-MAC Goals :**
  - Low Power operation
  - Effective collision avoidance
  - Simple implementation
  - Small code size and RAM usage
  - Efficient channel utilization at low & high data rates
  - Scalable to large numbers of nodes
  - ...
- **B-MAC employs an adaptive **preamble sampling** scheme to reduce duty cycle and minimize idle listening**

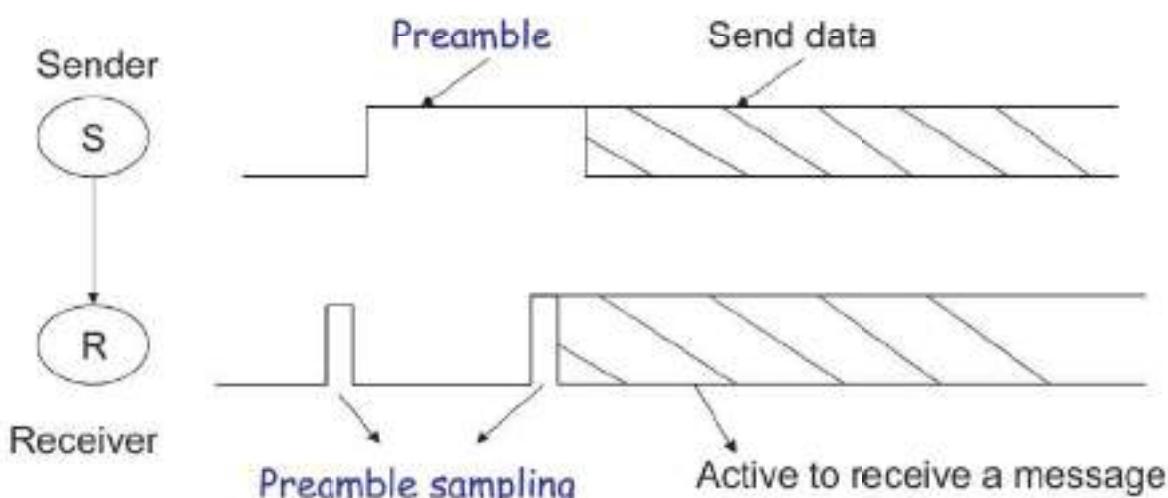
## B-MAC

---

- **Low power listening (LPL)**
  - Goal: minimize listen cost
  - Nodes periodically wakeup at every cycle check if preamble signals
  - If signal is detected, node powers up in order to receive the packet
  - **Sender use long preamble to notify receiver**
  - Sender and receiver turn off radios after data receive or time-out

## Low Power Listening: Preamble Sampling

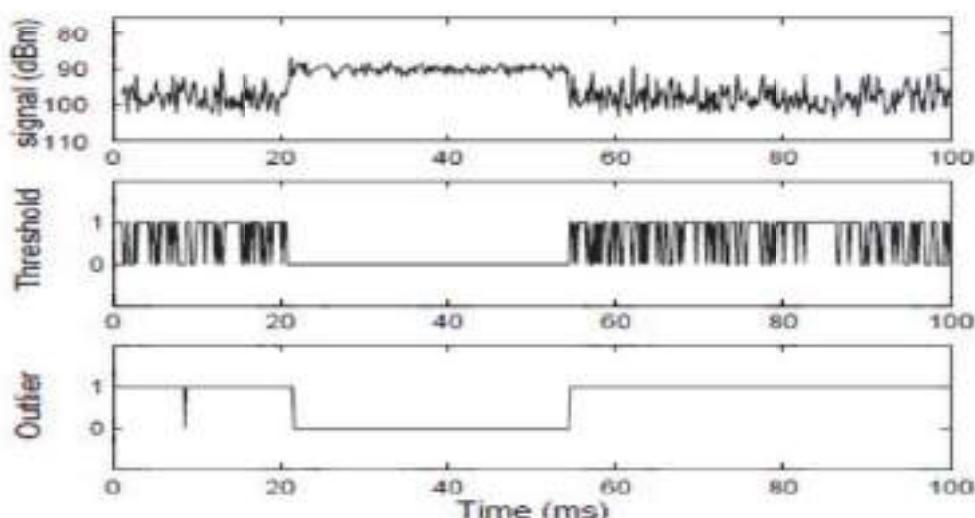
- ▶ Preamble is not a packet but a physical layer RF pulse
  - ▶ Minimize overhead



|Preamble| ≥ Sampling period

## B-MAC

- ▶ Clear channel assessment (CCA)
  - ▶ CCA effectiveness for a typical wireless channel
  - ▶ CCA is used to determine the state of the medium

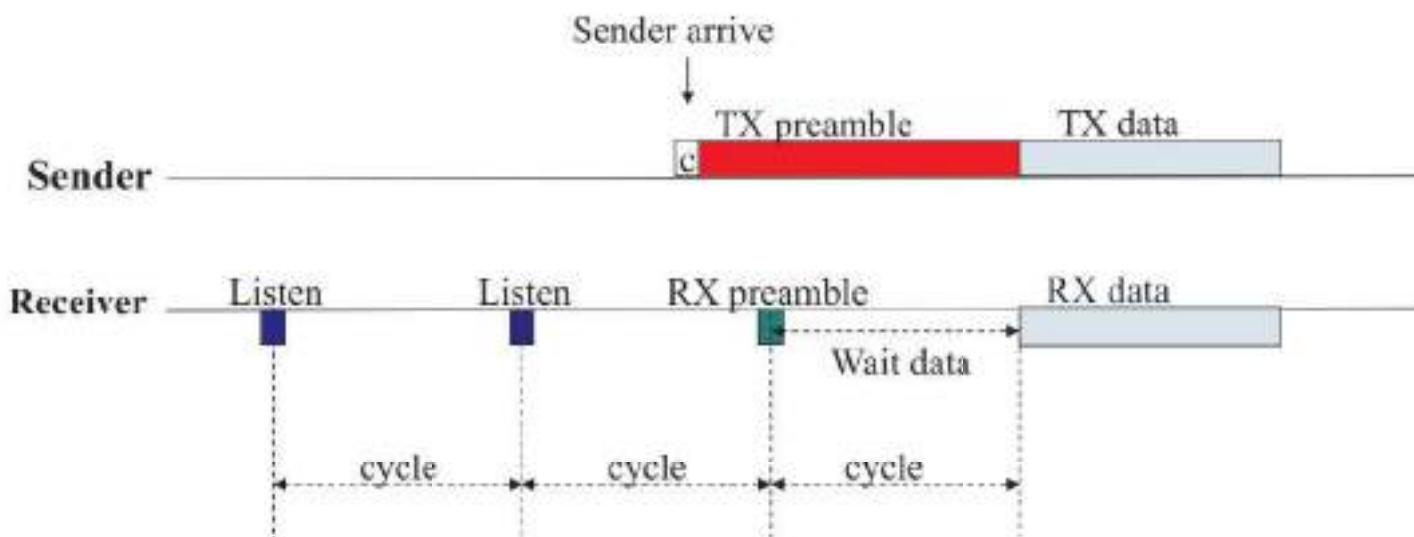


0=busy, 1=clear, Packet arrives between 22 and 54 ms

## B-MAC

---

- ▶ Check if any preamble signal
- ▶ Clear channel assessment (CCA)
  - Before transmit, adapts to noise floor by sampling channel when it is assumed to be free



## B-MAC- Summary

---

- ▶ B-MAC is a non-time-synchronization method, it uses a long enough preamble to notify the receiver.
- ▶ Power saving method:
  - Self-defined wakeup/sleep interval
  - Long preamble notification
- ▶ Transmit Characteristic:
  - Contention method through Clear Channel Assessment algorithm

## **B-MAC- Summary**

---

### › **Advantage**

- Doesn't need any synchronization
- RTS/CTS (optional)
- Clean and simple interface

### › **Disadvantage**

- Transmission delay will be long
- Bad performance when heavy traffic load

## **B-MAC- Summary**

---

### ► **Advantage**

- Doesn't need any synchronization
- RTS/CTS (optional)
- Clean and simple interface

### ► **Disadvantage**

- Transmission delay will be long
- Bad performance when heavy traffic load

## **Traffic-Adaptive Medium Access Protocol- TRAMA**

---

- TRAMA reduces energy consumption by ensuring that unicast and broadcast transmissions incur no collisions
- TRAMA assumes that time is slotted and divides time into random access periods and schedule access periods
- TRAMA avoids assigning time slots to nodes with no traffic to send

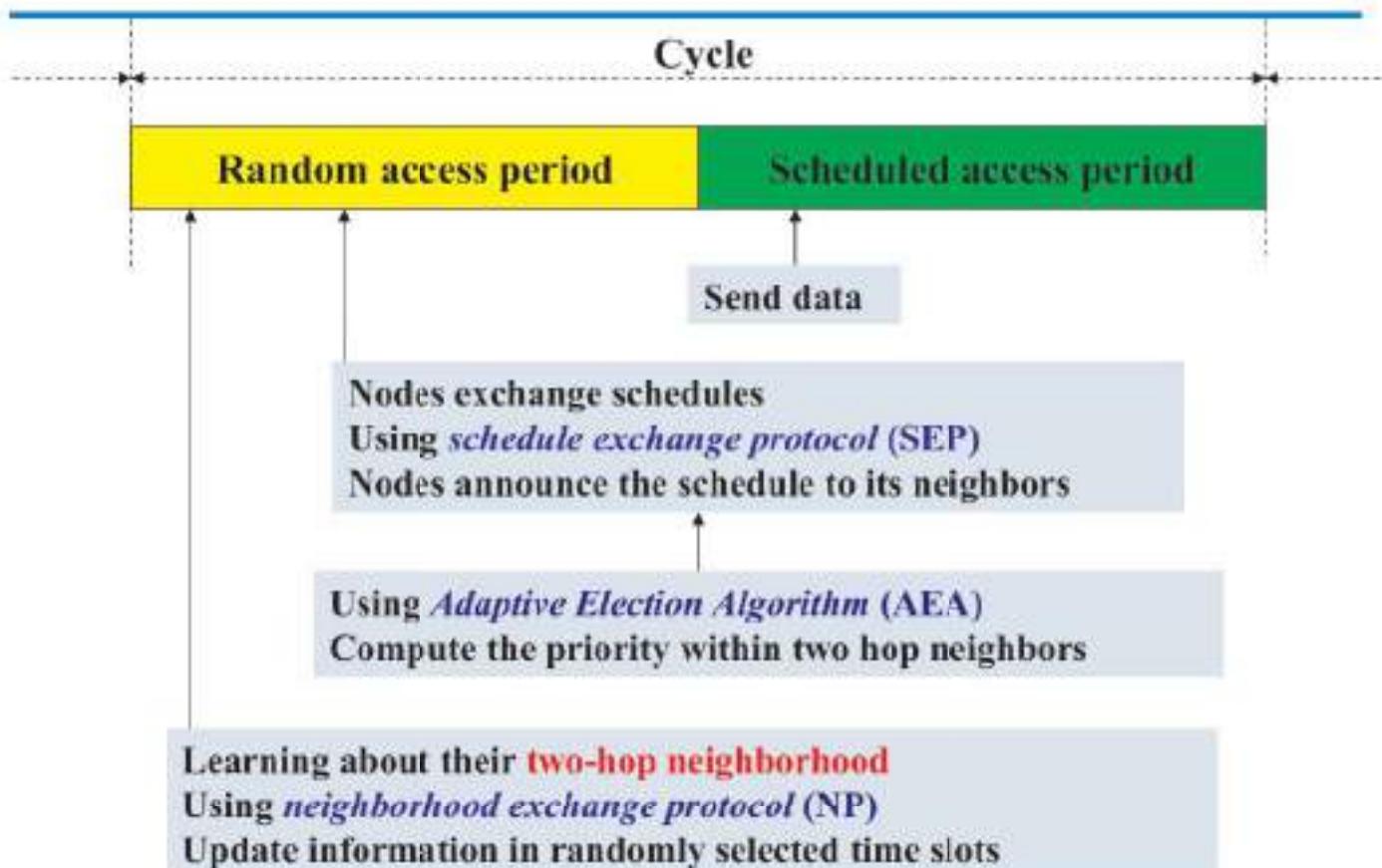
# TRAMA

---

- ▶ Nodes need globally synchronized
- ▶ Time divided into:
  - Random access periods
  - Scheduled access periods
- ▶ Three main protocols:
  - Neighbor Protocol (NP)
  - Adaptive Election Algorithm (AEA)
  - Schedule Exchange Protocol (SEP)

# TRAMA

---



## TRAMA

---

- ▶ **Neighborhood Exchange Protocol**
  - A node picks randomly a number of time slots and transmits small control packets in these without carrier sensing
  - These packets contain incremental neighbor information, that is only those neighbors that belong to new neighbors or neighbors missing during the last cycle
- ▶ **Schedule Exchange Protocol**
  - A node transmits its current transmission schedule and also picks up its neighbors' schedules

## TRAMA

---

- **Schedule Exchange Protocol**
  - Each node compute the length of ***SCHEDULE\_INTERVAL*** based on the rate at which packets are produced by higher layer application
  - Nodes use **AEA** algorithm pre-compute the number of slots in time interval **[ $t, t + SCHEDULE\_INTERVAL]$**
  - Node select the highest priority slots in the duration of ***SCHEDULE\_INTERVAL*** as its transmitting slots
  - Node uses its last transmitting slot in this duration, to announce its next schedule by looking ahead the next ***SCHEDULE\_INTERVAL***
  - Nodes announce their schedule via schedule packets

## TRAMA

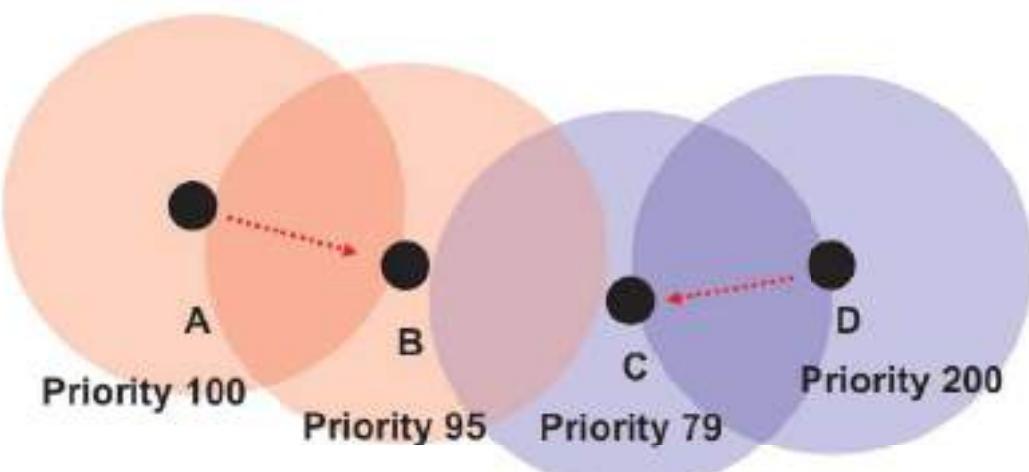
---

- ▶ How Adaptive Election Algorithm (AEA) to decide which slot a node can use in scheduled access period?
  - Use node identifier  $x$
  - Use globally known hash function  $h$
  - For a time slot  $t$ , compute
    - ✓ priority  $p = h(x \text{ XOR } t)$
  - Compute this priority for next  $k$  time slots for node itself and all two-hop neighbors
  - Node uses those time slots for which it has the highest priority

## TRAMA

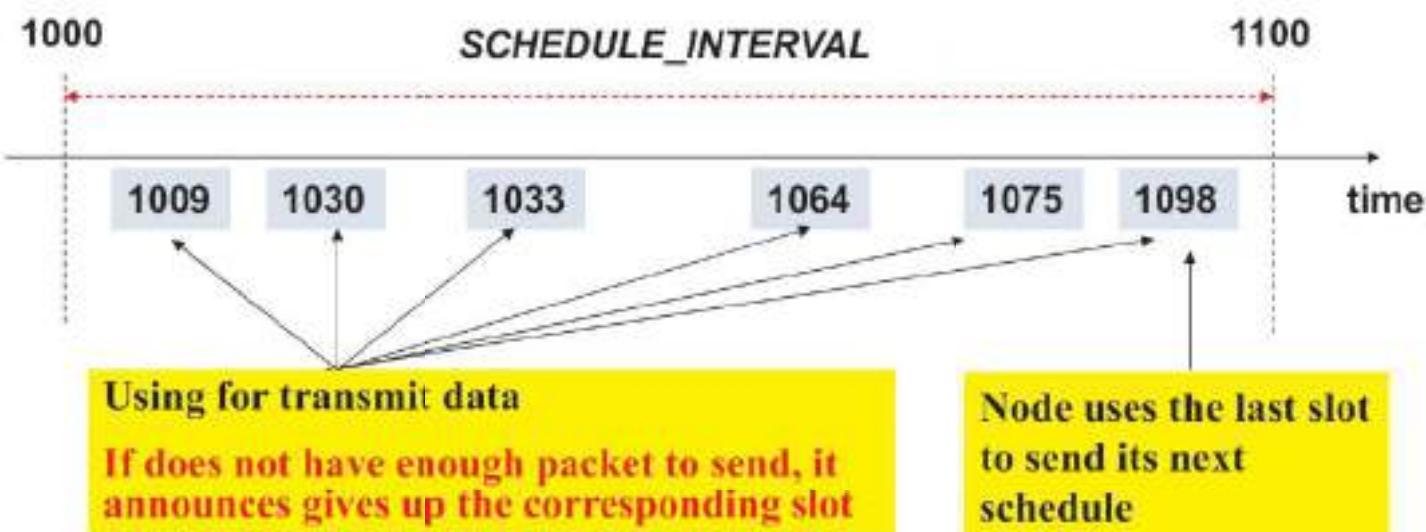
---

- ▶ For example
  - Both  $A$  and  $D$  could transmit in the timeslot because they have the highest priority in their two hop neighbors



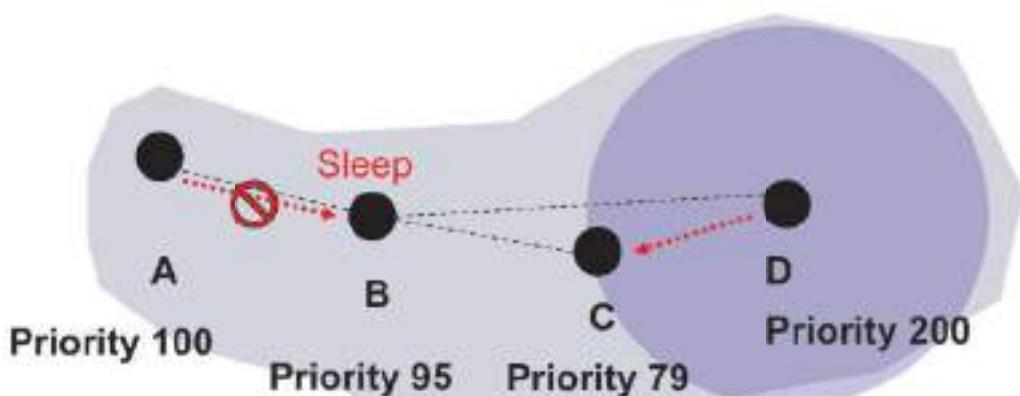
TRAMA

- ▶ During time slot is 1000
  - ▶ When *SCHEDULE\_INTERVAL* is 100
  - ▶ The node need to compute the transmitting slots between [1000, 1100]



TRAMA

- ▶ Inconsistency problem
    - ▶ If  $B$  looks at its schedule information and  $D$  will transmit data to  $C$ ,  $B$  switch to sleep mode.
      - ▶  $B$  will end up missing  $A$ 's transmission



## TRAMA

---

### ► Solution of Inconsistency Problem

- Node B will denote node A as **Alternate Winner** if node A want to transmit data to node B
- If **Alternate Winner** and the **Absolute Winner** (node D) are not interfered for each other then both nodes can transmit concurrently

## TRAMA- Summary

---

### ■ Global synchronized time slot

### ► Power saving method:

- Higher percentage of sleep time and less collision probability is achieved compared to CSMA based protocols

### ► Transmit Characteristic:

- Contention-Free TDMA
- Adaptive Election Algorithm decide transmission

## TRAMA- Summary

---

### ► Advantages

- Only use two hop neighbor information can decide transmission priority
- Higher percentage of sleep time, less collision probability and higher maximum throughput than contention-based S-MAC

### ► Disadvantages

- Higher delay problem
- Substantial memory/CPU requirements for schedule computation

## DMAC

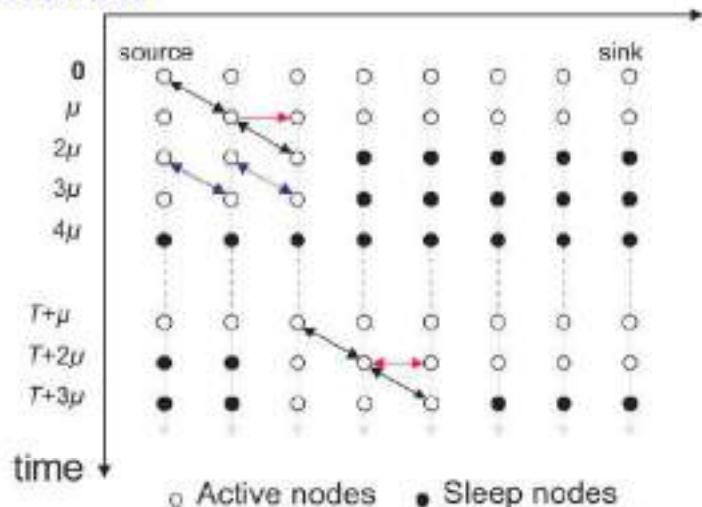
---

- DMAC achieves very low latency for convergecast communications
  - DMAC could be summarized as an improved Slotted Aloha algorithm in which slots are assigned to the sets of nodes based on a data gathering tree
  - DMAC also adjusts the duty cycles adaptively according to the traffic load in the network

DMAC

### ■ The data forwarding interruption problem (DFI)

- Only the next hop of receiver can overhear the data transmission
  - Nodes out of hearing range will sleep until next cycle/interval

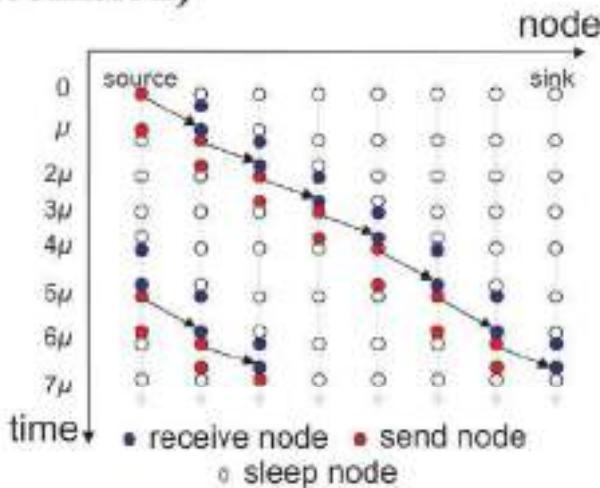
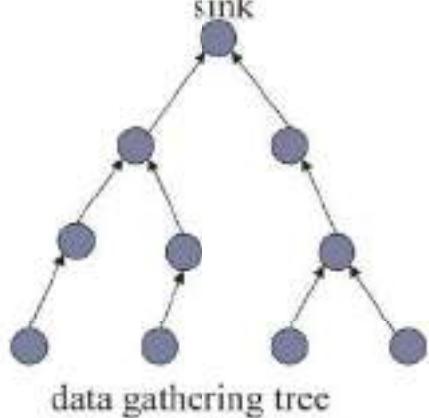


### In S-MAC, DFI causes sleep delay

DMAC

### ➤ Staggered Wakeup Schedule

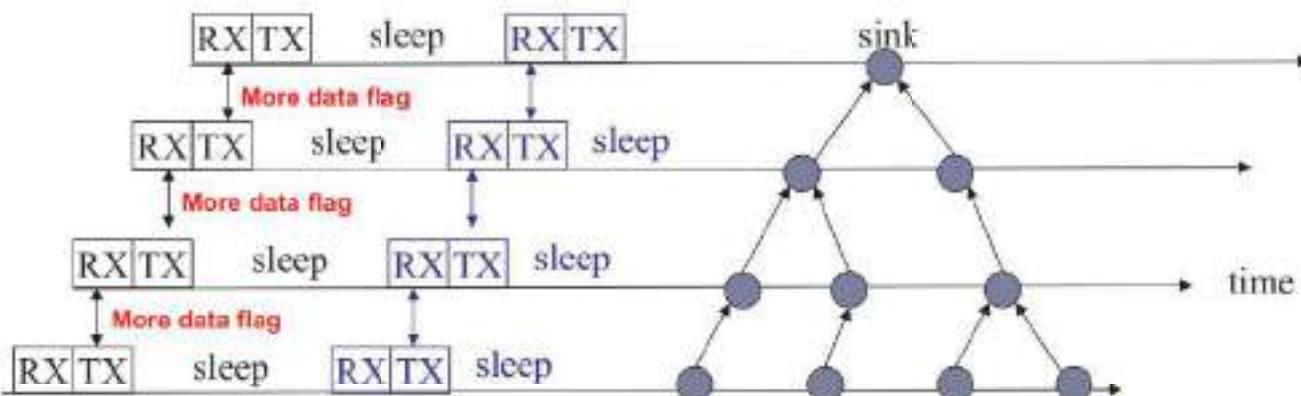
- Data gathering from sensor nodes to sink by data gathering tree
  - Nodes on multi-hop path to wake-up sequentially like a chain reaction (a node will only send one packet every  $5\mu$ s in DMAC in order to avoid collision)



# DMAC

---

- When nodes has multiple packets to send
  - DMAC use slot-by-slot mechanism
  - Piggyback a more data flag in MAC header
  - Node not active at next slot, but schedule a  $3\mu$  sleep then goes to receiving state.



## DMAC-Summary

---

- Need external time synchronized in prescribe area
- Power saving method:
  - Sleep schedule of a node an offset that depends upon its depth on the tree
- Transmit Characteristic:
  - Improved Slotted Aloha algorithm
  - Contention-Free slots are assigned based on a data gathering tree

## DMAC-Summary

---

### ► Advantage:

- DMAC achieves very good latency compared to other sleep/listen period assignment methods

### ► Disadvantage

- Collision avoidance methods are not utilized, if number of nodes that have the same schedule try to send to the same node, collisions will occur

## MAC compare

---

	Time sync needed	Type	Adaptive to changes
S-MAC/ T-MAC	No	CSMA	Good
B-MAC	No	CSMA/CCA	Good
TRAMA	Yes	TDMA/CSMA	Good
DMAC	Yes	TDMA/ Slotted Aloha	Weak
LEACH	Yes	TDMA/CDMA	Weak

## References

1. Ilker Demirkol, Cem Ersoy, Fatih Alagöz , "MAC Protocols for Wireless Sensor Networks: A Survey," Communications Magazine, IEEE , April 2006
2. Deborah Estrin, John Heidemann, and Wei Ye, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks,"IEEE INFOCOM 2002.
3. W. Ye, J. Heidemann, and D. Estrin, "Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks," IEEE/ACM Trans. Net. 2004 ,
4. Koen Langendoen and Tijs van Dam, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks," The First ACM Conference on Embedded Networked Sensor Systems (Sensys & 03), pp. 171–180, 2003
5. DavidCuller, JasonHill, and JosephPolastre, "Versatile Low Power Media Access for Wireless Sensor Networks," the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys), November 3-5, 2004
6. A. El-Hoiydi, "Spatial TDMA and CSMA with Preamble Sampling for Low Power Ad Hoc Wireless Sensor Networks," Proc. ISCC 2002
7. C. C. Enz *et al.*, "WiseNET: An Ultralow-Power Wireless Sensor Network Solution," *IEEE Comp.*, vol. 37, no. 8, Aug. 2004.
8. V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy-Efficient, Collision-Free Medium Access Control for Wireless Sensor Networks," Proc. ACM SenSys '03, Los Angeles, CA, Nov. 2003, pp. 181–92.
9. W. Rabiner Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocols for Wireless Microsensor Networks," Hawaii International Conference on System Sciences (HICSS '00), January 2000.
10. G. Lu, B. Krishnamachari, and C. S. Raghavendra, "An Adaptive Energy-Efficient and Low-Latency MAC for Data Gathering in Wireless Sensor Networks," Proc. 18th Int'l. Parallel and Distrib. Processing Symp., Apr.2004, p. 224.
11. Holger KarlAndreas Willig , "Protocols and architectures for wireless sensor networks,"

# Channel correction Mechanisms

- Forward error correction (we see now)
- Adaptive equalization (We'll see shortly)
- Adaptive modulation and coding (We'll see shortly)
- Diversity techniques and MIMO (We'll see shortly)
- OFDM (We have seen)
- Spread spectrum techniques (We have seen)
- Bandwidth expansion (We'll see shortly)

CS 442 WSN U2

## Bit level error detection/correction

Single-bit, multi-bit or burst errors introduced due to channel noise

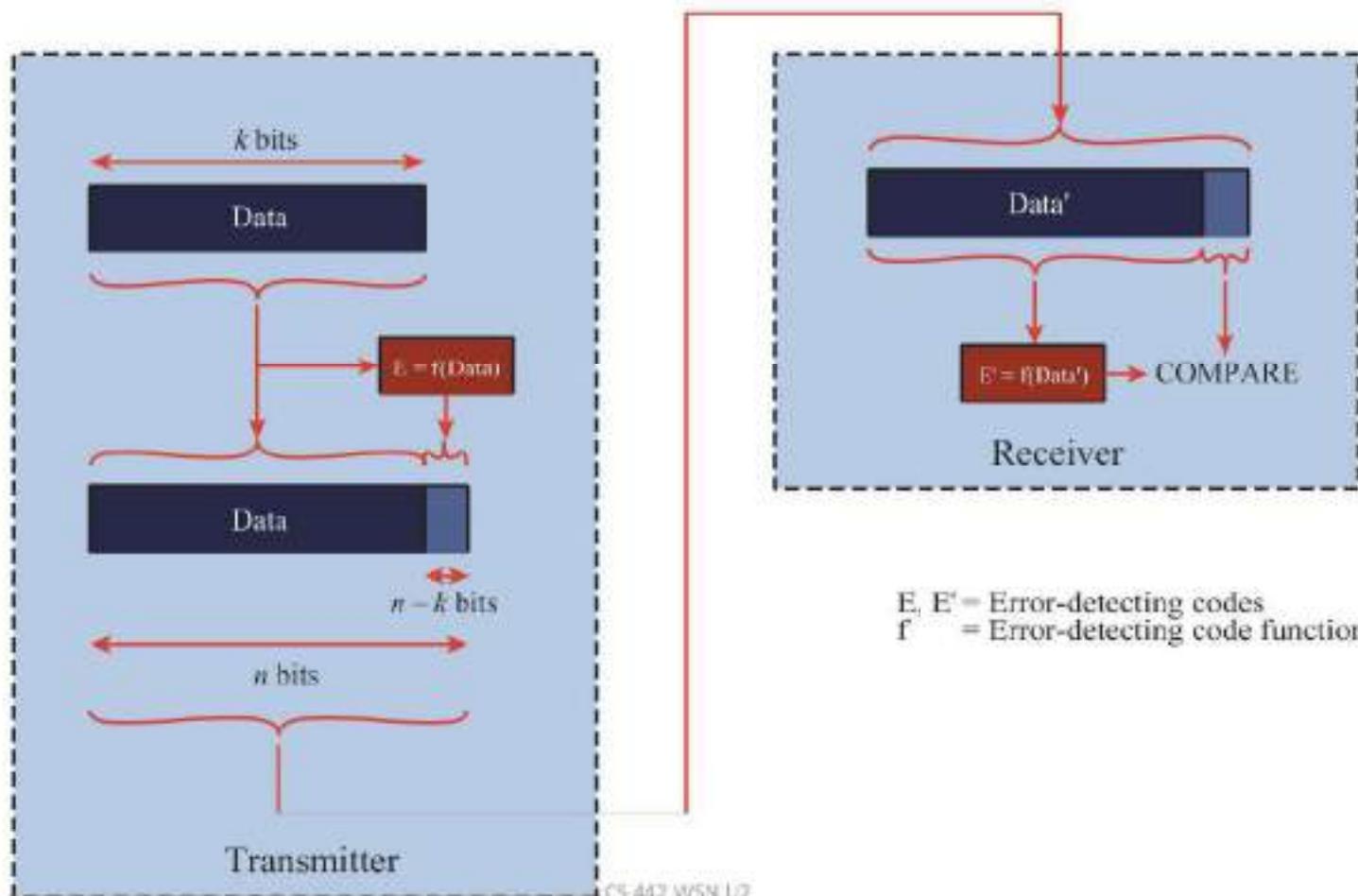
- Detected using redundant information sent along with data
- Full Redundancy:
  - Send everything twice
  - Simple but inefficient
- Common Schemes:
  - Parity
  - Cyclic Redundancy Check (CRC)
  - Checksum

# Error Detection Process

- Transmitter
  - For a given frame, an error-detecting code (check bits) is calculated from data bits
  - Check bits are appended to data bits
- Receiver
  - Separates incoming frame into data bits and check bits
  - Calculates check bits from received data bits
  - Compares calculated check bits against received check bits
  - Detected error occurs if mismatch

CS-442 WSN L2

## Error Detection Process



CS-442 WSN L2

# Parity Check

- Parity bit appended to a block of data
- Even parity
  - Added bit ensures an even number of 1s
- Odd parity
  - Added bit ensures an odd number of 1s
- Example, 7-bit character [1110001]
  - Even parity [11100010]
  - Odd parity [11100011]

CS-442 WSN I/2

# Cyclic Redundancy Check (CRC)

- Transmitter
  - For a  $k$ -bit block, transmitter generates an  $(n-k)$ -bit frame check sequence (FCS)
  - Resulting frame of  $n$  bits is exactly divisible by predetermined number
- Receiver
  - Divides incoming frame by predetermined number
  - If no remainder, assumes no error

CS-442 WSN I/2

# Wireless Transmission Errors

- Error detection requires retransmission
- Detection is inadequate for wireless applications
  - Error rate on wireless link can be high, results in a large number of retransmissions
  - Long propagation delay compared to transmission time

CS 442 WSN U2

## Frame level error correction

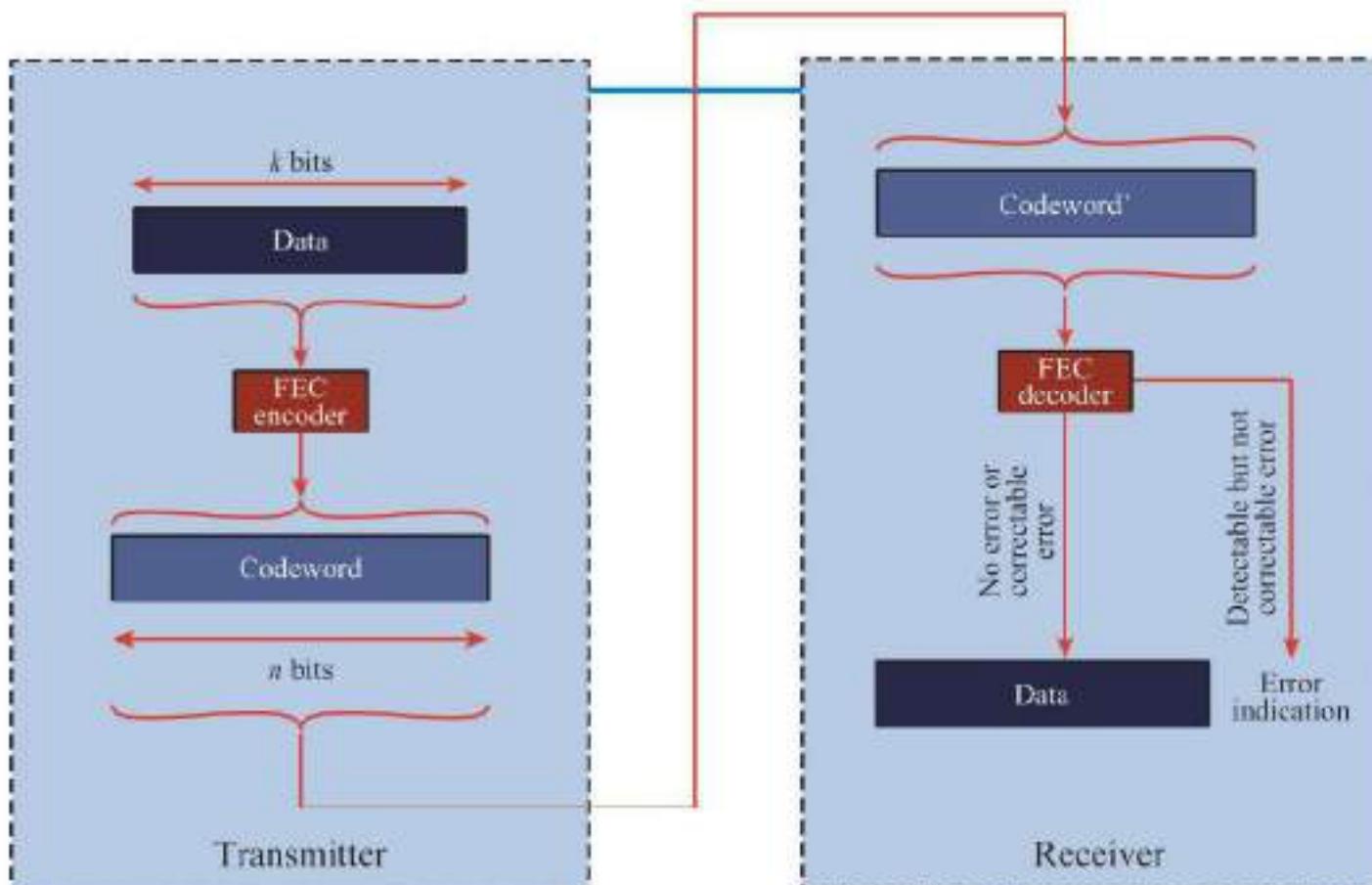
- Problems in transmitting a sequence of frames over a lossy link
  - frame damage, loss, reordering, duplication, insertion
- Solutions:
  - Forward Error Correction (FEC)
    - Use of redundancy for packet level error correction
    - Block Codes, Turbo Codes
  - Automatic Repeat Request (ARQ)
    - Use of acknowledgements and retransmission
    - Stop and Wait; Sliding Window

# Block Error Correction Codes

- Transmitter
  - Forward error correction (FEC) encoder maps each  $k$ -bit block into an  $n$ -bit block codeword
  - Codeword is transmitted; analog for wireless transmission
- Receiver
  - Incoming signal is demodulated
  - Block passed through an FEC decoder

CS 442 WSN U2

## Forward Error Correction Process



# FEC Decoder Outcomes

- No errors present
  - Codeword produced by decoder matches original codeword
- Decoder detects and corrects bit errors
- Decoder detects but cannot correct bit errors; reports uncorrectable error
- Decoder incorrectly corrects bit errors
  - Error pattern looks like a different block of data was sent
- Decoder detects no bit errors, though errors are present

CS-442 WSN I/2

# Block Code Principles

- Hamming distance – for 2  $n$ -bit binary sequences, the number of different bits
  - E.g.,  $v_1=011011$ ;  $v_2=110001$ ;  $d(v_1, v_2)=3$
- Redundancy – ratio of redundant bits to data bits
- Code rate – ratio of data bits to total bits
- Coding gain – the reduction in the required  $E_b/N_0$  to achieve a specified BER of an error-correcting coded system

CS-442 WSN I/2

# Decoding process

- Coding table

Data block	Codeword
00	00000
01	00111
10	11001
11	11110

- Received: 00100
  - Not valid, error is detected
  - Correction?
    - One bit away from 00000
    - Two bits away from 00111
    - Three bits away from 11110
    - Four bits away from 11001
  - Most likely 00000 was sent, assume data was 00
    - But others could have been sent, albeit much less likely

CS-442 WSN I/2

# Decoding process

- Received: 01100
  - Two bits from 00000
  - Two bits from 11110
  - No other codes closer
  - Cannot decode. Only know bit errors are detected

Efficient version: Turbo Codes

CS-442 WSN I/2

# Automatic Repeat Request (ARQ)

- Mechanism used in data link control and transport protocols
- Relies on use of an error detection code (such as CRC)
- Flow Control
- Error Control

CS-442 WSN I/2

## Flow Control

- Reasons for breaking up a block of data before transmitting:
  - Limited buffer size of receiver
  - Retransmission of PDU due to error requires smaller amounts of data to be retransmitted
  - On shared medium, larger PDUs occupy medium for extended period, causing delays at other sending stations

CS-442 WSN I/2

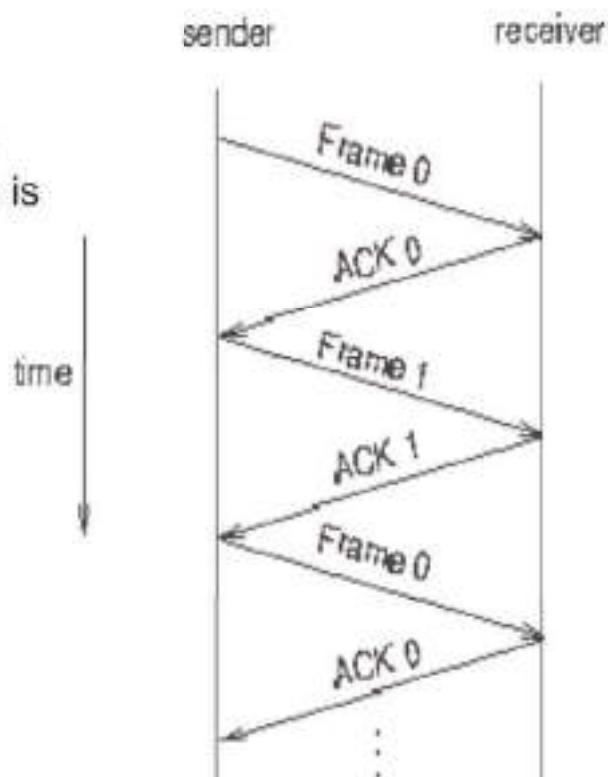
# Flow Control

- Assures that transmitting entity does not overwhelm a receiving entity with data
- Protocols with flow control mechanism allow multiple PDUs in transit at the same time
- PDUs arrive in same order they're sent
- Sliding-window flow control
  - Transmitter maintains list (window) of sequence numbers allowed to send
  - Receiver maintains list allowed to receive

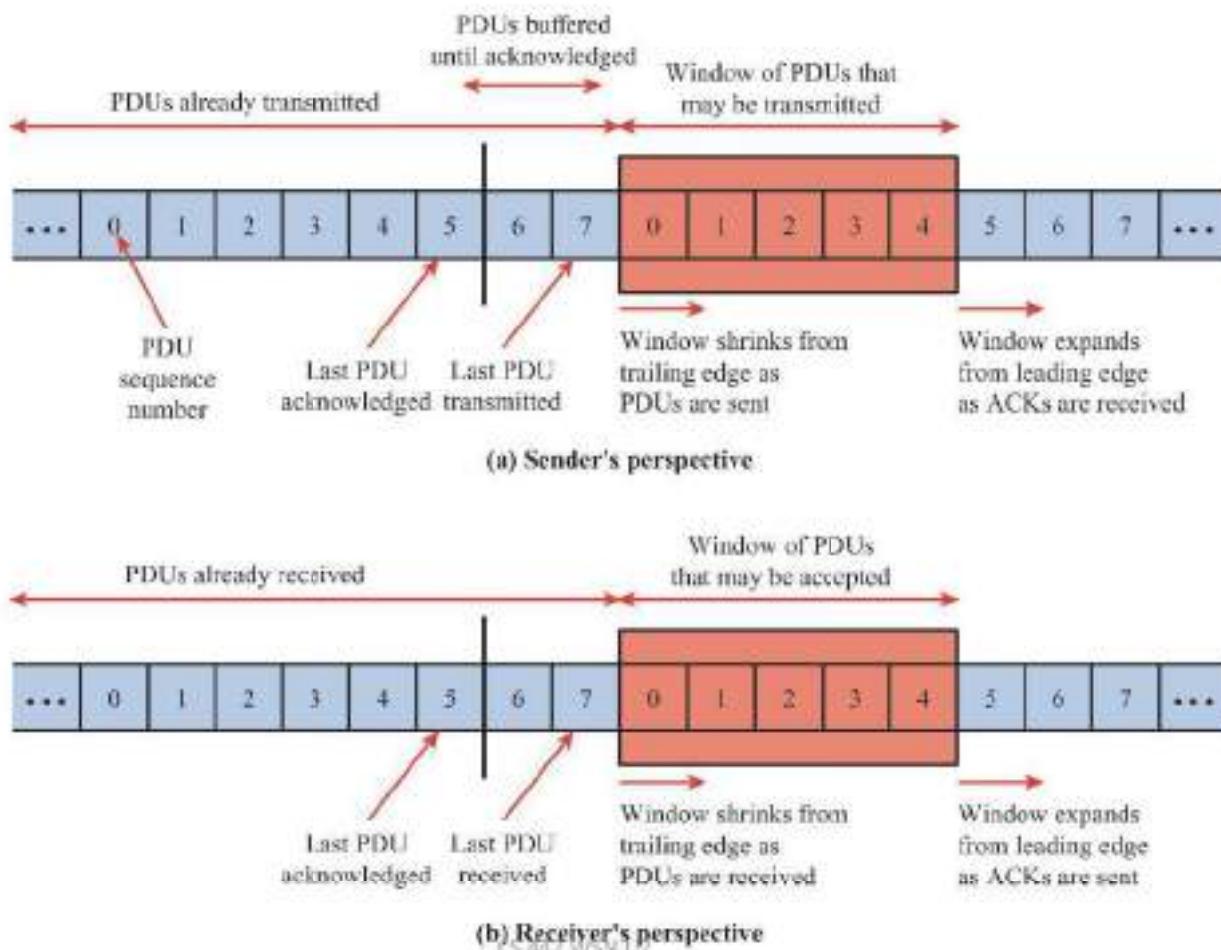
CS 442 WSN U2

## Stop and Wait ARQ

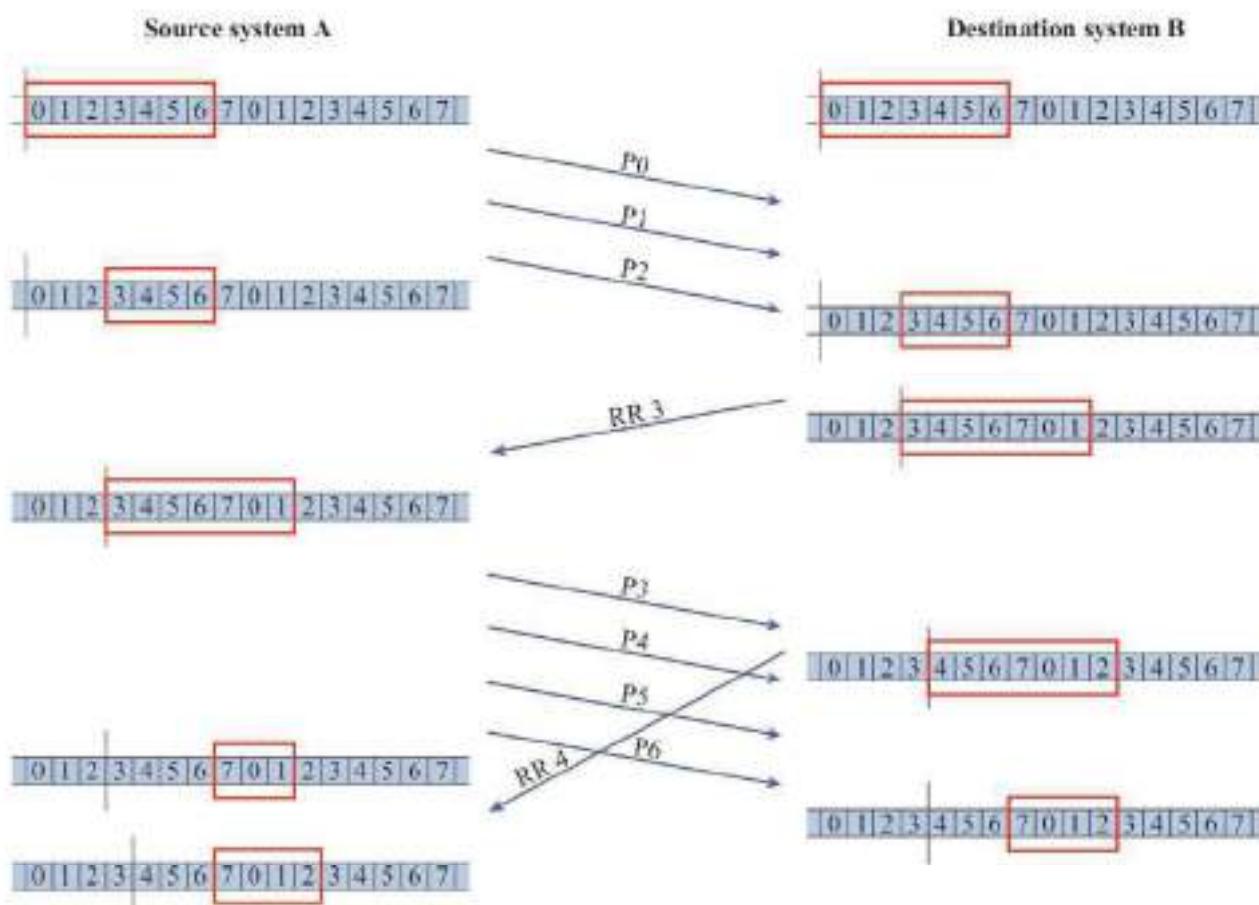
- Sender waits for ACK (acknowledgement) after transmitting each frame; keeps copy of last frame.
- Receiver sends ACK if received frame is error free.
- Sender retransmits frame if ACK not received before timer expires.
- Simple to implement but may waste bandwidth.
- Efficient Version: Sliding Window



## Sliding-Window Depiction



## Example of a Sliding-Window ARQ Protocol

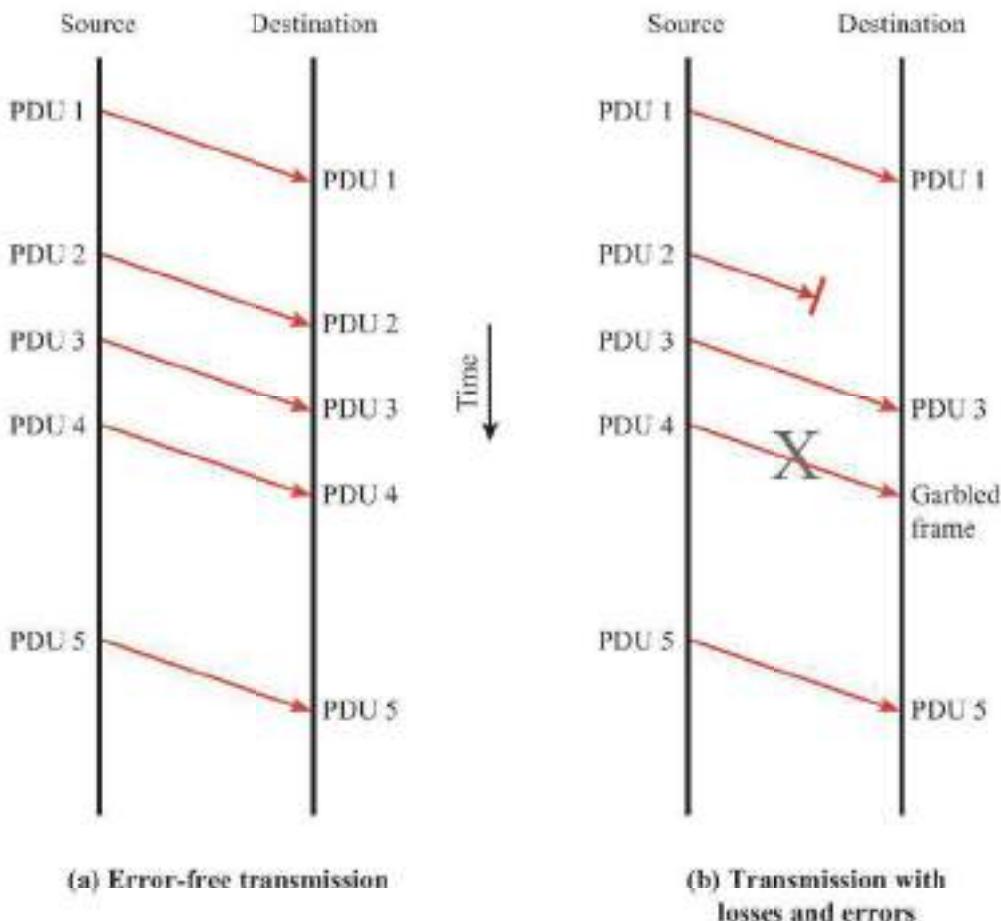


# Error Control

- Mechanisms to detect and correct transmission errors
- Types of errors:
  - Lost PDU : a PDU fails to arrive
  - Damaged PDU : PDU arrives with errors

CS-442 WSN I/2

## PDU Transmission Model



CS-442 WSN I/2

# Error Control Requirements

- Error detection
  - Receiver detects errors and discards PDUs
- Positive acknowledgement
  - Destination returns acknowledgment of received, error-free PDUs
- Retransmission after timeout
  - Source retransmits unacknowledged PDU
- Negative acknowledgement and retransmission
  - Destination returns negative acknowledgment to PDUs in error

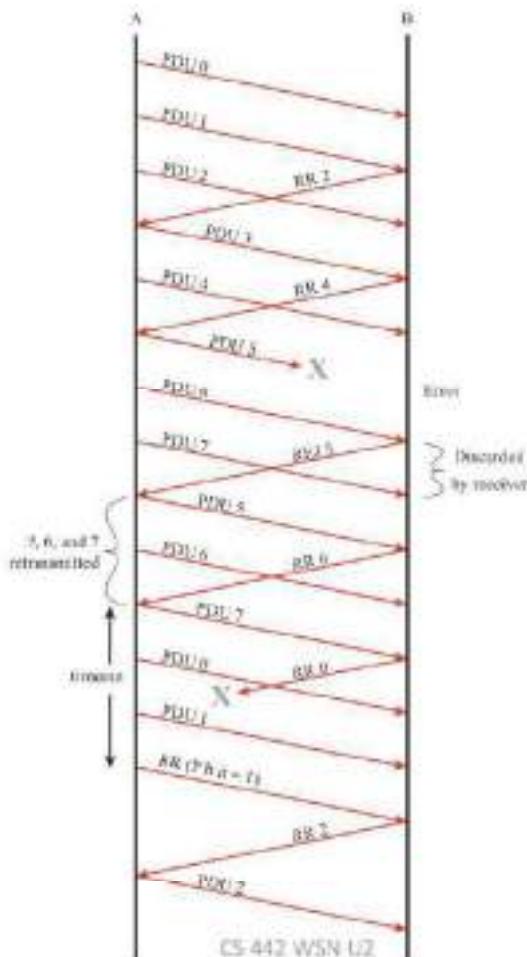
CS-442 WSN I/2

## Go-back-N ARQ

- Acknowledgments
  - RR = receive ready (no errors occur)
  - REJ = reject (error detected)
- Contingencies
  - Damaged PDU
  - Damaged RR
  - Damaged REJ

CS-442 WSN I/2

## Go-back-N ARQ



## HYBRID ARQ

- Hybrid Automatic Repeat Request (HARQ)
  - Neither FEC or ARQ is adequate in practical situations
    - FEC may add unnecessary redundancy
    - ARQ may cause excessive delays from retransmissions
  - HARQ is widely used
  - Uses combination of FEC and ARQ

# Channel correction Mechanisms

- Forward error correction (We have seen)
- Adaptive equalization (we see now)
- Adaptive modulation and coding (we see now)
- Diversity techniques and MIMO (we see now)
- OFDM (We have seen)
- Spread spectrum techniques (We have seen)
- Bandwidth expansion (we see now)

# Channel correction Mechanisms

- Forward error correction (We have seen)
- Adaptive equalization
- Adaptive modulation and coding (we see now)
- Diversity techniques and MIMO
- OFDM (We have seen)
- Spread spectrum techniques (We have seen)
- Bandwidth expansion

CS-442 WSN I/2

## Adaptive modulation and coding (AMC)

- Modulation : formats the signal to best transmit bits
  - To overcome noise
  - To transmit as many bits as possible
- Coding : detects and corrects errors
- AMC adapts to channel conditions
  - 100's of times per second
  - Measures channel conditions
  - Sends messages between transmitter and receiver to coordinate changes

CS-442 WSN I/2

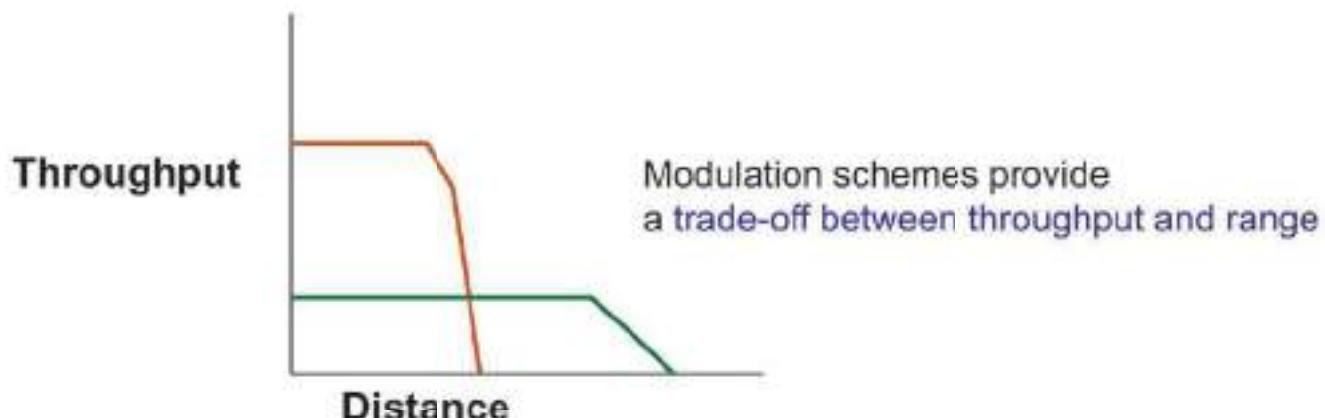
# Adaptive Modulation

- Channel conditions are time-varying
- Received signal-to-noise ratio changes with time



# Adaptive Modulation

- Multi-rate radios are capable of transmitting at several rates, using different modulation schemes
- Choose modulation scheme as a function of channel conditions



# Adaptive Modulation

- If physical layer chooses the modulation scheme transparent to MAC
  - MAC cannot know the time duration required for the transfer
- Must involve MAC protocol in deciding the modulation scheme
  - Some implementations use a sender-based scheme for this purpose [Kamerman97]
  - Receiver-based schemes can perform better [Holland01mobicom]

## Sender-Based "Autorate Fallback" [Kamerman97]

- Probing mechanisms
- Sender decreases bit rate after X consecutive transmission attempts fail
- Sender increases bit rate after Y consecutive transmission attempt succeed

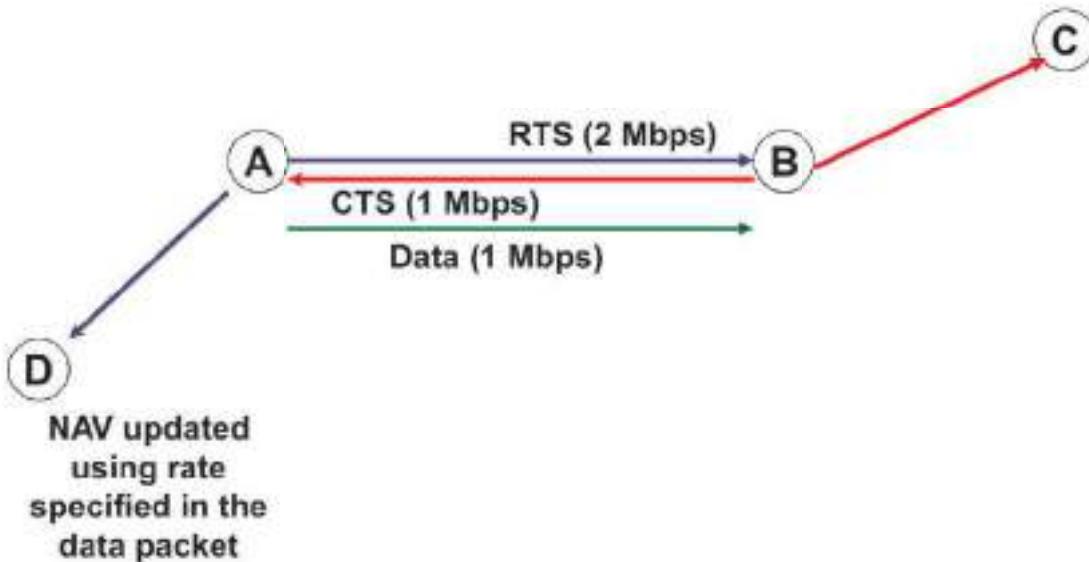
## Autorate Fallback

- Advantage
  - Can be implemented at the sender, without making any changes to the 802.11 standard specification
- Disadvantage
  - Probing mechanism does not accurately detect channel state
  - Channel state detected more accurately at the receiver
  - Performance can suffer
    - Since the sender will periodically try to send at a rate higher than optimal
    - Also, when channel conditions improve, the rate is not increased immediately

## Receiver-Based Autorate MAC [Holland01mobicom]

- Sender sends RTS containing its best rate estimate
- Receiver chooses best rate for the conditions and sends it in the CTS
- Sender transmits DATA packet at new rate
- Information in data packet header implicitly updates nodes that heard old rate

# Receiver-Based Autorate MAC Protocol



## Channel correction Mechanisms

- Forward error correction (We have seen)
- Adaptive equalization (we see now)
- Adaptive modulation and coding (We have seen)
- Diversity techniques and MIMO (we see now)
- OFDM (We have seen)
- Spread spectrum techniques (We have seen)
- Bandwidth expansion (we see now)

# Channel correction Mechanisms

- Forward error correction (We have seen)
- Adaptive equalization (we see now)
- Adaptive modulation and coding (we see now)
- Diversity techniques and MIMO (we see now)
- OFDM (We have seen)
- Spread spectrum techniques (We have seen)
- Bandwidth expansion (we see now)

CS-442 WSN I/2

## Adaptive Equalization

- Can be applied to transmissions that carry analog or digital information
  - Analog voice or video
  - Digital data, digitized voice or video
- Used to combat intersymbol interference
- Involves gathering dispersed symbol energy back into its original time interval
- Techniques
  - Lumped analog circuits
  - Sophisticated digital signal processing algorithms

CS-442 WSN I/2

# Diversity Techniques

- Diversity is based on the fact that individual channels experience independent fading events
- Space diversity – techniques involving physical transmission path, spacing antennas
- Frequency diversity – techniques where the signal is spread out over a larger frequency bandwidth or carried on multiple frequency carriers
- Time diversity – techniques aimed at spreading the data out over time
- Use of diversity
  - Selection diversity – select the best signal
  - Combining diversity – combine the signals

CS-442 WSN I/2

## MULTIPLE INPUT MULTIPLE OUTPUT (MIMO) ANTENNAS

- Use antenna arrays for
  - Diversity – different signals from different antennas
  - Multiple streams – parallel data streams
  - Beamforming – directional antennas
  - Multi-user MIMO – directional beams to multiple simultaneous users
- Modern systems
  - $4 \times 4$  (4 transmitter and 4 receiver antennas)
  - $8 \times 8$
  - Two dimensional arrays of 64 antennas
  - Future: Massive MIMO with many more antennas

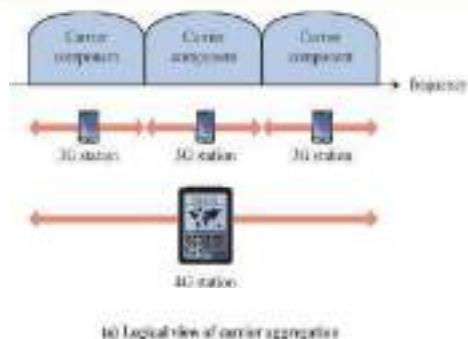
CS-442 WSN I/2

# Bandwidth expansion

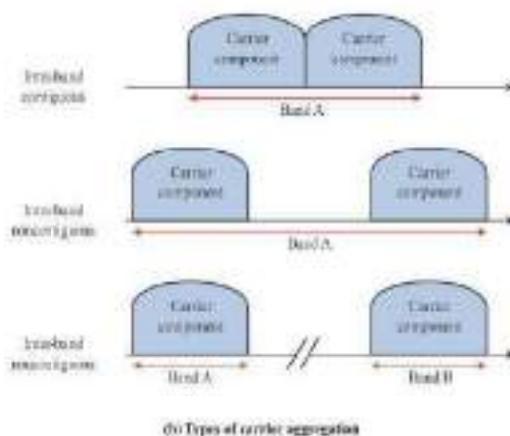
- A signal can only provide a limited bps/Hz
  - More bandwidth is needed
- **Carrier aggregation**
  - Combine multiple channels
    - Example: Fourth-generation LTE combines third-generation carriers
- Frequency reuse
  - Limit propagation range to an area
  - Use the same frequencies again when sufficiently far away
  - Use large coverage areas (macro cells) and smaller coverage areas (outdoor picocells or relays and indoor femtocells)
- Millimeter wave (mmWave)
  - Higher carrier frequencies have more bandwidth available
  - 30 to 300 GHz bands with millimeter wavelengths
  - Yet these are expensive to use and have problems with obstructions

CS 442 WSN U2

## LTE Carrier Aggregation



(a) Logical view of carrier aggregation



(b) Types of carrier aggregation

## **Unit 2 -- Recommend Reading**

---

- ▶ See in Google drive following PDF:

### **Class slides**

<b>Stalling's book</b>	<b>: Chap 1,2,5,6,7,8</b>
<b>Rapport's book</b>	<b>: Chap 1,3,4,5,6,</b>
<b>Karl's book</b>	<b>: Chap 4,6</b>

- ▶ Next – Unit 3 (WLAN,WPAN standards)

## **Unit 2 -- Recommend Reading**

---

- ▶ See in Google drive following PDF:

### **Class slides**

<b>Stalling's book</b>	<b>: Chap 1,2,5,6,7,8</b>
<b>Rapport's book</b>	<b>: Chap 1,3,4,5,6,</b>
<b>Karl's book</b>	<b>: Chap 4,6</b>

- ▶ Next – Unit 3 (WLAN,WPAN standards)

# **CS 442**

# **Wireless Sensor Network**

## **Unit 3**

CS 442 WSN Unit-3

### **Unit 3:**

Low power PAN, LAN Standards, IEEE 802.11, 802.15, 802.15.4 and Zigbee.

## **Unit 3**

## **WLAN, WPAN standards**

# IEEE 802 Standards Working Groups

Number	Topic
★ 802.1	Overview and architecture of LANs
★ 802.2 ↓	Logical link control
★ 802.3 *	Ethernet
★ 802.4 ↓	Token bus (was briefly used in manufacturing plants)
★ 802.5	Token ring (IBM's entry into the LAN world)
★ 802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 ↑	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
★ ★ 802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
★ 802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

★ You have studied in Computer Network Course

★ We study in this course

## Interfaces, Protocols, Standards

- ▶ Interface
- ▶ Protocol
- ▶ Standards

# IEEE 802.11

CS 442 WSN Unit-3

## Wireless Local Area Networks

- The proliferation of laptop computers and other mobile devices (PDAs and cell phones) created an *obvious* application level demand for wireless local area networking.
- Companies jumped in, quickly developing *incompatible* wireless products in the 1990's.
- Industry decided to entrust standardization to IEEE committee that dealt with wired LANS – *namely, the IEEE 802 committee!!*

# Categories of Wireless Networks

- **Base Station** :: all communication through an **access point** {note hub topology}. Other nodes can be fixed or mobile.
- **Infrastructure Wireless** :: base station network is connected to the wired Internet.
- **Ad hoc Wireless** :: wireless nodes communicate directly with one another.
- **MANETs (Mobile Ad Hoc Networks)** :: ad hoc nodes are mobile.

7

## Wireless LANs

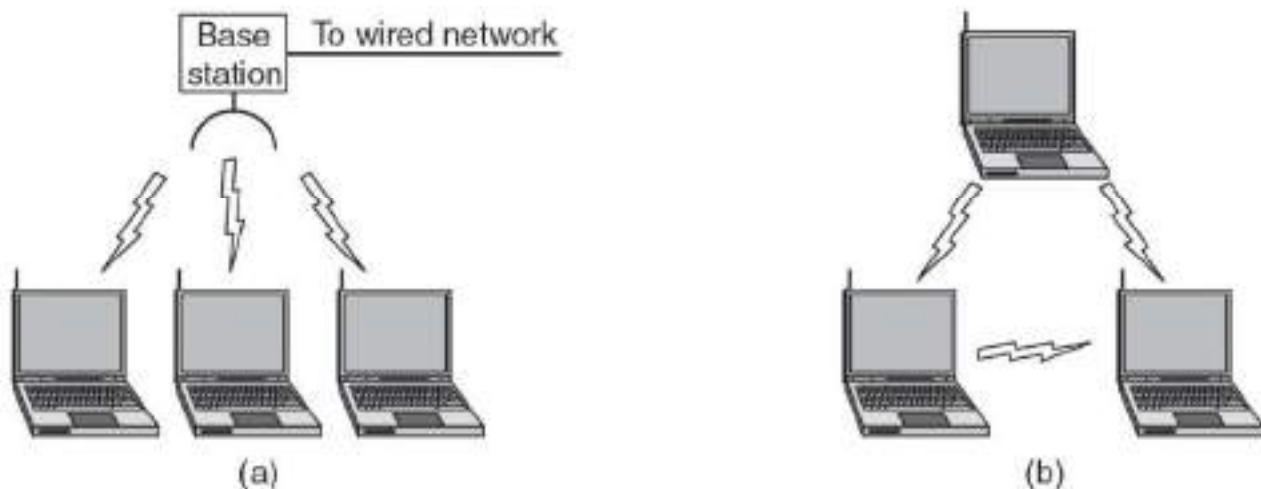
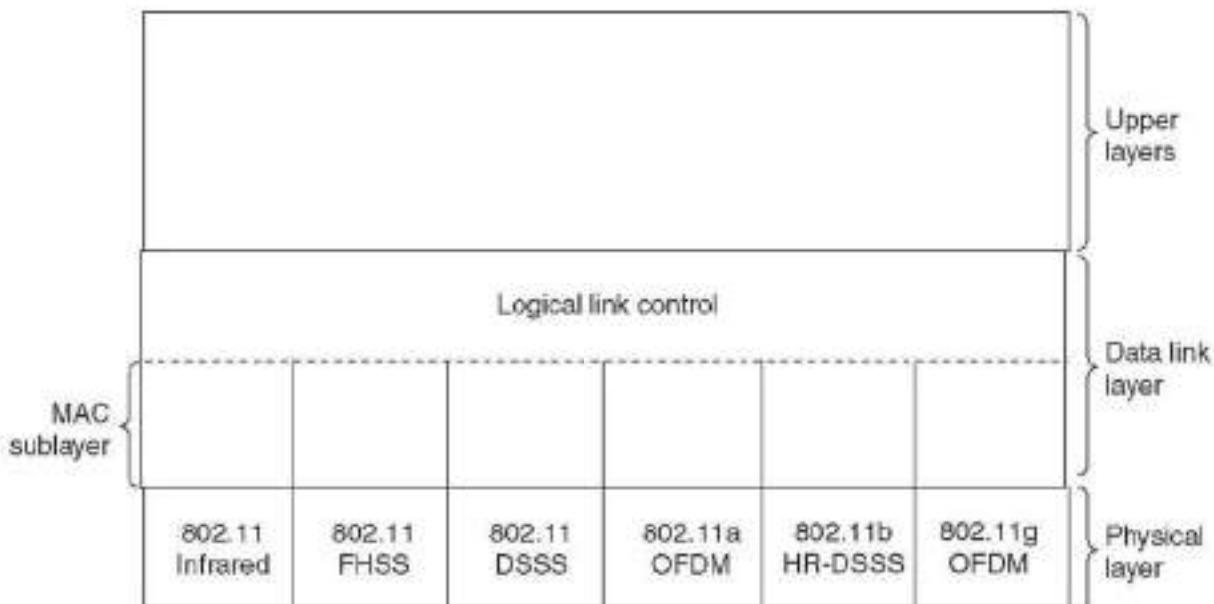


Figure 1-36.(a) Wireless networking with a base station. (b) Ad hoc networking.

8

# The 802.11 Protocol Stack



Part of the 802.11 protocol stack.

9

## 802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management
- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions

DLC	LLC	
PHY	MAC	MAC Management
	PLCP	PHY Management
	PMD	

Station Management

10

# The 802.11 Protocol Architecture

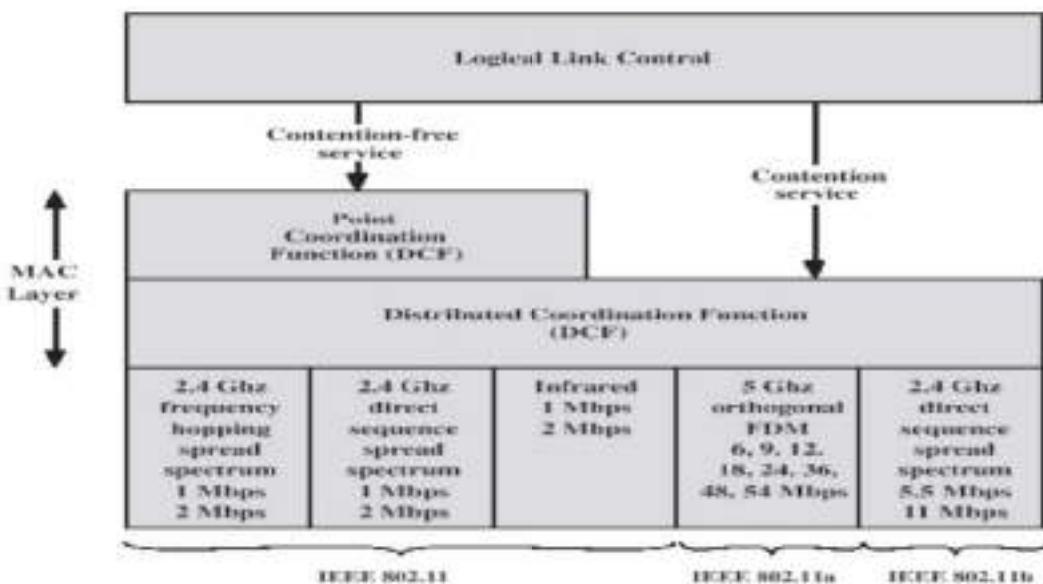
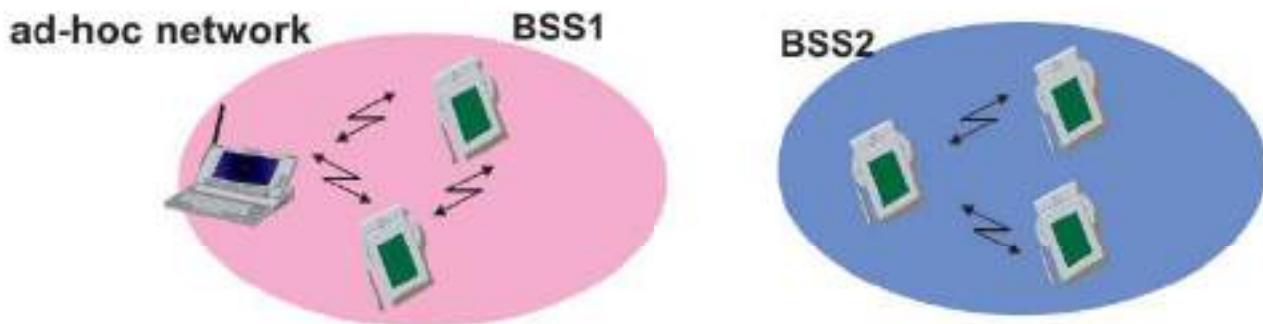


Figure 14.5 IEEE 802.11 Protocol Architecture

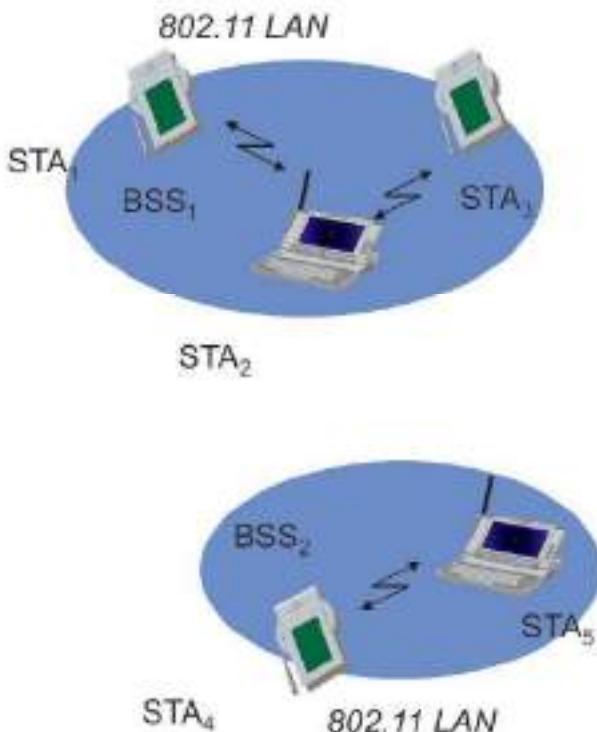
11

## Components of IEEE 802.11 architecture

- The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN
- The ovals can be thought of as the coverage area within which member stations can directly communicate
- The Independent BSS (IBSS) is the simplest LAN. It may consist of as few as two stations



# 802.11 - ad-hoc network (DCF)

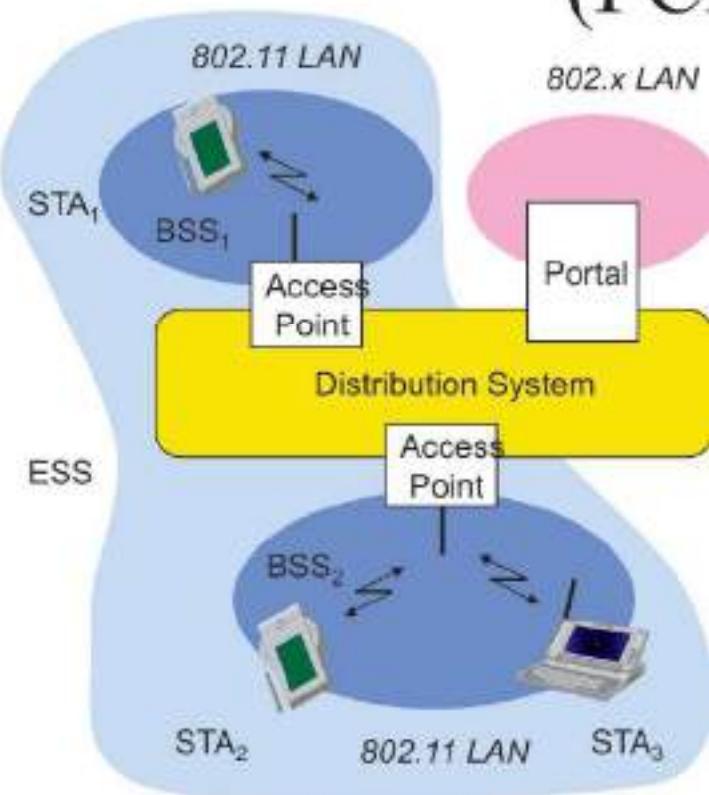


- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS): group of stations using the same radio frequency

13

# 802.11 - infrastructure network

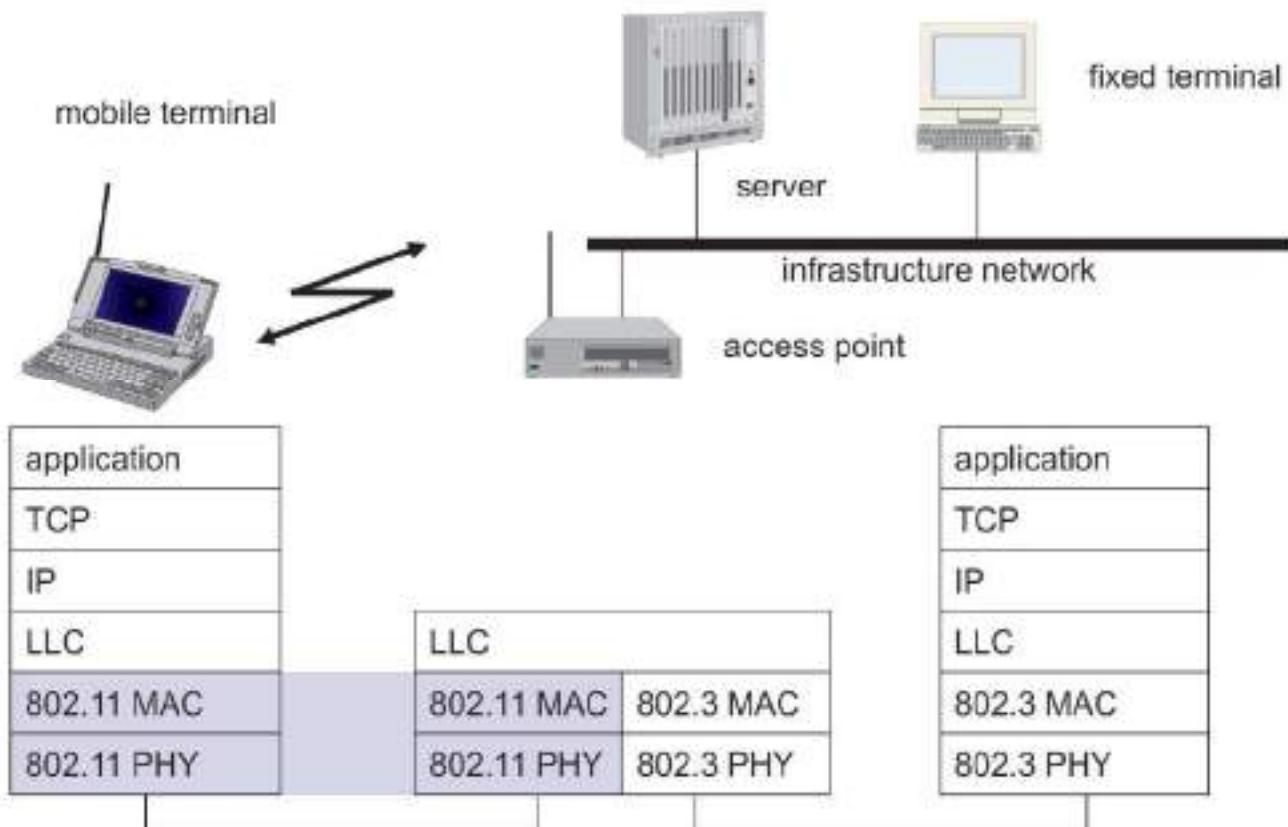
## (PCF)



- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

14

# 802.11- in the TCP/IP stack



## 802.11 Physical Layer

- Physical layer conforms to OSI (five options)
  - 1997: **802.11** infrared, FHSS, DHSS
  - 1999: **802.11a** OFDM and **802.11b** HR-DSSS
  - 2001: **802.11g** OFDM
- **802.11 Infrared**
  - Two capacities 1 Mbps or 2 Mbps.
  - Cannot penetrate walls.
- **802.11 FHSS (Frequency Hopping Spread Spectrum)**
  - 79 channels, each 1 MHz wide at low end of 2.4 GHz ISM band.
  - Same pseudo-random number generator used by all stations.
  - Dwell time: min. time on channel before hopping (400 msec).

# 802.11 Physical Layer

- **802.11 DSSS (Direct Sequence Spread Spectrum)**
  - Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA see Tanenbaum sec. 2.6.2).
  - Each bit transmitted as 11 chips (Barker seq.), PSK at 1Mbaud.
  - 1 or 2 Mbps.
- **802.11a OFDM (Orthogonal Frequency Divisional Multiplexing)**
  - Compatible with European HiperLan2.
  - 54Mbps in wider 5.5 GHz band → transmission range is limited.
  - Uses 52 FDM channels (48 for data; 4 for synchronization).
  - Encoding is complex ( PSM up to 18 Mbps and QAM above this capacity).
  - E.g., at 54Mbps 216 data bits encoded into into 288-bit symbols.
  - More difficulty penetrating walls.

17

# 802.11 Physical Layer

- **802.11b HR-DSSS (High Rate Direct Sequence Spread Spectrum)**
  - **11a and 11b shows a split in the standards committee.**
  - **11b** approved and hit the market before **11a**.
  - Up to 11 Mbps in 2.4 GHz band using 11 million chips/sec.
  - Note in this bandwidth all these protocols have to deal with interference from microwave ovens, cordless phones and garage door openers.
  - Range is 7 times greater than **11a**.
  - **11b and 11a are incompatible!!**

18

## 802.11 Physical Layer

- **802.11g OFDM(Orthogonal Frequency Division Multiplexing)**
  - Supports 54 Mbps.
  - Uses 2.4 GHz frequency for greater range.

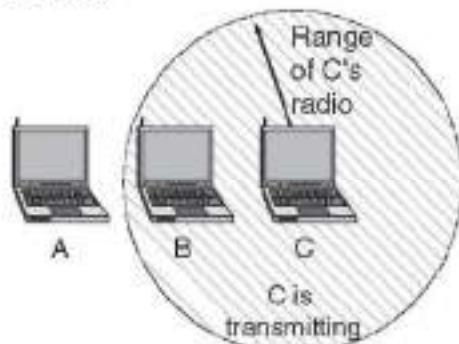
19

## 802.11 MAC Sublayer Protocol

- In 802.11 wireless LANs, “seizing channel” does not exist as in 802.3 wired Ethernet.
- Two additional problems:
  - Hidden Terminal Problem
  - Exposed Station Problem
- To deal with these two problems 802.11 supports two modes of operation **DCF (Distributed Coordination Function)** and **PCF (Point Coordination Function)**.
- **All implementations must support DCF, but PCF is optional.**

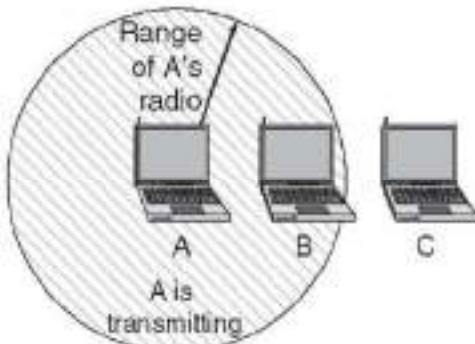
20

A wants to send to B  
but cannot hear that  
B is busy



(a)

B wants to send to C  
but mistakenly thinks  
the transmission will fail



(b)

(a) The hidden station problem. (b) The exposed station problem.

## The Hidden Terminal Problem

- Wireless stations have transmission ranges and not all stations are within radio range of each other.
- Simple CSMA will not work!
- C transmits to B.
- If A “*senses*” the channel, it will not hear C’s transmission and falsely conclude that A can begin a transmission to B.

# The Exposed Station Problem

- The inverse problem.
- B wants to send to C and listens to the channel.
- When B hears A's transmission, B falsely assumes that it cannot send to C.

# **CS 442**

# **Wireless Sensor Network**

## **Unit 5**

**Unit-5      Network layer / Routing:** Adhoc network routing, Data centric routing, Hierarchical routing protocols, Geographical routing, Location based routing.

CS 442 WSN Unit-5

## **Outline**

---

- **Introduction**
- **WSN routing Challenges**
- **Routing protocol Design Issues**
- **Flat Routing**
- **Hierarchical Routing**
- **Flat vs. Hierarchical**
- **Location-based Routing**
- **Routing Protocols Based on Protocol Operation**
- **Future Directions**
- **Conclusions**

# Outline

---

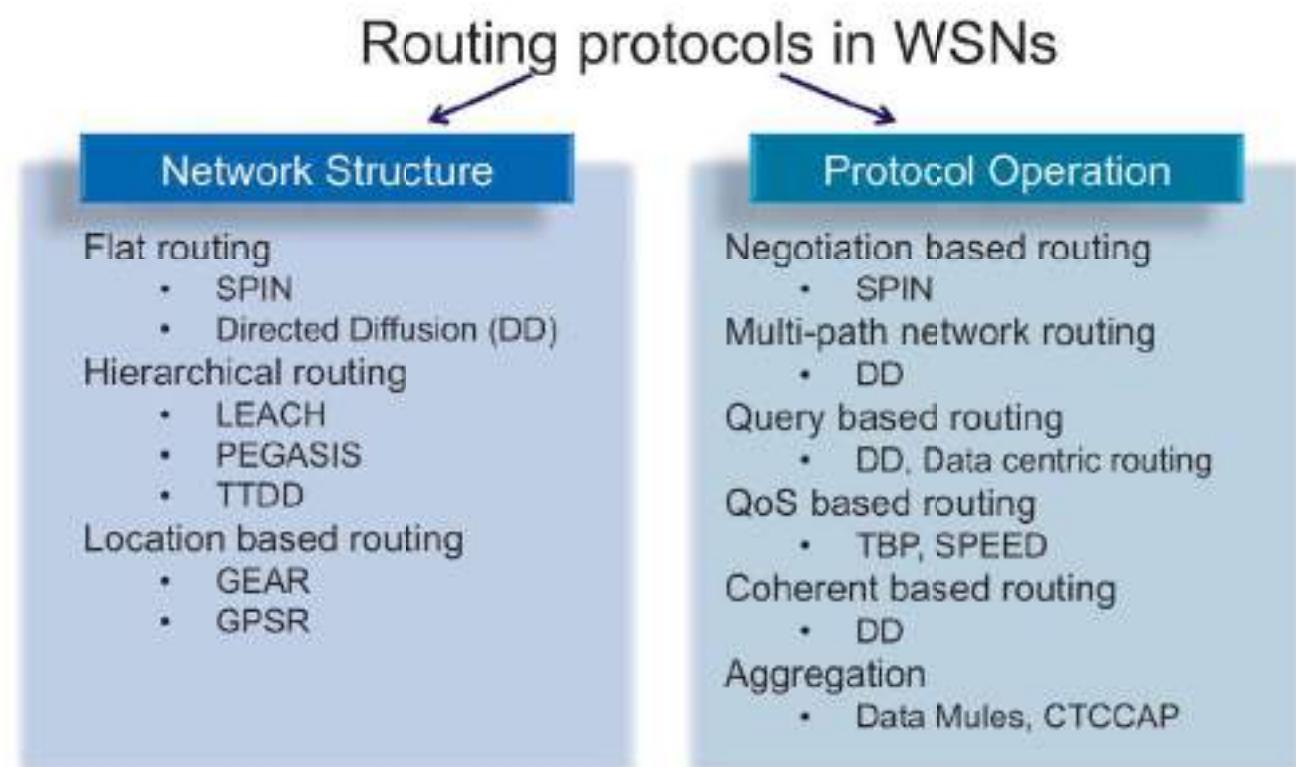
- ▶ **Introduction**
- ▶ **Challenges**
- ▶ **Design Issues**
- ▶ **Flat Routing**
- ▶ **Hierarchical Routing**
- ▶ **Flat vs. Hierarchical**
- ▶ **Location-based Routing**
- ▶ **Routing Protocols Based on Protocol Operation**
- ▶ **Future Directions**
- ▶ **Conclusions**

## Introduction (1/2)

---

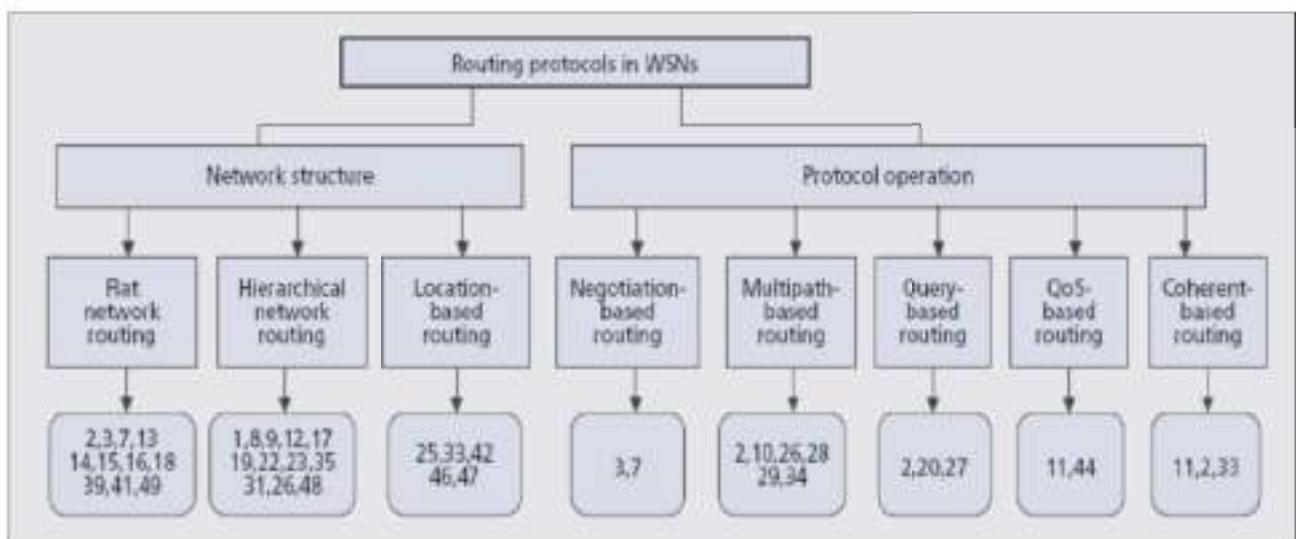
- ▶ Routing protocols in WSNs Differ depending on the application and network architecture
- ▶ Classified into three categories based on the underlying network structure:
  - ▶ Flat: Nodes are assigned equal roles
  - ▶ Hierarchical: Nodes will play different roles
  - ▶ Location-based: Nodes' positions are exploited to route data
- ▶ Classified into multipath-based, query-based, negotiation-based, QoS-based, and coherent-based depending on the protocol operation
- ▶ Trade-offs between energy and communication overhead savings

# Routing Protocols in WSNs: taxonomy



5

## Introduction (2/2)



# Outline

---

- ▶ **Introduction**
- ▶ **Challenges**
- ▶ **Design Issues**
- ▶ **Flat Routing**
- ▶ **Hierarchical Routing**
- ▶ **Flat vs. Hierarchical**
- ▶ **Location-based Routing**
- ▶ **Routing Protocols Based on Protocol Operation**
- ▶ **Future Directions**
- ▶ **Conclusions**

## Challenges (1/2)

---

- ▶ Due to the relatively large number of sensor nodes, it is not possible to build a **global addressing scheme** for the deployment of a large number of sensor nodes as the overhead of ID maintenance is high
- ▶ Applications of sensor networks require the few of sensed **data from multiple sources** to a particular BS
- ▶ Sensor nodes are tightly **constrained in terms of energy, processing, and storage capacities**

## Challenges (2/2)

---

- ▶ In most application scenarios, nodes in WSNs are generally stationary after deployment except for maybe a few mobile nodes.
- ▶ Sensor networks are application-specific
- ▶ Position awareness of sensor nodes is important since data collection is normally based on the location
- ▶ Data collected based on common phenomena, so there is a high probability that this data has some redundancy

## Outline

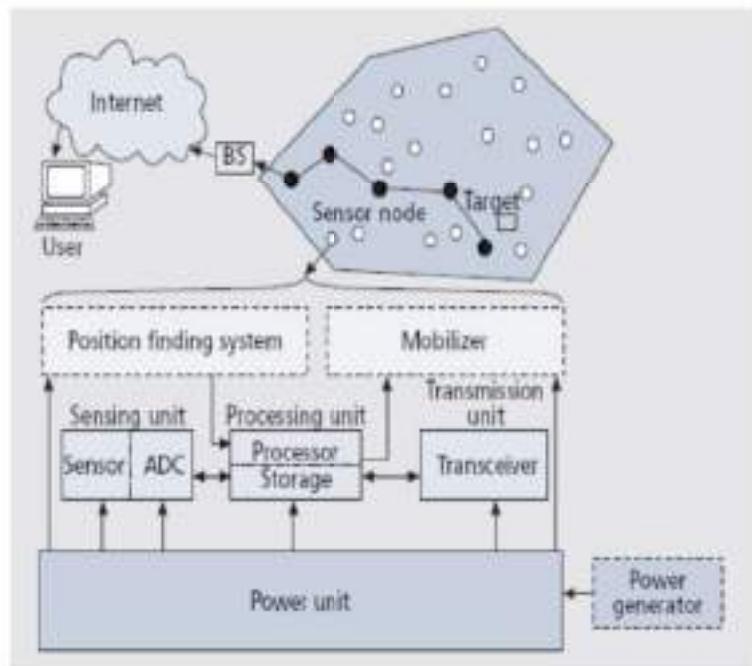
---

- ▶ Introduction
- ▶ Challenges
- ▶ Design Issues
- ▶ Flat Routing
- ▶ Hierarchical Routing
- ▶ Flat vs. Hierarchical
- ▶ Location-based Routing
- ▶ Routing Protocols Based on Protocol Operation
- ▶ Future Directions
- ▶ Conclusions

## Design Issues (1/4)

---

- ▶ The main design goals of WSNs is to carry out data communication while
- ▶ trying to **prolong the lifetime** of the network
- ▶ and **prevent connectivity degradation**
- ▶ by employing **aggressive energy management techniques**



## Design Issues (2/4)

---

- ▶ Node deployment: application-dependent
  - ▶ Manual (deterministic): data is routed through predetermined paths
  - ▶ Randomized: nodes are scattered randomly, creating an ad hoc routing infrastructure
  - ▶ Distribution of nodes is not uniform, optimal clustering becomes necessary
- ▶ Energy consumption without losing accuracy
  - ▶ Use up their limited supply of energy
  - ▶ The malfunctioning of some sensor nodes
- ▶ Data reporting method
  - ▶ Time-driven: for application requiring periodic data monitoring
  - ▶ Event-driven: react due to a certain event (time-critical ap)
  - ▶ Query-driven: response to a query (time-critical ap)
  - ▶ Hybrid

## Design Issues (3/4)

---

- › **Node/link heterogeneity**
  - › For example, hierarchical protocols designate a cluster head node
- › **Fault tolerance**
  - › The failure of sensor nodes should not affect the overall task of the sensor network
- › **Scalability**
  - › Any routing scheme must be able to work with huge number of sensor nodes
- › **Network dynamics**
  - › Nodes can be mobile
  - › The phenomenon can be mobile
- › **Transmission media**
  - › The required bandwidth is low(1-100 kb/s)
  - › TDMA-based protocols conserve more energy than contention-based protocols (like CSMA)

## Design Issues (4/4)

---

- › **Connectivity**
  - › Density in sensor networks
  - › Depends on the possibly random distribution of nodes
- › **Coverage**
  - › A sensor's view of the environment is limited in both range and accuracy
- › **Data aggregation**
  - › Sensor nodes may generate significant redundant data
  - › To reduce the number of transmissions
- › **Quality of service**
  - › Network lifetime often is considered more important
  - › Bounded latency for data delivery is a condition for time-constrained applications

# Outline

---

- ▶ **Introduction**
- ▶ **Challenges**
- ▶ **Design Issues**
- ▶ **Flat Routing**
- ▶ **Hierarchical Routing**
- ▶ **Flat vs. Hierarchical**
- ▶ **Location-based Routing**
- ▶ **Routing Protocols Based on Protocol Operation**
- ▶ **Future Directions**
- ▶ **Conclusions**

# Outline

---

- ▶ **Introduction**
- ▶ **Challenges**
- ▶ **Design Issues**
- ▶ **Flat Routing**
- ▶ **Hierarchical Routing**
- ▶ **Flat vs. Hierarchical**
- ▶ **Location-based Routing**
- ▶ **Routing Protocols Based on Protocol Operation**
- ▶ **Future Directions**
- ▶ **Conclusions**

## (A) Flat Routing

---

- ▶ Each node plays the same role
- ▶ Data-centric routing
  - ▶ Due to not feasible to assign a global id to each node
  - ▶ Save energy through data negotiation and elimination of redundant data
- ▶ Protocols
  - ▶ Sensor Protocols for Information via Negotiation (SPIN)
  - ▶ Directed diffusion (DD)
  - ▶ Rumor routing (RR)
  - ▶ Minimum Cost Forwarding Algorithm (MCFA)
  - ▶ Gradient-based routing (GBR)
  - ▶ Information-driven sensor querying/Constrained anisotropic diffusion routing (IDSQ/CADR)
  - ▶ COUGAR
  - ▶ ACQUIRE
  - ▶ Energy-Aware Routing
  - ▶ Routing protocols with random walks

## Sensor protocols for information via negotiation (SPIN)

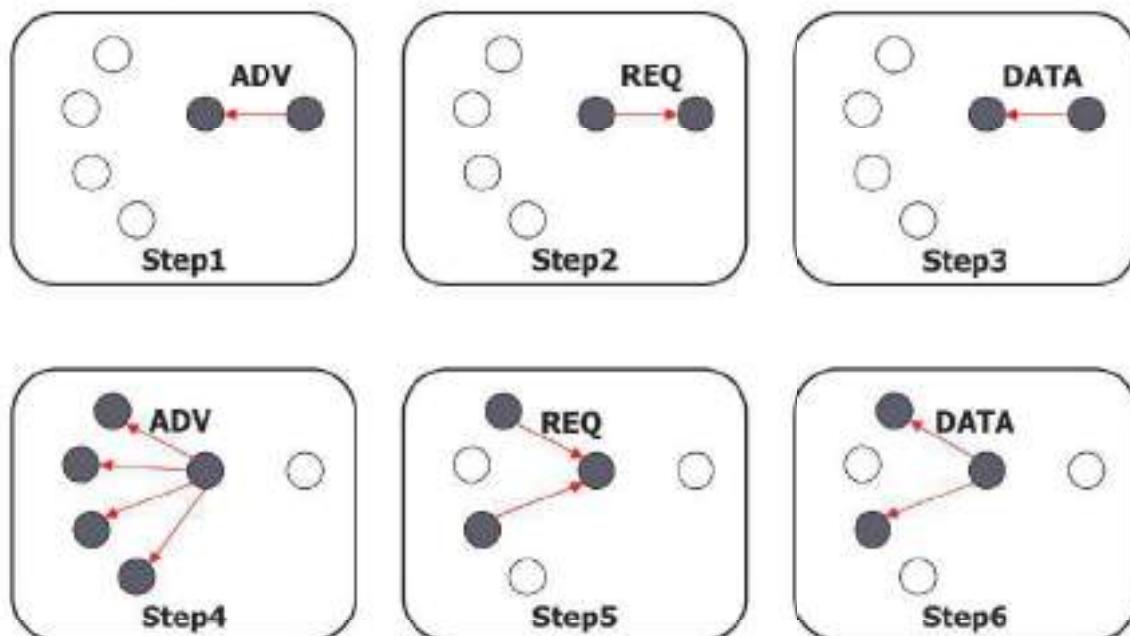
---

- ▶ **Features**
  - ▶ Negotiation
    - ▶ to operate efficiently and to conserve energy
    - ▶ using a meta-data
  - ▶ Resource adaptation
    - ▶ To extend the operating lifetime of the system
    - ▶ monitoring their own energy resources
- ▶ **SPIN Message**
  - ▶ ADV – new data advertisement
  - ▶ REQ – request for ADV data
  - ▶ DATA – actual data message
- ▶ ADV, REQ messages contain only meta-data

## Sensor protocols for information via negotiation (SPIN)

---

- Operation process



## Sensor protocols for information via negotiation (SPIN)

---

- ▶ **Resource adaptive algorithm**
  - ▶ When energy is plentiful
    - ▶ Communicate using the 3-stage handshake protocol
  - ▶ When energy is approaching a low-energy threshold
    - ▶ If a node receives ADV, it does not send out REQ
    - ▶ Energy is reserved to sensing the event
- ▶ **Advantage**
  - ▶ Simplicity
    - ▶ Each node performs little decision making when it receives new data
    - ▶ Need not forwarding table
  - ▶ Robust to topology change
- ▶ **Drawback**
  - ▶ Large overhead
  - ▶ Data broadcasting

## Directed Diffusion (DD)

---

- ▶ **Feature**
  - ▶ Data-centric routing protocol
  - ▶ A path is established between sink node and source node
  - ▶ Localized interactions
    - ▶ The propagation and aggregation procedures are all based on local information
- ▶ **Four elements**
  - ▶ **Interest**
    - ▶ A task description which is named by a list of attribute-value pairs that describe a task
  - ▶ **Gradient**
    - ▶ Path direction, data transmission rate
  - ▶ **Data message**
  - ▶ **Reinforcement**
    - ▶ To select a single path from multiple paths

# Directed Diffusion (DD)

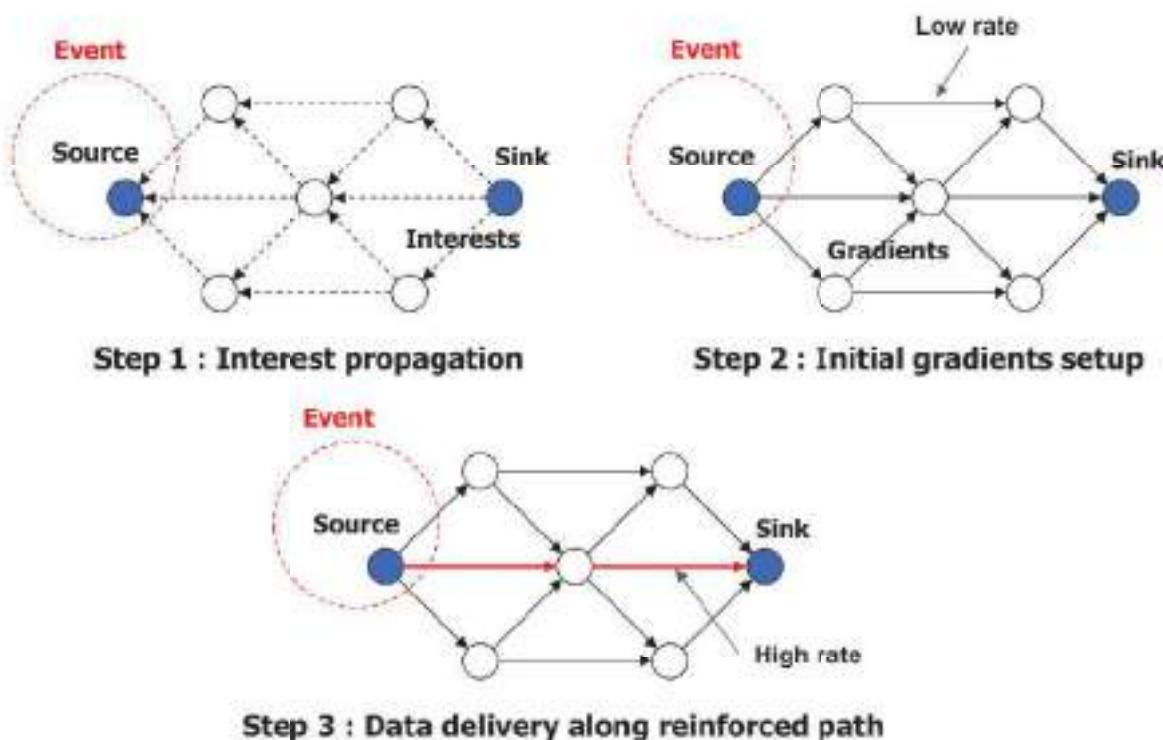
---

- ▶ **Feature**
  - ▶ Data-centric routing protocol
  - ▶ A path is established between sink node and source node
  - ▶ Localized interactions
    - ▶ The propagation and aggregation procedures are all based on local information
- ▶ **Four elements**
  - ▶ **Interest**
    - ▶ A task description which is named by a list of attribute-value pairs that describe a task
  - ▶ **Gradient**
    - ▶ Path direction, data transmission rate
  - ▶ **Data message**
  - ▶ **Reinforcement**
    - ▶ To select a single path from multiple paths

# Directed Diffusion (DD)

---

- ▶ Basic scheme



# Directed Diffusion (DD)

---

- ▶ **Advantage**
  - ▶ **Small delay**
    - ▶ Always transmit the data through shortest path
  - ▶ **Robust to failed path**
- ▶ **Drawback**
  - ▶ **Imbalance of node lifetime**
    - ▶ The energy of node on shortest path is drained faster than another
  - ▶ **Time synchronization technique**
    - ▶ To implement data aggregation
    - ▶ Not easy to realize in a sensor network
  - ▶ **The overhead involved in recording information**
    - ▶ Increasing the cost of a sensor node

## Rumor Routing (RR)

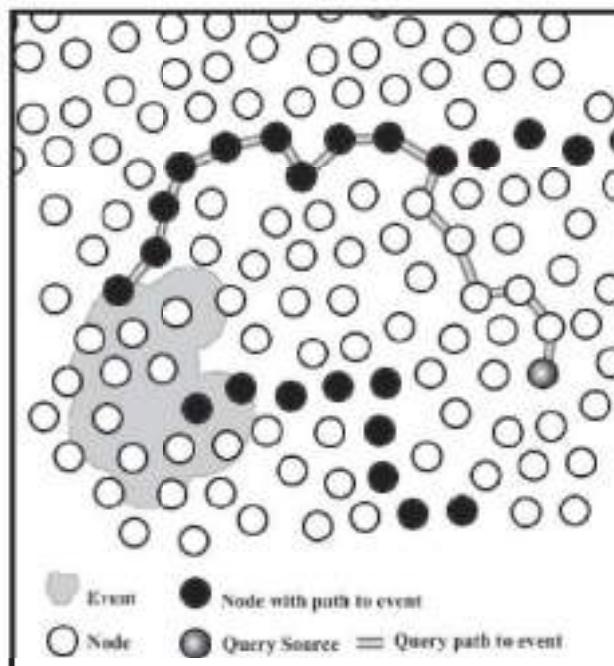
---

- ▶ **Feature**
  - ▶ Combine query flooding and event flooding
  - ▶ Discovering arbitrary paths instead of the shortest path
  - ▶ Rumor routing is attractive only when
    - ▶ The number of queries is larger than a threshold
    - ▶ The number of events is smaller than another threshold
- ▶ **Assumption**
  - ▶ The network is composed of densely distributed nodes
  - ▶ Only short distance transmissions
  - ▶ Immobile nodes

# Rumor Routing

---

- ▶ **Basic scheme**
  - ▶ Each node maintain
    - ▶ A lists of neighbors
    - ▶ An event table
  - ▶ When a node detects an event
    - ▶ Generate an agent
    - ▶ Let it travel on a random path
    - ▶ The visited node form a gradient to the event
  - ▶ When a sink needs an event
    - ▶ Transmit a query
    - ▶ The query meets some node which lies on the gradient
      - Route establishment



# Rumor Routing

---

- ▶ The node sensing an event probabilistically generates an agent. The probability of generating an agent is an algorithm parameter...
- ▶ In order to propagate directions to the event as far as possible in the network, a straightening algorithm is used
  - ▶ The agent maintains a list of recently seen nodes.
  - ▶ When picking its next hop, it will first try nodes not in the list.

# Minimum Cost Forwarding Algorithm (MCFA)

---

## ► Objective

- ▶ Establish the cost field
- ▶ Transmit the data through the minimum-cost path

## ► Feature

- ▶ Optimality
  - ▶ Minimum cost path criteria : hop count, energy consumption, delay etc.
- ▶ Simplicity
  - ▶ Need not to maintain forwarding table
  - ▶ Need not to know an ID for a neighbor node

# Minimum Cost Forwarding Algorithm (MCFA)

---

## ► Operation process

- ▶ Each node stores its cost to the sink
- ▶ The sink broadcasts an ADV message
  - ▶ containing its own cost (0 initially)
- ▶ Each node receiving the message transmits neighbor node
  - ▶ Add the cost in ADV message to its own cost
- ▶ The cost field is set up
  - ▶ after the ADV message propagates through the network
- ▶ The source transmits an information through cost field

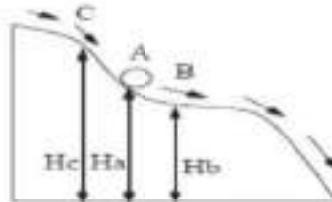
## ► Drawback

- ▶ Limited network size
  - ▶ The time to set the cost field is directly proportional to the size of the network
- ▶ Load is not balanced

## Minimum Cost Forwarding Algorithm (MCFA)

---

- ▶ The direction of routing is always known – toward the fixed external BS
- ▶ The BS broadcasts a message with the cost set to zero, while every node initially sets its least cost to the BS to infinity
- ▶ To check if the estimate in the message plus the link on which it is received is less than the current estimate.



Water at A on the slope goes only to B, since B's altitude is less than that of A's, while  $H_c > H_a$ , so A will not go to C.



Figure 2: Forwarding along the minimum-energy path

## Outline

---

- ▶ Introduction
- ▶ Challenges
- ▶ Design Issues
- ▶ Flat Routing
- ▶ **Hierarchical Routing**
- ▶ Flat vs. Hierarchical
- ▶ Location-based Routing
- ▶ Routing Protocols Based on Protocol Operation
- ▶ Future Directions
- ▶ Conclusions

# Outline

---

- › **Introduction**
- › **Challenges**
- › **Design Issues**
- › **Flat Routing**
- › **Hierarchical Routing**
- › **Flat vs. Hierarchical**
- › **Location-based Routing**
- › **Routing Protocols Based on Protocol Operation**
- › **Future Directions**
- › **Conclusions**

## Hierarchical Routing

---

- › Nodes will play different roles
- › Advantages related to scalability and efficient communication
- › Mainly two-layer routing
  - › Select cluster heads
  - › Routing
- › Protocols
  - › Low Energy Adaptive Clustering Hierarchy (LEACH)
  - › Power-Efficient Gathering in Sensor Information Systems (PEGASIS)
  - › Threshold-Sensitive Energy Efficient Protocols
  - › Small Minimum energy communication network (MECN)
  - › Self-organizing protocol (SOP)
  - › Virtual grid architecture routing
  - › Hierarchical power-aware routing
  - › Two –Tier Data Dissemination (TTDD)

## Low-energy adaptive clustering hierarchy (LEACH)

---

- Randomly select sensor nodes as cluster-heads, so the high energy dissipation in communicating with the base station is spread to all sensor nodes in the sensor network.
- Set-up phase
  - each sensor node chooses a random number between 0 and 1
  - If this random number is less than the threshold  $T(n)$ , the sensor node is a cluster-head.

$$T(n) = \begin{cases} \frac{P}{1 - P[r \bmod(1/P)]} & \text{if } n \in G, \\ 0 & \text{otherwise,} \end{cases}$$

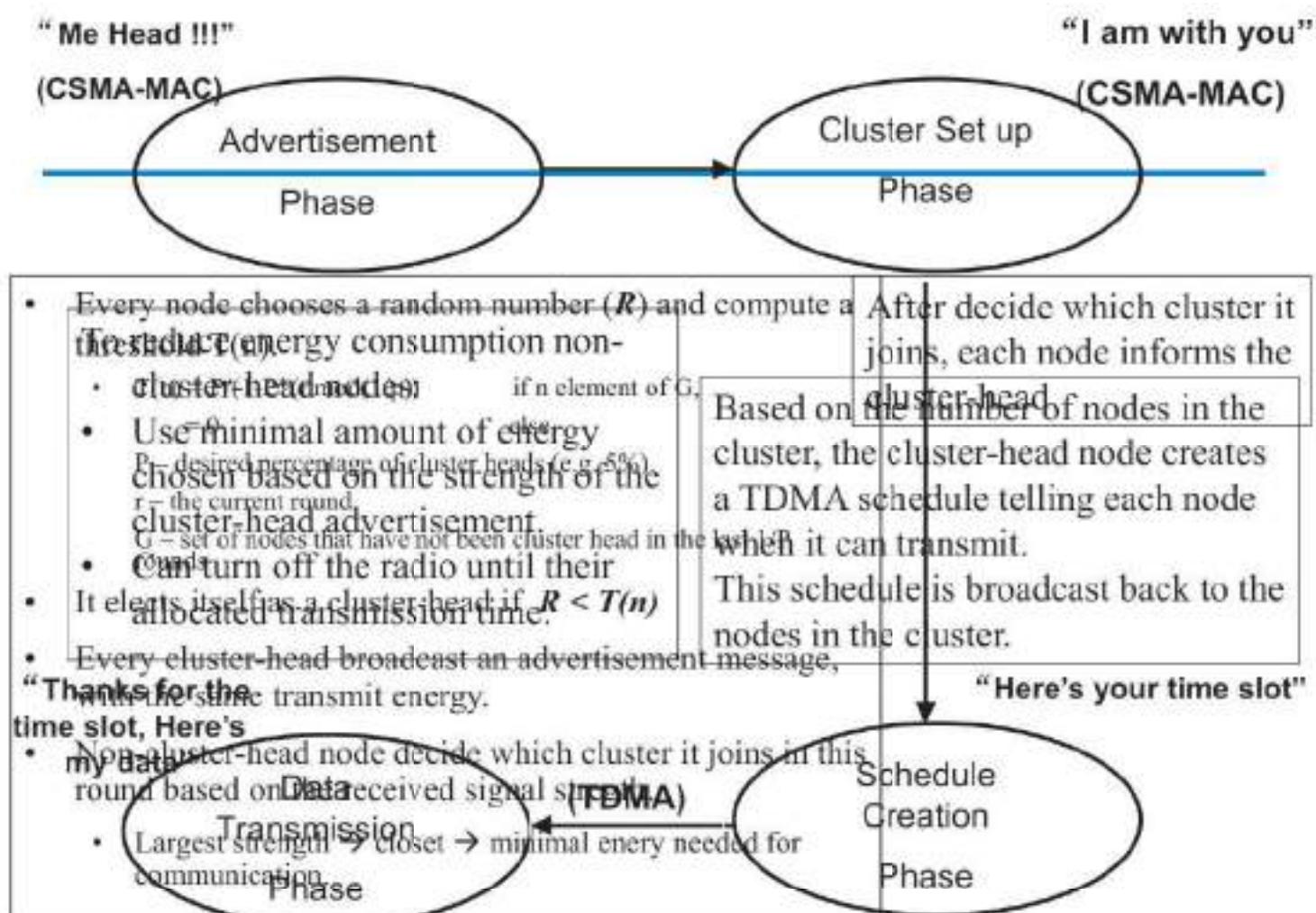
## Low-energy adaptive clustering hierarchy (LEACH)

---

- Set-up phase
  - The cluster-heads advertise to all sensor nodes in the network
  - The sensor nodes inform the appropriate cluster-heads that they will be a member of the cluster. (base on signal strength)
  - Afterwards, the cluster-heads assign the time on which the sensor nodes can send data to the cluster-heads based on a TDMA approach.

# Low-energy adaptive clustering hierarchy (LEACH)

- ▶ Steady phase
  - ▶ the sensor nodes can begin sensing and transmitting data to the cluster-heads.
  - ▶ The cluster-heads also aggregate data from the nodes in their cluster before sending these data to the base station.
- ▶ After a certain period of time spent on the steady phase, the network
  - ▶ goes into the set-up phase again and
  - ▶ enters into another round of selecting the cluster-heads.



## Different Phases in LEACH protocol

<b>Advertisement</b>	<ul style="list-style-type: none"> <li>• Every node chooses a random number (<math>R</math>) and compute a threshold <math>T(n)</math>.</li> <li>• <math>T(n) = P(1 - P^{r \bmod(1/P)})</math> if <math>n \in G</math>,</li> </ul>
<b>Phase</b>	$= 0 \quad \text{else}$ <p>P – desired percentage of cluster heads (e.g. 5%)  <math>r</math> – the current round  <math>G</math> – set of nodes that have not been cluster head in the last <math>1/P</math> rounds</p> <ul style="list-style-type: none"> <li>• It elects itself as a cluster-head if <math>R &lt; T(r)</math></li> <li>• Every cluster-head broadcast an advertisement message, with the same transmit energy.</li> <li>• Non-cluster-head node decide which cluster it joins in this round based on the received signal strength.</li> <li>• Largest strength <math>\rightarrow</math> closest <math>\rightarrow</math> minimal energy needed for communication.</li> </ul>
<b>Cluster Set up</b>	
<b>Phase</b>	After decide which cluster it joins, each node informs the cluster-head
<b>Schedule Creation</b>	
<b>Phase</b>	Based on the number of nodes in the cluster, the cluster-head node creates a TDMA schedule telling each node when it can transmit. This schedule is broadcast back to the nodes in the cluster.
<b>Data Transmission</b>	
<b>Phase</b>	To reduce energy consumption non-cluster-head nodes: <ul style="list-style-type: none"> <li>• Use minimal amount of energy chosen based on the strength of the cluster-head advertisement.</li> <li>• Can turn off the radio until their allocated transmission time.</li> </ul>

## Low-energy adaptive clustering hierarchy (LEACH)

- $p=0.05$
- $0.0500 = 0.05/(1-0.05^0)$
- $0.0526 = 0.05/(1-0.05^1)$
- $0.0555 = 0.05/(1-0.05^2)$
- $0.0588 = 0.05/(1-0.05^3)$
- $0.0625 = 0.05/(1-0.05^4)$
- $0.0666 = 0.05/(1-0.05^5)$
- $0.0714 = 0.05/(1-0.05^6)$
- $0.0769 = 0.05/(1-0.05^7)$
- $0.0833 = 0.05/(1-0.05^8)$
- $0.0909 = 0.05/(1-0.05^9)$
- $0.1000 = 0.05/(1-0.05^{10})$
- $0.5000 = 0.05/(1-0.05^{18})$
- $1.0000 = 0.05/(1-0.05^{19})$
- Number of clusters may not fixed in any round.
- To avoid the case that there is no cluster-head in a round... (PE-WASU'04, Oct. 7, 2004)
  - Simply skips the round which has no cluster-heads elected

$$T(n) = \begin{cases} \frac{P}{1 - P[r \bmod(1/P)]} & \text{if } n \in G, \\ 0 & \text{otherwise.} \end{cases}$$

## **Power-Efficient Gathering in Sensor Information Systems (PEGASIS)**

---

### ▶ **Assumption**

- ▶ All nodes have location information about all other nodes
- ▶ Sensor nodes are immobile

### ▶ **Feature**

- ▶ Chain-based power efficient protocol
- ▶ The chain construction by greedy algorithm
  - ▶ Each node has global knowledge
- ▶ Dynamic leader selection
  - ▶ To evenly distribute the energy load
- ▶ Data fusion

## **Power-Efficient Gathering in Sensor Information Systems (PEGASIS)**

---

### ▶ **Performance**

- ▶ PEGASIS Outperforms LEACH
  - ▶ By eliminating the overhead of dynamic cluster formation
  - ▶ By minimizing the total sum of transmission distances
  - ▶ By limiting the number of transmissions

### ▶ **Problem**

- ▶ To obtain a global knowledge is difficult
  - ▶ It is not suitable for sensor networks
- ▶ Scalability problem
- ▶ Very long delay

## Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

---

### ► Performance

- ▶ PEGASIS Outperforms LEACH
  - ▶ By eliminating the overhead of dynamic cluster formation
  - ▶ By minimizing the total sum of transmission distances
  - ▶ By limiting the number of transmissions

### ► Problem

- ▶ To obtain a global knowledge is difficult
  - ▶ It is not suitable for sensor networks
- ▶ Scalability problem
- ▶ Very long delay

## (13) Threshold-Sensitive Energy Efficient Protocols

---

### ► Terminology

- ▶ Hard Threshold ( $H_T$ )
  - ▶ A threshold value for the sensed attribute
  - ▶ The absolute value of the attribute
- ▶ Soft Threshold ( $S_T$ )
  - ▶ A small change in the value of the sensed attribute which triggers the node to switch on its transmitter

### ► Feature

- ▶ Cluster-based routing protocol based on LEACH
- ▶ Time critical application
- ▶ The user can control the trade-off between energy efficiency and accuracy
  - ▶ A smaller value of the  $S_T$ 
    - more accurate picture of the network
    - increased energy consumption

# Threshold-Sensitive Energy Efficient Protocols

---

- › **Basic scheme**
  - › A gain of sensing value
  - › Decision whether to report it or not
    - › Based on the values of  $H_t$  and  $S_t$
  - › Data are reported only
    - › When the sensed value exceeds  $H_T$
    - › When the value's change is bigger than  $S_T$
- › **Drawback**
  - › Cannot allocate the time slot
    - › Each node turn on its transmitter all the time
  - › Cannot distinguish a node which does not sense a "big" change from a dead or failed node
  - › Collision occurrence in the cluster

## Outline

---

- › **Introduction**
- › **Challenges**
- › **Design Issues**
- › **Flat Routing**
- › **Hierarchical Routing**
- › **Hierarchical vs. Flat**
- › **Location-based Routing**
- › **Routing Protocols Based on Protocol Operation**
- › **Future Directions**
- › **Conclusions**

# Hierarchical vs. Flat

---

Hierarchical routing	Flat routing
Reservation-based scheduling	Contention-based scheduling
Collisions avoided	Collision overhead present
Reduced duty cycle due to periodic sleeping	Variable duty cycle by controlling sleep time of nodes
Data aggregation by clusterhead	Node on multihop path aggregates incoming data from neighbors
Simple but non-optimal routing	Routing can be made optimal but with an added complexity.
Requires global and local synchronization	Links formed on the fly without synchronization
Overhead of cluster formation throughout the network	Routes formed only in regions that have data for transmission
Lower latency as multiple hops network formed by cluster-heads always available	Latency in waking up intermediate nodes and setting up the multipath
Energy dissipation is uniform	Energy dissipation depends on traffic patterns
Energy dissipation cannot be controlled	Energy dissipation adapts to traffic pattern
Fair channel allocation	Fairness not guaranteed

## Outline

---

- ▶ **Introduction**
- ▶ **Challenges**
- ▶ **Design Issues**
- ▶ **Flat Routing**
- ▶ **Hierarchical Routing**
- ▶ **Flat vs. Hierarchical**
- ▶ **Location-based Routing**
- ▶ **Routing Protocols Based on Protocol Operation**
- ▶ **Future Directions**
- ▶ **Conclusions**

# Location-Based Routing Protocols

---

- ▶ **Nodes' positions are exploited to route data**
  - ▶ Sensor nodes are addressed by means of their locations
  - ▶ Distance can be estimated on the basis of incoming signal strengths
- ▶ **Example Protocols:**
  - ▶ Geographic Adaptive Fidelity
  - ▶ Geographic and Energy Aware Routing
  - ▶ MFR, DIR and GEDIR
  - ▶ The Greedy Other Adaptive Face Routing
  - ▶ SPAN

# Location-Based Routing Protocols

---

- ▶ **Nodes' positions are exploited to route data**
  - ▶ Sensor nodes are addressed by means of their locations
  - ▶ Distance can be estimated on the basis of incoming signal strengths
- ▶ **Example Protocols:**
  - ▶ Geographic Adaptive Fidelity
  - ▶ Geographic and Energy Aware Routing
  - ▶ MFR, DIR and GEDIR
  - ▶ The Greedy Other Adaptive Face Routing
  - ▶ SPAN

## Outline

---

- ▶ **Introduction**
- ▶ **Challenges**
- ▶ **Design Issues**
- ▶ **Flat Routing**
- ▶ **Hierarchical Routing**
- ▶ **Flat vs. Hierarchical**
- ▶ **Location-based Routing**
- ▶ **Routing Protocols Based on Protocol Operation**
- ▶ **Future Directions**
- ▶ **Conclusions**

## Routing Protocols Based on Protocol Operation

---

- ▶ Multipath Routing Protocols
- ▶ Query-Based Routing

### Multipath Routing Protocols

---

- ▶ Use multiple paths in order to enhance network performance
  - ▶ Fault tolerance
  - ▶ Balance energy consumption
  - ▶ Energy-efficient
  - ▶ Reliability
- ▶ E.g.
  - ▶ MPR

# **Query-Based Routing**

---

- ▶ **Destination nodes** propagate a query for data
- ▶ **Usually these queries are described in natural language or high-level query language**
  
- ▶ **E.g.**
  - ▶ Directed diffusion
  - ▶ Rumor routing protocol

## **Outline**

---

- ▶ **Introduction**
- ▶ **Challenges**
- ▶ **Design Issues**
- ▶ **Flat Routing**
- ▶ **Hierarchical Routing**
- ▶ **Flat vs. Hierarchical**
- ▶ **Location-based Routing**
- ▶ **Routing Protocols Based on Protocol Operation**
- ▶ **Future Directions**
- ▶ **Conclusions**

## **Future Directions (1/2)**

---

- **QoS**
- **Nodes mobility**
- **Exploit redundancy**
- **Tiered architectures**
- **Exploit spatial diversity and density of sensor nodes**
- **Achieve desired global behavior with adaptive localized algorithms**

## **Future Directions (2/2)**

---

- **Leverage data processing inside the network and exploit computation near data sources to reduce communication**
- **Time and location synchronization**
- **Localization**
- **Self-configuration and reconfiguration**
- **Secure routing**
- **Integration of sensor networks with wired networks**

# Outline

---

- › **Introduction**
- › **Challenges**
- › **Design Issues**
- › **Flat Routing**
- › **Hierarchical Routing**
- › **Flat vs. Hierarchical**
- › **Location-based Routing**
- › **Routing Protocols Based on Protocol Operation**
- › **Future Directions**
- › **Conclusions**

## Conclusions : Routing protocols for WSN

---

- › They have the **common objective** of trying to extend the lifetime of network
- › **Trade-off** energy and communication overhead
- › There are still many challenges that need to be solved

# **End of Unit 5**