



## CENG797 Ad Hoc Networks

E. Onur

Wireless Systems, Networks and Cybersecurity Laboratory  
Department of Computer Engineering  
Middle East Technical University  
Ankara Turkey

February 28, 2022

# Outline I

## PART 1: INTRODUCTION

- 1 Objectives
- 2 Ad Hoc Networks
- 3 Research and Design Issues in Ad Hoc Networks
- 4 Classification of Ad Hoc Networks
- 5 Applications

## PART 2: WIRELESS TECHNOLOGY

- 6 Objectives
- 7 Classification of Wireless Technologies
- 8 Short-range Wireless Technologies
- 9 Low-power Wide Area Network Standards
- 10 Wrap-up

## PART 3: WIRELESS COMMUNICATION

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations

# Outline II

- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

## PART 4: MODELING

- 25 Objectives
- 26 What is a Graph?
- 27 Representation
- 28 Modeling Ad Hoc Networks as Graphs
- 29 Scale Free Graphs

# Outline III

- 30 Geometric Random Graph for Ad Hoc Networks
- 31 Mobility Modeling

## PART 5: LINK LAYER

- 32 Data Link Layer
- 33 Sharing the Medium
- 34 Contention Free MAC Protocols
- 35 Contention Based MAC Protocols

## PART 5: AD HOC MAC SUBLAYER

- 36 MAC Issues in Ad Hoc Networks
- 37 Contention-based protocols
- 38 Contention-based protocols with reservation mechanisms
- 39 Contention-based protocols with scheduling
- 40 MAC Protocols with Directional Antennas
- 41 Multi-channel MAC Protocols
- 42 Power Control MAC Protocol

## PART 6: NETWORK LAYER

# Outline IV

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

## PART 7: MULTICAST ROUTING

- 53 Introduction to Multicasting
- 54 Multicasting in Ad Hoc Networks
- 55 Operation of Multicast Routing Protocols
- 56 Cross-layer Reference Model for Multicast Routing
- 57 Classification of Multicast Routing Protocols

# Outline V

- 58 Tree-based Multicast Routing Protocols
- 59 Mesh-based Multicast Routing Protocols

## PART 8: TRANSPORT LAYER

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)
- 62 Transport Layer in Ad Hoc Networks
- 63 Classification
- 64 Feedback-Based TCP
- 65 TCP with Explicit Link Failure Notification
- 66 Split TCP
- 67 Ad Hoc Transport Protocol (ATP)

# Lecture 1: Introduction, Positioning and Applications

# Agenda

- 1 Objectives
- 2 Ad Hoc Networks
- 3 Research and Design Issues in Ad Hoc Networks
- 4 Classification of Ad Hoc Networks
- 5 Applications

# Lecture Objectives

At the end of this lecture, you will be able to

1. **define** ad hoc networks and their types
2. **describe** the history of ad hoc networks
3. **discuss** future ad hoc networking applications
4. **define** some wireless technologies [1]
5. **compare** the existing standards for wireless communications



# Hype Cycle - Gartner

## Emerging Technologies, 2019



# Agenda

- 1 Objectives
- 2 Ad Hoc Networks
- 3 Research and Design Issues in Ad Hoc Networks
- 4 Classification of Ad Hoc Networks
- 5 Applications

# Wireless Networks

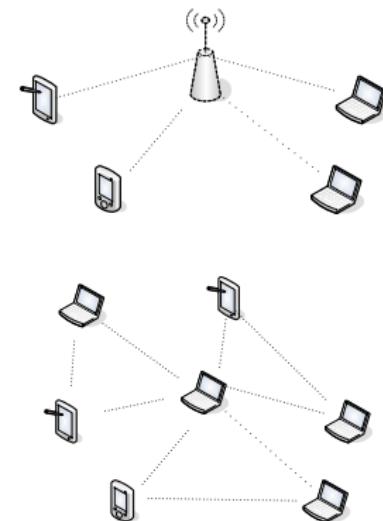
There are two broad types of wireless networks:

- **Infrastructure-based**

- Relies on an infrastructure
- Commonly the base stations or access points (AP) are fixed and stationary
- Network management and control is on the infrastructure
- Examples: WIFI, Cellular mobile networks, LORA

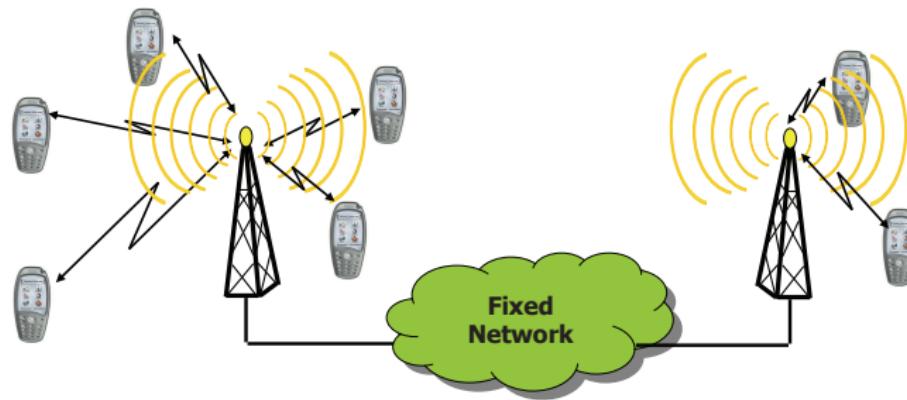
- **Infrastructure-less**

- No centralized, fixed access point
- Intelligence (management and control planes) are distributed
- aka: ad hoc networks

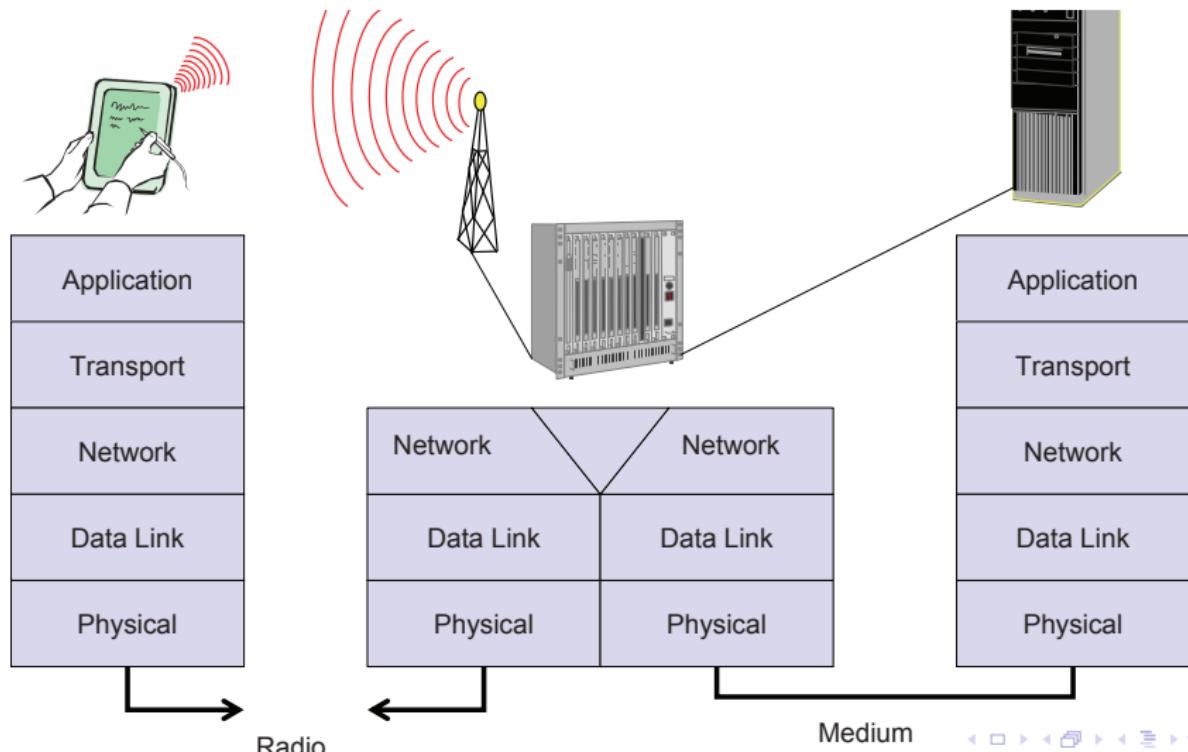


# Infrastructure-based Wireless Networks

Management by the base station

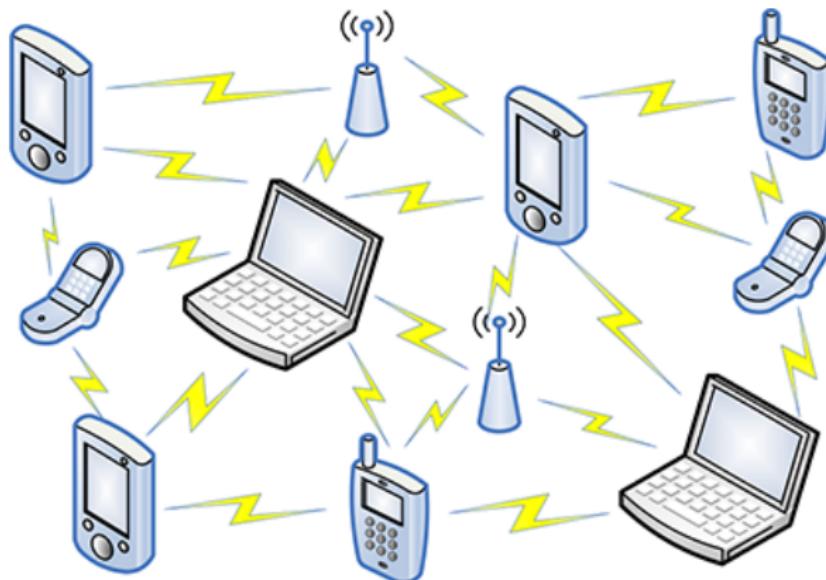


# Reference Model for Infrastructure-based Wireless Networks



# What is an Ad Hoc Network (broad sense)?

Take control and management intelligence from center and distribute to entities



# Formal Definition of Ad Hoc Networks

## An ad hoc network [2]

is a (possibly mobile) **collection** of communications devices (nodes) that wish to **communicate**, but have **no fixed infrastructure** available, and have no predetermined organization of available links. Individual nodes are responsible for **dynamically discovering** which other nodes they can directly communicate with. A key assumption is that not all nodes can directly communicate with each other, so nodes are required to **relay** packets on behalf of other nodes in order to deliver data across the network. A significant feature of ad hoc networks is that **rapid changes** in connectivity and link characteristics are introduced due to node mobility and power control practices.

# Formal Definition of Mobile Ad Hoc Networks (IETF)

## A “mobile ad hoc network” (MANET) [3]

is an **autonomous** system of **mobile routers** (and associated hosts) connected by wireless links—the union of which form an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network’s wireless topology may change rapidly and **unpredictably**. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

# Highlights of the Formal Definition

An ad hoc network is a collection of computing/communicating devices where

- devices are called nodes
- nodes **dynamically** form a temporary network **without the use of any existing network infrastructure** or centralized administration
- nodes discover each other
- nodes **relay packets** of each other
- nodes may be **mobile**
- **topology may (frequently) change** because of mobility or power control
- May be stand-alone, may be connected to the Internet

# The word Ad Hoc?

## Cambridge Dictionary [adjective before noun]

made or happening only for a particular purpose or need, **not planned before it happens**

## Cambridge American Dictionary [adjective, adverb]

for a particular purpose or need, esp. for an immediate need

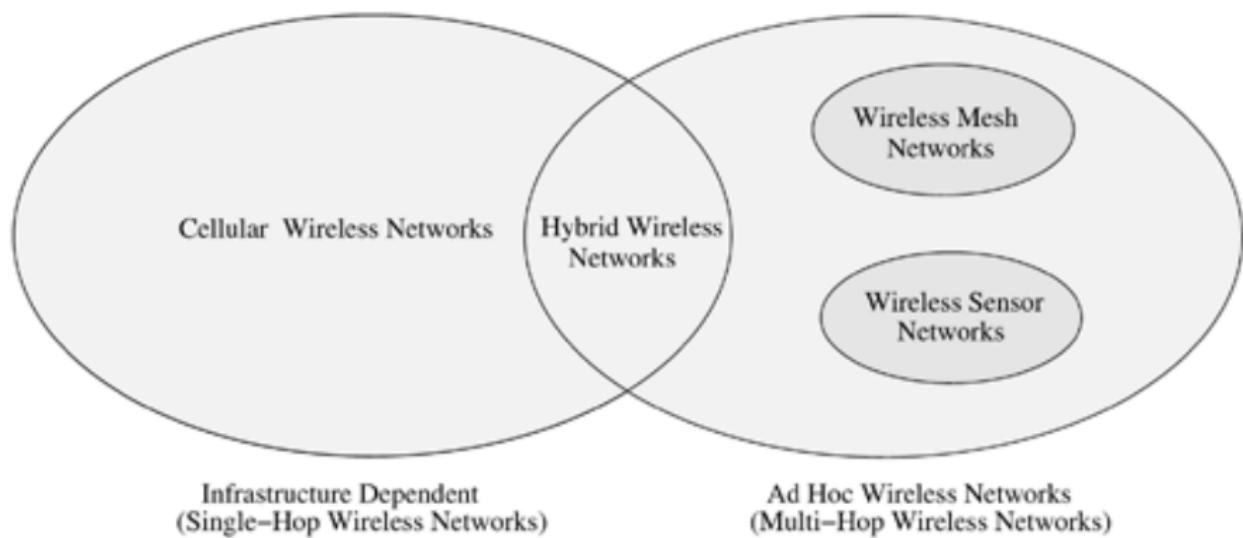
## Cambridge Business Dictionary [adjective]

happening or existing only for a particular purpose and not previously planned

# Major Challenges

- **Scalability**: can be broadly defined as whether the network is able to provide an acceptable level of service to users/applications/packets even in the presence of a large number of nodes. Scalability is closely related as to how quickly control overhead increases as a function of an increase in the number of nodes and link changes.
- **Energy efficiency**: No infrastructure means batter-driven nodes. Energy sources must be used efficiently.
- **Quality of service (QoS)**: Radio channel, topology is unpredictable. Adapt to changes!
- **Security**: Shared medium, hostile environment, distribution of control and management introduce additional security challenges.
- **Gap between reality and models**: radio channel propagation models, mobility models, deployment models, traffic models etc may not resemble real-life.
- **THE HOLY GRAIL**: A one-size-fits-all solution

# MANET versus Cellular Networks



# Comparison

Cellular Mobile Networks	Ad Hoc Networks
Infrastructure-based	Infrastructure-less
Fixed, prelocated base station	No base station, rapid deployment
Static backbone topology	Very dynamic topology, multihop
Stable connectivity	Irregular connectivity
Planned deployment	Self-organizing
High setup costs	Cost-effective
Large setup time	Less setup time
Single-hop	Multiple-hops
Centralized routing	Distributed routing
Guaranteed bandwidth	Shared radio channel
Seamless connectivity	Frequent path breaks
Circuit switched	Packet switched
Easier time synch	Time synch consumes bandwidth
High maintenance cost	Self-organized

# Advantages of Ad Hoc Networks

- Self- $x$  where  $x \in \{ \text{forming, healing, balancing, ...} \}$
- Well suited to free unlicensed spectrum: significant savings given typical auction prices
- Cheap nodes (mass production)
- Low start-up costs, easy (temporary) set-up
- No need to install base stations
- Increased spectral efficiency
- Increased mobility and flexibility
- Power efficiency
- Growth of network coverage by increase in number of users

# History

- 1968-1971, **ALOHANET**, University of Hawaii, Norman Abramson [4]
  - ALOHA: Additive Links On-line Hawaii Area, Led to PRNET
  - ARPA, a single-hop wireless packet data network
  - Menehune (dwarf): The central node communications processor
- 1972, DARPA Packet Radio Networks (**PRNET**) [5], [6]
  - Consists of mobile repeaters, terminals and dedicated mobile stations
  - Repeaters relay radio packets (repeater to repeater until destination)
  - ALOHA, CSMA and distance-vector routing
  - Rapidly deployable, self-initializing, self-organizing, no network management and administration problems
  - Media access, error control, flow control, routing issues, transport issues
- 1980's, Survivable Adaptive Radio Networks (**SURAN**) (link state routing)
- PRNET and SURAN's objective: To provide packet-switched networking to mobile battlefield elements in an infrastructure-less, hostile environment (soldiers, tanks, aircraft, etc., forming the nodes).

# Standardization

## Internet Engineering Task Force (IETF) MANET

(proposed June 2, 1997, started June 12, 1997) The purpose of the Mobile Ad Hoc Networks (MANET) working group is to standardize IP routing protocol functionality suitable for wireless routing applications within both static and dynamic topologies with increased dynamics due to node motion or other factors.

# Agenda

- 1 Objectives
- 2 Ad Hoc Networks
- 3 Research and Design Issues in Ad Hoc Networks
- 4 Classification of Ad Hoc Networks
- 5 Applications

# Research and Design Issues in Ad Hoc Networks

1. Medium access
2. Routing
3. Multicasting
4. Broadcasting
5. Transport layer
6. Cooperation
7. Security
8. QoS
9. Energy
10. Addressing and service discovery
11. Scalability
12. Deployment considerations

# Medium Access Issues in Ad Hoc Networks

## Medium Access Control (MAC)

The primary responsibility of a medium access control (MAC) protocol in ad hoc wireless networks is the **distributed arbitration for the shared channel** for transmission of packets.

- Distributed operation
- Synchronization
- Hidden-terminal problem
- Exposed-terminal problem
- Throughput
- Access delay
- Fairness
- Real-time traffic support
- Resource reservation
- Measuring resource availability for admission control
- Power control
- Rate control
- Directional antennas

# Routing Issues in Ad Hoc Networks

## Routing Protocols are responsible for

Exchanging the route info; finding a feasible path based on some criteria; gathering information about the path breaks; mending the broken paths; and utilizing minimum bandwidth.

- Mobility
- Bandwidth constraints
- Error-prone shared channel ( $BER \approx 10^{-5}$  to  $10^{-3}$  versus  $10^{-9}$  for wired)
- Location-dependent collisions
- Constraints on cpu, power, buffer space etc
- Minimal route acquisition delay
- Rapid route reconfiguration and loop-free distributed routing
- Minimal control overhead and scalability
- QoS: being able to provide some level of bandwidth, delay, jitter, packet delivery ratio, or throughput
- Support for time-sensitive traffic: hard real-time and soft real-time
- Security and privacy

# Multicasting/Broadcasting Issues in Ad Hoc Networks

Example: point to multi-point communication in emergency applications.

- Robustness
- Efficiency
- Control overhead
- QoS
- Group management
- Scalability
- Security
- Broadcast storm problem

# Transport Layer Issues in Ad Hoc Networks

TCP will not work well because of path breaks, frequent topology changes introduce stale routes, high channel error rate, frequent network partitioning,...

- End-to-end reliable data transport
- Flow control
- Congestion control
- Mobility
- Frequent path breaks
- Latency for path maintenance
- Bit errors at PHY
- Collisions at MAC

# Cooperation Issues in Ad Hoc Networks

## Cooperation

**Five rules:** kin selection, direct reciprocity, indirect reciprocity, network reciprocity, group selection [7].

- Rational devices?
- Payoff functions and costs
- External or internal incentives
- Discounting (infinite horizon)
- Reputation
- Cooperative or non-cooperative games
- Imperfect/incomplete information
- How to enforce cooperation: money, reputation, threat, high-level being, government, ...

## Games

Multiple access game, forwarder's dilemma, jamming game, etc.

# Quality of Service Issues in Ad Hoc Networks

## Quality of service (QoS)

is the **performance level** of services offered by a service provider or a network to the user. QoS provisioning often requires negotiation between the host and the network, resource reservation schemes, priority scheduling, and call admission control. QoS in ad hoc networks can be on a per flow, per link, or per node basis.

- QoS parameters (delay, jitter, loss, ...),
- QoS-aware routing, MAC, ...
- QoS frameworks (holistic perspective)

# Self Organization Issues in Ad Hoc Networks

## Self-organizing Networks (SON)

organizing and maintaining the network by itself. **Neighbor discovery, topology organization, and topology reorganization.**

- QoS parameters (delay, jitter, loss, ...),
- QoS-aware routing, MAC, ...
- QoS frameworks (holistic perspective)

# Security Issues in Ad Hoc Networks

## Self-organizing Networks (SON)

Attack vectors can be classified into: vulnerability of channel or node, absence of infrastructure, dynamic topology.

- Denial of service
- Resource consumption: energy consumption, buffer depletion
- Host impersonation
- Information disclosure
- Interference
- Network layer hello flooding, black hole, sink hole, selective forwarding, wormhole, Sybil,
- Jamming, tampering, unfairness, sleep deprivation
- Link collision, exhaustion,
- Eavesdropping, traffic analysis
- Node replication, packet injection, packet duplication, packet alteration

# Addressing and Service Discovery Issues in Ad Hoc Networks

## Addressing

An address that is globally unique in the connected part of the ad hoc wireless network is required for a node in order to participate in communication. **Auto-configuration of addresses** is required to allocate non-duplicate addresses to the nodes. In networks where the topology is highly dynamic, frequent partitioning and merging of network components require duplicate address-detection mechanisms in order to maintain unique addressing throughout the connected parts of the network.

## Service Discovery

Nodes in the network should be able to locate services that other nodes provide. Hence efficient **service advertisement** mechanisms are necessary. Topological changes force a change in the location of the service provider as well, hence fixed positioning of a server providing a particular service is ruled out.

# Energy Management Issues in Ad Hoc Networks

## Energy Management

Energy management is defined as the process of managing the **sources and consumers of energy** in a node or in the network as a whole for enhancing the lifetime of the network.

- Transmission power
- Battery energy management: chemical properties, discharge patterns, and by the selection of a battery from a set of batteries that is available for redundancy
- Processor power management: clock speed and the number of instructions executed per unit time
- Devices power management: Sleep scheduling (OS)

# Scalability Issues in Ad Hoc Networks

There are various **definitions** of scalability:

- **Administrative scalability:** The ability for an increasing number of organizations or users to access a system.
- **Functional scalability:** The ability to enhance the system by adding new functionality without disrupting existing activities.
- **Load scalability:** The ability for a distributed system to expand and contract to accommodate heavier or lighter loads, including, the ease with which a system or component can be modified, added, or removed, to accommodate changing loads.
- **Geographic scalability:** The ability to maintain effectiveness during expansion from a local area to a larger region.
- **Heterogeneous scalability:** the ability to adopt components from different vendors.

# Deployment Issues in Ad Hoc Networks

- Low cost of deployment
- Incremental deployment
- Short deployment time
- Reconfiguration possibility
- Deployment scenario: military, emergency, commercial, home, ...
- Longevity of network (required lifetime)
- Coverage area
- Service availability: ability of an ad hoc wireless network to provide service even with the failure of certain nodes
- Integration with other networks and infrastructure
- Choice of protocols

# Agenda

- 1 Objectives
- 2 Ad Hoc Networks
- 3 Research and Design Issues in Ad Hoc Networks
- 4 Classification of Ad Hoc Networks**
- 5 Applications

# Classification of Ad Hoc Networks

- Mobile Ad Hoc Networks (MANET)
- Vehicular Ad Hoc Networks (VANET)
- Wireless Sensor Actuator Networks (WSAN)
- Wireless Mesh Networks (WMN)

There are other classifications: homogeneous/heterogeneous, single-tier/multi-tier,

# Mobile Ad Hoc Networks (MANET)

- Infrastructure-less, self-\* network of mobile devices
- Highly dynamic topology
- Every device runs not only data plane (forwarding) but also control plane (routing) in layer three
- May employ spatial multiplexing
- Physical layer limitations are severe
- Limited bandwidth
- Throughput scales with rate  $\sqrt{N}$  where  $N$  is the network size
- Cooperation required in heterogeneous MANETs

# Vehicular Ad Hoc Networks (VANET)

- Spontaneous data exchange among vehicles
- A part of the Intelligent Transportation System: cooperative driving, collision avoidance, info sharing,
- V2V: vehicle-to-vehicle communication
- V2I: vehicle-to-infrastructure communication
- Mobility of devices confined with the roads
- Higher mobility

# Flying Ad Hoc Networks (FANET)

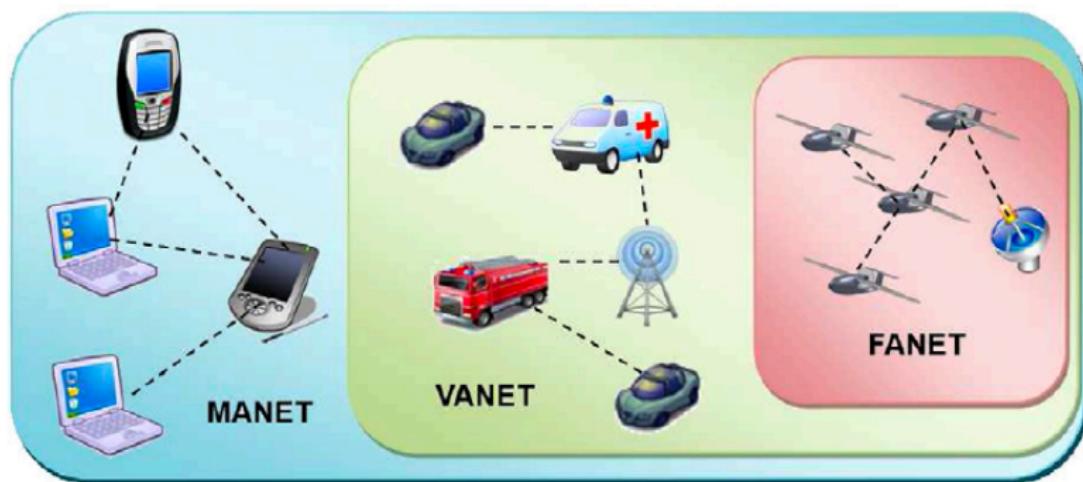
- A MANET in essence
- Mobility is much much higher
- Topology changes are much much frequent
- Peer-to-peer and convergecast communication both required
- Typical inter-node distances much larger
- Energy mostly consumed for flying
- Lower density
- Three-dimensional scenarios
- Different propagation characteristics

# MANET versus VANET versus FANET

Take the following with **discount**, the application dictates the requirements.

Measure	MANET	VANET	FANET
Cost of deployment	low	high	high
Mobility	low	high	very high
Topology changes	slow	fast	fast
Mobility	unpredictable	confined to roads (partially predictable)	unpredictable or regular
Mode of operation	infrastructure-less	hybrid	hybrid
Node density	low	high	very low
Computational power of nodes	limited	high	high

# MANET versus VANET versus FANET



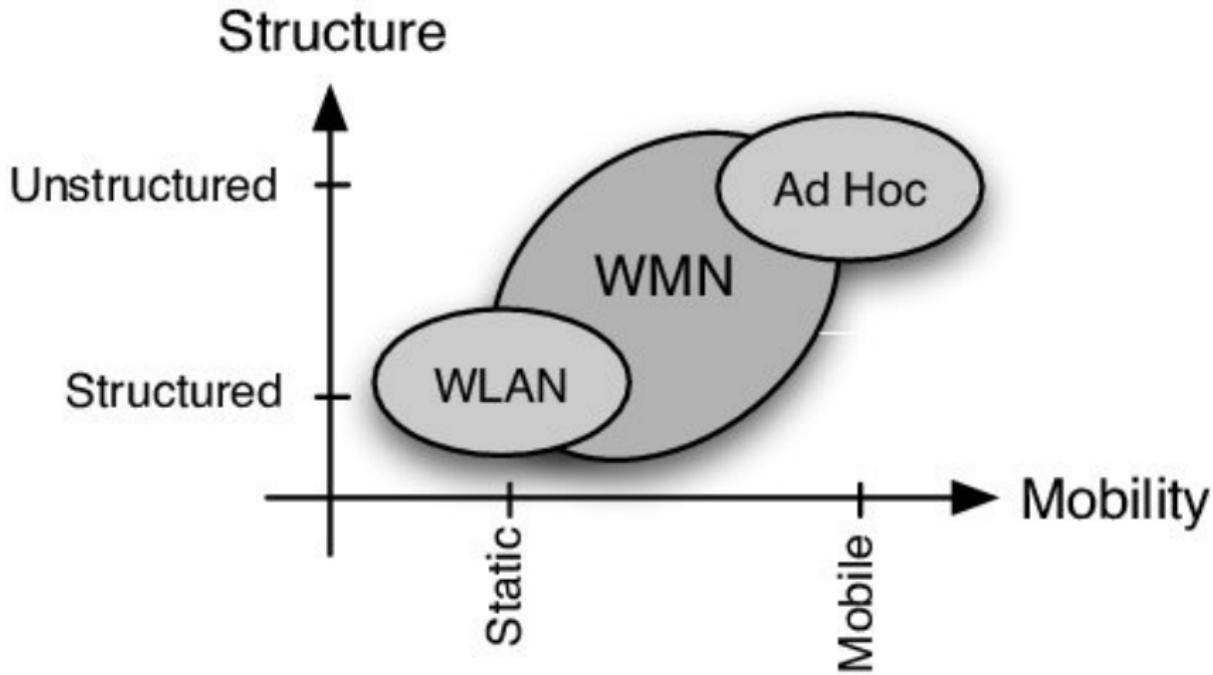
# Wireless Sensor (Actuator) Networks (WSAN)

- Large-scale, dense deployment of (mostly) stationary nodes over an area
- Nodes are equipped with sensors and actuators
- Sensed phenomenon digitized and conveyed to a center (sink)
- Short- or long-range low-power radio, ( mostly multi-hop) convergecast communication
- Small-sized, constrained (cpu, memory, disk, power, etc.), cheap nodes
- Mostly battery-driven nodes: extremely high energy efficiency requirement
- Autonomous

# Wireless Mesh Networks (WMN)

- **mesh:** rich interconnection among nodes
- Composed of mesh routers, mesh clients and gateways
- Less mobility of clients, infrequent topology changes
- Can call it: Low-mobility MANET!
- Redundant links, robustness to failures
- Integrated to legacy networks
- Applications: broadband home network, metropolitan area networks, transportation systems

# WMN versus Ad hoc Networks



# Agenda

- 1 Objectives
- 2 Ad Hoc Networks
- 3 Research and Design Issues in Ad Hoc Networks
- 4 Classification of Ad Hoc Networks
- 5 Applications

# Applications of Ad Hoc Networks

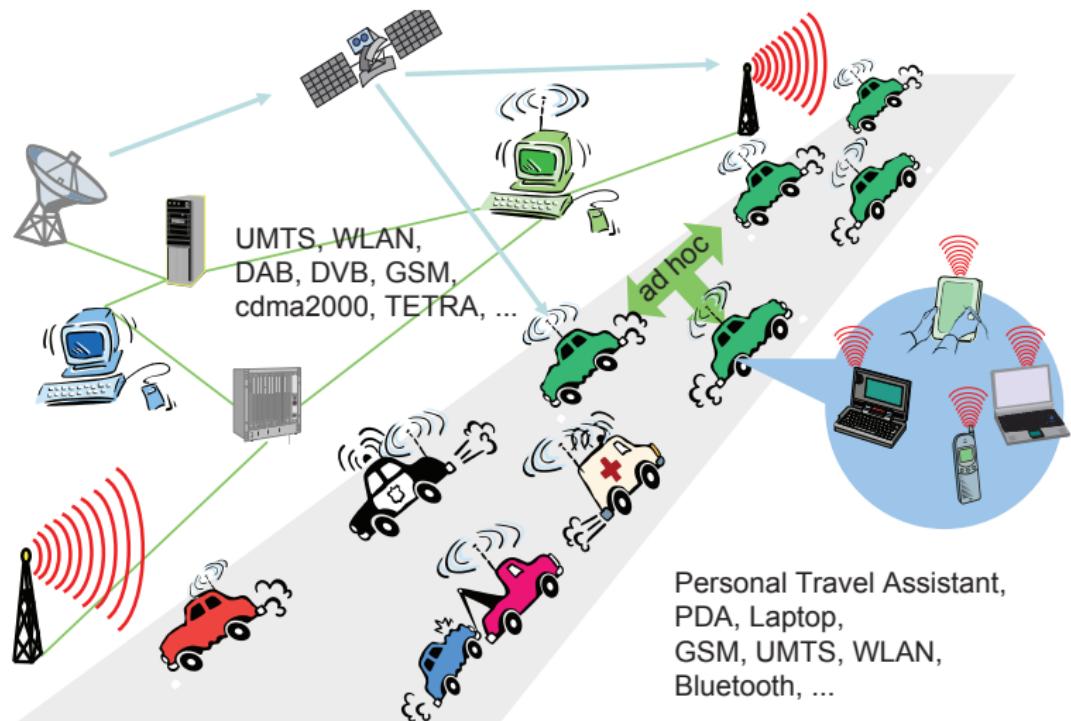
Ad hoc networks are suited for use in situations where infrastructure is either not available, not trusted, or should not be relied on in times of emergency. A few examples include:

- military soldiers in the field
- sensors scattered throughout a city for biological detection
- an infrastructureless network of notebooks in a conference or campus
- robot networks
- rare animal tracking
- space exploration
- undersea operations
- and temporary offices such as campaign headquarters

## Utopia

Global Infosphere (Ad Hoc Internet): all network elements form a gigantic ad hoc wireless network using unlicensed spectrum, bypassing the existing infrastructure.

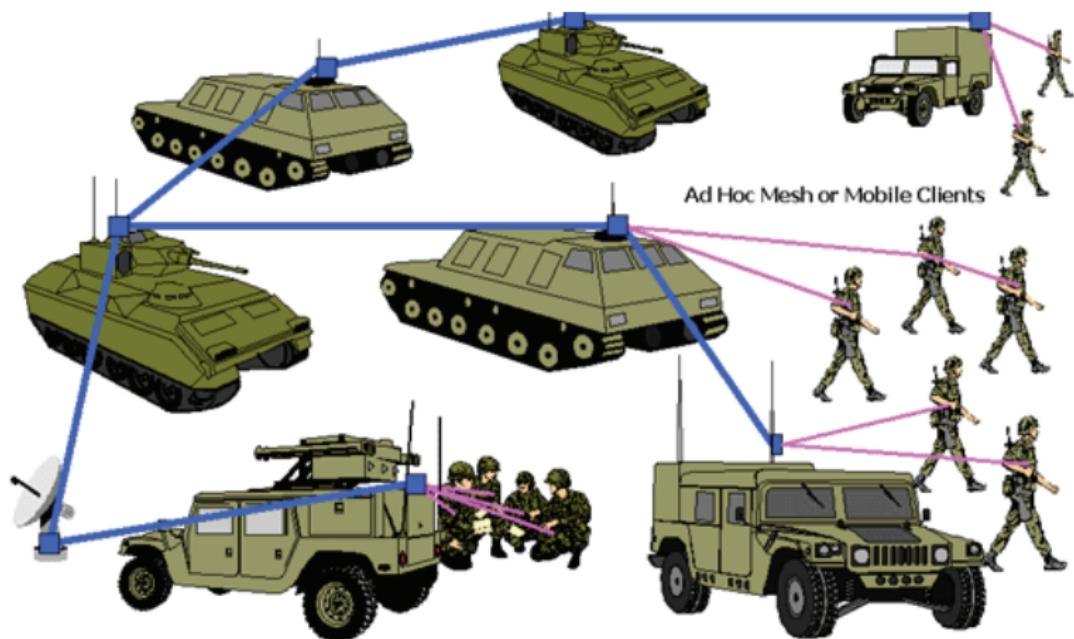
## Application: Road Traffic



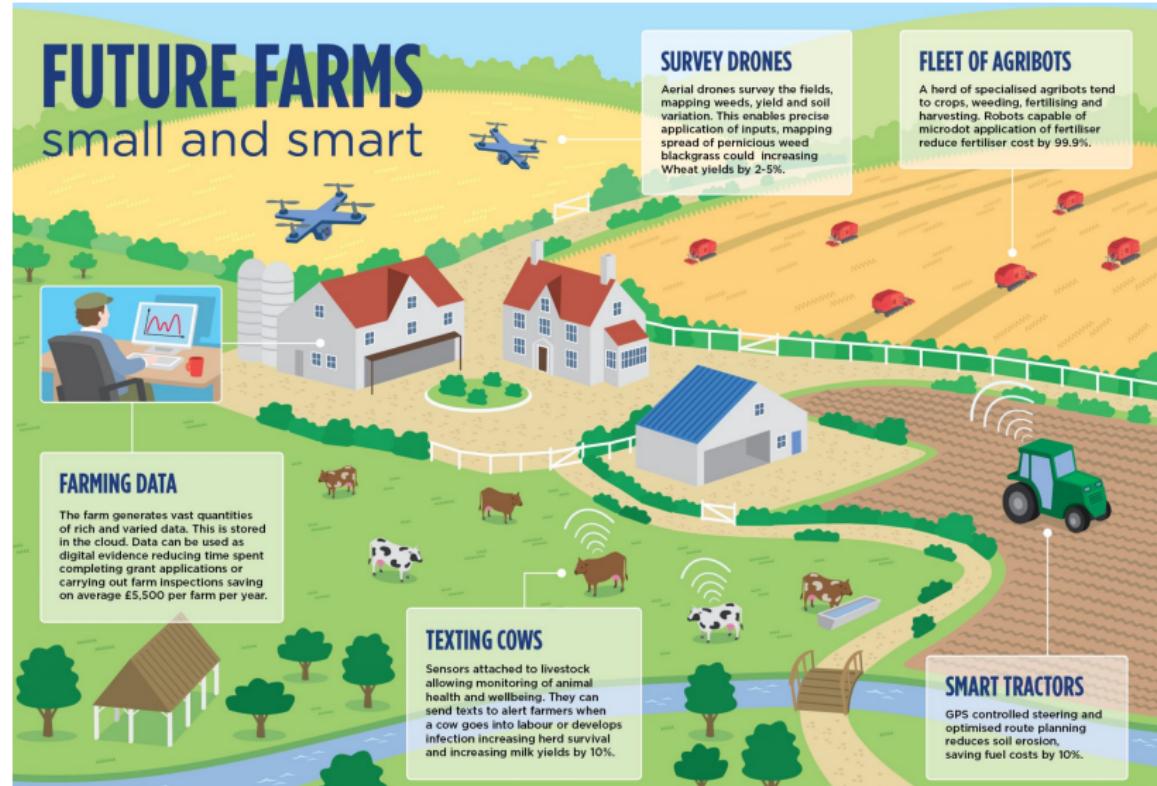
# Application: Disaster Recovery



# Application: Battlefield



# Application: Smart Farm



# What Did We Learn Today?

- Introduction to ad hoc networks
- Architectures
- Sample applications
- Research challenges and issues

# References

## Reading

- Sarkar, Chapter 1
- Manoj Chapter 5
- F. Baker, "An outsider's view of MANET," Internet Engineering Task Force document (text file), 17 March 2002.
- M. Frodigh, et al, "Wireless Ad Hoc Networking: The Art of Networking without a Network," Ericsson Review, No. 4, 2000. online

## Lecture 2: Wireless Technologies

# Agenda

## 6 Objectives

- 7 Classification of Wireless Technologies
- 8 Short-range Wireless Technologies
- 9 Low-power Wide Area Network Standards
- 10 Wrap-up

# Lecture Objectives

At the end of this lecture, you will be able to

1. **define** basic wireless technologies that can be employed in ad hoc networks
2. **compare** the existing standards for wireless communications



# Agenda

6 Objectives

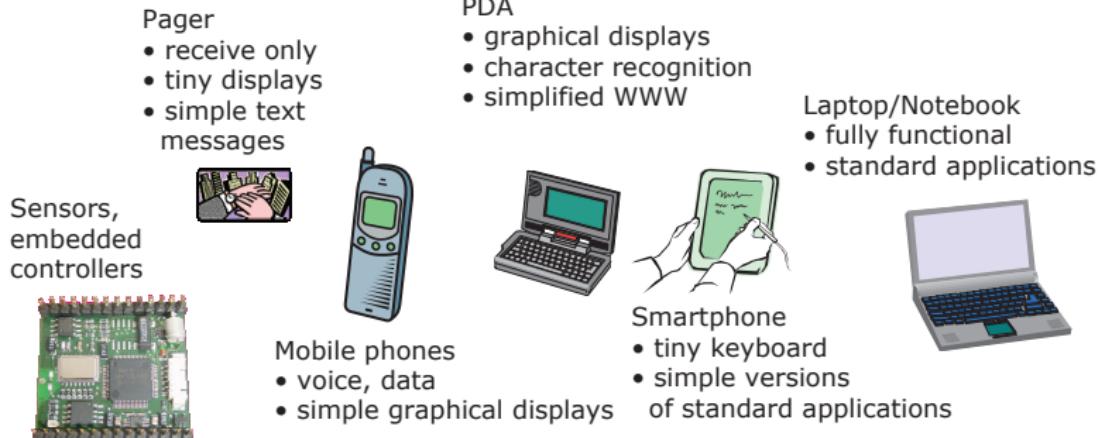
7 Classification of Wireless Technologies

8 Short-range Wireless Technologies

9 Low-power Wide Area Network Standards

10 Wrap-up

# Devices

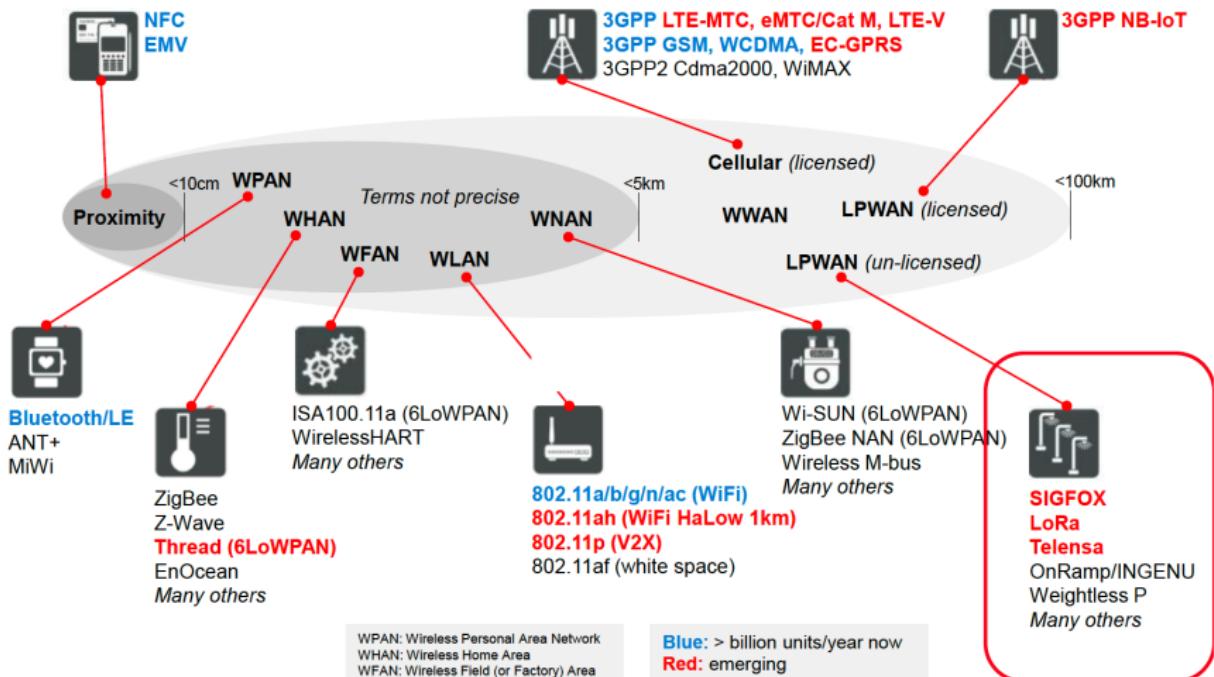


No clear separation between device types possible  
(e.g. smart phones, embedded PCs, ...)

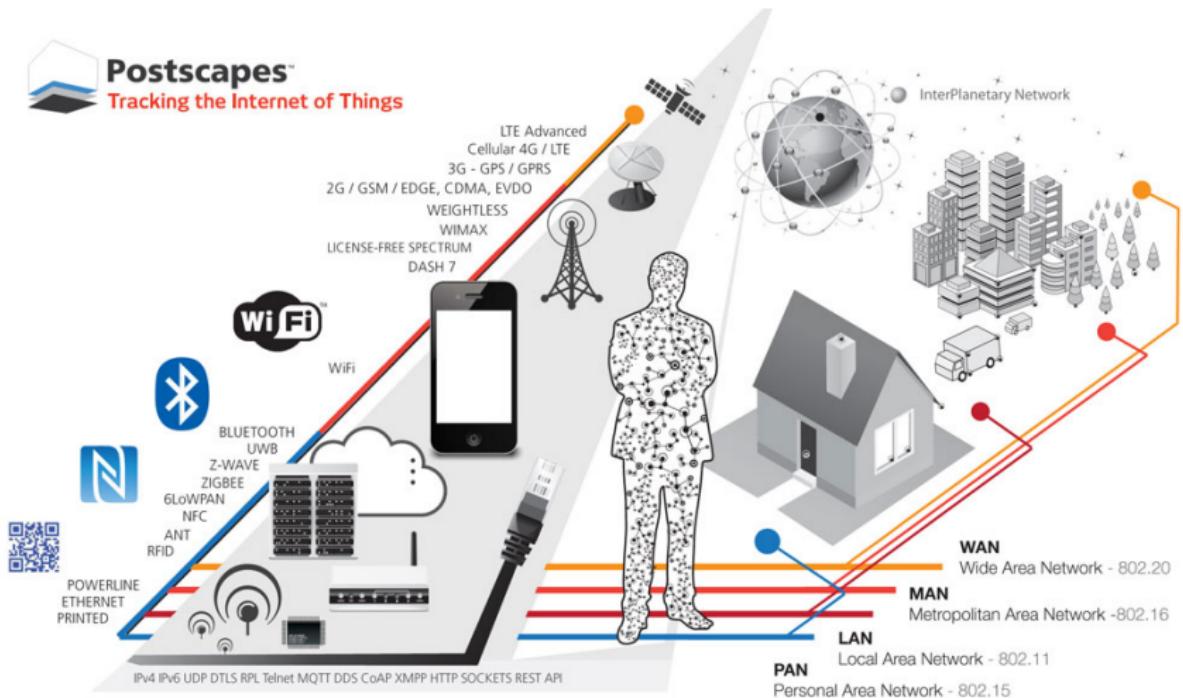
# Too many wireless connectivity standards?



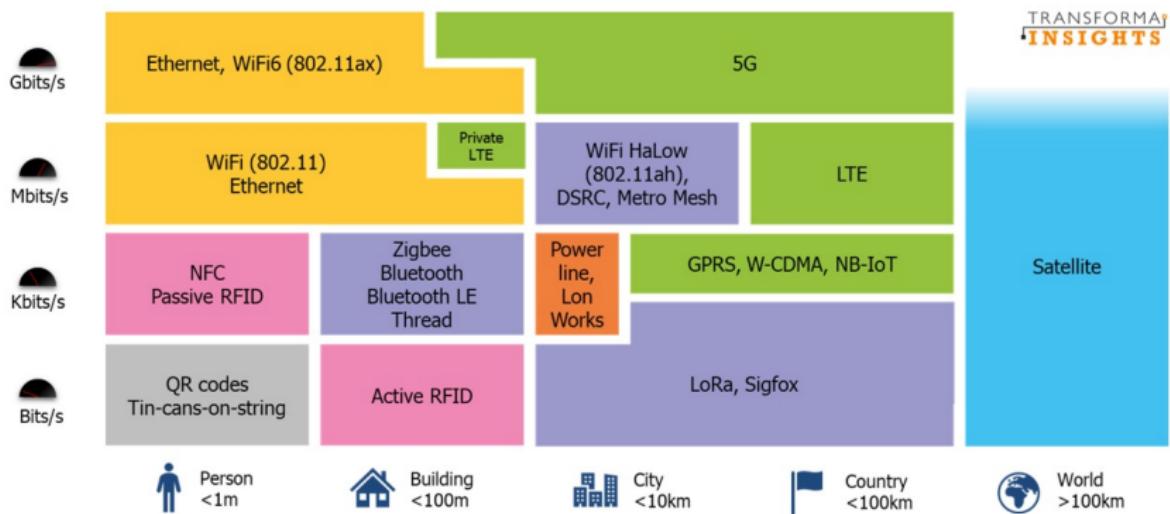
# Region-based Classification



# Region-based Classification



# Taxonomy of Wireless Technologies



# Agenda

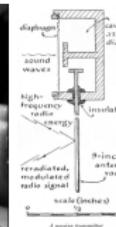
- 6 Objectives
- 7 Classification of Wireless Technologies
- 8 Short-range Wireless Technologies**
- 9 Low-power Wide Area Network Standards
- 10 Wrap-up

# Short-range Wireless Technologies

- **RFID**: Radio-frequency Identification
- **NFC**: Near-field Communications
- **IrDA**: Infrared Data Association
- **IEEE 802.15 Family**
- **Bluetooth and Bluetooth Low Energy (BLE)**
- **Zigbee**
- **Thread**
- **Wi-Fi**

# RFID: Radio-frequency Identification I

Application: Identification, Tracking, Locating, Monitoring, ...



## Great Embassy Seal Bug: The Thing

In 1946, Soviet school children presented a two foot wooden replica of the Great Seal of the United States to Ambassador Averell Harriman. During George F. Kennan's ambassadorship in 1952, a Secret technical surveillance countermeasures (TSCM) Inspection discovered that the seal contained a microphone and a resonant cavity which could be stimulated from an outside radio signal. Mic is active only when a radio signal of the correct frequency was sent from an external transmitter.

# RFID: Radio-frequency Identification II

- Wireless non-contact system.
- Used for automatic identification.
- Made of two separate parts
  - A reader or interrogator.
  - A transponder or tag containing data.
- Works from  $<1\text{cm}$  range to  $>10\text{m}$ .
- Frequency: from  $\approx 135\text{ KHz}$  to  $5.8\text{ GHz}$  range.
- Two types of tags:
  - **Passive**: has no energy source except the reader. Operate without battery, derive power from the field generated by the reader, less expensive, unlimited life, require more powerful readers and orientation sensitivity.
  - **Active**: has a battery or another form of energy source (Energy harvesting). Powered by an internal battery, finite lifetime (because of battery), greater range, better noise immunity, and higher data transmission rates

# RFID: Radio-frequency Identification III

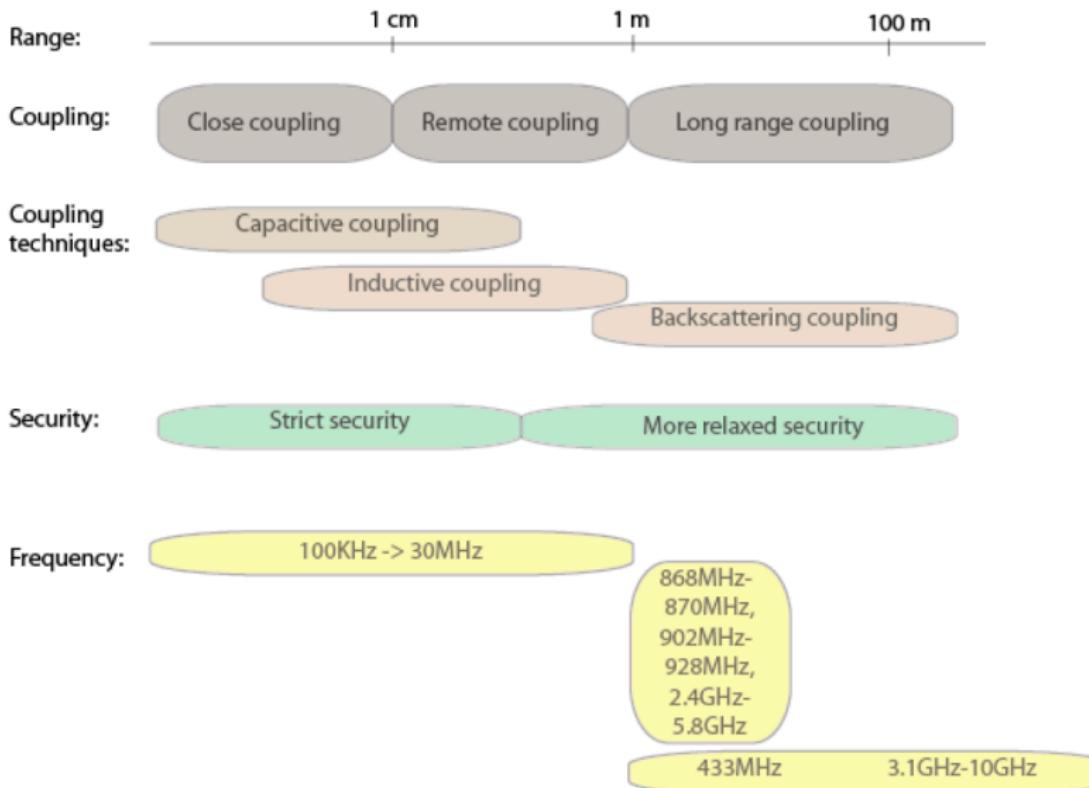
Three coupling techniques are:

- **Backscatter**: the signal leaves the reader, hits the tag, parts of the signal is reflected back, and the reflected signal properties can be changed by adding a load across the tag antenna (modulating)
- **Inductive Coupling**: the tag is in close proximity (less than  $\lambda/2\pi$ ); mutual inductance between two coils; and data transmission is done via load modulation
- **Capacitive Coupling**: the tag is in very close proximity (inside the reader); plate capacitors constructed from coupling surface isolated from one another; and data transmission is done via load modulation.

## Backscatter networks: Tag-to-tag Communication

**Hot research topic**: Cheap form of ad hoc networking using RFID principles with backscatter coupling.

# RFID: Radio-frequency Identification IV



# NFC: Near-field Communications I

NFC is an RFID with the following properties:

- Frequency:  $13.56\text{ MHz} \pm 7\text{ KHz}$ .
- Range:  $< 20\text{ cm}$ .
- Inductive coupling.
- Data rate: 106 kbps to 424 kbps.
- Tags can be active/passive.
- Digital Modulation: ASK, PSK or FSK.
- Standards: RFID standard ISO 14443, ISO 18092 and ECMA-340.

# IrDA: Infrared Data Association I

- **Point-to-point**, narrow-angle ( $15^\circ$ ), ad hoc data transmission standard
- **Point-and-shoot**, LoS, low BER, half-duplex
- Range: from contact to at least 1-2 meters
- Bidirectional communication; 9.6 Kbps up to 1 Gbps.
- Modulation: baseband, no carrier
- Wireless optical communication; wavelength: 850–900 nm
- Frequency below the red end of spectrum making it invisible

Bluetooth	IrDA
Penetrate solid objects	Almost impossible
Omnidirectional	Directional
Broadcast	One-to-one communication
Security mechanisms	Narrow-beam $\Rightarrow$ deafness
Cost: xxx	x

# IrDA: Infrared Data Association II

## Line Codes:

- **SIR**: 9.6–115.2 kbit/s, asynchronous, RZI (return-to-zero)
- **MIR**: 0.576–1.152 Mbit/s, RZI
- **FIR**: 4 Mbit/s,
- **VFIR**: 16 Mbit/s, NRZ
- **UFIR**: 96 Mbit/s, NRZI, 8b/10b
- **GigaIR**: 512 Mbit/s – 1 Gbit/s, NRZI, 2-ASK, 4-ASK, 8b/10b

# IrDA: Infrared Data Association III

Protocol stack:

- **IrPHY**: SIR, MIR, ..., GigaIR
- **IrLAP**: Link layer. Access control, discovery of partners, establishing reliable bidirectional connection, distribution of the primary/secondary device roles, negotiation of QoS parameters
- **IrLMP**: Multiplexer. Provides multiple logical channels; allows change of primary/secondary devices
- **Tiny TP**: Tiny Transport Protocol. Segmentation and reassembly, flow control.
- **IrCOMM**: OSI layer 5-7. Device acts like serial or parallel port
- **IrLAN**: Infrared Local Area Network on Tiny TP. Access point or peer-to-peer

# IEEE 802.15 Protocol Architecture

Bluetooth, Zigbee, 60 GHz

## 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

# Bluetooth I

- Universal short-range wireless capability
- Operates in the 2.4 GHz ISM band: available globally for unlicensed users
- Frequency-hop Spread Spectrum (FHSS)
- Supports up to 8 devices in a *piconet*
- Omnidirectional, NLOS transmission through walls
- 10 m to 100 m range
- Low cost
- 1 mW power
- Extend range with external power (100 meters)
- Started as IEEE 802.15.1: New standards come from the Bluetooth Special Interest Group (Bluetooth SIG)
- Bluetooth 2.0, 2.1, 3.0, 4.0 and 5.0

# Bluetooth II

## Application areas:

- Data and voice access points
  - Real-time voice and data transmissions
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
- Ad hoc networking
  - Can establish connection with another when in range

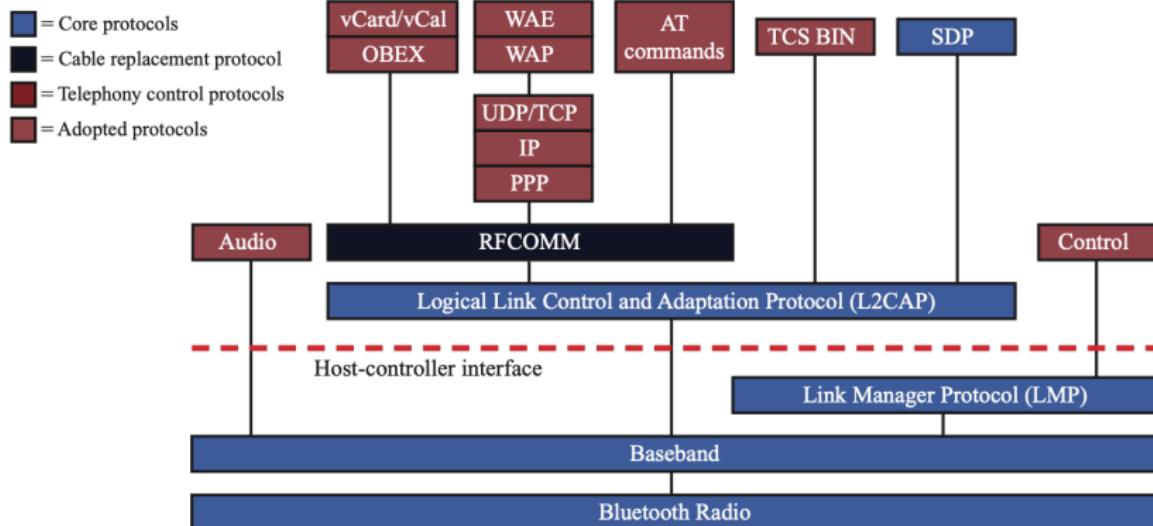


# Bluetooth III

## Bluetooth Standards Documents:

- Core specifications
  - Details of various layers of Bluetooth protocol architecture
- Profile specifications
  - Use of Bluetooth technology to support various applications
- We first focus on
  - 2.1 Basic/Enhanced Data Rate (BR/EDR)
- Later standards
  - 3.0 Alternative MAC/PHY (AMP)
  - 4.0 Bluetooth Smart (Bluetooth Low Energy)

# Bluetooth IV



AT	= Attention sequence (modem prefix)	TCS BIN	= Telephony control specification - binary
IP	= Internet Protocol	UDP	= User Datagram Protocol
OBEX	= Object exchange protocol	vCal	= Virtual calendar
PPP	= Point-to-Point Protocol	vCard	= Virtual card
RFCOMM	= Radio frequency communications	WAE	= Wireless application environment
SDP	= Service discovery protocol	WAP	= Wireless application protocol
TCP	= Transmission control protocol		

# Bluetooth V

## Stack

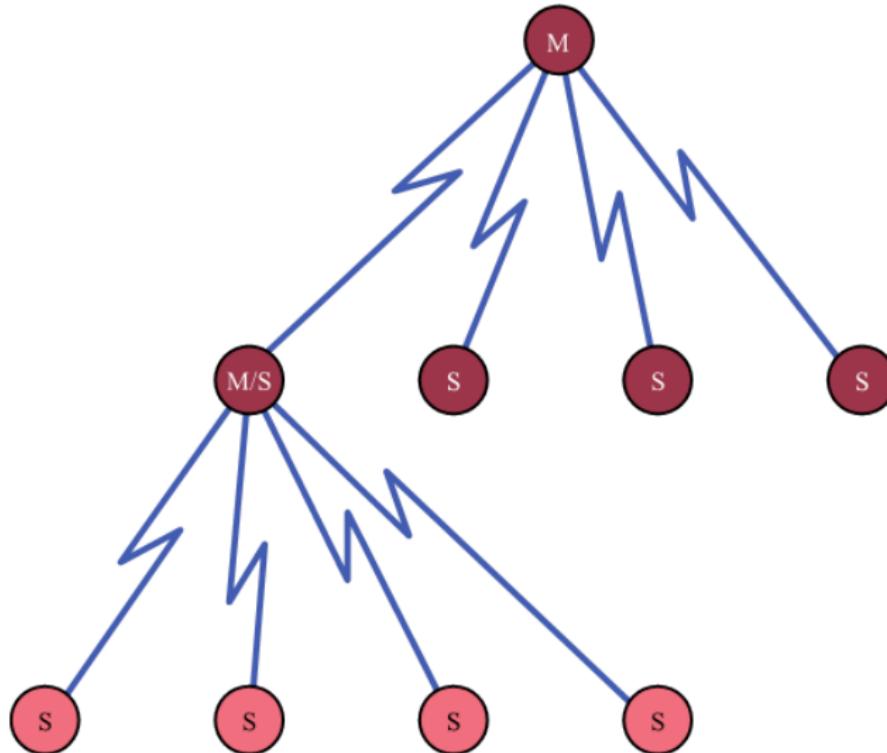
- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)
- Cable replacement protocol
  - RFCOMM
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols: PPP, TCP/UDP/IP, OBEX, WAE/WAP

# Bluetooth VI

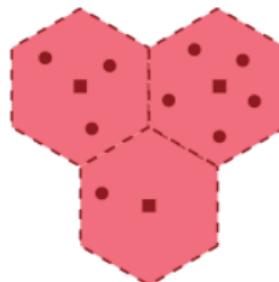
## Piconets and Scatternets

- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel and phase
- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth
- Bluetooth and IEEE 802.15

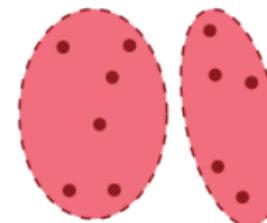
# Bluetooth VII



# Bluetooth VIII



(a) Cellular system (squares represent stationary base stations)



(b) Conventional ad hoc systems



(c) Scatternets

# Bluetooth IX

Bluetooth uses FHSS: Frequency Hopping Spread Spectrum Radio Specification

- Classes of transmitters
  - **Class 1:** Outputs 100 mW for maximum range
    - ▶ Power control mandatory
    - ▶ Provides greatest distance, 100 m
  - **Class 2:** Outputs 2.4 mW at maximum
    - ▶ Power control optional
    - ▶ Range 10 m
  - **Class 3:** Nominal output is 1 mW
    - ▶ Lowest power
    - ▶ Range 1 m
  - **Class 4:** Nominal output is 0.5 mW
    - ▶ Lowest-Lowest power
    - ▶ Range 0.5 m

# Bluetooth X

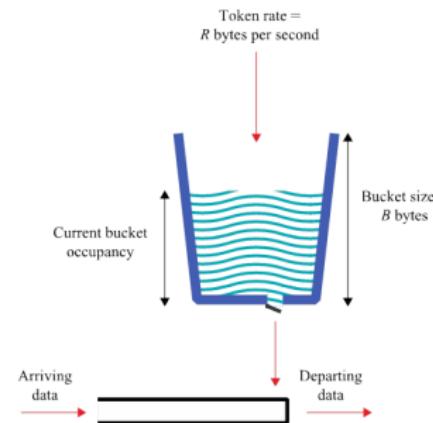
## Physical Links between Master and Slave

- **Synchronous connection oriented (SCO)**
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- **Asynchronous connectionless (ACL)**
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist
- **Extended Synchronous connection oriented (eSCO)**
  - Reserves slots just like SCO
  - But these can be asymmetric
  - Retransmissions are supported

# Bluetooth XI

## Flow Specification:

- Service type
- Token rate (bytes/second)
- Token bucket size (bytes)
- Peak bandwidth (bytes/second)
- Latency (microseconds)
- Delay variation (microseconds)



# Bluetooth XII

## Bluetooth 3.0+HS: High Speed

- Up to 24 Mbps
- New controller compliant with 2007 version of IEEE 802.11
- Known as Alternative MAC/PHY (AMP)
  - Optional capability
- Bluetooth radio still used for device discovery, association, setup, etc.
- Allows more power efficient Bluetooth modes to be used, except when higher data rates are needed

# Bluetooth XIII

## Bluetooth 4.0: Bluetooth Low Energy

- An intelligent, power-friendly version of Bluetooth
- Can run long periods of time on a single battery
  - Or scavenge for energy
- Also communicates with other Bluetooth-enabled devices
  - Legacy Bluetooth devices or Bluetooth-enabled smartphones
  - Great feature
- Possible successful technology for the Internet of Things
  - For example, health monitoring devices can easily integrate with existing smartphones

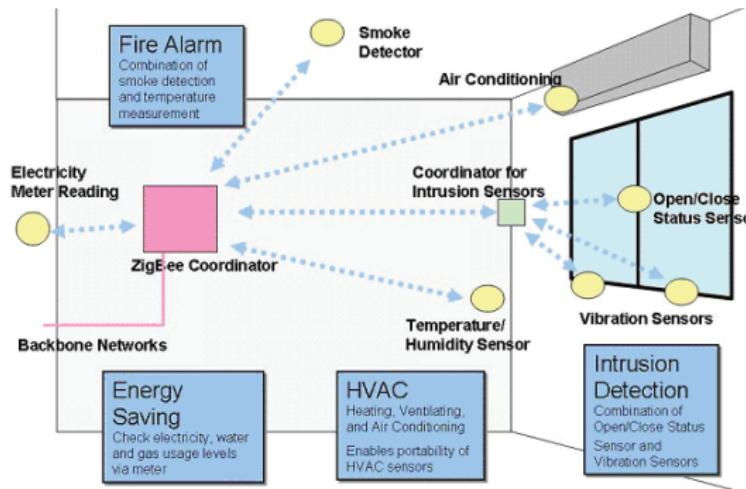
# Bluetooth XIV

## Bluetooth 5.0: for Internet of Things (IoT)

- BLE with 2x speed, 4x range
- 2 Mbit/s PHY for LE
- LE Long Range
- Maximum transmit power: +20 dBm (100 mW)
- Angle of Arrival (AoA) and Angle of Departure (AoD) which are used for location and tracking of devices
- Mesh-based model hierarchy
- Advertisement (beaconing) and channel selection algorithms revised

# Zigbee I

- Specification of protocols for small, low-power radios
- Low data rate (1Mbps bit-rate) PAN/WSN technology
- Has provisions for multi-hop
- Low bandwidth
- Power consumption ZigBee: 10mA vs. BT: 100mA
- Production costs (2005) ZigBee: 1 vs. BT: 3
- Development costs Codesize ZB/codesize BT =  $\frac{1}{2}$

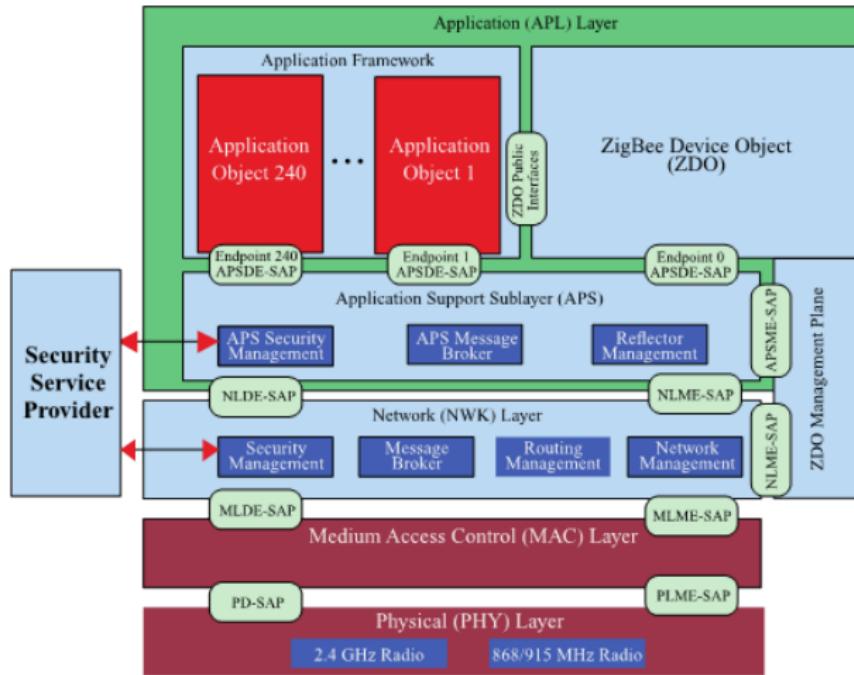


# Zigbee II

- Extends IEEE 802.15.4 standards
- Low data rate, long battery life, secure networking
- Data rates 20 to 250 kbps
- Operates in ISM bands
  - 868 MHz (Europe), 915 MHz (USA and Australia), 2.4 GHz (worldwide)
- Quick wake from sleep
  - 30 ms or less compared to Bluetooth which can be up to 3 sec.
  - ZigBee nodes can sleep most of the time
- ZigBee complements the IEEE 802.15.4 standard by adding four main components
  - Network layer provides routing
  - Application support sublayer supports specialized services.
  - ZigBee device objects (ZDOs) are the most significant improvement
    - ▶ Keep device roles, manage requests to join the network, discover devices, and manage security.
  - Manufacturer-defined application objects allow customization.

# Zigbee III

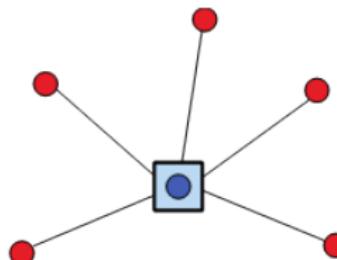
- IEEE 802.15.4 defined
- ZigBee™ Alliance defined
- End manufacturer defined
- Layer function
- Layer interface



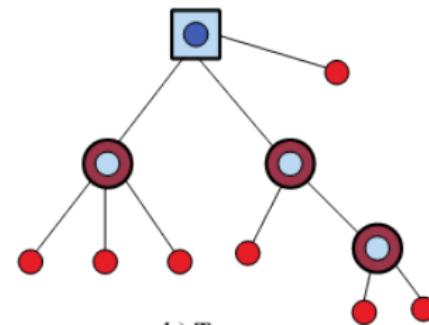
# Zigbee IV

- Star, tree, or general mesh network structures
- ZigBee Coordinator
  - Creates, controls, and maintains the network
  - Only one coordinator in the network
  - Maintains network information, such as security keys
- ZigBee Router
  - Can pass data to other ZigBee devices
- ZigBee End Device
  - Only enough funct. to talk to a router/coordinator
  - Cannot relay information
  - Sleeps most of the time
  - Less expensive to manufacture

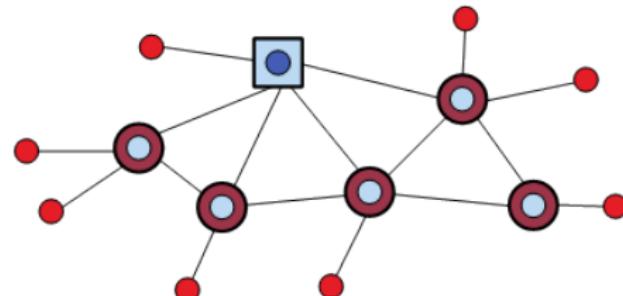
# Zigbee V



a) Star



b) Tree



c) Mesh

- ZigBee Coordinator
- ZigBee Router
- ZigBee End Device

# Zigbee VI

- Industry consortium
- Maintains and publishes the ZigBee standard
  - ZigBee specifications in 2004
  - ZigBee PRO completed in 2007
    - ▶ Enhanced ZigBee
    - ▶ Profile 1 – home and light commercial use
    - ▶ Profile 2 – more features such as multicasting and higher security
- Application profiles: Allow vendors to create interoperable products if they implement the same profile
  - ▶ ZigBee Building Automation (Efficient commercial spaces)
  - ▶ ZigBee Health Care (Health and fitness monitoring)
  - ▶ ZigBee Home Automation (Smart homes)
  - ▶ ZigBee Input Device (Easy-to-use touchpads, mice, keyboards, wands)
  - ▶ ZigBee Light Link (LED lighting control)
  - ▶ ZigBee Network Devices (Assist and expand ZigBee networks)
  - ▶ ZigBee Retail Services (Smarter shopping)
  - ▶ ZigBee Remote Control (Advanced remote controls)
  - ▶ ZigBee Smart Energy 1.1 (Home energy savings)
  - ▶ ZigBee Smart Energy Profile 2 (IP-based home energy management)
  - ▶ ZigBee Telecom Services (Value-added services)

# Zigbee vs. Bluetooth

## ZigBee

- Very low duty cycle, very long primary battery life
- Static and dynamic star and mesh networks, >65,000 nodes, low latency
- Ability to remain quiescent for long periods without communications

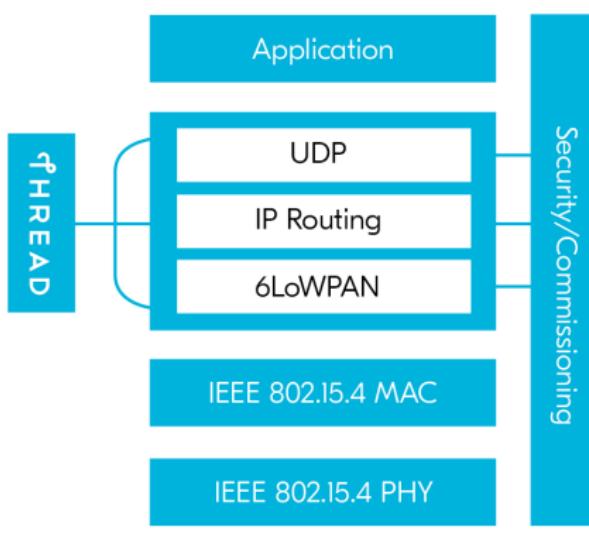
## Bluetooth

- Moderate duty cycle
- Very high QoS and very low, guaranteed latency
- Quasi-static star network, ability to participate in more than one network
- Frequency Hopping Spread Spectrum is difficult to create extended networks without large synchronization cost.

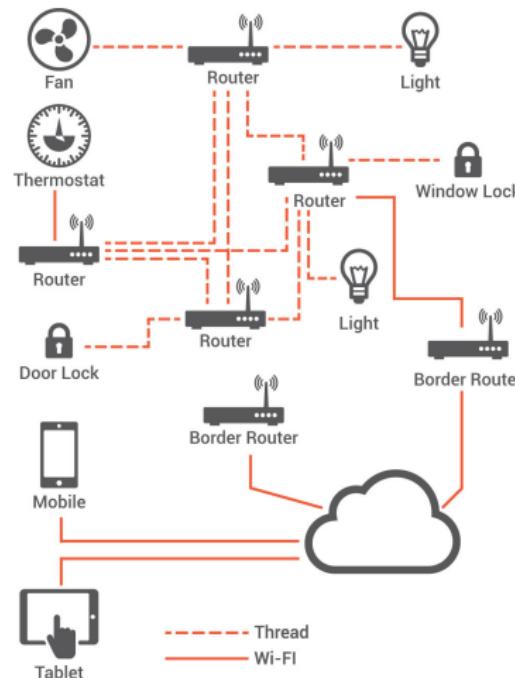
# Thread I

- On top of IEEE 802.15.4
- Open Protocol: Google, Apple, Siemens, ... supports: [openthread.org](http://openthread.org)
- Mostly Internet of Things
- IPv6 on 6LoWPAN and UDP at transport layer
- Extremely low power, range 20,30 m, 250 kbps
- Mesh network: no single point of failure, easy network setup, self-forming and -healing,
- Sleep scheduling
- 1 Leader, 32 routers, 511 end devices/router

# Thread II



# Thread III



# Thread IV

- A Thread device is either a Router (Parent) or an End Device (Child)
- A Thread device is either a Full Thread Device (maintains IPv6 address mappings) or a Minimal Thread Device (forwards all messages to its Parent)
- A Router Eligible End Device can promote itself to a Router, and vice versa Every Thread network partition has a Leader to manage Routers
- A Border Router is used to connect Thread and non-Thread networks
- A Thread network might be composed of multiple partitions

# Thread V

- A Thread network consists of three scopes: Link-Local, Mesh-Local, and Global
- A Thread device has multiple unicast IPv6 addresses
- An RLOC (Routeing Locator) represents a device's location in the Thread network
- An ML-EID (Mesh Local Endpoint Identifier) is unique to a Thread device within a partition and should be used by applications
- Thread uses multicast to forward data to groups of nodes and routers
- Thread uses anycast when the RLOC of a destination is unknown

# Thread VI

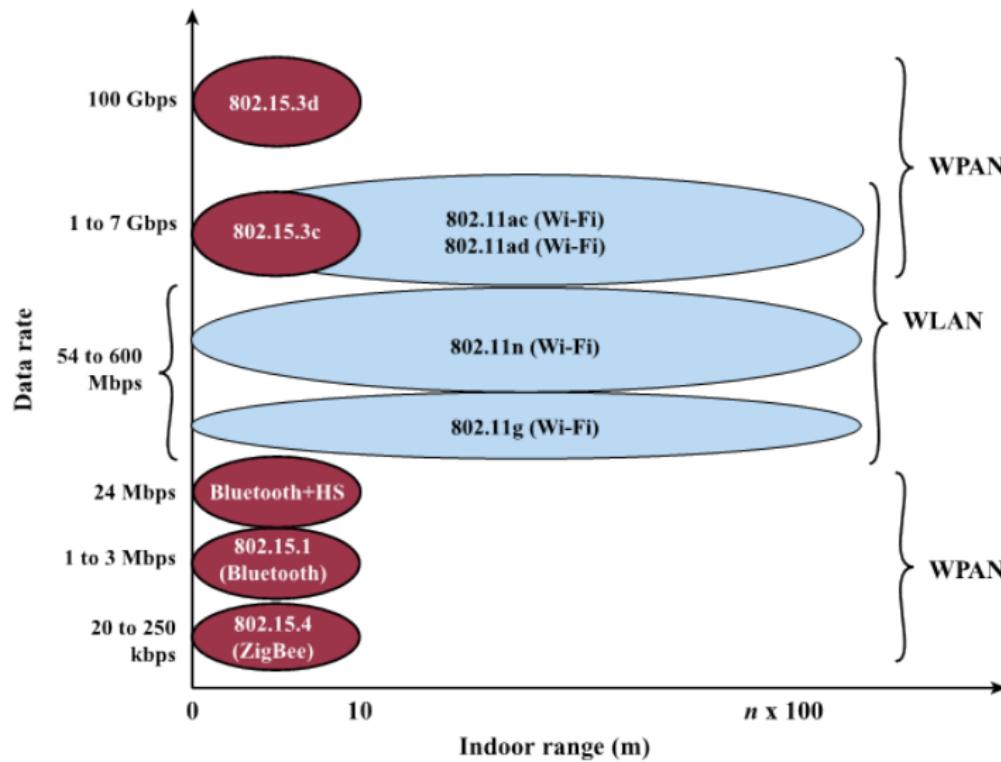
- Routers must form a **Connected Dominating Set (CDS)**, which means:
  - There is a Router-only path between any two Routers.
  - Any one Router in a Thread network can reach any other Router by staying entirely within the set of Routers.
  - Every End Device in a Thread network is directly connected to a Router.
- A **distributed algorithm** maintains the CDS, which ensures a minimum level of redundancy. Every device initially attaches to the network as an End Device (Child). As the state of the Thread network changes, the algorithm adds or removes Routers to maintain the CDS.
- Thread **adds Routers** to:
  - Increase coverage if the network is below the Router threshold of 16
  - Increase path diversity
  - Maintain a minimum level of redundancy
  - Extend connectivity and support more Children
- Thread **removes Routers** to:
  - Reduce the Routing state below the maximum of 32 Routers
  - Allow new Routers in other parts of the network when needed

## Thread VII

A **connected dominating set** of a graph  $G$  is a set  $D$  of vertices with two properties:

- Any node in  $D$  can reach any other node in  $D$  by a path that stays entirely within  $D$ . That is,  $D$  induces a connected subgraph of  $G$ .
- Every vertex in  $G$  either belongs to  $D$  or is adjacent to a vertex in  $D$ . That is,  $D$  is a dominating set of  $G$ .

## 12.10 Wireless Local Networks I



# Comparison of Short-range Wireless Technologies

	RFID	NFC	Zigbee	Thread	BLE	Bluetooth	Wi-Fi
Range (m)	10	0.10	200	200	300	100	300
Frequency GHz	0.01356 0.433 0.84 0.96 2.4	0.01356	2.4	2.4	2.4	2.4	2.4/5
Topology	P2P	P2P	mesh	mesh	P2P, Star	P2P, Star, Mesh	P2P, Star
Rate (kbps)	≈8	64-400	250	250	1400	2100	depends
Power req.	Very low	Very low			Low	High	Very high
Open standard	Yes	Yes			Yes	Yes	Yes
Network size			500+	350+	30	8	250
Setup time	<0.1 ms	<0.1 ms				<6 s	
Modulation	ASK, FSK, PSK Load modulation	ASK Load mod.					

# Agenda

- 6 Objectives
- 7 Classification of Wireless Technologies
- 8 Short-range Wireless Technologies
- 9 Low-power Wide Area Network Standards**
- 10 Wrap-up

# Low-power Wide Area Network Standards

- Sigfox
- LoRa
- NB-IoT
- LTE-M

# Comparison of Low-power Wide Area Network Standards

	Sigfox	LoRa	NB-IoT	LTE-M
Cellular	No	No	Yes	Yes
Frequency	Unlic. <1 GHz	Unlic. <1 GHz	Licensed LTE	Licensed LTE
Bandwidth	100 Hz	125/250/500 kHz	200 kHz	1.4 MHz
Throughput (UL/DL)	100/65 bps	50 kbps	50 kbps	300/375 kbps
Range (km)	25+	10+	15+	11+
Latency	Very high	High	Low	Very low
Security	No	Good	Great	Great
Mobility	No	Yes	Partial	Yes
Roaming	No	No	Not yet	Yes
Open standard	No	No	Yes	Yes

# Comparison of Wireless Technologies

	Zigbee	Cellular	Wi-Fi	Bluetooth
Standard	802.15.4	GSM	802.11	802.15.1
Focus	Monitoring	Voice	Internet	Cable repl.
Resources	4-32KB	16MB	1MB	250KB
Life(day)	100-1000	1-7	.5-5	1-7
N/W size	$2^{64}$	1	32	7
Rate(kbps)	20 -250	64-128	11.000+	720
Range(m.)	1-100+	1000+	1-100	1-10+
Success	Power reliability, cost	Reach quality	Speed Flexibility	Cost Convenience

# Agenda

- 6 Objectives
- 7 Classification of Wireless Technologies
- 8 Short-range Wireless Technologies
- 9 Low-power Wide Area Network Standards
- 10 Wrap-up

# Research Challenges

- Smart, directional antennas
- Transmission power control, energy efficiency
- Multiple channels (MAC)
- Routing, dependability
- Fairness and Quality of Service (QoS)
- Transport layer
- Security and cooperation
- Mitigating malicious nodes

# What Did We Learn Today?

- Wireless technology overview
- Introduction to ad hoc networks
- Architectures
- Sample applications
- Research challenges

# References

## Compulsory Reading

Course book (Sarkar), Chapter 1.

## Optional Reading

- Akyildiz, I. F., Wang, X. and Wang, W., "Wireless Mesh Networks: A Survey," Computer Networks Journal (Elsevier), March 2005. PDF
- Akyildiz, I. F., and Kasimoglu, I. H., "Wireless Sensor and Actor Networks: Research Challenges," Ad Hoc Networks Journal (Elsevier), Vol. 2, pp. 351-367, October 2004. PDF

## Lecture 3: Overview of Wireless Communications

# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

# Objectives

After the end of the lectures, you will be able to

- Discuss characteristics of wireless signals,
- Understand spectrum considerations,
- Describe the simple path loss model,
- Discuss the impact of noise on channel performance,
- Describe mechanisms for channel correction.

The slides are from [8].

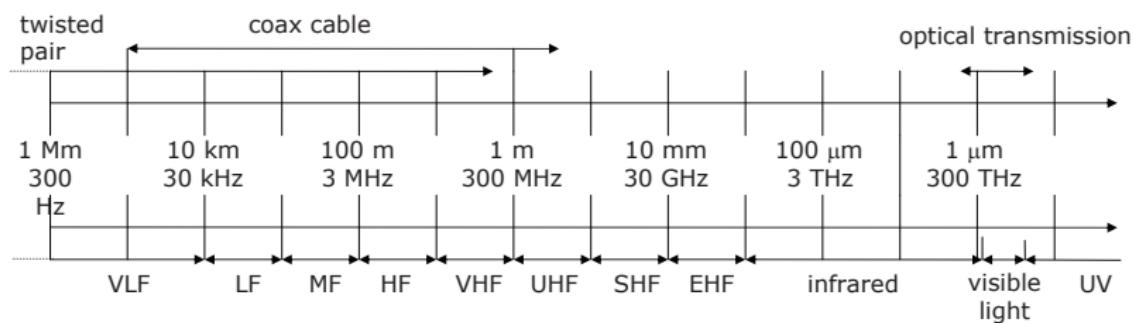
# Agenda

- 11 Objectives
- 12 **Wireless Signals**
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

# Frequencies for Communication

- VLF = Very Low Frequency
- LF = Low Frequency
- MF = Medium Frequency
- HF = High Frequency
- VHF = Very High Frequency

UHF = Ultra High Frequency  
SHF = Super High Frequency  
EHF = Extra High Frequency  
UV = Ultraviolet Light



# Frequency and Wavelength

$$\lambda = c/f$$

- $\lambda$  is the wavelength
- $c$  is the speed of light  $c \cong 3 \times 10^8$  m/s
- $f$  is the frequency

Example frequencies

- VHF-/UHF-ranges for mobile radio
- SHF and higher for directed radio links, satellite communication
- Wireless LANs use frequencies in UHF to SHF range

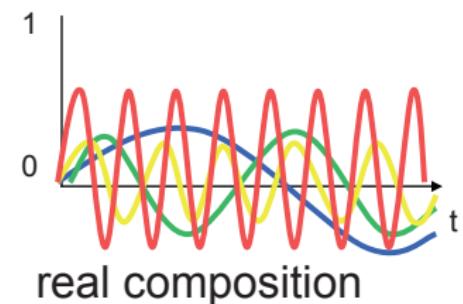
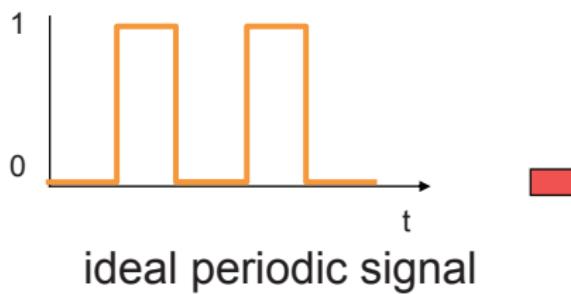
What is the wavelength of 802.11 b/g in cm? (Frequency = 2.4 GHz?)

# Signals

- physical representation of data
- function of time and location
- signal parameters: parameters representing value of data
- signal parameters of periodic signals
  - $T$  is the period,  $f$  is the frequency where  $f = 1/T$ ,  $A$  is the amplitude and  $\phi$  is the phase shift
  - e.g., sine wave (for a carrier):  $s(t) = A_t \sin(2\pi f_t t + \phi_t)$

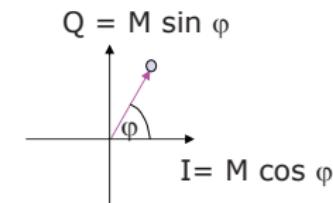
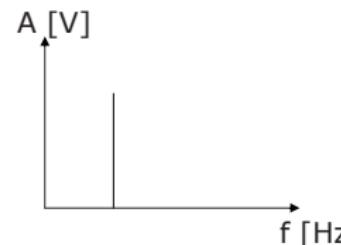
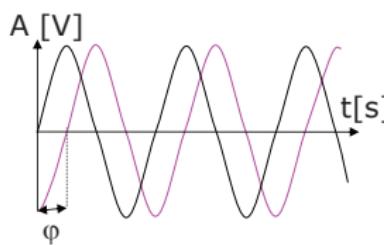
# Signals

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$



# Representation of Signals

- Amplitude: in time domain
- Frequency spectrum: in frequency domain
- Phase state diagram: amplitude  $M$  and phase  $\phi$  in polar coordinates



# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations**
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

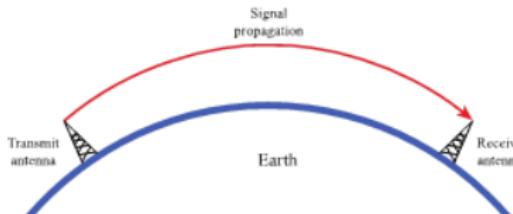
# Spectrum considerations

- Controlled by regulatory bodies
  - Carrier frequency
  - Signal Power
  - Multiple Access Scheme
    - ▶ Divide into time slots -Time Division Multiple Access (TDMA)
    - ▶ Divide into frequency bands - Frequency Division Multiple Access (FDMA)
    - ▶ Different signal encodings - Code Division Multiple Access (CDMA)
- Federal Communications Commission (FCC) in the United States regulates spectrum
  - Military, Broadcasting, Public Safety, Mobile, Amateur, Government exclusive, non-government exclusive, or both, Many other categories
- Industrial, Scientific, and Medical (ISM) bands
  - Can be used without a license
  - As long as power and spread spectrum regulations are followed
- ISM bands are used for
  - WiFi, Bluetooth, Zigbee, ...
  - Ad hoc networks

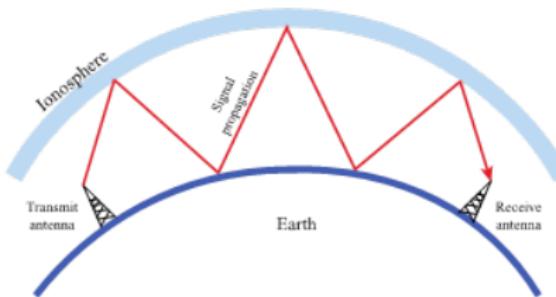
# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes**
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

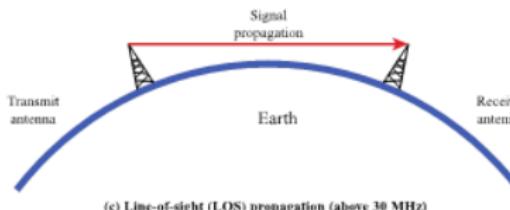
# Wireless Propagation Modes



(a) Ground wave propagation (below 2 MHz)



(b) Sky wave propagation (2 to 30 MHz)



(c) Line-of-sight (LOS) propagation (above 30 MHz)

- Ground-wave propagation
- Sky-wave propagation
- Line-of-sight propagation

# Ground Wave Propagation

- Follows contour of the earth
- Can propagate considerable distances
- Frequencies up to 2 MHz
- Example
  - AM radio
- Reason 1: Wavefront near the earth tilts downward and follows the earth's curvature
- Reason 2: Diffraction: waves in this frequency range are scattered by the atmosphere in such a way that they do not penetrate the upper atmosphere

# Sky Wave Propagation

- Signal reflected from ionized layer of atmosphere back down to earth
- Signal can travel a number of hops, back and forth between ionosphere and earth's surface
- Reflection effect caused by refraction
- Examples
  - Amateur radio (ham radio): non-commercial exchange of messages, wireless experimentation, self-training, private recreation, radiosport, contesting, and emergency communication
  - CB (citizen band) radio: short-distance person-to-person bidirectional voice communication

# Line-of-Sight Propagation

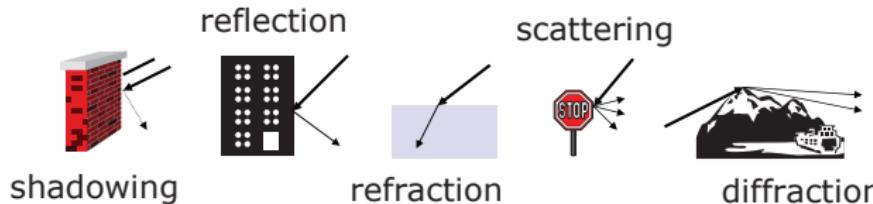
- Transmitting and receiving antennas must be within line of sight
  - Satellite communication - signal above 30 MHz not reflected by ionosphere
  - Ground communication - antennas within effective line of site due to refraction
- Refraction: communication is possible within an effective line of sight

# Five basic propagation mechanisms

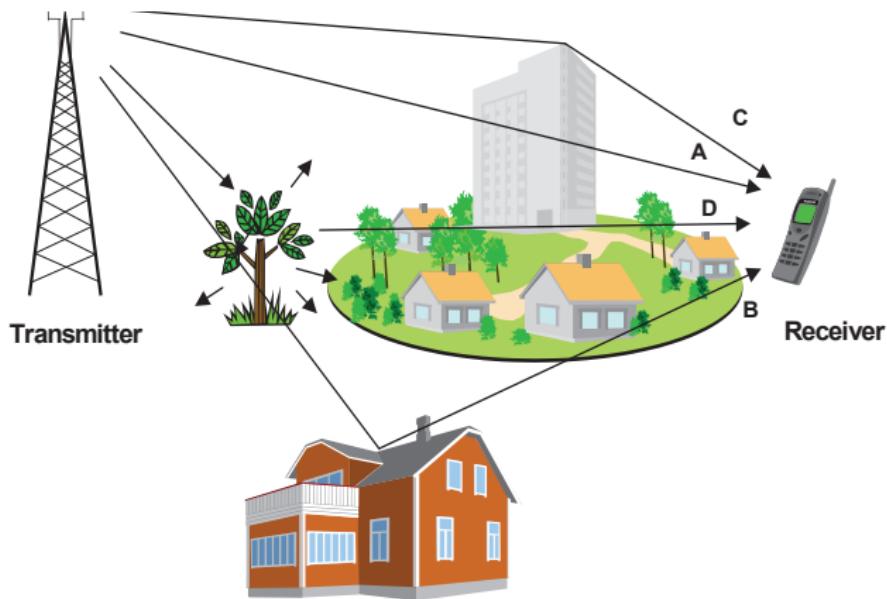
- Free-space propagation: **path loss**
- **Transmission**
  - Through a medium, density of medium is influential
  - **Refraction** occurs at boundaries: bending of microwaves by the atmosphere
    - ▶ Velocity of electromagnetic wave is a function of the density of the medium
    - ▶ When wave changes medium, speed changes
    - ▶ Wave bends at the boundary between media
- **Reflections**
  - Waves impinge upon surfaces that are large compared to the signal wavelength
- **Diffraction**
  - Secondary waves behind objects with sharp edges
- **Scattering**
  - Interactions between small objects or rough surfaces

# Signal Propagation

- Receiving power proportional to  $1/d^\eta$  (path-loss exponent  $\eta = 2$  in vacuum,  $d$ : distance)
- 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 (sharp irregularities)



# Multipath Propagation



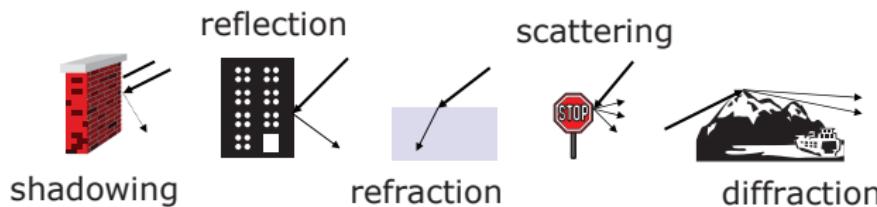
A: free space, B: reflection, C: diffraction, D: scattering

**reflection:** object is large compared to wavelength

**scattering:** object is small or its surface irregular

# Multipath Propagation

- Signal can take many different paths between sender and receiver due to reflection, scattering, diffraction
- The signal reaches a receiver directly and phase shifted: **distorted signal depending on the phases of the different parts**
- Time dispersion: signal is dispersed over time: **interference with neighbor symbols, Inter Symbol Interference (ISI)**



# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas**
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

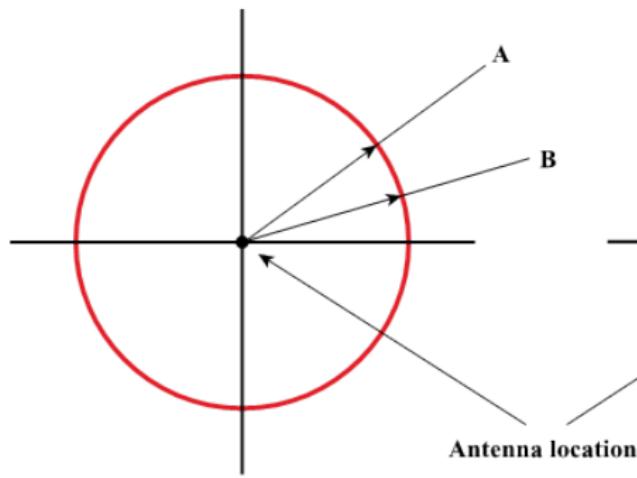
# Antennas

- An antenna is an electrical conductor or system of conductors
  - 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

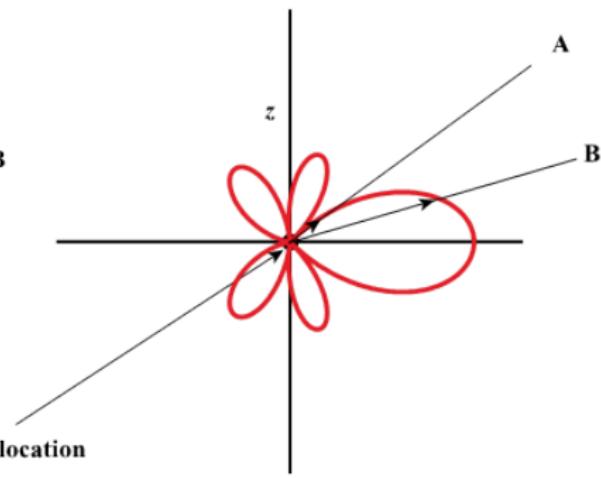
# Radiation Patterns

- Radiation pattern
  - Graphical representation of radiation properties of an antenna
  - Depicted as two-dimensional cross section
- Beam width (or half-power beam width)
  - Measure of directivity of antenna
- Reception pattern
  - Receiving antenna's equivalent to radiation pattern
- Sidelobes
  - Extra energy in directions outside the mainlobe
- Nulls
  - Very low energy in between mainlobe and sidelobes

# Antenna Radiation Patterns



(a) Omnidirectional



(b) Directional

# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation**
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

# Attenuation

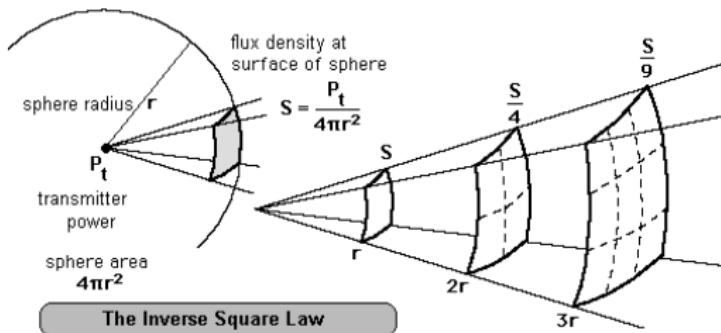
- Strength of signal falls off with distance over transmission medium
- Attenuation factors for unguided media:
  - Received signal must have sufficient strength so that circuitry in the receiver can interpret the signal
  - Signal must maintain a level sufficiently higher than noise to be received without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

# Free Space Loss

Since  $P_r = P_t \frac{\lambda^2}{(4\pi d)^2}$ , free space loss under ideal isotropic antenna becomes

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

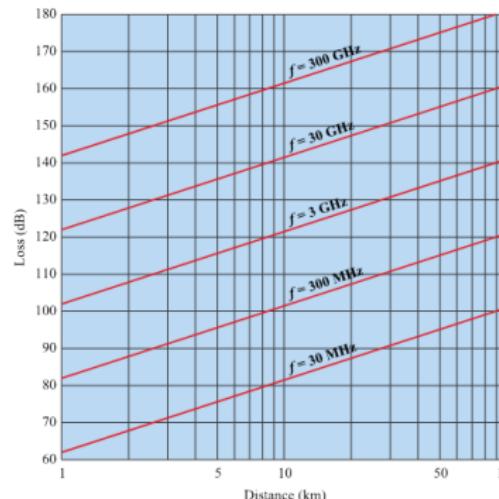
where  $P_t$  = transmit power,  $P_r$  = received signal power,  $\lambda$  = carrier wavelength,  $d$  = distance between antennas,  $c$  = speed of light ( $3 \times 10^8$  m/s). Ideal area of antenna is  $\lambda^2/4\pi$



# Free Space Loss

Free space loss equation can be recast:

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



# Path Loss Exponent in Practical Systems

Practical systems – reflections, scattering, etc.

$$P_r = K_{d_0} P_t \left( \frac{d_0}{d} \right)^{-\eta}$$

where  $K_{d_0}$  is factor measured at distance  $d_0$  meters,  $P_r$  is the received signal strength,  $P_t$  is transmit power and  $d$  is the transmitter-to-received distance.

Environment	Path Loss Exponent, $\eta$
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

# 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 such as Urban, Small- or medium-sized city, Large city, Suburban, Rural

# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise**
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

# Categories of Noise

- Thermal Noise
- Intermodulation noise
- Crosstalk
- Impulse Noise

# Thermal Noise

- Thermal noise due to agitation of electrons
- Present in all electronic devices and transmission media
- Cannot be eliminated
- Function of temperature
- Particularly significant for satellite communication

# Thermal Noise I

- Amount of thermal noise to be found in a bandwidth of 1Hz in any device or conductor is:

$$N_0 = kT$$

- unit:  $W/Hz$
- $N_0$  = noise power density in watts per 1 Hz of bandwidth
- $k$  = Boltzmann's constant =  $1.3803 \times 10^{-23}$  J/K
- $T$  = temperature, in Kelvins (absolute temperature)

- Noise is assumed to be independent of frequency
- Thermal noise present in a bandwidth of  $B$  Hertz (in watts):

$$N = kTB$$

- or, in decibel-watts

$$= -228.6dBW + 10 \log T + 10 \log B$$

# Noise Terminology

- 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

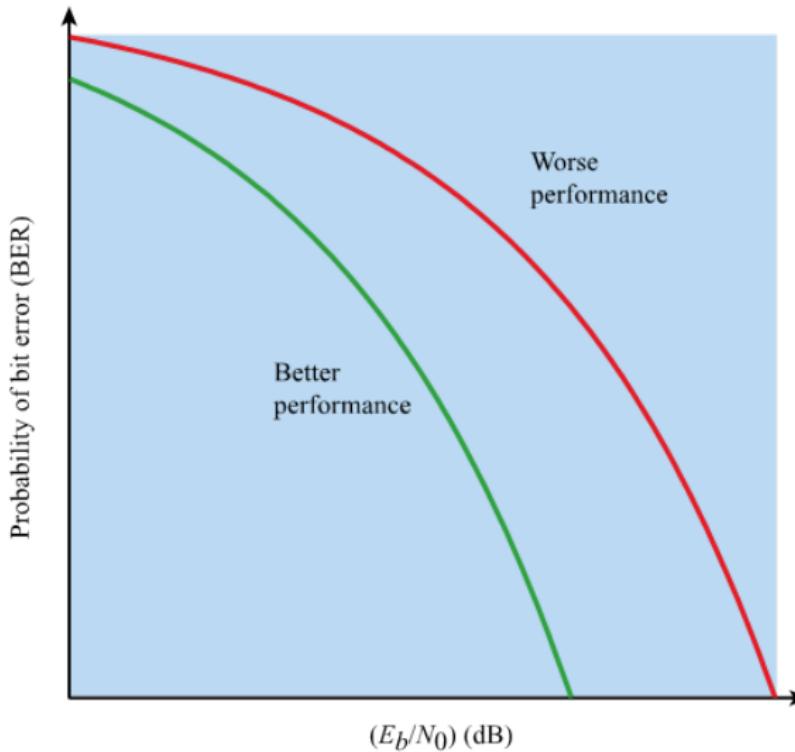
# Expression $E_b/N_0$

- Ratio of signal energy per bit to noise power density per Hertz

$$\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR}$$

- The bit error rate (i.e., bit error probability) for digital data is a function of  $E_b/N_0$ 
  - Given a value for  $E_b/N_0$  to achieve a desired error rate, parameters of this formula can be selected
  - As bit rate  $R$  increases, transmitted signal power must increase to maintain required  $E_b/N_0$

# BER versus $E_b/N_0$ Curves



# Spectral Efficiency

## Spectral Efficiency (bps/Hz)

refers to the information rate that can be transmitted over a given bandwidth in a specific communication system

## Area Spectral Efficiency, (bit/s)/Hz/m<sup>2</sup>, in (bit/s)/Hz per cell

is a measure of the quantity of users or services that can be simultaneously supported by a limited bandwidth in a defined geographic area.

System	Spec. Eff.	Area Spec.Eff.
2G cellular GSM 1991	0.52	0.17
3G cellular CDMA2000 1x PD 2002	0.125	0.1720
Fixed WiMAX IEEE 802.16d 2004	4.8	1.2
4G cellular LTE 2009	4.08	16.32
4G cellular LTE-Advanced 2013[9]	3.75	30
Wi-Fi IEEE 802.11a/g 2003	2.7	0.9
Wi-Fi IEEE 802.11n 2007	3.61 (up to 3.75)	5.0 (4x4, 40 MHz)
Wi-Fi IEEE 802.11ac 2012	5.42	14.4 (8x8, 160 MHz)
Wi-Fi IEEE 802.11ax 2019	7.5	20 (8x8, 160 MHz)
WiGig IEEE 802.11ad 2013	3	3
Digital cable TV DVB-C 1994	6.33	N/A
Broadband CATV modem DOCSIS 3.1 2016	9.84	N/A
Broadband modem ADSL2 downlink 0	12.47	N/A
Broadband modem ADSL2+ downlink 0	13.59	N/A
Telephone modem V.92 downlink 1999	14.0	N/A

# Shannon Limit, Spectral Efficiency vs $E_b/N_0$ I

For an AWGN channel,  $C = B \log\left(1 + \frac{S}{N_0 B}\right)$ .

Therefore,  $\frac{C}{B} = \log\left(1 + \frac{S}{N_0 B}\right)$

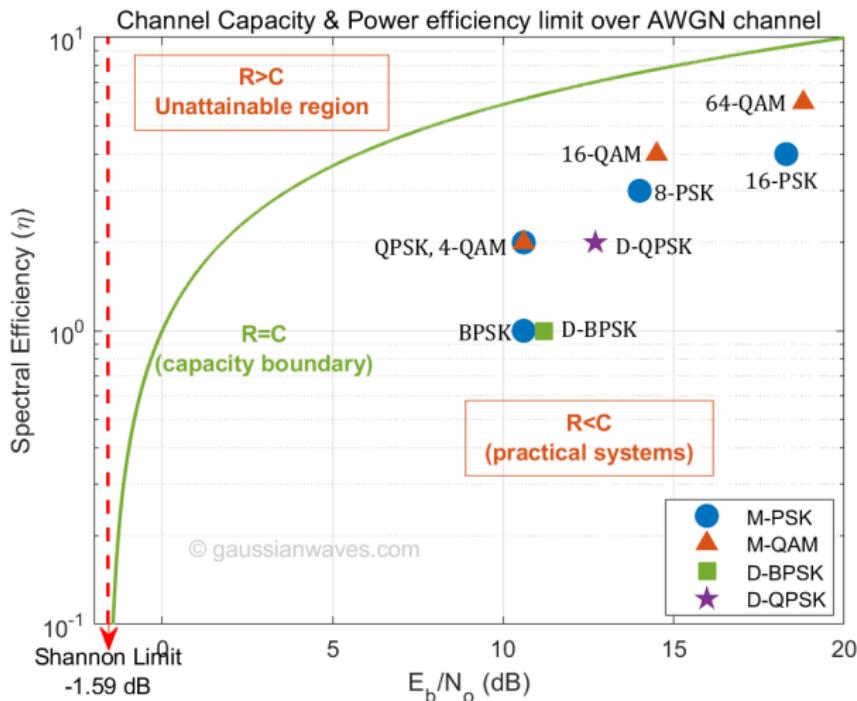
Since  $S = CE_b$ , we can write  $\frac{C}{B} = \log\left(1 + \frac{E_b C}{N_0 B}\right)$ .

Therefore,

$$\frac{E_b}{N_0} = \frac{2^{C/B} - 1}{C/B}$$

is the minimum SNR to achieve the spectral efficiency  $C/B$  bps/Hz.

# Shannon Limit, Spectral Efficiency vs $E_b/N_0$ II

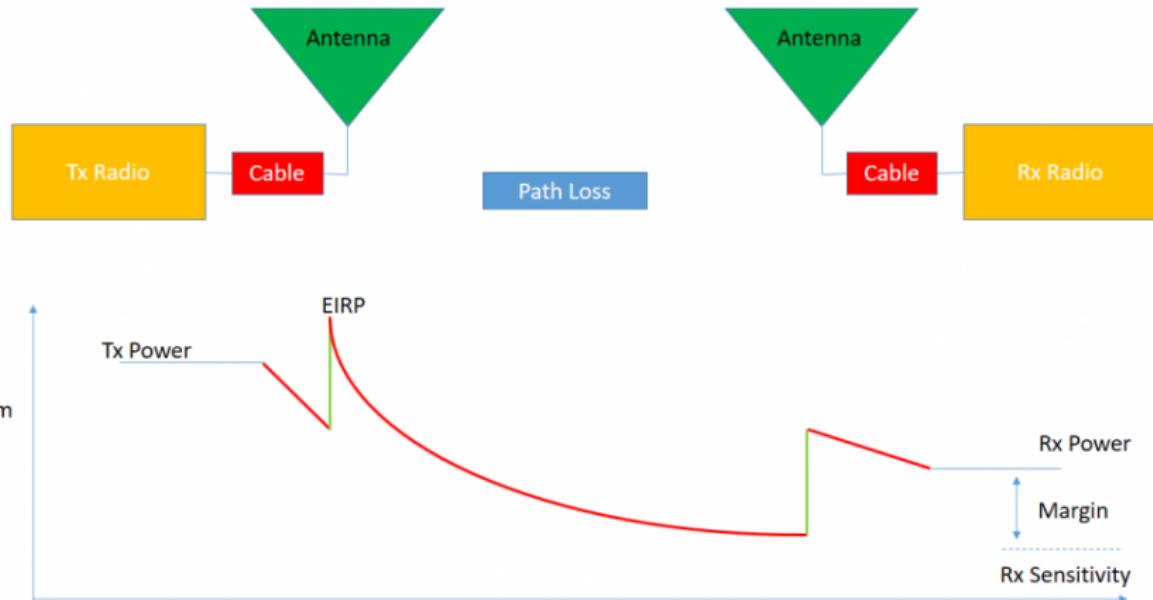


# Link Budget I

Typical factors in link budget are

- Transmit Power (in dBm),
- Antenna Gain, Diversity Gain
- Receiver Sensitivity
- Margins
  - Shadow Margin, Interference Margin, Fading Margin
- Losses
  - Cable losses
  - Obstruction losses during transmission
  - Electronic Losses: Combiner Loss, Filter Loss, etc.
- Gains are added, Losses are subtracted (e.g.,  $f = 1900$  MHz)

# Link Budget II



# Link Budget III

- $B$ : Bandwidth in Hz (e.g., 80 kHz)
- $R$ : Rate (capacity) in bps (e.g., 40 kbps)
- $T$ : System Temperature (e.g., 290 K, Kelvin)
- $k$  Boltzman constant,  $1.38 \times 10^{-23}$  J/K
- Noise figure of receiver: a measure of the amount of noise added by the receiver (e.g., 15 dB)
- $E_b$  = Energy required per bit of information (e.g.,  $E_b/N_0 = 14.2$  dB = 26.3 in linear scale for  $10^{-6}$  of BER)
- $N_0 = kT$  thermal noise per dimension (in 1Hz of bandwidth)
- $N = N_0 B = kTB$  Noise power (depends on bandwidth)
- Noise floor (of receiver) = Noise power + Noise figure
- SNR required at receiver based on  $E_b/N_0$  ratio; use  $SNR = \frac{E_b R}{N_0 B}$  (in linear scale). Note that  $R/B$  is the spectral efficiency.
- Receiver sensitivity = Noise floor + SNR

# Link Budget IV

$$N = kTB = 1.38 \times 10^{-23} \times 290 \times 80000 = 2.4 \times 10^{-13} = -126 \text{ dBm}$$

$$\text{Noise floor} = -126 \text{ dBm} + 15 \text{ dB} = -111 \text{ dBm}$$

$$\text{SNR} = E_b/N_0 \times R/B = 26.3 \times 40000/80000 = 11 \text{ dB}$$

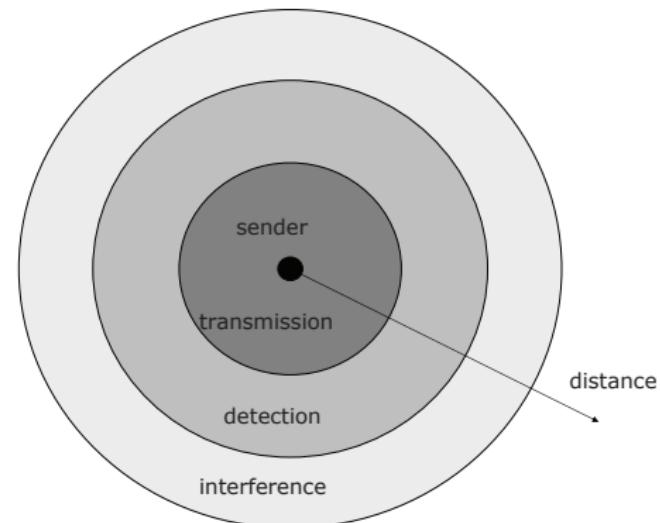
$$\text{Receiver Sensitivity} = -111 \text{ dBm} + 11 \text{ dB} = -100 \text{ dBm}$$

Then we need:

Transmit Power + Gains = Receiver Sensitivity + Losses + Path Loss + Margins  
(in dB scale)

# Signal Propagation

- 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



# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading**
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

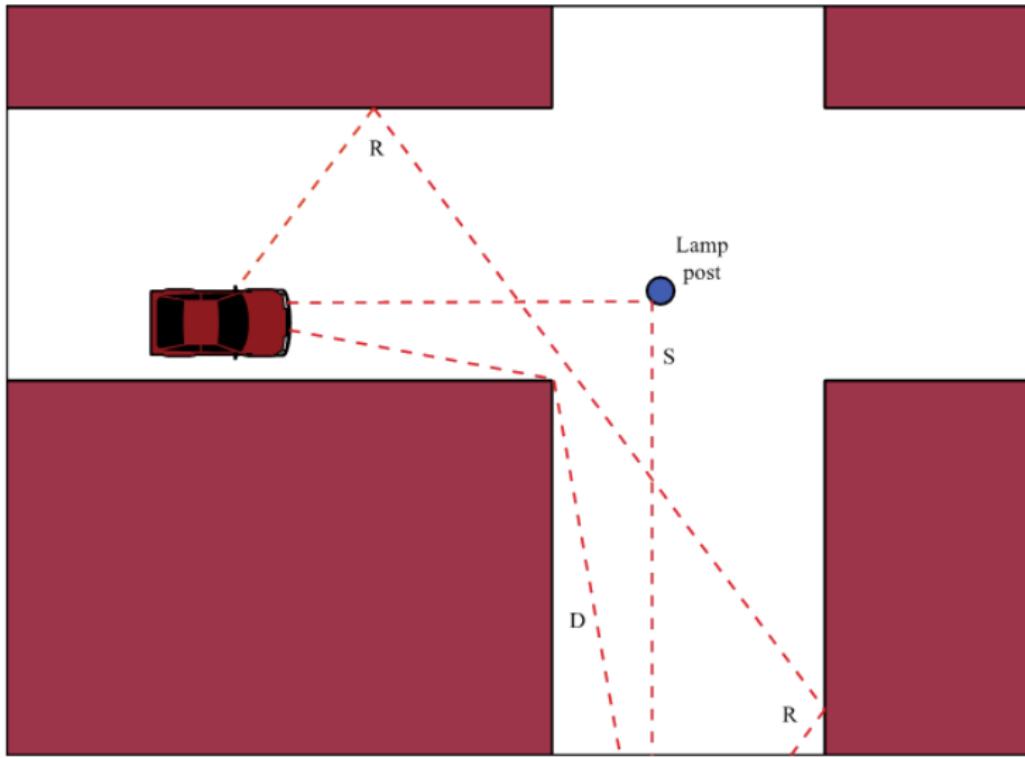
# Other Impairments

- Atmospheric absorption - water vapor and oxygen contribute to attenuation
- Multipath - obstacles reflect signals so that multiple copies with varying delays are received
- Refraction - bending of radio waves as they propagate through the atmosphere

# The Effects of Multipath Propagation

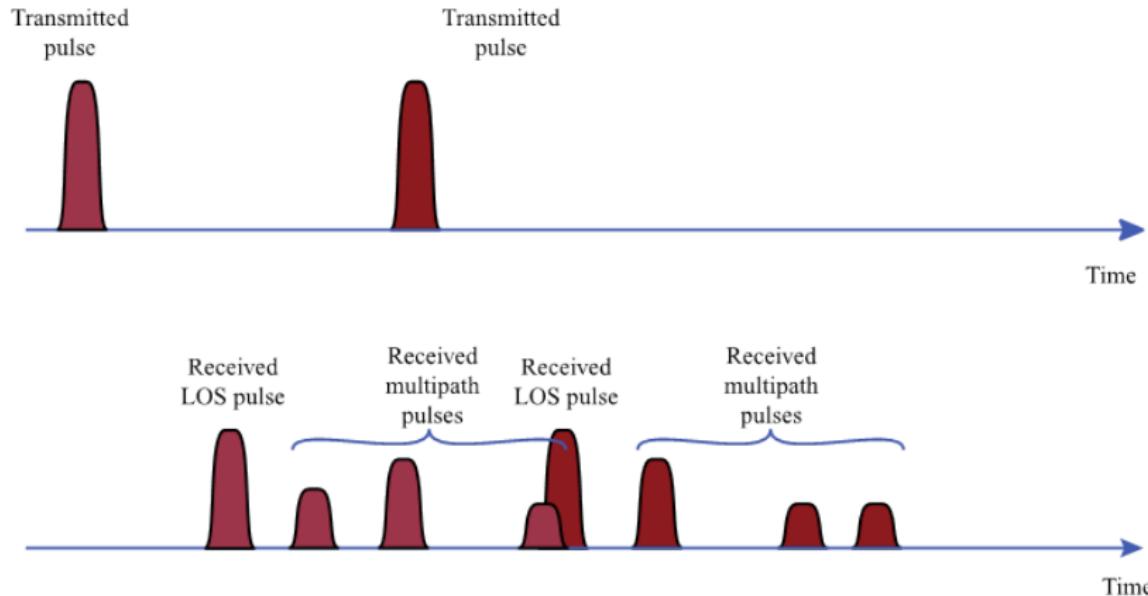
- Reflection, diffraction, and scattering
- Multiple copies of a signal may arrive at different phases
  - If phases add destructively, the signal level relative to noise declines, making detection more difficult
- Intersymbol interference (ISI)
  - One or more delayed copies of a pulse may arrive at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

# Sketch of Three Important Propagation Mechanisms

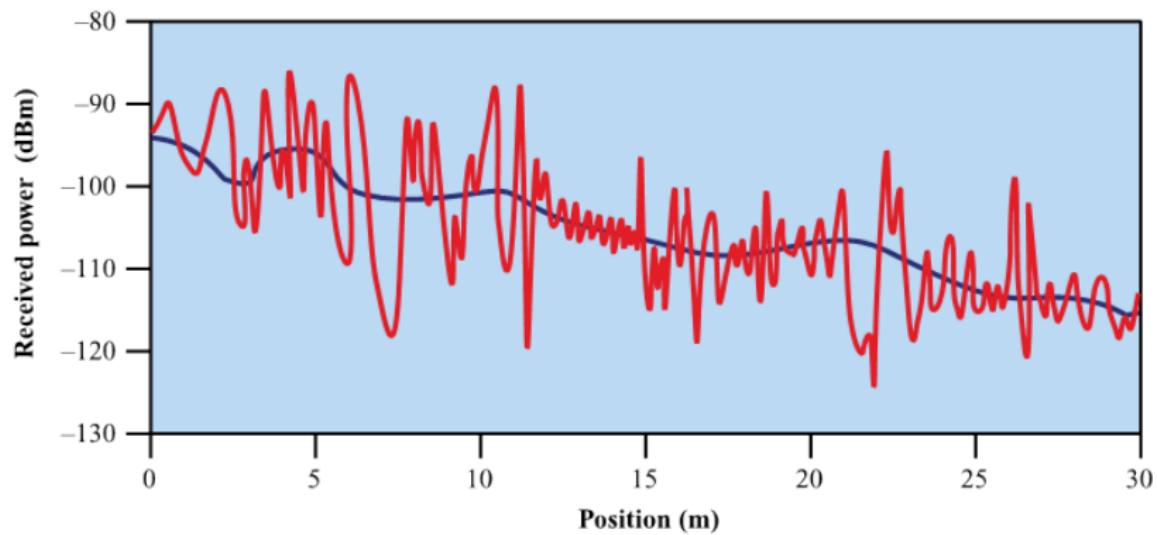


# Two Pulses in Time-Variant Multipath

## Intersymbol Interference



# Large- and Small-Scale Fading in Urban Mobile Envi.



# Types of Fading I

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

# Shadow Fading

- Shadowing occurs when line of sight is blocked - Modeled by a random signal component  $X_\sigma$
- Measurement studies show that  $X_\sigma$  can be modeled with a lognormal distribution; normal in dB with mean zero and standard deviation  $\sigma$  dB
- Thus at the designed cell edge only 50% of the locations have adequate RSS
- All in dB:  $P_r = P_t - L_{dB} + X_\sigma$
- $\sigma$ : Rural 3 dB, suburban 6 dB, urban 8 dB, dense urban 10 dB
- To combat shadowing
  - Reduce cell size
  - Increase transmit power
  - Make the receiver more sensitive

# Types of Fading: Doppler Spread I

- Frequency fluctuations caused by movement
- **Coherence time**  $T_c$  characterizes Doppler shift
  - How long a channel remains the same
- Coherence time  $T_c > T_b$  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  $T_b = 1/100 \times 10^3 = 10 \mu\text{s}$
- $T_c > T_b$ ?  $70 \text{ ms} > 10 \mu\text{s}$ ?
- True, so slow fading

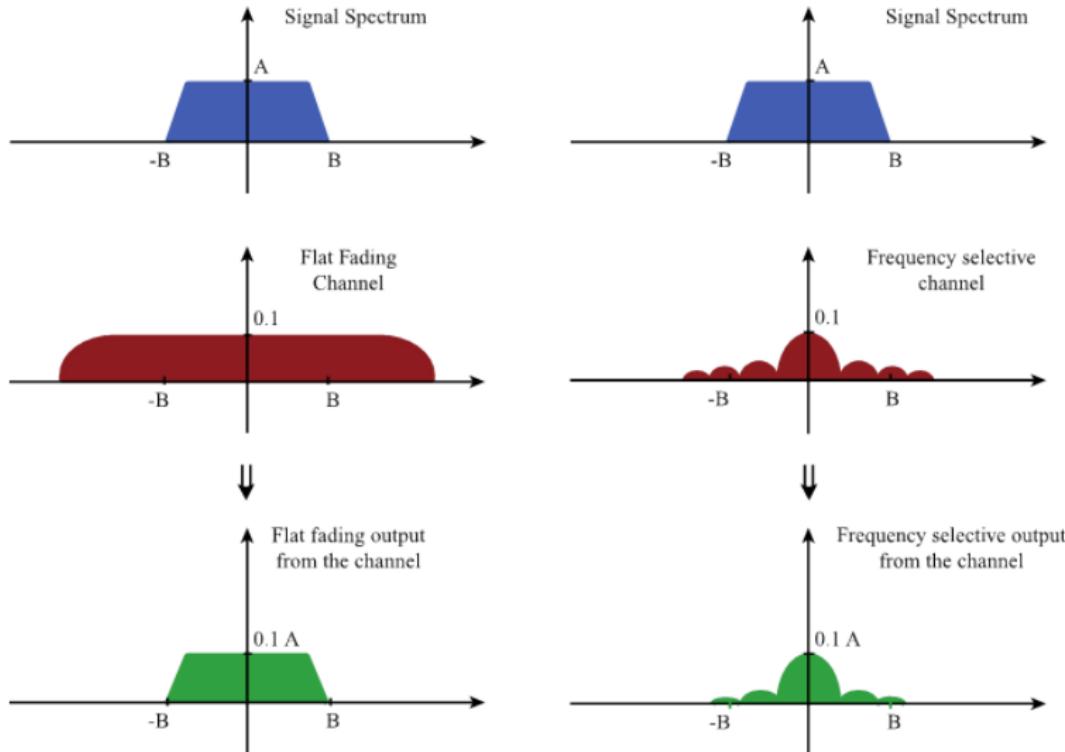
# Types of Fading: Multipath fading I

- 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  $B_c > B_s$ , then flat fading
  - The signal bandwidth fits well within the channel bandwidth
- Otherwise, frequency selective fading

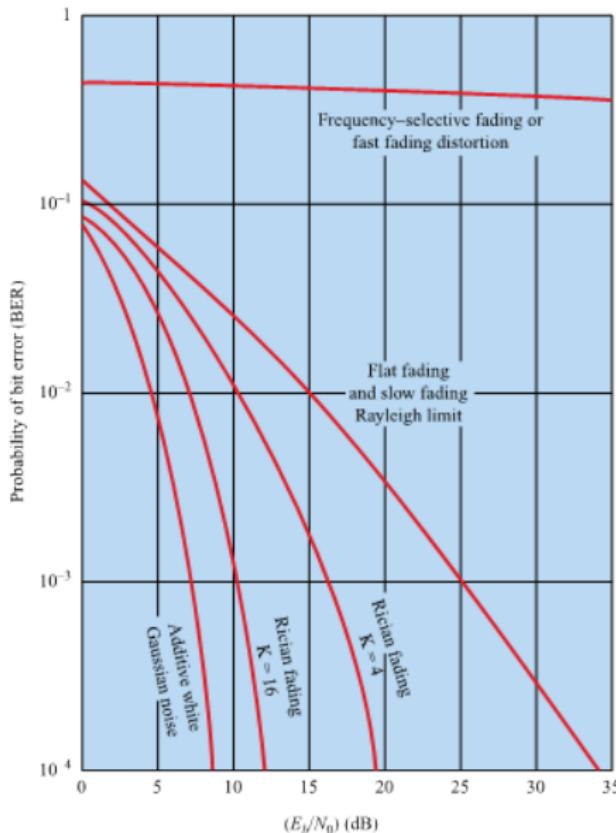
**Example**  $B_c = 150$  kHz, bit rate  $r_b = 100$  kbps

- Assume signal bandwidth  $B_s \approx r_b$ ,  $B_s = 100$  kHz
- $B_c > B_s$ ?  $150$  kHz  $> 100$  kHz?
- Using a factor of 10 for  $>$ ,  $150$  kHz is not more than  $10 \times 100$  kHz
- False, so frequency selective fading

# Flat and Frequency Selective Fading



# Theoretic BER for Various Fading Conditions



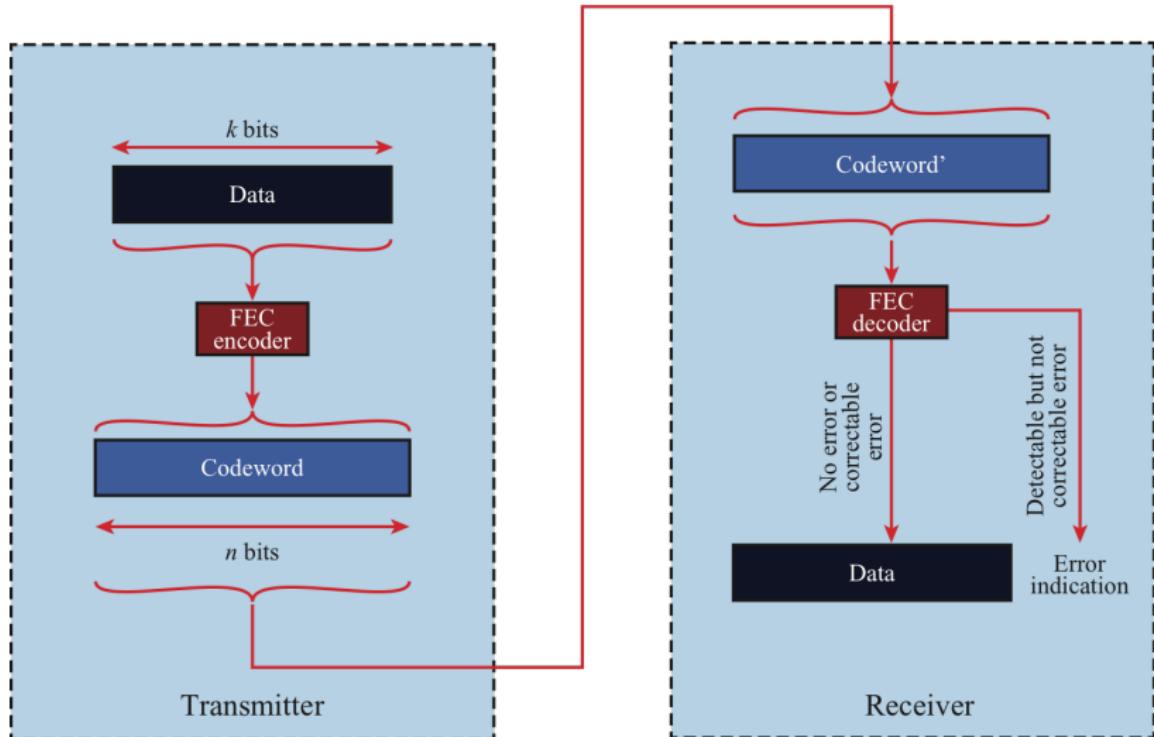
# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms**
  - 20 Modulation of Analog Signals for Digital Data
  - 21 Coding and Error Control
  - 22 Automatic Repeat Request
  - 23 Orthogonal Frequency Division Multiplexing (OFDM)
  - 24 Spread Spectrum Techniques

# Channel Correction Mechanisms

- Forward error correction
- Adaptive equalization
- Adaptive modulation and coding
- Diversity techniques and MIMO
- OFDM
- Spread spectrum
- Bandwidth expansion

# Forward Error Correction Process



# Forward Error Correction

- Transmitter adds error-correcting code to data block
  - Code is a function of the data bits
- Receiver calculates error-correcting code from incoming data bits
  - If calculated code matches incoming code, no error occurred
  - If error-correcting codes don't match, receiver attempts to determine bits in error and correct

# 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

# 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

# Adaptive Modulation and Coding (AMC)

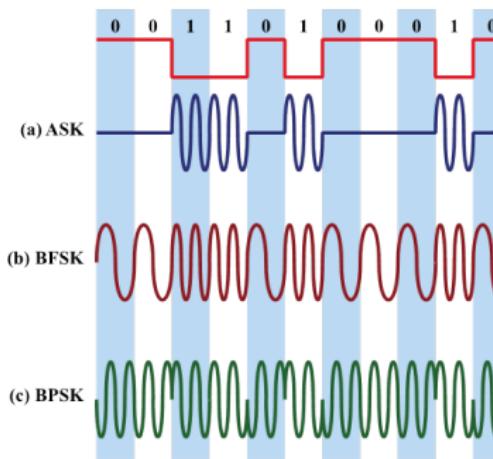
- The modulation process formats the signal to best transmit bits
  - To overcome noise
  - To transmit as many bits as possible
- Coding detects and corrects errors
- AMC adapts to channel conditions
  - 100's of times per second
  - Measures channel conditions
  - Sends messages between transmitter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

# Agenda

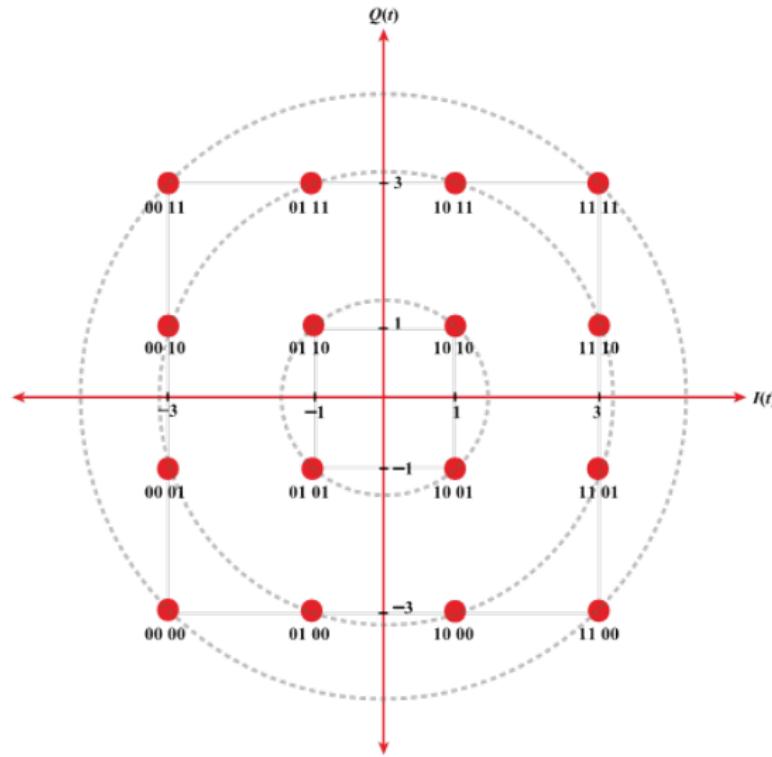
- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data**
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

# Signal 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



# 16QAM Constellation Diagram



# Bit Error Rate (BER)

- Performance must be assessed in the presence of noise
- **Bit error probability** is probably a clearer term
  - BER is not a rate in bits/sec, but rather a probability
  - Commonly plotted on a log scale in the y-axis and  $E_b/N_0$  in dB on the x-axis
  - As  $E_b/N_0$  increases, BER drops
- Curves to the lower left have better performance
  - Lower BER at the same  $E_b/N_0$
  - Lower  $E_b/N_0$  for the same BER

# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control**
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

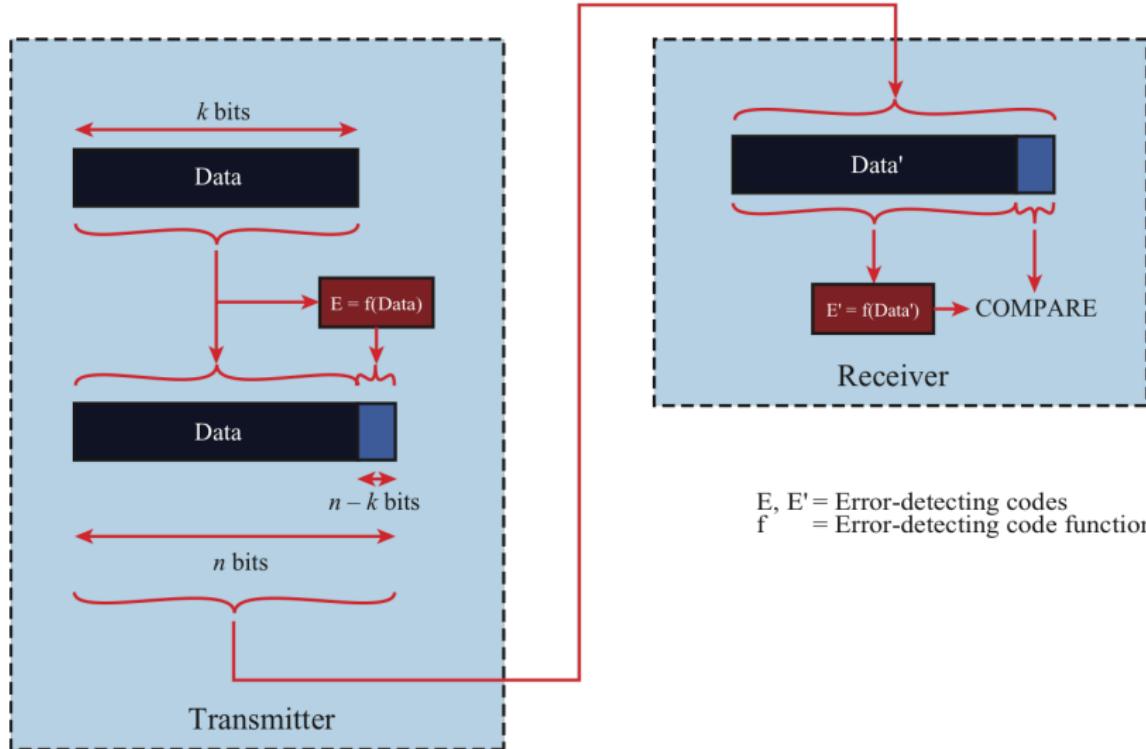
# Coding and Error Control

- Error detection codes
  - Detects the presence of an error
- Automatic repeat request (ARQ) protocols
  - Block of data with error is discarded
  - Transmitter retransmits that block of data
- Error correction codes, or forward correction codes (FEC)
  - Designed to detect and correct errors

# Error Detection Probabilities

- Definitions
  - $P_b$  : Probability of single bit error (BER)
  - $P_1$  : Probability that a frame arrives with no bit errors
  - $P_2$  : While using error detection, the probability that a frame arrives with one or more undetected errors
  - $P_3$  : While using error detection, the probability that a frame arrives with one or more detected bit errors but no undetected bit errors
- With no error detection  $P_1 = (1 - P_b)^F$  and  $P_2 = 1 - P_1$  and  $P_3 = 0$ 
  - $F$  = Number of bits per frame

## Error Detection Process



# 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

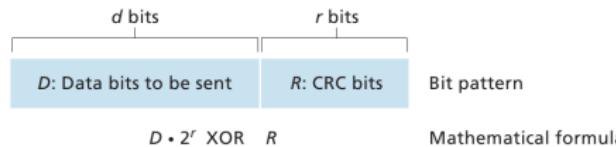
# Parity Check

- 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]

# Error Detection and Correction

## Cyclic Redundancy Check (CRC)

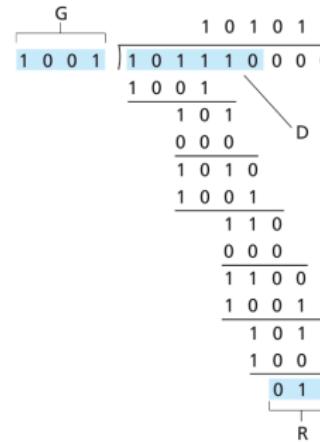
$$\begin{array}{r} 1011 \text{ XOR } 0101 = 1110 \\ 1001 \text{ XOR } 1101 = 0100 \end{array}$$



- more powerful error-detection coding
- view data bits,  $D$ , as a binary number
- choose  $r + 1$  bit pattern (generator),  $G$
- choose CRC bits  $R$  (of length  $r$ ) such that
  - $D||R$  is divisible by  $G$  modulo 2
  - receiver knows  $G$ , divides  $D||R$  by  $G$ . Non-zero remainders indicates error
- Ethernet, 802.11, WiFi, ATM

# Error Detection and Correction

## Cyclic Redundancy Check (CRC)



$$D \times 2^r \oplus R = nG$$

$$D \times 2^r = nG \oplus R$$

$$R = \text{Remainder} \left( \frac{D \times 2^r}{G} \right)$$

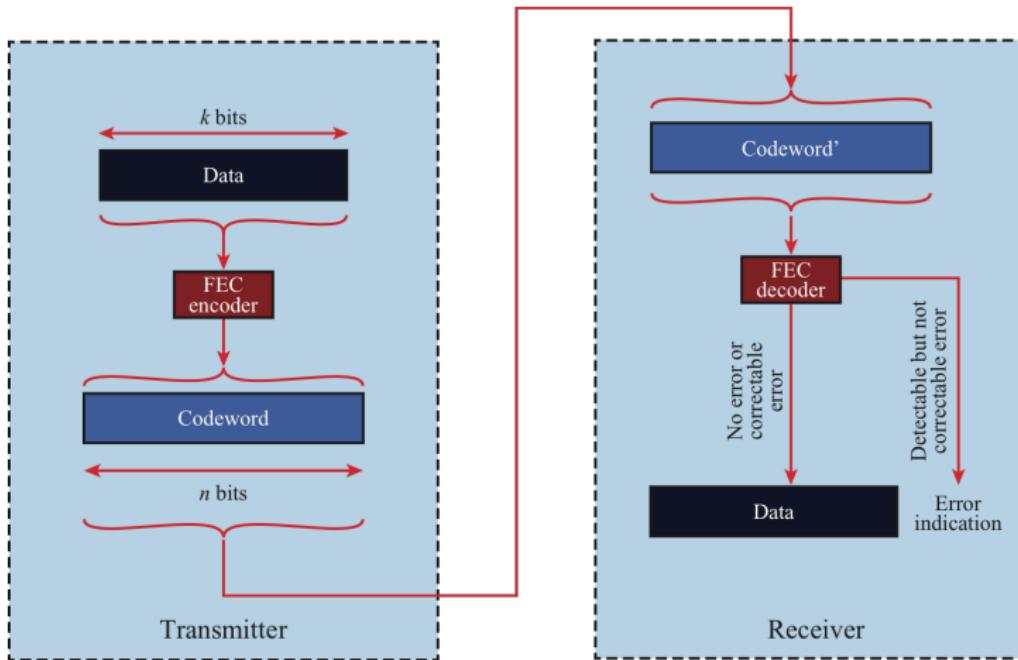
# Wireless Transmission Errors

- Error detection requires retransmission
- Detection 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

# 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

# Forward Error Correction Process



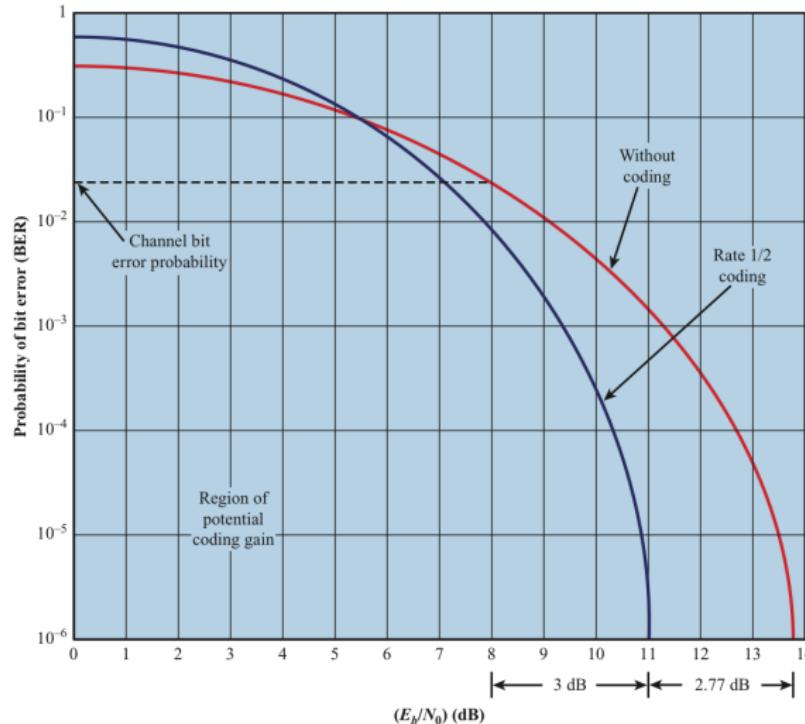
# FEC Decoder Outcomes

- 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

# 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
- Required performance  $d$  bit errors, then the Hamming distance has to be
  - $d + 1$  to detect  $d$  bit errors,
  - $2d + 1$  to correct  $d$  bit errors.

# How Coding Improves System Performance



# Decoding process

- Coding table
- | Data     | 00    | 01    | 10    | 11    |
|----------|-------|-------|-------|-------|
| Codeword | 00000 | 00111 | 11001 | 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 11110
    - Most likely 00000 was sent, assume data was 00 (but others could have been sent, albeit much less likely)
  - Received: 01100
    - Two bits from 00000, Two bits from 11110
    - No other codes closer, Cannot decode. Only know bit errors are detected

# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request**
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

# Automatic Repeat Request

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

# Hybrid ARQ I

- 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

# Hybrid ARQ II

- Additional HARQ approaches
  - Soft decision decoding
  - Chase combining
    - ▶ Soft decision information from a previous frame not corrected by FEC is used with retransmissions
    - ▶ Chase combining uses exact same frames retransmitted each time
  - Incremental redundancy
    - ▶ Different, maybe more, coding used each retransmission
    - ▶ Uses less overhead for the first transmissions
    - ▶ Provides stronger correction

# Hybrid ARQ III

- Additional approaches
  - Puncturing
    - ▶ Remove bits to decrease the coding rate, say from 1/2 to 1/3
    - ▶ Replace bits at the receiver with random values
    - ▶ Result may still be effective enough to correct errors
    - ▶ Allows easier adaptation of coding rates
  - Channel quality information will be used to find the best adaptive modulation and coding for HARQ
  - Parallel HARQ processes can proceed while others are waiting for retransmissions

# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)**
- 24 Spread Spectrum Techniques

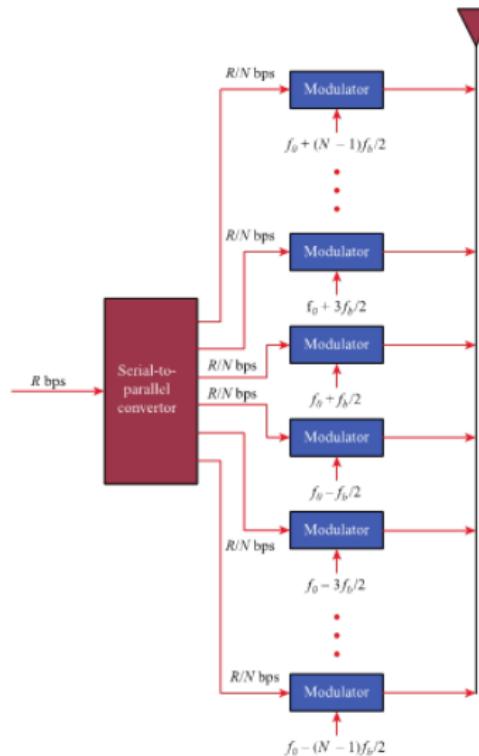
# Orthogonal Frequency Division Multiplexing (OFDM)

- 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
  - LTE, WIFI, ADSL,...

# How OFDM works

- 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  $N/R$ )

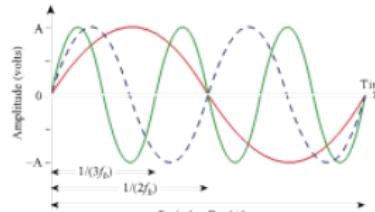
# Conceptual Understanding of OFDM



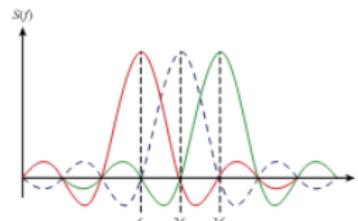
# Orthogonality

- 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

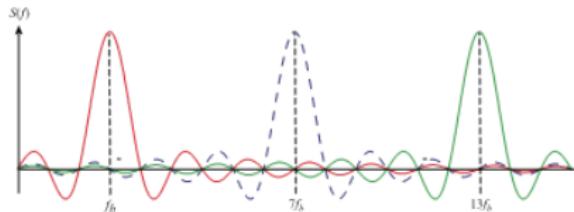
# Illustration of Orthogonality of OFDM



(a) Three subcarriers in time domain



(b) Three orthogonal subcarriers in frequency domain



(c) Three carriers using traditional FDM

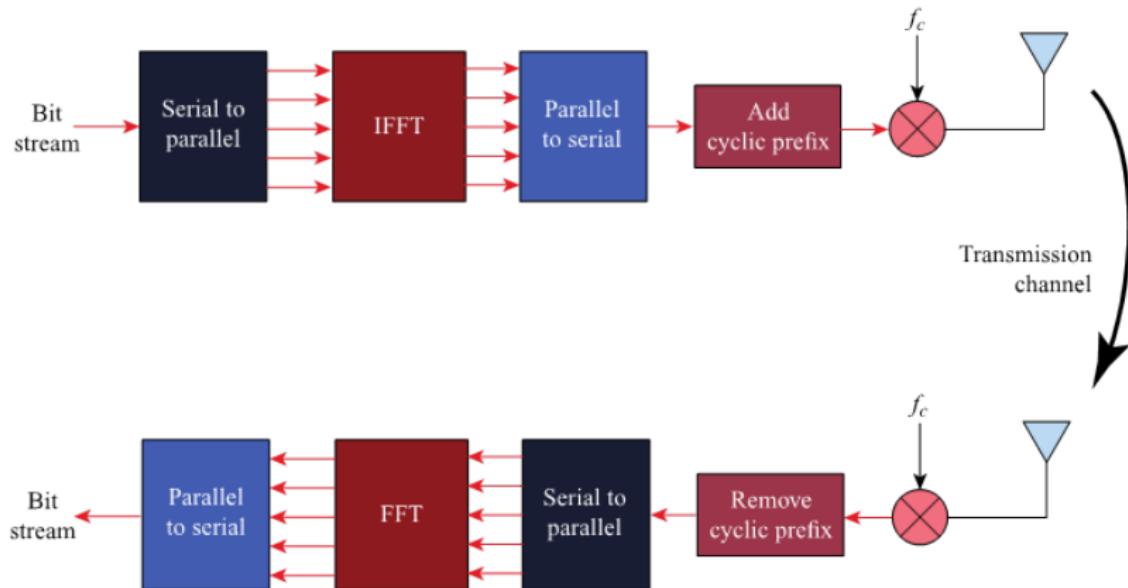
# Benefits of OFDM

- Frequency selective fading only affects some subcarriers
- 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

# OFDM Implementation

- Inverse Fast Fourier Transform (IFFT)
  - The OFDM concept would use  $N$  oscillators for  $N$  different subcarrier frequencies
    - ▶ Expensive for transmitter and receiver
  - Discrete Fourier Transform (DFT) processes digital signals
    - ▶ If  $N$  is a power of two, the computational speed dramatically improves by using the fast version of the DFT (FFT).
    - ▶ OFDM uses the Inverse FFT to compute the data stream to be transmitted
    - ▶ Then it is sent on the carrier using only one oscillator

# IFFT Implementation of OFDM



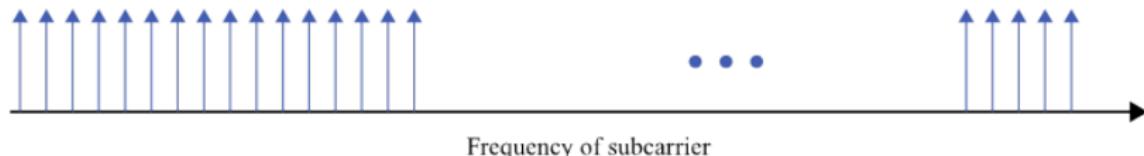
FFT = fast Fourier transform

IFFT = inverse fast Fourier transform

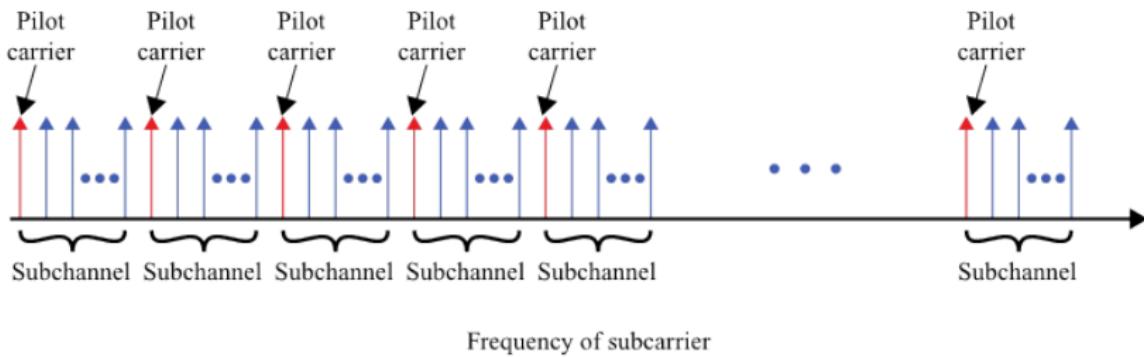
# OFDMA I

- Orthogonal Frequency Division Multiple Access (OFDMA) uses OFDM to share the wireless channel
  - Different users can have different slices of time and different groups of subcarriers
  - Subcarriers are allocated in groups
    - ▶ Called subchannels or resource blocks
    - ▶ Too much computation to allocate every subcarrier separately
- Single-carrier FDMA (SC-FDMA)
  - Similar structure and performance to OFDMA
  - Lower peak to average power ratio than OFMDA
  - Mobile user benefits - battery life, power efficiency, lower cost
    - ▶ Good for uplinks
  - Multiple access is not possible
    - ▶ At one time, all subcarriers must be dedicated to one user

# OFDM and OFDMA



(a) OFDM



(b) OFDMA (adjacent subcarriers)

# Opportunistic scheduling I

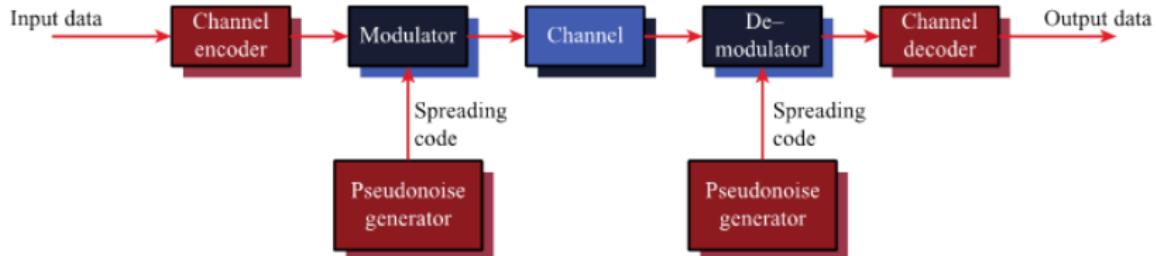
- Schedule subchannels and power levels based on
  - Channel conditions
  - Data requirements
- Adjust in a dynamic fashion
  - Use channel variations as an opportunity to schedule the best choice in users
    - ▶ Hence the term opportunistic scheduling
  - Criteria (maybe more than one used simultaneously)
    - ▶ System efficiency - pick users with best throughput
    - ▶ Fairness - proportional fairness considers the ratio of users' current rates to the users' average rates to know when a channel is best for them
    - ▶ Requirements - audio, video
    - ▶ Priority - public safety, emergency, or priority customers

# Agenda

- 11 Objectives
- 12 Wireless Signals
- 13 Spectrum considerations
- 14 Wireless Propagation Modes
- 15 Antennas
- 16 Attenuation
- 17 Categories of Noise
- 18 Types of Fading
- 19 Channel Correction Mechanisms
- 20 Modulation of Analog Signals for Digital Data
- 21 Coding and Error Control
- 22 Automatic Repeat Request
- 23 Orthogonal Frequency Division Multiplexing (OFDM)
- 24 Spread Spectrum Techniques

# Spread Spectrum

- 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



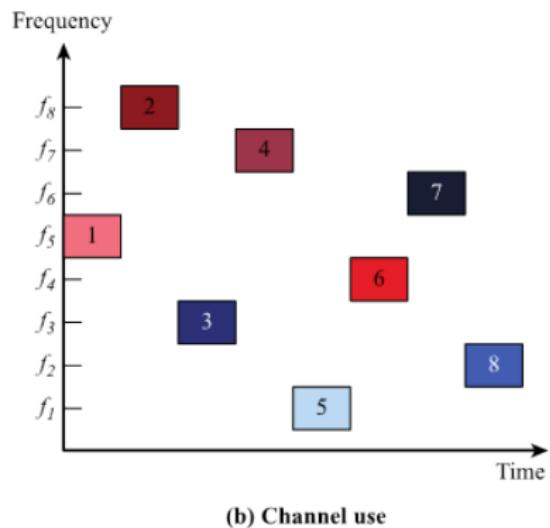
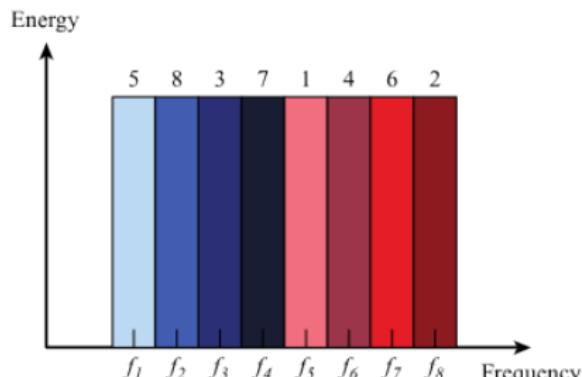
# Spread Spectrum

- On receiving end, digital sequence is used to demodulate the spread spectrum signal
- Signal is fed into a channel decoder to recover data
- What can be gained from apparent waste of spectrum?
  - Immunity from various kinds of noise and multipath distortion
  - Can be used for hiding and encrypting signals
  - Several users can independently use the same higher bandwidth with very little interference
- Two broad types:
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)

# 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
- 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

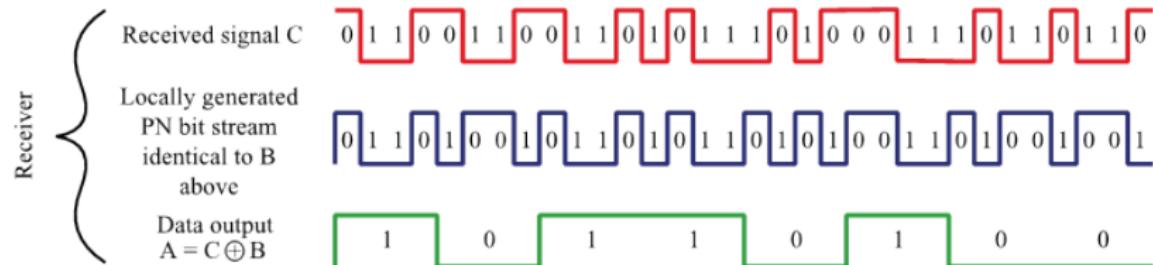
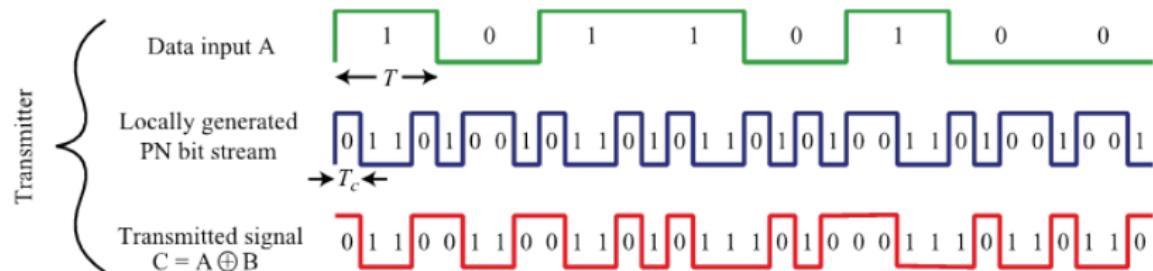
# Frequency Hopping Example I



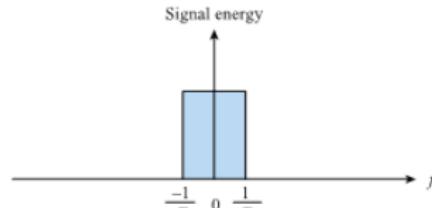
# Direct Sequence Spread Spectrum (DSSS)

- 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 (Figure 5.30)

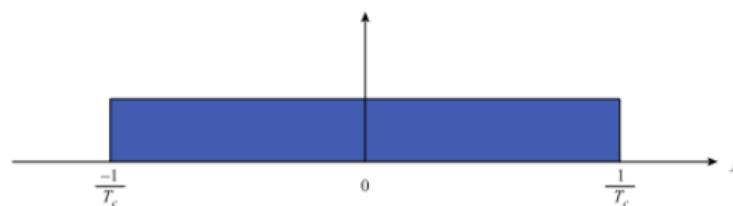
# Example of Direct Sequence Spread Spectrum



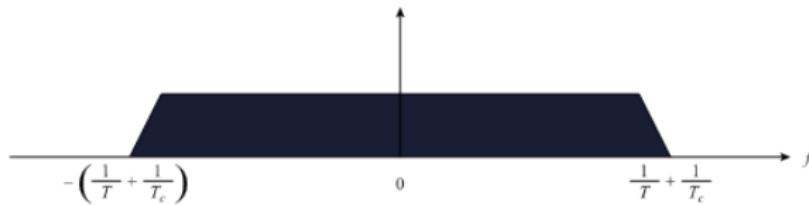
# Approximate Spectrum of DSSS Signal



(a) Spectrum of data signal



(b) Spectrum of pseudonoise signal



(c) Spectrum of combined signal

# Code-Division Multiple Access (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

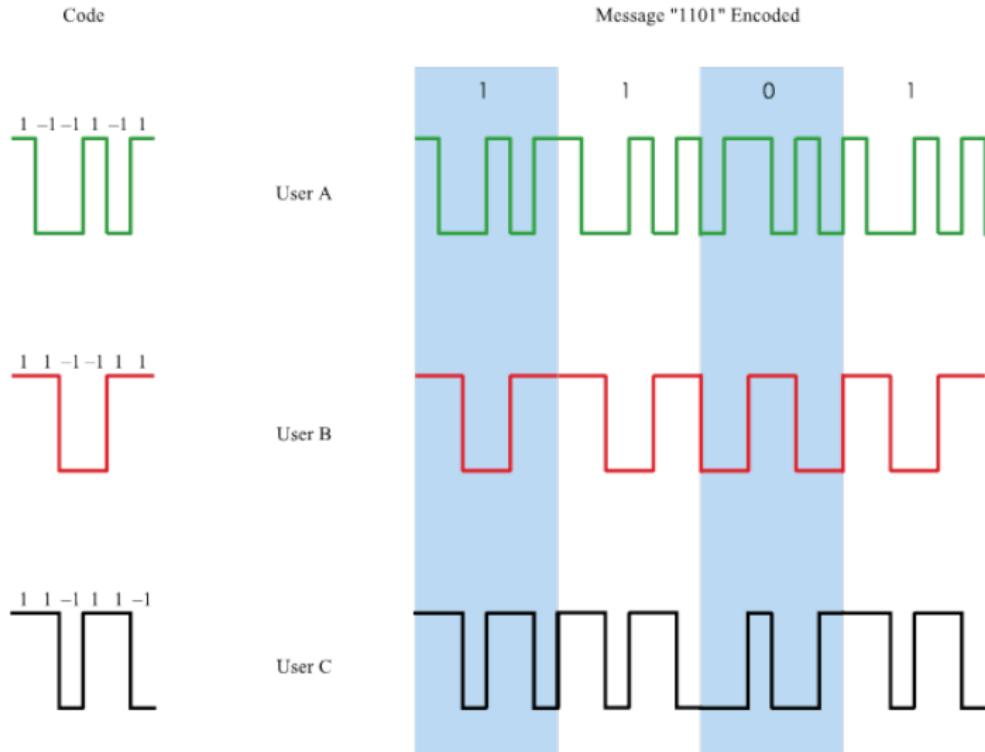
# CDMA Example

- 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

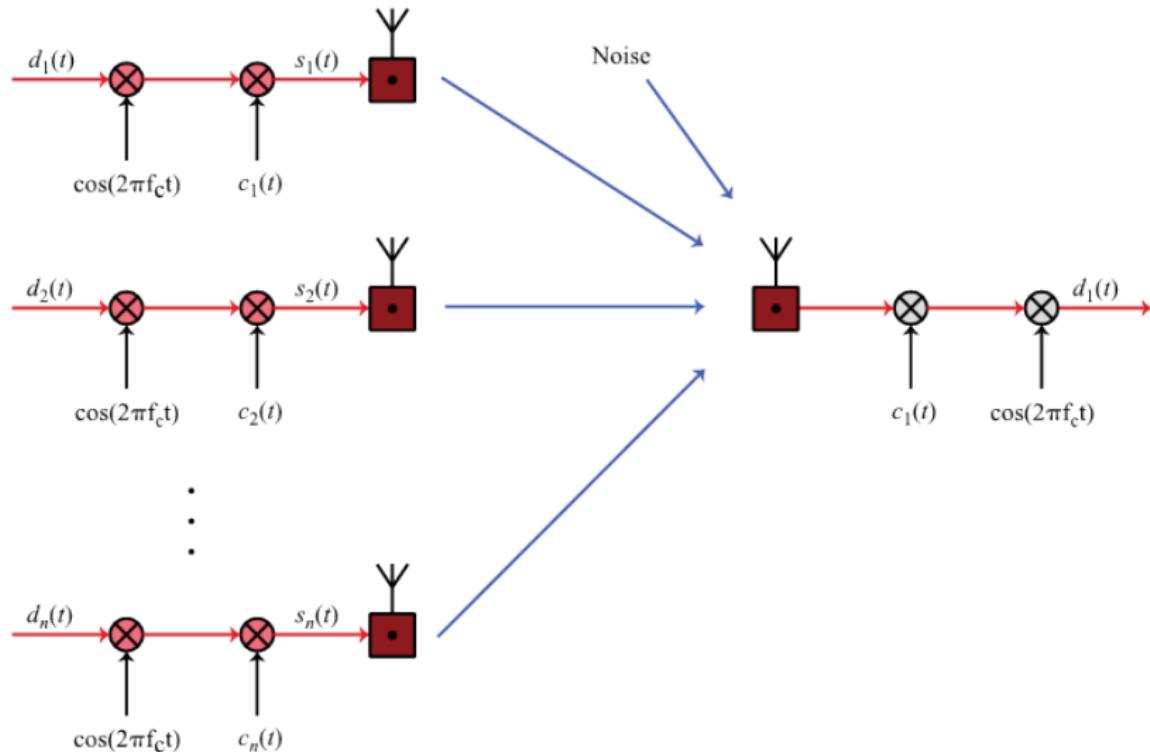
# CDMA Example



# CDMA Example

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

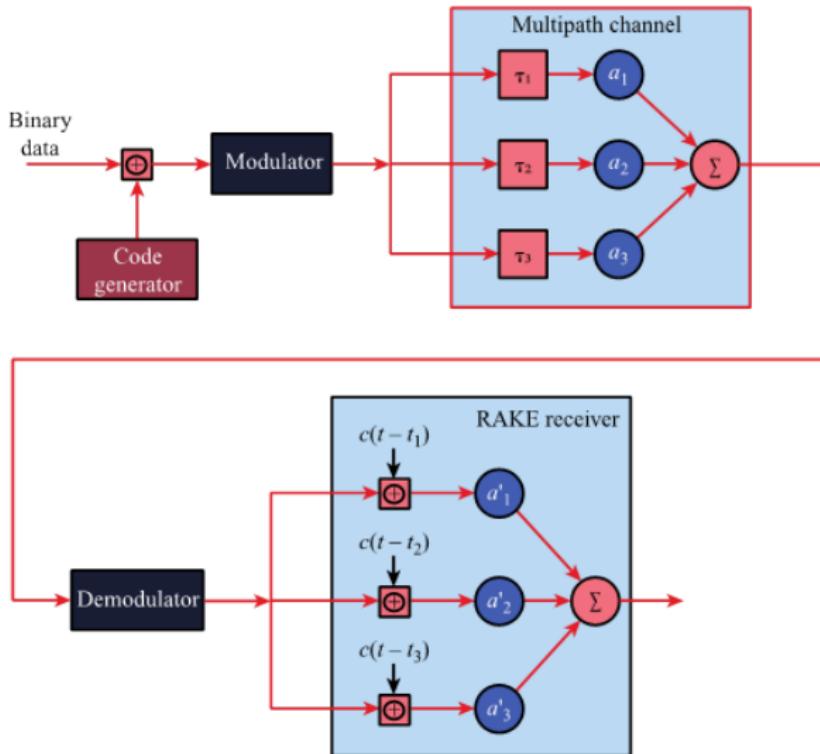
# CDMA in a DSSS Environment



# Rake receiver

- RAKE receiver
  - Multiple versions of a signal arrive more than one chip interval apart
  - RAKE receiver attempts to recover signals from multiple paths and combine them
- This method achieves better performance than simply recovering dominant signal and treating remaining signals as noise

# Principle of RAKE Receiver



# Categories of Spreading Sequences

- Spreading Sequence Categories
  - PN sequences
  - Orthogonal codes
- For FHSS systems
  - PN sequences most common
- For DSSS systems not employing CDMA
  - PN sequences most common
- For DSSS CDMA systems
  - PN sequences
  - Orthogonal codes

# PN Sequences

- PN generator produces periodic sequence that appears to be random
- PN Sequences
  - Generated by an algorithm using initial seed
  - Sequence is not statistically random but will pass many test of randomness
  - Sequences referred to as pseudorandom numbers or pseudonoise sequences
  - Unless algorithm and seed are known, the sequence is impractical to predict

## Lecture 4: Models of Ad Hoc Networks

# Agenda

- 25 Objectives
- 26 What is a Graph?
- 27 Representation
- 28 Modeling Ad Hoc Networks as Graphs
- 29 Scale Free Graphs
- 30 Geometric Random Graph for Ad Hoc Networks
- 31 Mobility Modeling

# Objectives

At the end of this lectures, you will be able to

- define graph models for ad hoc networks [9],
- define mobility models for ad hoc networks [10]

# Agenda

- 25 Objectives
- 26 **What is a Graph?**
- 27 Representation
- 28 Modeling Ad Hoc Networks as Graphs
- 29 Scale Free Graphs
- 30 Geometric Random Graph for Ad Hoc Networks
- 31 Mobility Modeling

# What is a Graph?

A finite graph  $G(V, E)$  is a pair  $(V, E)$ , where  $V$  is a finite set and  $E$  is a binary relation on  $V$ .

The elements of the set  $V$  are called **vertices** (or **nodes**) and those of set  $E$  are called **edges** (**links**).

**Undirected graph:** The edges are unordered pairs of  $V$  (i.e. the binary relation is symmetric).

e.g., undirected  $G(V, E)$ ;  $V = a, b, c$ ,  $E = \{\{a, b\}, \{b, c\}\}$

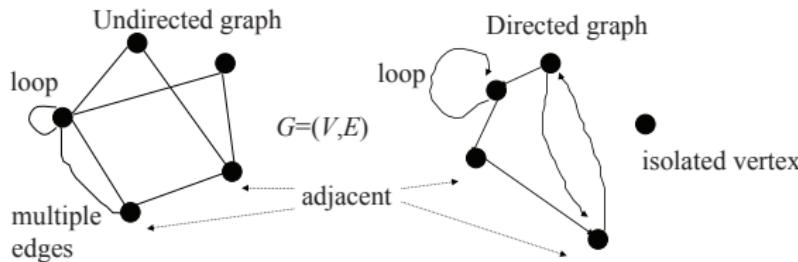
**Directed graph (digraph):** The edges are ordered pairs of  $V$  (i.e. the binary relation is not necessarily symmetric).

e.g., digraph  $G(V, E)$ ;  $V = \{a, b, c\}$ ,  $E = \{(a, b), (b, c)\}$

# Why Graphs?

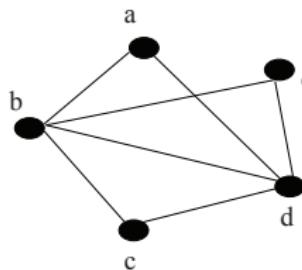
- Many problems can be stated in terms of a graph
- The properties of graphs are well-studied
- Many algorithms exist to solve problems posed as graphs
- Many problems are already known to be intractable
- By reducing an instance of a problem to a standard graph problem, we may be able to use well-known graph algorithms to provide an optimal solution
- Graphs are excellent structures for storing, searching, and retrieving large amounts of data; e.g., routing table?

# Graph Terminology



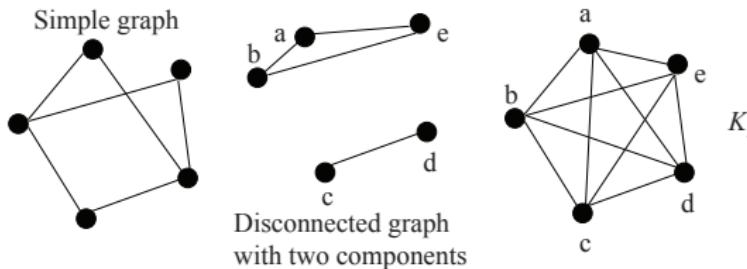
- **incidence:** an edge (directed or undirected) is incident to a vertex that is one of its end points.
- **degree of a vertex:** number of edges incident to it
- Nodes of a digraph can also be said to have an **indegree** and an **outdegree**
- **adjacency:** two vertices connected by an edge are adjacent

# Travel in Graphs



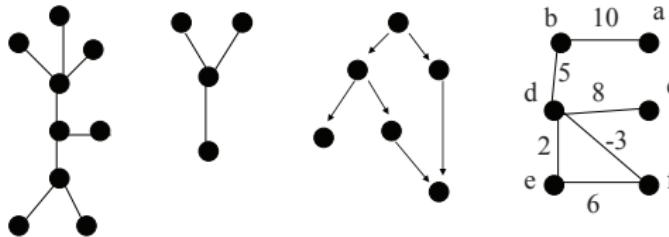
- **walk:** no restriction; e.g., walk: a-b-d-a-b-c
  - **closed:** if the starting vertex is also the ending vertex
  - **open:** if the starting vertex is not the ending vertex
- **path:** no vertex can be repeated; e.g. path: a-b-c-d-e
- **trail:** no edge can be repeated; e.g. trail: a-b-c-d-e-b-d
- **circuit:** a closed trail (ex: a-b-c-d-b-e-d-a)
- **cycle:** closed path (ex: a-b-c-d-a)
- **length:** number of edges in the path, trail, or walk

# Graph Types



- **simple graph:** an undirected graph with no loops or multiple edges between the same two vertices
- **multi-graph:** any graph that is not simple
- **connected graph:** all vertex pairs are joined by a path
- **disconnected graph:** at least one vertex pairs is not joined by a path
- **complete graph:** all vertex pairs are adjacent
- **$K_n$ :** the completely connected graph with  $n$  vertices ( $n(n - 1)/2$  edges)

# Graph Types



- **acyclic graph (forest):** a graph with no cycles
- **tree:** a connected, acyclic graph (one path between each vertex)
- **rooted tree:** a tree with a **root** or *distinguished* vertex
- **leaves:** the terminal nodes of a rooted tree
- **directed acyclic graph (DAG):** a digraph with no cycles
- **weighted graph:** any graph with weights associated with the edges (edge-weighted) and/or the vertices (vertex-weighted)

# Connectedness

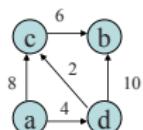
Let  $G_1(V_1, E_1)$  and  $G_2(V_2, E_2)$  be two graphs.

- union of  $G_1$  and  $G_2$ :  $G_1 \cup G_2 = G(V_1 \cup V_2, E_1 \cup E_2)$
- connected graph: a graph is connected if it cannot be expressed as the union of two graphs, and disconnected otherwise.
- strongly connected **digraph**: A digraph  $D$  is strongly connected if, for any two vertices  $v$  and  $w$  of  $D$ , there is a path from  $v$  to  $w$ .
- component: any disconnected graph  $G$  can be expressed as the union of connected graphs, each of which is a component of  $G$
- handshaking lemma, Euler, 1736: in any graph the sum of all the vertex-degrees is an even number (corollary: in any graph the number of vertices of odd degree is even)
- null graph:  $G = (V, E)$  where  $E = \emptyset$
- regular graph: a graph in which each vertex has the same degree

# Agenda

- 25 Objectives
- 26 What is a Graph?
- 27 Representation**
- 28 Modeling Ad Hoc Networks as Graphs
- 29 Scale Free Graphs
- 30 Geometric Random Graph for Ad Hoc Networks
- 31 Mobility Modeling

# Graph Representation



	a	b	c	d
a		8	4	
b				
c	6			
d	10	2		

	a	c (8), d (4)
a		
b		
c	b (6)	
d	c (2), b (10)	

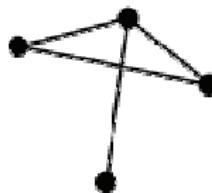
Adjacency list

	1	2	3	4	5
a	8			4	
b	t			t	
c	6	t	t		
d		2	10	t	

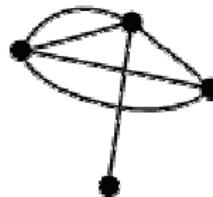
Incidence matrix

- undirected graphs: usually represented as digraphs with two directed edges per actual undirected edge.
- adjacency matrix: a  $|V| \times |V|$  matrix; each cell  $i, j$  contains weight of edge between  $v_i$  and  $v_j$  (0 for no edge)
- adjacency list: a  $|V|$  array where each cell  $i$  contains a list of all vertices adjacent to  $v_i$
- incidence matrix: a  $|V|$  by  $|E|$  array where each cell  $i, j$  contains a weight (HEAD for unweighted graphs) if the vertex  $i$  is head of edge  $j$  or TAIL if vertex  $i$  is tail of edge  $j$

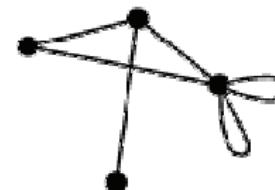
# Example Graphs



Simple graph



multiple links



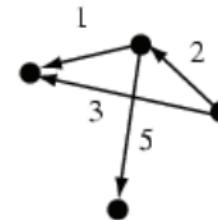
self loops



Directed graph



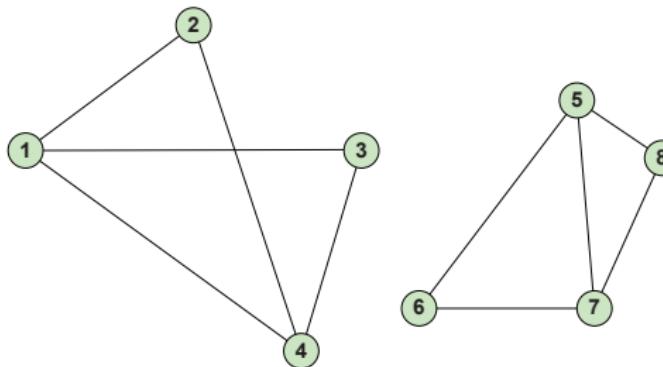
Directed graph



Weighted graph

[Weisstein, Eric W. "Simple Graph." From MathWorld--A Wolfram Web Resource](#)

# Example Graphs



Is this a graph (simple graph)?

$G(V, E)$

Vertex set:  $V=\{1,2,3,4,5,6,7,8\}$

Edge set:  $E=\{(1,2) (1,3) (1,4) (2,4) (3,4) (6,7) (5,6) (5,7) (5,8) (7,8)\}$

# Graph Terminology

- **Degree:** The degree of node  $d_i$  is the number of direct neighbors of that node in the network

$$d_i = \sum_{j=1}^N a_{ij}$$

where

$$a_{ij} = \begin{cases} 1 & \text{if there is edge between } v_i \text{ and } v_j; \\ 0 & \text{otherwise.} \end{cases}$$

- **Connectedness:** A graph  $G$  is connected if there exists a path  $\{i, \dots, j\}$  between any pair of nodes  $i$  and  $j$ .
- **Disconnectedness:** When there is no path between at least one node pair, the network is said to be disconnected.

# Graph Terminology

- Hopcount: number of hops on the path between a source and a destination.
- Average hopcount: average value of the hopcount between all possible source-destination node pairs.
- Shortest path: The shortest path between two nodes is the one having the shortest length (shortest number of hops).
- Diameter: Let  $S$  be the set of the lengths of the shortest paths between all pairs of nodes in the network. The diameter of the graph is the maximum of  $S$ .

# Graph Terminology

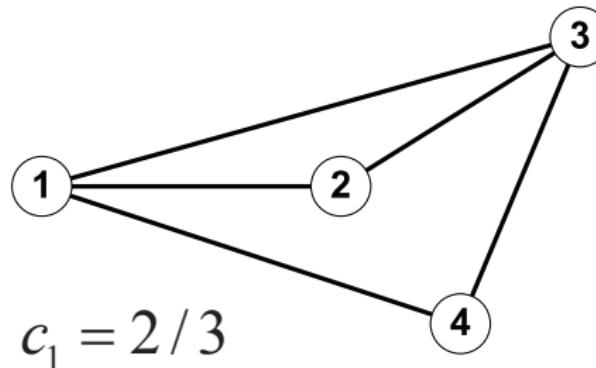
- **Local correlation:** Let node  $i$  be connected to node  $j$ . If the probability of node  $i$  being connected to the neighbors of node  $j$  is higher than the probability of node  $i$  being connected to other nodes in the network, edges are locally correlated
- **Clustering coefficient:** For node  $i$  with  $d_i = 2$ , an edge  $(u, v)$  is opposite to node  $i$  if there exist edges  $(i, v)$  and  $(i, u)$ . The clustering coefficient of node  $i$  is defined as:

$$c_i = \frac{\text{number of opposite edges of } i}{d_i (d_i - 1) / 2}$$

Local correlation increases clustering coefficient

Large clustering coefficient does not mean high local correlation

# Clustering Coefficient



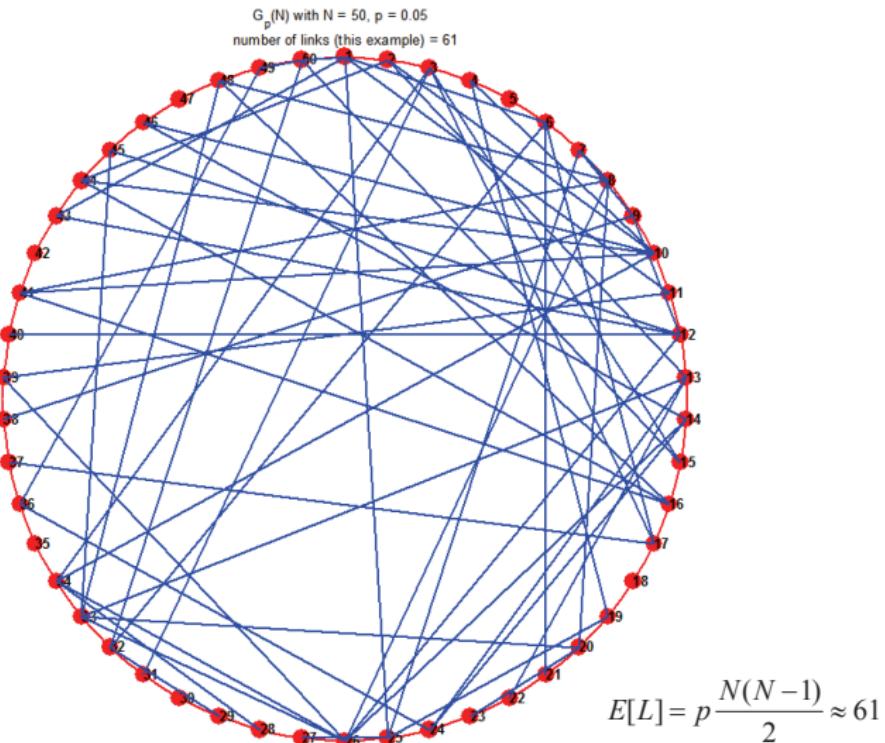
# Agenda

- 25 Objectives
- 26 What is a Graph?
- 27 Representation
- 28 Modeling Ad Hoc Networks as Graphs**
- 29 Scale Free Graphs
- 30 Geometric Random Graph for Ad Hoc Networks
- 31 Mobility Modeling

# Graph Types

- Random graph: A graph of  $N$  nodes and  $L$  links:  $L$  is chosen **randomly** and **independently** from  $N(N - 1)/2$  possible links.
- Scale-free graph: A model proposed for real-world networks. Degree distribution follows a power law, at least asymptotically. For example, degree distribution is  $k^{-\gamma}$  where  $k$  is the degree,  $2 < \gamma < 3.5$  is independent of network size,  $N$
- Geometric random graph

# Random Graph



# Random Graph: Degree

A random graph  $G_p(N)$  of  $N$  nodes and  $L$  links

There are  $\binom{N(N-1)/2}{L}$  equiprobable random graphs

Any pair of nodes are linked with the probability  $p$  so that (expected number of edges):

$$E[L] = p \frac{N(N-1)}{2}$$

Degree of nodes follows Binomial distribution.

$$\text{Prob}\{d_i = k\} = \binom{N-1}{k} p^k (1-p)^{(N-1-k)}$$

If  $p(N) = \lambda/N$  for a constant  $\lambda > 0$  then  $\text{Prob}\{d_i = k\} \approx \exp(-\lambda) \lambda^k / k!$

The mean (expected) degree  $z = (N-1)p$

The variance =  $(N-1)p(1-p)$

Probability that a node is isolated =  $(1-p)^{N-1}$

# Random Graph: Hop count

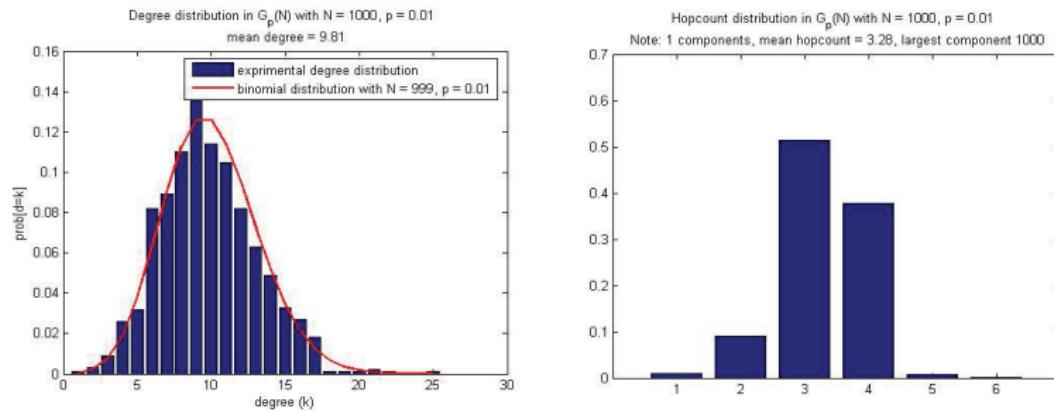
A random graph  $G_p(N)$  of  $N$  nodes and  $L$  links

## How to approximate?

- given mean degree  $z = E[d]$  start from any point,
- after 1 hop  $z$  nodes are expected to have been reached,
- after  $h$  hops  $z^h$  nodes are expected to have been reached (assuming a tree-like graph structure with no self-loops),
- all  $N$  nodes are expected to have been reached when  $N \approx z^h$

Then, expected hop count by approximation is  $E[h] \approx \frac{\log(N)}{\log(E[d])}$

# Random Graph: Degree and Hop count



Theoretical

$$\text{Mean degree} = E[d] = 999 * 0.01 = 9.99$$

$$\text{Mean hopcount} = E[h] = \log(1000) / \log(9.99) = 3.0$$

# Can We Use Random Graphs to Model Ad Hoc Networks?

## Local correlation

none in random graphs, however, ad hoc networks have

## Distance

does not matter in random graphs, however, link probability depends on distance in ad hoc networks

# Agenda

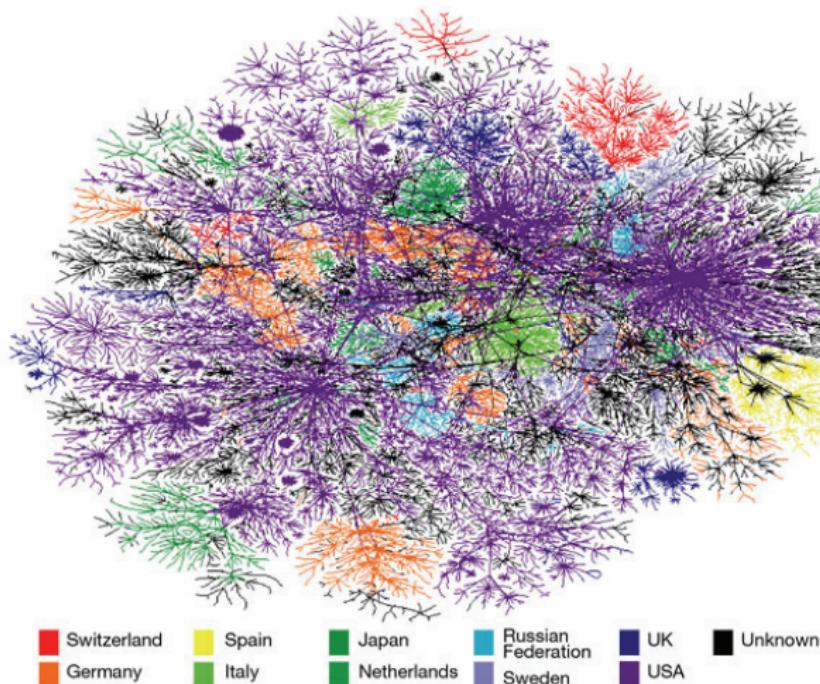
- 25 Objectives
- 26 What is a Graph?
- 27 Representation
- 28 Modeling Ad Hoc Networks as Graphs
- 29 Scale Free Graphs**
- 30 Geometric Random Graph for Ad Hoc Networks
- 31 Mobility Modeling

# Question

## Immune to Accidents but Vulnerable to Attacks

If you want to do an intentional attack to collapse the Internet, what would you do?

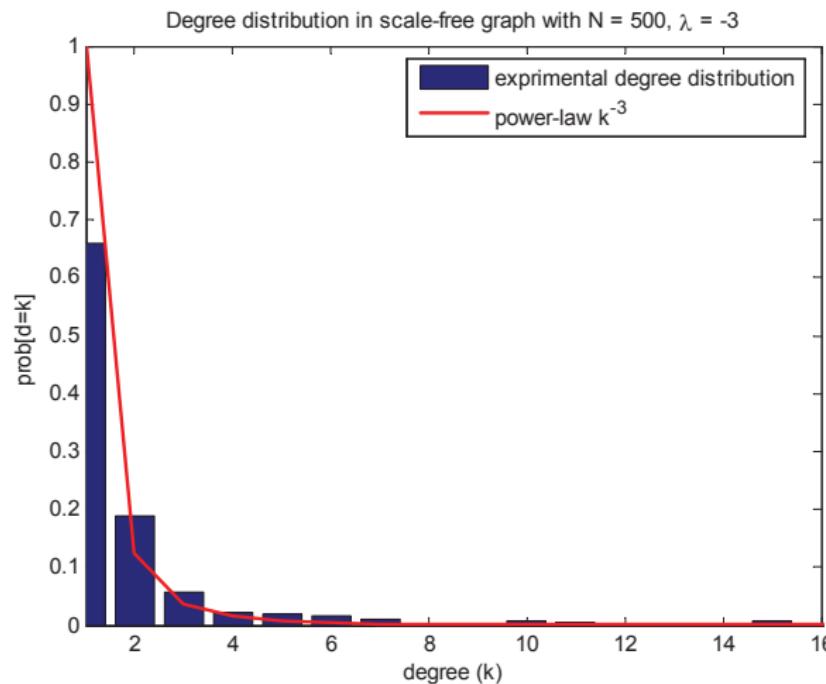
# Scale Free Graphs, e.g. Internet



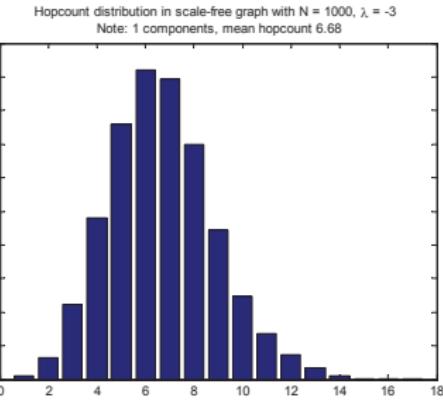
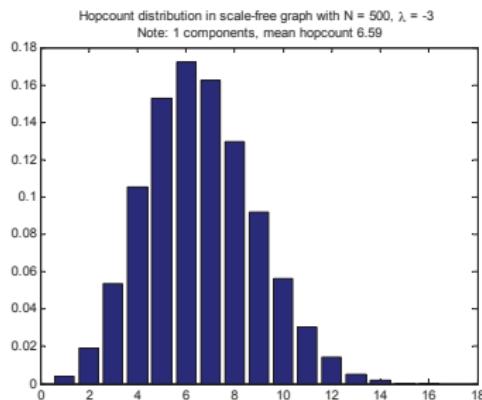
# Scale Free Graphs: Degree and Hop count

- A model proposed for real-world networks like the social networks, Internet (routers as well as webpages) and biological networks
- Degree distribution is **not binomial**, but **has a power-law tail**: degree distribution is  $k^{-\gamma}$  where  $k$  is the degree,  $2 < \gamma < 3.5$  is independent of network size,  $N$
- $\gamma$  is independent from network size, hence the name *scale-free*
- Typical values for  $\gamma$  in real-world networks: 2 - 3.5
- Networks that follow power laws are called 'scale-free networks' because they are not tied to a specific scale
- They are extremely inhomogeneous: whereas most nodes have one or two links, a few highly connected nodes will have a large number of links and so play a key role in the behavior of the network.

# Scale Free Graphs: Degree



# Scale Free Graphs: Hop count



Small-world property!

# Scale Free Graphs: Small World

## Small-world property

A network is said to have the small-world property when the hopcount in that network is not strongly affected by an increase in the network size

Examples: *six degrees of separation* in social networks (S. Milgram, 1967); Web pages on the Internet (see *Linked* by Barabasi)

Most nodes are not neighbors of one another, but most nodes can be reached from every other by a small number of hops or steps.

How to generate: new nodes are added to a pre-existing network, and connected to each of the original nodes with a probability proportional to the number of connections each of the original nodes already had. New nodes are more likely to attach to hubs than peripheral nodes.

# How Robust is Internet?

- The performance of the scale-free network is almost unchanged by the random removal of nodes up to a large deletion rate.
- The immunity of this network's performance to random error suggests two features about the network structure
  - most of the nodes are just 'end users', the removal of which does not affect the paths between other nodes;
  - the existence of highly connected nodes
- These two competing requirements found the perfect balance in scale-free networks
- The most effective way of destroying a network is to attack its most connected nodes
- For the scale-free network, in which there are nodes of high connectivity, the effect of targeted attack is much more severe

# News About Internet

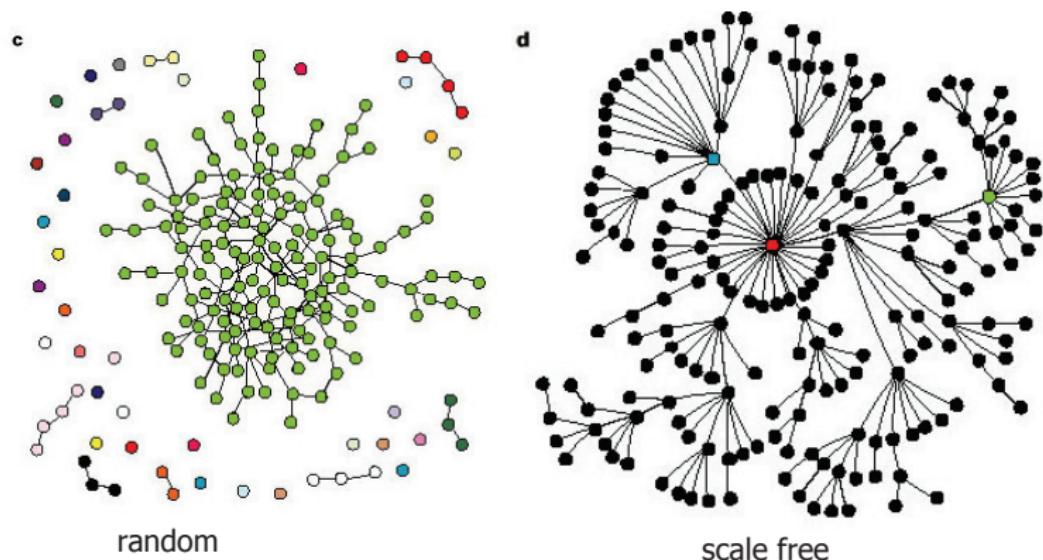
## Good News

The good news is that we do not have to worry about random fluctuations of these networks

## Bad News

The bad news is that Internet terrorists could cause great damage by targeting the most connected routers or web sites.

# Random Graph versus Scale Free



# Agenda

- 25 Objectives
- 26 What is a Graph?
- 27 Representation
- 28 Modeling Ad Hoc Networks as Graphs
- 29 Scale Free Graphs
- 30 Geometric Random Graph for Ad Hoc Networks**
- 31 Mobility Modeling

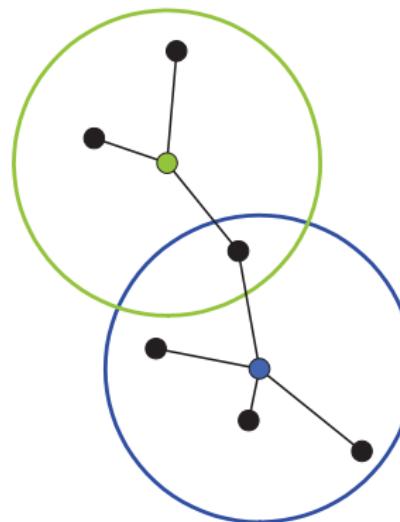
# Pathloss Geometric Random Graph

Random graph denoted with  $G_p(N)$

Geometric random graph denoted with  $G_{p(r)}(N)$

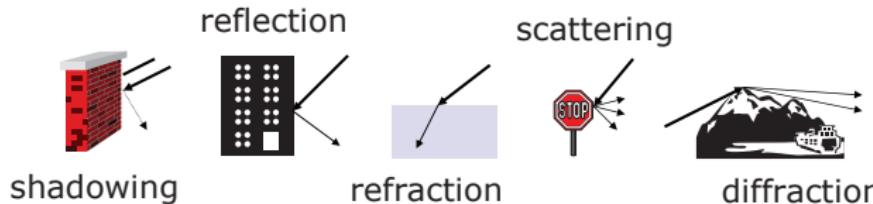
$p(r)$  depends on the distance between nodes

Geometric graph models are suitable for modeling ad hoc networks depending on  $p(r)$



# Pathloss Geometric Random Graph

- Pathloss: Receiving power proportional to  $1/d^\eta$  (path-loss exponent  $\eta = 2$  in vacuum,  $d$ : distance)
- Not realistic because of other influential factors such as
  - fading (frequency dependent)
  - shadowing
  - reflection at large obstacles
  - refraction depending on the density of a medium
  - scattering at small obstacles
  - diffraction at edges



# Pathloss Geometric Random Graph: Degree

Assume a pair of **random points** are selected as the position of 2 nodes in a convex field.

The distance between these two nodes,  $x$  is denoted with the **random variable  $X$**  where the probability density and cumulative distribution functions are represented with  $f_X(x)$  and  $F_X(x)$ , respectively.

Let  $g(x)$  denote probability of having a stable communication link between these two nodes.

**Pathloss model:** Assume that if the distance between the sender and receiver antennas of the nodes is less than a threshold distance  $d_c$  (communication range), nodes can communicate; otherwise, cannot.

Therefore,  $g_X(x) = 1$  if  $x \leq d_c$  and zero otherwise.

# Pathloss Geometric Random Graph: Degree

When two nodes are positioned randomly in the field, the expected value of the connectivity probability,  $\mathcal{P}$  of these two randomly positioned homogeneous nodes with maximum communication range  $d_c$  is

$$\mathcal{P} = \int_{-\infty}^{\infty} g_{\mathbf{x}}(x) f_{\mathbf{x}}(x) dx = \int_0^{d_c} f_{\mathbf{x}}(x) dx = F_{\mathbf{x}}(d_c).$$

## Bernoulli trial setup

Selecting two random points in a field and checking whether the Euclidean distance between these two points is smaller than the maximum communication range ( $d_c$ ) can be considered as a **Bernoulli trial** with **success probability  $\mathcal{P}$** .

**Bernoulli trial:** a single experiment which can have one of two possible outcomes; e.g., tossing a coin.

# Pathloss Geometric Random Graph: Degree

## Bernoulli trial setup

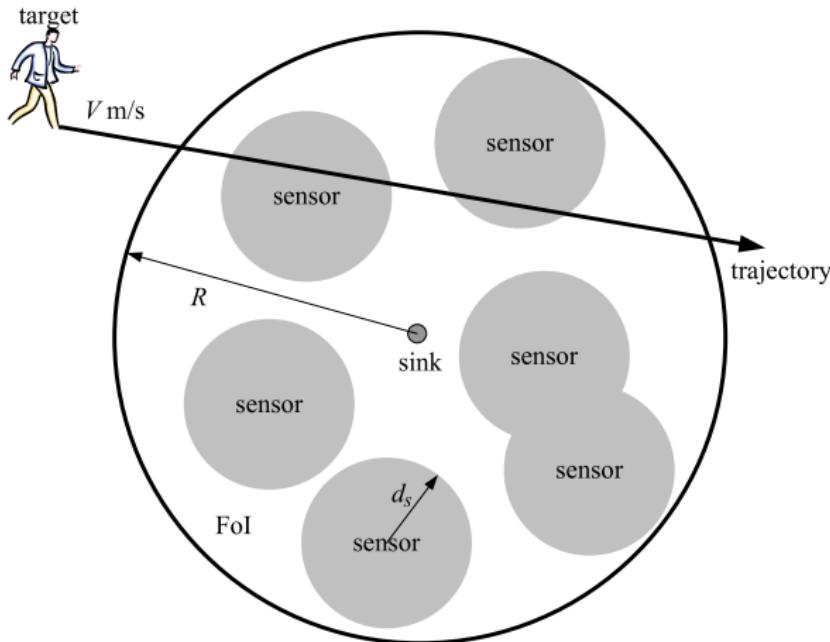
Choose two random points in the circular Fol and assume that the nodes are located on these points. If the distance between these two random points is less than  $d_c$ , then two nodes can communicate with each other successfully and the trial is a success. If the distance is larger than  $d_c$ , then the trial fails.

If  $N$  homogeneous nodes are deployed, then the probability that a randomly positioned node is in the communication range of  $k$  out of other  $N - 1$  nodes follows the **binomial distribution**  $\mathcal{B}(N - 1, \mathcal{P})$ . **Connectivity degree follows Binomial distribution for random deployment**

**Mean connectivity degree,  $E[k]$**  is the expected value of the binomial distribution where success probability of the trial is  $\mathcal{P}$ .

$$E[k] = (N - 1)\mathcal{P}. \quad (1)$$

# Pathloss Geometric Random Graph: Degree; e.g., Circular Field



# Pathloss Geometric Random Graph: Degree; e.g., Circular Field

When a pair of nodes are randomly deployed in the circular field with radius  $R$ , the pdf of the distance between these points is

$$f_x(x) = \frac{2x}{R^2} \left( 1 - \frac{2}{\pi} \sin^{-1} \left( \frac{x}{2R} \right) - \frac{x}{\pi R} \sqrt{1 - \frac{x^2}{4R^2}} \right),$$

where  $0 \leq x \leq 2R$  and  $f_x(x) = 0$  if  $x > 2R$ .

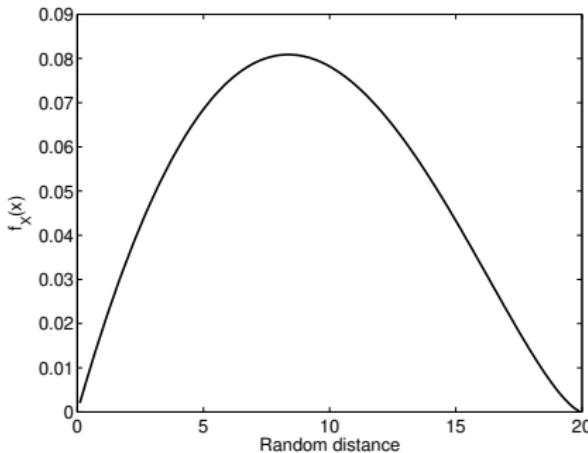
Then, the cdf is

$$F_x(x) = \frac{1}{\pi R^3} \left[ 2(R^3 - Rx^2) \sin^{-1} \left( \frac{x}{2R} \right) \right. \\ \left. - \frac{x}{4\pi R^3} \left[ (2R^2 + x^2) \sqrt{4 - \frac{x^2}{R^2}} - 4\pi Rx \right] \right],$$

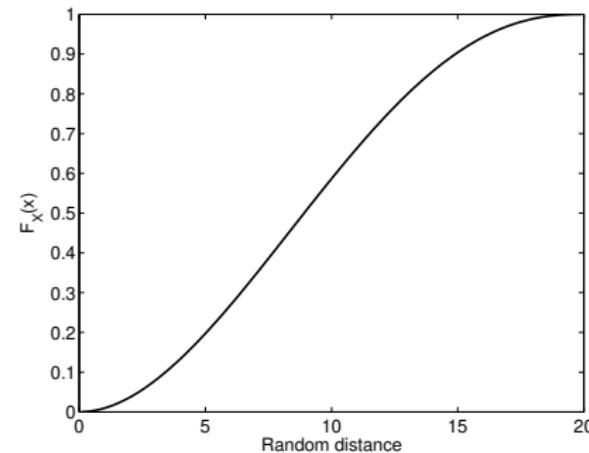
where  $0 \leq x \leq 2R$  and  $F(x) = 1$  if  $x \geq 2R$ .

# Pathloss Geometric Random Graph: Degree; e.g., Circular Field

Probability density (pdf) and cumulative distribution function (cdf) where  $R = 20$  meters.



pdf



cdf

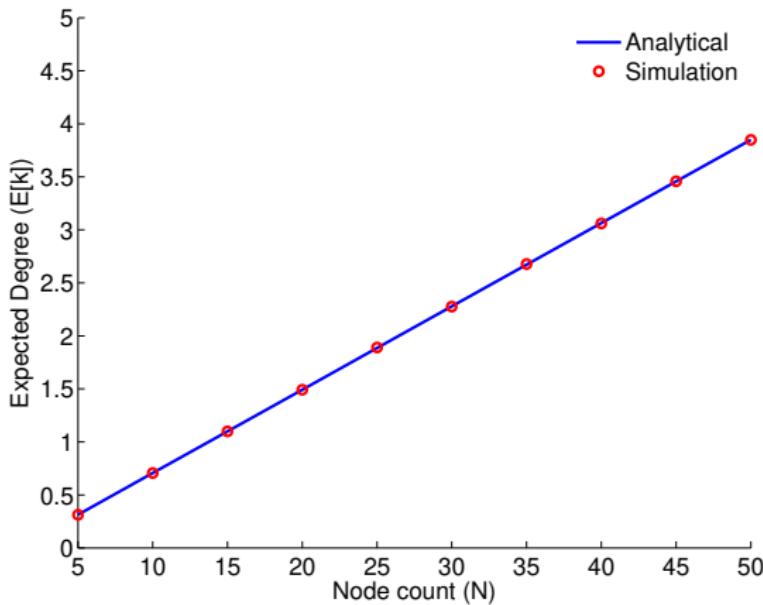
# Pathloss Geometric Random Graph: Degree; e.g., Circular Field

The expected value of the distance between the random points is  $2.84d_c/\pi$ . Denote  $\xi = d_c/R$  which is the normalized communication range, then

$$\mathcal{P} = \frac{2 - 2\xi^2}{\pi} \sin^{-1}\left(\frac{\xi}{2}\right) - \frac{(2\xi + \xi^3)}{4\pi} \sqrt{4 - \xi^2} + \xi^2$$

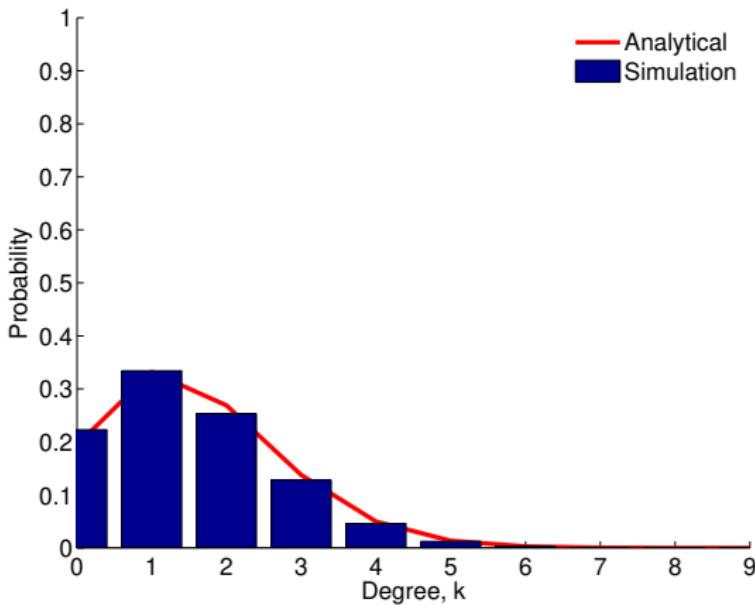
The expected connectivity degree is  $k = (N - 1)\mathcal{P}$  when  $N$  nodes are uniformly randomly deployed in a circular field.

# Pathloss Geometric Random Graph: Degree; e.g., Circular Field



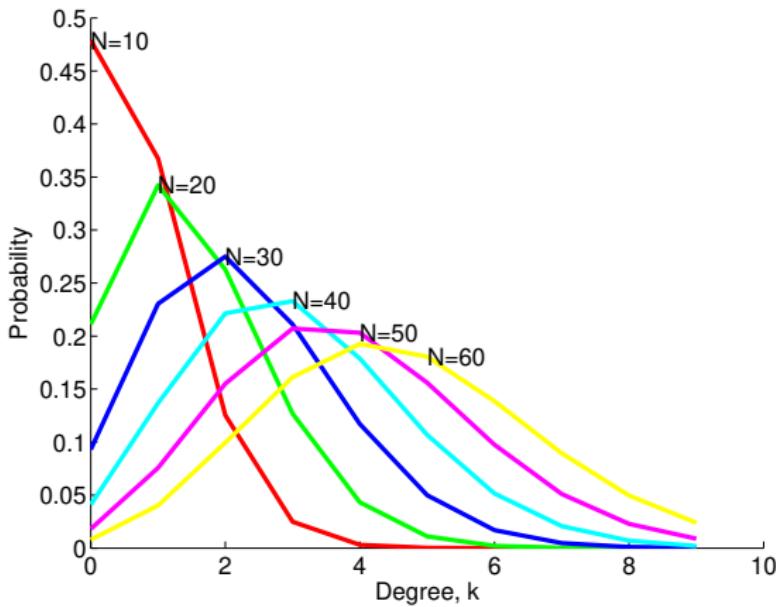
10000 simulation runs,  $R = 100$  m,  $d_c = 30$  m

# Pathloss Geometric Random Graph: Degree; e.g., Circular Field



100000 simulation runs,  $R = 100$  m,  $d_c = 20$  m,  $N = 20$

# Pathloss Geometric Random Graph: Degree; e.g., Circular Field

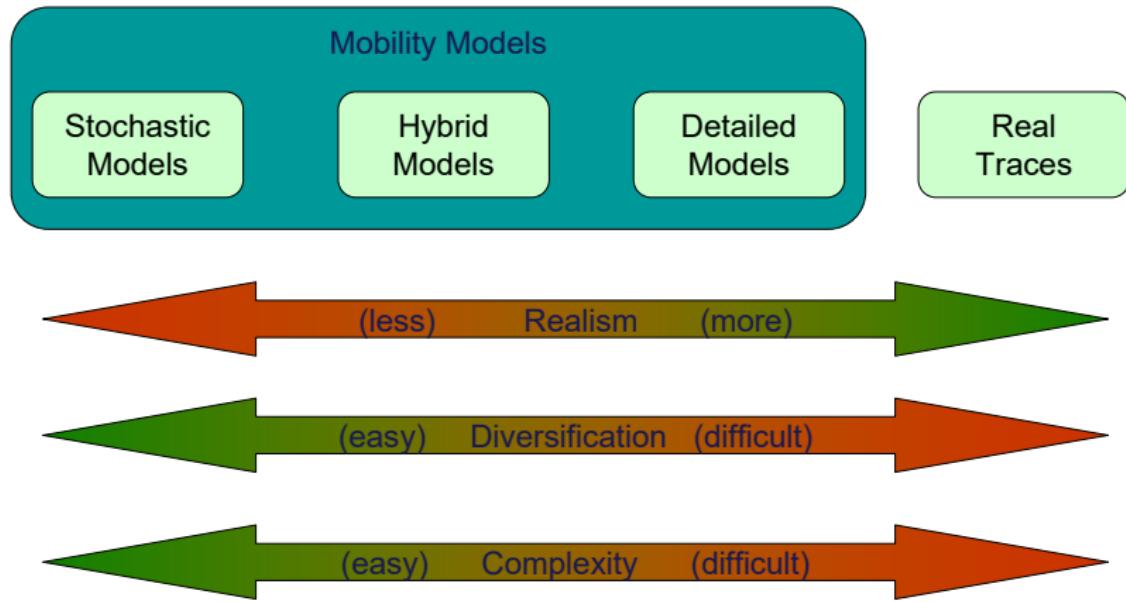


100000 simulation runs,  $R = 100$  m,  $d_c = 30$  m

# Agenda

- 25 Objectives
- 26 What is a Graph?
- 27 Representation
- 28 Modeling Ad Hoc Networks as Graphs
- 29 Scale Free Graphs
- 30 Geometric Random Graph for Ad Hoc Networks
- 31 Mobility Modeling**

# Mobility Model Classification I



Source [10]

# Mobility Model Classification II

## Comparison Measures:

- **Realism** is the degree of accuracy of the mobility model, with respect to the movements of mobile nodes in a real scenario
- **Diversification** qualifies the ability of a model to diversify to a large number of different scenarios, including different types of mobile nodes (e.g., vehicles, pedestrians, zebras) and different types of environments (e.g., campus, conference, city).
- **Complexity** is a measure of the computational resources required to produce the traces for the simulation.

# Mobility Model Classification III

## Classification:

- **Stochastic models** rely primarily on random movements, without imposing any constraints on the movement of the nodes. Examples random waypoint, random direction. Not tied to any particular scenario.
- **Detailed models**, custom-built for a particular scenario. E.g., for a detailed mobility model of students in a campus, the student's schedules, means of arriving on campus (bus, bike, car), location of parking lots and classrooms, library, .. can be considered
- **Hybrid models** aim to balance the realism of detailed models with the diversification convenience of stochastic models. Can be categorized as obstacle, and tracebased mobility models.
- **Real traces** are collections of trajectories of real users in a particular scenario. CRAWDAD <https://crawdad.org> is making several such collections available to researchers.

# Stochastic Mobility Models

## Random Waypoint Mobility Model (RWP)

- RWP assumes a fixed number of nodes in a fixed size rectangle
- Uniform randomly deployed nodes in the rectangle
  - Each node moves independently of the others
  - Chooses a random destination
  - Chooses a random speed
  - When it arrives at the destination it chooses a random pause time
- fairly easy to diversify
- not realistic
- node density is not uniform random after warm-up
- RWP uses a bounding rectangle, the **inter-meeting times** (i.e., time between two nodes will be in wireless range of each other) decay exponentially; in real life, the inter-meeting times have a power-law distribution.
- Sufficiently large rectangle solves the inter-meeting time problem

# Stochastic Mobility Models

## Random Walk Mobility Model (RWM)

- Each node
  - chooses a random direction (uniformly distributed in  $[0, 2\pi]$ )
  - chooses and a random speed (also uniformly distributed in  $[v_{min}; v_{max}]$ );
  - then moves for a time period (or over a fixed distance) with this speed,
  - then repeats its choice.
- Nodes reflect from edges
- Unrealistic
- Long term: nodes stay in the middle of field
- RWM has the same exponential inter-meeting times as RWP

# Stochastic Mobility Models

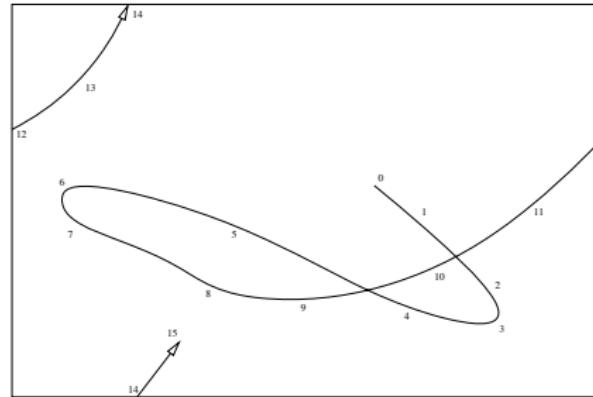
## Random Direction Mobility Model (RDM)

- Each node
  - chooses a direction and travels on in that direction with a random speed until it encounters an edge.
  - then chooses another direction and repeats the algorithm.
- it results in a uniform stationary distribution in the rectangle,
- unrealistic as RWP and RWM
- sudden changes in speed and direction

# Stochastic Mobility Models

## Smooth Mobility Model (SM)

- To avoid the unrealistic and sudden changes as well as the edge effects of RWP, RWM, and RDM, Haas proposed a smooth mobility model
- Each node changes speed and direction smoothly
- The world is a torus, resulting in smooth trajectories
- In SM, each node is characterized by a motion vector  $(v, q)$ , where  $v$  is the speed of the node and  $q$  is the direction. The position  $(x, y)$  of a node and its motion vector are updated periodically



# Group Mobility Models

- Nodes are split in several smaller groups, and each group acts seemingly independently of the other groups
- Each group moves randomly (RWP)
- Each node in the group moves randomly around the group center
- First step toward realism
- Classical examples include military, search and rescue, and public safety, but also students or employees in a campus.
- Has two sub-models where any flat-earth model above can be employed
  - Group model
  - Individual model

# Obstacle Models

- Above models are unrealistic since there are no obstacles
- Restrict the degrees of freedom for movements
- In **Manhattan mobility model** nodes can only move on a grid (of roads)
  - Move on a grid
  - At an intersection: go straight with a probability of 0.5 or turn left or right with a probability of 0.25
  - it does not implement lane changes or stop lights and vehicles can do U-turns in the middle of the highway
  - far more realistic model for vehicular networks than any of the stochastic models
- In **Freeway mobility model**, nodes follow the rules on Freeways (with multiple lanes and two directions).
  - the nodes are restricted to follow the existing roads
  - the nodes are restricted to follow their lanes without passing the vehicles in front
  - have limited acceleration and breaking capabilities.
  - better model for a scenario involving vehicles on a highway than RWP, it is not well suited for a scenario involving students in a campus or participants at a conference.

# Trace-based Mobility Models I

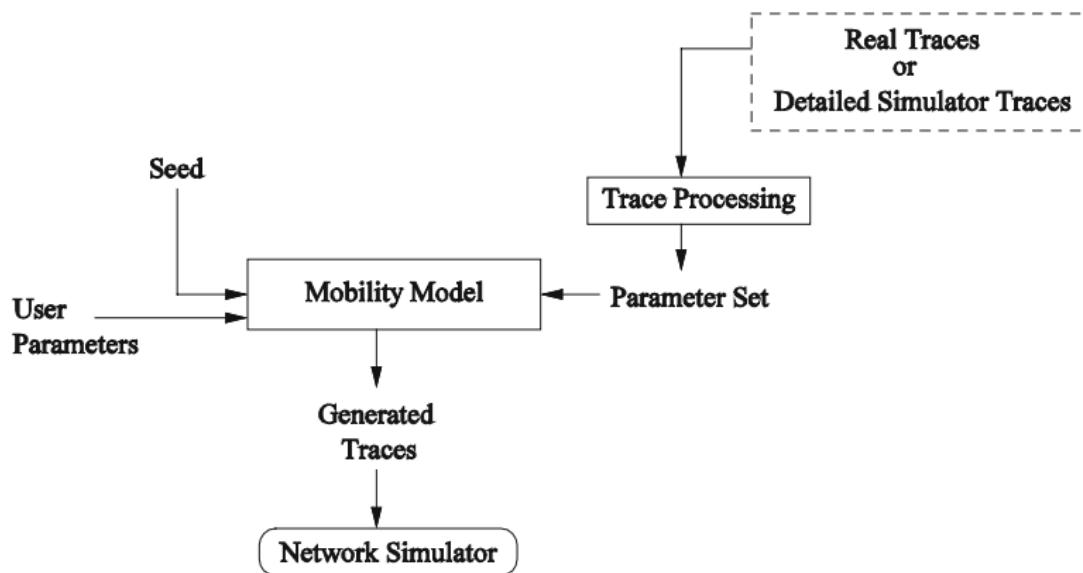
- Aim to replicate/emulate the type of movements in a sample trace
- Given a sample trace from a target scenario, many similar traces can be produced.
- A target protocol can be used for validation of the generated traces against the real traces.

# Trace-based Mobility Models II

Parameter set:

- The inter-arrival and inter-departure times of the nodes (and thus, the resulting number of nodes).
- The existence of hotspots in the scenario.
- The existence of groups (time and size), perhaps quantified by the average number of neighbors.
- Inter-meeting times.
- The distribution of pause times.
- The distribution of node speeds.

# Trace-based Mobility Models III



# Further Research Topics I

- Network measures
  - Size
  - Link Density
  - Node Density
  - Planar Network Density
  - Average degree
  - Average shortest path length (or characteristic path length)
  - Optimal path
  - Diameter of a network
  - Clustering coefficient
  - Connectedness
  - Node centrality
  - Node influence
- Centrality Measures
  - Betweenness Centrality
  - Closeness Centrality
  - Information Centrality
  - Lobby Index

# Further Research Topics II

- Component Measures
  - Number of Components
  - Component Coefficient
  - Number of Communities
  - Community Modularity
- Link-level measures
  - Link Duration
  - Re-Healing Period
  - Number of Connected Periods

## Lecture 5: Data Link Layer: Frame and Share

# Objectives

- to identify the key services in link layer
- to classify MAC protocols [11]
- to assess the channel utilization by various MAC protocols
- to compare applicability of various MAC protocols in ad hoc networks

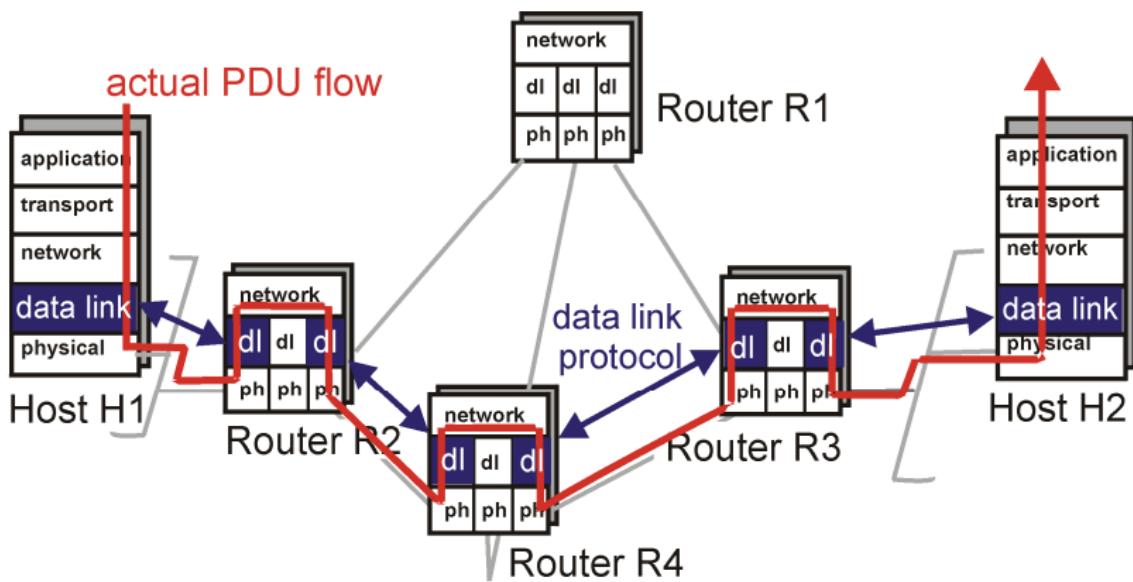
# Agenda

- 32 Data Link Layer
- 33 Sharing the Medium
- 34 Contention Free MAC Protocols
- 35 Contention Based MAC Protocols

# Functions of Data Link Layer

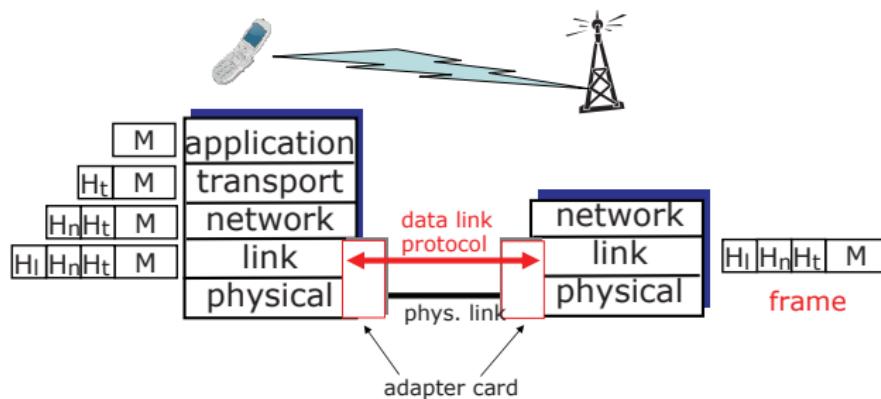
- Services
  - Ensures that data is transferred correctly **between adjacent network nodes**
  - **Detect and correct errors** that may occur in the physical layer
  - Share a common medium
  - Addressing (point-to-point versus broadcast)
  - Framing
- Sub-layers
  - **Logical link control (LLC):** provides multiplexing and flow control mechanisms that make it possible for multi network protocols to correlate with multipoint network
  - **Medium access control (MAC):** how to access the common channel?

# Scenario



# Services of the Logical Link Control Sublayer: Framing

- Protocol data unit is a **frame**: frame length, bit stuffing, byte stuffing, code violation
- Data-link layer is responsible for transferring frame from one node to another node over a **link**
- Encapsulate datagram into frame, adding a header and a trailer (for error detection)
- Physical addresses in frame header identify source, destination



# Services of the Logical Link Control Sublayer

## Flow control

- pacing between sender and receivers
- slow receivers must not be swamped by fast senders

## Error Detection

- errors caused by signal attenuation, noise
- receiver detects presence of errors: signal sender for retransmission or drops frame

## Error Correction

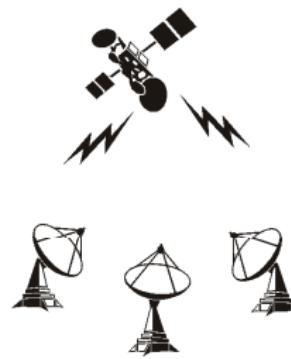
- receiver identifies and corrects bit error(s) without resorting to retransmission

# MAC Sublayer: Medium Access Control

A MAC protocol defines how each mobile unit can **share the limited wireless bandwidth** resource in an efficient manner.



shared wireless  
(e.g. Wavelan)



satellite



cocktail party

# Agenda

- 32 Data Link Layer
- 33 **Sharing the Medium**
- 34 Contention Free MAC Protocols
- 35 Contention Based MAC Protocols

# Multiple Access Protocols

- single shared communication channel
- two or more simultaneous transmissions by nodes: interference
- only one node can send successfully at a time

## Multiple access protocol

- distributed algorithm that determines how stations share channel, i.e., determine when station can transmit
- communication about channel sharing must use channel itself!
- design considerations
  - synchronous or asynchronous
  - information needed about other stations
  - robustness (e.g., to channel errors)
  - performance

# Performance Measures

## Throughput

percentage of successfully transmitted frames per unit time

## Delay

interval between the datagram arrival time at the data link layer of sender and the time sender realizes successful reception by receiver

## Fairness

measures how fair the channel allocation is among the flows in the different mobile nodes

## Energy efficiency

e.g., fraction of the useful energy consumption to the total energy spent.

# Medium Access Protocols (MAC)

Can we apply medium access methods from fixed networks?

- Example: **Carrier Sense Multiple Access with Collision Detection**
  - **CSMA/CD**: Send as soon as the medium is free, listen into the medium if a collision occurs (legacy method in IEEE 802.3)
- Problems in wireless networks
  - signal strength decreases proportional to the square of distance
  - sender would apply CS and CD, but the collisions happen at the receiver
  - a sender might not **hear** the collision, i.e., **CD does not work**
  - **CS might not work** if, e.g., a terminal is hidden

# Collision Detection (CD)

In wired CSMA/CD, due to small attenuation along the wire, collision can be detected by looking for abnormalities in power level, code violation or discrepancy between transmitted data and actual data on the cable.

**CD use in radio channels is inhibited; why?**

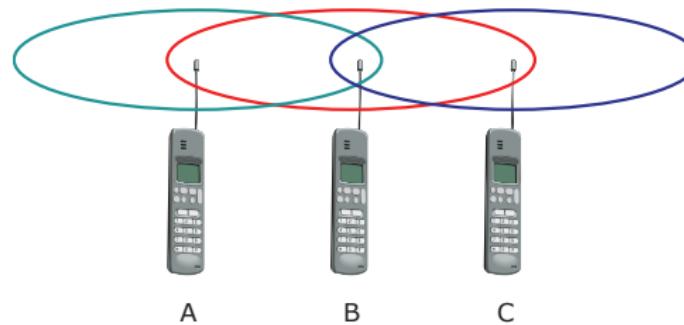
CSMA as used in wired networks cannot be directly used in wireless networks:

- hidden node problem
- in the same wireless channel, the outgoing signal can easily overwhelm the incoming signal due to high signal attenuation in wireless channels. This problem makes it difficult for a sender to directly detect collisions in a wireless channel.

Solution: Wait for ACK or use collision avoidance (CA)

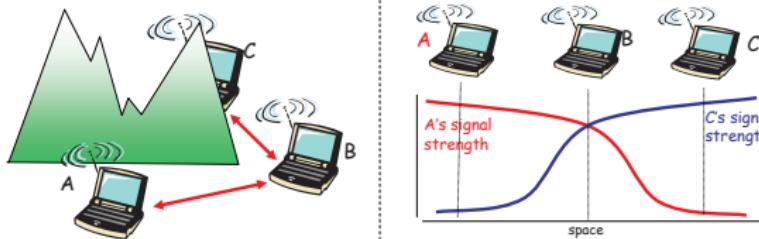
# Hidden Terminal Problem

- A sends to B, C cannot receive A
- C wants to send to B, C senses *free* medium (CS fails)
- collision at B, A cannot receive the collision (CD fails)
- A is **hidden** for C



- CS:**Carrier Sense**
- CD:**Collision Detection**

# Hidden Terminal Problem



## Hidden terminal problem

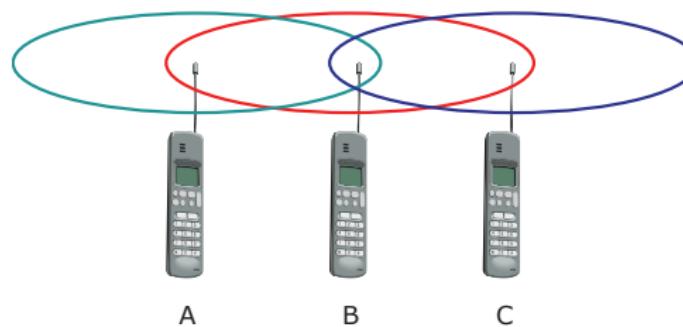
- B, A hear each other
- B, C hear each other
- A, C cannot hear each other
- means A, C unaware of their interference at B

## Signal fading

- B, A hear each other
- B, C hear each other
- A, C cannot hear each other
- interfering at B

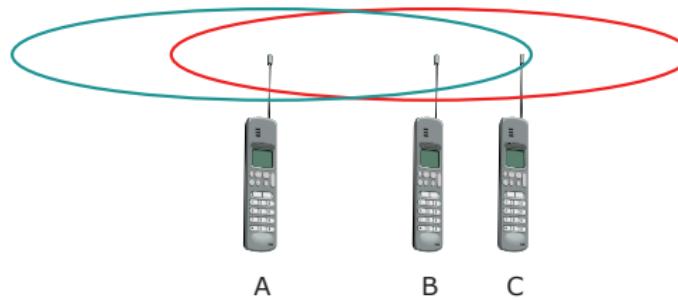
# Exposed Terminal Problem

- B sends to A, C wants to send to another terminal (not A or B)
- C has to wait, CS signals a medium in use
- but A is outside the radio range of C  $\Rightarrow$  waiting is not necessary
- C is **exposed to B**

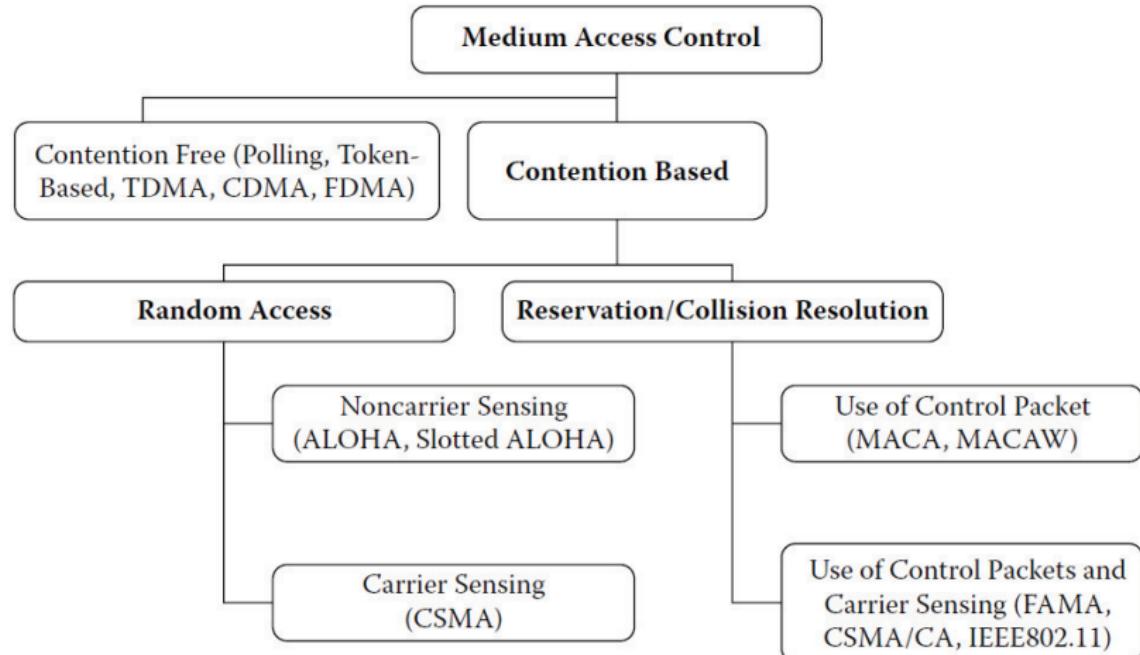


# Near and Far Terminals

- Terminals A and B send, C receives
- Signal strength decreases proportional to **square** of distance
- B's signal drowns out A's signal
- C cannot receive A  $\implies$  Power control needed



# Classification of MAC Protocols



# Agenda

- 32 Data Link Layer
- 33 Sharing the Medium
- 34 Contention Free MAC Protocols**
- 35 Contention Based MAC Protocols

# Contention Free MAC Protocols

## SDMA (Space Division Multiple Access)

segment **space** into sectors, use directed antennas, cells

## FDMA (Frequency Division Multiple Access)

assign **a certain frequency**

## TDMA (Time Division Multiple Access)

assign fixed frequency **for a certain amount of time**

## CDMA (Code Division Multiple Access)

**all terminals** send on the same frequency probably **at the same time** and can use the **whole bandwidth** of the transmission channel

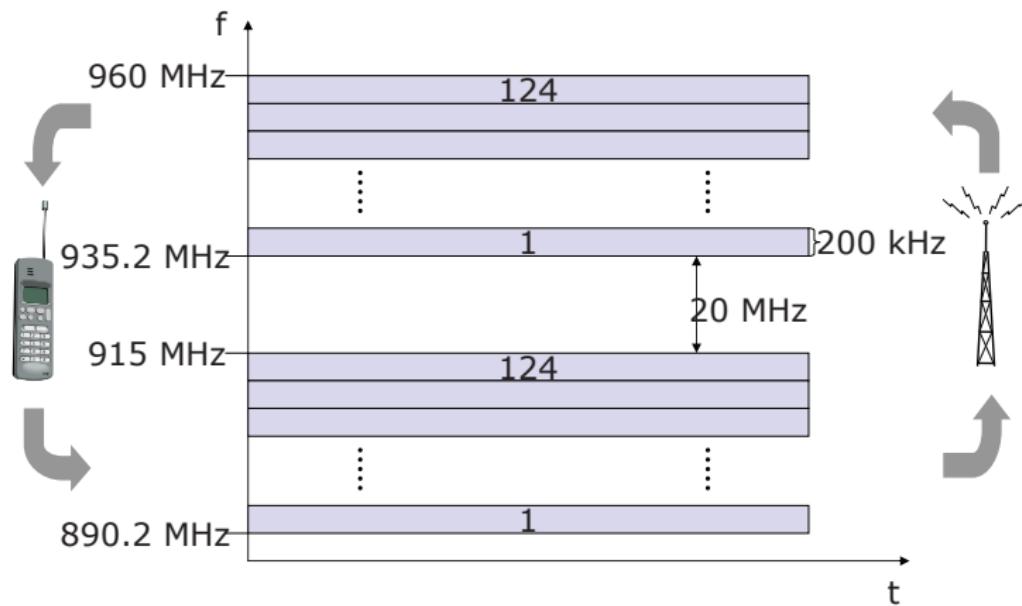
Do you remember the multiplexing schemes? **Same idea!**

# SDMA: Space Division Multiple Access

- Allocate a separate space to users
- Typical application: assign optimal base station to user
- SDMA used in combination with other schemes
- SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing space division multiplexing.
- Directional antennas also play a significant role

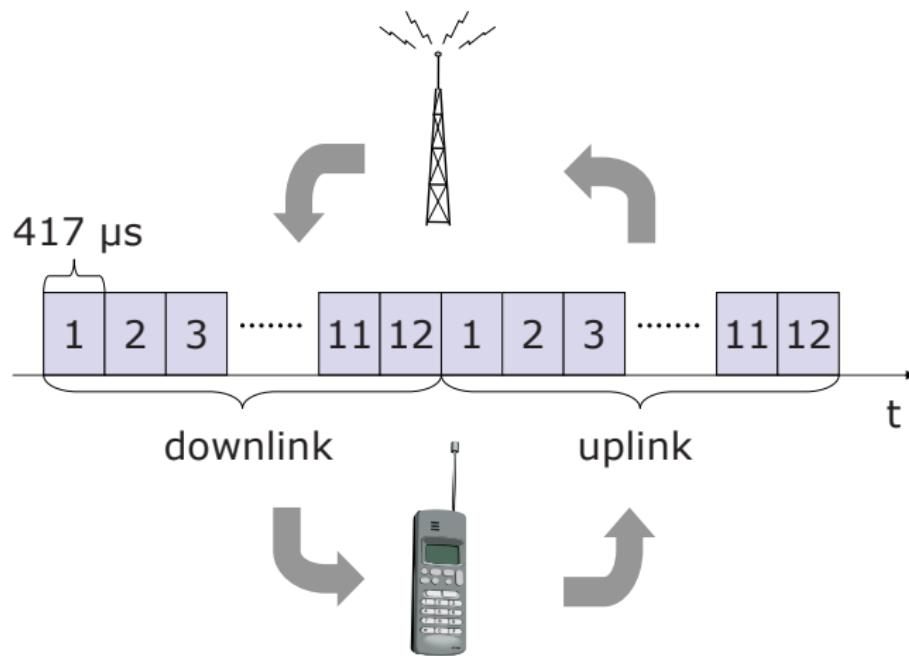
# FDMA: Frequency Division Multiple Access

GSM example:



# TDMA: Time Division Multiple Access

DECT example:



# CDMA: Code Division Multiple Access

- all terminals send on the same frequency at the same time and can use the whole bandwidth
- each sender has a unique random number, the sender XORs the signal with this random number
- the receiver can *tune* into this signal if it knows the pseudo random number

## Disadvantages

higher complexity of a receiver; all signals should have the same strength at a receiver

## Advantages

all terminals can use the same frequency, no planning needed; huge code space (e.g.  $2^{32}$ ) compared to frequency space; interferences is not coded; forward error correction and encryption can be easily integrated

# Comparison of Contention Free MAC Protocols

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km <sup>2</sup>	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Dis-advantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	still faces some problems, higher complexity, lowered expectations; will be integrated with TDMA/FDMA

# Agenda

- 32 Data Link Layer
- 33 Sharing the Medium
- 34 Contention Free MAC Protocols
- 35 Contention Based MAC Protocols**

# Contention-Based MAC

contention (noun) disagreement that results from opposing arguments  
contend (verb) to compete in order to win something

## Random Access

With random access-based schemes, such as ALOHA, a node may access the channel as soon as it is ready

Naturally, more than one node may transmit at the same time, causing collisions, **Utilization?**

## Reservation or Collision Resolution

Reservation approach involves setting up some sort of a reservation prior to data transmission To solve the hidden and exposed-terminal problems:  
Request-to-send/clear-to-send (RTS/CTS) control packets to prevent collisions

# Random Access Protocols

## When node has packet to send

transmit at full channel data rate  $R$

no a priori coordination among nodes

- 2 or more transmitting nodes cause **collision**
- How to detect/sense collisions?
- How to recover from collisions?

Examples: pure (unslotted) ALOHA, slotted ALOHA, CSMA, CSMA/CD, CSMA/CA

# ALOHA

## Sotted ALOHA assumptions

all frames have same size

time is divided into equal size slots; a slot = time to transmit 1 frame

nodes start to transmit frames only at beginning of slots (aligned)

nodes are synchronized

if 2 or more nodes transmit in slot, all nodes detect collision

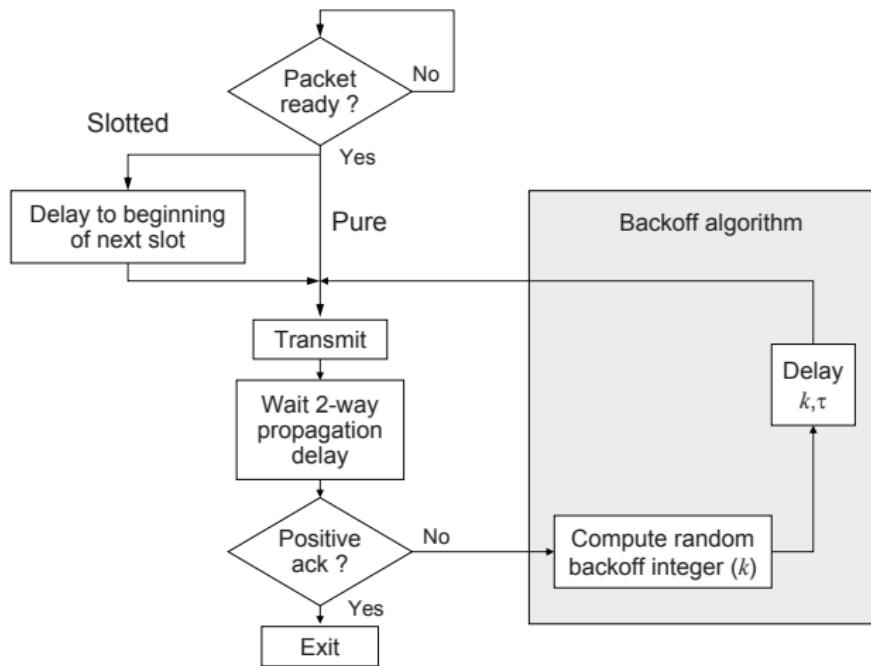
## Unsotted ALOHA assumptions

simpler, no synchronization

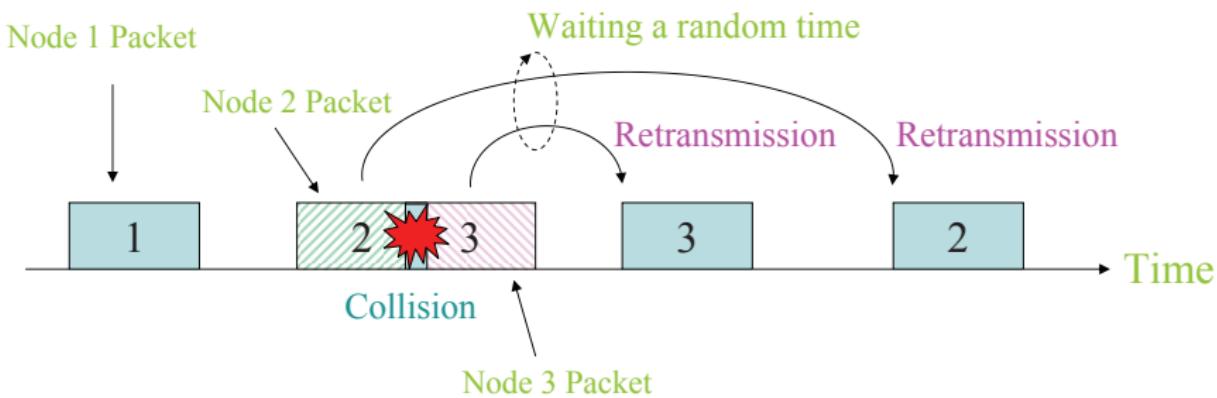
when frame first arrives transmit immediately

collision probability larger

# ALOHA Flowchart



# ALOHA Collision Resolution



# ALOHA Efficiency

## Definition

Efficiency is the long-run fraction of successful slots when there's many nodes, each with many frames to send

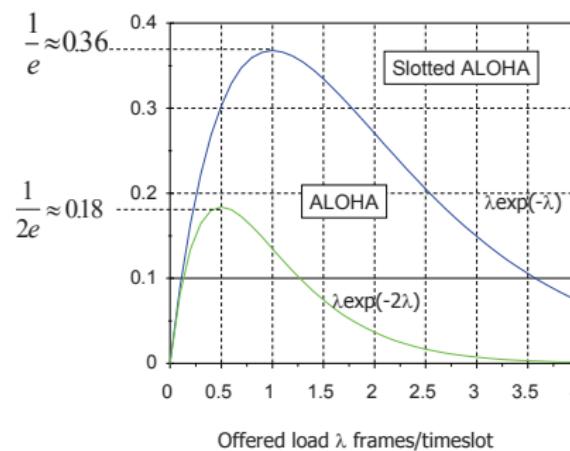
- Assume there are  $N$  nodes with many frames to send
- Each node transmits in a slot with probability  $p$
- Probability that only 1 node succeeds in a slot is  $p(1 - p)^{N-1}$
- Probability that any  $k$  nodes try to transmit in a slot is  
$$f(k; N, p) = \binom{N}{k} p^k (1 - p)^{N-k}$$

Is this binomial distribution?

# ALOHA Efficiency

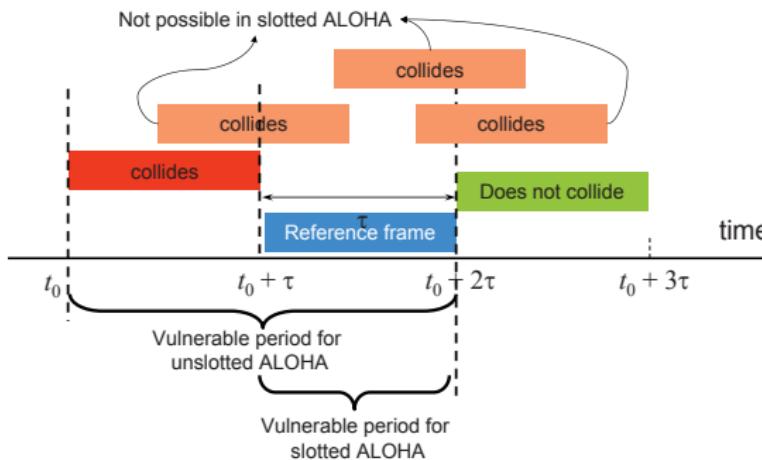
- Binomial distribution converges towards Poisson distribution as  $N \rightarrow \infty$  with  $\lambda = Np$
- Therefore  $f(k; N, p)$  becomes  $f(k; \lambda) = \frac{\lambda^k e^{-\lambda}}{k!}$
- Efficiency =  $f(k = 1; \lambda = Np) = \lambda e^{-\lambda}$

Why  $k = 1$ ? Why slotted ALOHA is more efficient?



# ALOHA Efficiency

- Any node which tries to transmit in the vulnerable period of the reference frame collides with the reference frame.
- Vulnerable period of unslotted ALOHA is twice that of slotted ALOHA.



# CSMA: Carrier Sense Multiple Access

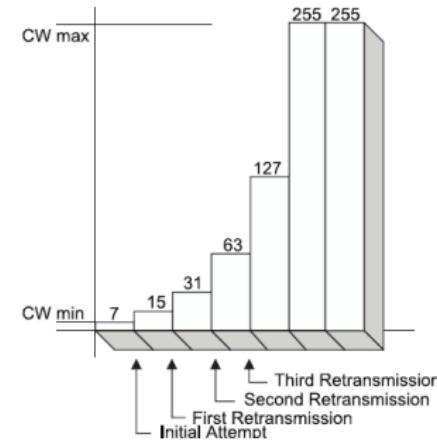
Basic idea: **LISTEN BEFORE TRANSMIT** Do we do this in real life?

- If channel sensed idle: transmit entire frame
- If channel sensed busy, defer transmission (back-off)

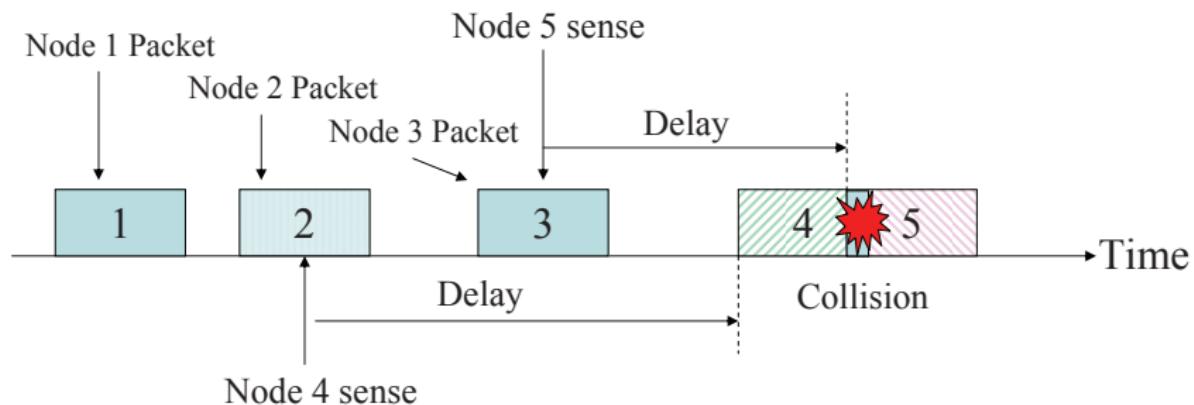
Each terminal chooses a random back-off time

Random back-off decrease the probability of collision

Random back-off time is chosen uniformly from values between  $CW_{min}$  and  $CW_{max}$  in contention window



# CSMA Collision Resolution



# CSMA Types

## Non-persistent CSMA

1. If the medium is idle, transmit immediately
2. If the medium is busy, wait random amount of time and do step 1

Waste idle time if the backoff time is too long

## 1-persistent CSMA

1. If the medium is idle, transmit immediately
2. If the medium is busy, continue to listen until medium becomes idle, and then transmit immediately

There will always be a collision if two nodes want to retransmit

Transmission attempts are stopped after few trials

# CSMA Types

## $p$ -persistent CSMA

1. If the medium is idle, transmit with probability  $p$ , and delay for worst case propagation delay for one packet with probability  $(1 - p)$
2. If the medium is busy, continue to listen until medium becomes idle, then go to step 1
3. If transmission is delayed by one time slot, continue with step 1

Do you see the trade-off between non-persistent and 1-persistent?

What should  $p$  be?

# CSMA Types

What should  $p$  be?

## **$p$ -persistent CSMA**

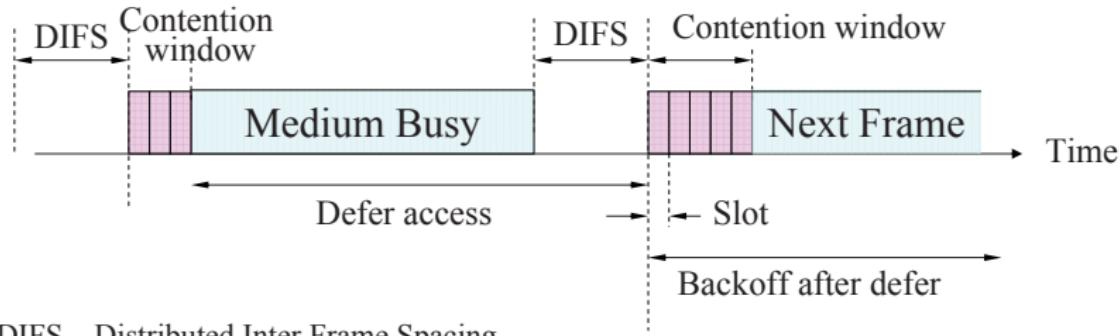
Assume there are  $N$  active nodes (having a packet to be sent)  
Then, expected number of transmissions is  $Np$ .

If  $Np > 1$  collisions occur, therefore **select  $p$  such that  $Np \leq 1$**

# CSMA/CA, CA:Collision Avoidance

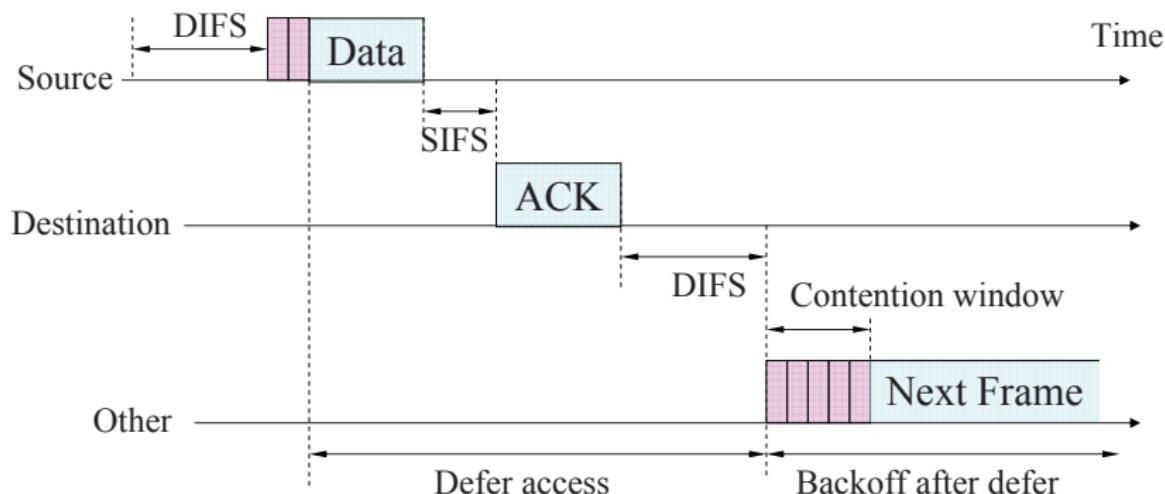
- Terminal ready to transmit senses the medium.
- If medium is busy it waits until the end of current transmission.
- It again waits for an additional predetermined time period DIFS (Distributed inter frame Space).
- Then picks up a random number of slots (the initial value of backoff counter) within a contention window to wait before transmitting its frame.
- If there are transmissions by other terminals during this time period (backoff time), the terminal freezes its counter.
- It resumes count down after other terminals finish transmission + DIFS. The terminal can start its transmission when the counter reaches to zero.

# CSMA/CA, CA:Collision Avoidance



# CSMA/CA/ACK, ACK:Acknowledgement

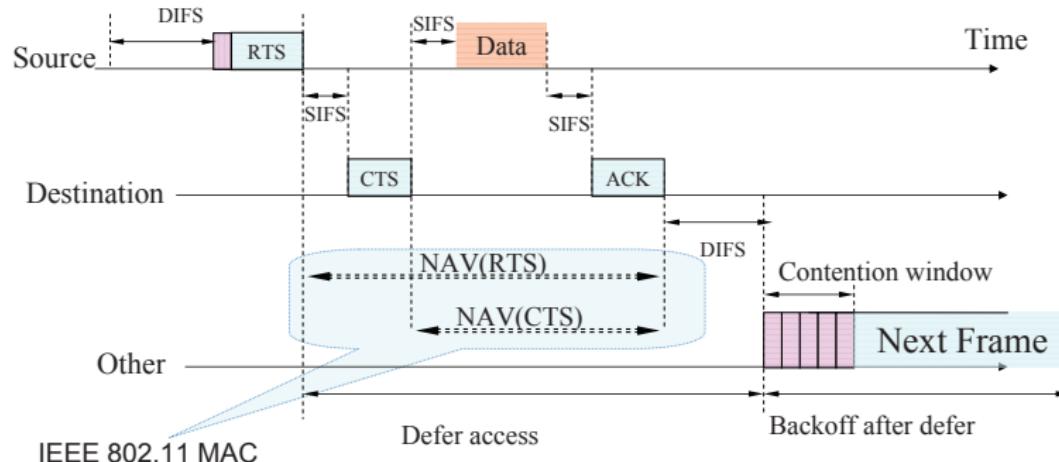
Immediate Acknowledgements from receiver upon reception of data frame without any need for sensing the medium, SIFS ; DIFS



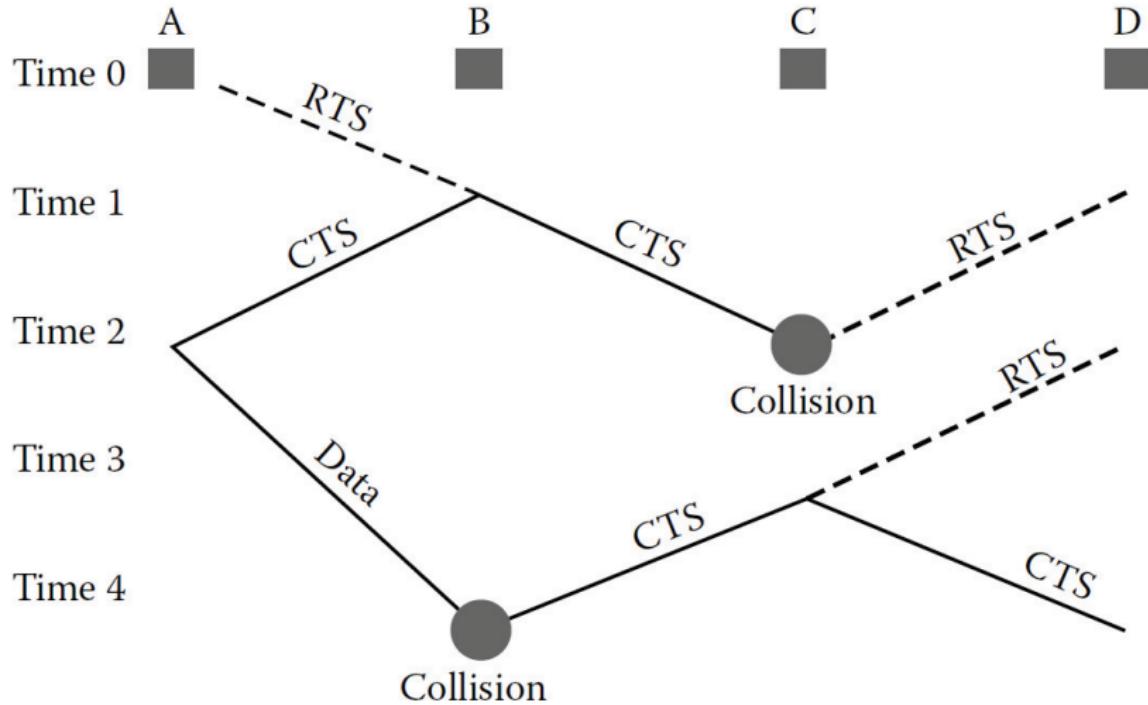
SIFS – Short Inter Frame Spacing

# CSMA/CA with Reservation, RTS&CTS

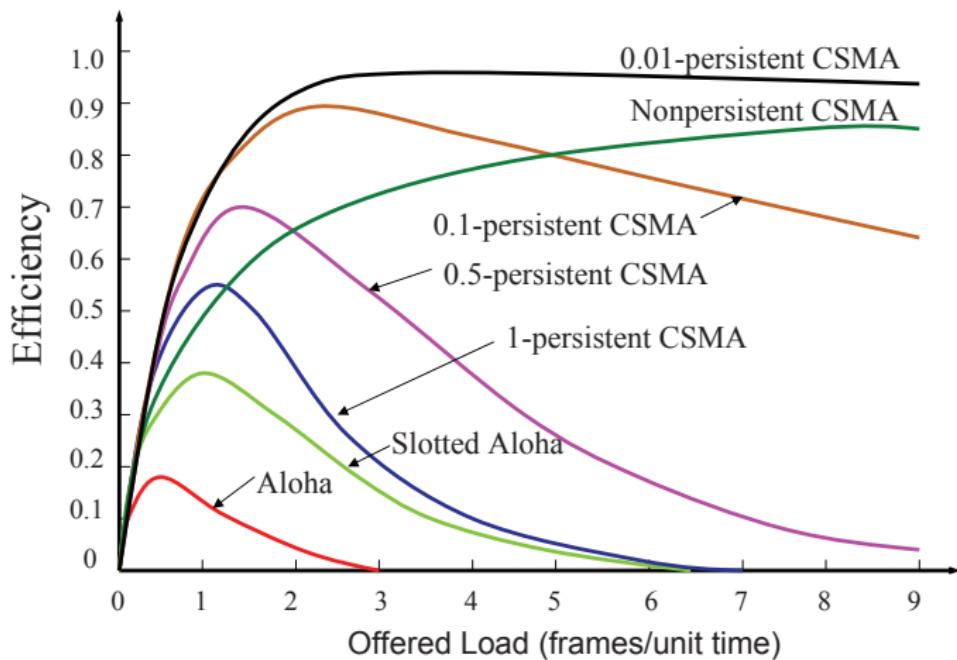
RTS/CTS is used for **reserving channel** for data transmission so that the collision can only occur in control message  
RTS (request to send), CTS (clear to send)  
NAV(Network allocation vector) for virtual sensing



# CSMA/CA with Reservation, RTS CTS Collisions



# Comparison of Random Access Protocols



## Lecture 6: Medium Access Control in Ad Hoc Networks

# Objectives

- to classify MAC protocols for ad hoc networks [1]
- to compare applicability of various MAC protocols in ad hoc networks

# Agenda

- 36 MAC Issues in Ad Hoc Networks
- 37 Contention-based protocols
- 38 Contention-based protocols with reservation mechanisms
- 39 Contention-based protocols with scheduling
- 40 MAC Protocols with Directional Antennas
- 41 Multi-channel MAC Protocols
- 42 Power Control MAC Protocol

# Can we apply conventional MAC?

- ISM Band: free license, crowded
- Share a common broadcast radio channel
- Limited bandwidth compared to wired networks: **precious resource**
- Wireless is more error prone
- Capacity (random variable) can be influenced by: fading, noise, interference
- Mobility and topology changes impact routing
- Are the links bidirectional?
- Power constraints? **another precious resource**
- Security: eavesdropping is easy over wireless
- Collisions happen at the receiver: Senders may not detect collisions
- Hidden/exposed terminals
- Signal strength decays exponentially with distance

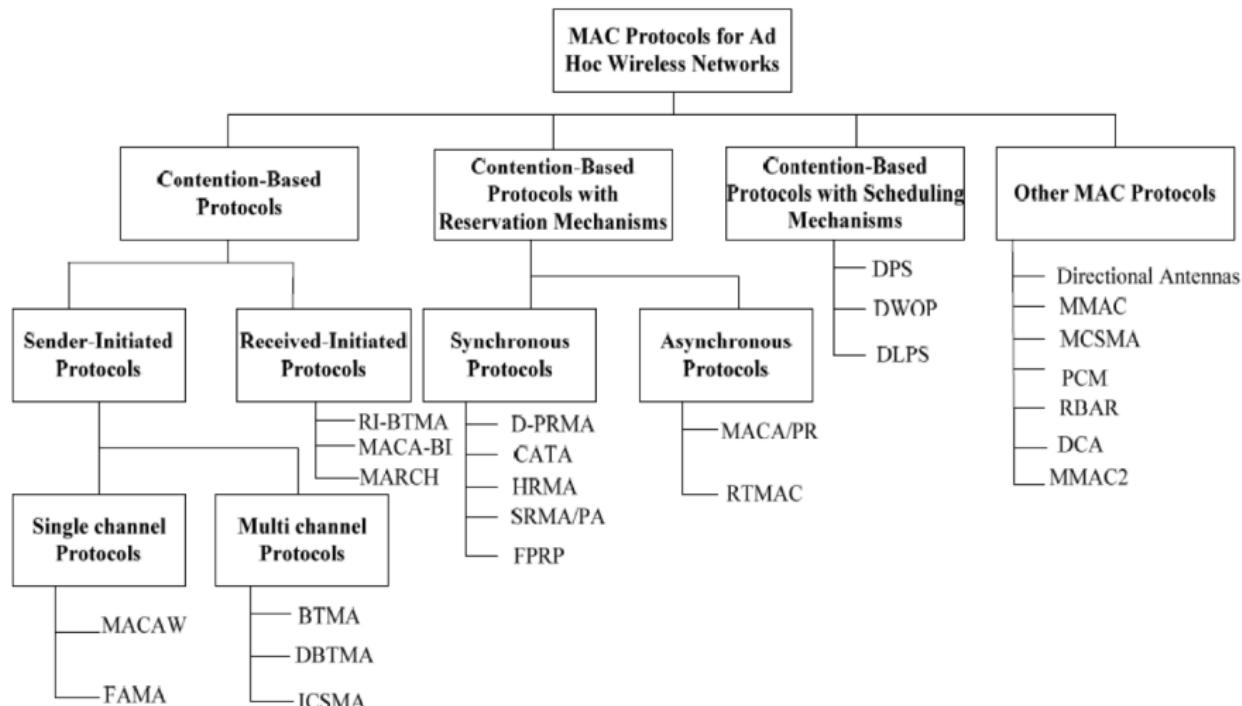
# Design Issues

- Maximize **bandwidth efficiency**: the ratio of the bandwidth used for actual data transmission to the total available bandwidth
  - Scarcity of resources (**spectrum**)
- Quality of service support
  - Time-critical communication, resource reservation mechanism
  - Bandwidth reservation is difficult in dynamic topologies
- Synchronization for reservation
- Hidden and Exposed Terminal Problems
- Error-Prone Shared Broadcast Channel
- Distributed Nature, Lack of Central Coordination
- Mobility of Nodes

# Design Goals

- Should be distributed
- Provide QoS support for real-time traffic
- Low **access delay**: the average delay experienced by any packet to get transmitted
- Bandwidth ( $B$ ) efficiently used
- Fair allocation of  $B$  to nodes
- Minimize the effects of hidden and exposed terminal problems
- Low control overhead
- Scalable to large networks
- Support power control and time synchronization
- Adaptive data rate control
- Exploit directional antennas (reduced interference, increased spectrum utilization, reduced power consumption)

# Classification I



# Classification II

- Contention-based protocols
  - **Fight for channel**
  - A node does not make any resource reservation *a priori*
  - Contend with neighbors for access
  - It cannot provide QoS guarantee
  - Two types of random access:
    - ▶ Sender-initiated protocols, single-channel or multi-channel,
    - ▶ Receiver-initiated protocols
- Contention-based protocols with reservation mechanisms
  - **Fight for reservation**
  - Support real-time traffic
  - Reserve bandwidth *a priori*
  - Synchronous protocols: global time synchronization is difficult to achieve
  - Asynchronous protocols: not require global synchronization
- Contention-based protocols with scheduling
  - **Fight for schedule**
  - Packet scheduling at nodes and
  - Scheduling nodes for access to the channel

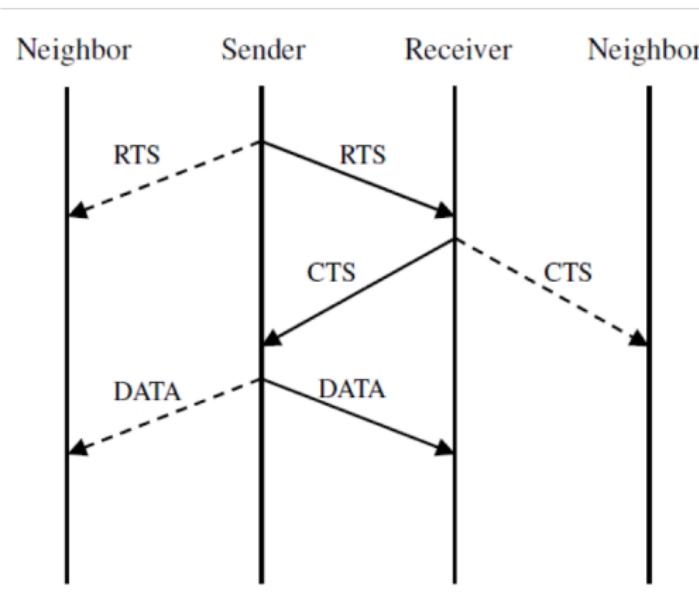
# Agenda

- 36 MAC Issues in Ad Hoc Networks
- 37 **Contention-based protocols**
- 38 Contention-based protocols with reservation mechanisms
- 39 Contention-based protocols with scheduling
- 40 MAC Protocols with Directional Antennas
- 41 Multi-channel MAC Protocols
- 42 Power Control MAC Protocol

# Multiple Access Collision Avoidance Protocol (MACA) I

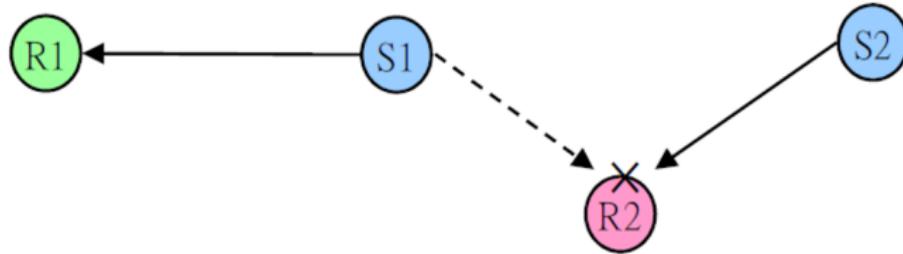
- Multiple access collision avoidance protocol proposed by Karn in 1990
- MACA does not make use of carrier-sensing: Similar to ALOHA
- Request-to-send (RTS), clear-to-send (CTS), DATA messages
- **Duration of an RTS** must be at least twice the maximum channel propagation delay.
- Use binary exponential back-off (BEB) algorithm for retry
- Both the RTS and CTS packets carry the expected duration of the data packet transmission
- A node near the receiver (overcome hidden node problem)
  - Hearing the CTS packet, defers its transmission till the receiver receives the data packet
- A node near the sender (overcome exposed node problem)
  - A node that only hears the RTS is free to transmit simultaneously when the sender is transmitting data

# Multiple Access Collision Avoidance Protocol (MACA) II



# A Media Access Protocol for WLANs (MACAW) I

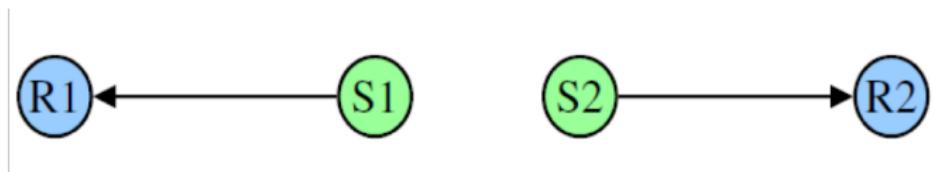
- Back-off mechanism used in MACA starves flows
- Back-off algorithm has been modified by Bharghavan in 1994 [12]
  - Packet header has an additional field carrying the current back-off counter value of the transmitting node
  - A node receiving the packet copies this value into its own back-off counter



# A Media Access Protocol for WLANs (MACAW) II

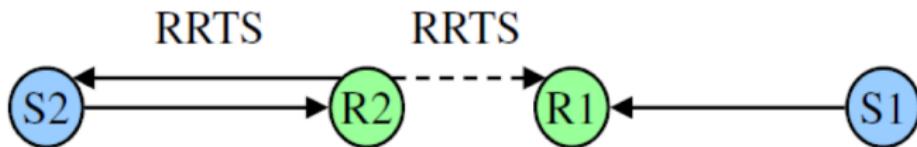
- To prevent large variations in the back-off values
  - Multiplicative increase and linear decrease (MILD)
    - ▶ Collision: back-off is increased by a multiplicative factor (1.5)
    - ▶ Successful: back-off is decreased by one
    - ▶ Less contention and larger throughput
- Implement per flow fairness
  - Multiple queues at every node (running backoff algorithm independently)
- An extra control packet ACK
  - If ACK is not received by sender, the sender would retry by transmitting an RTS for the same packet
  - The back-off counter is incremented
  - The receiver, instead of sending back a CTS, sends an ACK for the packet received

# A Media Access Protocol for WLANs (MACAW) III



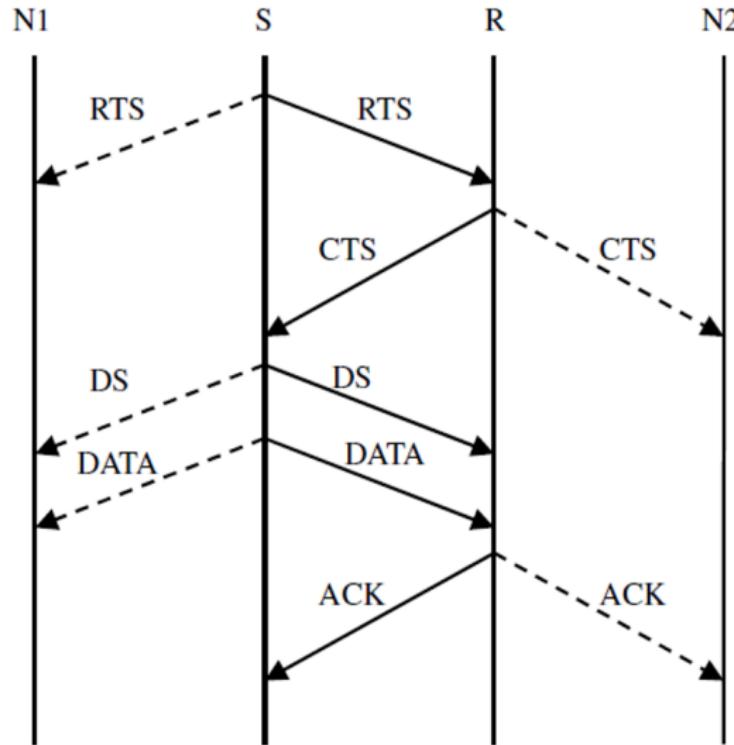
- Exposed node problem
  - MACA seems to solve exposed terminal: not really
  - S2 does not know if RTS/CTS between S1 and R1 is successful
  - Solution: data-sending (DS) packet
  - Before transmitting the data packet, the source node transmits the data-sending (DS) packet to ensure RTS-CTS exchange successful

# A Media Access Protocol for WLANs (MACAW) IV

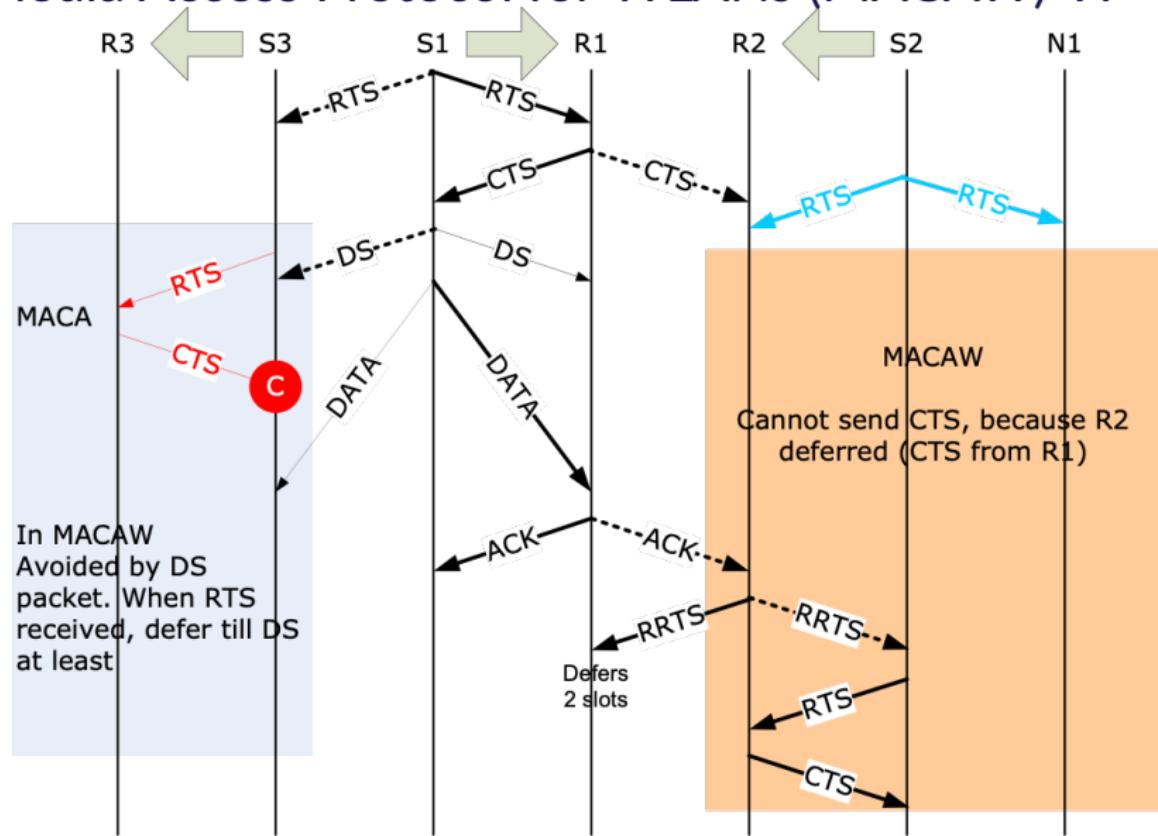


- Another control packet: request for request to send (RRTS)
  - Synchronization information needs to be propagated to the concerned nodes
  - If a node had received an RTS previously for which it was not able to respond because there exists on-going transmission, then it waits for the next contention period and transmits RRTS

# A Media Access Protocol for WLANs (MACAW) V



# A Media Access Protocol for WLANs (MACAW) VI



# MACA versus MACAW

- CSMA: collision happens at the receiver, therefore RTS/CTS/DATA becomes necessary, → MACA
- MACA: Solves hidden and exposed terminal (take with discount)
- MACA
  - lets tx failures corrected by transport layer,
  - exposed terminals can send, but CTS will collide
- MACAW corrects tx failures in datalink layer
- MACAW introduces DS and RRTS
- Cooperation
  - Through RRTS
  - By copying contention window size in headers

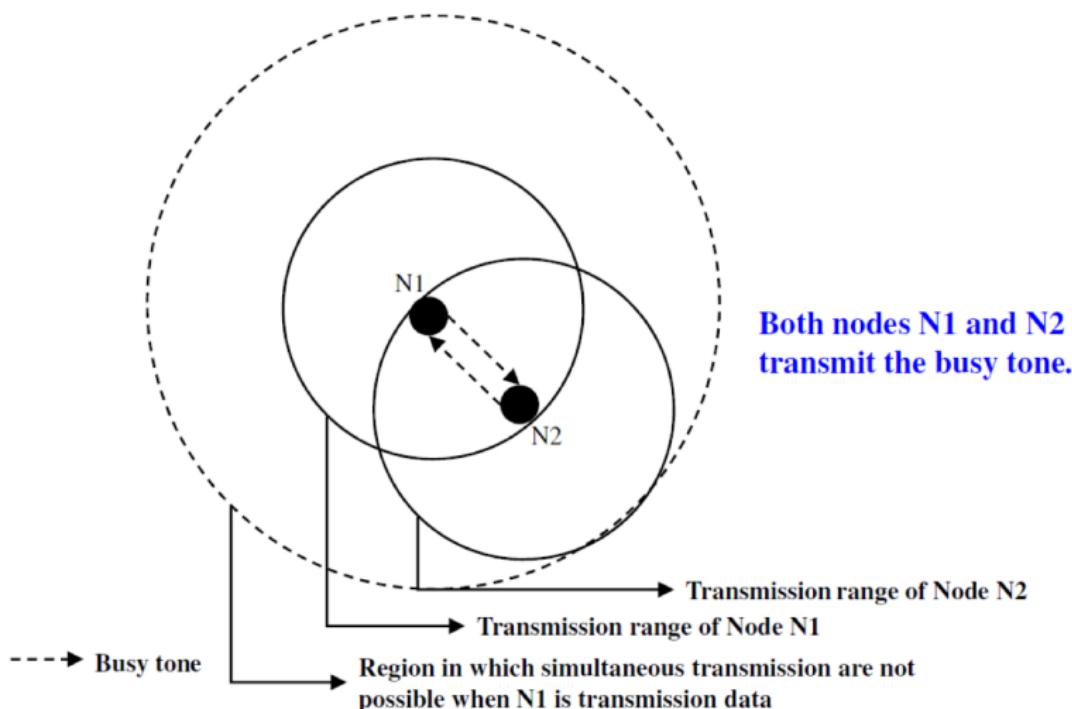
# FAMA: Floor Acquisition MAC [13]

- Before transmitting get the floor (gain control of channel)
- Based on a channel access discipline which consists of a carrier-sensing operation and a collision-avoidance dialog between the sender and the intended receiver of a packet.
- MACA is a FAMA type (already discussed)
- FAMA-NTR: FAMA w/ Non-persistent Transmit Request
  - Before sending a packet, the sender senses the channel
  - If channel is busy, the sender back-off a random time and retries later
  - If the channel is free, the sender sends RTS and waits for a CTS packet
  - If the sender cannot receive a CTS, it takes a random back-off and retries later
  - If the sender receives a CTS, it can start transmission data packet
  - To allow the sender to send a burst of packets, the receiver is made to wait a time duration  $\tau$  seconds after a packet is received

# Busy Tone Multiple Access Protocols (BTMA) I

- The transmission channel is split into:
  - Data packet transmissions: a data channel
  - Busy tone signal: a control channel
- When a node is ready for transmission, it senses the channel to check whether the busy tone is active
  - If not, it turns on busy tone signal and starts data transmission
  - Otherwise, it reschedules the packet for transmission after some random rescheduling delay.
- Any node that senses the carrier on the data channel, transmits busy tone on the control channel
- When a node is transmitting, no other node in the two-hop neighborhood of the transmitting node is permitted to simultaneously transmit

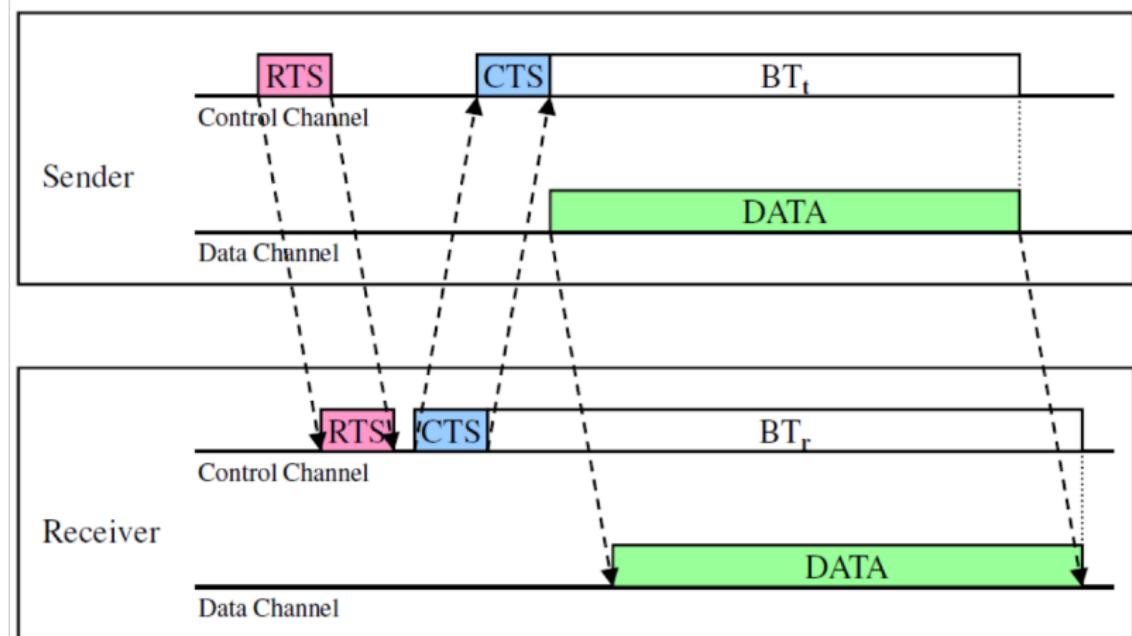
# Busy Tone Multiple Access Protocols (BTMA) II



# DBTMA: Dual Busy-tone MAC [14] I

- The transmission channel is divided into:
  - The data channel, data packet transmission
  - The control channel, RTS, CTS, busy tones
- Use two busy tones on the control channel,  $BT_t$  and  $BT_r$ :
  - $BT_t$ : indicate that it is transmitting on the data channel
  - $BT_r$ : indicate that it is receiving on the data channel
  - Two busy tone signals are two sine waves at different frequencies
- When a node is ready to transmit a data packet
  - First sense the channel to determine whether the  $BT_r$  signal is active
    - ▶  $BT_r$  signal → a neighbor is receiving packets
    - ▶ No  $BT_r$  signal → transmit RTS packet
  - Upon RTS packet (destined node), checks whether the  $BT_t$  tone is active
    - ▶  $BT_t$  signal → a neighbor transmits packets
    - ▶ No  $BT_t$  signal → Sending CTS packet and turn on the  $BT_r$  signal
  - Sender: receive CTS → turn on  $BT_t$  → start data → turn off  $BT_t$
  - Receiver: receive data turn off  $BT_r$  signal
- DBTMA has better network utilization than MACA(W) (why?)

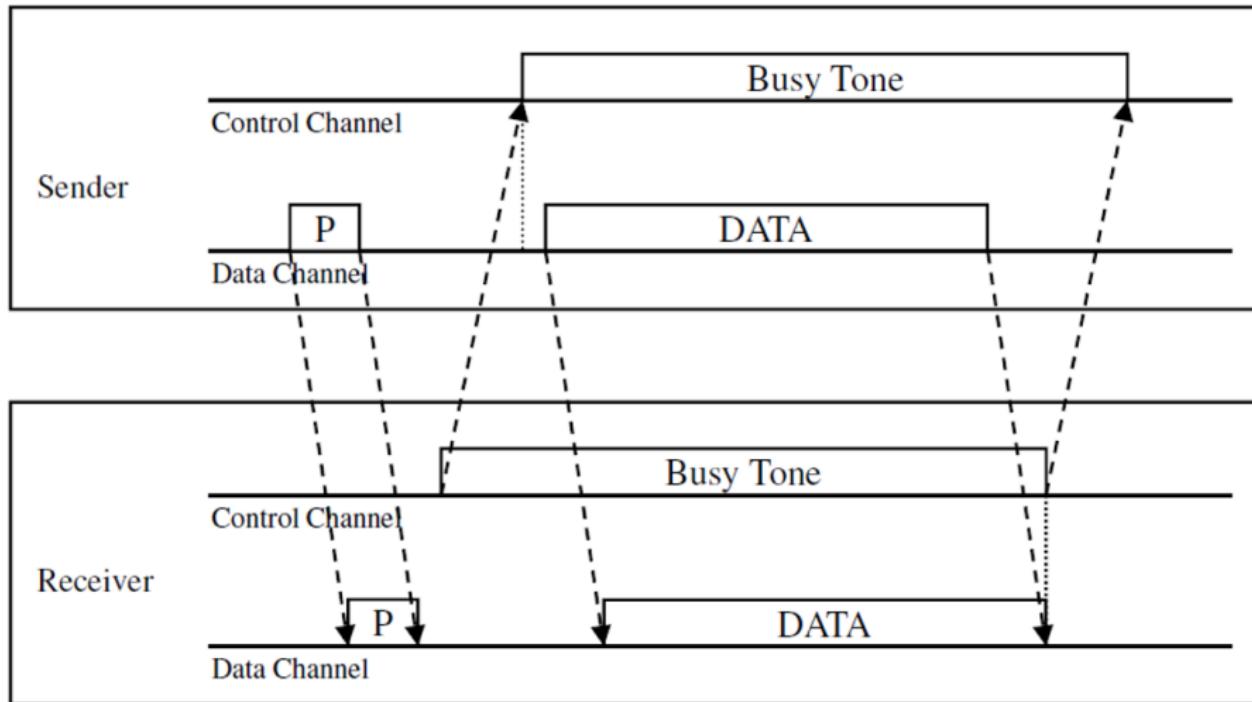
## DBTMA: Dual Busy-tone MAC [14] II



# RI-BTMA: Receiver-Initiated Busy Tone MAC I

- The available bandwidth is divided into two slotted channels:
  - The data channel: data packet transmission
    - ▶ Only if it finds the busy tone to be absent on the control channel
  - The control channel: busy tone signal
- Data packet: a **preamble** and the actual data packet
- The busy tone serves two purposes:
  - Ack the sender the successful reception of preamble
  - Inform the nearby hidden nodes about the impending transmission
- **The basic protocol**
  - No backlog buffers packets that suffer collisions cannot be retransmitted
- **The controlled protocol**
  - Backlogged mode → backlog buffer is non-empty
  - Backlog buffers: transmitting a backlogged packet in the next idle slot with a probability  $q$
  - Non-backlogged mode transmitting a non-backlogged packet in the next idle slot with a probability  $p$

# RI-BTMA: Receiver-Initiated Busy Tone MAC II

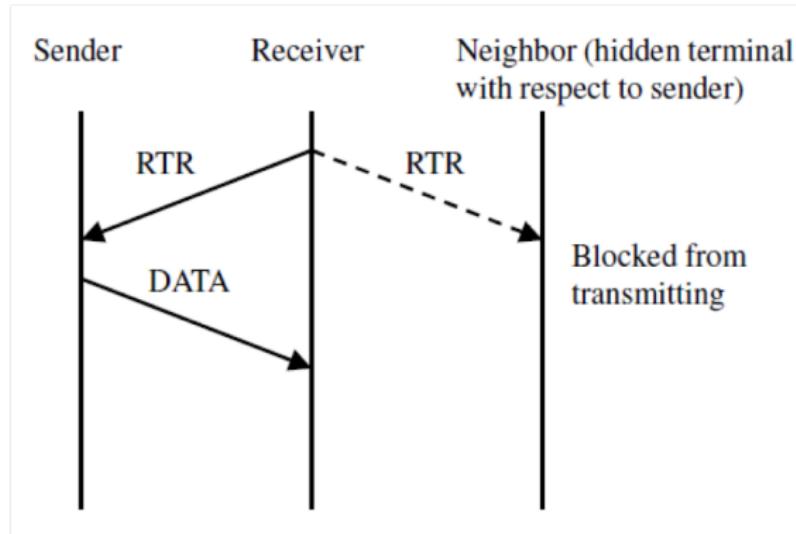


**P** Preamble Packet

# MACA-BI: MACA by Invitation I

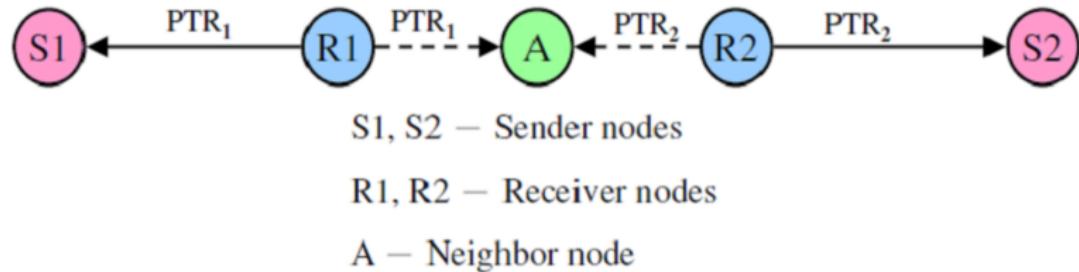
- MACA-BI is a receiver-initiated MAC protocol
  - Receiver sends ready to receive (RTR)
  - Sender responds by sending a DATA packet
- Receiver estimates the average arrival rate of packets
- Problems:
  - Receiver may not have an exact knowledge about the traffic rates
  - The protocol allowing the sender to declare its backlog through the RTS control packet, if an RTR packet is not arrived within a given timeout
  - Hidden terminal problem is overcome in MACA-BI
  - However, the hidden terminal problem still affects the control packet transmission
    - ▶ RTR packets can collide with DATA packets

# MACA-BI: MACA by Invitation II



# MACA-BI: MACA by Invitation III

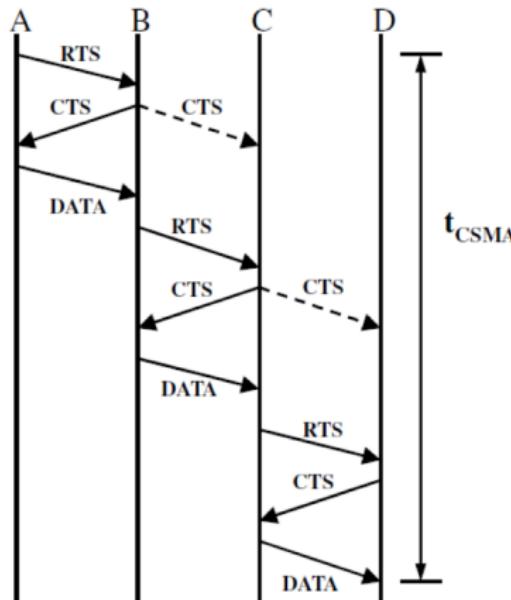
## Hidden terminal problem in MACA-BI



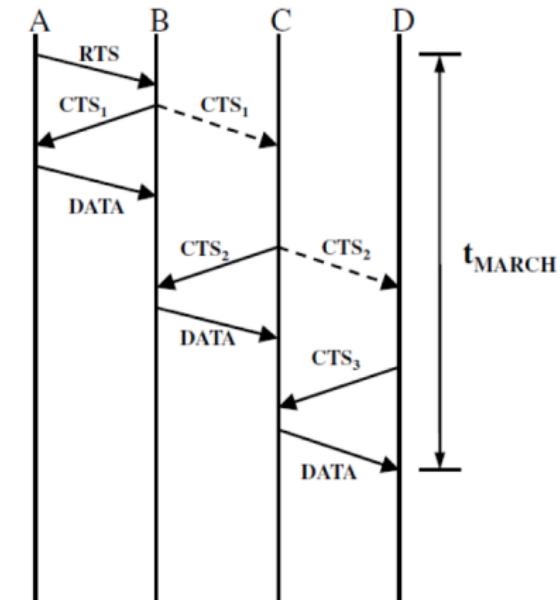
# Media Access with Reduced Handshake (MARCH) I

- MARCH does not require any traffic prediction mechanism
- The RTS packet is used only for the first packet of the stream
  - MACA: RTS → CTS → DATA → RTS → CTS. . .
  - MARCH: RTS → CTS1 → DATA → CTS2 → DATA ...
- The CTS packet: MAC address of the sender, receiver, and the route identification number (RTid )
- The throughput of MARCH is significantly high when compared to MACA, while the control overhead is much less

# Media Access with Reduced Handshake (MARCH) II



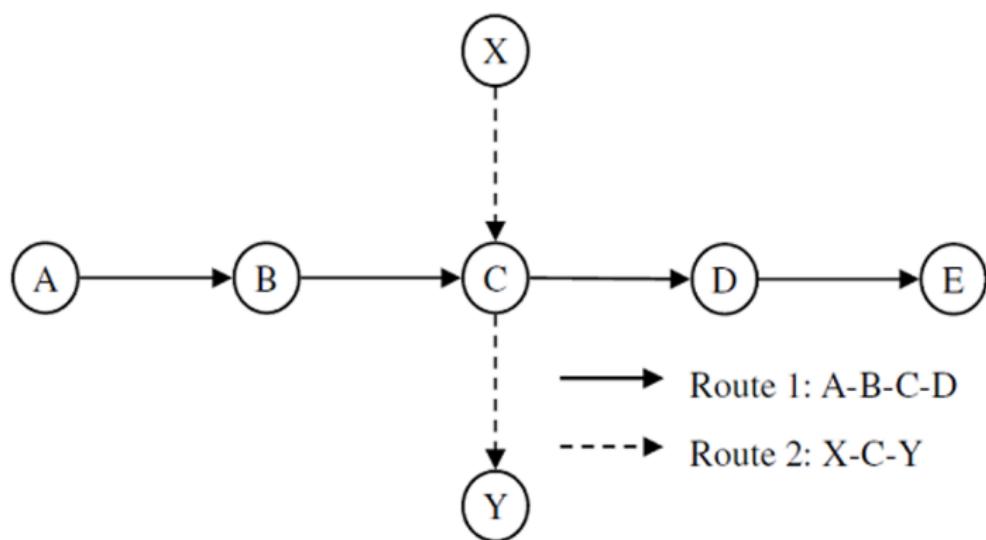
CSMA



MARCH

# Media Access with Reduced Handshake (MARCH) III

- The  $RT_{id}$  avoids misinterpretation of CTS packets and initiation of false CTS-only handshake
- For example, when node Y received a CTS with  $RT_{id}$  = route 1, it does not respond



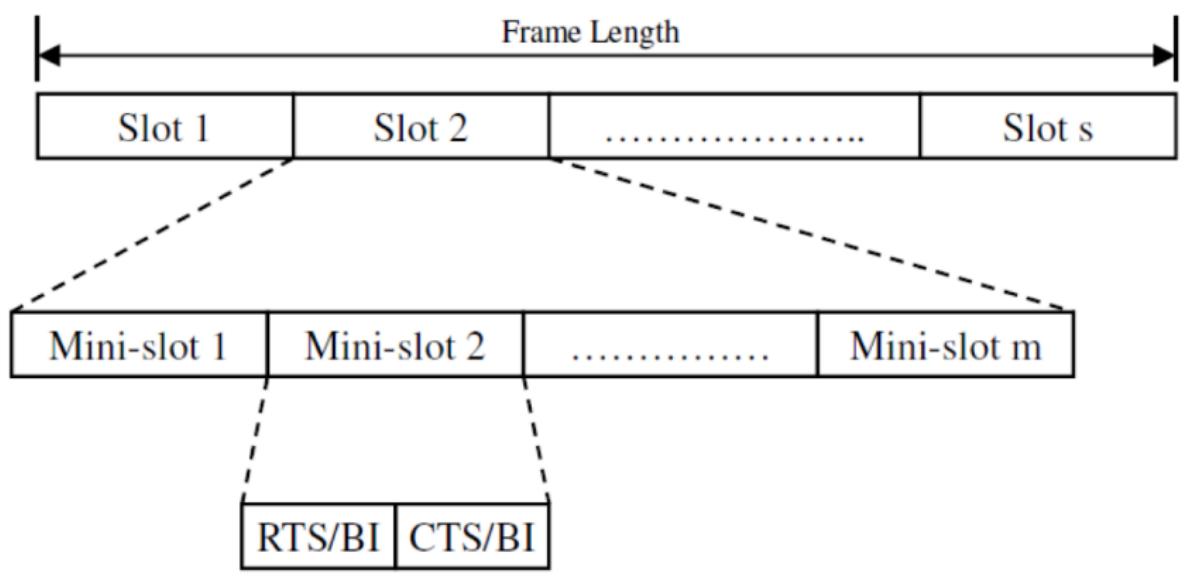
# Agenda

- 36 MAC Issues in Ad Hoc Networks
- 37 Contention-based protocols
- 38 Contention-based protocols with reservation mechanisms**
- 39 Contention-based protocols with scheduling
- 40 MAC Protocols with Directional Antennas
- 41 Multi-channel MAC Protocols
- 42 Power Control MAC Protocol

# D-PRMA: Distributed Packet Reservation Multiple Access Protocol I

- The channel is divided into fixed and equal sized frames along the time axis.
- The RTS/BI and CTS/BI are used for slot reservation and for overcoming the hidden terminal problem
- If a terminal wins the contention through mini-slot 1, the extra  $(m - 1)$  mini-slots of this slot will be granted to the terminal as the payload
- For voice node, the same slot in each subsequent frame can be reserved until the end of its packet transmission
- In the other cases, the extra  $(m - 1)$  mini-slots are continuously used for contention, and the winner of this contention will be granted the reservation of the same slot

# D-PRMA: Distributed Packet Reservation Multiple Access Protocol II



# D-PRMA: Distributed Packet Reservation Multiple Access Protocol III

- To prioritize voice terminals over data terminals
  - Voice terminals starts contenting from mini-slot 1 with probability  $p = 1$  while data terminals can start such content with  $p < 1$
  - Both voice and data terminals can content through the extra  $(m - 1)$  mini-slots with probability  $p < 1$
  - Only the winner of a voice terminal can reserve the same slot in each subsequent frame until the end of packet transmission while the winner of a data terminal can only use one slot
- Problem: When a terminal wins the contention in mini-slot 1, how to prevent other terminals in the same slot for contention ? (Use RTS/CTS)
- Problem: How to prevent a terminal from contending for a reserved slot in each subsequent slot ? (Transmit a busy indication (BI) signal RTS/BI (receiver) (why?) and CTS/BI (sender) in mini-slot 1)

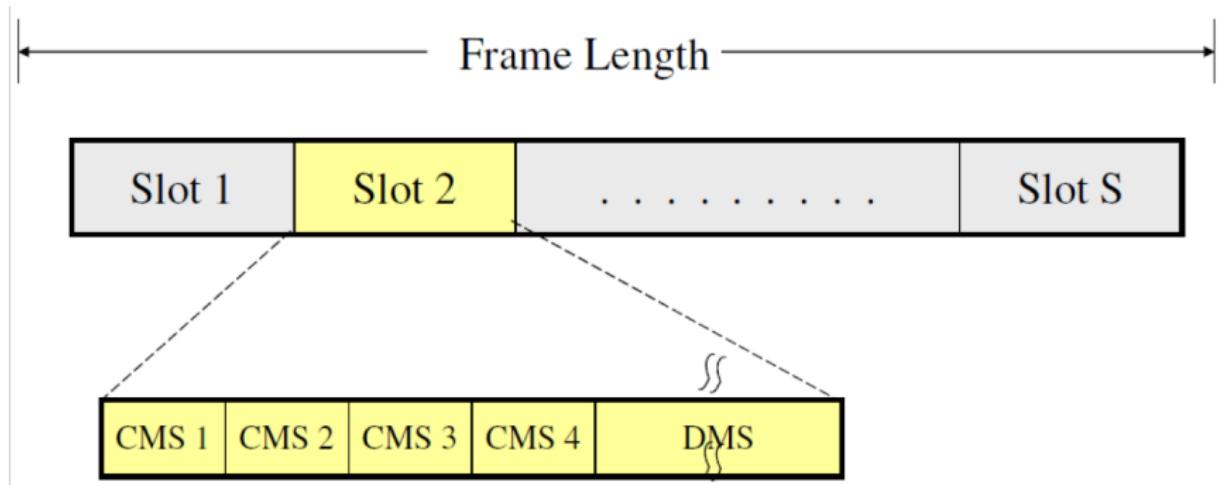
# CATA: Collision Avoidance Time Allocation Protocol I

- Support broadcast, unicast, and multicast transmissions simultaneously
- Each frame consists of S slots and each slot is further divided into five mini-slots
  - CMS1: Slot Reservation (SR)
  - CMS2: RTS
  - CMS3: CTS
  - CMS4: not to send (NTS)
  - DMS: Data transmission
- Each node receives data during the DMS of current slot transmits an SR in CMS1
- Every node that transmits data during the DMS of current slot transmits an RTS in CMS2
- CMS3 and CMS4 are used as follows:
  - The sender of an intended reservation, if it senses the channel is idle in CMS1, transmits an RTS in CMS2
  - Then the receiver transmits a CTS in CMS3

# CATA: Collision Avoidance Time Allocation Protocol II

- If the reservation was successful the data can transmit I current slot and the same slot in subsequent frames
- Once the reservation was successfully, in the next slot both the sender and receiver do not transmit anything during CMS3 and during CMS4 the sender transmits a NTS
- If a node receives an RTS for broadcast or multicast during CMS2 or it finds the channel to be free during CMS2, it remains idle during CMS3 and CMS4
- Otherwise it sends a NTS packet during CMS4
- A potential multicast or broadcast source node that receives the NTS packet or detecting noise during CMS4, understands that its reservation is failed
- If it find the channel is free in CMS4, which implies its reservation was successful CATA works well with simple single-channel half-duplex radios

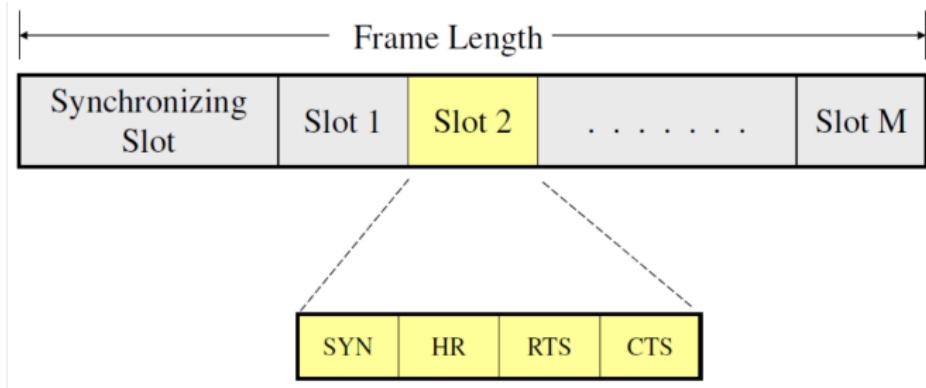
# CATA: Collision Avoidance Time Allocation Protocol III



# HRMA: Hop Reservation Multiple Access Protocol I

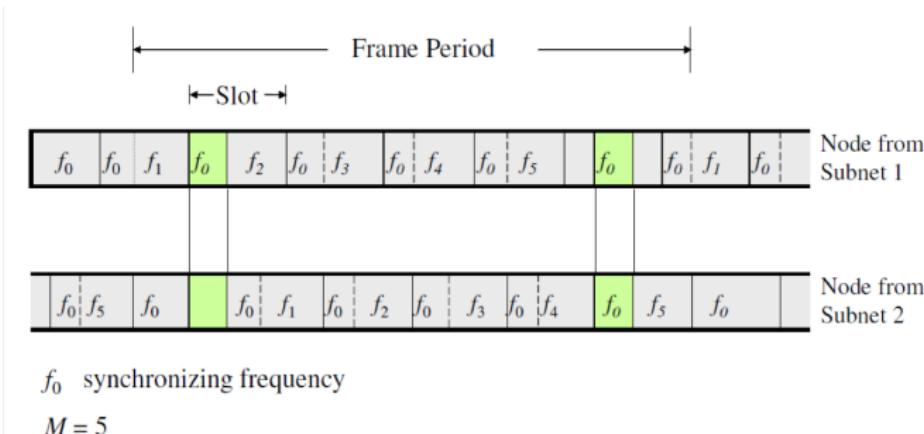
- HRMA is a multi-channel MAC protocol, based on halfduplex very slow frequency hopping spread spectrum (FHSS) radios
- Each time slot is assigned a separate frequency channel ( 1)
- Assumptions
  - $L$ : frequency channels
  - $f_0$ : dedicated synchronized channel frequency
  - The remaining  $L - 1$  frequencies are divided into frequency pairs denoted by  $(f_i, f_i^*), i = 1, 2, \dots, M$
  - Hop reservation (HR), RTS, CTS, DATA :  $f_i$
  - ACK:  $f_i^*$

# HRMA: Hop Reservation Multiple Access Protocol II



- All idle nodes hop to the synchronizing frequency  $f_0$  and exchange synchronization information
- Synchronizing slot: used to identify the beginning of a frequency hop and the frequency to be used in the immediately following hop
- Any two nodes from two disconnected networks have at least two overlapping time period of length  $\mu_s$  on the frequency  $f_0$

# HRMA: Hop Reservation Multiple Access Protocol III



- $\mu$  is the length of each slot
- $\mu_s$  is the length of the synchronization period on each slot, then the dwell time of  $f_0$  is  $\mu + \mu_s$

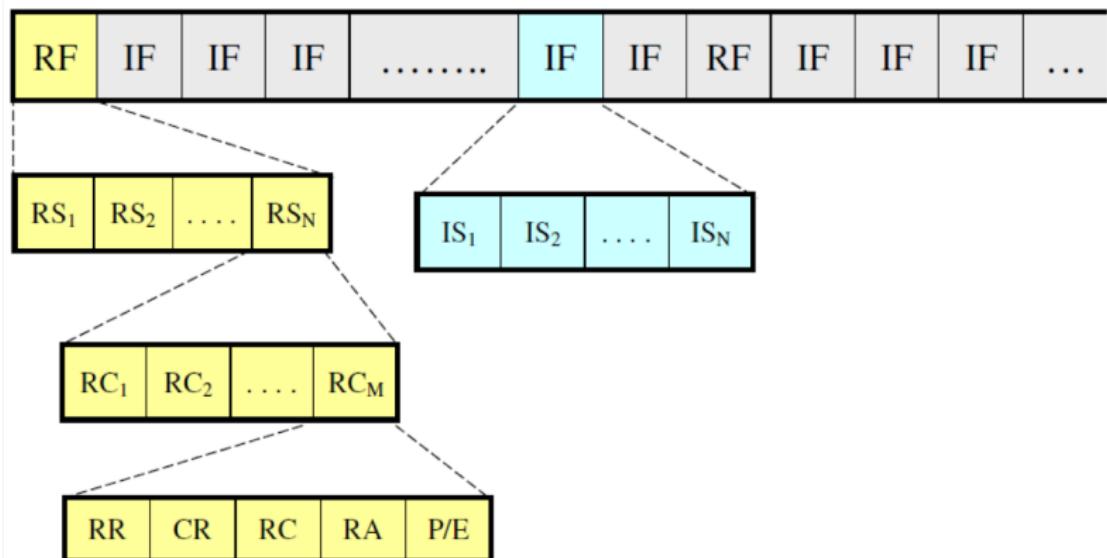
# HRMA: Hop Reservation Multiple Access Protocol IV

- A node ready to transmit data, it senses the HR period of the current slot
  - If the channel is idle during HR period, it transmits an RTS during RTS period and waits for CTS during CTS period
  - If the channel is busy during HR period, it backs off for a randomly multiple slots
- Suppose the sender needs to transmits data across multiple frames, it informs the receiver through the header of the data packet
  - The receiver node transmits an HR packet during the HR period of the same slot in next frame to informs its neighbors
  - The sender receiving the HR packet, it sends an RTS during the RTS period and jams other RTS packets
  - Both the sender and receiver remain silent during the CTS period

# FPRP: Five-Phase Reservation Protocol I

- FPRP is a single-channel TDMA-based broadcast scheduling protocol:
  - need global time synchronization
  - fully distributed and scalable
  - reservation process is localized; it involves only two-hop neighbors
- No hidden terminal problem
  - Time is divided into frames: reservation frame (RF) and information frame (IF)
  - Each RF has  $N$  reservation slots (RS) and each IF has  $N$  information slots (IS)
  - Each RS is composed of  $M$  reservation cycles (RCs)
  - With each RC, a five-phase dialog takes place
- Corresponding to IS, each node would be in one of the following three states: transmit (T), receive (R), and blocked (B)

# FPRP: Five-Phase Reservation Protocol II



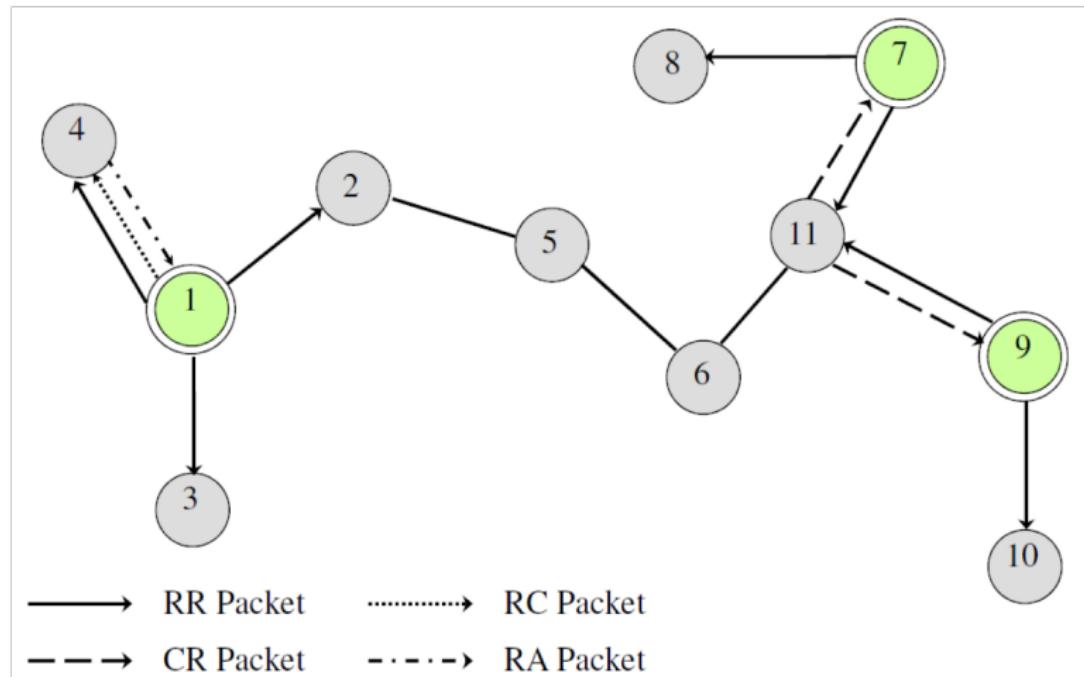
Five-phase reservation dialog

# FPRP: Five-Phase Reservation Protocol III

Five-phase protocol:

- Reservation request: send reservation request (RR) packet to dest.
- Collision report: if a collision is detected by any node, that node broadcasts a CR packet
- Reservation confirmation: a source node won the contention will send a RC packet to destination node if it does not receive any CR message in the previous phase
- Reservation acknowledgment: destination node acknowledge reception of RC by sending back RA message to source
- Packing and elimination: use packing packet and elimination packet

# FPRP: Five-Phase Reservation Protocol IV



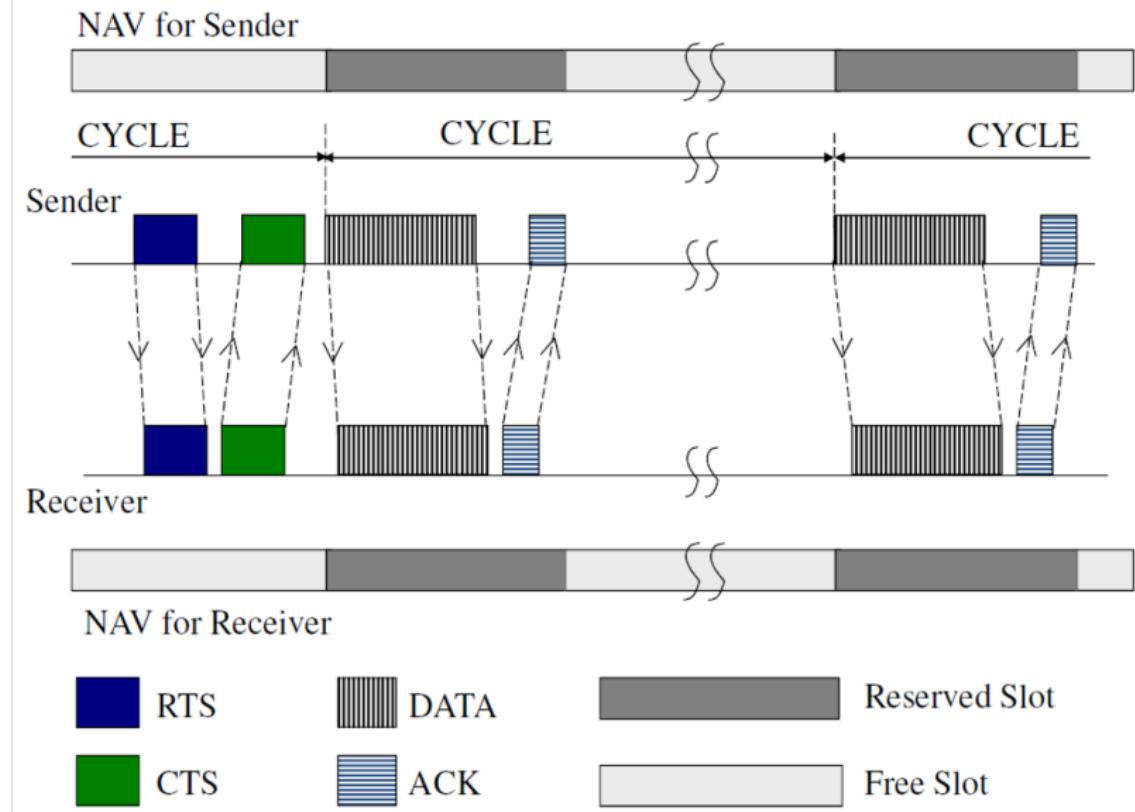
# MACA/PR: MACA with Piggy-Backed Reservation I

- MACA/PR is used to provide real time traffic support
- The main components: a MAC protocol (MACAW + non persistent CSMA), a reservation protocol, and a QoS routing protocol
- Each node maintains a reservation table (RT) that records all the reserved transmit and receive slots/windows of all nodes
- Non-real time packet: wait for a free slot in the RT + random time → RTS → CTS → DATA → ACK
- Real time packet:
  - Transmit real time packets at certain regular intervals (say CYCLE)
- RTS → CTS → DATA (carry reservation info for next data)  
ACK → ... → DATA (carry reservation info) → ACK
  - Hear DATA and ACK: update their reservation table
- The ACK packet serves to renew the reservation, in addition to recovering from the packet loss
  - Reservation fail: fail to receive ACK packets for a certain number of DATA packets

# MACA/PR: MACA with Piggy-Backed Reservation II

- For maintaining consistent information regarding free slots: Periodic exchange of reservation tables
- Best effort and real time packet transmissions can be interleaved at nodes
- When a new node joins: receive reservation tables from each of its neighbors and learns about the reservations made in the network
- QoS Routing protocol: DSDV (destination sequenced distance vector)
- MACA/PR does not require global synchronization among nodes
- Drawback: possibility of many fragmented free slots not being used at all

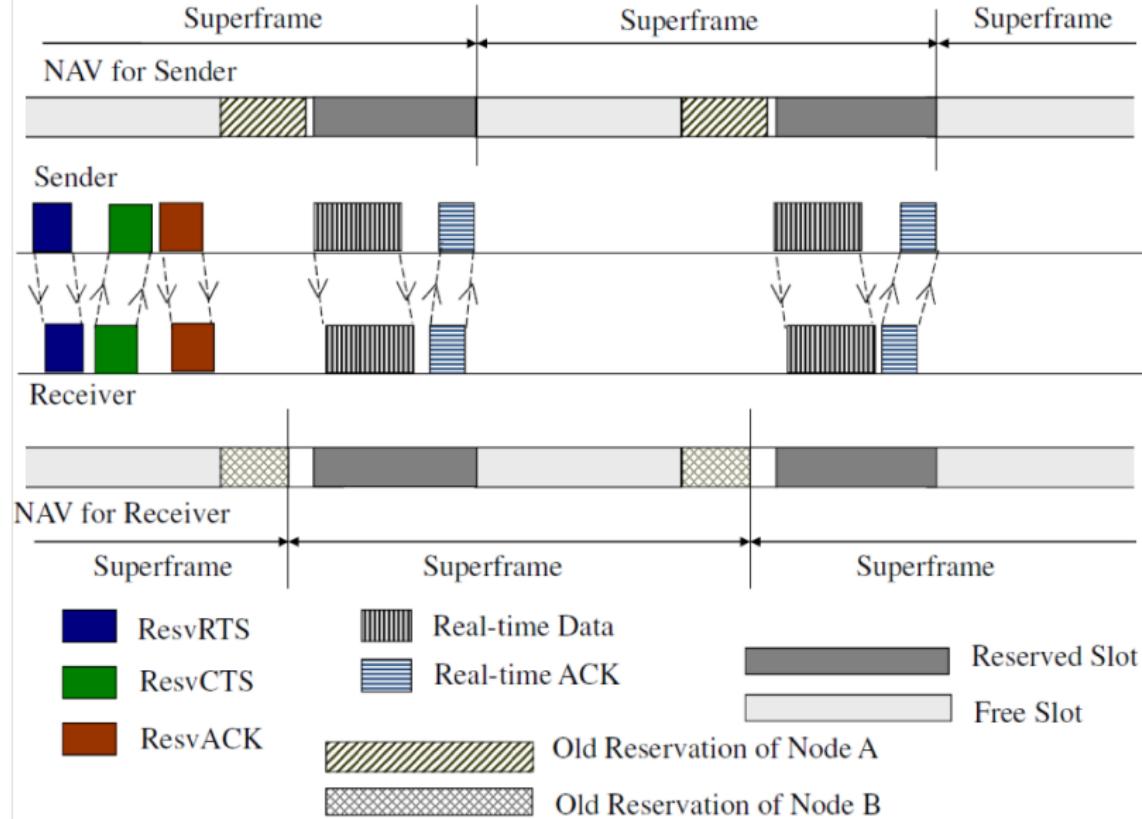
## MACA/PR: MACA with Piggy-Backed Reservation III



# RTMAC: Real Time Medium Access Control Protocol I

- The two components: MAC protocol and QoS routing protocol
- QoS routing: for end to end reservation + release of bandwidth
- MAC: medium access for best effort + reservation for real time
- Control packets
  - Real time : ResvRTS, ResvCTS, and ResvACK, half of DIFS
  - Best effort: RTS, CTS, and ACK
- The duration of each resv-slot is twice the maximum propagation delay
  - Transmit real time packets first reserves a set of resv-slots
  - The set of resv-slots for a connection is called a connection-slot
- The superframe for each node may not strictly align with the other nodes (use relative time for all reservation)

# RTMAC: Real Time Medium Access Control Protocol II



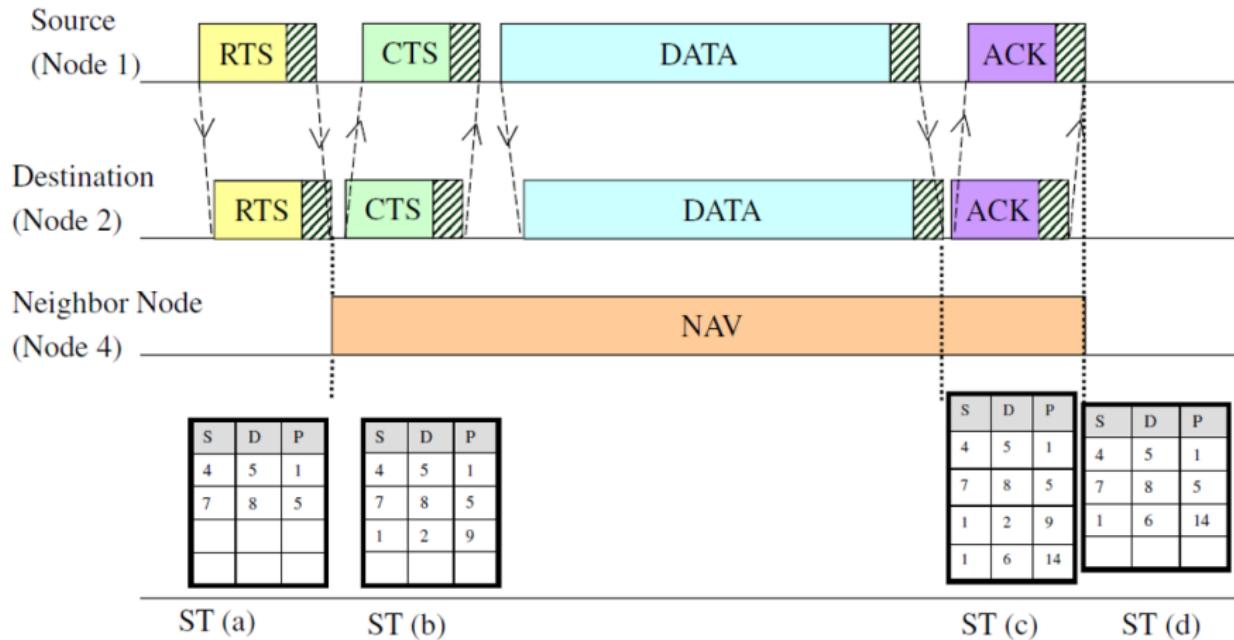
# Agenda

- 36 MAC Issues in Ad Hoc Networks
- 37 Contention-based protocols
- 38 Contention-based protocols with reservation mechanisms
- 39 Contention-based protocols with scheduling**
- 40 MAC Protocols with Directional Antennas
- 41 Multi-channel MAC Protocols
- 42 Power Control MAC Protocol

# DPS: Distributed Priority Scheduling and MAC I

- Provide differentiated QoS levels to different wireless applications in ad hoc networks
- Achievable by QoS-sensitive MAC and network layer scheduling
- Distributed scheduling problem with local information
- Basic mechanisms:
  - Piggyback information
  - Head-of-line (HoL) packet as the packet with the highest priority (lowest index)
  - RTS, CTS : carry current packet info
  - DATA, ACK: carry next head-of-line info

# DPS: Distributed Priority Scheduling and MAC II



Scheduling Table Updates at Neighbor Node 4

S – Source Id      D – Destination Id    P – Priority Index

Piggy-backed priority information

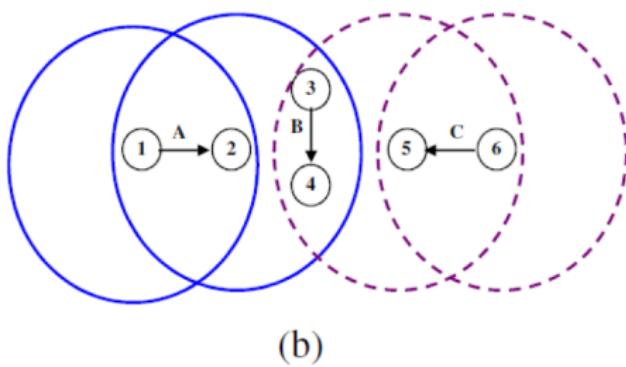
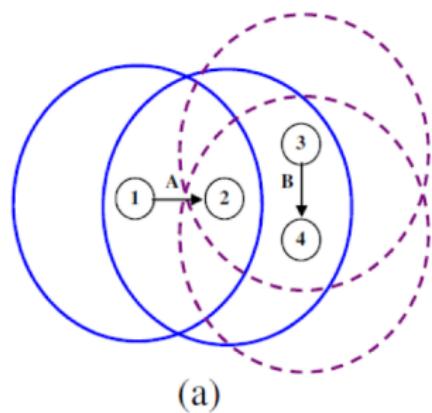
# DWOP: Distributed Wireless Ordering Protocol I

- DWOP based on the DSP, ensure that packet access the medium according to the order specified by an ideal reference schedule such as FIFO
- Each node builds up a scheduling table (ST) ordered according to the overheard arrival times
- A node is made eligible to contend for the channel only if its locally queued packet has a smaller arrival time compared to all other arrival times in its ST

# DWOP: Distributed Wireless Ordering Protocol II

- Scheduling problems: Information asymmetry and perceived collisions
- **Information asymmetry**: a transmitting node might not be aware of the arrival times of packets queued at another node which is not within its transmission range
- Solution: a receiver finds that the sender is transmitting out of order, an out-of-order notification is piggybacked by the receiver on the control packet (CTS/ACK)
- **Perceived collisions**: the ACK packet collides at the node, the corresponding entry in the ST will never be removed
- Solution: when a node observes that its rank remains fixed while packets whose PR are below the priority of its packet are being transmitted, it deletes the oldest entry from its ST

# DWOP: Distributed Wireless Ordering Protocol III



— Coverage region of flow A  
- - - Coverage region of flow B

— Coverage region of flow A  
- - - Coverage region of flow C

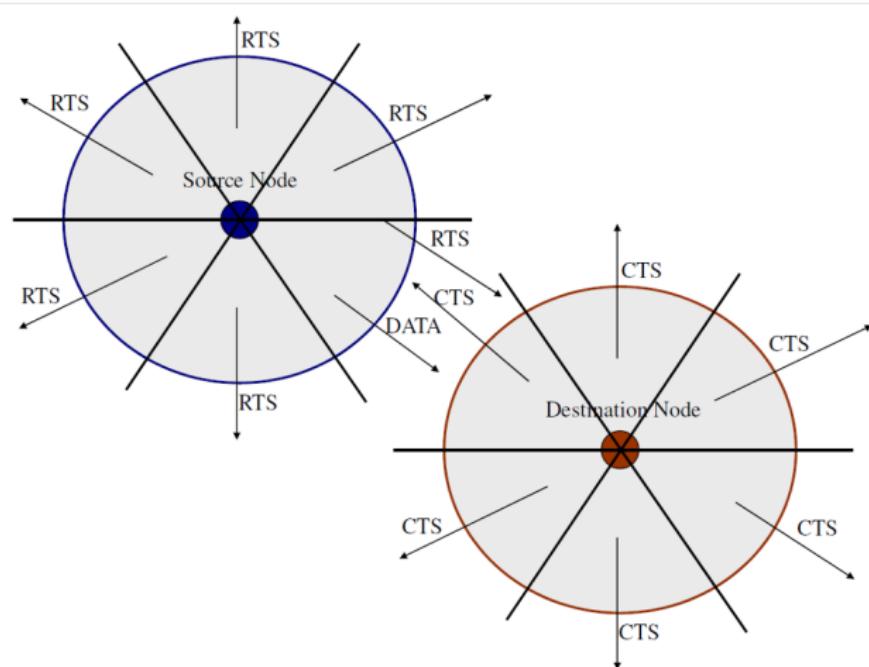
# Agenda

- 36 MAC Issues in Ad Hoc Networks
- 37 Contention-based protocols
- 38 Contention-based protocols with reservation mechanisms
- 39 Contention-based protocols with scheduling
- 40 MAC Protocols with Directional Antennas**
- 41 Multi-channel MAC Protocols
- 42 Power Control MAC Protocol

# MAC Protocols with Directional Antennas I

- Advantages
  - Reduced signal interference,
  - increased system throughput,
  - improved channel reuse
- Assumptions
  - Only one radio transceiver can transmit and receive only one packet at any given time
  - $M$  directional antennas, each antennas having a conical radiation pattern, spanning an angle of  $2\pi/M$  radians
  - Adjacent antennas never overlap
- If a node transmits when all its antennas are active, then the transmission's radiation pattern is similar to that of an omnidirectional antennas
- Packet transmission

# MAC Protocols with Directional Antennas II

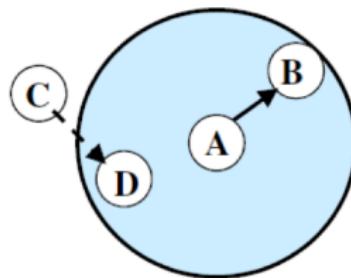


# DBTMA: Directional Busy Tone-Based MAC Protocol I

- Adapt the DBTMA protocol for use with directional antennas.
- Directional Antenna
  - $N$  antenna elements, a sector =  $360/N$
  - Unicast: only a single antenna element
  - Broadcast: all the antenna elements
- Protocol:
  - a) sender transmits RTS in all directions,
  - b) receiver sends back CTS to the sender with the direction of maximum power and turns on the BTr in the direction to the sender,
  - c) sender turns on the BTt in the direction of receiver and transmits data packet

This protocol is not guaranteed to be collision free

# DBTMA: Directional Busy Tone-Based MAC Protocol II

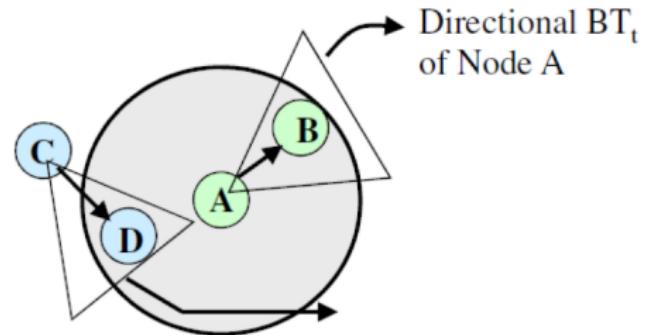


→ Active session

→ Request for transmission

■ Omnidirectional BT<sub>t</sub> of Node A

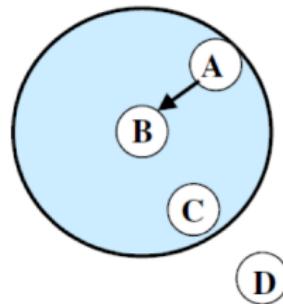
(a)



Directional transmission  
From Node C to Node D

(b)

# DBTMA: Directional Busy Tone-Based MAC Protocol III

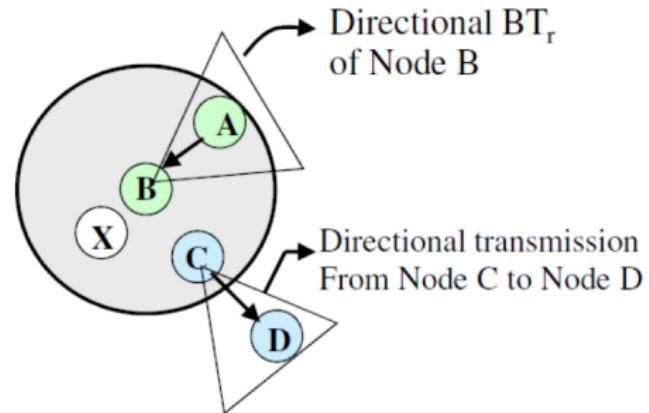


→ Active session



Omnidirectional BT<sub>r</sub> of Node B

(a)



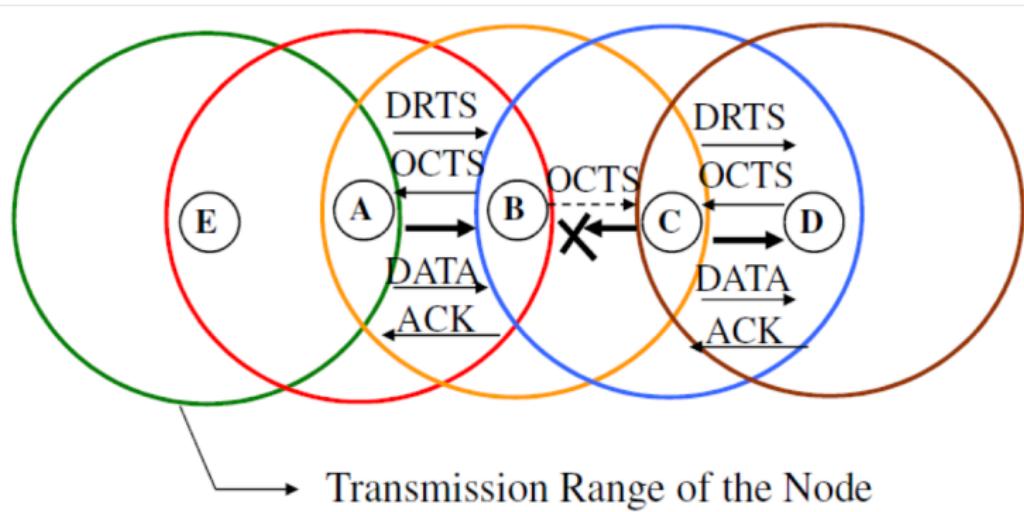
(b)

# D-MAC: Directional MAC Protocols I

- D-MAC: assume each node knows about the location of neighbors
- In the first directional MAC scheme (DMAC-1)
  - Directional RTS (DRTS) omni-directional CTS (OCTS) Directional DATA (DDATA) Directional ACK(DACK)
  - May increase the probability of control packet collisions
- In the second directional MAC scheme (DMAC-2)
  - Both the directional RTS (DRTS) and omni-directional RTS (ORTS) transmissions are used
  - Reduced control packet collisions
- Rules for using DRTS and ORTS:
  - ORTS: none of the directional antennas are blocked
  - DRTS : otherwise
  - Another packet called directional wait-to-send (DWTS) is used

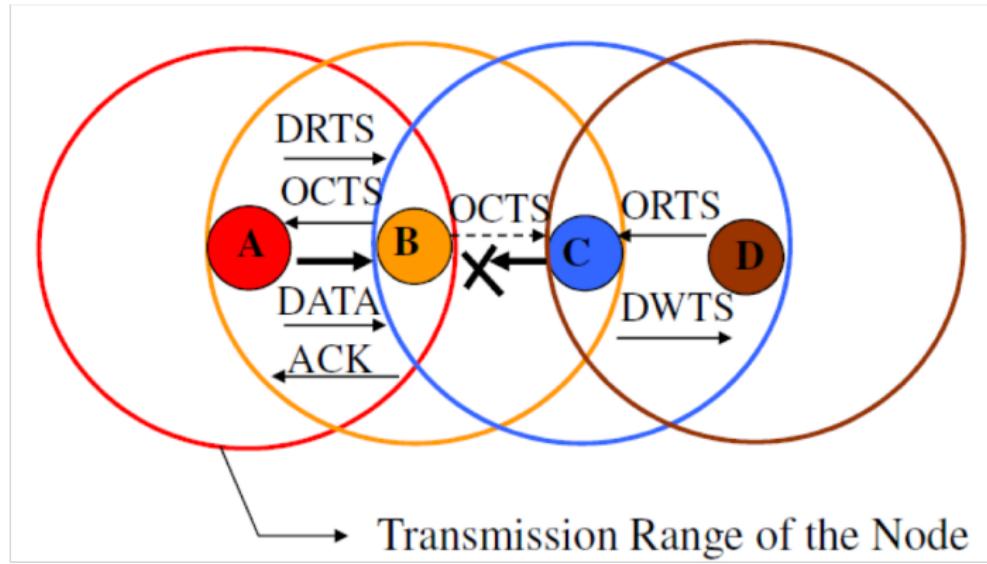
# D-MAC: Directional MAC Protocols II

If node E send a packet to node A, it will collide the OCTS or DACK



# D-MAC: Directional MAC Protocols III

- Control/Data Packet
- Data session
- Non-permissible session



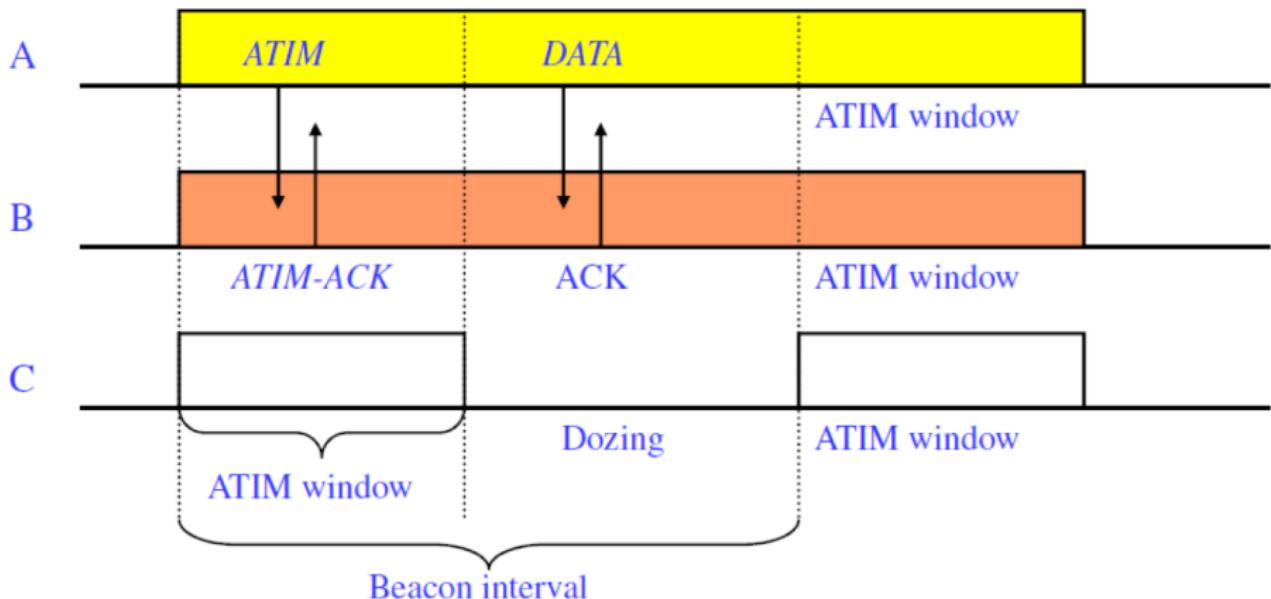
# Agenda

- 36 MAC Issues in Ad Hoc Networks
- 37 Contention-based protocols
- 38 Contention-based protocols with reservation mechanisms
- 39 Contention-based protocols with scheduling
- 40 MAC Protocols with Directional Antennas
- 41 Multi-channel MAC Protocols**
- 42 Power Control MAC Protocol

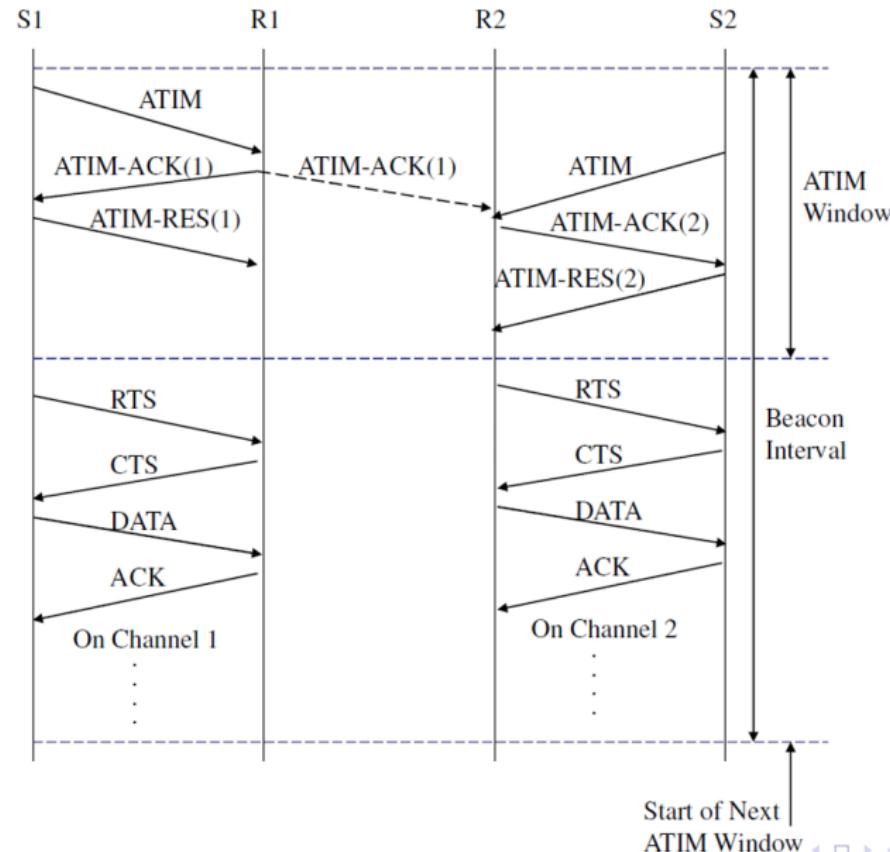
# MMAC: Multi-Channel MAC Protocol I

- Assumptions:
  - No dedicated control channel
  - N channels for data transmission
  - Each node maintains a data structure called PreferableChannelList (PCL)
- Three types for channels:
  - High preference channel (HIGH): the channel is selected by the current node and is used by the node
  - Medium preference channel (MID): a channel which is free and is not being currently used
  - Low preference channel (LOW): such a channel is already being used in the transmission range of the node by other neighboring nodes
- Time is divided into beacon intervals and every node is synchronized by periodic beacon transmissions
- Ad hoc traffic indication messages (ATIM) window is used to negotiate for channels for transmission
  - ATIM, ATIM-ACK, and ATIM-RES (ATIM-reservation) message
  - ATIM messages takes place on a particular channel (default channel)
- The receiver plays a dominant role in channel selection

# MMAC: Multi-Channel MAC Protocol II



# MMAC: Multi-Channel MAC Protocol III



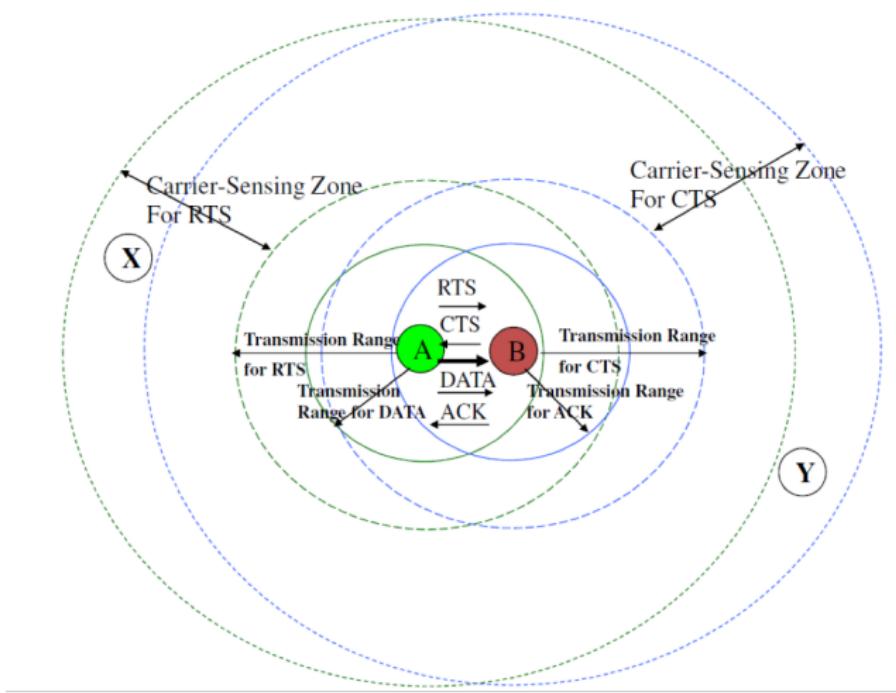
# Agenda

- 36 MAC Issues in Ad Hoc Networks
- 37 Contention-based protocols
- 38 Contention-based protocols with reservation mechanisms
- 39 Contention-based protocols with scheduling
- 40 MAC Protocols with Directional Antennas
- 41 Multi-channel MAC Protocols
- 42 Power Control MAC Protocol**

# Power Control MAC Protocol I

- The PCM allows nodes to vary their transmission power levels on a per packet basis
- BASIC scheme
  - RTS and CTS are transmitted with maximum power  $p_{max}$
  - The RTS is received at the receiver with signal level  $p_r$ , the receiver calculate the desired power level  $p$  based on the desired received power level  $I$ ,  $p_r$ , the transmitted power level  $p_{max}$ , and the noise level at receiver
- In the second method, when the source receives the CTS (in maximum power) packet, it calculates  $p_{desired}$  as follows:
  - $p_{desired} = (p_{max}/p_r) \times Rx_{thresh} \times c$ , where  $Rx_{thresh}$  is the minimum necessary received signal strength and  $c$  is the constant
  - Drawbacks: May increase the probability of collision

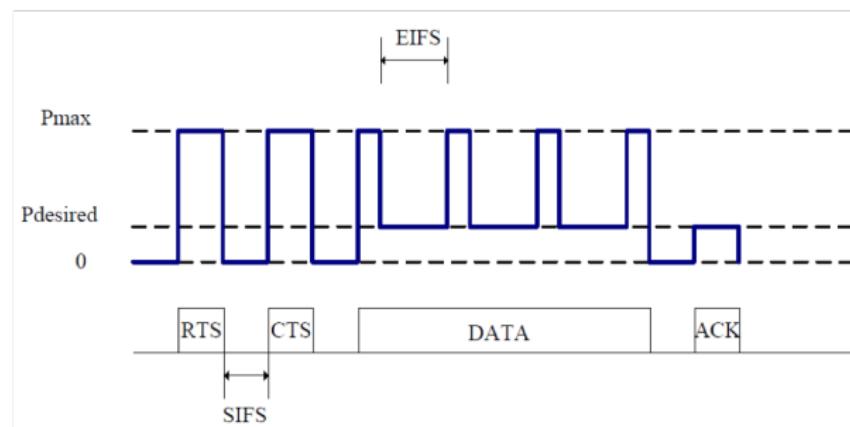
# Power Control MAC Protocol II



# Power Control MAC Protocol III

Solution:

- RTS and CTS are transmitted with maximum power  $p_{max}$
- Carrier-sensing zone: received signal not high enough to decode it correctly
- Transmit the DATA packet at maximum power level  $p_{max}$  periodically
- The duration of each such transmission must be larger than the time required for physical carrier sensing



# Summary

Future directions and current research:

- Hidden/exposed terminal problem
- Interference limited model
- Energy conservation
- Single channel v.s. Multiple channels
- Multi-hop networks
- Fairness among competing nodes
- Directional antennas
- QoS issues

## Lecture 7: Routing in Ad Hoc Networks

# Objectives

At the end of this lecture, you will be able to

- define the key terminology at the network layer [1],
- classify ad hoc routing protocols,
- define reactive and proactive routing protocols in ad hoc networks,
- define IETF standardized routing protocols.

# Agenda

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

# Terminology

- **Routing**: moving information across a network from a source to a destination where at least one intermediate node is encountered
- **Routing Components**
  1. Path determination  $\Rightarrow$  routing
  2. Information transport  $\Rightarrow$  forwarding
- **Host**: source or destination of traffic (data packets)
- **Router**: network components that forwards information packets towards their destination (in ad-hoc networks are nodes could be hosts as well as routers/relays)
- **Route**: the path, consisting of several links and routers, between a source and a destination

# Terminology

- **Routing metrics:** a measurable value indicating the goodness of a link or a path in the network. Common metrics are: path length, reliability, delay, bandwidth, load, communication cost
- **Routing information:** information regarding routes in the network that is kept at the routers (in routing tables). This information is dynamic
- **Routing protocol:** In a network with many nodes and links, routing protocols keep the routing information up-to-date despite the dynamics of the network, and find the optimum path between a source and a destination
- **Routing algorithm:** a static algorithm, in the heart of a routing protocol, that uses routing information to compute mathematically the optimum path, based on a single or multiple metrics, between any source-destination pair

# Terminology

- **Broadcasting**: sending a message on all outgoing links of a node to all its neighbors (our definition)
- **Hello message**: a short messages send directly to connected (reachable) nodes that contains the address of the transmitter along with some optional additional data (e.g. the list of a node's neighbors)
- **Tree**: a tree is a graph in which any two vertices are connected by exactly one path. A tree is a simple, undirected, connected, acyclic graph
- **Spanning tree**: tree composed of all the vertices and some (or perhaps all) of the edges of a graph

# Routing

## A famous quotation from RFC 791

A **name** indicates what we seek.

An **address** indicates where it is.

A **route** indicates how we get there.

### Forwarding: data plane

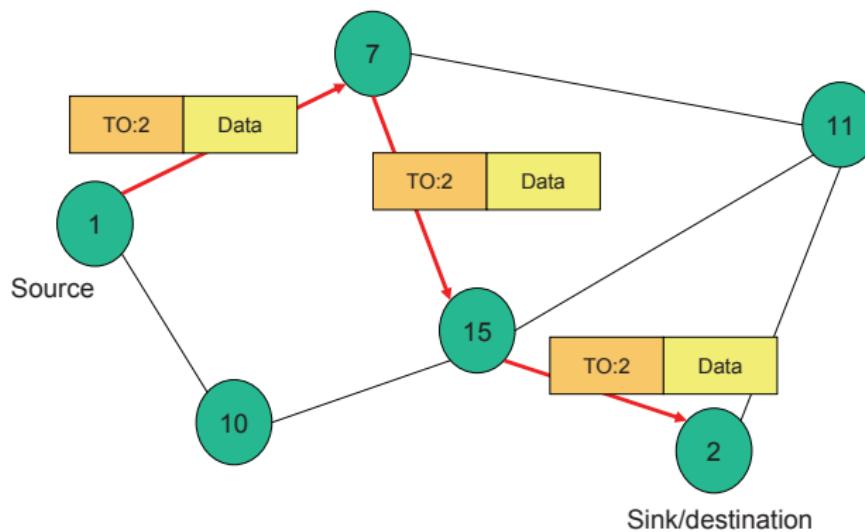
- Directing a data packet to an outgoing link
- Individual router using a forwarding table

### Routing: control plane

- Computing paths the packets will follow
- Routers talking amongst themselves
- Individual router creating a forwarding table

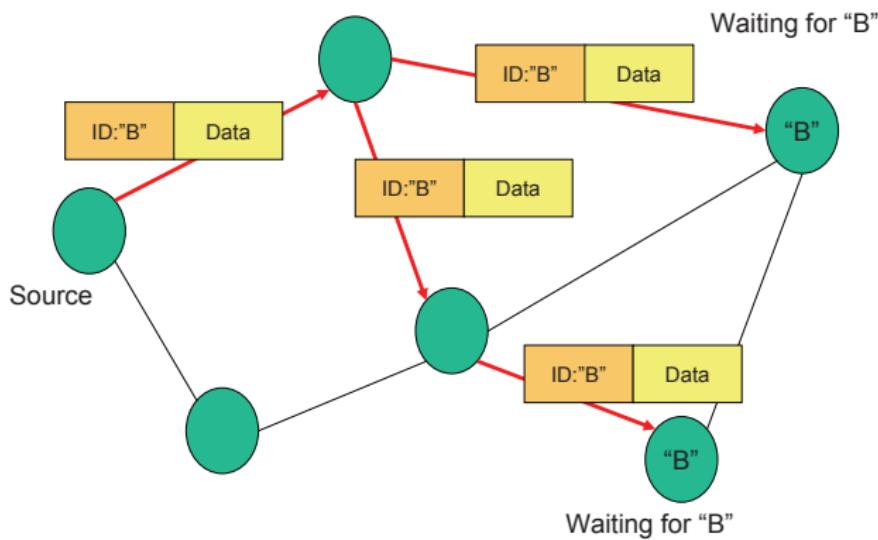
# Addressed Based Protocol

- Directed towards a well-specified particular destination (sink)
- Support for unicast, multicast, and broadcast messages



# Data Centric Forwarding

- Forwarding of messages to all / some appropriate nodes
- Routing decisions according to the *data*, i.e. encoding rules are needed



# Comparison

	<b>Address-based routing</b>	<b>Data-centric forwarding</b>
Routing approach	Identification of a path according to the destination address of the data message	Determination of the destination of a data message according to the content of the packet
Prerequisites	Network-wide unique addresses	Pre-defined message types and semantics
Routing techniques	Proactive routing (continuous state maintenance) or reactive routing (on-demand path finding)	(probabilistic) flooding schemes or interest-based reverse routing
Advantages	Usually low delays in connection setup and data dissemination	No address information required and simplified self-management and redundancy
Disadvantages	Network-wide unique address identifiers required	Increased overhead for single transmissions

# Main Tasks of Routing Protocols

## topology discovery

- I like to speak to x?
- Periodic advertisements, Hello.
- Query reply

## topology maintenance

- Where did x go? Or where did y, who knows where x is?
- Periodic detection message exchange? I'm alive?
- Transmission snooping.
- Timeouts?

# Agenda

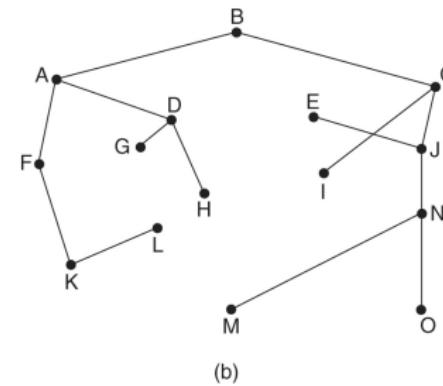
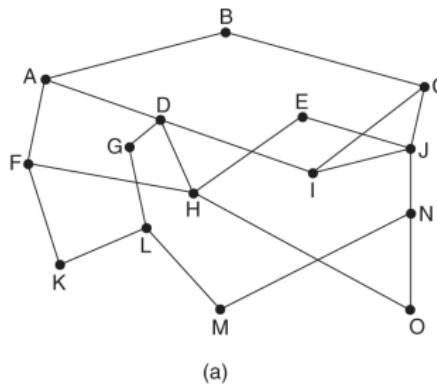
- 43 Introduction and Terminology
- 44 Legacy Routing Protocols**
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

## Optimality Principle

## Think about Dijkstra's Algorithm

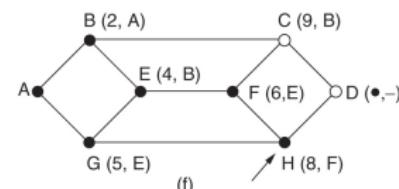
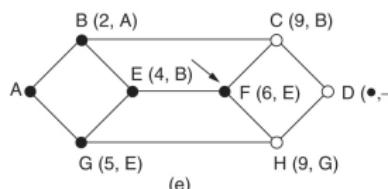
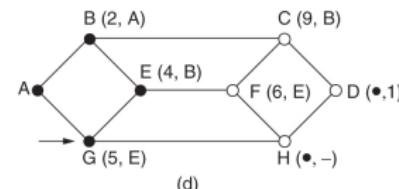
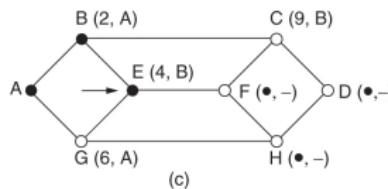
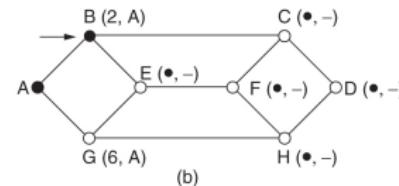
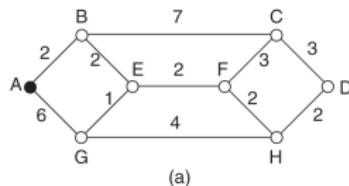
If a router F is on the optimal path from router L to router B, then the optimal path from F to B also follows the same route.

Apply the optimality principle  $\Rightarrow$  form a tree by taking the optimal path from every other router to a single router, B.



# Shortest Path: Dijkstra

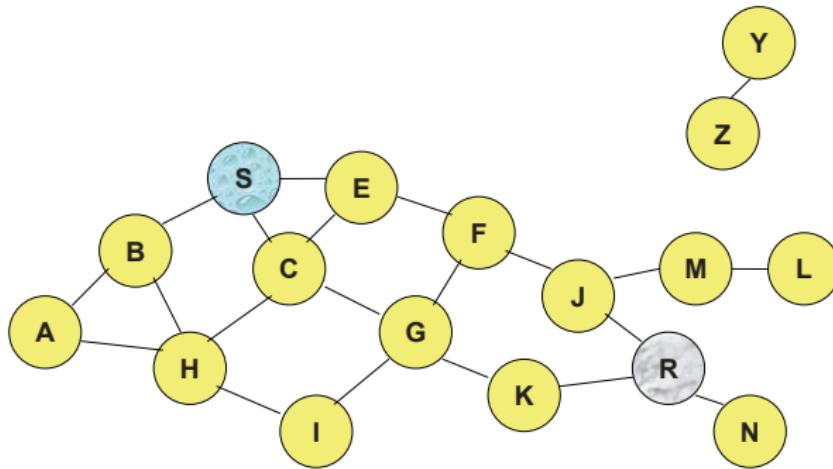
From A to D, 5 steps shown



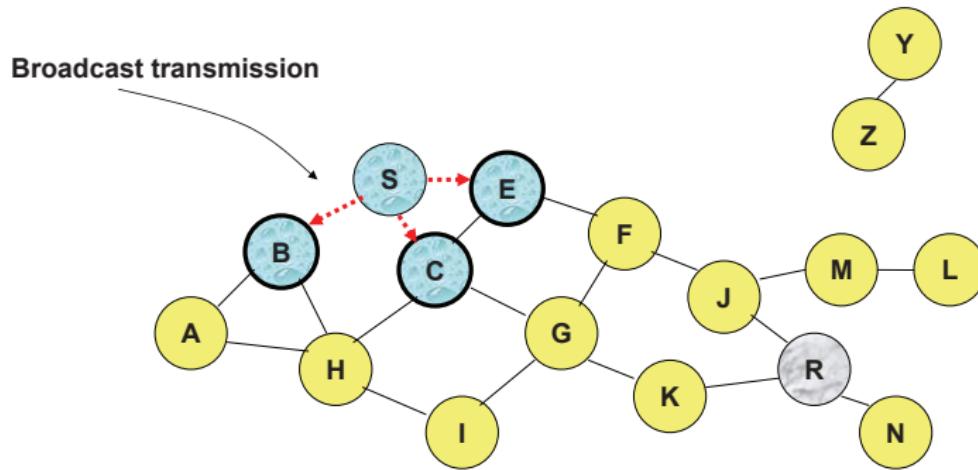
# Flooding

- A method for sharing information among all nodes
- Basic form: each node sends a messages to all other nodes, through broadcasting the message to all its neighbors
- Usually used for updating topology database
- Causes many duplicated packets and waste of resources
- Simple and reliable; very high overhead
- Can be used as a comparison metric
  - Always chooses the shortest path
  - Tries every possible path in parallel
  - No other algorithm may produce a shorter delay

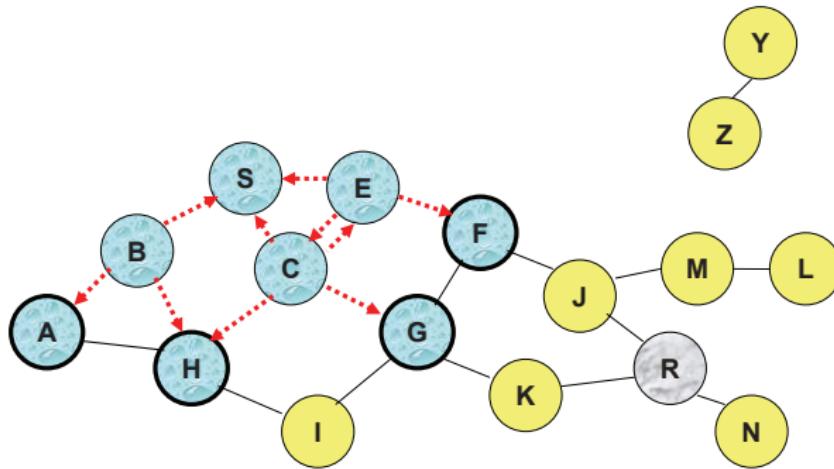
# Flooding



# Flooding

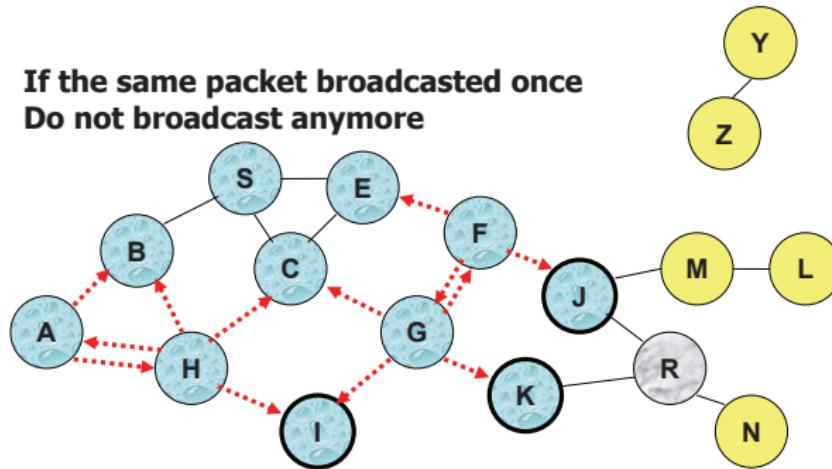


# Flooding

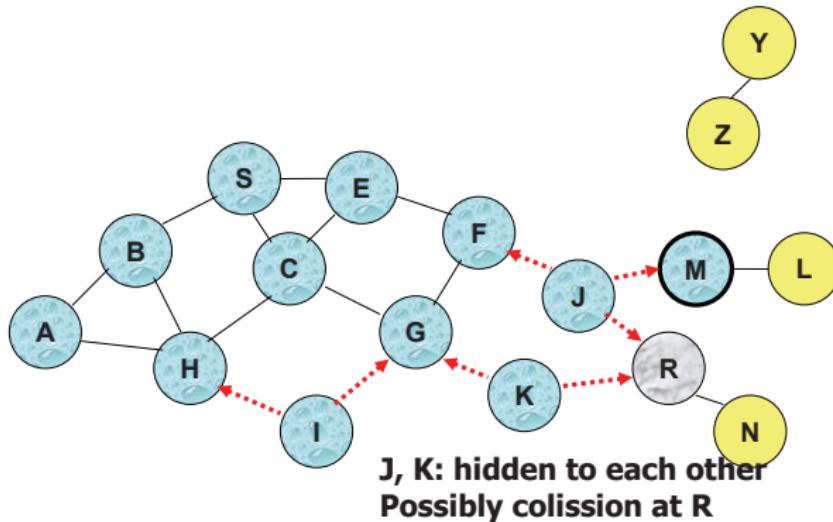


# Flooding

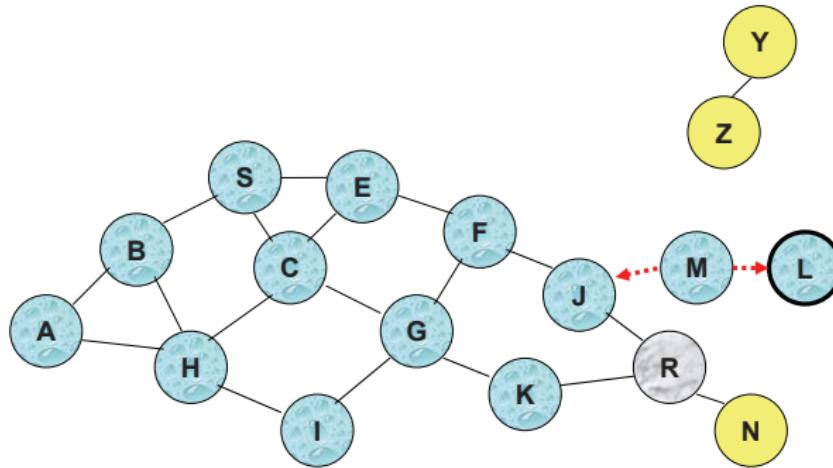
If the same packet broadcasted once  
Do not broadcast anymore



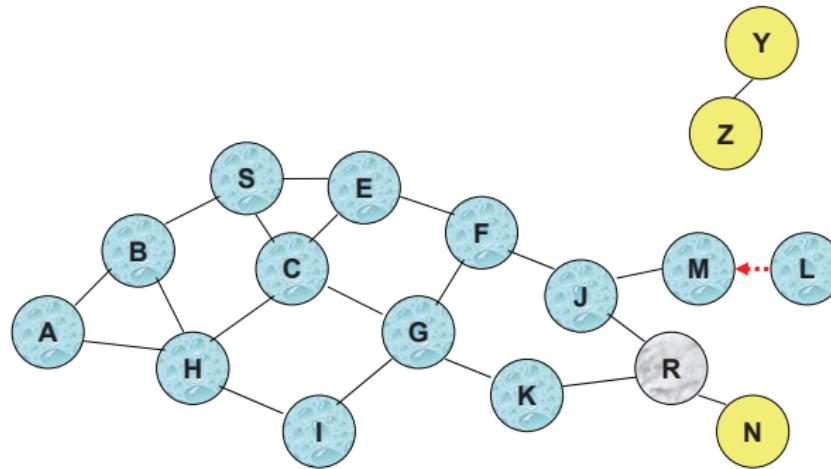
# Flooding



# Flooding



# Flooding



# Routing Table

- A routing table contains information to determine how to forward packets
- Source routing: Routing table is used to determine route to the destination to be specified in the packet
- Hop-by-hop routing: Routing table is used to determine the next hop for a given destination
- Virtual circuit routing: Routing table used to determine path to configure through the network
- A distributed algorithm is required to build the routing table
  1. Distance vector algorithms
  2. Link state algorithms

# Distance Vector Algorithms

- Each node begins with only the knowledge of the cost of its directly attached links
- Cost=1 then shortest path!
- Through an iterative process of calculation and exchange of information with neighbors a routing table is built for all destinations (next hop and distance to the destination)
- Result: each node has only information about the next hop to reach a destination
- Example: RIP (Routing Information Protocol) using distributed Bellman-Ford algorithm
- **routing by rumor**, as most routers depend on hearsay information, rather than on their personal knowledge of network topology.

# Link State Algorithms

- Each node begins with finding its neighbors
- Each node generates link state advertisements (LSAs) which are distributed to all nodes  $LSA = (\text{link id}, \text{state of the link}, \text{cost}, \text{neighbors of the link})$
- Each node maintains a database of all received LSAs (topological database or link state database), which describes the network has a graph with weighted edges
- Result: all nodes have complete topology, link cost information
- Each router uses its link state database to run a shortest path algorithm (Dijkstra's algorithm) to produce the shortest path to each network node
- Example: OSPF (Open Shortest Path First)

# Agenda

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks**
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

# When It Comes to Ad Hoc Networks

## Distance Vector (e.g., Bellman-Ford)

- Tables grow linearly with the number nodes
- Routing control overhead is linearly increasing with network size
- Convergence problems (count to infinity);
- Potential loops (mobility)

## Link State (e.g., OSPF)

- Link update flooding overhead caused by network size and frequent topology changes

**Conventional Routing Does Not Scale To Size And Mobility**

# IETF MANET Working Group

## MANET

The Mobile Ad-hoc Networking (manet) Working Group is a chartered working group within the Internet Engineering Task Force (IETF) to investigate and develop candidate standard Internet routing support for mobile, wireless IP autonomous segments.

IETF Home Page: at [www.ietf.org](http://www.ietf.org)

standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion or other factors.

# IETF RFC 2501

## RFC2501: Performance Issues and Evaluation Considerations

### MANETs have several salient characteristics

1. **Dynamic topologies:** Nodes move arbitrarily; network topology (multihop) change randomly, unpredictably, unidirectional links
2. **Bandwidth-constrained, variable capacity links:** Wireless links have lower capacity than their hardwired counterparts. Throughput after accounting for multiple access, fading, noise, and interference conditions is much less than the maximum transmission rate.
3. **Energy-constrained operation:** Some nodes rely on batteries
4. **Limited physical security:** prone to physical security threats

# IETF RFC 2501

## Requirements for Ideal Routing Protocol

- Fully distributed (scalability)
- Adaptive (topology changes)
- Minimum number of nodes involved for route computation
- Localized state (reduced global state)
- Loop-free, free from stale routes
- Limited number of broadcasts (collision avoidance)
- Quick and stable convergence
- Optimal resource utilization (bandwidth, processing, memory, battery)
- Localized updates
- Provision of QoS as demanded by the applications

# IETF RFC 2501

## Quantitative Metrics

- End-to-end data throughput and delay: Statistical measures of data routing performance (e.g., means, variances, distributions)
- Route Acquisition Time: time required to establish route(s) when requested
- Percentage Out-of-Order Delivery
- Efficiency: Average number of data bits transmitted/data bit delivered; average number of control bits transmitted/data bit delivered; average number of control and data packets transmitted/data packet delivered

# IETF RFC 2501

## Parameters Impacting the Performance

- Network size: measured in the number of nodes
- Network connectivity: the average degree of a node
- Topological rate of change: the speed with which a network's topology is changing
- Link capacity: bits/second after losses
- Fraction of unidirectional links
- Traffic patterns: non-uniform or bursty traffic patterns
- Mobility: when, and under what circumstances, is temporal and spatial topological correlation relevant to the performance of a routing protocol?
- Fraction and frequency of sleeping nodes: presence of sleeping and awakening nodes?

# MANET versus Traditional Routing

- Every node is a router in a MANET
- Topologies are dynamic in MANETs due to mobile nodes
- Routing in MANETs must consider both Layer 3 and Layer 2 information; e.g.; connectivity and interference
- MANET topologies tend to have many more redundant links than traditional networks
- A MANET *router* typically has a single interface
- Routed packet sent forward when transmitted, but also sent to previous transmitter
- Channel properties (capacity, error rates, etc.) vary in MANETs
- Interference is an issue in MANETs
- Channels can be asymmetric
- Power efficiency is an issue in MANETs
- Physical security

# Goals in Routing Algorithm Design

- Provide the maximum possible reliability - use alternative routes if an intermediate node fails.
- Choose a route with the least cost metric.
- Give the nodes the best possible response time and throughput.
- Route computation must be distributed. Centralized routing in a dynamic network is usually very expensive.
- Routing computation should not involve the maintenance of global state.
- Every node must have quick access to routes on demand.
- Each node must be only concerned about the routes to its destination.
- Broadcasts should be avoided (highly unreliable)
- It is desirable to have a backup route when the primary route has become stale.

# Goals in Routing Algorithm Design for WSN

- Exploit spatial diversity and density of sensors
- Build an adaptive node sleep schedule
- Explore the tradeoff between data redundancy and bandwidth consumption
- The nodes on deployment should create and assemble a network, adapt to device failure and degradation, manage mobility of sensor nodes and react to changes in task and sensor requirements
- Adaptability to traffic changes
- Allowing finer control over an algorithm rather than simply turning it on and off

# Agenda

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols**
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

# Classification of Ad Hoc Routing Protocols

## Routing information update

- Proactive or table-driven routing protocols
- Reactive or on-demand routing protocols
- Hybrid routing protocols

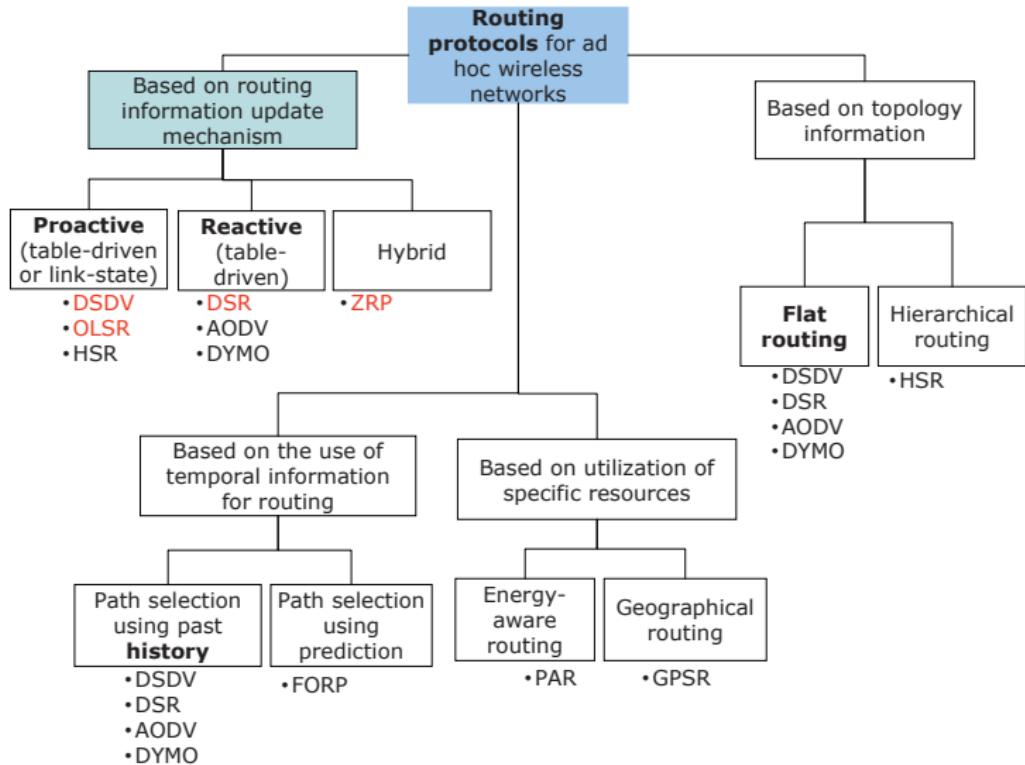
## Topology

- Flat topology routing protocols
- Hierarchical topology routing protocols

## Utilization of specific resources

- Power-aware routing
- Geographical information assisted routing

# Classification of Ad Hoc Routing Protocols



# Proactive versus Reactive Routing Protocols

## Proactive Routing Protocols

- Periodic exchange of control messages
- + immediately provide the required routes when needed
- - larger signalling traffic and power consumption.
- e.g., FSR, OLSR, DSDV

## Reactive Routing Protocols

- Attempts to discover routes only on-demand by flooding
- + smaller signalling traffic and power consumption.
- - long delay for application when no route to the destination is available  
e.g., DSR, AODV, Ant routing

# Proactive Routing Protocols

Similar to routing in fixed networks

Idea: start from an existing protocol, adapt it!

e.g., Destination Sequence Distance Vector (DSDV)

- Based on distributed Bellman Ford procedure. Every node maintains
  - a routing table
  - all available destinations
  - the next node to reach to destination
  - the number of hops to reach the destination
- Add aging information to route information propagated by distance vector exchanges; helps to avoid routing loops
- Periodically send full route updates
- On topology change, send incremental route updates
- Unstable route updates are delayed

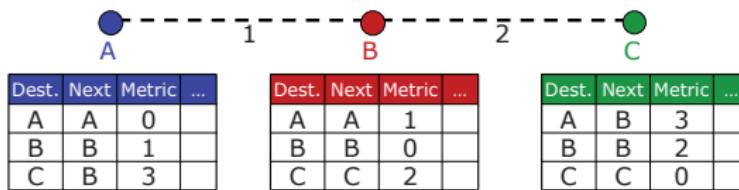
# Agenda

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector**
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

# Distance Vector Routing - Recap

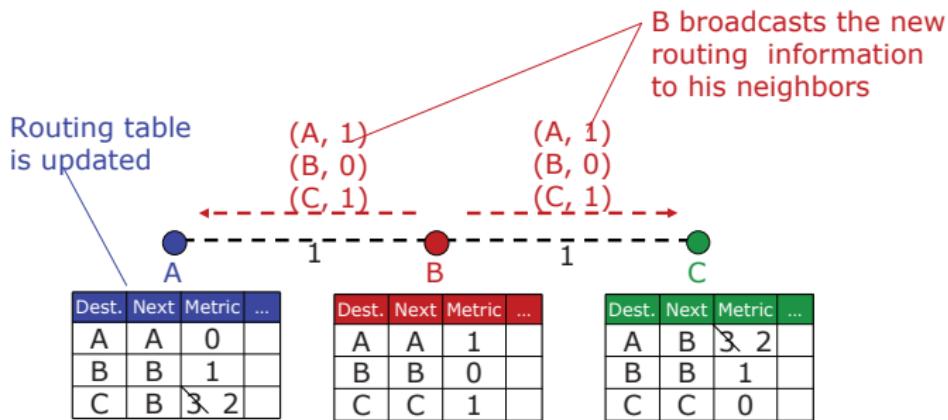
## Routing tables of each node

e.g., it takes 3 to reach C from A and the next hop is B

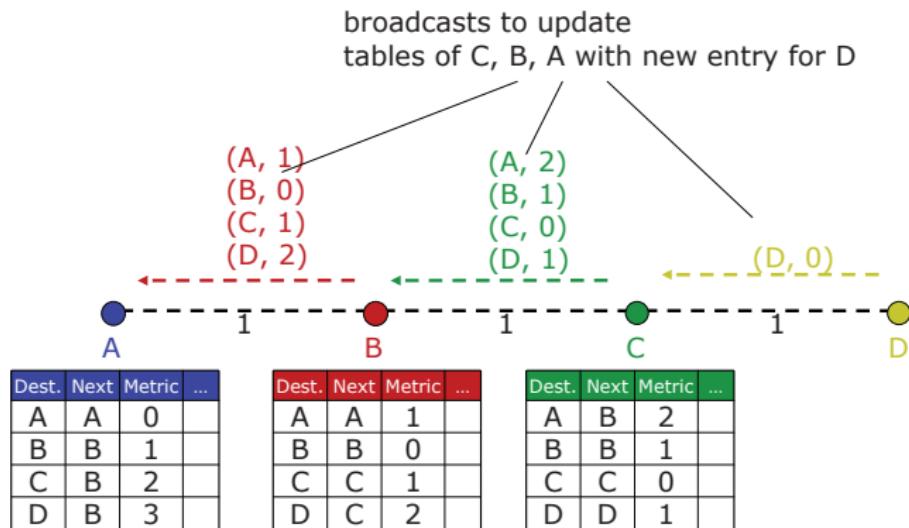


# Distance Vector Routing - Recap

**Event: BC link weight changes to 1 from 2**

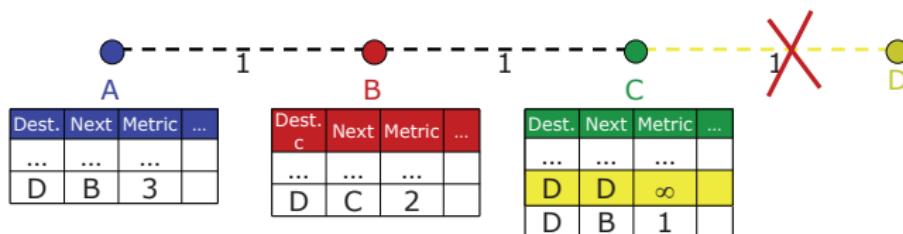


# Distance Vector Routing - Recap



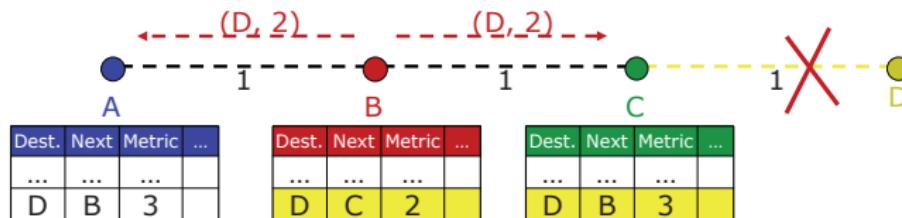
# Distance Vector Routing - Recap

**Event: node D leaves the network**



# Distance Vector Routing - Recap

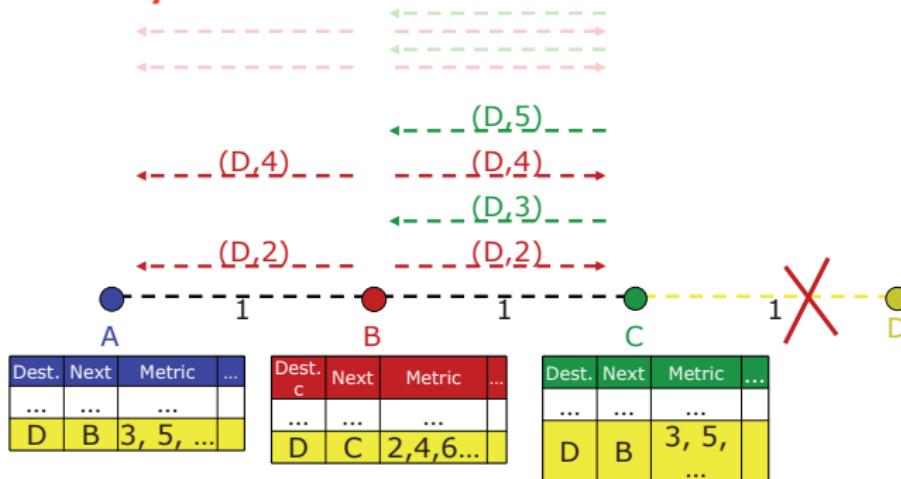
**Event: node D leaves the network**  
**Loop starts**



# Distance Vector Routing - Recap

**Event: node D leaves the network**

**Count to infinity**



# DSDV: Destination Sequence Distance Vector

## DSDV Routing tables of each node

e.g., it takes 3 to reach C from A and the next hop is B

Notice all sequence numbers are even! Why?



Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	3	C-586

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

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

# DSDV: Destination Sequence Distance Vector

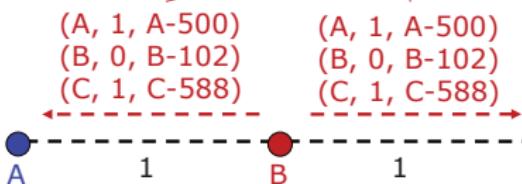
## Route Advertisement

**Event:** BC link weight changes to 1 from 2

B increases Seq.Nr from 100 -> 102

B broadcasts routing information

to Neighbors A, C including destination sequence numbers



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

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

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

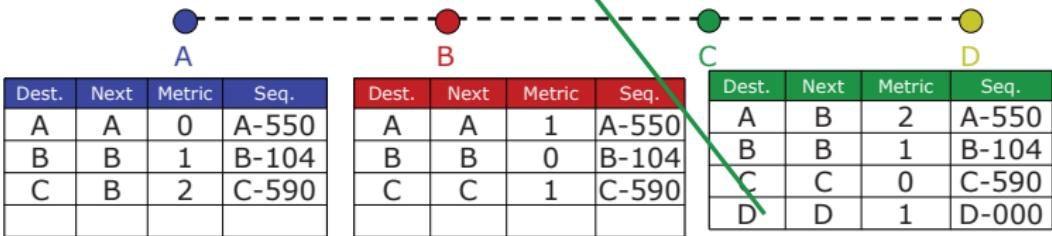
# DSDV: Destination Sequence Distance Vector

**Event: New node D joins the network**

2. Insert entry for D with sequence number D-000  
Then immediately broadcast own table

1. D broadcast for first time  
Send Sequence number D-000

$(D, 0, D-000)$

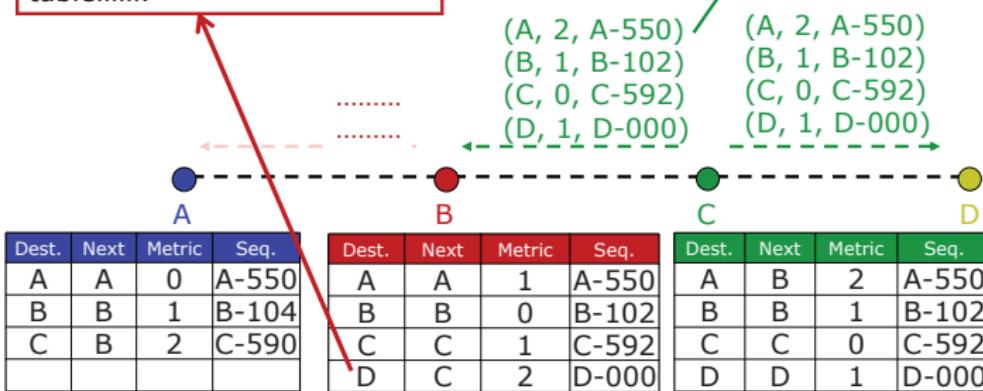


# DSDV: Destination Sequence Distance Vector

**Event: New node D joins the network (continued)**

4. B gets this new information and updates its table.....

3. C increases its sequence number to C-592 then broadcasts its new table.

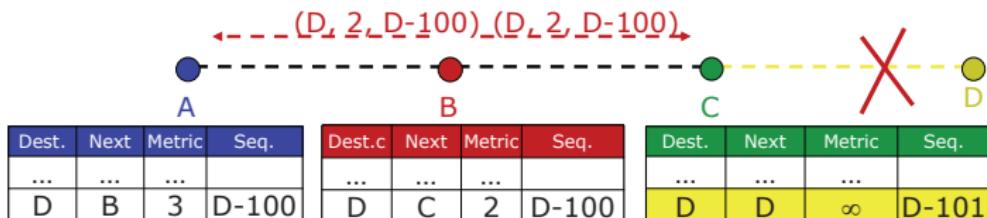


# DSDV: Destination Sequence Distance Vector

**Event: node D leaves the network**  
**NO LOOPS (Odd sequence number?)**  
**NO COUNT TO INFINITY**

2. B does its broadcast  
-> no affect on C (C knows that B has stale information because C has higher seq. number for destination D)  
-> no loop -> no count to infinity

1. Node C detects broken Link:  
-> Increase Seq. Nr. by 1  
(only case where not the destination sets the sequence number -> odd number)



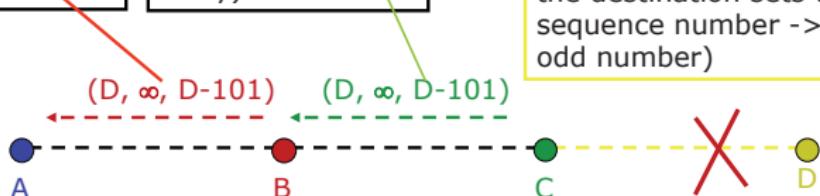
# DSDV: Destination Sequence Distance Vector

**Event: node D leaves the network (continued)**  
**Immediate Advertisement**

3. Immediate propagation  
B to A:  
(update information has higher Seq. Nr. -> replace table entry)

2. Immediate propagation  
C to B:  
(update information has higher Seq. Nr. -> replace table entry)

1. Node C detects broken Link:  
-> Increase Seq. Nr. by 1  
(only case where not the destination sets the sequence number -> odd number)



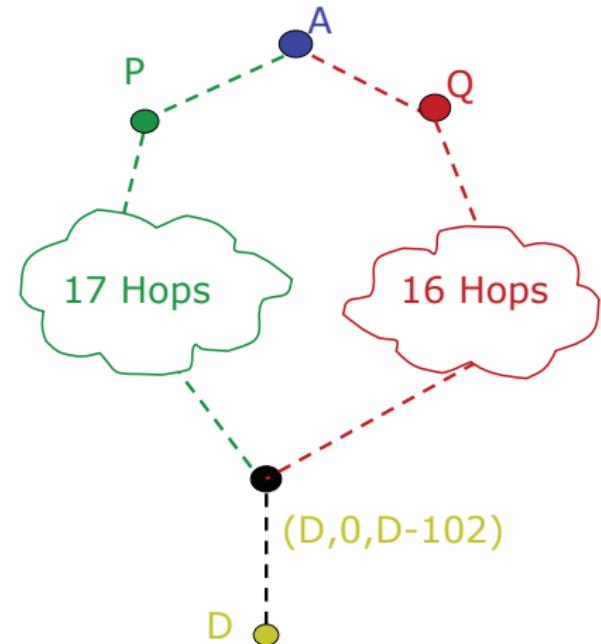
Dest.	Next	Metric	Seq.
...	...	...	...
D	B	3	D-100
D	B	$\infty$	D-101

Dest.c	Next	Metric	Seq.
...	...	...	...
D	C	2	D-100
D	C	$\infty$	D-101

Dest.	Next	Metric	Seq.
...	...	...	...
D	D	1	D-100
D	D	$\infty$	D-101

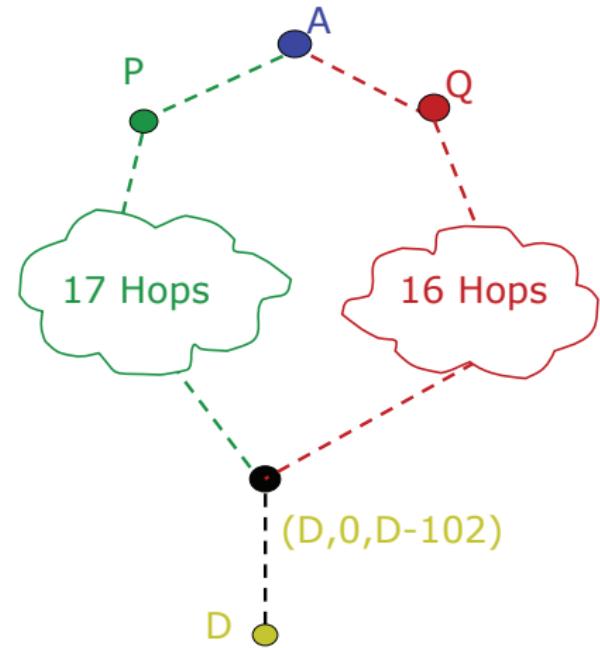
# DSDV Problem: Fluctuations

- ✓ Entry for D in A: [D, Q, 20, D-100]
- ✓ D makes Broadcast with Seq. Nr. D-102
- ✓ A receives from P Update (D, 21, D-102)  $\Rightarrow$  Entry for D in A: [D, P, 21, D-102]  $\Rightarrow$  A must propagate this route immediately
- ✓ A receives from Q Update (D, 20, D-102)  $\Rightarrow$  Entry for D in A: [D, Q, 20, D-102]  $\Rightarrow$  A must propagate this route immediately



# DSDV Problem: Damping Fluctuations

- Record last and avg. settling time in a table
- Settling time is time between first and best route for a given sequence
- **A** updates routing table on first arrival with newer sequence; but waits for advertisement
- Time to wait is twice avg. settling time



# Agenda

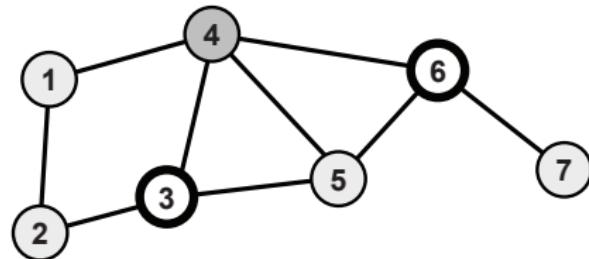
- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing**
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

# OLSR: Optimized Link State Routing

- Proactive (table-driven) routing protocol: route is available immediately when needed
- Based on the link-state algorithm: traditionally, all nodes flood neighbor information in a link-state protocol, but not in OLSR
- Nodes advertise only links with neighbors who are in its multipoint relay selector set: reduces size of control and flooding packets
- Does not require reliable transfer, since updates are sent periodically
- Does not need in-order delivery, sequence numbers prevent out-of-date information
- Uses hop-by-hop routing: routes are based on dynamic table entries maintained at intermediate nodes

# OLSR: Multipoint Relays (MPR)

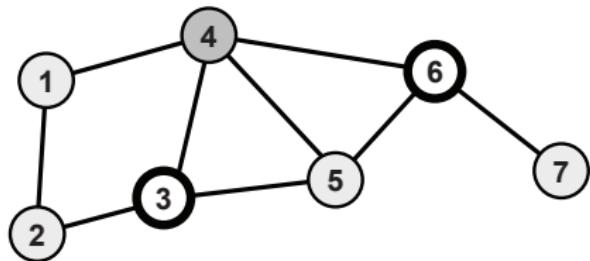
- Each node  $N$  selects a set of neighbor nodes as multipoint relays,  $MPR(N)$ , that retransmit control packets from  $N$
- Neighbors **not in  $MPR(N)$**  do not forward the packets
- $MPR(N)$  is selected such that all two-hop neighbors of  $N$  are covered by (one-hop neighbors) of  $MPR(N)$



One optimal set for Node 4:  $MPR(4)\{3, 6\}$   
Any other?

# OLSR: Multipoint Relay Selector Set (MS)

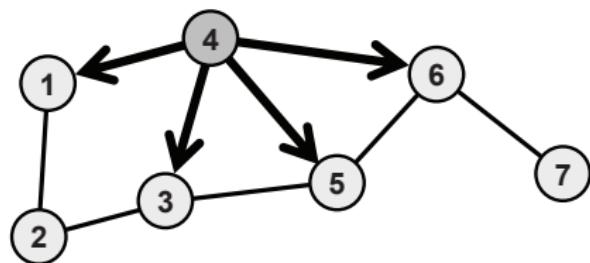
- The multipoint relay selector set for Node  $N$ ,  $MS(N)$ , is the set of nodes that choose Node  $N$  in their multipoint relay set
- Assumption: bidirectional links



$$MS(3)=\{\dots, 4, \dots\}$$
$$MS(6)=\{\dots, 4, \dots\}$$

# OLSR: Hello Messages I

- Each node uses HELLO messages to determine its MPR set
- All nodes periodically broadcast HELLO messages to their one-hop neighbors (bidirectional links)
- HELLO messages are not forwarded

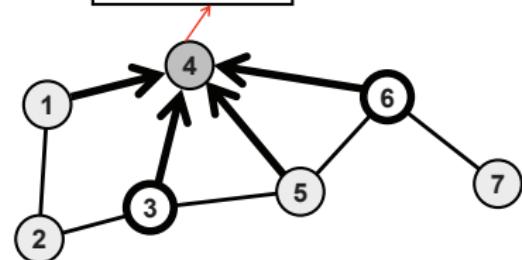


$\text{HELLO:} NBR(4) = \{1, 3, 5, 6\}$

# OLSR: Hello Messages II

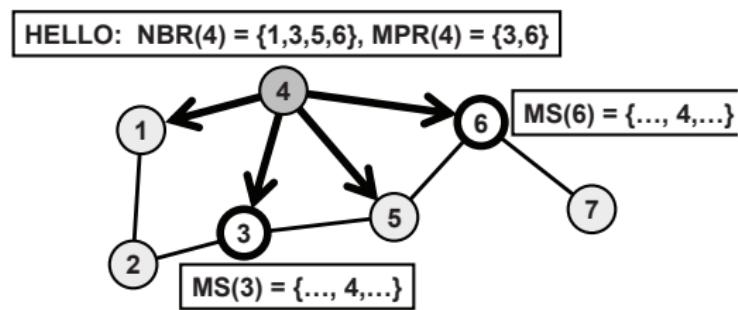
- Using the neighbor list in received HELLO messages, nodes can determine their two-hop neighborhood and an optimal (or near-optimal) MPR set
- A sequence number is associated with this MPR set
- Sequence number is incremented each time a new set is calculated

**At Node 4:**  
NBR(1) = {2}  
NBR(3) = {2,5}  
NBR(5) = {3,6}  
NBR(6) = {5,7}  
  
MPR(4) = {3,6}



# OLSR: Hello Messages III

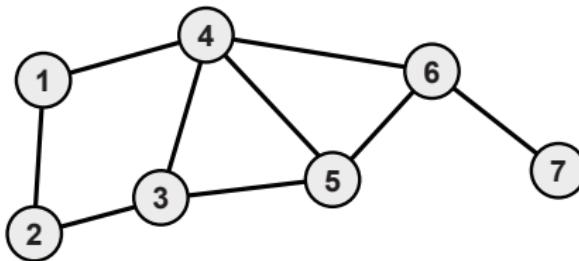
- Subsequent HELLO messages also indicate neighbors that are in the node's MPR set
- MPR set is recalculated when a change in the one-hop or two-hop neighborhood is detected



# OLSR: Topology Control Messages

- Nodes send topology information in Topology Control (TC) messages
- List of advertised neighbors (link information)
- Sequence number (to prevent use of stale information)
- A node generates TC messages only for those neighbors in its MS set
- Only MPR nodes generate TC messages
- Not all links are advertised
- A node processes all received TC messages, but only forwards TC messages if the sender is in its MS set
- Only MPR nodes propagate TC messages

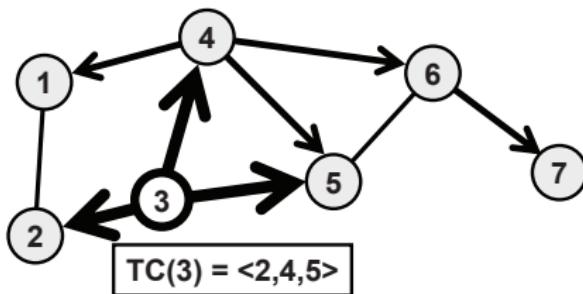
# OLSR Examples



$MPR(1) = \{ 4 \}$
$MPR(2) = \{ 3 \}$
$MPR(3) = \{ 4 \}$
$MPR(4) = \{ 3, 6 \}$
$MPR(5) = \{ 3, 4, 6 \}$
$MPR(6) = \{ 4 \}$
$MPR(7) = \{ 6 \}$

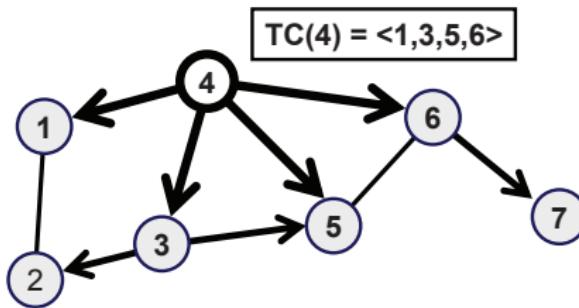
$MS(1) = \{ \}$
$MS(2) = \{ \}$
$MS(3) = \{ 2, 4, 5 \}$
$MS(4) = \{ 1, 3, 5, 6 \}$
$MS(5) = \{ \}$
$MS(6) = \{ 4, 5, 7 \}$
$MS(7) = \{ \}$

# OLSR Examples



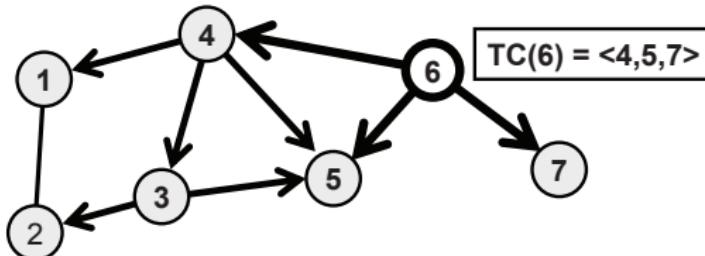
- Node 3 generates a TC message advertising nodes in  $MS(3) = \{2, 4, 5\}$
- Node 4 forwards Node 3's TC message since  $Node 3 \in MS(4) = \{1, 3, 5, 6\}$
- Node 6 forwards TC(3) since  $Node 4 \in MS(6)$

# OLSR Examples



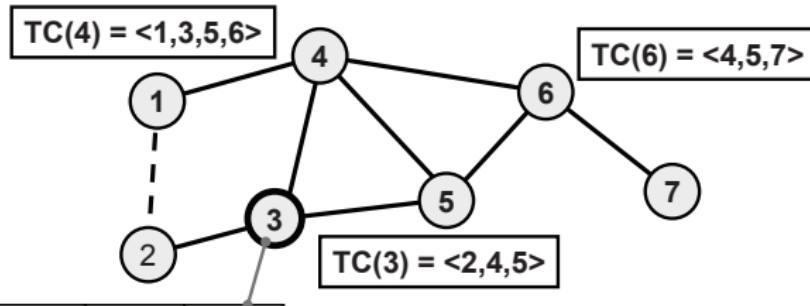
- Node 4 generates a TC message advertising nodes in  $MS(4) = \{1, 3, 5, 6\}$
- Nodes 3 and 6 forward TC(4) since  $Node\ 4 \in MS(3)$  and  $Node\ 4 \in MS(6)$

# OLSR Examples



- Node 6 generates a TC message advertising nodes in  $MS(6) = \{4, 5, 7\}$
- Node 4 forwards TC(6) from Node 6 and Node 3 forwards TC(6) from Node 4
- After Nodes 3, 4, and 6 have generated TC messages, all nodes have link-state information to route to any node

# OLSR Examples



Dest	Next	Hops
1	4	2
2	2	1
4	4	1
5	5	1
6	4 (5)	2
7	4 (5)	3

- Given TC information, each node forms a topology table
- A routing table is calculated from the topology table
- Note that Link 1-2 is not visible except to Nodes 2 and 3

# Agenda

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing**
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

# Reactive Routing: DSR

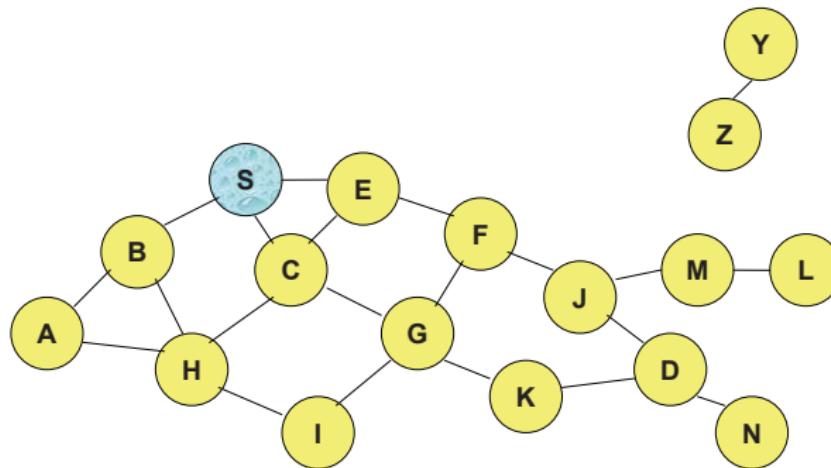
DSR: Dynamic Source Routing (IETF RFC 4728)

Source routing: entire path to destination supplied by source in packet header

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration.

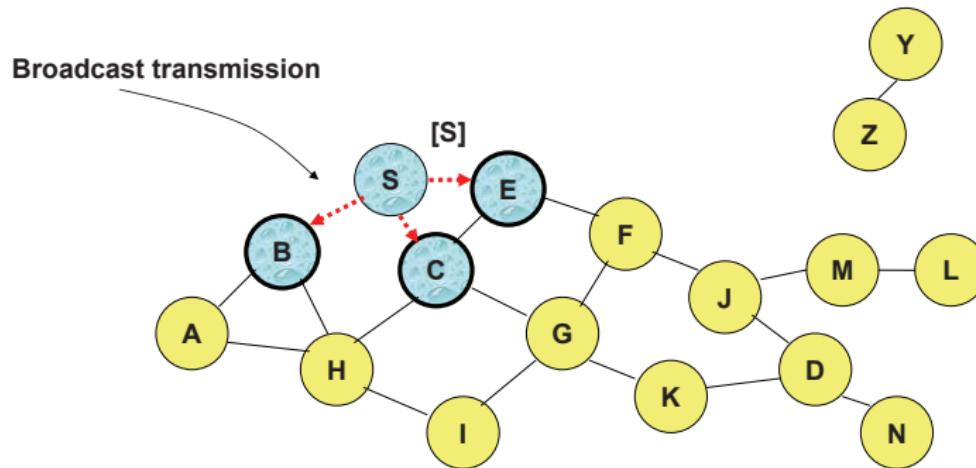
- Route discovery: Undertaken when source needs a route to a destination
- Route maintenance: Detect network topology changes; used when link breaks, rendering specified path unusable
- Intermediate nodes cache overheard routes
- Intermediate node may return Route Reply to source if it already has a path stored
- Destination may need to discover route to source to deliver Route Reply
- Route Request duplicate rejection (RREQ id)

# DSR: Route Discovery (Route Request [RREQ] Message)



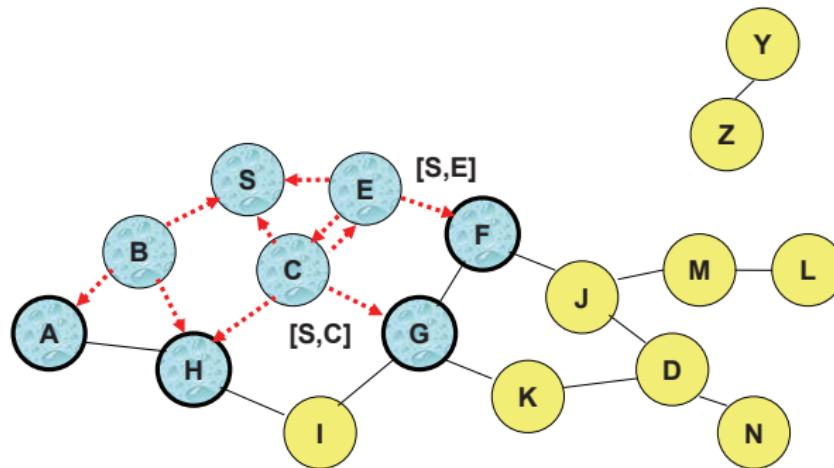
Represents a node that has received RREQ for D from S

# DSR: Route Discovery (Route Request [RREQ] Message)



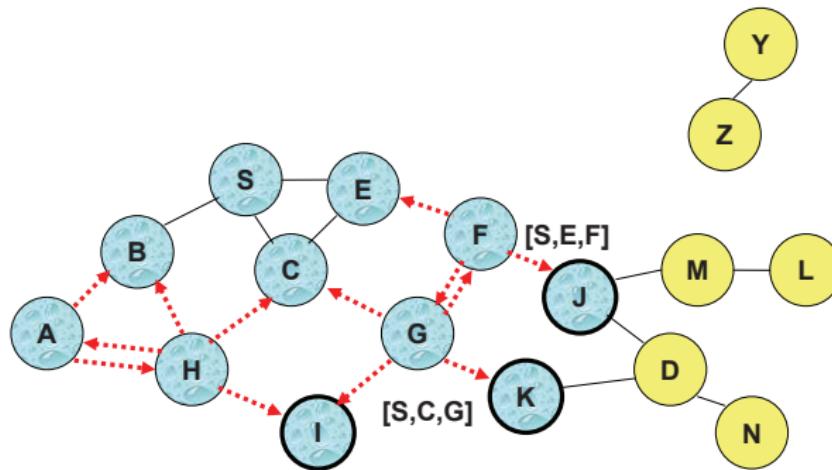
-----> Represents transmission of RREQ  
[X, Y] Represents list of identifiers appended to RREQ

# DSR: Route Discovery (Route Request [RREQ] Message)



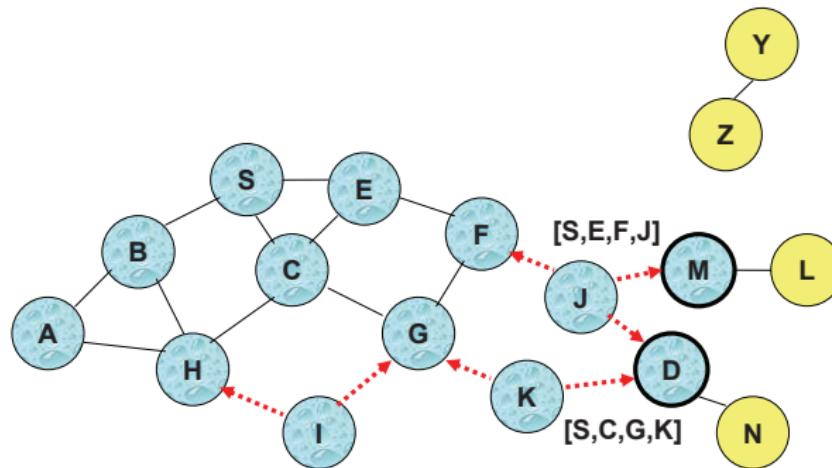
- Node H receives packet RREQ from two neighbors:  
**potential for collision**

# DSR: Route Discovery (Route Request [RREQ] Message)



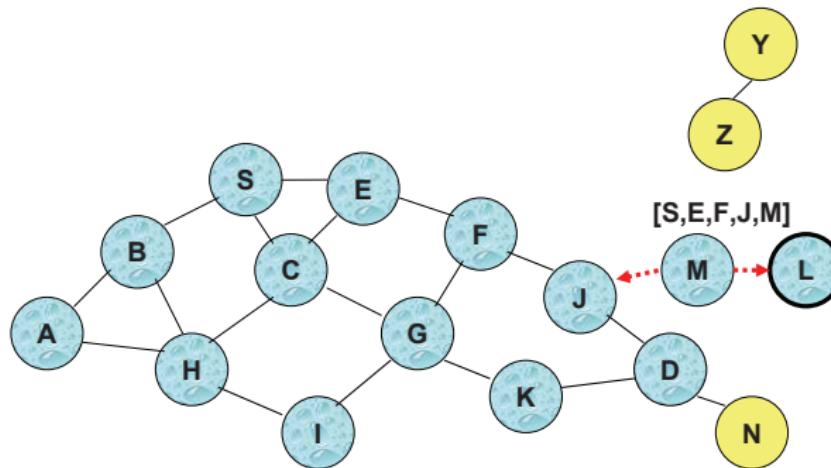
- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

# DSR: Route Discovery (Route Request [RREQ] Message)



- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are **hidden** from each other, their **transmissions may collide**

## DSR: Route Discovery (Route Request [RREQ] Message)



- Node D **does not forward** RREQ, because node D is the intended target of the route discovery

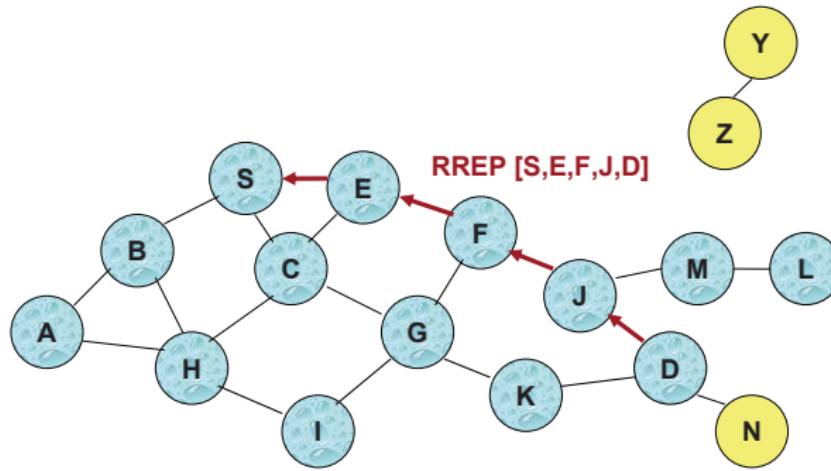
# DSR Route Reply (RREP)

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional
- To ensure this, RREQ should be forwarded only if it received on a link that is known to be bi-directional
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
- Unless node D already knows a route to node S
- If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked on the Route Request from D.
- If IEEE 802.11 MAC is used to send data, then links have to be bi-directional (since Ack is used)

# DSR Route Reply (RREP)

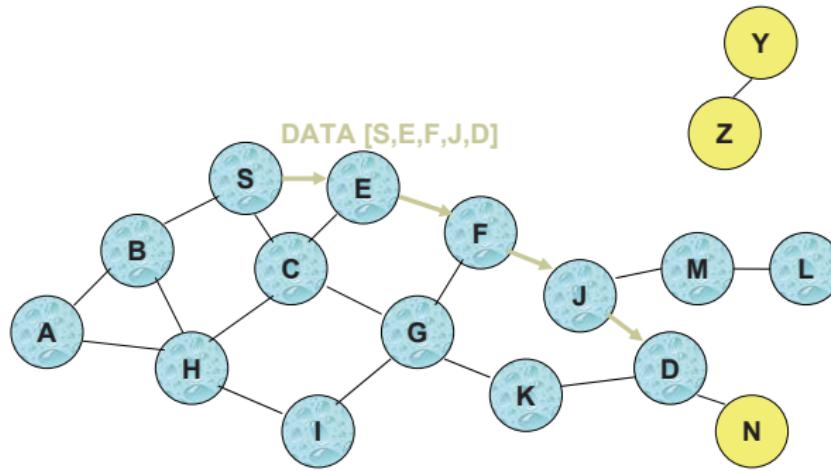
- Node S on receiving RREP, caches the route included in the RREP
- When node S sends a data packet to D, the entire route is included in the packet header
- hence the name source routing
- Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded

# DSR Route Reply (RREP)



- Node D sends back a Reply (RREP) to S with the path
- NOTE: If node D does not know a rout back to S it might be necessary to start it's own rout discovery to S.

# DSR Data Delivery (DATA)



Packet header size grows with route length

# DSR Advantages and Disadvantages

## Advantages

- Routes maintained only between nodes who need to communicate
- reduces overhead of route maintenance
- Route caching can further reduce route discovery overhead
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches

# DSR Advantages and Disadvantages

## Disadvantages

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network
- Care must be taken to avoid collisions between route requests propagated by neighboring nodes
- insertion of random delays before forwarding RREQ
- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches
- Increased contention if too many route replies come back due to nodes replying using their local cache
- Route Reply Storm problem
- Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route

# Agenda

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing**
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols

# AODV: Ad-hoc On-demand Distance Vector Routing

## IETF RFC 3561

- Pure on-demand routing protocol
- A node does not perform route discovery or maintenance until it needs a route to another node or it offers its services as an intermediate node
- Nodes that are not on active paths do not maintain routing information and do not participate in routing table exchanges
- Uses a broadcast route discovery mechanism
- **Hop-by-hop** protocol: intermediate nodes use lookup table to determine next hop based on destination
- Routes are based on dynamic table entries maintained at intermediate nodes
- Similar to Dynamic Source Routing (DSR), but DSR uses source routing

# AODV: Ad-hoc On-demand Distance Vector Routing

## Route Request (RREQ):

- Source broadcasts Route Request (RREQ) message for specified destination
- Intermediate node Forward message toward destination

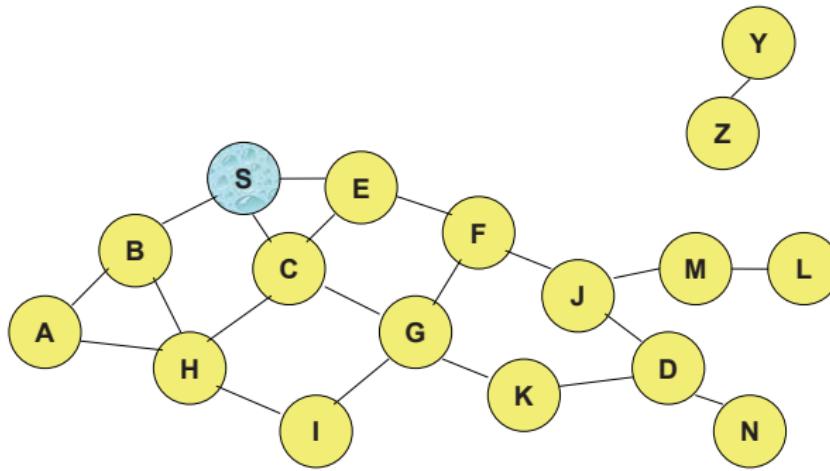
## Route Reply (RREP)

- Destination unicasts Route Reply msg to source
- Intermediate node create next-hop entry for destination and forward the reply
- If source receives multiple replies, uses one with lowest hop count

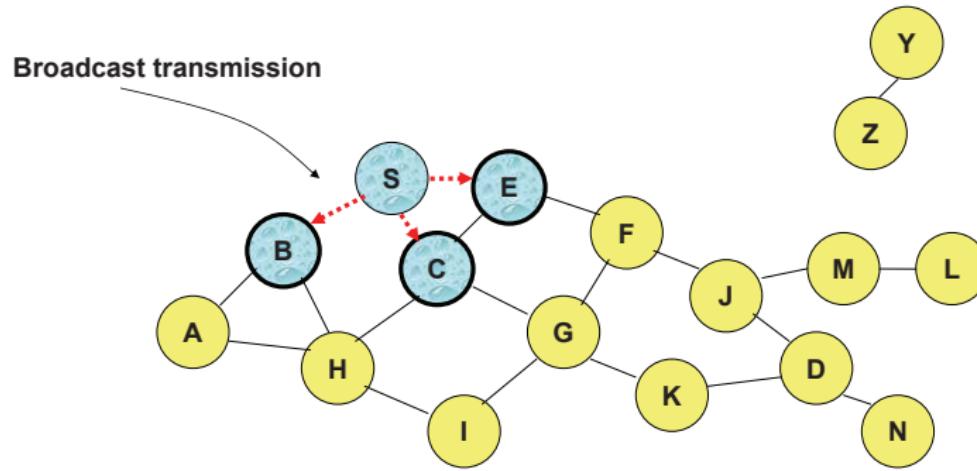
## Link breakage: Route Error (RERR)

- Contains list of unreachable destinations
- Sent to **precursors**: neighbors who recently sent packet which was forwarded over broken link

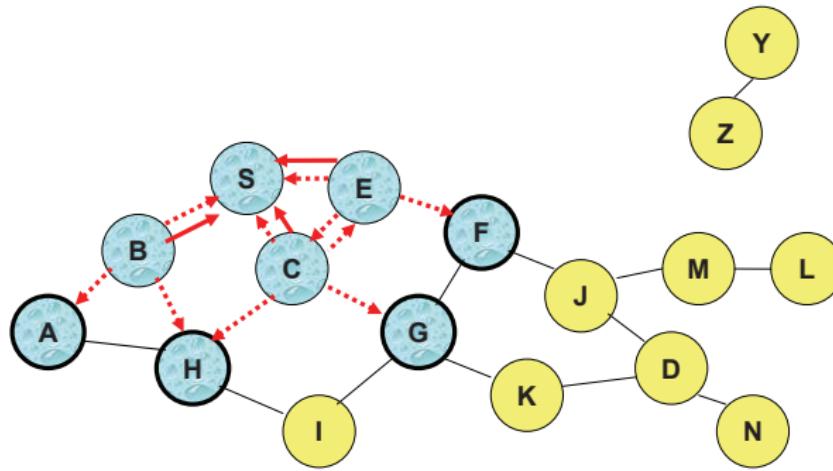
# AODV Messaging



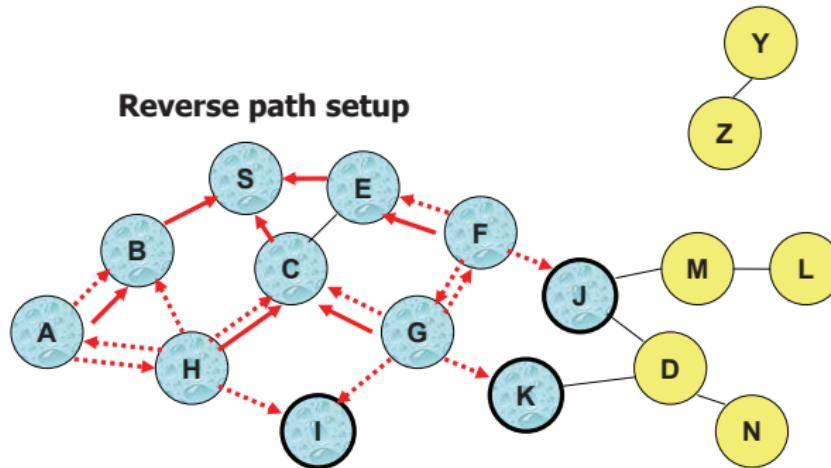
# AODV Messaging



## AODV Messaging

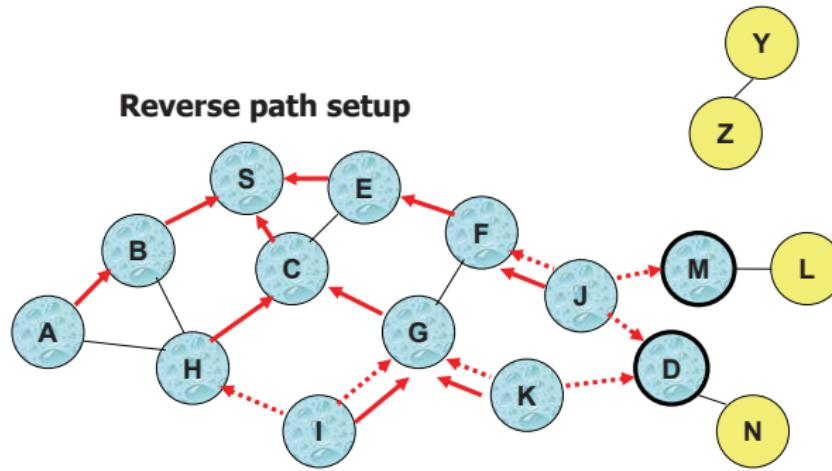


# AODV Messaging

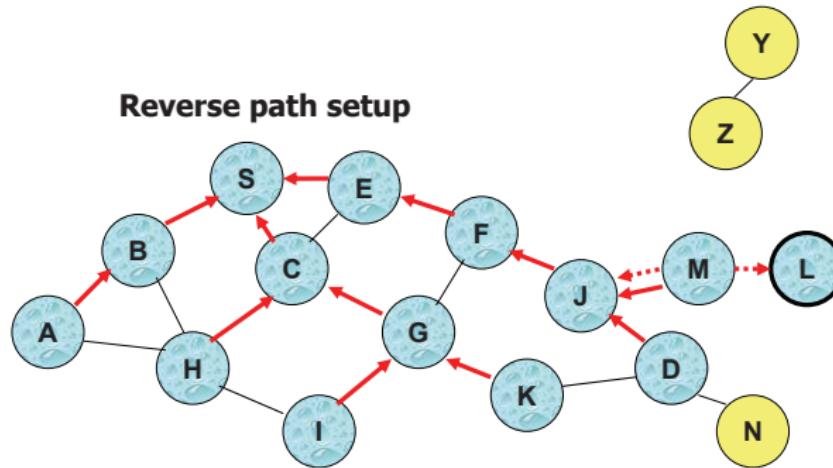


- Node C receives RREQ from G and H, but does not forward it again, because node C has **already forwarded RREQ once**

# AODV Messaging



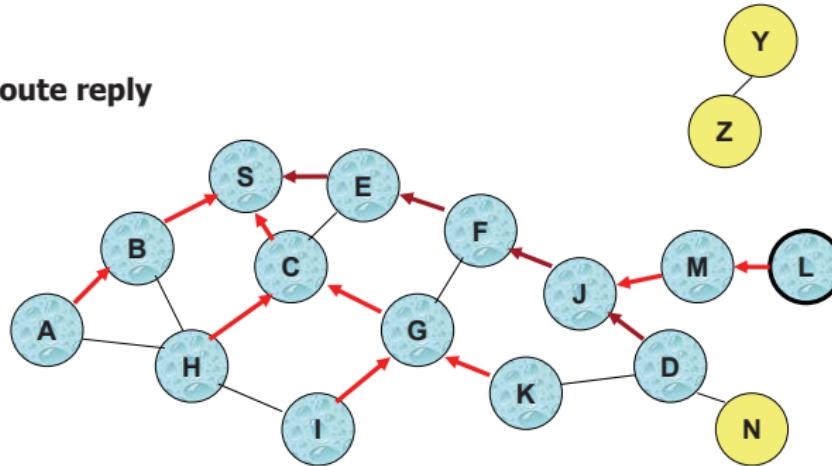
# AODV Messaging



- Node D **does not forward** RREQ, because node D is the **intended target** of the RREQ

# AODV Messaging

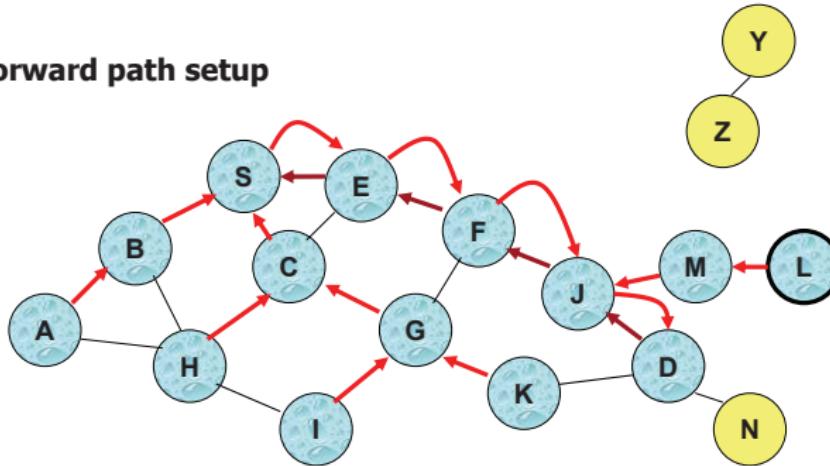
Route reply



← Represents links on path taken by RREP

# AODV Messaging

## Forward path setup

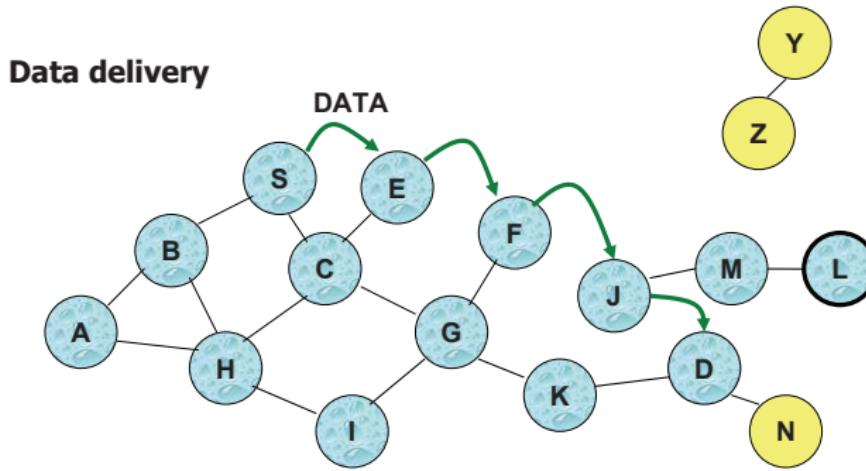


Forward links are setup when RREP travels along the reverse path



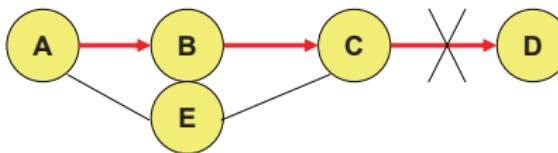
Represents a link on the forward path

# AODV Messaging



- Routing table entries used to forward data packet.
- Route is not included in packet header.

# AODV: Why sequence numbers?



To avoid old/broken routes and to prevent loops

Assume that A does not know about failure of link C-D because RERR sent by C is lost

Now C performs a route discovery for D. Node A receives the RREQ (say, via path C-E-A)

Node A will reply since A knows a route to D via node B

Results in a loop (for instance, C-E-A-B-C )

# AODV: Summary

- Routes need not be included in packet headers
- Nodes maintain routing tables containing entries only for routes that are in active use
- At most one next-hop per destination maintained at each node
- DSR may maintain several routes for a single destination
- Unused routes expire even if topology does not change

# Agenda

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols**
- 52 Hierarchical Routing Protocols

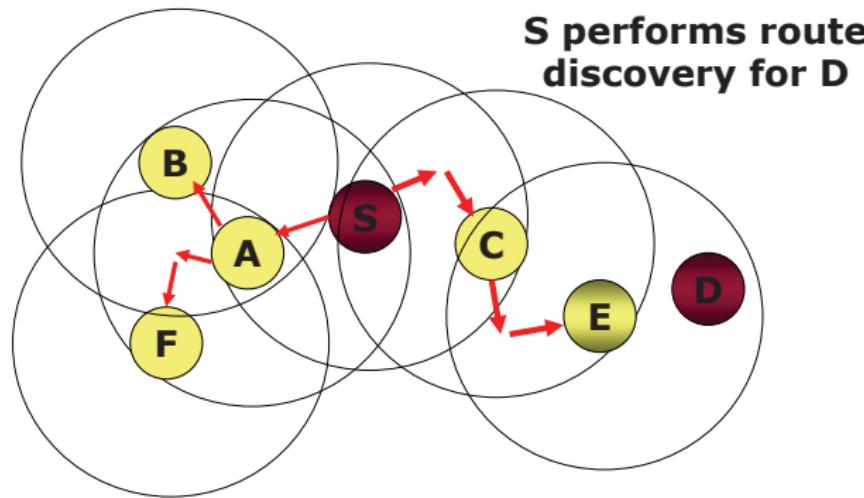
# Hybrid Routing Protocol, e.g., Zone Routing (ZRP)

Proactive protocol: which pro-actively updates network state and maintains route regardless of whether any data traffic exists or not

Reactive protocol: which only determines route to a destination if there is some data to be sent to the destination

# ZRP: Zone Routing Protocol

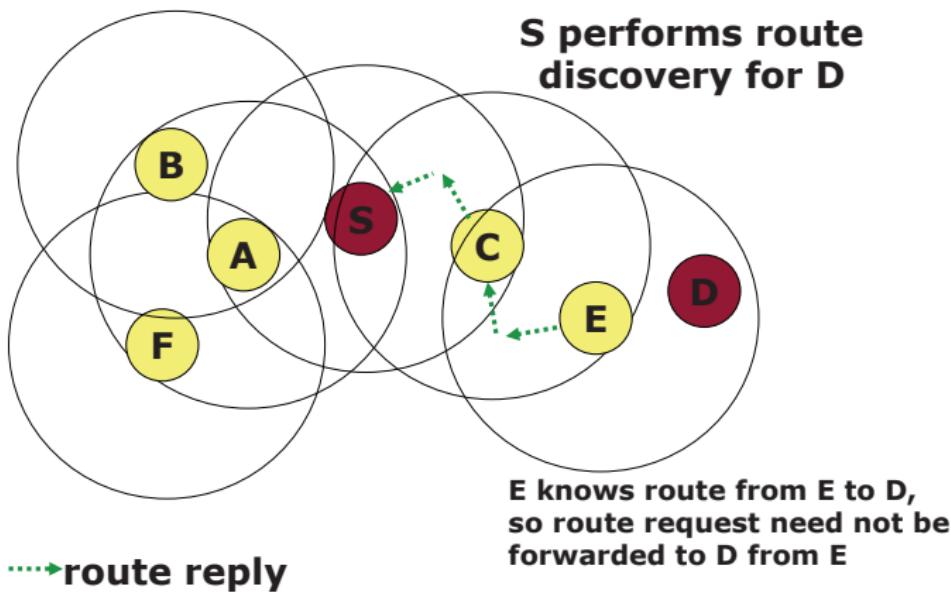
**Zone Radius =  $d = 2$**



→ Denotes route request

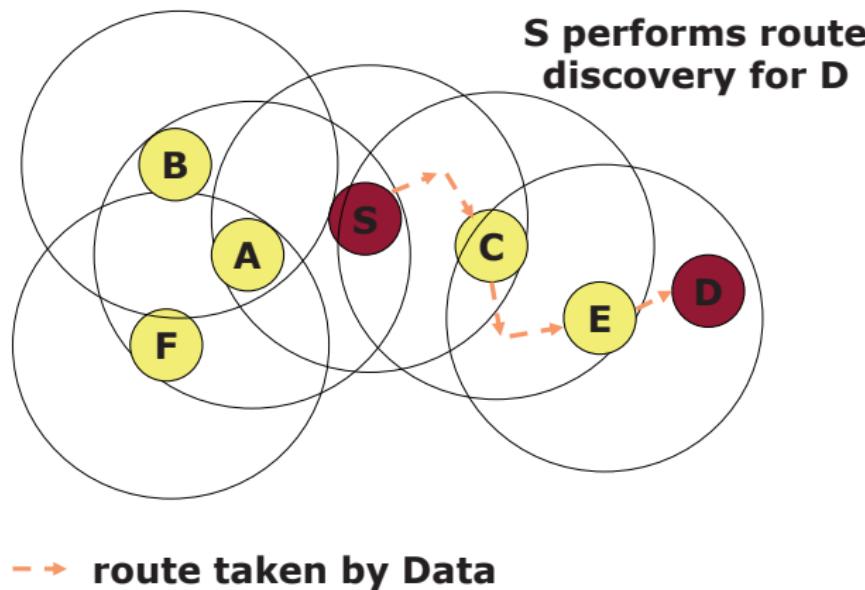
# ZRP: Zone Routing Protocol

## ZRP: Example with $d = 2$



# ZRP: Zone Routing Protocol

## ZRP: Example with $d = 2$



# Agenda

- 43 Introduction and Terminology
- 44 Legacy Routing Protocols
- 45 Requirements of Routing in Ad Hoc Networks
- 46 Classification of Ad Hoc Routing Protocols
- 47 DSDV: Destination Sequence Distance Vector
- 48 OLSR: Optimized Link State Routing
- 49 DSR: Dynamic Source Routing
- 50 AODV: Ad-hoc On-demand Distance Vector Routing
- 51 Hybrid Routing Protocols
- 52 Hierarchical Routing Protocols**

# Hierarchical Algorithms

Scalability: MANET protocols often do not perform well for large networks (especially if not dense)

- Global topology is based on the connectivity of each mobile node

Clusters can be used to provide scalability

- Clusters are formed (dynamically, of course) to provide hierarchy
- Global routing is done to clusters
- Local routing is done to nodes within a cluster
- Clusters of clusters (super-clusters) can be formed to extend hierarchy
- Similar in principle to IP subnets

# Hierarchical Algorithms

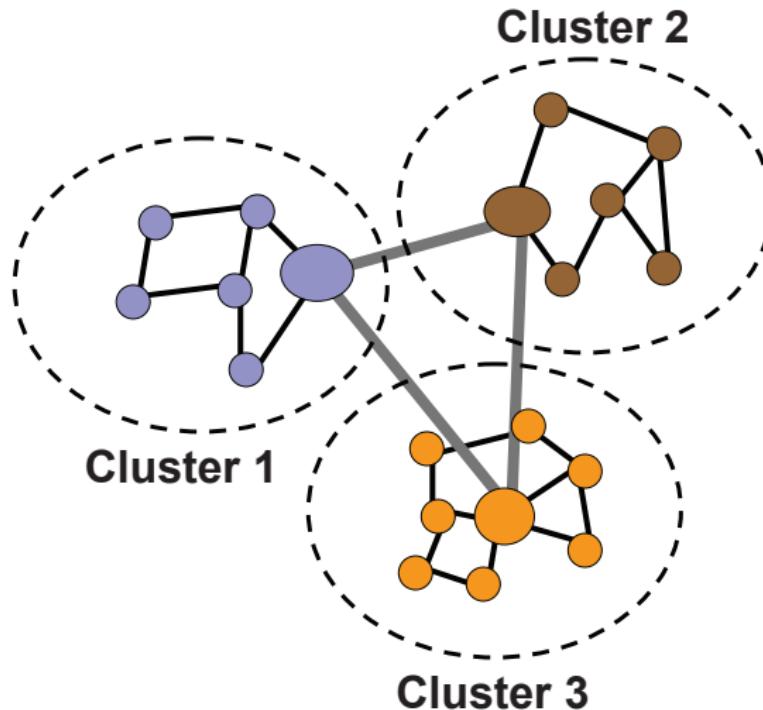
A special node, called the cluster-head, is designated in each cluster

- Responsible for routing data to or from other clusters
- May be a special node, or may be designated through a clustering algorithm

## Algorithms

- **Clustering**: form clusters
- **Cluster-head identification**: may be an integral part of the clustering algorithm
- **Routing**: some routing algorithm is still needed at each level of the hierarchy

# Hierarchical Algorithms Example



## Lecture 8: Multicast Routing

# Objectives

At the end of this lecture, you will be able to

- define the basic IP multicast service model,
- classify multicast protocols for ad hoc networks [1]
- describe tree- and mesh-based multicast approaches

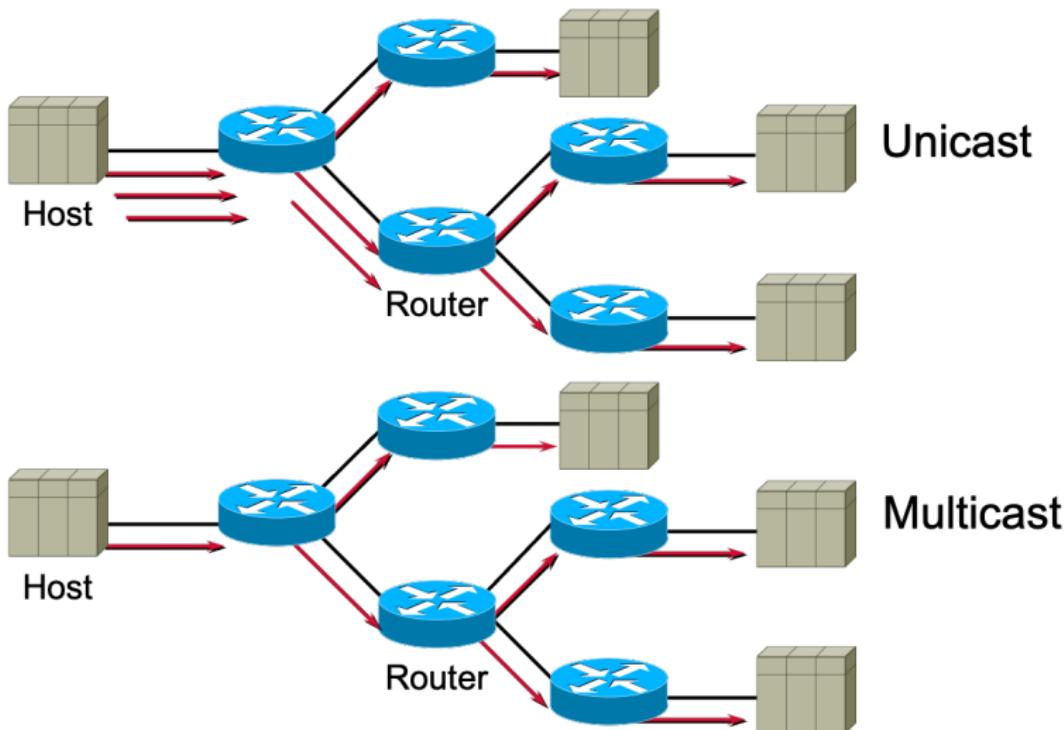
# Agenda

- 53 Introduction to Multicasting
- 54 Multicasting in Ad Hoc Networks
- 55 Operation of Multicast Routing Protocols
- 56 Cross-layer Reference Model for Multicast Routing
- 57 Classification of Multicast Routing Protocols
- 58 Tree-based Multicast Routing Protocols
- 59 Mesh-based Multicast Routing Protocols

# Why Multicast and Applications

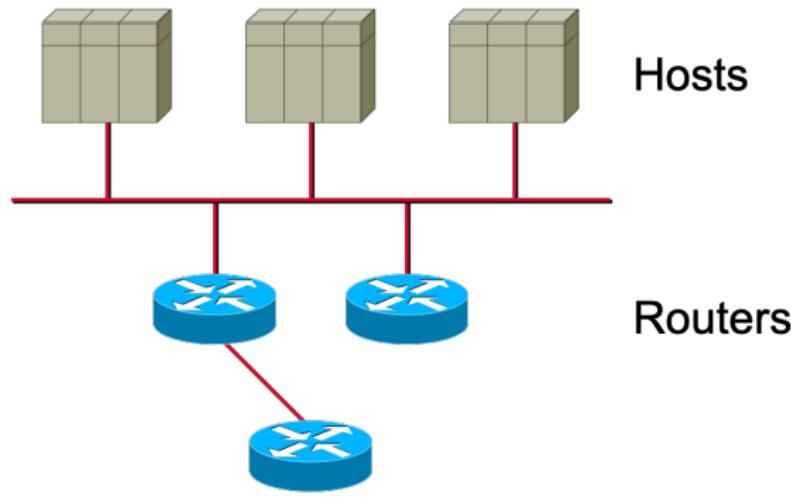
- Why multicast?
  - When sending same data to multiple receivers
  - Better bandwidth utilization
  - Lesser host/router processing
  - Receivers' addresses unknown
- Applications
  - Video/audio conferencing
  - Resource discovery/service advertisement
  - Stock distribution
  - Eg. IPTV

# What is Multicasting |



# IP Multicast Service Model I

Host-to-Router Protocols (IGMP)



Multicast Routing Protocols (PIM)

# IP Multicast Service Model II

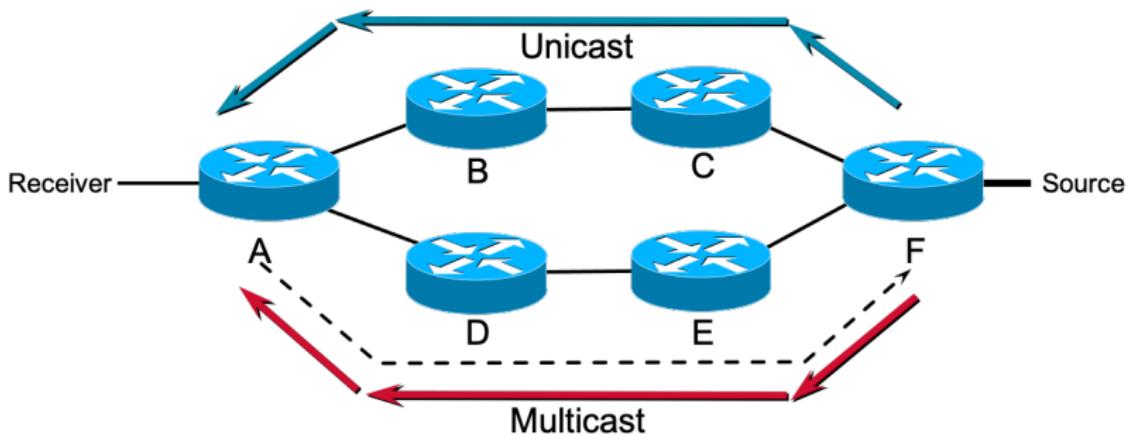
## Internet Group Management Protocol—IGMP

- How hosts tell routers about group membership
- Routers solicit group membership from directly connected hosts
- RFC 1112 specifies first version of IGMP
- IGMP v2 and IGMP v3 enhancements
- Supported on UNIX systems, PCs, and MAC
- Class D address, high-order 3 bits are set (224.0.0.0)
- 224.0.0.1: all multicast systems on subnet
- 224.0.0.2: all routers on subnet
- Low order 23 bits of IP address map into low order 23 bits of MAC address (e.g., 224.2.2.2 – 01005e.020202)

## IP Multicast Service Model III

## Multicast Routing Protocols (Reverse Path Forwarding)

- What is RPF? A router forwards a multicast datagram if received on the interface used to send unicast datagrams to the source

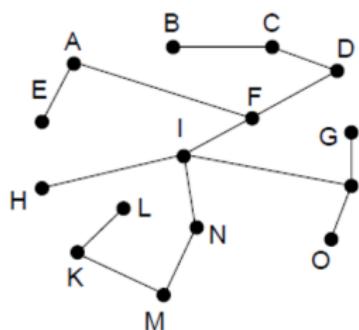
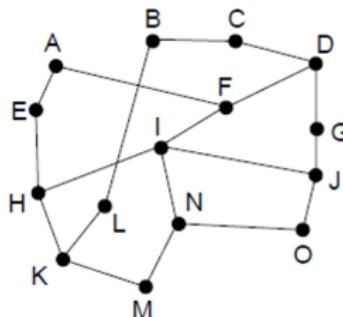


# Broadcast Routing

## Broadcast

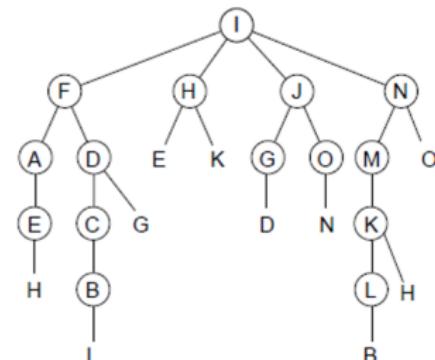
sends a packet to all nodes

- **Reverse Path Forwarding (RPF):** send broadcast received on the link to the source out all remaining links
- Alternatively, can build and use sink trees at all nodes



Network

Sink tree for I



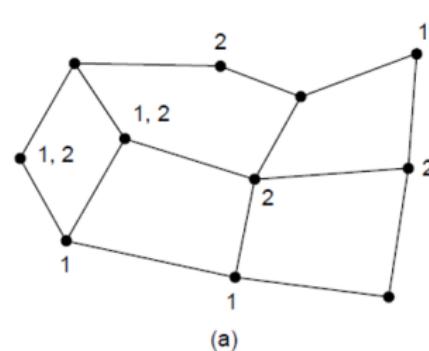
RPF from I

# Multicast Routing I

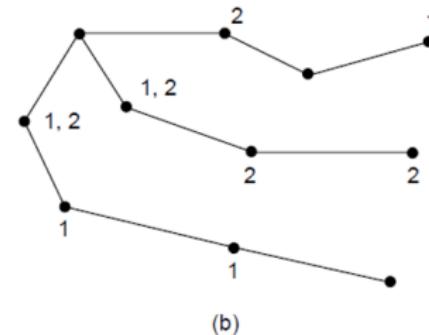
## Multicast

sends to a subset of the nodes called a group, establishes a sink or spanning tree for a group of nodes, uses a different tree for each group and source and then a multicast packet sent to all nodes in the group traverses each node and each link in the tree only once

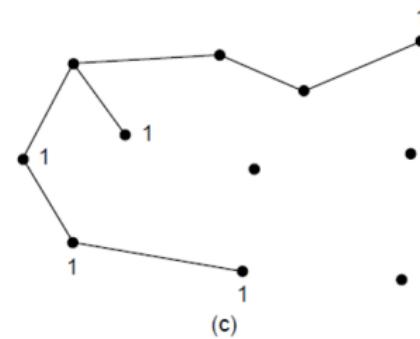
# Multicast Routing II



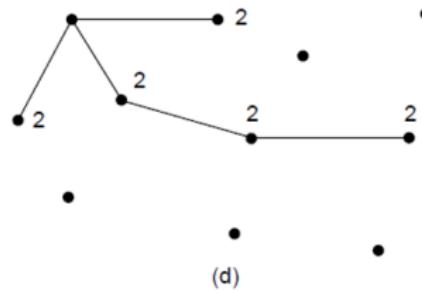
(a)



(b)



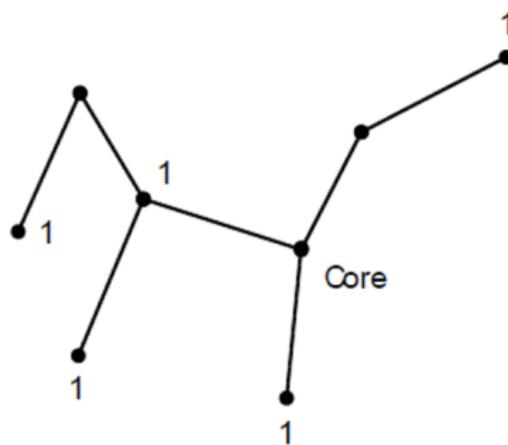
(c)



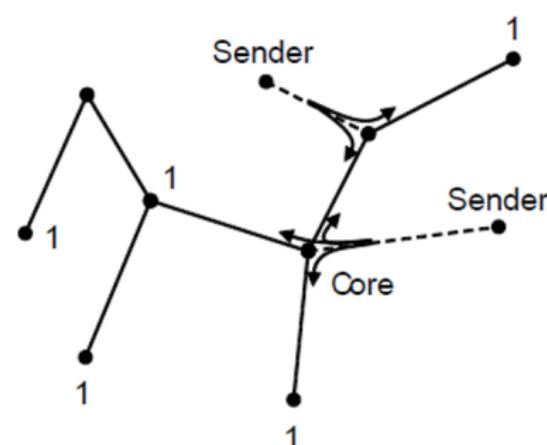
(d)

# Multicast Routing III

- Core-Based Tree (CBT) uses a single tree to multicast
- Tree is the sink tree from core node to group members
- Multicast heads to the core until it reaches the CBT



(a)



(b)

# Agenda

- 53 Introduction to Multicasting
- 54 **Multicasting in Ad Hoc Networks**
- 55 Operation of Multicast Routing Protocols
- 56 Cross-layer Reference Model for Multicast Routing
- 57 Classification of Multicast Routing Protocols
- 58 Tree-based Multicast Routing Protocols
- 59 Mesh-based Multicast Routing Protocols

# Why Not Legacy Protocols in Ad Hoc Networks I

Conventional IP multicast protocols will not work well

- Dynamic topology
- Low bandwidth
- Less reliable channels
- Long convergence times
- Transient routing loops

In a wired network, the basic approach is to establish a routing tree (acyclic connected graph consisting of nodes of the group), a packet sent traverses each node and link in the routing tree exactly once. Continuous topology changes will create many routing tree update packets and yield excessive control and processing overhead.

# Issues of Multicasting in Ad Hoc Networks I

- **Robustness:** a multicast routing protocol should be robust enough to sustain the mobility of the nodes and achieve a high packet delivery ratio under link failures.
- **Efficiency:** Multicast efficiency is defined as the ratio of the total number of data packets received by the receivers to the total number of (data and control) packets transmitted in the network.
- **Control overhead:** the total number of control packets transmitted for maintaining the multicast group is kept to a minimum.
- **Quality of service:** throughput, delay, jitter, and reliability
- **Dependency on the unicast routing protocol:** it is desirable if the multicast routing protocol is independent of any specific unicast routing protocol
- **Resource management:** use minimum power by reducing the number of packet transmissions. To reduce memory usage, it should use minimum state information.

# Agenda

- 53 Introduction to Multicasting
- 54 Multicasting in Ad Hoc Networks
- 55 Operation of Multicast Routing Protocols**
- 56 Cross-layer Reference Model for Multicast Routing
- 57 Classification of Multicast Routing Protocols
- 58 Tree-based Multicast Routing Protocols
- 59 Mesh-based Multicast Routing Protocols

# Operation of Multicast Routing Protocols I

Broad classification: source- or receiver-initiated

**Source-initiated:** source initiated tree construction

- **Soft-state maintenance:** Two-pass protocol. Multicast tree is updated periodically by control packets, source(s) of multicast group periodically floods **JoinReq** (request to join) propagated by all nodes and reaches to all receivers. Receivers may reply with **JoinRep** (join reply) propagated in the reverse path of Joinreq. JoinRep establishes state of interim routers. No route repair procedure.
- **Hard-state maintenance:** Similar to soft-state approach, but with a route repair procedure. The upstream node detecting failure of link to a downstream node, initiated the tree construction with a JoinReq.

# Operation of Multicast Routing Protocols II

**Receiver-initiated:** receiver uses flooding to search for paths to the source(s)

- **Soft-state maintenance:** Three-phase protocol. Receiver floods **JoinReq**. Sources and current receivers of the group can reply with **JoinRep**. **JoinRep** with smallest hop count is selected. **JoinAck** (**Join Acknowledgement**) is forwarded along reverse path of **JoinRep**. Route maintenance, receiver periodically floods **JoinReq**.
- **Hard-state maintenance:** Similar to soft-state approach, but with a route repair procedure. The downstream node initiates a **JoinReq** to repair a broken link.

# Agenda

- 53 Introduction to Multicasting
- 54 Multicasting in Ad Hoc Networks
- 55 Operation of Multicast Routing Protocols
- 56 Cross-layer Reference Model for Multicast Routing**
- 57 Classification of Multicast Routing Protocols
- 58 Tree-based Multicast Routing Protocols
- 59 Mesh-based Multicast Routing Protocols

# Cross-layer Reference Model for Multicast Routing I

## Medium Access Control:

- Channel access
- Neighbor discovery and health control

## Network Layer:

- Unicast routing information handler
- Multicast/group information handler
- Forwarding module
- Tree/mesh construction module
- Session maintenance module (route/tree repair)
- Route caching

## Application Layer:

- Packet transmit/receive controller
- Multicast session initiator/terminator

# Agenda

- 53 Introduction to Multicasting
- 54 Multicasting in Ad Hoc Networks
- 55 Operation of Multicast Routing Protocols
- 56 Cross-layer Reference Model for Multicast Routing
- 57 Classification of Multicast Routing Protocols**
- 58 Tree-based Multicast Routing Protocols
- 59 Mesh-based Multicast Routing Protocols

# Classification I

Based on application transparency:

- Application-independent
- Application-dependent

Application-independent can be classified based on topology

- Tree-based: single path between source and receiver, efficient
  - Source-tree based: Source is the root
  - Shared-tree based: A single tree is shared by various sources where a core node is the root
- Mesh-based: may be more than one path, robust,

# Classification II

Based on initiation of multicast session:

- Source-initiated
- Receiver-initiated

Based on topology maintenance mechanism:

- Soft-state: periodic control packets, high packet delivery ratio and high control overhead
- Hard-state: control packets generated when a link breaks, low packet delivery ratio and low overhead

# Agenda

- 53 Introduction to Multicasting
- 54 Multicasting in Ad Hoc Networks
- 55 Operation of Multicast Routing Protocols
- 56 Cross-layer Reference Model for Multicast Routing
- 57 Classification of Multicast Routing Protocols
- 58 Tree-based Multicast Routing Protocols**
- 59 Mesh-based Multicast Routing Protocols

# Tree-based Multicast Routing Protocols I

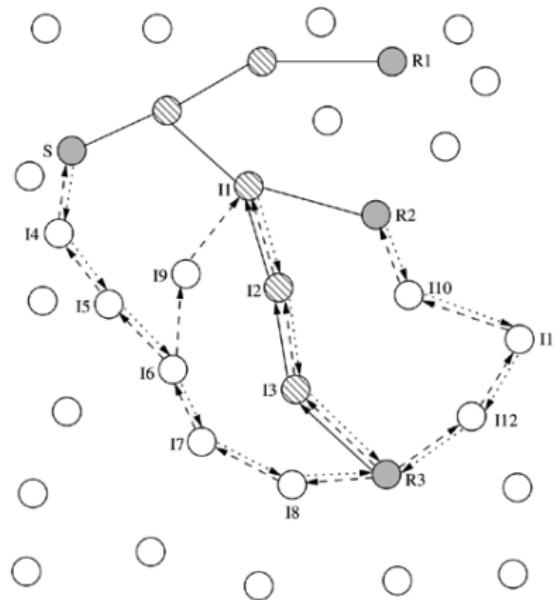
Tree-base: when the multicast group receivers are connected to source over a single path.

Criterion	Source-based tree	Shared tree
Number of trees	One per source	One per network
Scalability in source count	Less	More
Bandwidth req. in source count	more	less
Amount of state info	High	Lower

# Bandwidth-efficient Multicast Routing Protocol (BEMRP) I

- Find the nearest forwarding node instead of a path to source
- Hard-state approach is used: rejoin after a failure
- Avoids periodic control packet, hence bandwidth-efficient
- Tree initialization phase
  - Receivers initiate, floods *join* packet
  - Forwarders respond with *reply* packet
  - Receiver selects a reply and sends a reserve packet
  - Smallest hop count is used to break tie if multiple *join* or *reply* packets are received.
  - Tree configuration is done on a link break

# Bandwidth-eff Multicast Routing Protocol (BEMRP) II

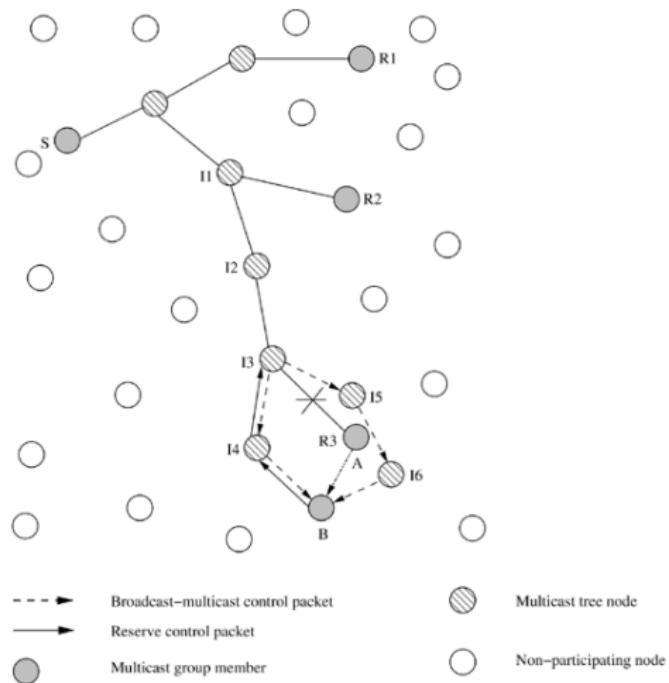


## Tree construction

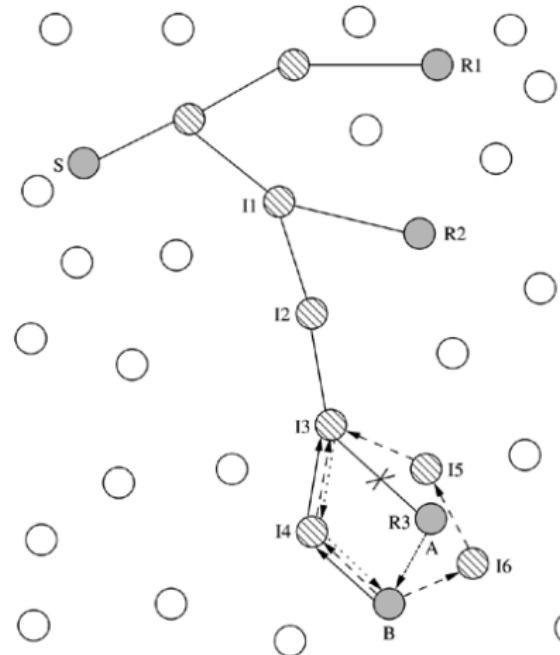
- Join control packet
- Reply control packet
- Reserve control packet
- Multicast tree node
- Multicast group member
- Non-participating node

# Bandwidth-eff Multicast Routing Protocol (BEMRP) III

Broadcast multicast scheme, R3 moves from A to B



# Bandwidth-eff Multicast Routing Protocol (BEMRP) IV

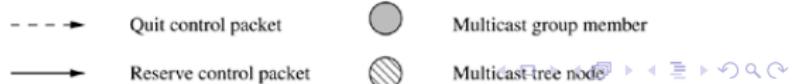
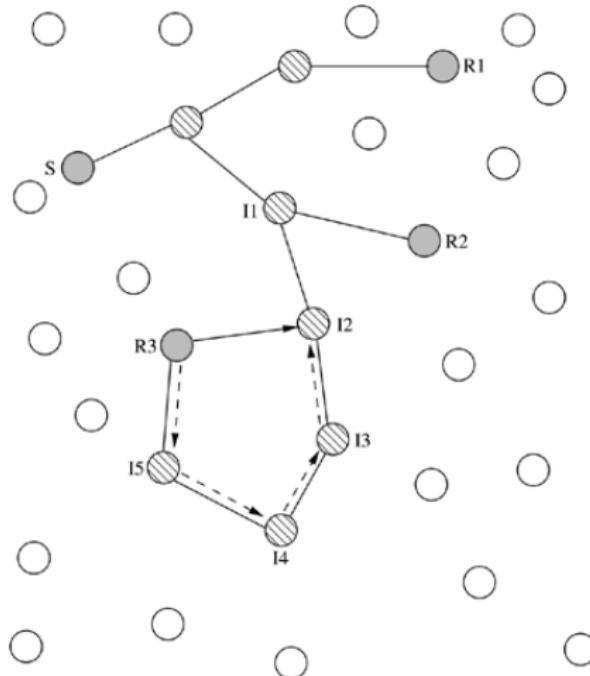


Local rejoin scheme:

- Join control packet
  - Reply control packet
  - Reserve control packet
- Multicast tree node
  - Multicast group member
  - Non-participating node

# Bandwidth-eff Multicast Routing Protocol (BEMRP) V

**Prunning:** when a tree node or receiver gets in the coverage of other tree nodes  
When a node receives a multicast packet from another node quicker.

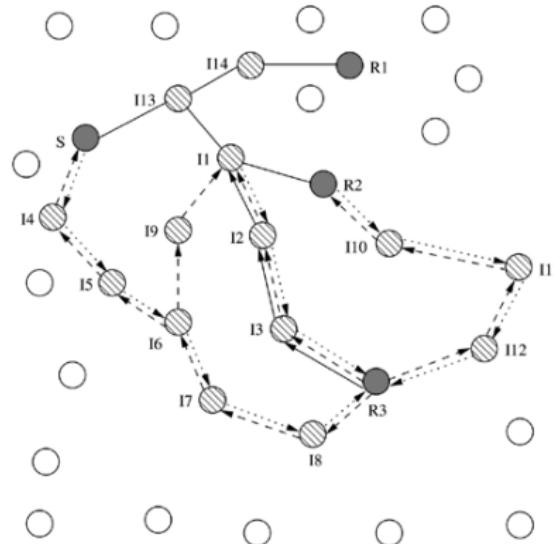


# Multicast Ad Hoc On Demand DV Routing (MAODV) I

- Extension of AODV for multicast (+broad- and uni-cast)
- Sequence numbers ensure freshness
- Group leader (first node joining the group) updates sequence number and broadcasts using group hellos (GRPH)
- Nodes join by a unicast RREQ to group leader (if leader known)
- Nodes join by a broadcast RREQ if leader is not known
- RREP (seq, distance) unicast by a member of group on getting a RREQ
- Most recent and shortest member is selected and multicast activation (MACT) is sent (interim nodes understand participating in tree)

# Multicast Ad Hoc On Demand DV Routing (MAODV) II

## Construction



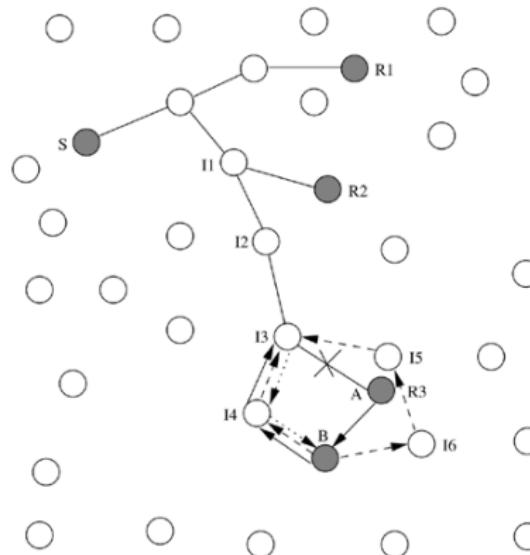
- Multicast group member → RREQ control packet
- Multicast tree node → RREP control packet
- Non-participating node → MACT control packet

# Multicast Ad Hoc On Demand DV Routing (MAODV) III

- Tree maintenance: **expanding ring search** using RREQ, RREP, MACT
- Downstream node issues a fresh RREQ (hop count to leader, last seq)
- RREQ is answered by members having a fresher ( $\{seq\}$ ) sequence number and a smaller hop count to leader
- Member who leaves sends a PRUNE message upstream
- Any node hearing a GRPH, initiates leader election to have a single leader

# Multicast Ad Hoc On Demand DV Routing (MAODV) IV

Maintenance, R3 moves from A to B



# Multicast Ad Hoc On Demand DV Routing (MAODV) V

- unicast and multicast route discovery unified which reduces overhead
- free from loops
- poor packet delivery under mobility
- congestion along the upstream members of the tree
- a shared tree is used
- single point of failure

# Agenda

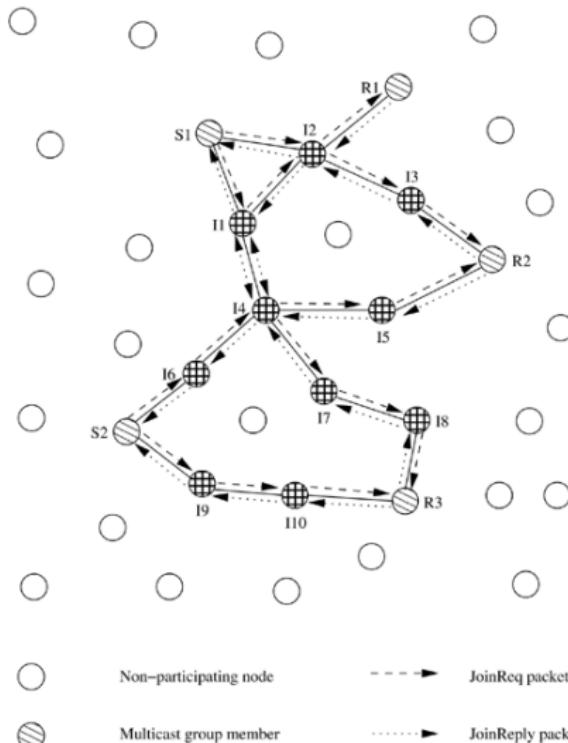
- 53 Introduction to Multicasting
- 54 Multicasting in Ad Hoc Networks
- 55 Operation of Multicast Routing Protocols
- 56 Cross-layer Reference Model for Multicast Routing
- 57 Classification of Multicast Routing Protocols
- 58 Tree-based Multicast Routing Protocols
- 59 Mesh-based Multicast Routing Protocols

# On-demand Multicast Routing Protocol (ODMRP) I

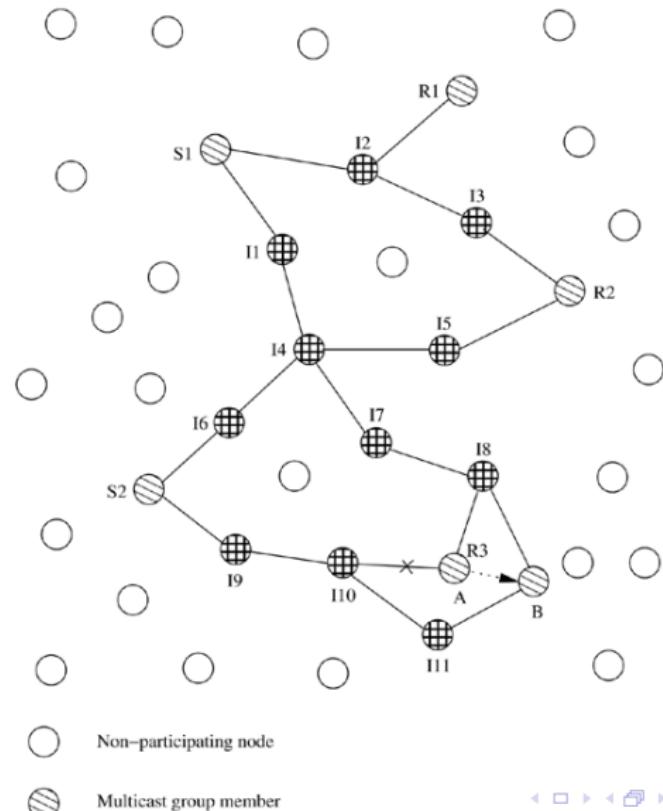
- a **mesh** is formed by forwarding nodes between sources and receivers
- forwarding nodes keep message-cache to detect duplicate packets and JoinReq
- sources flood JoinReq periodically
- receivers send JoinReply using reverse shortest path
- interim nodes receiving JoinReply become a forwarder in mesh
- soft-state maintenance is employed, robust but high overhead
- disadvantage: increased number of packet transmissions (since more than one path), reduced multicast efficiency

# On-demand Multicast Routing Protocol (ODMRP) II

## Maintenance



# On-demand Multicast Routing Protocol (ODMRP) III



# Summary I

- Multicast in wired networks
- Difference in ad hoc networks
- Multicast approaches (tree vs mesh) in ad hoc networks
- BEMRP, MAODV, ODMRP

## Lecture 9: Transport Layer

# Objectives

At the end of this lecture, you will be able to

- discuss the classical transmission control protocol,
- discuss the issues in designing a transport layer protocol for ad hoc networks [1],
- classify the transport layer protocols designed for ad hoc networks,
- to discuss some example transport layer implementations in ad hoc networks.

# Agenda

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)
- 62 Transport Layer in Ad Hoc Networks
- 63 Classification
- 64 Feedback-Based TCP
- 65 TCP with Explicit Link Failure Notification
- 66 Split TCP
- 67 Ad Hoc Transport Protocol (ATP)

# Transport Services and Protocols

- provide **logical communication** between application processes running on different hosts
- transport protocols run in end systems (in classical systems)
  - sender: breaks application messages into segments, passes to network layer
  - receiver: reassembles segments into messages, passes to application layer

# Transport Services and Protocols

- reliable, in-order delivery (TCP)
  - congestion control
  - flow control
  - connection setup
- unreliable, unordered delivery (UDP)
  - no-frills extension of "best-effort" IP
- services not available:
  - delay guarantees
  - bandwidth guarantees

# Three Important Functions of Transport Layer Protocol

will be the focus in this lecture

- **flow control**: do not send faster than the receiver can handle
- **end-to-end reliability**: send packets with no bit errors, no packet losses, and in-order delivery of packets
- **congestion control**: do not send faster than the network can handle

# Agenda

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)**
- 62 Transport Layer in Ad Hoc Networks
- 63 Classification
- 64 Feedback-Based TCP
- 65 TCP with Explicit Link Failure Notification
- 66 Split TCP
- 67 Ad Hoc Transport Protocol (ATP)

# Transmission Control Protocol (TCP)

Introduction (RFCs: 793,1122,1323, 2018, 2581)

- **point-to-point**: one sender, one receiver
- **reliable, in-order byte stream**: no "message boundaries"
- **pipelined**: TCP congestion and flow control set window size
- **full duplex data**: bi-directional data flow in same connection
- **connection-oriented**: handshaking (exchange of control msgs) inits sender, receiver state before data exchange
- **flow controlled**: sender will not overwhelm receiver

# Transmission Control Protocol (TCP) I

- byte-stream protocol: cumulative ACK with next expected octet number
- counts bytes not packets
- **credit-based flow control**: advertised window set by the destination
- flow window (f wnd): number of unacked bytes the source can send to the destination based on empty buffer space of destination
- **congestion control**: number of packets within the Internet kept below the level at which network performance drops significantly
- congestion window (c wnd) number of unacked bytes source can send based on congestion in network
- Manifestation: **lost packets** (buffer overflow at routers) or **long delays** (queueing in router buffers)
- implicit congestion control: timer expiry (high congestion) and 3DUPACK (mediocre congestion)
- Approach: slow start (SS), congestion avoidance (CA), fast retransmit (FR)

# Transmission Control Protocol (TCP) II

## Slow start (SS)

- $cwnd = 1$ , for each ACK  $cwnd ++$  (assume counting packets not bytes)
- $cwnd = 1, 2, 4, 8, \dots$  until  $ssthresh$ , exponential increase
- starts slowly, but probes exponentially fast
- when  $cwnd \geq ssthresh$ , move to Congestion Avoidance (CA)
- at any state, timer expires: move back to SS ( $ssthresh=cwnd/2$ ,  $cwnd=1$ )
- at any state, 3DUPACK:  $\frac{1}{2}cwnd$  move to Fast Recovery (FR)

# Transmission Control Protocol (TCP) III

## Congestion Avoidance (CA)

- for fairness,  $cwnd++$  FOR ALL ACKS in a window
- at any state, timer expires: move back to SS ( $ssthresh=cwnd/2$ ,  $cwnd=1$ )
- at any state, 3DUPACK:  $\frac{1}{2}cwnd$  move to Fast Recovery (FR)

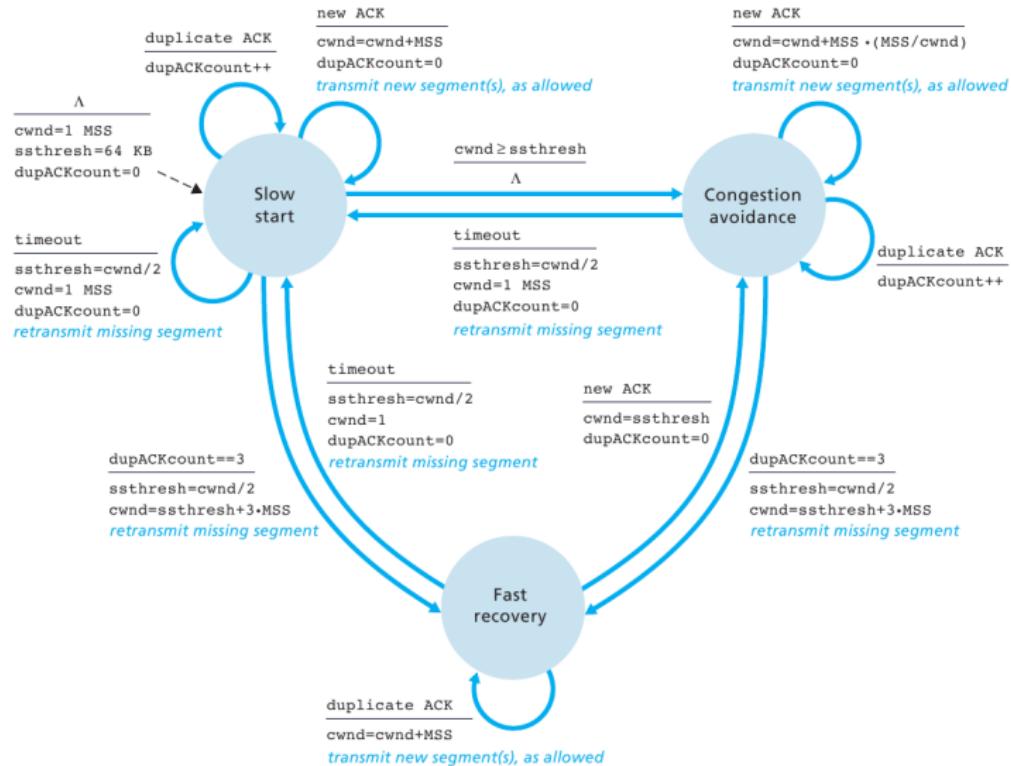
## Fast Recovery (FR) (in TCP Reno)

- On a new ACK return back to previous congestion state (SS or CA)
- at any state, timer expires: move back to SS ( $ssthresh=cwnd/2$ ,  $cwnd=1$ )

**AIMD:** Additive increase of  $cwnd$  in CA and multiplicative decrease of  $cwnd$  in FR help share capacity fairly

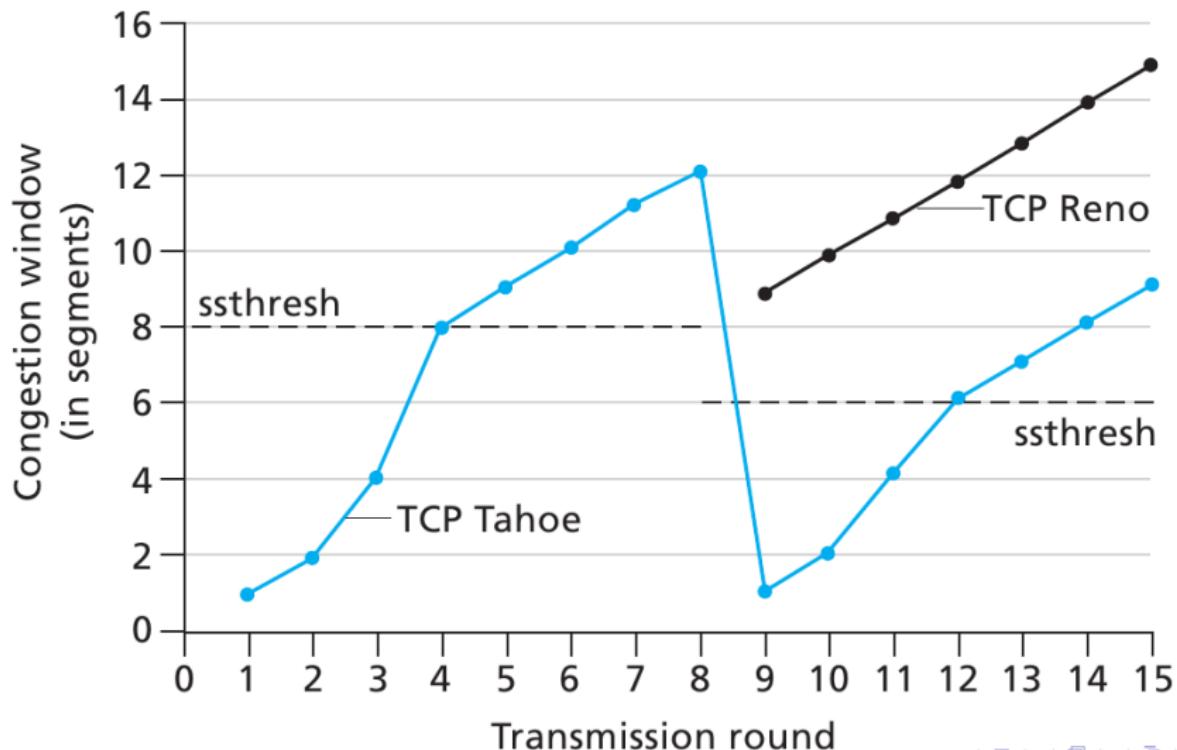
# TCP Congestion Control

## TCP Congestion Control



# TCP Congestion Control

## Evolution of TCP's Congestion Window



# Transmission Control Protocol (TCP)

Round Trip Time, Timeout

## How to set TCP timeout value?

- longer than RTT but RTT varies
- too short: premature timeout, unnecessary retransmissions
- too long: slow reaction to segment loss

## How to estimate RTT?

- SampleRTT: measured time from segment transmission until ACK receipt, ignore retransmissions
- SampleRTT will vary, want estimated RTT "smoother": average several recent measurements, not just current SampleRTT

$$\text{EstimatedRTT} = (1 - \alpha) \text{ EstimatedRTT} + \alpha \text{ SampleRTT}$$

$$\text{DevRTT} = (1 - \beta) \text{ DevRTT} + \beta |\text{SampleRTT} - \text{EstimatedRTT}|$$

$$\text{TimeoutInterval} = \text{EstimatedRTT} + 4 \text{ DevRTT}$$

# Agenda

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)
- 62 Transport Layer in Ad Hoc Networks**
- 63 Classification
- 64 Feedback-Based TCP
- 65 TCP with Explicit Link Failure Notification
- 66 Split TCP
- 67 Ad Hoc Transport Protocol (ATP)

# Issues

- **Induced traffic:** broadcast channel and local contention, a link-level transmission affects the neighbor nodes of both the sender and receiver of the link; forward data packets induce backward ack packets
- **Induced throughput unfairness:** throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layers such as the network and MAC layers
- **Separation of congestion control, reliability, and flow control:** Reliability and flow control are end-to-end activities, whereas congestion can at times be a local activity, these may have to be handled separately
- **Power and bandwidth constraints**
- **Misinterpretation of congestion:** Traditional mechanisms of detecting congestion in networks, such as packet loss and retransmission timeout, are not suitable because of error rates of wireless channel, location-dependent contention, hidden terminal problem, packet collisions, path breaks due to mobility, and node failure due to a drained battery
- **Completely decoupled transport layer:** cross-layer is required for adaptation to changing context
- **Dynamic topology:** frequent path breaks, partitioning and remerging of



# Design Goals I

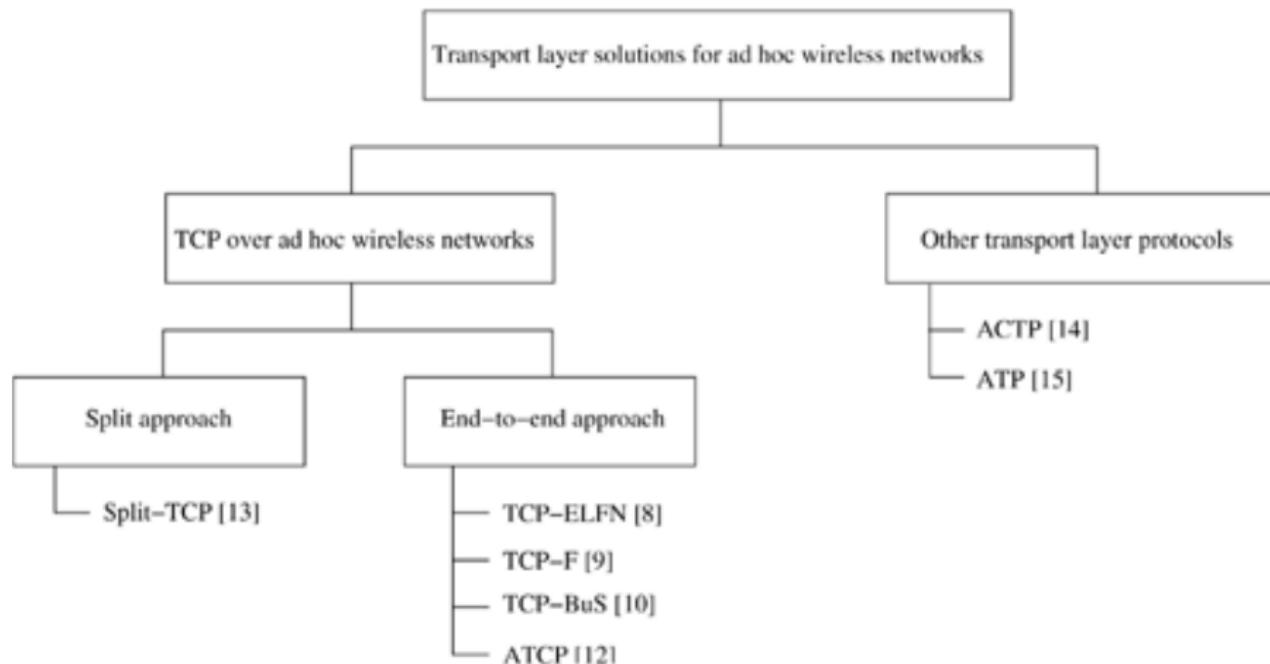
The transport layer protocol should ...

- maximize the throughput per connection.
- provide throughput fairness across contending flows.
- incur minimum connection setup and connection maintenance overheads
- minimize the resource requirements for scalability
- have mechanisms for congestion control and flow control in the network.
- provide reliable connections and unreliable transport
- be able to adapt to the dynamics of the network
- use bandwidth efficiently.
- be aware of resource constraints (battery power, buffer size, CPU...)
- make use of information from the lower layers to improve throughput.
- have a well-defined cross-layer interaction framework for effective, scalable, and protocol-independent interaction with lower layers.
- maintain end-to-end semantics

# Agenda

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)
- 62 Transport Layer in Ad Hoc Networks
- 63 Classification**
- 64 Feedback-Based TCP
- 65 TCP with Explicit Link Failure Notification
- 66 Split TCP
- 67 Ad Hoc Transport Protocol (ATP)

# Classification



# Why Does TCP Not Perform Well in MANETs? I

- **Misinterpretation of packet loss:** Traditional TCP was designed for wired networks where the packet loss is mainly attributed to network congestion. Ad hoc wireless networks experience a much higher packet loss due to factors such as high bit error rate (BER) in the wireless channel, increased collisions due to the presence of hidden terminals, presence of interference, location-dependent contention, uni-directional links, frequent path breaks due to mobility of nodes, and the inherent fading properties of the wireless channel.
- **Frequent path breaks:** Once a path is broken, the routing protocol initiates a route reestablishment process. This route reestablishment process takes a significant amount of time to obtain a new route to the destination. The route reestablishment time is a function of the number of nodes in the network, transmission ranges of nodes, current topology of the network, bandwidth of the channel, traffic load in the network, and the nature of the routing protocol. If the route reestablishment time is greater than the timeout period, TCP will assume congestion which is not the case.

# Why Does TCP Not Perform Well in MANETs? II

- **Effect of path length:** It is found that the TCP throughput degrades rapidly with an increase in path length in string (linear chain) topology ad hoc wireless networks. The possibility of a path break increases with path length.
- **Misinterpretation of congestion window:** the congestion window may not reflect the maximum transmission rate acceptable to the network and the receiver.
- **Asymmetric link behavior:** The directional links can result in delivery of a packet to a node, but failure in the delivery of the acknowledgment back to the sender.
- **Uni-directional path:** RTS-CTS-DATA-ACK on the reverse path for ACK packets is too overwhelming. Forward and reverse paths may contend.
- **Multipath routing:** out-of-order packets because of multi-path routing, which in turn generates a set of duplicate acknowledgments (DUPACKs) which cause additional power consumption and invocation of congestion control.

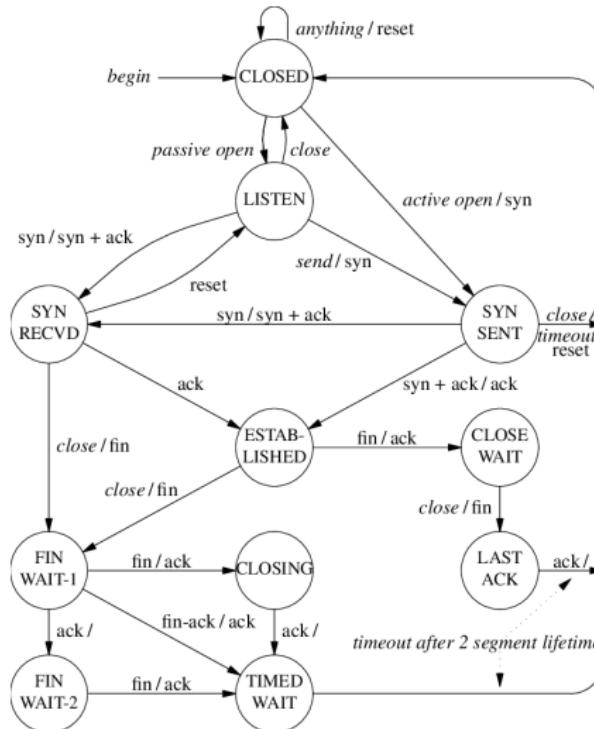
# Agenda

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)
- 62 Transport Layer in Ad Hoc Networks
- 63 Classification
- 64 Feedback-Based TCP**
- 65 TCP with Explicit Link Failure Notification
- 66 Split TCP
- 67 Ad Hoc Transport Protocol (ATP)

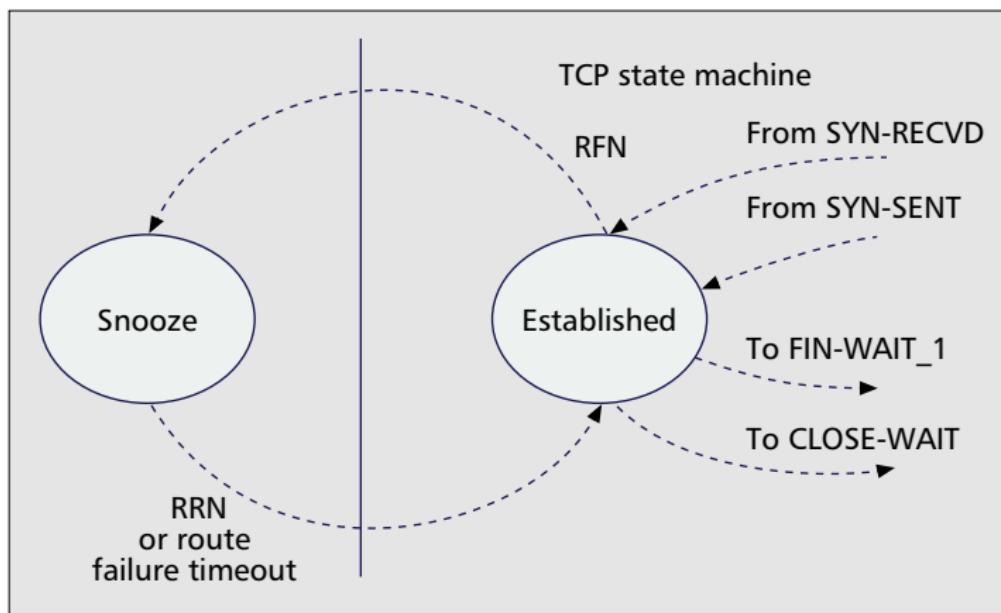
# Feedback-Based TCP [15] I

- Modified TCP with feedback from network layer
- Requires reliable link layer
- Expectation: routing protocol repairs broken link quickly
- Objective: minimize the throughput degradation resulting from the frequent path breaks
- Upon detection of packet loss, the TCP-F sender invokes congestion control algorithm leading to the exponential back-off of retransmission timers and a decrease in congestion window size.
- Undesirable actions of TCP
  - When there is no route available, there is no need to retransmit packets that will not reach the destination.
  - Packet retransmission wastes precious battery power and scarce bandwidth.
  - In the period immediately following the restoration of the route, the throughput will be unnecessarily low as a result of the slow start recovery mechanism, even though there may be no congestion in the network.

# Feedback-Based TCP [15] II



# Feedback-Based TCP [15] III



# Feedback-Based TCP [15] IV

## Separation of functions

treating route failure as congestion (and invoking congestion control) is not advisable because congestion and route failure are disparate phenomena which have to be handled independently and separately.

## Idea of TCP-F

the source is informed of the route failure so that it does not unnecessarily invoke congestion control and can refrain from sending any further packets until the route is restored.

# Feedback-Based TCP [15] V

- On Route Failure Notification (RFN)
  - Snooze: Stop sending any packets (new or retransmissions)
  - Marks all of its existing timers as invalid
  - Freezes the send window of packets
  - Freezes values of other state variables such as retransmit timer value and window size
  - Starts a route failure timer which corresponds to a worst case route reestablishment time
- On Route Reestablishment Notification (RRN)
  - changes to an active state from the snooze state
  - flushes out all unacknowledged packets in its current window
  - resumes at the same rate as before the route failure occurred
  - TCP's congestion control mechanism can now take over

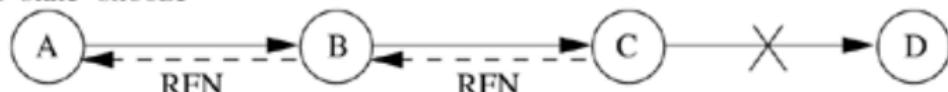
# Feedback-Based TCP [15] VI

TCP state=connected



(a) TCP-F connection from A to D

TCP state=snooze



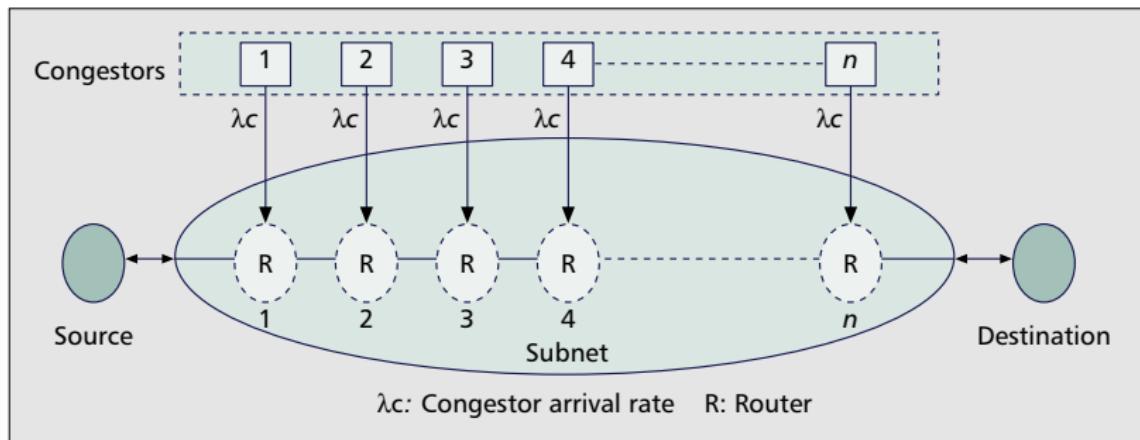
(b) Link C-D breaks and C originates RFN

TCP state=connected



(c) Link C-D rejoins and C originates RRN

# Feedback-Based TCP [15] VII



# Feedback-Based TCP [15] VIII

Further points to be addressed:

- overhead on routers
- effect of multiple failures on the same route
- effect of congestion on the feedback mechanism
- effect of failure on multiple transport connections

# Agenda

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)
- 62 Transport Layer in Ad Hoc Networks
- 63 Classification
- 64 Feedback-Based TCP
- 65 TCP with Explicit Link Failure Notification**
- 66 Split TCP
- 67 Ad Hoc Transport Protocol (ATP)

# TCP with Explicit Link Failure Notification [16]

- similar to TCP-F, except for the handling of explicit link failure notification (ELFN)
  - ICMP destination unreachable packet, or
  - piggybacking to route error packet
- probe packets check whether a route is established
- decouples the path break information from the congestion information by the use of ELFN
- less dependent on the routing protocol
- in a partitioned network (long route establishment), too many probe packets
- congestion window used after a new route is obtained may not reflect the achievable transmission rate

# Agenda

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)
- 62 Transport Layer in Ad Hoc Networks
- 63 Classification
- 64 Feedback-Based TCP
- 65 TCP with Explicit Link Failure Notification
- 66 Split TCP**
- 67 Ad Hoc Transport Protocol (ATP)

# Split TCP [17] I

- **problem:** degradation of throughput with increasing path length
- **channel capture effect:** leads to certain flows capturing the channel for longer time durations, thereby reducing throughput for other flows
- Split-TCP [17] provides a unique solution to this problem by splitting the transport layer objectives into congestion control and end-to-end reliability.

## Split TCP [17] II

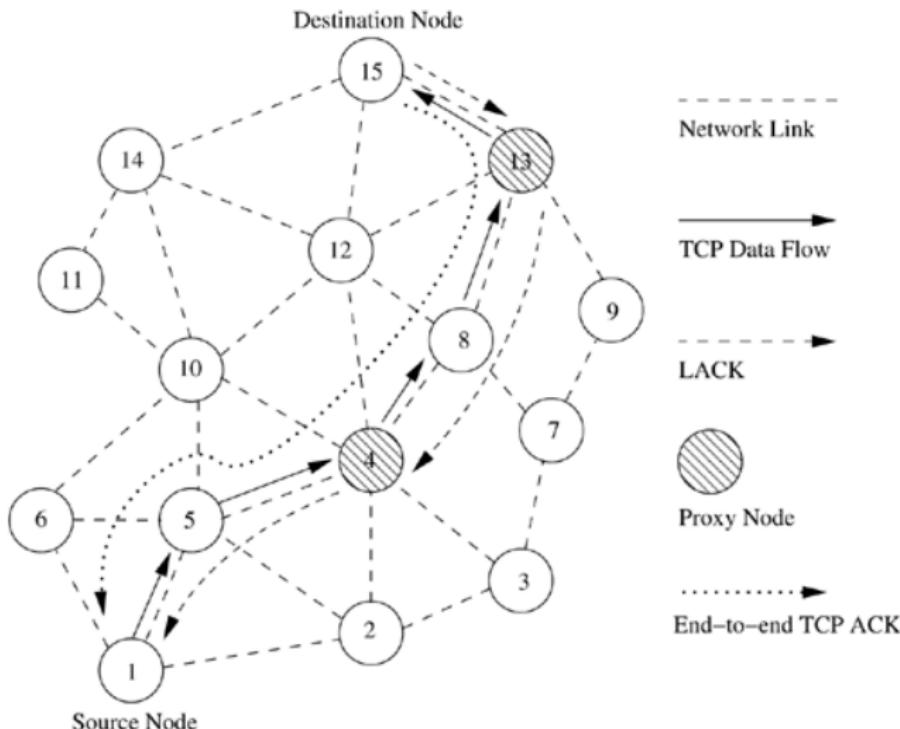
### Split1: Separation of congestion control and end-to-end reliability

The **congestion control** is mostly a local phenomenon due to the result of high contention and high traffic load in a local region. This demands local solutions. **Reliability** is an end-to-end requirement and needs end-to-end acknowledgments.

### Split2: Concatenate short path to form the long path

Split-TCP splits a **long** TCP connection into a set of **short** concatenated TCP connections (called segments or zones) with a number of selected intermediate nodes (known as **proxy nodes**) as terminating points of these short connections.

## Split TCP [17] III



- a **proxy node** receives the TCP packets, reads its contents, stores it in its

# Agenda

- 60 Introduction to Transport Layer
- 61 Recap of Transmission Control Protocol (TCP)
- 62 Transport Layer in Ad Hoc Networks
- 63 Classification
- 64 Feedback-Based TCP
- 65 TCP with Explicit Link Failure Notification
- 66 Split TCP
- 67 Ad Hoc Transport Protocol (ATP)**

# Ad Hoc Transport Protocol (ATP) [18] I

- Not a variant of TCP
- The major aspects by which ATP defers from TCP are
  - coordination among multiple layers,
  - **rate-based** transmissions,
  - decoupling congestion control and reliability, and
  - assisted congestion control.
- ATP uses services from network and MAC layers for improving its performance
- ATP uses information from lower layers for
  - estimation of the initial transmission rate,
  - detection, avoidance, and control of congestion, and
  - detection of path breaks.
- unlike TCP, ATP utilizes a **timer-based transmission**, where the transmission rate is decided by the granularity of the timer which is dependent on the congestion in the network.

# Ad Hoc Transport Protocol (ATP) [18] II

- congestion control mechanism is decoupled from the reliability and flow control mechanisms.
- network congestion information is obtained from the intermediate nodes, whereas the flow control and reliability information are obtained from the ATP receiver.
- intermediate nodes attach the **congestion information** to every ATP packet and the ATP receiver collates it before including it in the next ACK packet.
- congestion information is expressed in terms of the **weighted averaged queuing delay** and **contention delay** experienced by the packets at every intermediate node (**rate feedback field** of packets)
- receivers collate congestion info and conveys back to source in selective-ACK (SACK)
- after a path break, **Quick-start**: Source probes, intermediate nodes attach congestion info, receiver tells source in a SACK
- ATP receiver includes flow control information in the SACK packets

# Ad Hoc Transport Protocol (ATP) [18] III

- if an ATP sender **has not received any ACK packets** for two consecutive feedback periods, it undergoes a multiplicative decrease of the transmission rate
- after a third such period without any ACK, the connection is assumed to be lost and the ATP sender goes to the connection initiation phase during which it periodically generates probe packets
- when a path break occurs, the network layer detects it and originates an ELFN packet toward the ATP sender
- ATP sender freezes the sender state, periodically originates probe packets to know the status of the path. With a successful probe, the sender begins data transmission again.
- **major disadvantage** of ATP is the lack of interoperability with TCP.

# Summary

- legacy TCP-Tahoe and TCP-Reno
- issues of congestion control and reliability in ad hoc networks
- classification: split, e2e or brand-new
- TCP variants customized for ad hoc networks
- new protocols independent of TCP designed for ad hoc networks

# References I

- [1] C. S. R. Murthy and B. Manoj, *Ad hoc wireless networks: Architectures and protocols*. Pearson, 2004.
- [2] R. Ramanathan and J. Redi, "A brief overview of ad hoc networks: Challenges and directions," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 20-22, 2002.
- [3] F Baker, "An outsider's view of manet. draf-baker-manet-review-01," *Network Working Group, Internet-Draft*, 2002.
- [4] N. Abramson, "The aloha system: Another alternative for computer communications," in *Proceedings of the November 17-19, 1970, Fall Joint Computer Conference*, ser. AFIPS '70 (Fall), Houston, Texas, 1970, 281-285, ISBN: 9781450379045. DOI: 10.1145/1478462.1478502.
- [5] J. Jubin and J. D. Tornow, "The darpa packet radio network protocols," *Proceedings of the IEEE*, vol. 75, no. 1, pp. 21-32, 1987.
- [6] R. Kahn, "The organization of computer resources into a packet radio network," *IEEE Transactions on Communications*, vol. 25, no. 1, pp. 169-178, 1977.
- [7] M. A. Nowak, "Five rules for the evolution of cooperation," *Science*, vol. 314, no. 5805, pp. 1560-1563, 2006.
- [8] C. Beard and W. Stallings, *Wireless Communication Networks and Systems*. Prentice Hall, 2016, vol. 1.
- [9] R. Hekmat, *Ad-hoc networks: fundamental properties and network topologies*. Springer, 2006.
- [10] S. Misra, I. Woungang, and S. C. Misra, *Guide to wireless ad hoc networks*. Springer, 2009.
- [11] J. H. Schiller, *Mobile communications*. Pearson, 2003.
- [12] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: A media access protocol for wireless lan's," *ACM SIGCOMM Computer Communication Review*, vol. 24, no. 4, pp. 212-225, 1994.

# References II

- [13] C. L. Fullmer and J. J. Garcia-Luna-Aceves, "Floor acquisition multiple access (FAMA) for packet-radio networks," *SIGCOMM Comput. Commun. Rev.*, vol. 25, no. 4, 262–273, Oct. 1995, ISSN: 0146-4833. DOI: 10.1145/217391.217458.
- [14] Z. J. Haas and Jing Deng, "Dual busy tone multiple access (DBTMA): A multiple access control scheme for ad hoc networks," *IEEE Transactions on Communications*, vol. 50, no. 6, pp. 975–985, 2002. DOI: 10.1109/TCOMM.2002.1010617.
- [15] K. Chandran, S. Raghunathan, S. Venkatesan, and R. Prakash, "A feedback-based scheme for improving tcp performance in ad hoc wireless networks," *IEEE Personal Communications*, vol. 8, no. 1, pp. 34–39, 2001. DOI: 10.1109/98.904897.
- [16] G. Holland and N. Vaidya, "Analysis of tcp performance over mobile ad hoc networks," *Wireless Networks*, vol. 8, no. 2-3, pp. 275–288, 2002.
- [17] S. Kopparty, S. V. Krishnamurthy, M. Faloutsos, and S. K. Tripathi, "Split tcp for mobile ad hoc networks," in *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, vol. 1, 2002, 138–142 vol.1. DOI: 10.1109/GLOCOM.2002.1188057.
- [18] K. Sundaresan, V. Anantharaman, Hung-Yun Hsieh, and A. R. Sivakumar, "Atp: A reliable transport protocol for ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 6, pp. 588–603, 2005. DOI: 10.1109/TMC.2005.81.