Introduction to Computer Networks

COSC 4377

Lecture 21

Spring 2012

April 9, 2012

Announcements

- HW10 due this week
- Student presentations

HW10

- Latency measurements
- Plotting latency

- Get your user id today

Today’s Topics

- Wireless Networks

Wireless

- Today: wireless networking truly ubiquitous
  - 802.11, 3G, (4G), WiMAX, Bluetooth, RFID, …
  - Sensor networks, Internet of Things
  - Some new computers have no *wired* networking
- What’s behind the scenes?

Wireless is different

- Signals sent by the sender don't always reach the receiver intact
  - Varies with space: *attenuation*, *multipath*
  - Varies with time: conditions change, *interference*, *mobility*
- *Distributed*: sender doesn't know what happens at receiver
- Wireless medium is inherently *shared*
  - No easy way out with switches

Implications

- Different mechanisms needed
- Physical layer
  - Different knobs: antennas, transmission power, encodings
- Link Layer
  - Distributed medium access protocols
  - Topology awareness
- Network, Transport Layers
  - Routing, forwarding
- Most advances *do not* abstract away the physical and link layers

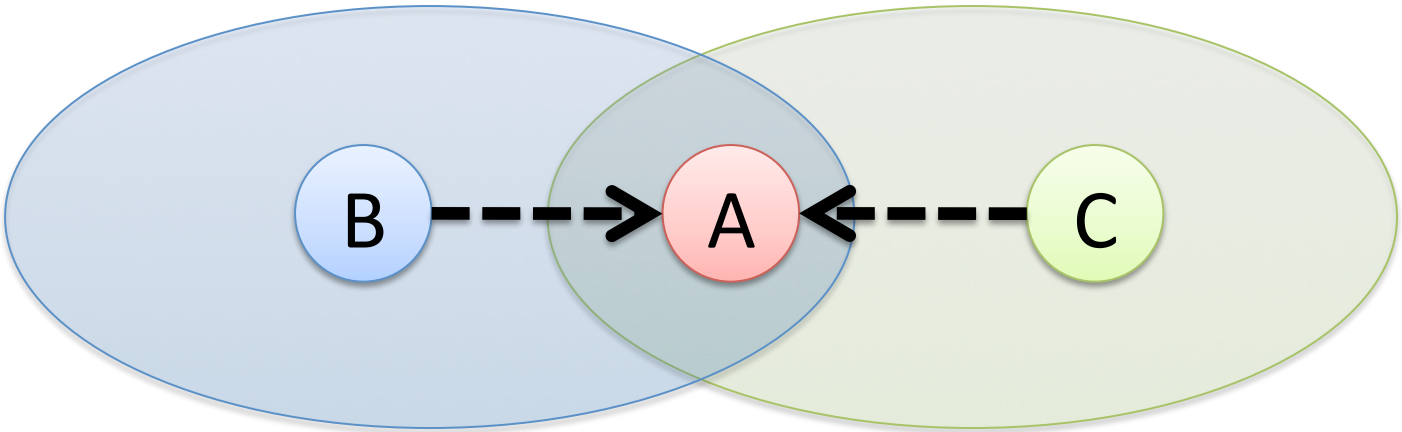
Interference

- External sources
  - E.g., 2.4GHz unlicensed ISM band
  - 802.11
  - 802.15.4 (ZigBee), 802.15.1 (Bluetooth)
  - 2.4GHz phones
  - Microwave ovens
- Internal sources
  - Nodes in the same network/protocol can (and do) interfere
- Multipath
  - Self-interference (destructive)

Link Layer

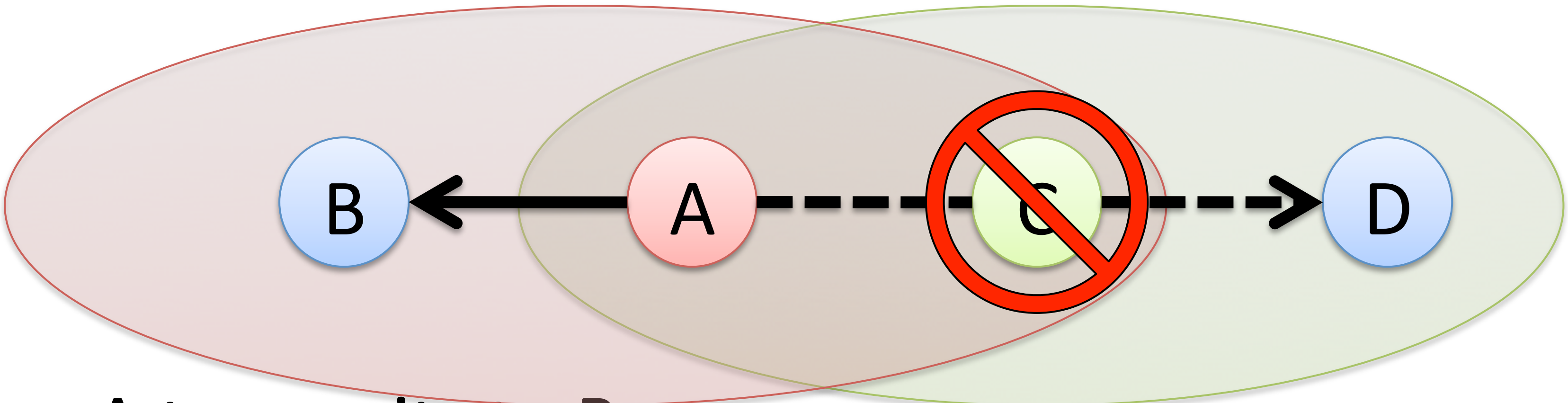
- Medium Access Control
  - Should give 100% if one user
  - Should be efficient and fair if more users
- Ethernet uses CSMA/CD
  - Can we use CD here?
- No! Collision happens at the receiver
- Protocols try to *avoid* collision in the first place

Hidden Terminals



- A can hear B and C
- B and C can't hear each other
- They both interfere at A
- B is a *hidden terminal* to C, and vice-versa
- Carrier sense at sender is useless

Exposed Terminals



- A transmits to B
- C hears the transmission, backs off, even though D would hear C
- C is an *exposed* terminal to A's transmission

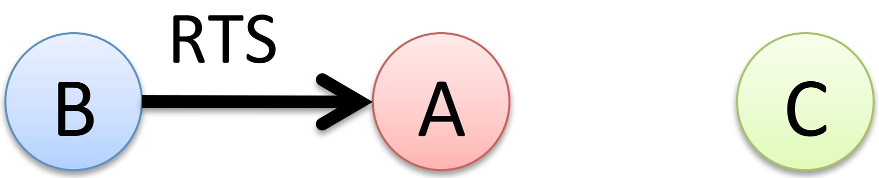
Key points

- No global view of collision
  - Different receivers hear different senders
  - Different senders reach different receivers
- Collisions happen at the *receiver*
- Goals of a MAC protocol
  - Detect if receiver can hear sender
  - Tell senders who might interfere with receiver to shut up

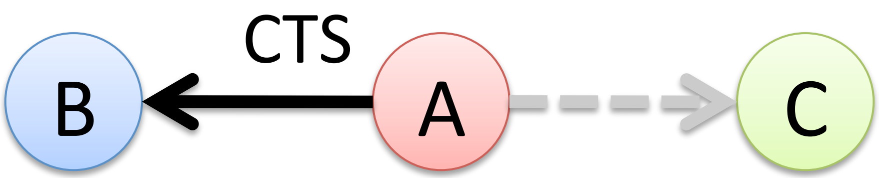
RTS/CTS

- Idea: transmitter can check availability of channel at receiver
- Before every transmission
  - Sender sends an RTS (Request-to-Send)
  - Contains length of data (in *time* units)
  - Receiver sends a CTS (Clear-to-Send)
  - Sender sends data
  - Receiver sends ACK after transmission
- If you don't hear a CTS, assume collision
- If you hear a CTS for someone else, shut up

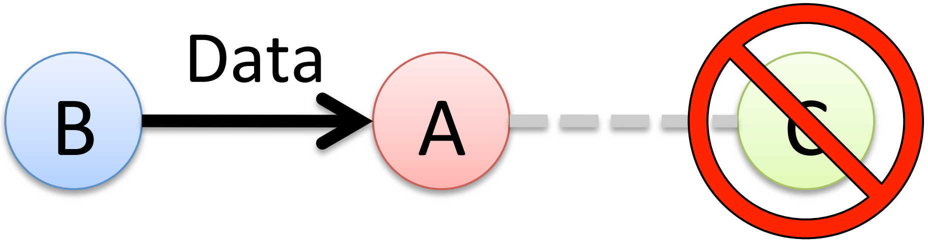
RTS/CTS



RTS/CTS



RTS/CTS



Benefits of RTS/CTS

- Solves hidden terminal problem
- Does it?
  - Control frames can still collide
  - E.g., can cause CTS to be lost
  - In practice: reduces hidden terminal problem on data packets

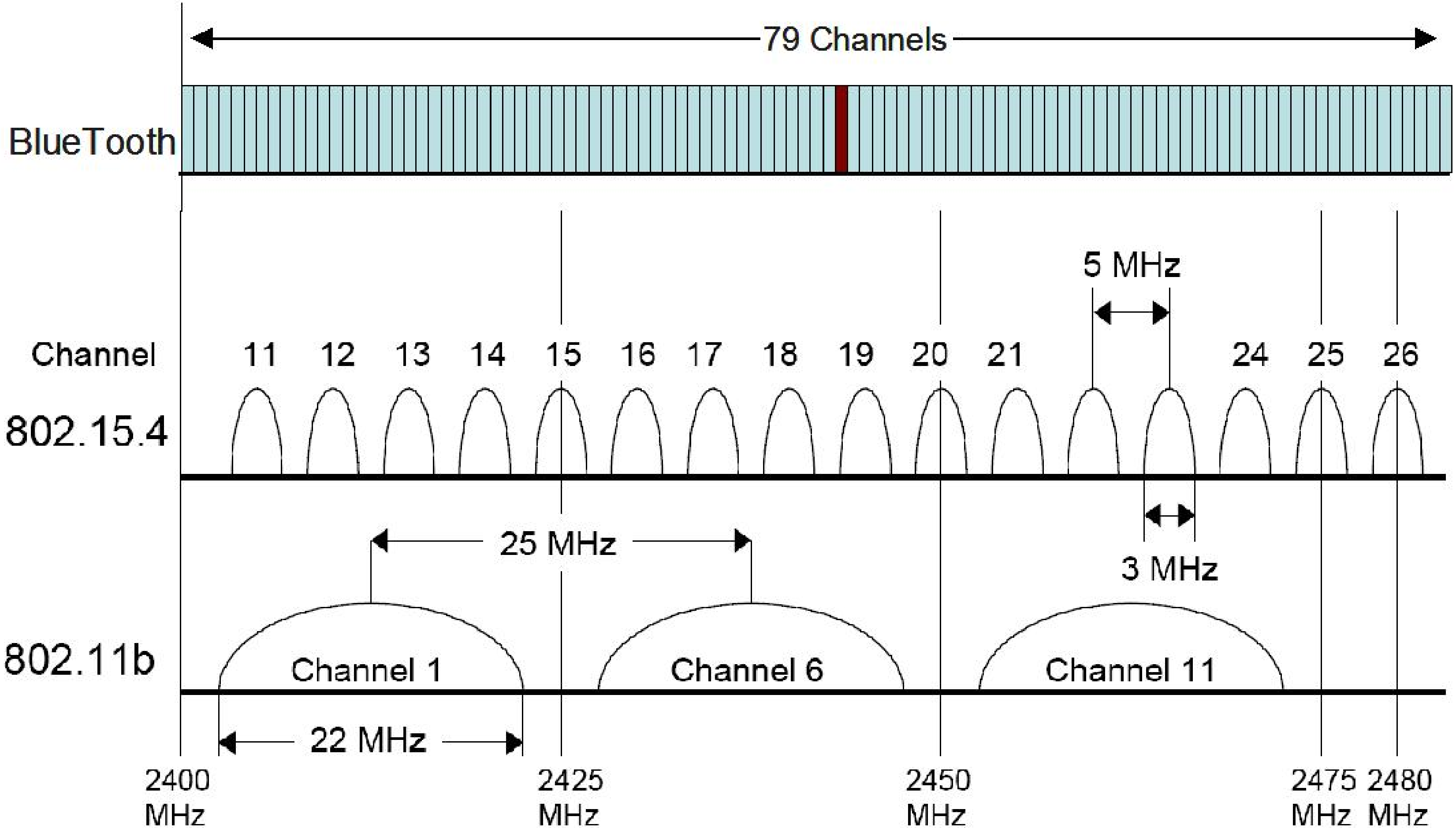
Drawbacks of RTS/CTS

- Overhead is too large for small packets
  - 3 packets per packet: RTS/CTS/Data (4-22% for 802.11b)
- RTS still goes through CSMA: can be lost
- CTS loss causes lengthy retries
- 33% of IP packets are TCP ACKs
- In practice, WiFi doesn't use RTS/CTS

Other MAC Strategies

- Time Division Multiplexing (TDMA)
  - Central controller allocates a time slot for each sender
  - May be inefficient when not everyone sending
- Frequency Division
  - Multiplexing two networks on same space
  - Nodes with two radios (think graph coloring)
  - Different frequency for upload and download

ISM Band Channels



Network Layer

- What about the network topology?
- Almost everything you use is *single hop*!
  - 802.11 in infrastructure mode
  - Bluetooth
  - Cellular networks
  - WiMax (Some 4G networks)
- Why?
  - Really hard to make multihop wireless efficient

WiFi Distribution System

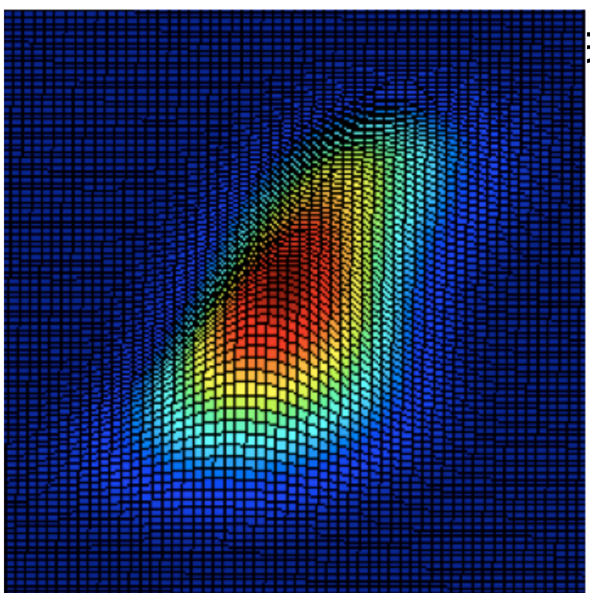
- 802.11 typically works in *infrastructure mode*
  - Access points – fixed nodes on wired network
- Distribution system connects Aps
  - Typically connect to the same Ethernet, use learning bridge to route to nodes' MAC addresses
- Association
  - Node negotiates with AP to get access
  - Security negotiated as well (WEP, WPA, etc)
  - Passive or active

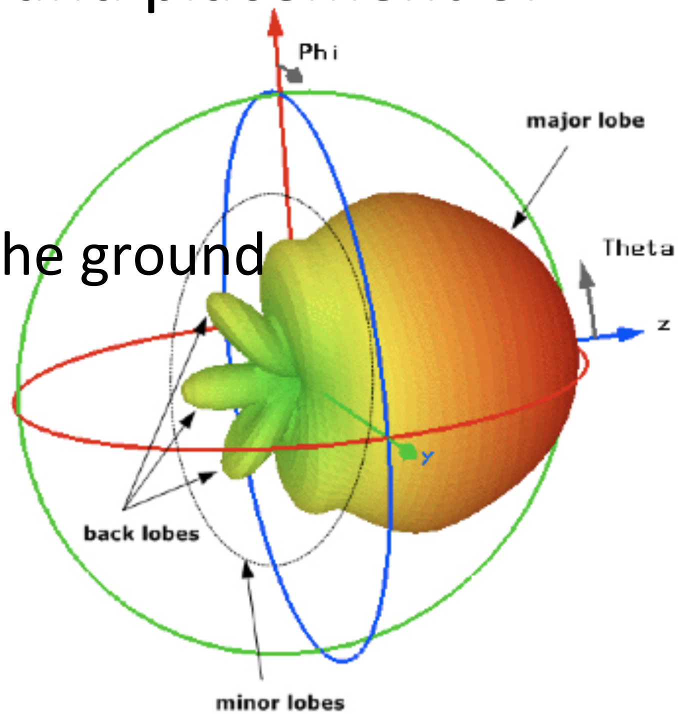
Wireless Multi-Hop Networks

- Some networks are multihop, though!
  - Ad-hoc networks for emergency areas
  - Vehicular Networks
  - Sensor Networks
    - E.g., infrastructure monitoring
  - Multihop networking to share Internet access

What can happen to signals?

- Attenuation
  - Signal power attenuates by $\sim r^2$ factor for omni-directional antennas in free-space
  - Exponent depends on type and placement of antennas
    - antennas
    - close to the ground

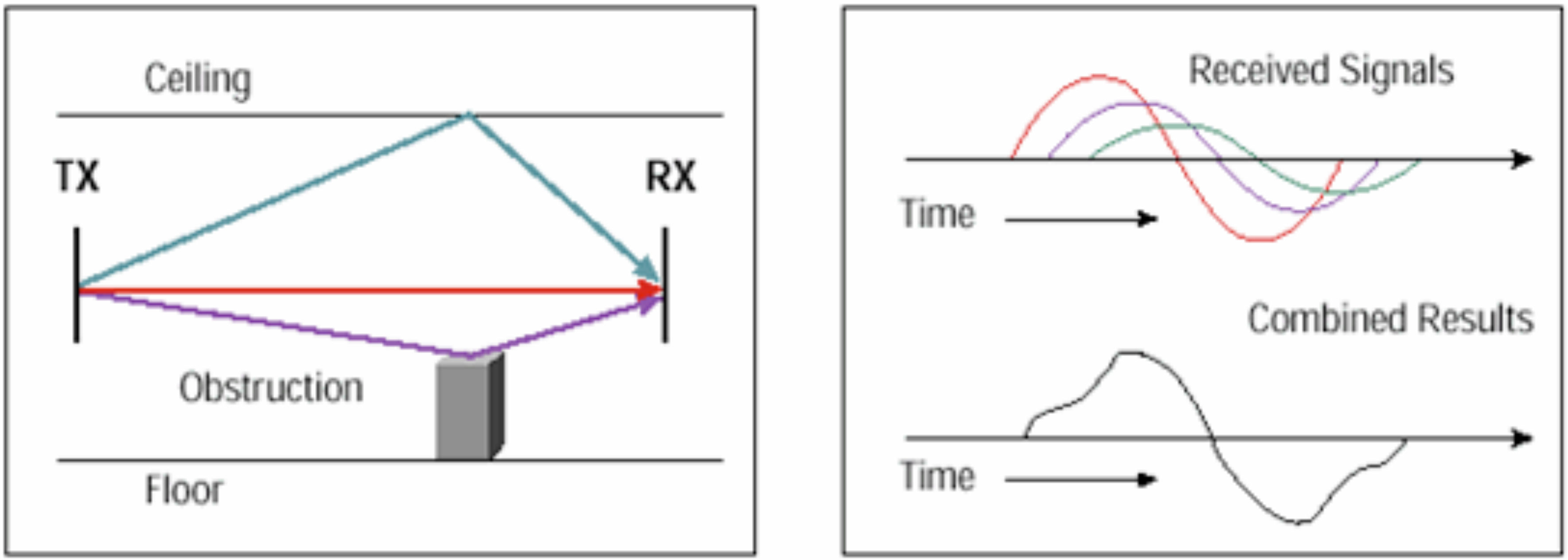




Interference

- External sources
  - E.g., 2.4GHz unlicensed ISM band
  - 802.11
  - 802.15.4 (ZigBee), 802.15.1 (Bluetooth)
  - 2.4GHz phones
  - Microwave ovens
- Internal sources
  - Nodes in the same network/protocol can (and do) interfere
- Multipath
  - Self-interference (destructive)

Multipath



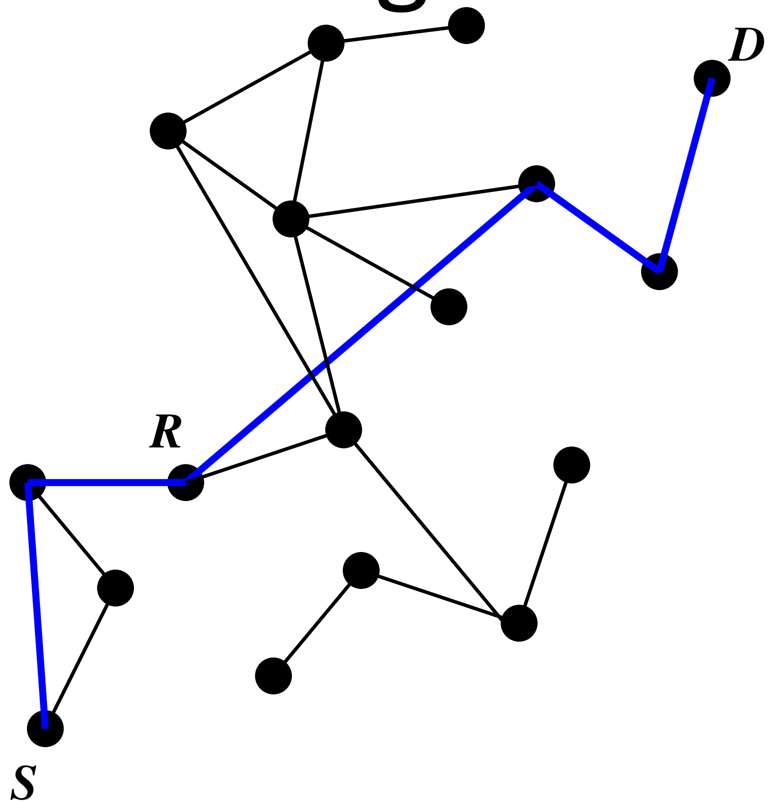
- May cause attenuation, destructive interference

Picture from Cisco, Inc.

Many Challenges

- Routing
  - Link estimation
- Multihop throughput dropoff

The Routing Problem



- Find a route from S to D
- Topology can be very dynamic

Routing

- Routing in ad-hoc networks has had a lot of research
  - General problem: any-to-any routing
  - Simplified versions: any-to-one (base station), one-to-any (dissemination)
- DV too brittle: inconsistencies can cause loops
- DSDV
  - Destination Sequenced Distance Vector

DSDV

- Charles Perkins (1994)
- Avoid loops by using sequence numbers
  - Each destination increments own sequence number
    - Only use EVEN numbers
  - A node selects a new parent if
    - Newer sequence number or
    - Same sequence number and *better* route
  - If disconnected, a node increments destination sequence number to next ODD number!
  - No loops (only transient loops)
  - Slow: on some changes, need to wait for root

Many Others

- DSR, AODV: on-demand
- Geographic routing: use nodes' physical location and do greedy routing
- Virtual coordinates: derive coordinates from topology, use greedy routing
- Tree-based routing with on-demand shortcuts
- …