CS263: Wireless Communications and Sensor Networks

Matt Welsh

Lecture 6: Bluetooth and 802.15.4
October 6, 2005

Today's Lecture

Bluetooth

- Standard for Personal Area Networks (PANs)

IEEE 802.15.4

- New standard for Low Power Wireless Networks

Bluetooth basics

Short-range, high-data-rate wireless link for personal devices

- Originally intended to replace cables in a range of applications
- e.g., Phone headsets, PC/PDA synchronization, remote controls

Operates in 2.4 GHz ISM band

- Same as 802.11 and 802.15.4!
- Frequency Hopping Spread Spectrum across ~ 80 channels

Somewhat bulky application interfaces

- Not just simple byte-stream data transmission
- Rather, complete protocol stack to support voice, data, video, file transfer, etc.
  - *Bluetooth operates at a higher level than 802.11 and 802.15.4*

Bluetooth basics cont'd

Maximum data rate of up to 720 Kbps

- *But, requires large packets (> 300 bytes)*

Class 1: Up to 100mW (20 dBm) transmit power, ~100m range

- *Class 1 requires that devices adjust transmit power dynamically to avoid interference with other devices*

Class 2: Up to 2.4 mW (4 dBm) transmit power

Class 3: Up to 1 mW (0 dBm) transmit power

Security is “optional”

- Many devices on the market do not take security seriously

Usage Models

Wireless audio

- e.g., Wireless headset associated with a cell phone
- Requires guaranteed bandwidth between headset and base
- No need for packet retransmission in case of loss

Cable replacement

- Replace physical serial cables with Bluetooth links
- Requires mapping of RS232 control signals to Bluetooth messages

LAN access

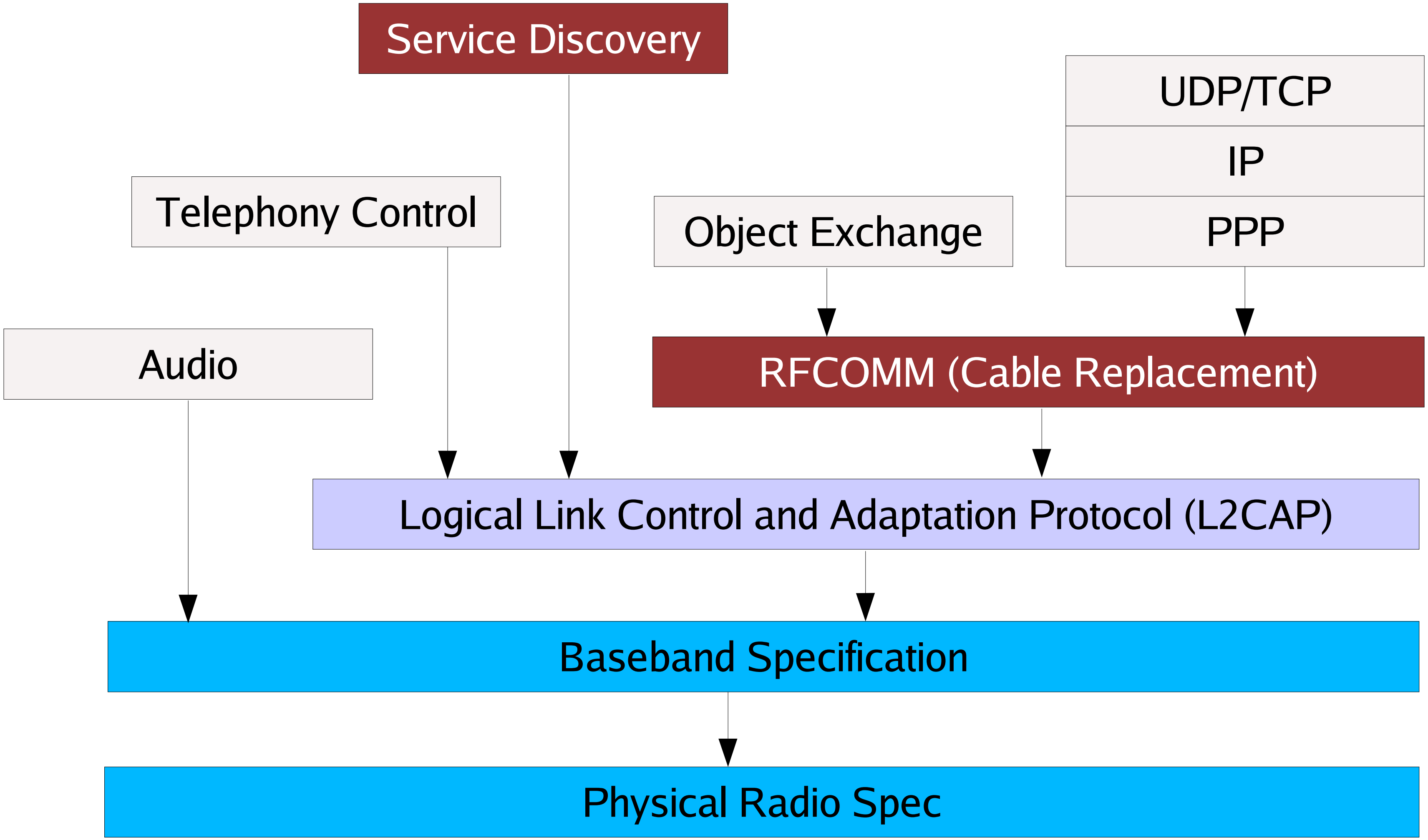
- Allow wireless device to access a LAN through a Bluetooth connection
- Requires use of higher-level protocols on top of serial port (e.g., PPP)

File transfer

- Transfer calendar information to/from PDA or cell phone
- Requires understanding of object format, naming scheme, etc.

Lots of competing demands for one radio spec!

Protocol Architecture



Piconet Architecture

One master and up to 7 slave devices in each *Piconet*:

Master controls transmission schedule of all devices in the Piconet

- Time Division Multiple Access (*TDMA*): Only one device transmits at a time

Frequency hopping used to avoid collisions with other Piconets

- 79 physical channels of 1 MHz each, hop between channels 1600 times a sec

Scatternets

Combine multiple Piconets into a larger Scatternet

- Device may act as master in one Piconet and slave in another
  - *Each Piconet using different FH schedule to avoid interference*
- Can extend the range of Bluetooth, can route across Piconets

Baseband Specification

79 1-MHz channels defined in the 2.4 GHz ISM band

- Gaussian FSK used as modulation, 115 kHz frequency deviation

Frequency Hopping Spread Spectrum

- Each Piconet has its own FH schedule, defined by the master
- 1600 hops/sec, slot time 0.625 ms

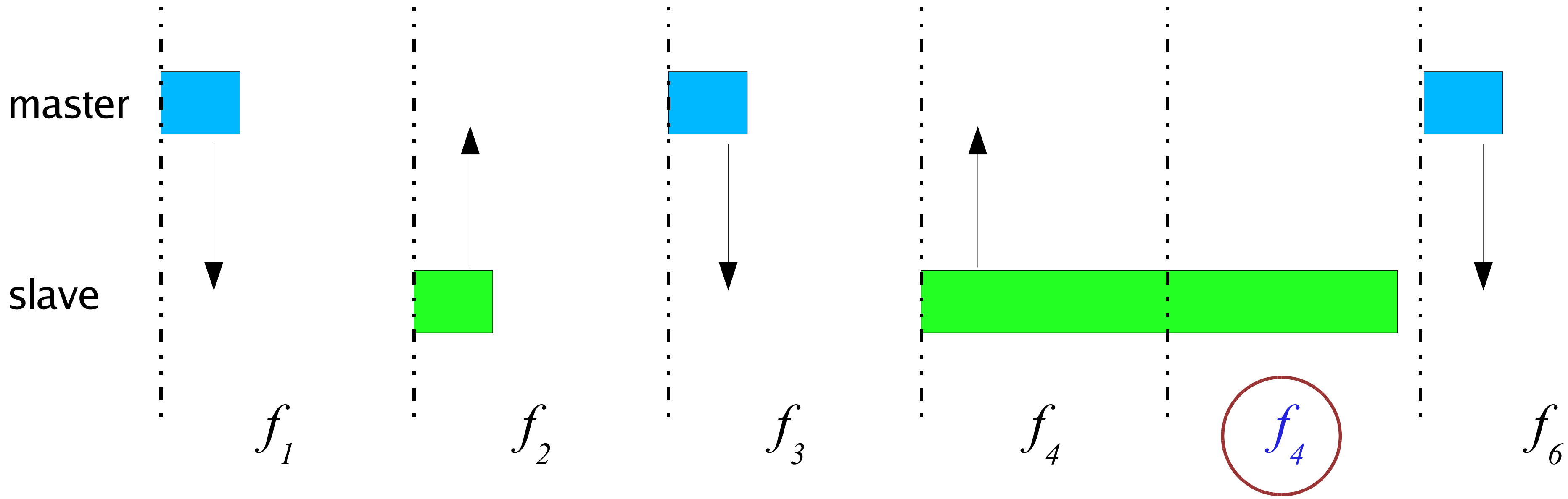
Time Division Duplexing

- Master transmits to slave in one time slot, slave to master in the next

TDMA used to share channel across multiple slave devices

- Master determines which time slots each slave can occupy
- Allows slave devices to sleep during inactive slots

Time slots



Each time slot on a different frequency

- According to FH schedule

Packets may contain ACK bit to indicate successful reception in the *previous* time slot

- Depending on type of connection...
- e.g., Voice connections do not use ACK and retransmit

Packets may span multiple slots – stay on same frequency

Physical and Logical Links

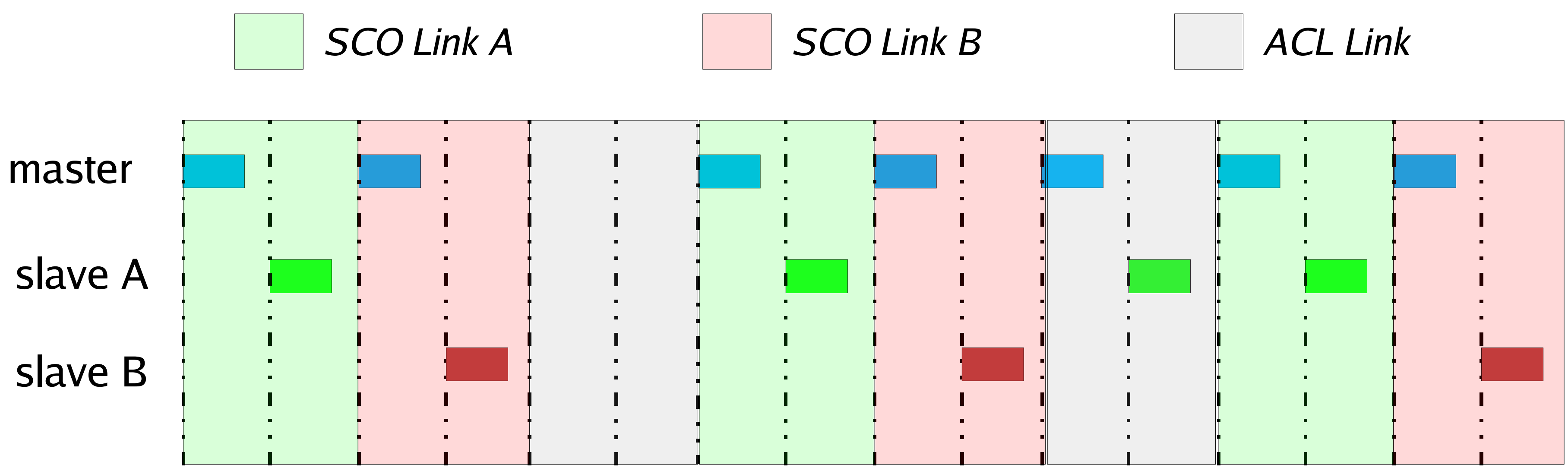
Bluetooth supports two types of physical links.

Synchronous Connection Oriented (SCO):

- Slave assigned to two consecutive slots at regular intervals
    - *Just like TDMA...*
- No use of retransmission ... *why??*

Asynchronous Connectionless (ACL)

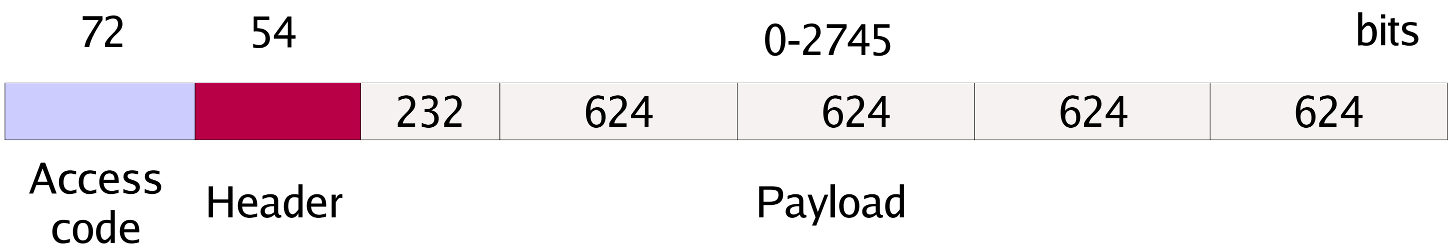
- Allows non-SCO slots to be used for "on demand" transmissions
- Slave can only reply if it was addressed in previous slot by master



Packet Formats

Bluetooth supports 14 different payload formats!

- Different formats for control, voice, and data packets
- Frames can span 1, 3, or 5 slots
- Different levels of error coding: No coding, 1/3, or 2/3 FEC



What is the maximum bandwidth that Bluetooth can achieve?

- Counting only application payload bytes, no CRC or FEC
- 5-slot packet, no protection: 341 payload bytes
- Total time = 5 * (0.625) ms = 3.125 ms
  - *But ... need to count an extra slot from the master for ACK!*
- Total bandwidth is therefore 341 bytes / (6 * 0.625 ms) = 710 kbps
  - *Most texts say either 721 or 723 kbps is the max.*
  - *This depends on definition of "kilobit" -- I use 1024 bits.*
  - *Stallings text claims DH5 packet has 341 bytes of payload. Appears to be only 339 (plus 2-byte CRC).*

IEEE 802.15.4 and ZigBee

Emerging standard for low-power wireless monitoring and control

- Scale to many devices
- Long lifetime is important (contrast to Bluetooth)
- 10-75m range typical
- Designed for industrial process monitoring, control, medical devices, etc.
- High data rate for small packets (~200 Kbps for 75 byte packets)

IEEE 802.15.4

- Physical and MAC layer
- Combination of CSMA and TDMA schemes

ZigBee

- Network and application layer on top of 802.15.4
- Still emerging, standard not yet available outside of ZigBee Alliance

ZigBee™ Alliance

Chipcon/Ember CC2420

Single-chip 802.15.4 radio transceiver, $5

- Incorporated into the Telos motes you are going to use in this class...

- 1.8V supply, consumes 19.7 mA receiving, 17.4 mA transmit
- Easy to integrate: Open source software drivers
- Supports 802.15.4 PHY and encryption in hardware
  - *MAC still implemented in software*

802.15.4 PHY

802.15.4 defines several frequency ranges:

- 16 channels in the 2.4 GHz band (5 MHz per channel)
- 10 channels in the 915 MHz band (2 MHz per channel)
- 1 channel in the 868 MHz band

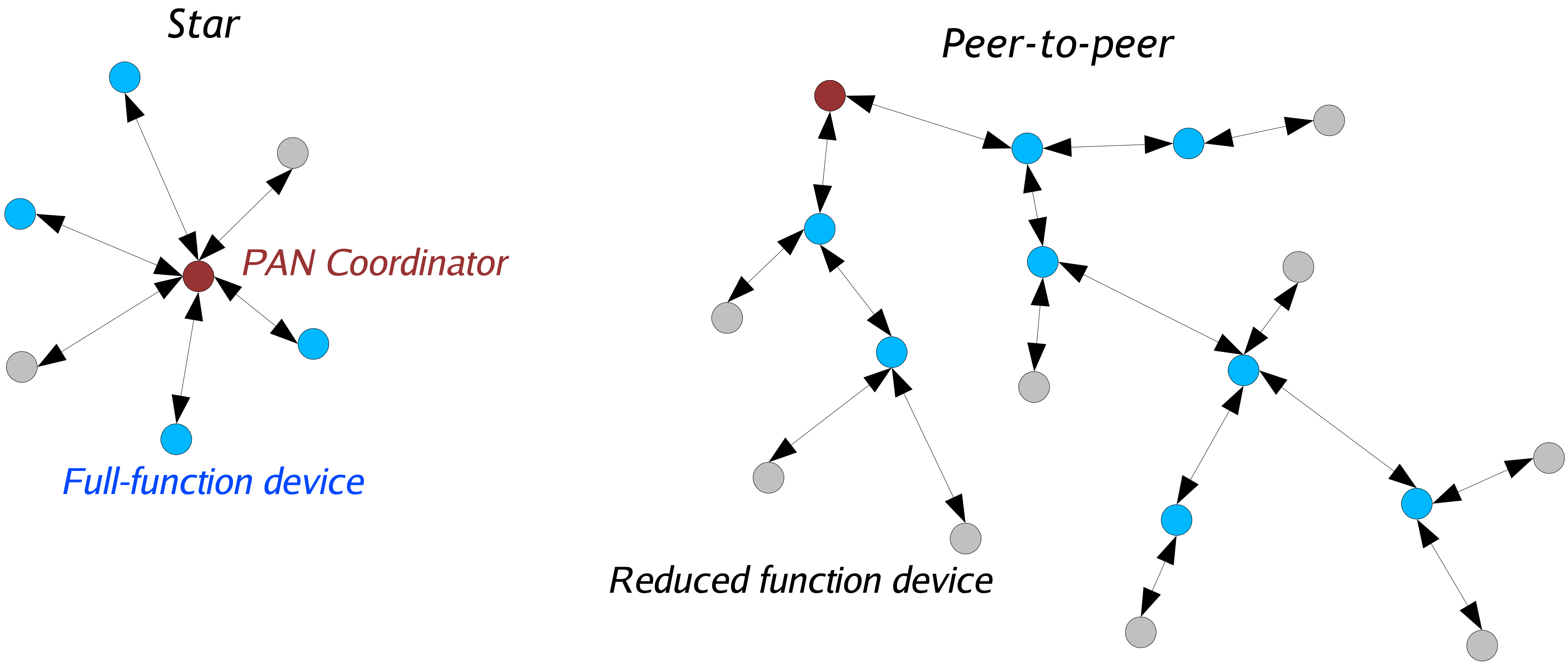
Direct Sequence spreading used for 2.4 GHz band

- Each 4-bit nibble mapped onto quasi-orthogonal 32-bit chipping code
- Modulated using offset-QPSK

Data transmitted at a rate of 2 million chips/sec

- 32-bit chip maps onto 4-bit raw data symbol
- So, effective data rate is ((2,000,000) / (32)) * 4 = 250,000 bits/sec
  - *Note that this is only 244 Kbps if 1 Kbit = 1024 bits.*

Network Topologies



Every network has a unique *Personal Area Network Coordinator*

- Coordinator responsible for network management tasks, e.g., associating new nodes, transmitting beacons, etc.
- Star network: All nodes must talk to PAN (like 802.11)
- Peer-to-peer network: Individual nodes can talk to each other
    - *Only Full Function Devices can actually route messages*

Superframe Structure

Superframe broken into 16 time slots between beacons

- Beacons transmitted periodically by PAN coordinator
- Used to synchronize nodes in a network to a common timebase.

Two types of time slots:

- **Contention Access Period**: Nodes use CDMA/CA to transmit
- **Contention Free Period**: Nodes assigned *guaranteed time slots*, as in TDMA
- Assignment of guaranteed slots performed by PAN Coordinator

Basic MAC Scheme

Beacon messages not subject to CSMA

- Used to coordinate network and are not expected to suffer collisions

CSMA/CA scheme very similar to 802.11

- Nodes listen before transmitting
- Random backoff between 0 – N time slots
- Double N each time a collision occurs

Transmitter can request ACK for each message

- Bit set in header to tell receiver an ACK is needed
- ACK will be transmitted shortly after reception (without CSMA)
- UnACK'd messages will be retransmitted up to some fixed number of times

Power Saving Features

To save power, it's a good idea to power down a node's radio

- Means that node cannot transmit or receive

Coordinator can define *idle period* within the superframe

- Means that all nodes can sleep during that time (even the coordinator!!)

However, individual nodes can enter a low-power state any time.

What does this mean for sending data to this node?

Power Saving Features

To save power, it's a good idea to power down a node's radio

- Means that node cannot transmit or receive

Coordinator can define *idle period* within the superframe

- Means that all nodes can sleep during that time (even the coordinator!!)

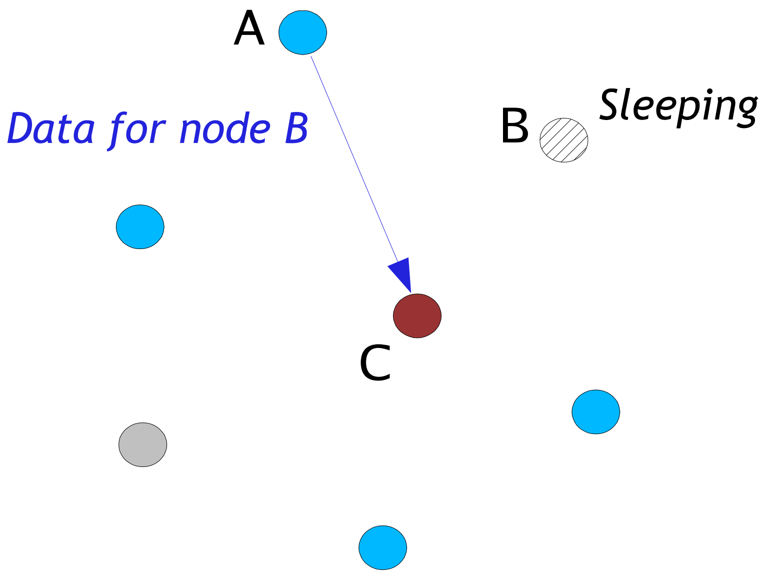
However, individual nodes can enter a low-power state any time.

What does this mean for sending data to this node?

- The receiver won't hear any incoming transmissions ....
- Should the transmitter just keep trying to send the same message?
- Is this really a “transmission failure” (e.g., caused by collisions)?

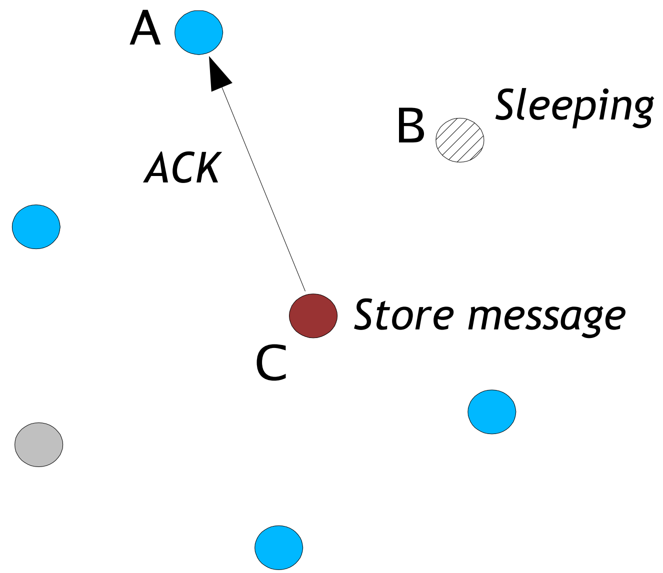
Poll-based Transfer

Solution: Poll-based transfer.



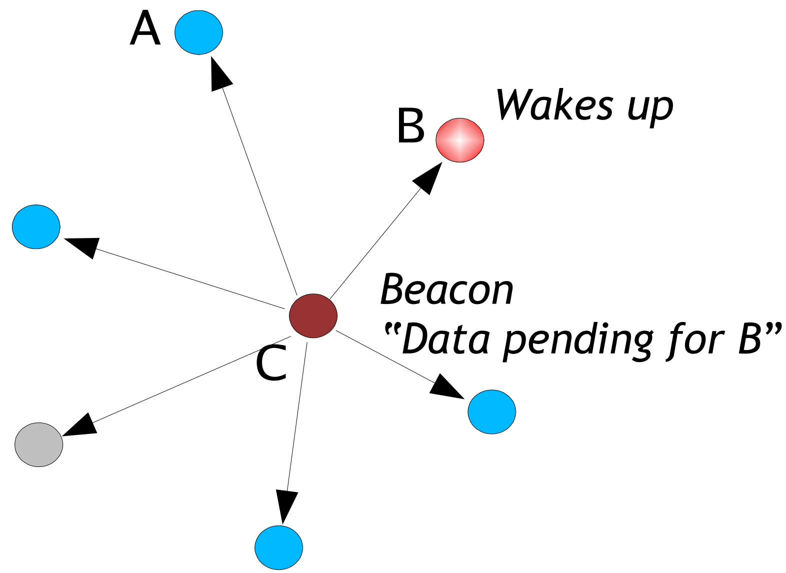
Poll-based Transfer

Solution: Poll-based transfer.



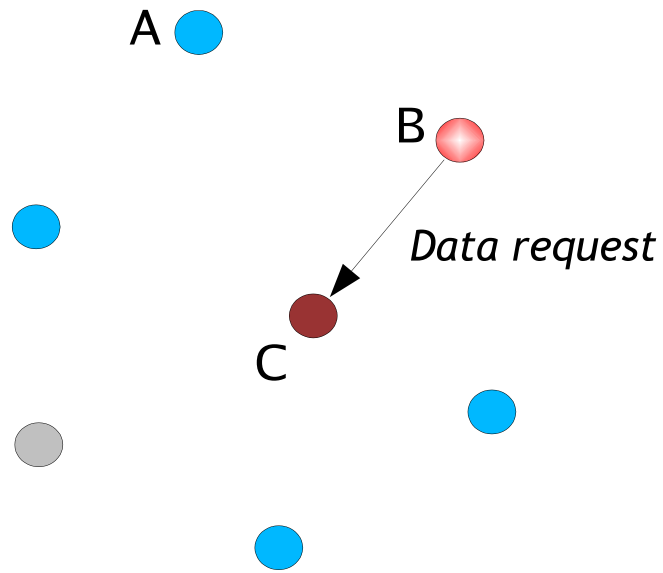
Poll-based Transfer

Solution: Poll-based transfer.



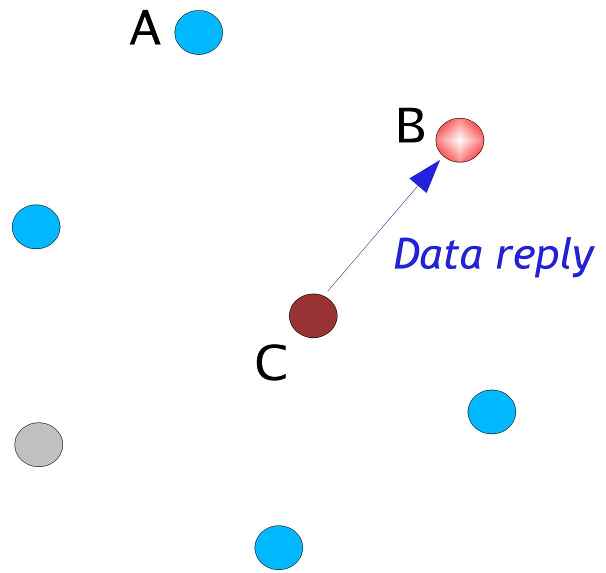
Poll-based Transfer

Solution: Poll-based transfer.



Poll-based Transfer

Solution: Poll-based transfer.



- Allows nodes to sleep when not requiring use of the radio
- Increases latency for communications
- Requires coordinator to buffer messages for individual nodes.

Next Lecture (Thursday, October 13!)

Starting new segment of the course: Research papers

A review of current routing protocols for Ad Hoc mobile wireless networks,
E. Royer and C.-K. Toh, IEEE Personal Communications, 1999.

A High-Throughput Path Metric for Multi-Hop Wireless Routing,
Douglas De Couto, Daniel Aguayo, John Bicket, and Robert Morris, Mobicom'03

Write a separate summary for each paper (in one email please!)

Your paper summaries should:

- Give a brief overview of the paper (in your own words)
- Offer 3 “insights” about the paper: Either complements or critiques