Lecture 06
802.15.4

CS433 – Wireless Protocols for IoT

Branden Ghena – Spring 2026

Materials in collaboration with
Pat Pannuto (UCSD) and Brad Campbell (UVA)

Northwestern

Assignment Schedule

- Hw: BLE Packets
  - Due by end-of-day Thursday
- Lab: BLE
  - Due next week Thursday
  - Goal: Wireshark parts by Thursday this week
- Quiz today
  - We’ll stop at around 1:30 pm to do a 15-minute quiz
  - Tell your friends if they’re not here

Today's Goals

- Introduction to 802.15.4

- Overview of physical layer details

- Exploration of link layer
  - Network topologies
  - Communication structure
  - Access control
  - Packet structure

References

- 802.15.4 Specification [2006]
  - “Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”

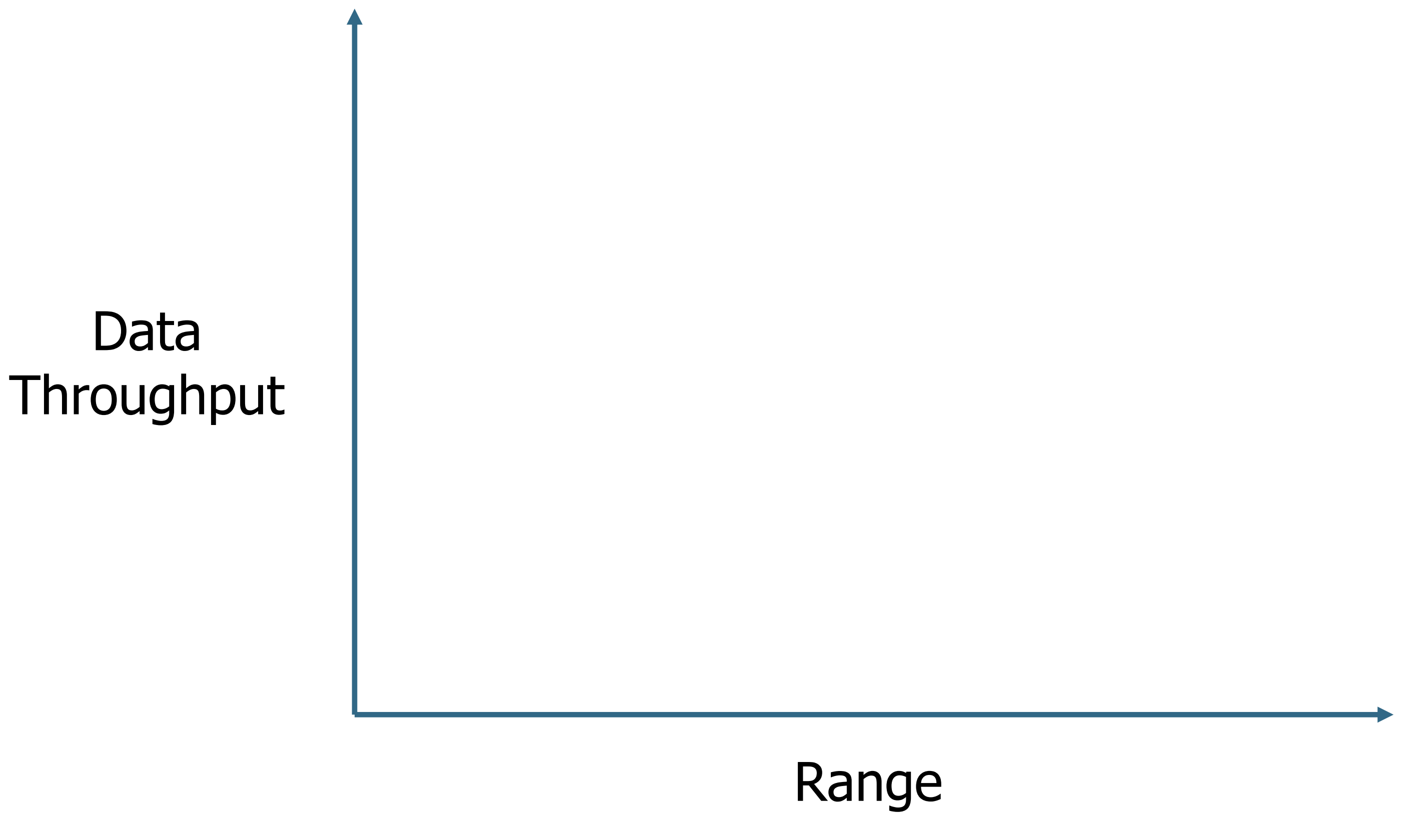
Other helpful references:

- Paper introducing the 802.15.4 draft
- NXP 802.15.4 Stack User Guide
- 2005 presentation on 802.15.4

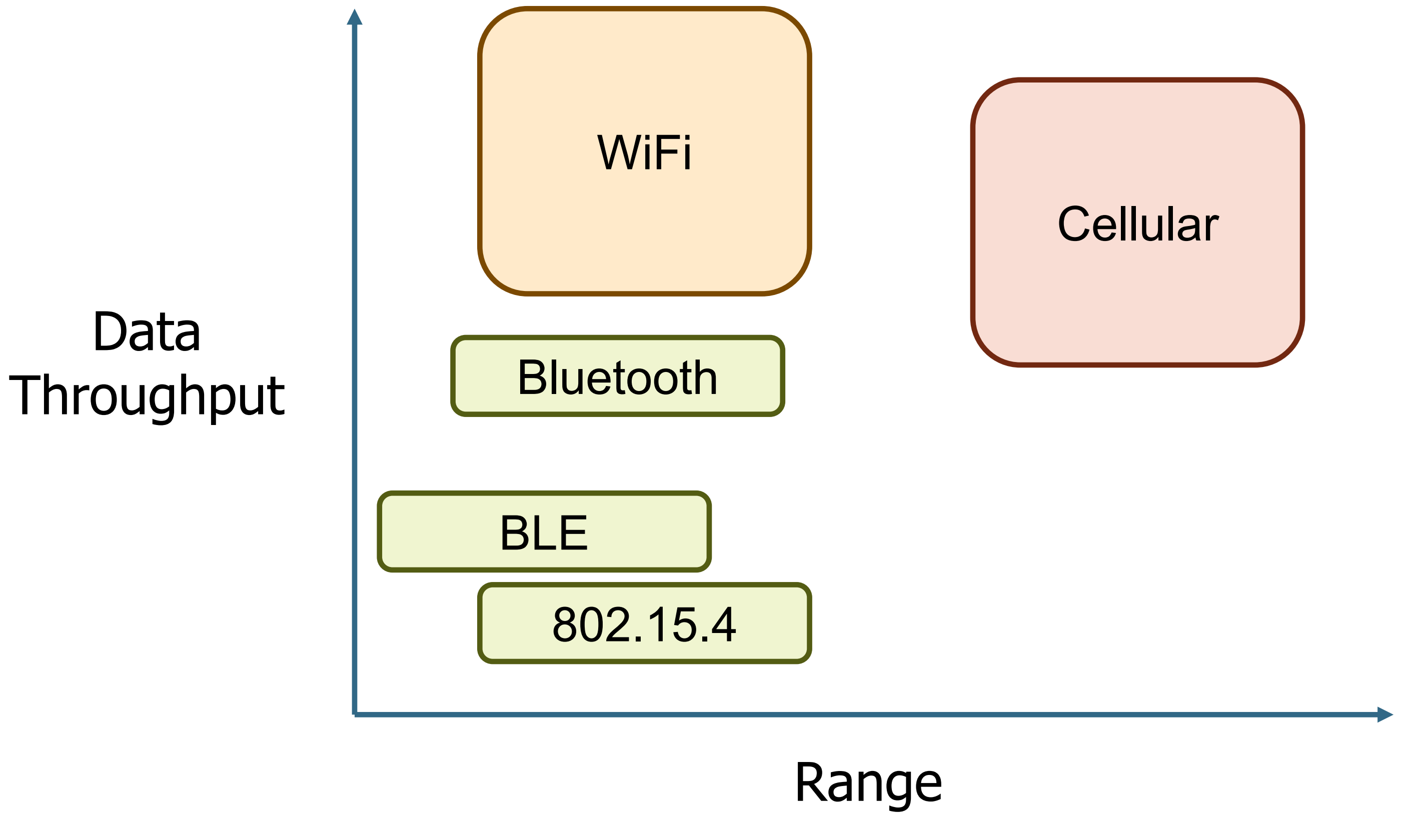
Outline

- **Overview**
- Physical Layer
- Link Layer
- Packet Structure

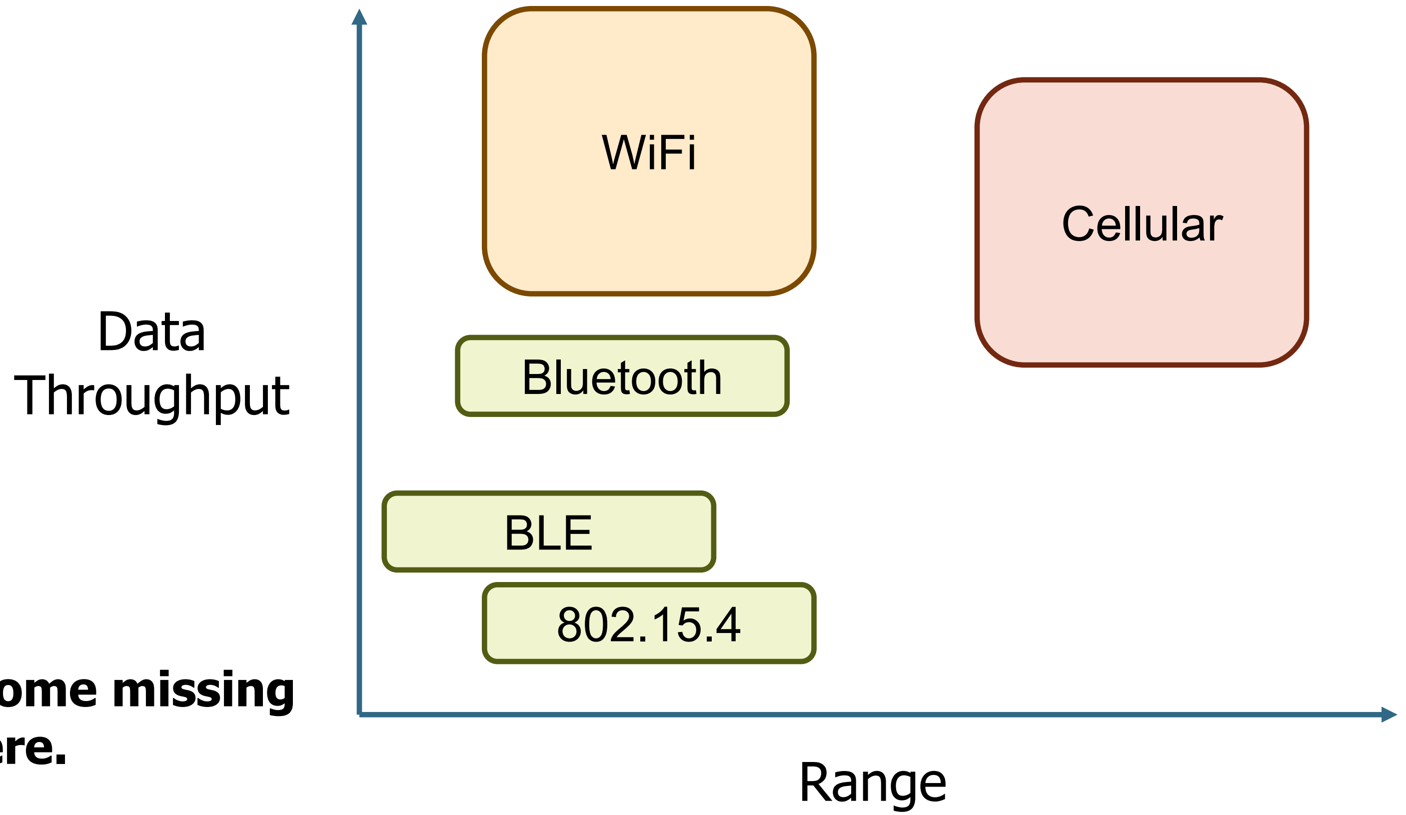
Comparison of networks



Comparison of networks



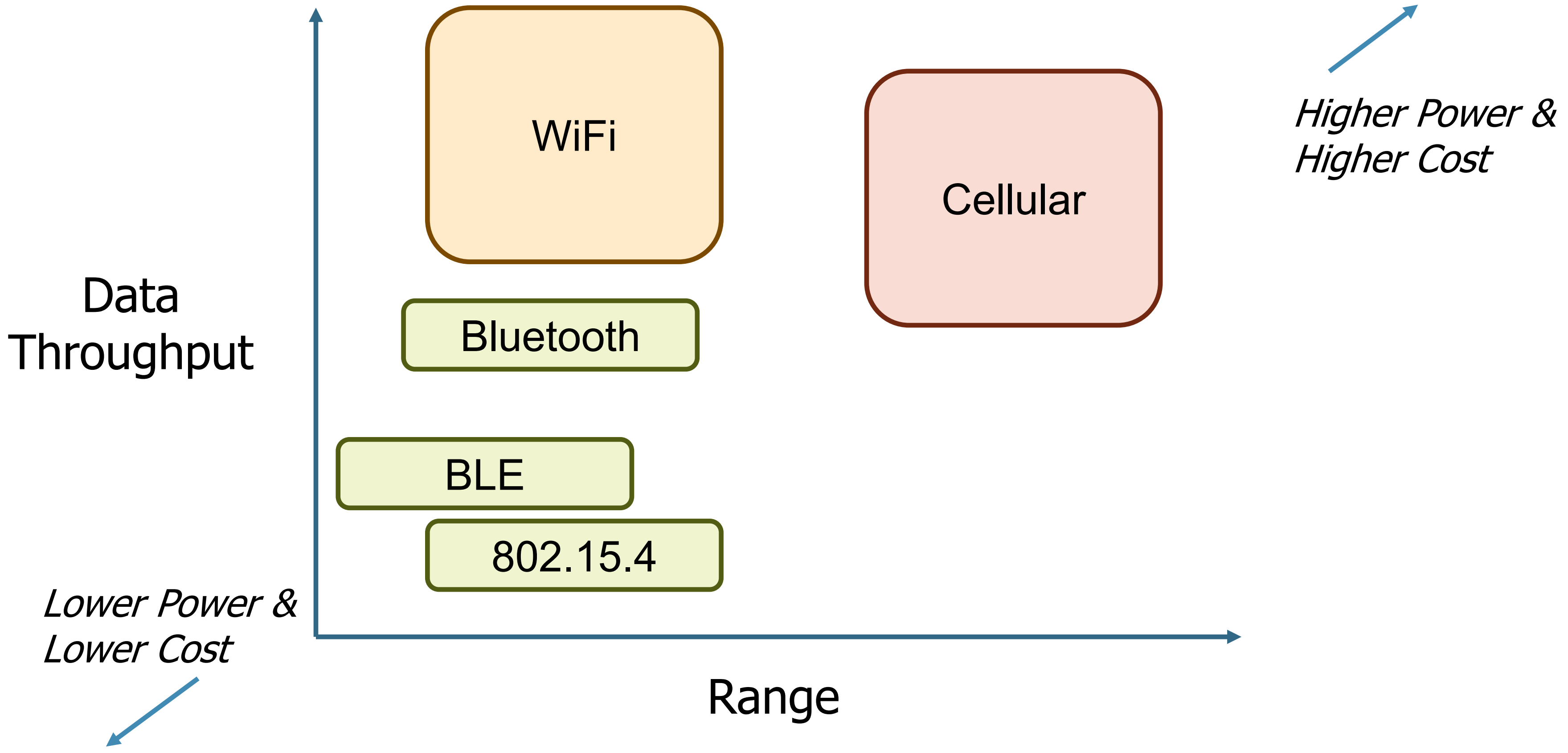
Comparison of networks



There are some missing qualities here.

Why be closer to the origin?

Comparison of networks



IEEE 802

- Network standards for variable-sized packets
  - Ethernet
  - WiFi
  - WPANs
- E.g. **not** networks that send periodic constant-sized packets
- Specifies PHY and Link layers
- Another example standard:
  - IEEE 754: Floating Point

Name	Description	Status
IEEE 802.1	Higher Layer LAN Protocols Working Group	Active
IEEE 802.2	LLC	Disbanded
IEEE 802.3	Ethernet	Active
IEEE 802.4	Token bus	Disbanded
IEEE 802.5	Token Ring MAC layer	Disbanded
IEEE 802.6	MANs (DQDB)	Disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	Disbanded
IEEE 802.8	Fiber Optic TAG	Disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	Disbanded
IEEE 802.10	Interoperable LAN Security	Disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	Active
IEEE 802.12	100BaseVG	Disbanded
IEEE 802.13	Unused[2]	reserved for Fast Ethernet development[3]
IEEE 802.14	Cable modems	Disbanded
IEEE 802.15	Wireless PAN	Active
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	hibernating
IEEE 802.17	Resilient packet ring	Disbanded
IEEE 802.18	Radio Regulatory TAG	?
IEEE 802.19	Wireless Coexistence Working Group	?
IEEE 802.20	Mobile Broadband Wireless Access	Disbanded
IEEE 802.21	Media Independent Handoff	hibernating
IEEE 802.22	Wireless Regional Area Network	hibernating
IEEE 802.23	Emergency Services Working Group	Disbanded
IEEE 802.24	Vertical Applications TAG	?

IEEE 802.15

- Wireless Personal-Area Networks (WPAN)
  - All the things within the workspace of a person
  - Conceptually smaller domain that the Local Area Network
  - Realistically about the same thing as a LAN

- Formerly included a Bluetooth spec
  - Bluetooth SIG took over governance

Name	Description	Status
IEEE 802.15.1	Bluetooth certification	Disbanded
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	Hibernating[4]
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	?
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	Active
IEEE 802.15.5	Mesh networking for WPAN	?
IEEE 802.15.6	Body area network	Active
IEEE 802.15.7	Visible light communications	?

802.15.4 (LR-WPANs) Overview "Low-Rate Wireless Personal Area Networks"

- Goals
  - "The IEEE 802.15 TG4 was chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity." [TG4]

- Applications
  - "Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation." [TG4]
  - Ultimately home automation, industrial control/monitoring, vehicular sensing, agriculture; really most machine-to-machine (M2M) sensor applications

- Other contemporary technologies
  - WiFi 802.11b and Bluetooth Classic
    - Too complex in specification and overachieving in capability

IEEE 802.15.4

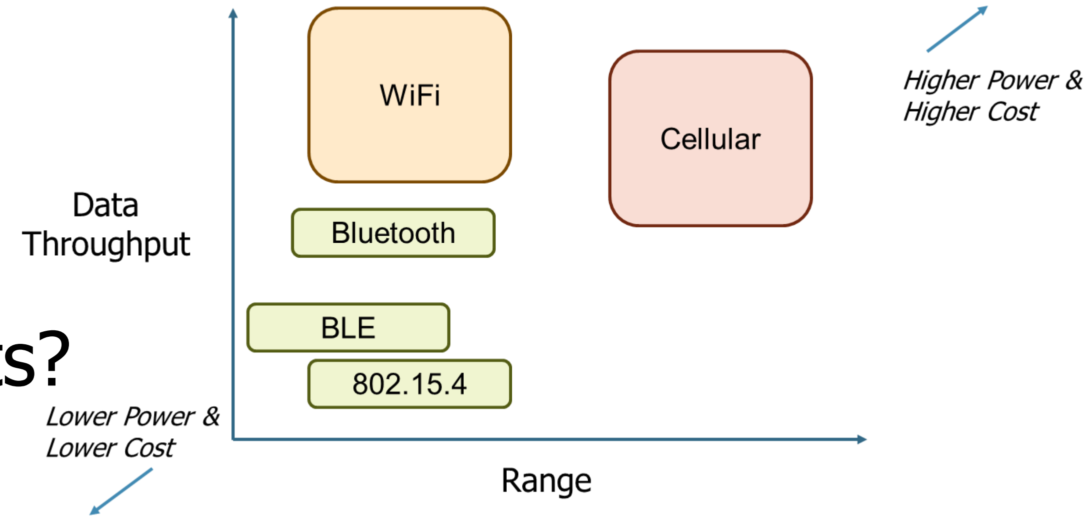
- Low-Rate Wireless PAN
  - 250 kbps, ~100 m range
  - Radio hardware available with low-power and low-cost

- Specification: 2003
  - Also 2006, 2011, 2015, and 2020 revisions
    - Mostly various added capabilities such as extra PHY layers
    - Also define optional security, scheduling, and larger frame sizes

- We'll mostly work off of the 2006 version
  - Thread is based on 2006 version
  - Zigbee is based on the original 2003 version
  - Roughly 200 pages of meaningful specification (100 of appendices)
    - Compare to 3000 pages of Bluetooth/BLE

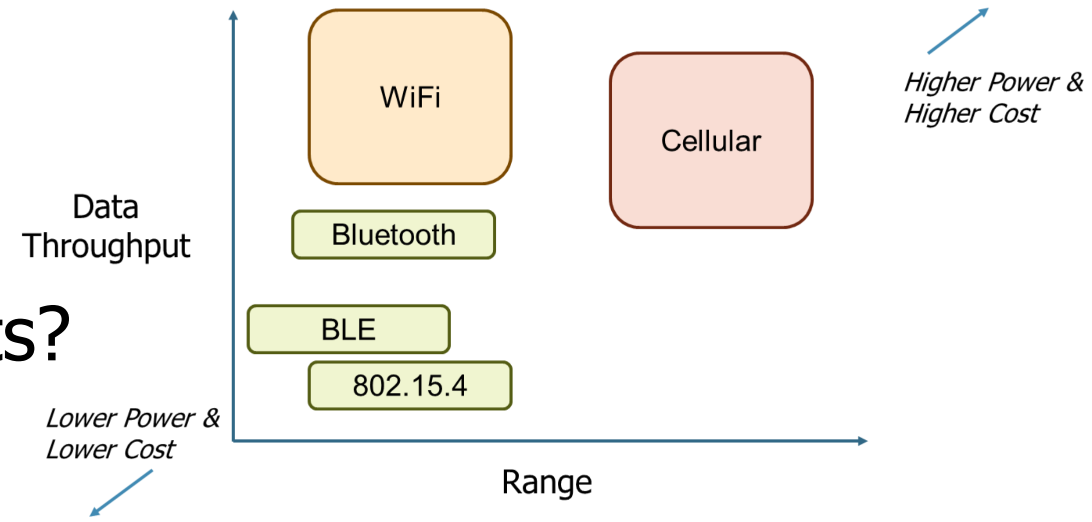
Break + Open Question

- Given 802.15.4's placement in terms of throughput, range, power, and cost: what are use-case constraints?



Break + Open Question

- Given 802.15.4's placement in terms of throughput, range, power, and cost: what are use-case constraints?



  - Not human-centric communication
    - Would need higher throughput
  - Still lower-energy and low-cost (similar to BLE)
    - Plausible for battery-operated devices
  - Range is focused on local-area (household-ish)
  - Bonus: long-term network, rather than ad-hoc point-to-point like BLE

Outline

- Overview
- **Physical Layer**
- Link Layer
- Packet Structure

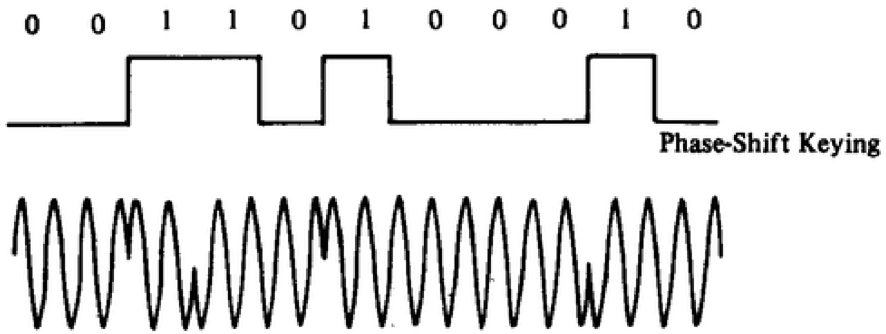
802.15.4 Physical Layers

- Multiple options of physical layers are supported
  - We'll focus on 2.4 GHz (2400 MHz)

Table 1—Frequency bands and data rates

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Physical Layer



- O-QPSK modulation
  - Offset Quadrature Phase-Shift Keying
    - 4 bits per symbol
  - Twice the data rate of BPSK for same Bit-Error Rate
  - Cost: more complicated design of receivers
    - Which is pretty minimal with all the transistors we've got
    - Plus the ability to reuse previous designs

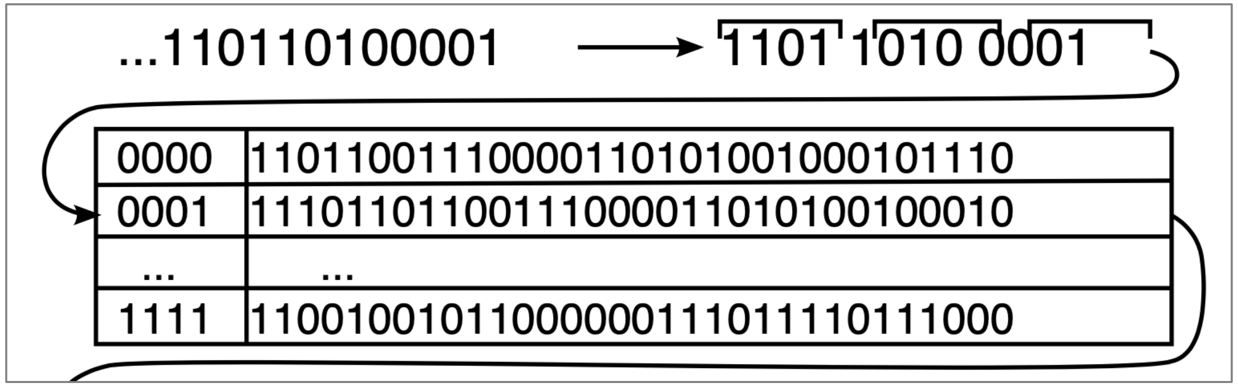
- Symbols versus bits
  - A symbol is the unit of data transfer for a modulated signal
    - Does not necessarily correspond 1:1 with bits
  - The rate of symbols per second is a baudrate

  - 62.5 kBaud = 62500 symbols/second = 250000 bits/second = 250 kbps

802.15.4 actually sends way more data than symbols

- For every 4 bits we want to send (one symbol)
  - 802.15.4 sends 32 bits of data instead

- There’s a mapping from bit pattern to “chip pattern”
  - One mapping that all 802.15.4 PHY layers must use
  - This idea is called “Direct Sequence Spread Spectrum” (DSSS)

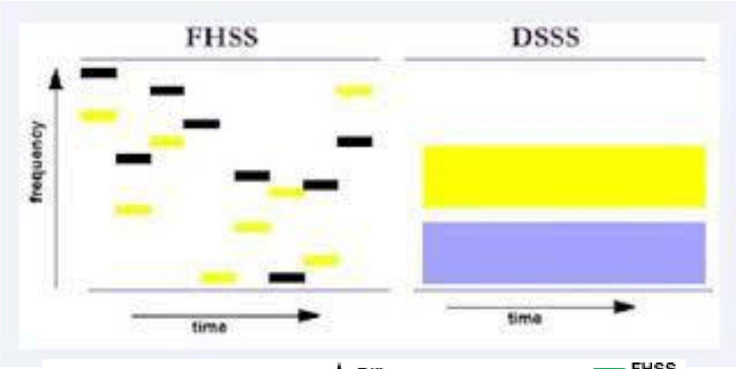


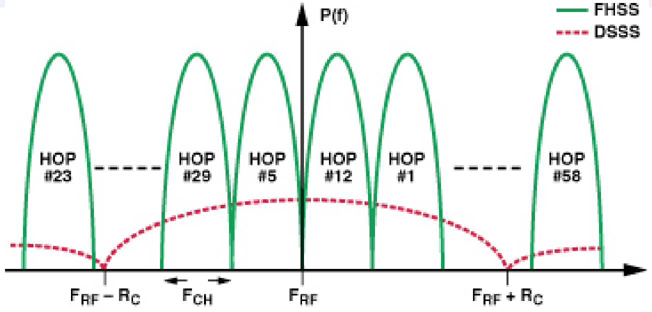
Direct Sequence Spread Spectrum (DSSS)

- Increases the <u>signal</u> bandwidth of a transmission beyond <u>information</u> bandwidth
  - Send sequences of chips, which are a translation of one symbol to a pattern of many bits
  - Chips are transmitted much faster than symbols, essentially increasing the data rate
- Enables better interference avoidance
  - Received bits are correlated against codes to see which is most likely
  - 802.15.4 tolerates many bit flips (see next slide)

Table 1. Zigbee symbol to chip mapping.

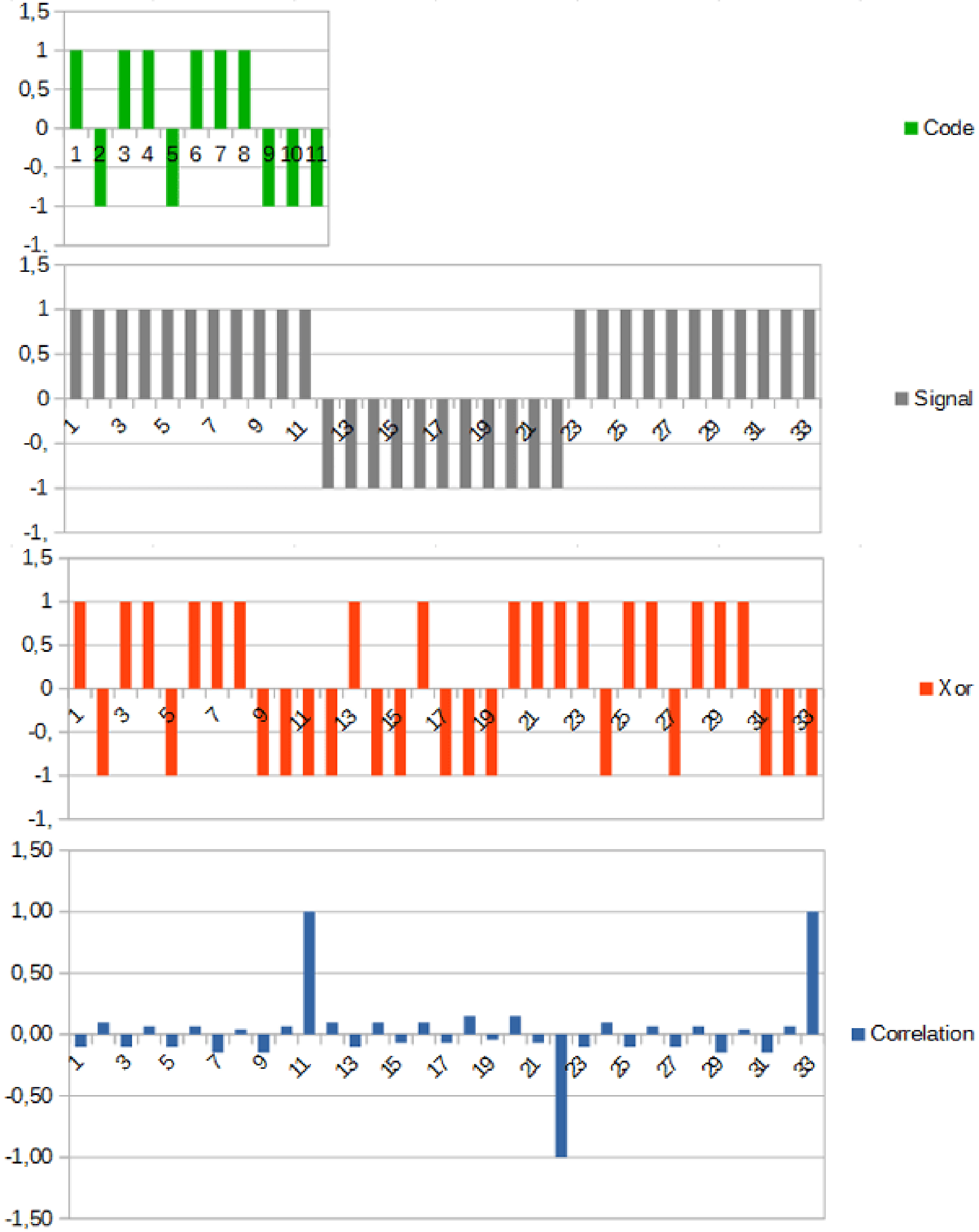
Zigbee Symbol	Chip Values ($c_0c_1....c_{30}c_{31}$)
0000	11011001110000110101001000101110
1000	11101101100111000011010100100010
0100	00101110110110011100001101010010
1100	00100010111011011001110000110101
0010	01010010001011101101100111000011
1010	00110101001000101110110110011100
0110	11000011010100100010111011011001
1110	10011100001101010010001011101101

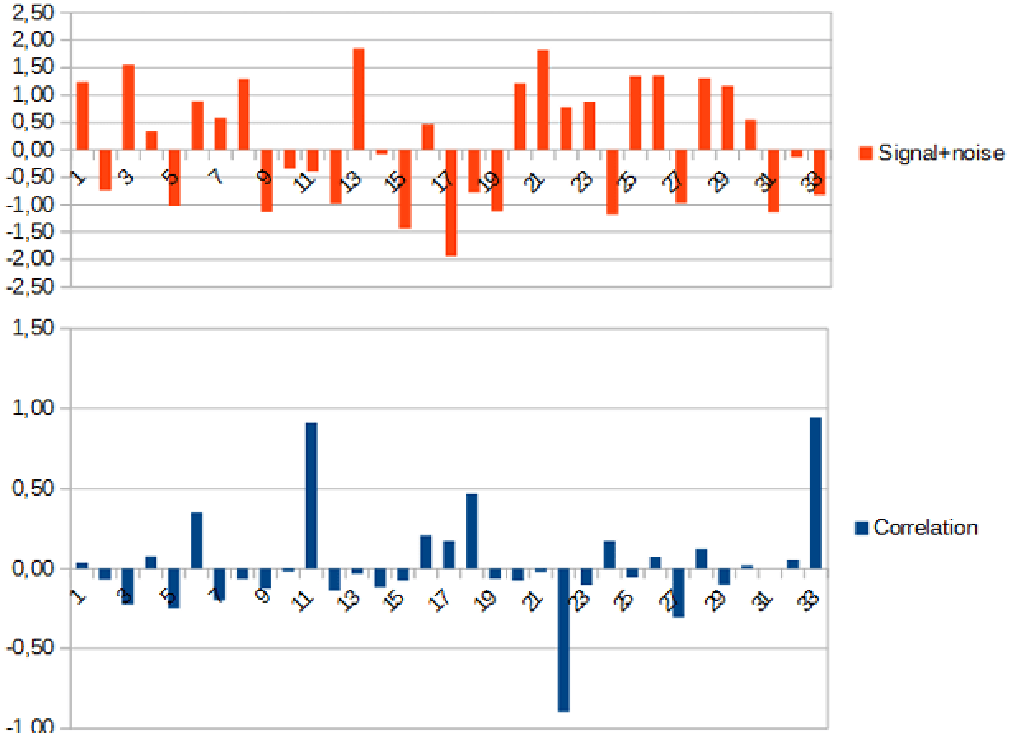




DSSS example

- Data sent is **101**
  - Code is longer than data, so we replicate bits
  - Data is recoverable, even with noise

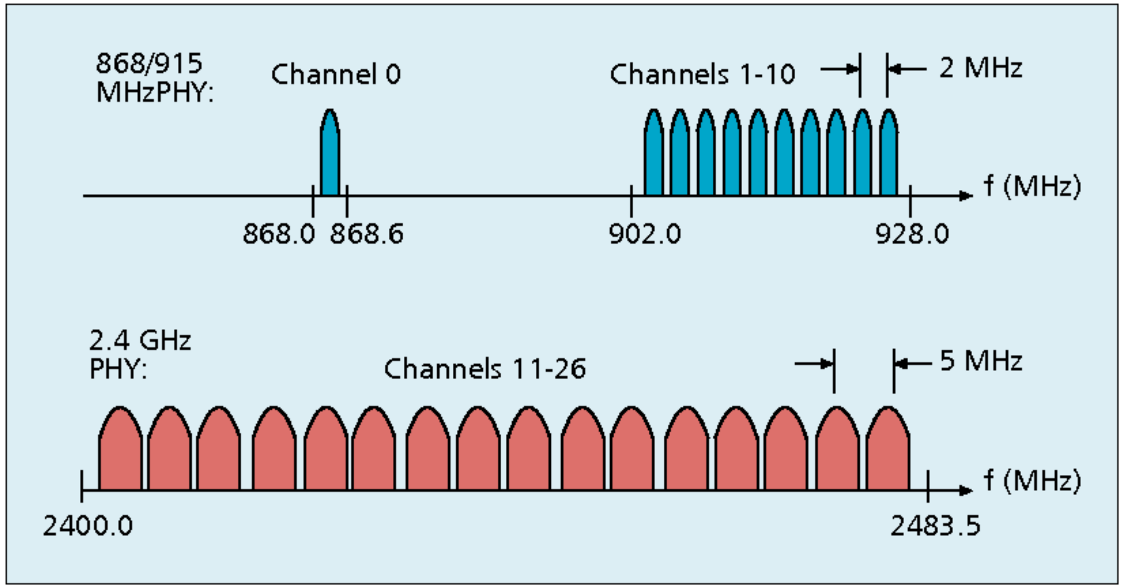


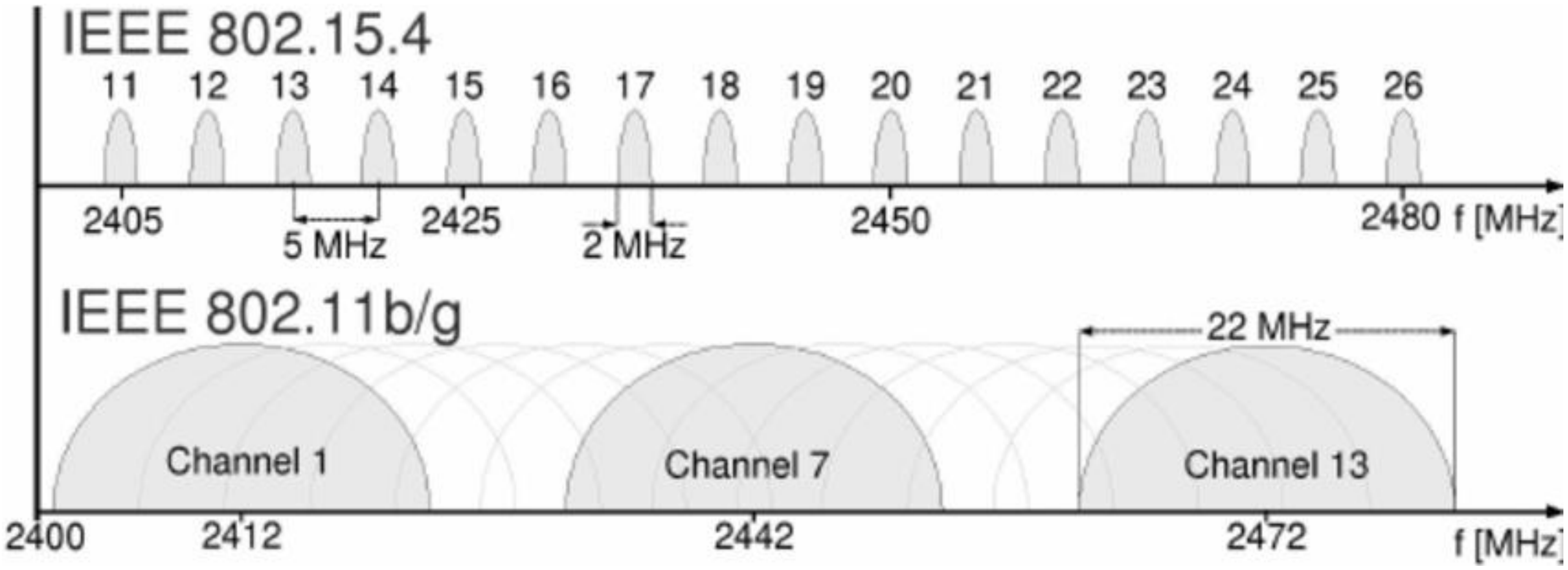


https://circuitcellar.com/research-design-hub/dsss-in-a-nutshell/

802.15.4 RF channels

- 27 channels across three bands
- 5 MHz channel separation at 2.4 GHz
  - Compare to 2 MHz for BLE





Regional bands

- Different RF bands have different regional availability

- Also have different rules
  - 915 MHz: 400 ms dwell time
  - 868 MHz: 1% duty cycle

	Channel	Center Frequency (MHz)	Availability
868 MHz Band	0	868.3	
915 MHz Band	1	906	
	2	908	
	3	910	
	4	912	
	5	914	
	6	916	
	7	918	
	8	920	
	9	922	
	10	924	
2.4 GHz Band	11	2405	
	12	2410	
	13	2415	
	14	2420	
	15	2425	
	16	2430	
	17	2435	
	18	2440	
	19	2445	
	20	2450	
	21	2455	
	22	2460	
	23	2465	
	24	2470	
	25	2475	
	26	2480	

Signal strength

- Transmit power
  - Typical: 0 dBm (remember: 0 dBm equals 1 mW)

- Receiver sensitivity
  - nRF52840 802.15.4: -100 dBm
    - Compare to BLE sensitivity of -95 dBm

  - Minimum acceptable (per spec): -85 dBm
  - Circa-2006 radios (CC2420): -95 dBm

- **Which has longer range, 802.15.4 or BLE? Why?**

Signal strength

- Transmit power
  - Typical: 0 dBm (remember: 0 dBm equals 1 mW)

- Receiver sensitivity
  - nRF52840 802.15.4: -100 dBm
    - Compare to BLE sensitivity of -95 dBm

  - Minimum acceptable (per spec): -85 dBm
  - Circa-2006 radios (CC2420): -95 dBm

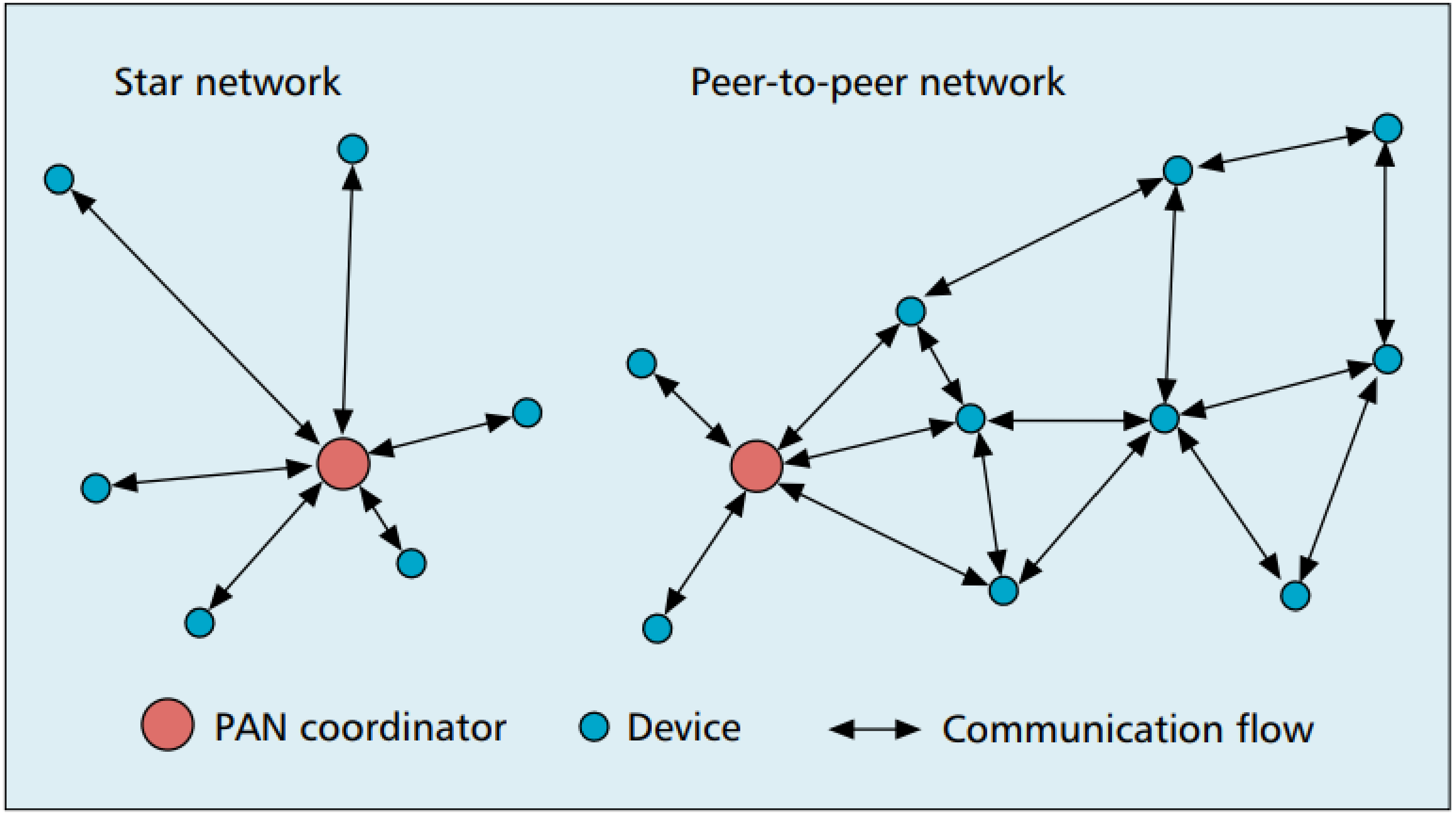
- **Which has longer range, 802.15.4 or BLE? Why?**
  - 802.15.4 with +5 dBm more margin;
    - lower bit rate plays into this, as does increased bandwidth

Outline

- Overview
- Physical Layer
- **Link Layer**
- Packet Structure

802.15.4 network topologies

- Only specifies PHY and MAC, but has use cases in mind



Star and Tree topologies

- PAN Coordinator
  - Receives and relays all messages
  - Most capable and power-intensive
- Coordinators (a.k.a. Routers)
  - Control "clusters"
  - Receives and relays to its children
  - Communicates up to parent coordinator
- End Devices
  - Only communicate with single parent coordinator
  - Least capable and power intensive

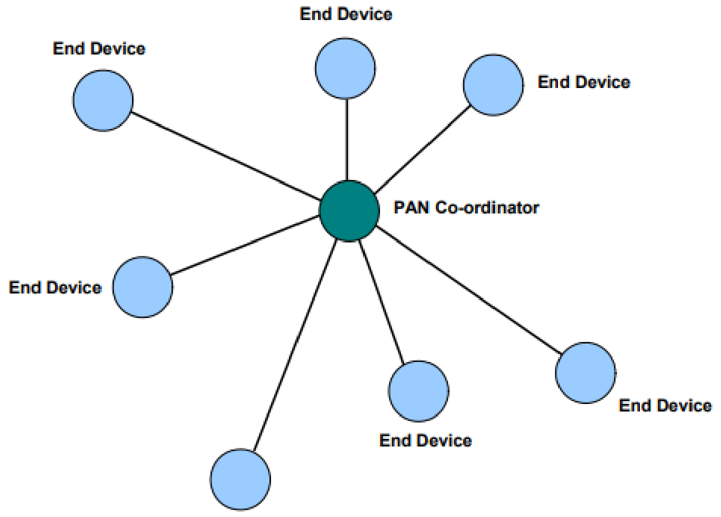


Figure 1: Star Topology

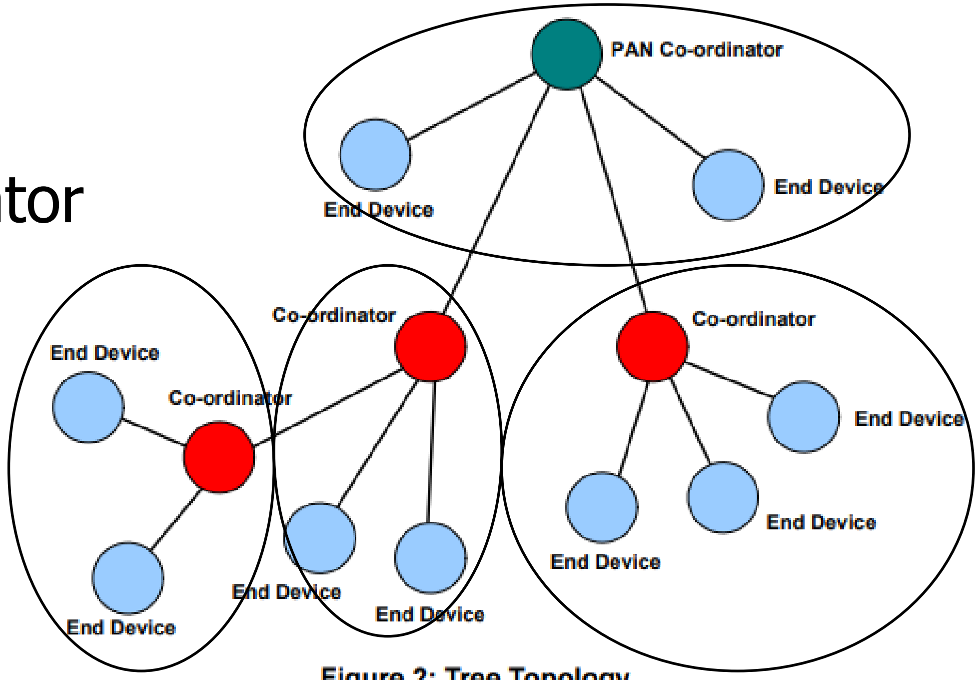


Figure 2: Tree Topology

Break + Mesh networks

- Most devices are capable of communicating with multiple neighbors

- **What are advantages of mesh?**

- **What are disadvantages of mesh?**

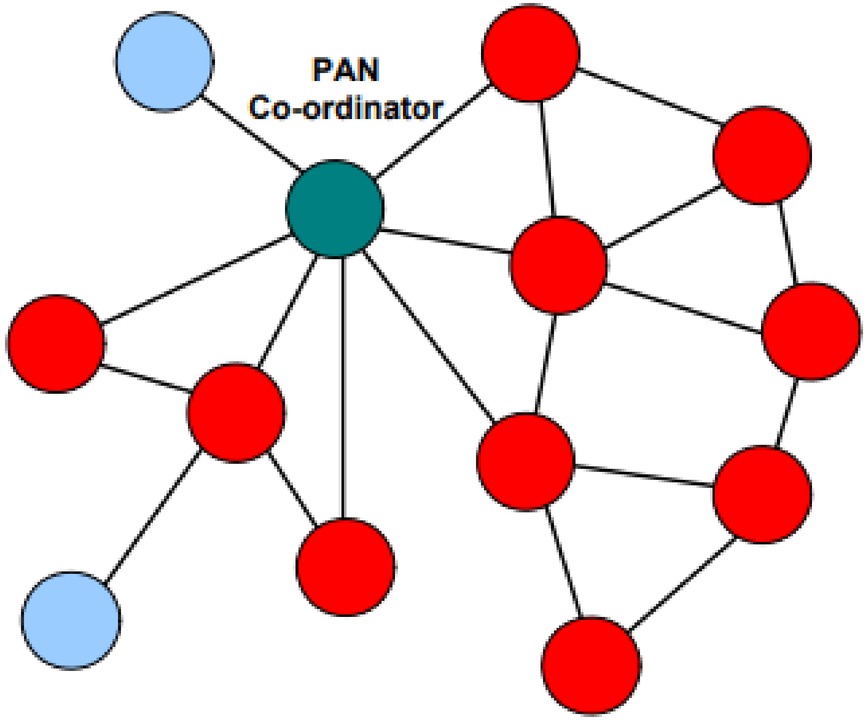


Figure 4: Mesh Topology

Break + Mesh networks

- Most devices are capable of communicating with multiple neighbors

- **What are advantages of mesh?**
  - Devices can communicate over longer distances
  - Device failures less likely to collapse the entire network
- **What are disadvantages of mesh?**
  - Some nodes have to spend more energy communicating
  - Network protocol becomes more complicated to manage routing

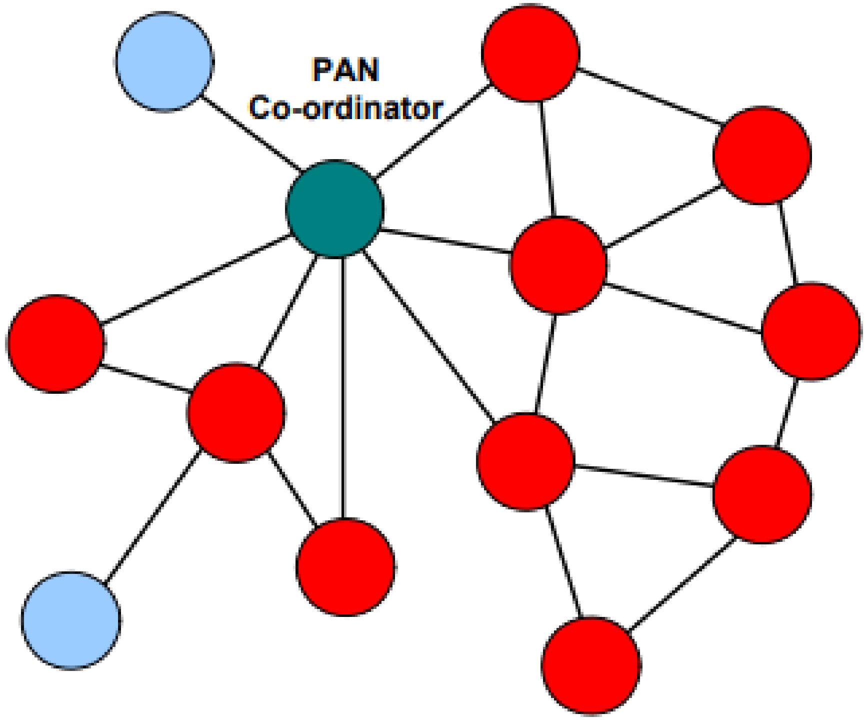


Figure 4: Mesh Topology

Structuring communication

- Big question for any protocol:
  when does each device transmit/listen?

- Transmitting: 802.15.4 uses CSMA

- Listening: multiple options
  1. Structured time windows for coordinating listening across network
     - More complexity, possibly less energy
  2. Coordinators just always listen
     - Less complexity, definitely more energy

Reminder: CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

1. First, wait a random amount (collision avoidance part)
2. Then, listen for a duration and determine if anyone is transmitting (carrier sense part)
   - If idle, you can transmit
   - If busy, repeat step 1 (often increasing maximum wait time)

- Can be combined with notion of slotting
  - Synchronize to slots (smaller than transmit times)
  - Wait for a number of slots
  - Listen for idle slots

Clear Channel Assessment (CCA)

- The “listen” part of CSMA/CA

- Variety of implementations are acceptable
  1. Energy above threshold
     - Energy for 8 symbol durations above threshold (RSSI)

  2. Carrier sense
     - Valid 802.15.4 carrier signal

  3. Energy AND/OR Carrier

Slotted CSMA/CA operation

- Have data to send
- Wait for next backoff slot (synchronized from beacon)
- Wait for 0-7 backoff slots (slot is 20 symbol durations: 320 us)
- Listen for two empty slots
  - Idle: Transmit
  - Occupied: wait 0-15 backoff slots and repeat
    - Next time: 0-31 backoff slots and repeat
    - Next time: 0-31 backoff slots and repeat (upper limit configurable)
    - Next time: 0-31 backoff slots and repeat
    - Next time: 0-31 backoff slots and repeat
    - Timeout

Unslotted CSMA/CA operation

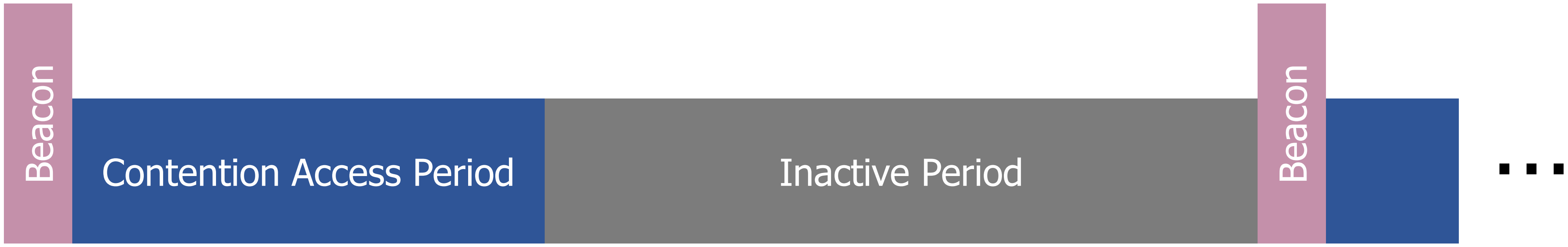
- Have data to send
- ~~Wait for next backoff slot (synchronized from beacon)~~
- Wait for 0-7 backoff slots (slot is 20 symbol durations: 320 us)
- Listen ~~for two empty slots~~
  - Idle: Transmit
  - Occupied: wait 0-15 backoff slots and repeat
    - Next time: 0-31 backoff slots and repeat
    - Next time: 0-31 backoff slots and repeat (upper limit configurable)
    - Next time: 0-31 backoff slots and repeat
    - Next time: 0-31 backoff slots and repeat
    - Timeout

Modes of operation – controls listening and sending

1. Beacon-enabled PAN
    - Slotted CSMA/CA
    - Structured communication patterns
    - Optionally with some TDMA scheduled slots
    - This is the complex, possibly more energy-efficient option

2. Non-beacon-enabled PAN
    - Unslotted CSMA/CA continuously
    - No particular structure for communication
        - Could be defined by other specifications, like Thread or Zigbee
    - This is the simple option

Beacon-enabled superframe structure



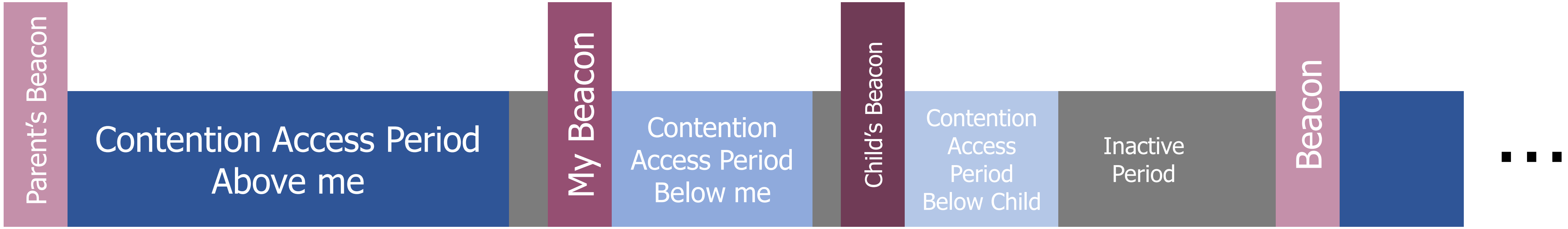
- Beacons occur periodically [15 ms – 245 seconds]
  - Devices must listen to each beacon
- Contention Access Period
  - Slotted CSMA/CA synchronized by beacon start time
- Inactive Period
  - No communication occurring. Assumes sleepy devices

Guaranteed Time Slots (GTS)

- PAN Coordinator may create a Contention Free Period with Guaranteed Time Slots
  - TDMA schedule assigned to specific devices
  - Slots eat up part of the Contention Access Period
  - No CSMA/CA within a guaranteed time slot

Handling tree-based topologies

- All coordinators listen to beacon from PAN coordinator
  - And can participate in that contention period
- Send their own beacons to child devices during inactive period
  - Children participate in that contention period



Non-beacon-enabled PAN

- Same idea, just no beacons
  - Which removes synchronization benefit (and slotted CSMA/CA)
  - Also removes beacon listening cost
    - Devices only need to check for activity before transmitting
  - Still need an algorithm to determine when it should receive data
    - All the time is a huge energy drain
    - Algorithms can get complicated here

Non-beacon-enabled PAN

- Same idea, just no beacons
  - Which removes synchronization benefit (and slotted CSMA/CA)
  - Also removes beacon listening cost
    - Devices only need to check for activity before transmitting
  - Still need an algorithm to determine when it should receive data
    - All the time is a huge energy drain
    - Algorithms can get complicated here
    - **Could BLE mechanism of listen-after-send apply?**

Non-beacon-enabled PAN

- Same idea, just no beacons
  - Which removes synchronization benefit (and slotted CSMA/CA)
  - Also removes beacon listening cost
    - Devices only need to check for activity before transmitting
  - Still need an algorithm to determine when it should receive data
    - All the time is a huge energy drain
    - Algorithms can get complicated here
    - **Could BLE mechanism of listen-after-send apply?**
      - Only if sending to a high-power device, not among equals

Receiving messages on End Devices

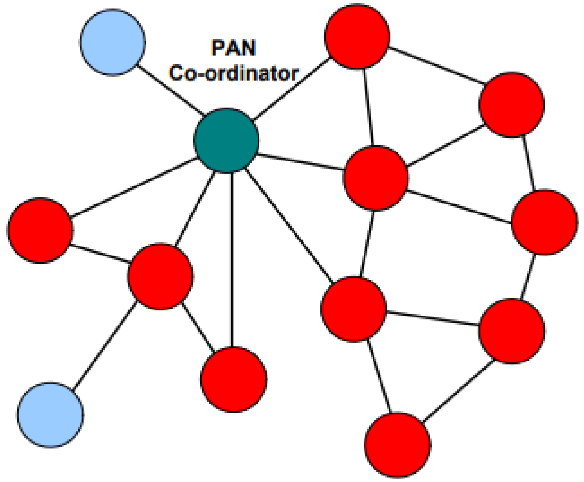


Figure 4: Mesh Topology

1. Listen during entire contention period
    - Can receive direct messages from any other device
    - Can immediately respond to messages as well

2. Request messages from Coordinator
    - Make all communication go through Coordinator
    - Send a request-for-data packet to coordinator to get information
    - Coordinator can include list of devices with pending data in beacon

- More complicated listening algorithms are possible
    - See B-MAC, X-MAC, A-MAC, etc.

Break + Question

- What are benefits/costs of using or not using beacons?
  - Beacons
  - No beacons

Break + Question

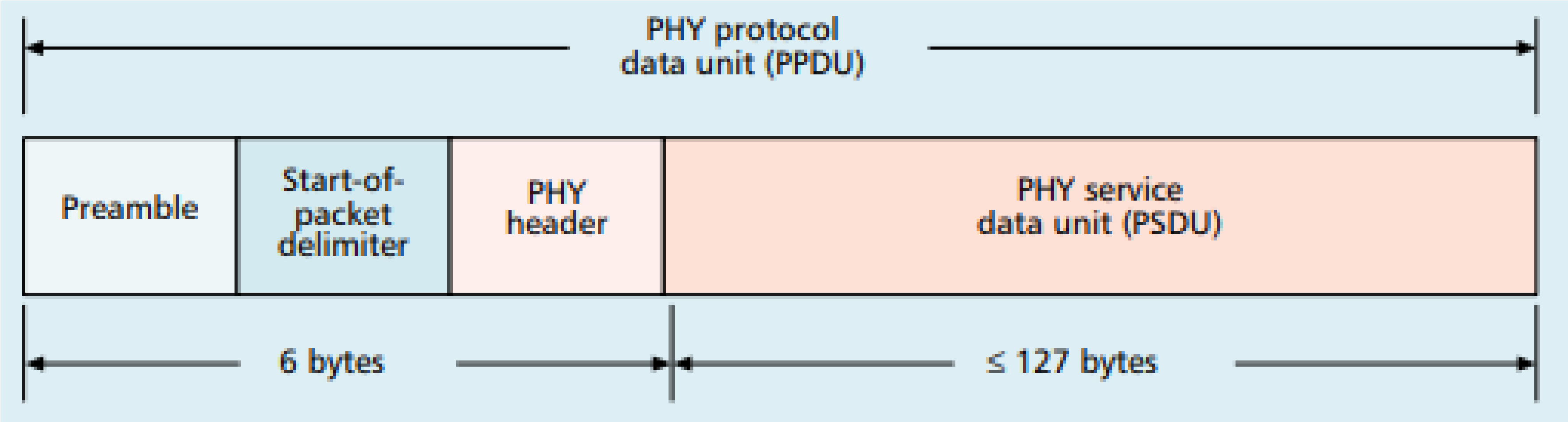
- What are benefits/costs of using or not using beacons?
  - Beacons
    - Enable energy savings by designating period with radios off
    - Enable structured communication like Guaranteed Slots
    - Require some central coordinator within range of all devices
    - Tradeoff in inactive period:
      - communication latency vs beacon-listening costs
  - No beacons
    - Enable all devices to be identical (no coordinator needed)
    - Require custom communication scheme
      - Could be better or worse for various qualities… (always-on radios?)

Outline

- Overview
- Physical Layer
- Link Layer
- **Packet Structure**

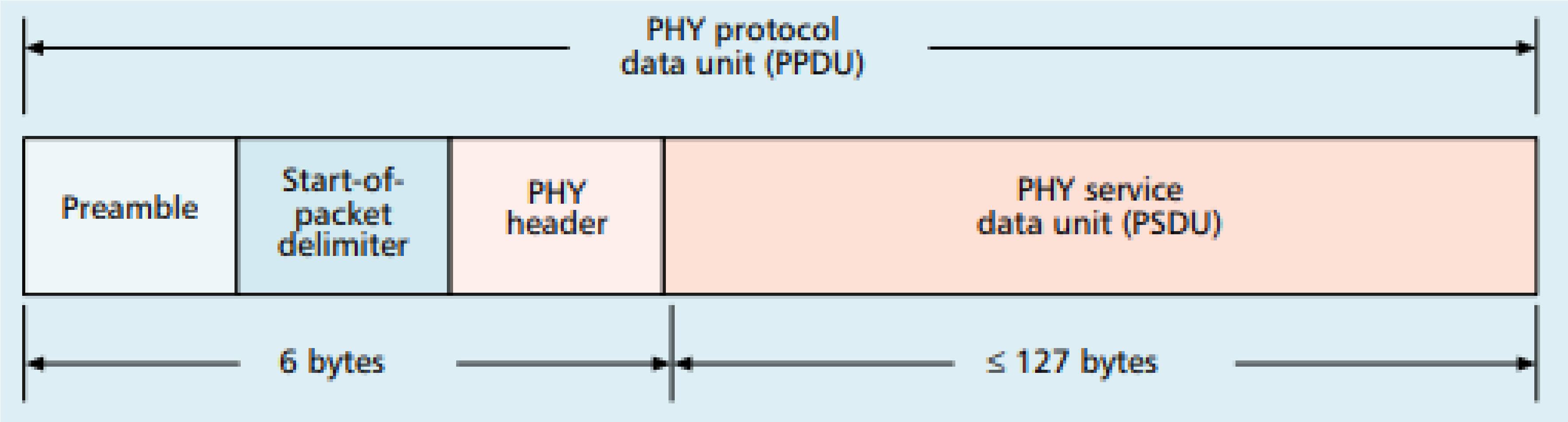
Base packet format

- Synchronization
  - Preamble: four bytes of zeros
  - Start-of-Packet: 0xA7
- PHY Header
  - One field: length 0-127
  - **Why still 8 bits?**



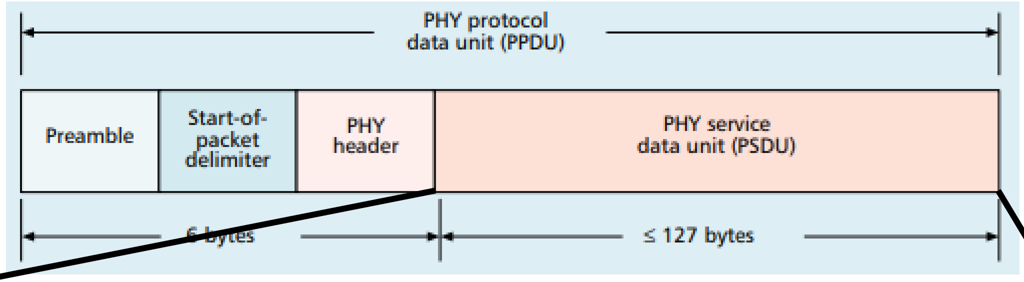
Base packet format

- Synchronization
  - Preamble: four bytes of zeros
  - Start-of-Packet: 0xA7
- PHY Header
  - One field: length 0-127
  - **Why still 8 bits?** **Because computers depend on bytes**



MAC frame format

- Overhead: 5-25 bytes



Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame check sequence
		Addressing fields					
MAC header						MAC payload	MAC footer

- **Frame control**
  - Header with flags
- **Sequence number**
  - 8-bit monotonically increasing
- Addressing fields
  - PAN and addresses
  - Varies based on frame type
- Frame payload
  - Depends on frame type
- Frame check sequence
  - 16-bit CRC

Frame control

Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame check sequence
		Addressing fields					
MAC header						MAC payload	MAC footer

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Security enabled	Frame pending	Ack. Req.	PAN ID compression	Reserved	Dest. addressing mode	Frame version	Source addressing mode

- **Frame type**
  - Type of payload included
  - Beacon, Data, Control, Ack
- Security enabled
  - Packet is encrypted
  - (extra 0-14 byte header)
- **Frame pending**
  - Fragmented packet
- **Acknowledgement required**
- PAN ID compression
  - No PAN ID if intra-network
- Addressing modes
  - Which fields to expect

BLE and 15.4 Packet Comparison

Some observations

- Both have frame types
    - LLID/PDU type for BLE

- 15.4 has
    - Sequence numbers
    - Requested acknowledgements
    - More addressing information

LSB			MSB
Preamble (1 octet)	Access Address (4 octets)	PDU (2 to 257 octets)	CRC (3 octets)

Figure 2.1: Link Layer packet format

LSB		MSB
Header (16 bits)	Payload	MIC (32 bits)

Figure 2.12: Data Channel PDU

Header					
LLID (2 bits)	NESN (1 bit)	SN (1 bit)	MD (1 bit)	RFU (3 bits)	Length (8 bits)

Figure 2.13: Data channel PDU header

LSB					MSB
PDU Type (4 bits)	RFU (2 bits)	TxAdd (1 bit)	RxAdd (1 bit)	Length (6 bits)	RFU (2 bits)

Figure 2.3: Advertising channel PDU Header

Connection Data Packet

Length (16 bits)	Channel ID (16 bits)	L2CAP SDU Length* (16 bits)	Information Payload (0 to 249 octets)

OR

Advertising PDU

Advertiser Address 6 Bytes	Advertiser Data (Payload) 0-31 Bytes

Frame types - Beacon

2	variable	variable	variable
Superframe Specification	GTS fields (Figure 45)	Pending address fields (Figure 46)	Beacon Payload
MAC Payload			

- Beacon
  - Information about the communication structure of this network
  - Sent in response to requests from scanning devices
  - Sent periodically at start of Superframes (if in use)
    - Sent without CSMA/CA

- MAC Header configuration
  - Source address only, broadcast to everyone

- Packet contents
  - Superframe details, including Guaranteed Time Slots (if any)
  - Pending addresses lists devices for which Coordinator has data

Frame types - Data

- Data
    - Data from higher-layer protocols
- MAC Header configuration
    - Source and/or Destination addresses as necessary
- Packet Contents
    - Whatever bytes are desired (122 bytes minus address sizes)
    - May be fragmented across packets for longer data

Frame types – MAC Command (i.e., control)

1	variable
Command Frame Identifier	Command Payload
MAC Payload	

- MAC Command
  - Various commands for supporting link layer
    - Join/leave network
    - Change coordinator within network
    - Request data from coordinator
    - Request Guaranteed Time Slot

- MAC Header configuration
  - Source and/or Destination addresses as necessary

Frame types - Acknowledgement

- Acknowledgement packet
  - Acknowledges a Data or MAC Command packet
  - Not beacons or other acknowledgements
    - Acknowledging acknowledgements gets problematic…
  - Retransmission if no acknowledgement received

- MAC Header
  - Repeats Sequence Number of acknowledged packet
  - No Source or Destination addresses

- Sent T_{IFS} after the packet it is acknowledging (immediately)
  - Time of Inter-Frame Spacing (standard delay between packets)

Analysis: maximum goodput

- Assume best possible case for data transmission
  - 133 total Bytes per packet (122 payload bytes + 11 bytes of headers)
    - At 250 kbps -> 4.256 ms duration
  - Plus Inter-frame spacing of 40 symbols
    - At 62.5 kBaud -> 0.640 ms duration

  - 122 Bytes / 4.896 ms -> **199 kbps goodput**

    - Compare to BLE advertisements: 9.92 kbps goodput
      - Better with BLE 5.0 extended advertisements

    - Compare to BLE connections: 520 kbps goodput
      - Better with BLE 6.0 improvements

Outline

- Overview
- Physical Layer
- Link Layer
- Packet Structure