

# **Lecture 03**

## **Data Link Layer + BLE Introduction**

CS433 – Wireless Protocols for IoT  
Branden Ghena – Spring 2025

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

# Administrivia

- Hw: Background
  - Goal: brush up on some embedded systems and networks background
  - Due tonight
  - Submit on Gradescope
- Lab: Wireshark
  - Goal: familiarize yourself with Wireshark
    - Install it, do some basic scanning, explore a little
  - We'll do checkoffs during lab time tomorrow
    - Friday 11:00-12:30 pm in Frances Searle 2370
    - See you all there!

# Partnership survey

- Labs (after this first one) will be in groups of exactly three
- I'm trying to
  1. Figure out what the groups are
  2. Match up students who need groups
- Please fill out the survey posted on Piazza
- I'll go through this weekend and match up groups

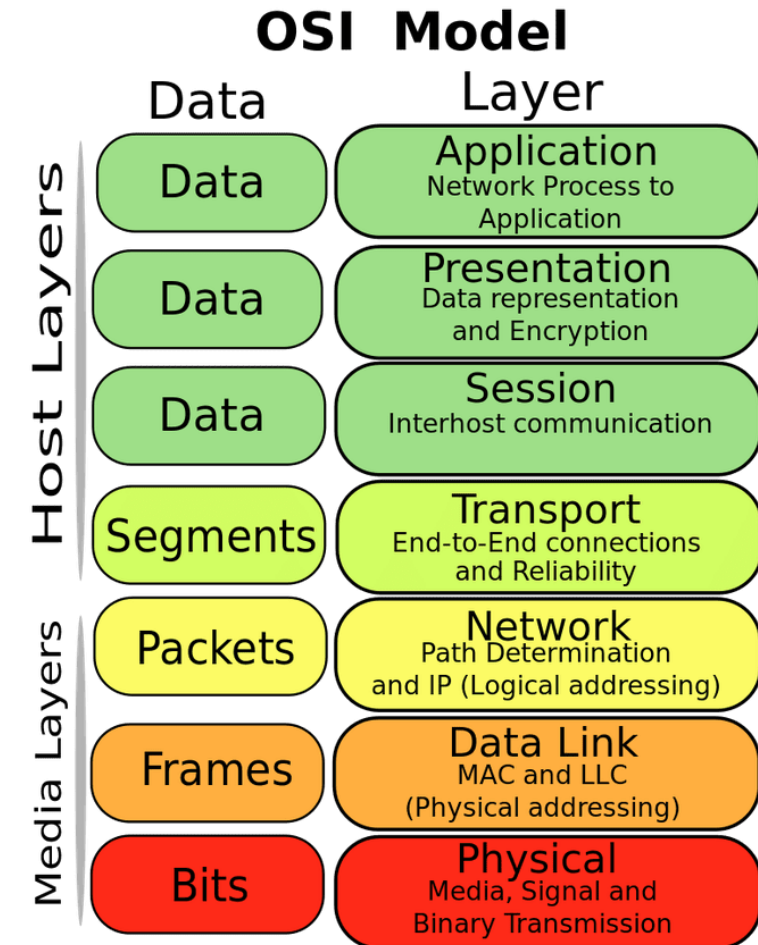
# Today's Goals

- Overview of concerns for the Data link layer
  - Speak the “lingo” of wireless communication
  - Present technology aspects that we will return to in specific protocols
- Describe Medium Access Control mechanisms
- Introduction to Bluetooth Low Energy
  - What are the goals of the protocol?
  - What do the lower layers look like?

# Review: OSI model of communication layers

- Transport
  - Sending data between applications
  - TCP and UDP
- Network
  - Sending data between networked computers
  - IP
- Data Link
  - Sending collections of bits
  - Ethernet, WiFi
- Physical
  - Sending individual bits
  - Ethernet, WiFi

Open Systems Interconnection (OSI)



# Review: A programmer's view of the internet

## 1. Hosts are mapped to a set of 32-bit **IP addresses**

- 129.105.7.30

## 2. The set of IP addresses is mapped to a set of identifiers called Internet **domain names**

- 129.105.7.30 is mapped to moore.wot.eecs.northwestern.edu

## 3. A process on one Internet host can communicate with a process on another Internet host over a **connection**

# Review: Signal qualities

## 1. Signal strength

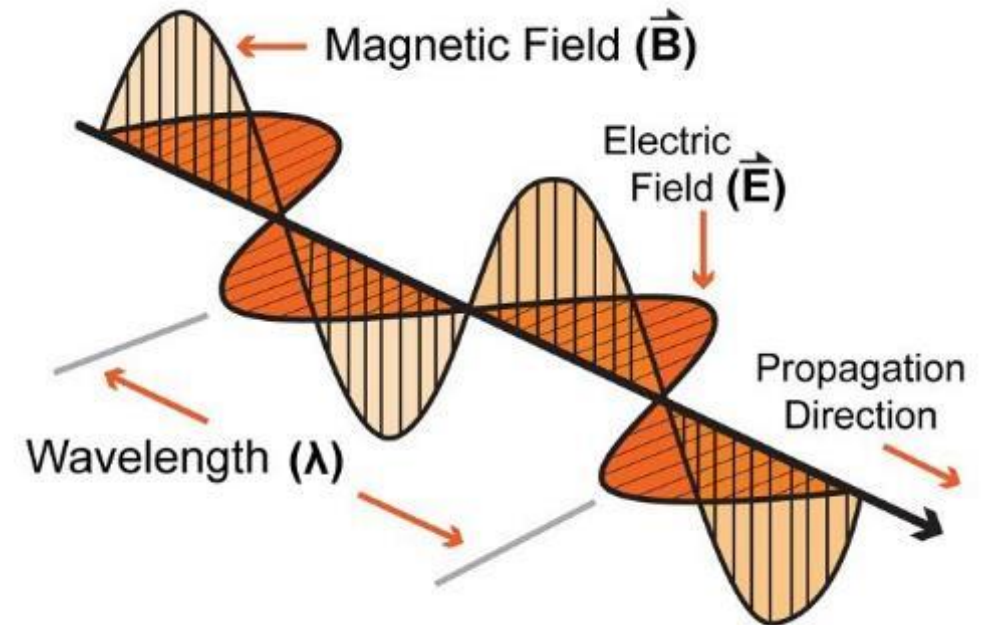
- The amount of energy transmitted/received

## 2. Signal frequency and bandwidth

- Which "channel" the signal is sent on

## 3. Signal modulation

- How data is encoded in the signal



# Review: Signal strength

- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)



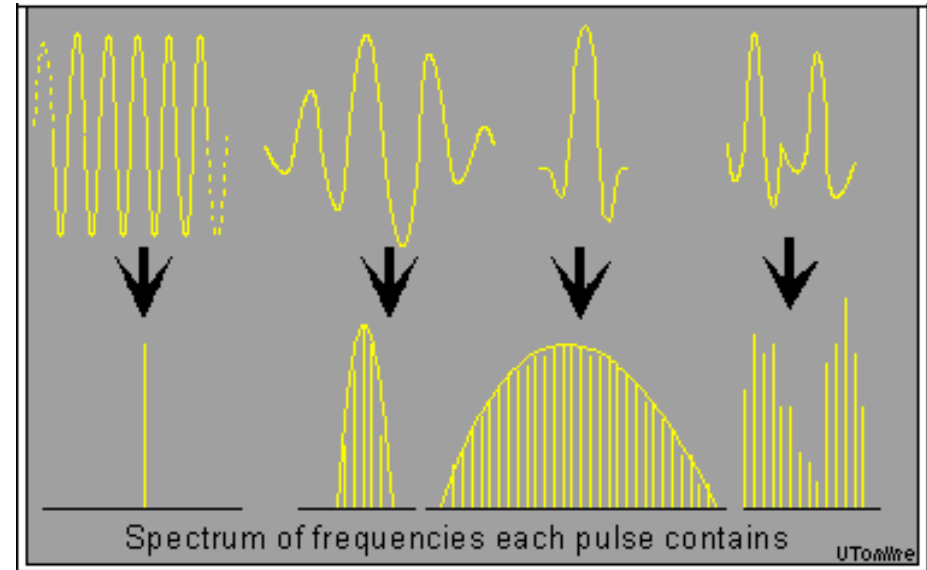


# Big Idea: many RF factors are interconnected

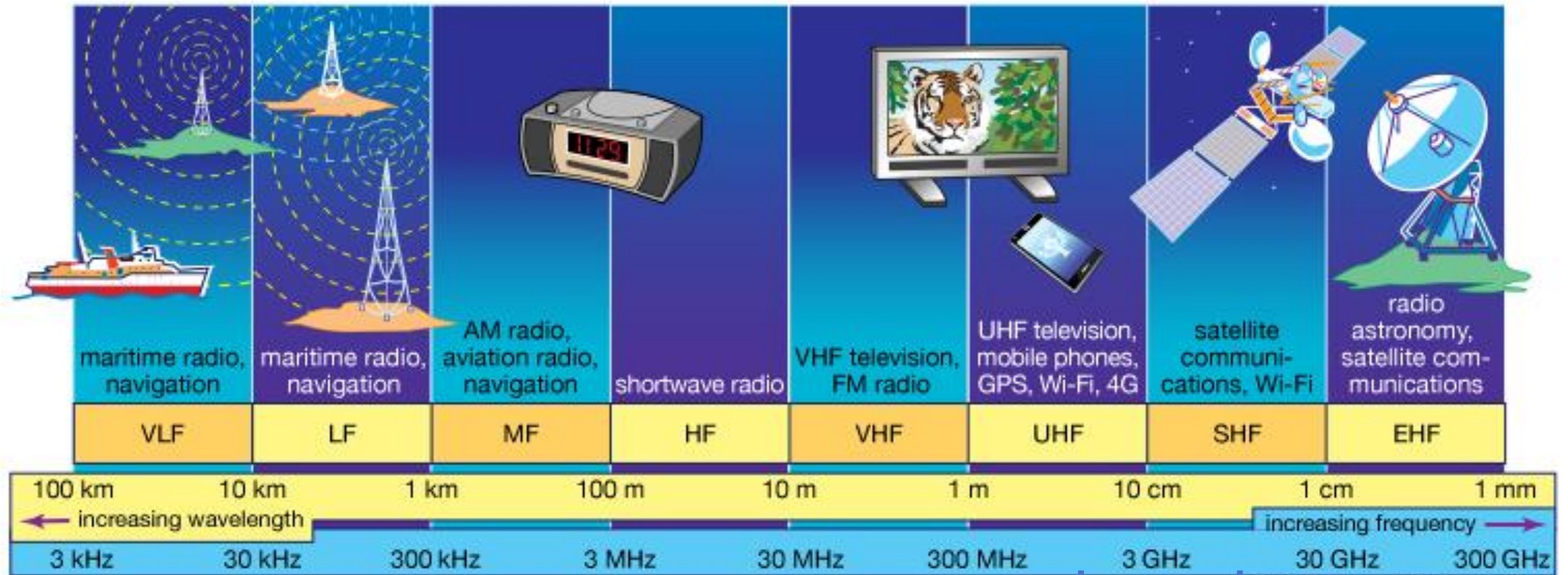
- Energy, Distance, Throughput, and Reliability are all interconnected in communication
- Protocols make choices of some and get the results on the others
- To get more distance, choose one or more:
  - Increase energy
  - Communicate slower
  - Accept a higher error rate

# Review: frequency and bandwidth

- A pure sinusoid is energy at exactly one frequency
- A messy sinusoid with data layered on top of it has nearby energy
  - There's a center of the signal energy
  - Plus some amount of width, which depends on how complicated the data layered on top is



# Review: RF communication frequencies



© 2013 Encyclopædia Britannica, Inc.

**IoT focus**

# Wireless spectrum is limited...and valuable

- FCC auctioned off 3.5 GHz spectrum in August 2020
  - 70 MHz
  - \$4.6 billion
- FCC auctioned off 2.5 GHz spectrum in 2022
  - \$427 million

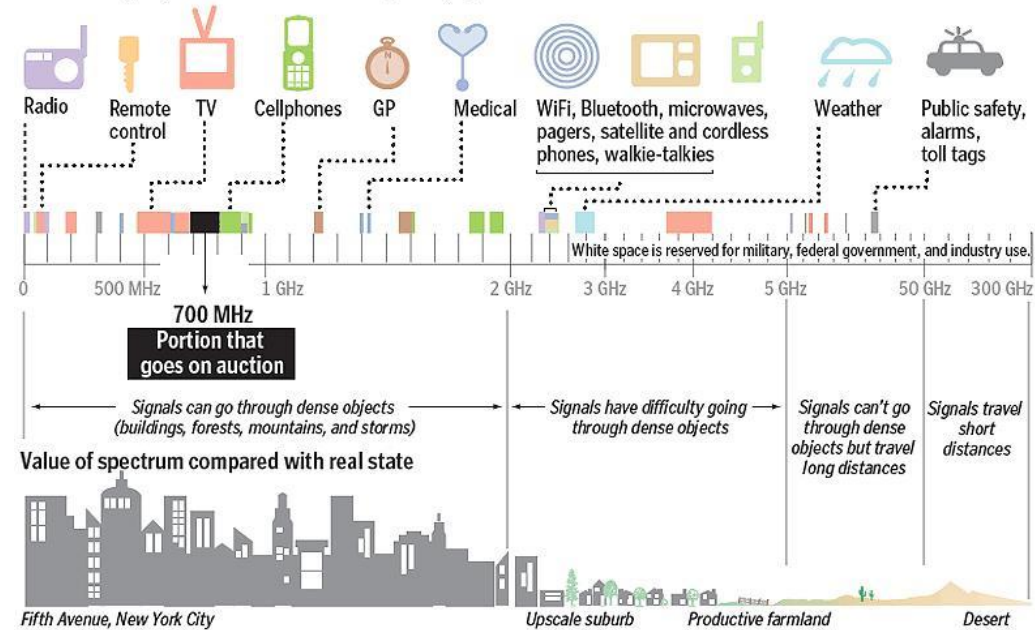


**Media Contact:**  
Will Wiquist, (202) 418-0509  
will.wiquist@fcc.gov

**For Immediate Release**

**FCC CONCLUDES FIRST 5G MID-BAND SPECTRUM AUCTION**  
*3.5 GHz Spectrum Will Promote Innovation and Advance U.S. Leadership in 5G*

Some everyday uses of the radio frequency spectrum



SOURCE: New America Foundation; FCC

JOAN McLAUGHLIN/GLOBE STAFF

WIRELESS

## T-Mobile pays \$304M to fill in holes in its 2.5 GHz spectrum

By Linda Hardesty · Sep 1, 2022 5:39pm

T-Mobile

2.5 GHz

spectrum auction

<https://www.fiercewireless.com/wireless/t-mobile-pays-304m-fill-holes-its-25-ghz-spectrum>

# Outline

- **Physical Layer**
  - Overview
  - Signal Strength
  - Signal Frequency and Bandwidth
  - **Signal Modulation**
- Data Link Layer
- BLE Background

# Signal qualities

## 1. Signal strength

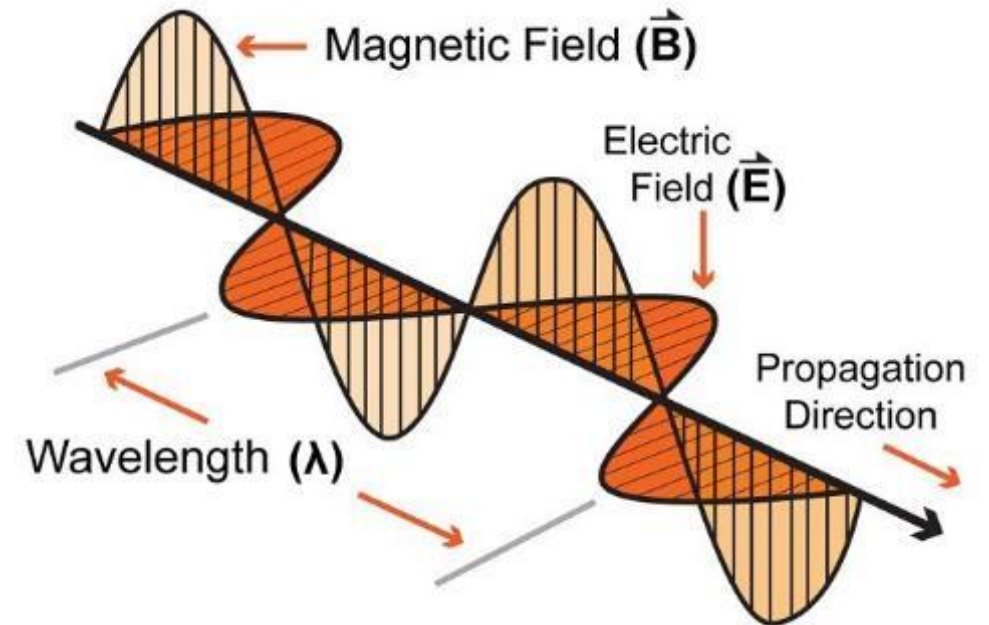
- The amount of energy transmitted/received

## 2. Signal frequency and bandwidth

- Which “channel” the signal is sent on

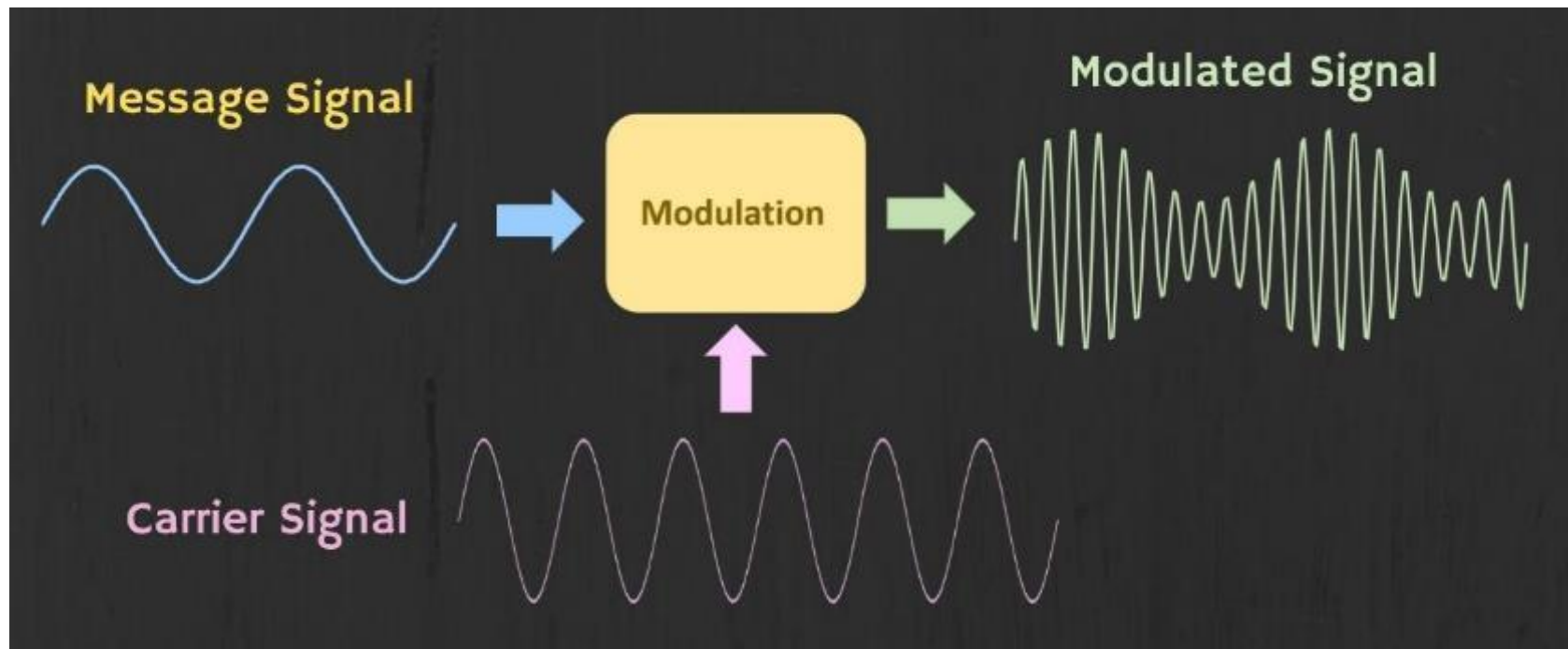
## 3. Signal modulation

- How data is encoded in the signal



# Modulation

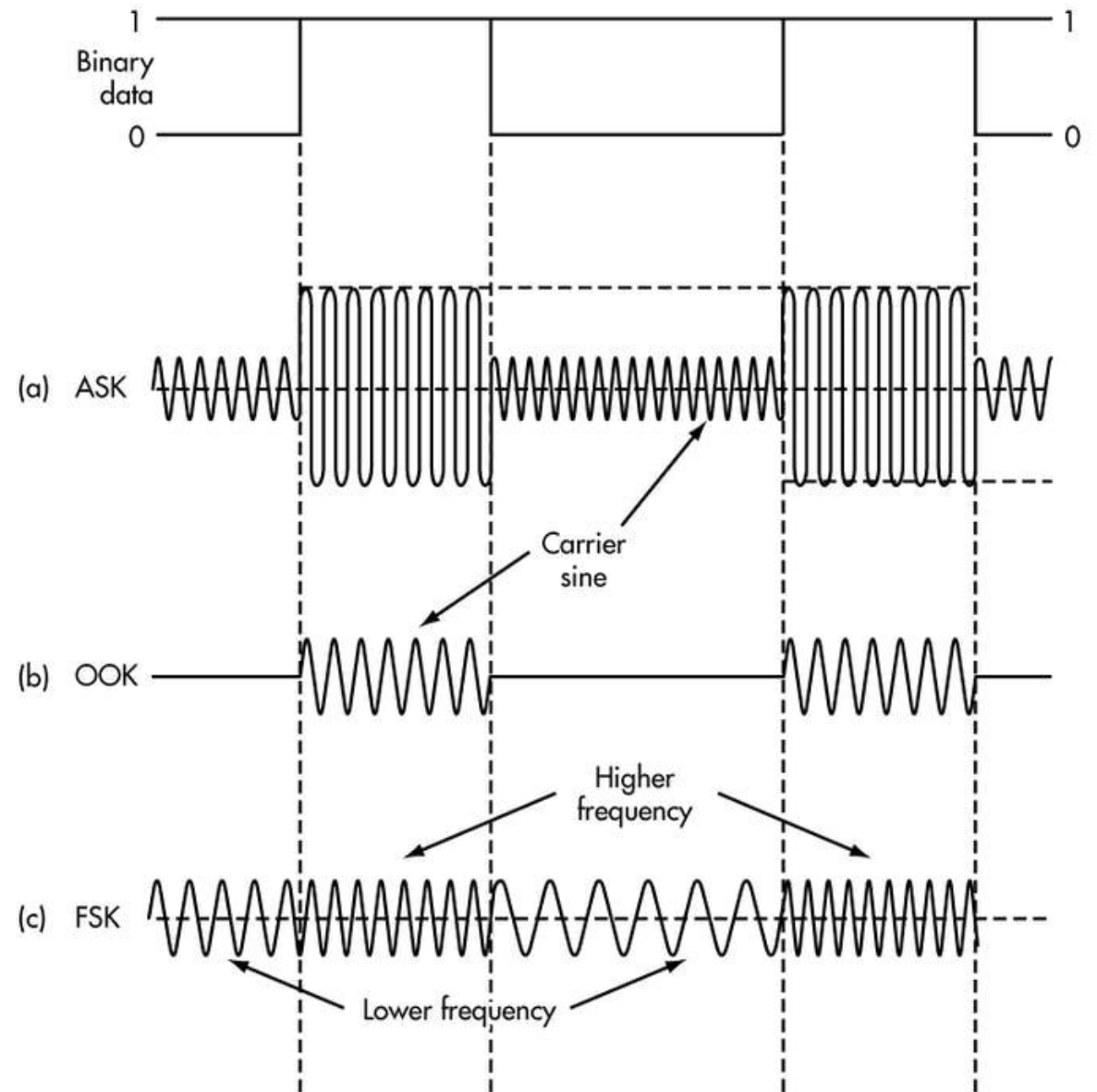
- Encoding signal data in an analog “carrier” signal
  - Carrier signal defines the frequency
  - Modulation scheme + data define bandwidth required





# Modulation types

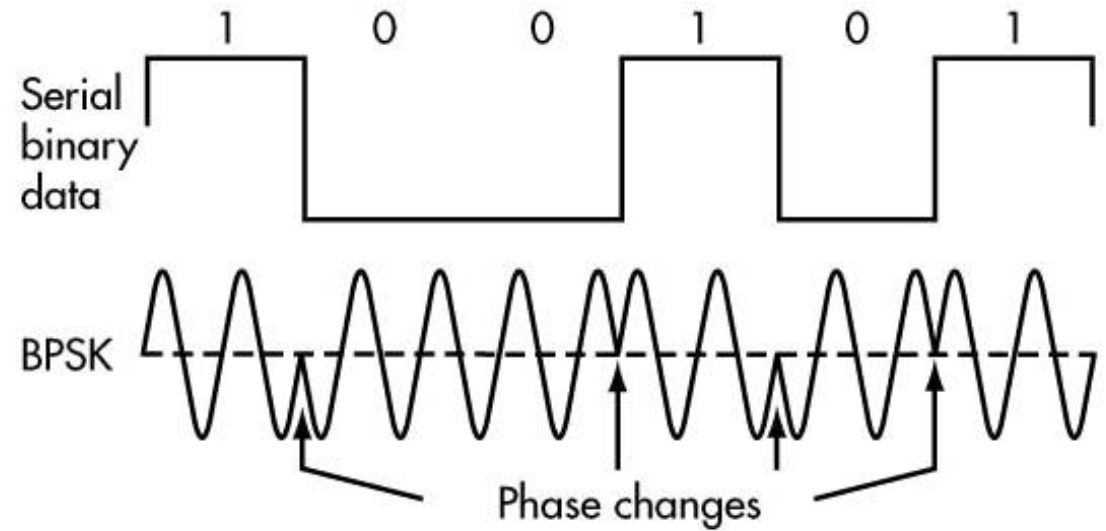
- Encoding binary data on a signal
- Amplitude-shift Keying (ASK)
  - Modify amplitude of carrier signal
  - On-Off Keying (OOK) is an extreme example
- Frequency-shift Keying (FSK)
  - Modify frequency of carrier signal





# Modulation types

- Phase-shift keying (PSK)
  - Modify phase of carrier signal
  - Often differential:  
the change signifies data
- More complicated possibilities exist
  - QAM (Quadrature Amplitude Modulation) combines amplitude and phase shift keying
    - Allows for more than one bit per “symbol”



# Modulation tradeoffs

- Various tradeoffs between different modulation schemes
  - Bandwidth requirements, transceiver hardware, immunity to noise, etc.
- ASK (amplitude) is simple but susceptible to noise
  - Noise exists in the real world
- FSK (frequency) is relatively simple and robust to noise, but uses more bandwidth
  - Bandwidth is limited, but this modulation is still commonly used
- PSK (phase) energy efficient and robust, but more complex hardware
  - More expensive hardware, but very commonly used

# Break + Video

- Excellent explanation of modulation techniques:  
<https://youtu.be/0faCad2kKeg?si=kK6l0g63XGVPdut9&t=240>
  - Listen for 3.5 minutes until 7:30 in the video
- “How Cell Service Actually Works” by Wendover Productions

# Outline

- Physical Layer
  - Overview
  - Signal Strength
  - Signal Frequency and Bandwidth
  - Signal Modulation
- **Data Link Layer**
- BLE Background

# Data Link Layer

- Framing
  - Combine arbitrary bits into a “packet” of data
- Logical link control
  - Manage transfer between transmitter and receiver
  - Error detection and correction
- Media access
  - Controlling which device gets to transmit next
- Inherently coupled to PHY and its decisions

# Framing

- Typical packet structure
  - Preamble - Existence of packet and synchronization of clocks
  - Header - Addresses, Type, Length
  - Data - Payload plus higher layer headers (e.g. IP packet)
  - Trailer - Padding, CRC



- Possible wireless considerations
  - Control information for Physical Layer
  - Ensure robustness for header
  - Explicit multi-hop routing
  - Possibly different data rates for different parts of packet

# Error control: detection and recovery

- Detection: only detect errors
  - Make sure corrupted packets get discarded
  - Cyclical Redundancy Checks
    - Detect single bit errors
    - Detect “burst” errors of several contiguous bits
- Recovery: also try to recover from small bit errors
  - Forward error correction
  - Retransmissions
  - Far more important for wireless because the cost of transmission is higher

# Medium Access Control

- How does a network determine which transmitter gets to transmit?
- Remember: the wireless medium is inherently broadcast
  - Two simultaneous transmitters may lose both packets



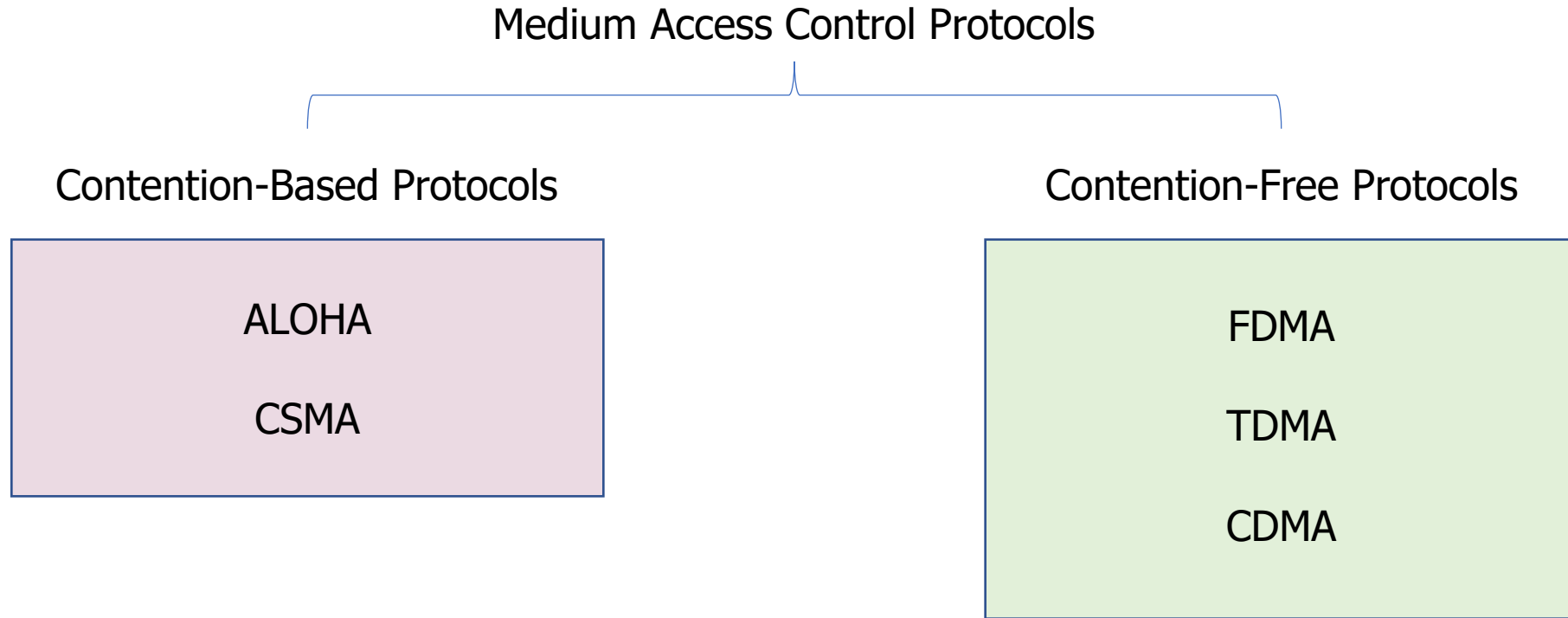
# Analogy: wireless medium as acoustic

- How do we determine who gets to speak?
  - Two simultaneous speakers also lose both “transmissions”
- **Task:** Break into groups of 5 students each
  - In a minute I’m going to ask each group a question
  - Everyone in the group needs to answer correctly
  - Fastest group to have everyone answer wins
  - If two people talk at the same time, that group loses

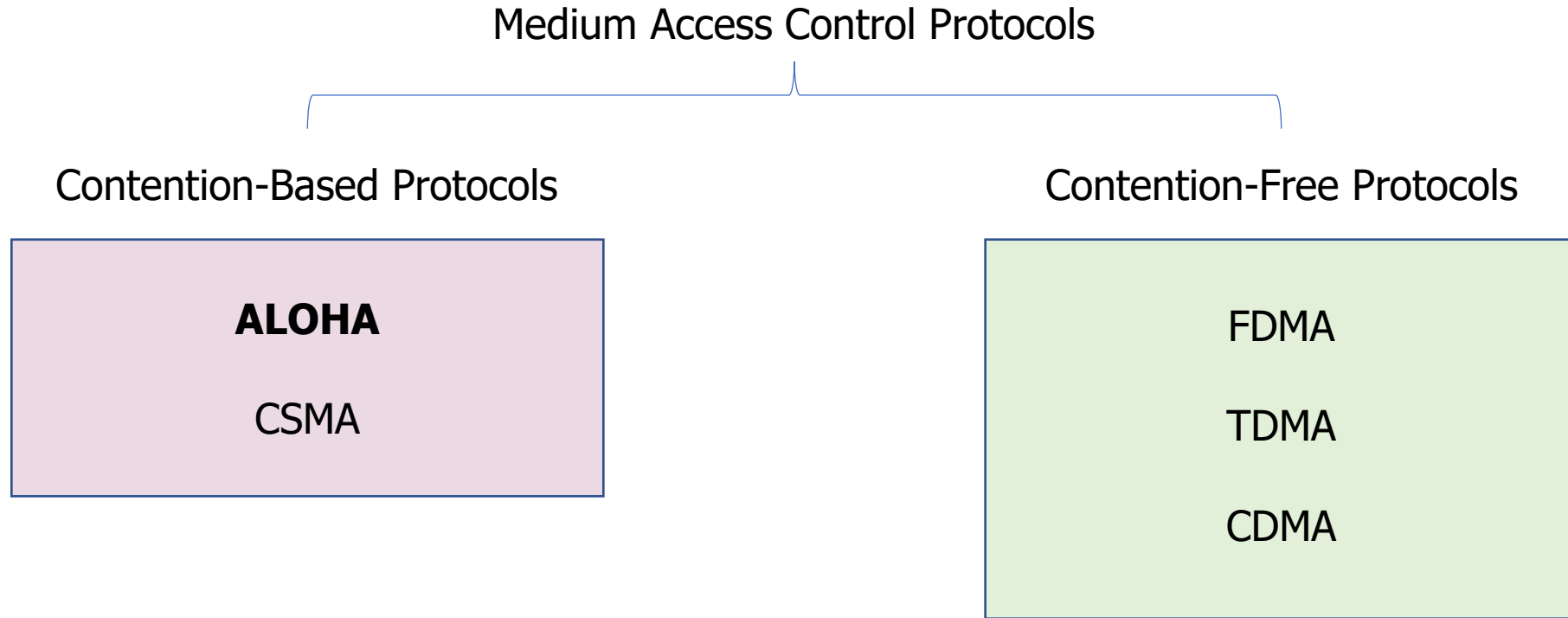
# Analogy: wireless medium as acoustic

- How do we determine who gets to speak?
  - Two simultaneous speakers also lose both “transmissions”
- Eye contact (or raise hand) -> out-of-band communication
- Wait until it's quiet for some time -> carrier sense multiple access
- Strict turn order -> time division multiple access
- Just speak and hope it works -> ALOHA
- Everybody sing at different tones -> frequency division multiple access (stretching the metaphor)
- Everyone speak in different languages -> code division multiple access (sort of, but not really)
- Others?

# MAC protocol categorization



# MAC protocol categorization

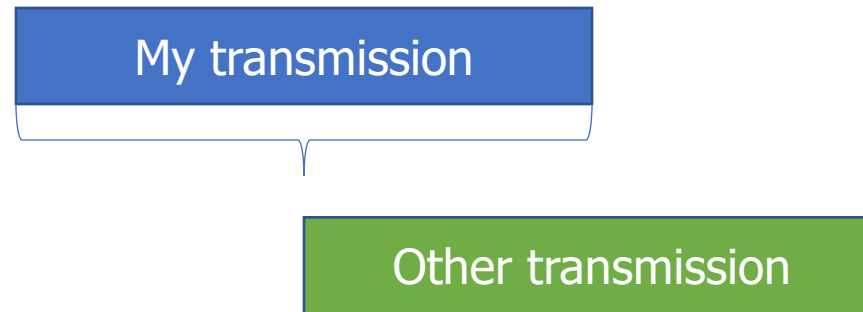


# ALOHA

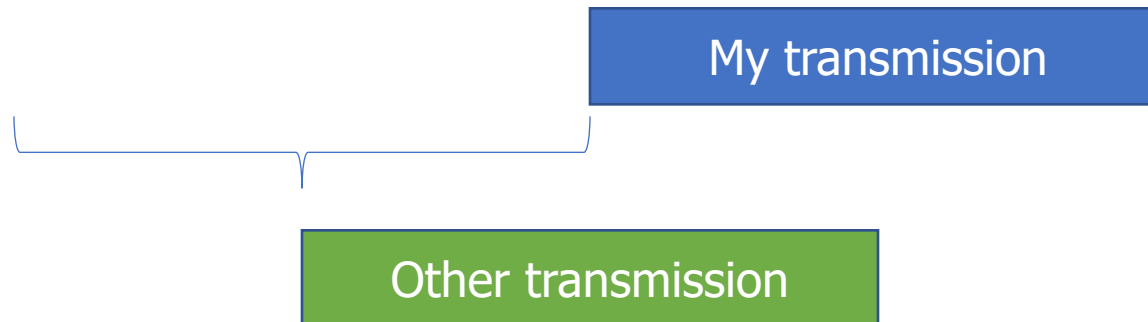
- ALOHAnet (1971)
  - University of Hawaii – Norman Abramson
  - First demonstration of wireless packet network
- Rules
  1. If you have data to send, send it
- Two (or more) simultaneous transmissions will collide and be lost
  - Wait a duration of time for an acknowledgement
  - If transmission was lost, try sending again “later”
    - Want some kind of exponential backoff scheme here

# Packet collisions

- Each packet transmission has a window of vulnerability
  - Twice the on-air duration of a packet
  - Transmissions during the packet are bad

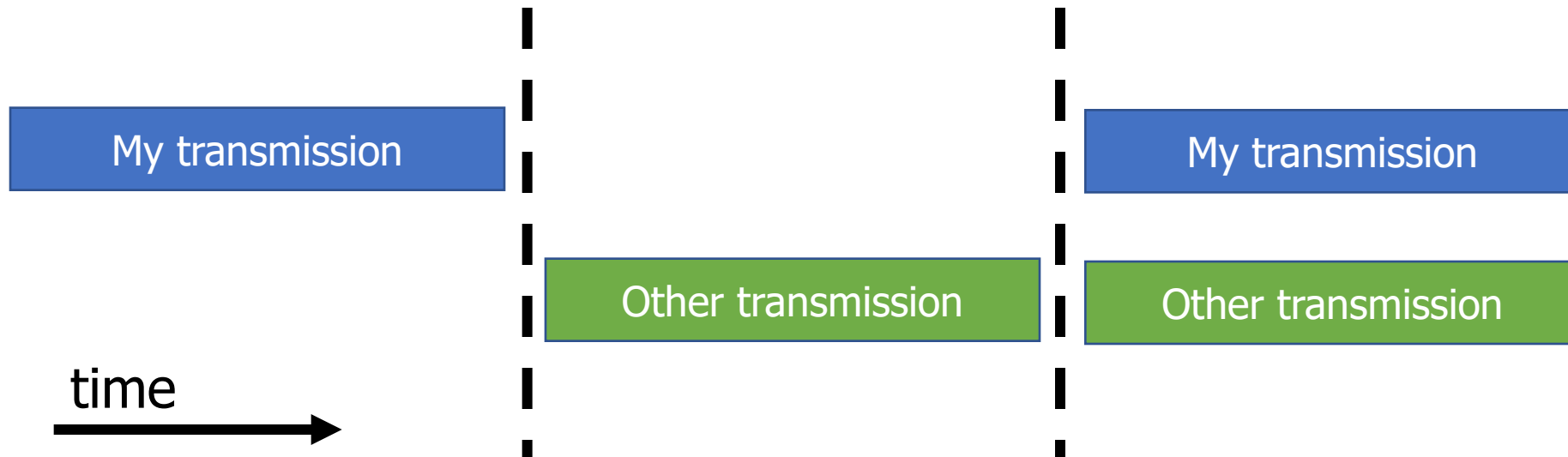


- Transmissions before packet can also be bad



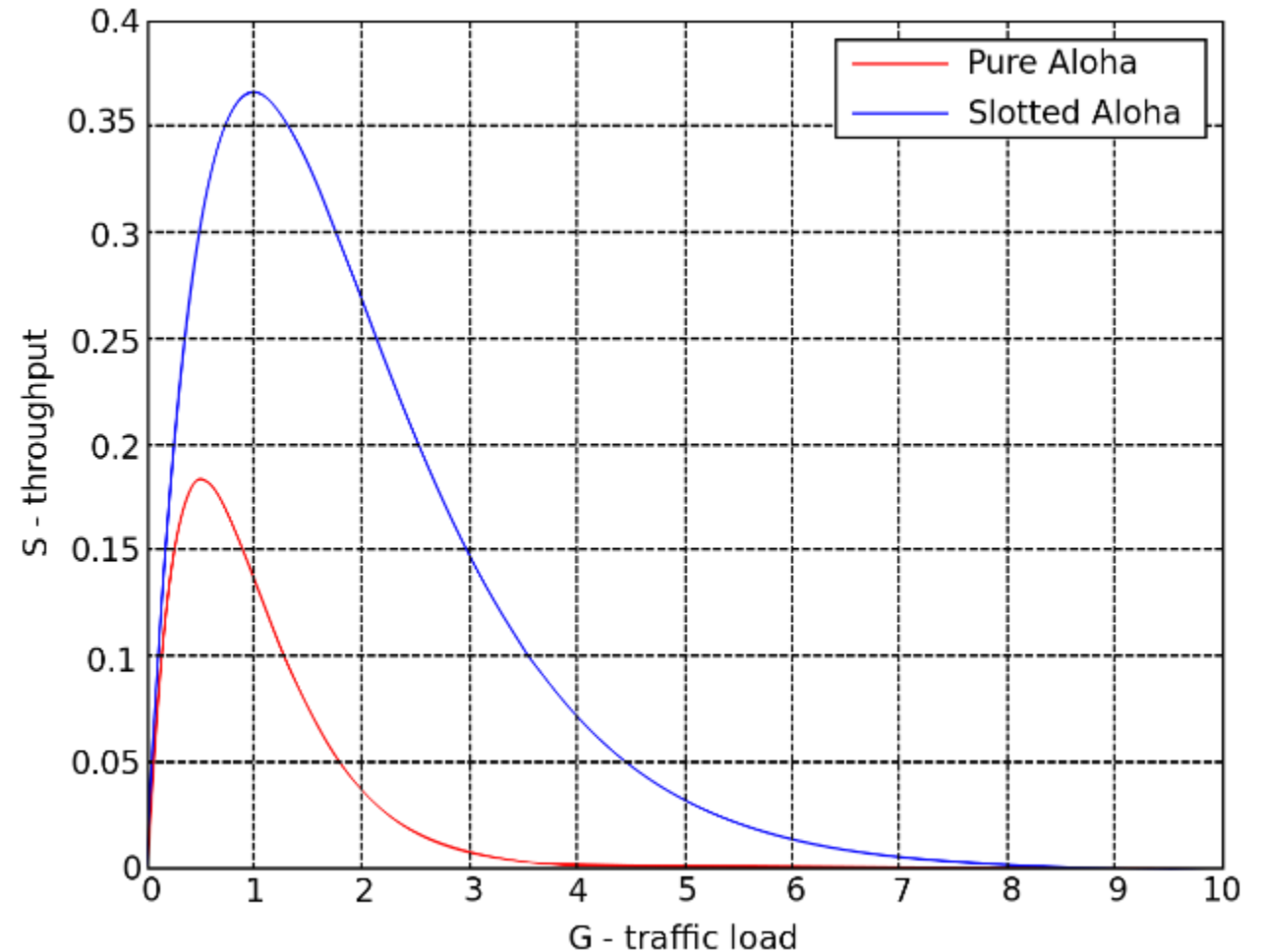
# Slotted ALOHA

- Split time into synchronized “slots”
- Any device can transmit whenever it has data
  - But it must transmit at the start of a slot
  - And its transmission cannot be longer than a slot
  - Removes half of the possibilities for collisions!
    - At the cost of some synchronization method



# ALOHA throughput

- It can be shown that traffic maxes out at
  - ALOHA: 18.4%
  - Slotted ALOHA: 36.8%
- Assuming Poisson distribution of transmission attempts
- Slotted throughput is double because the “before” collisions can no longer occur

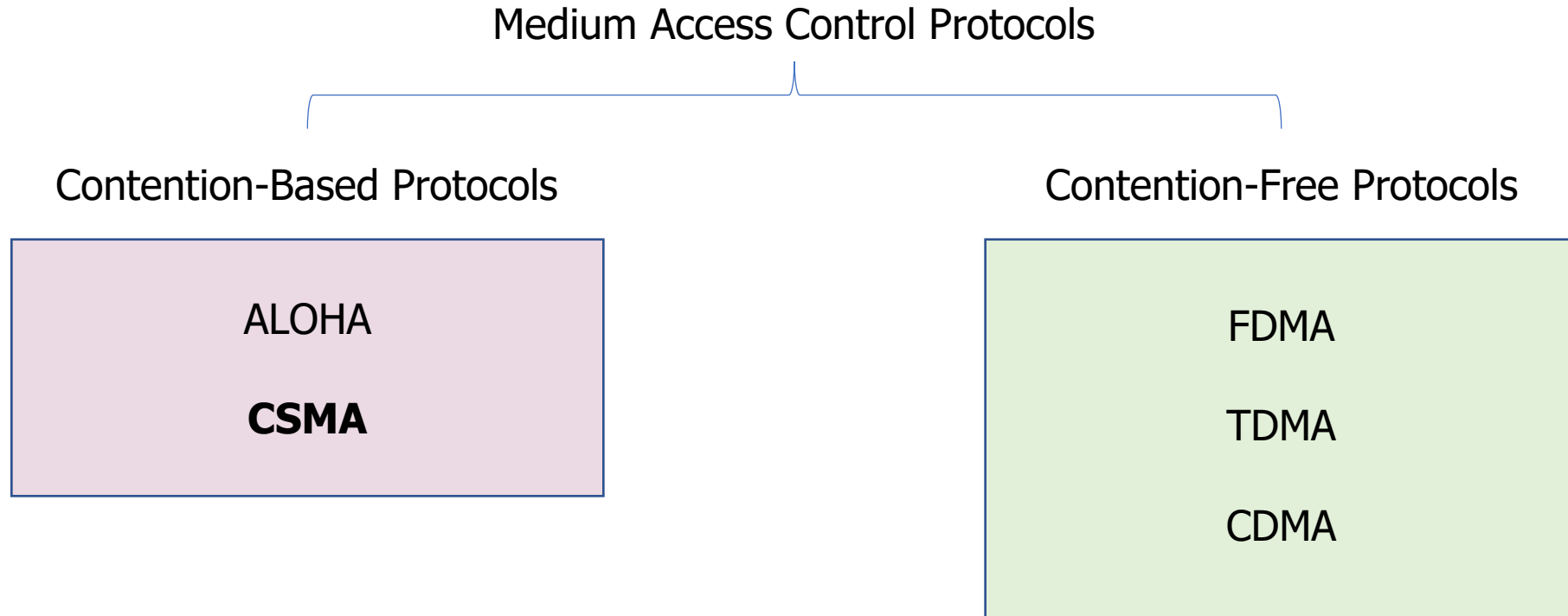




# Capture effect

- Actually, two packets at once isn't *always* a total loss
  - The louder packet can still sometimes be heard if loud enough
- How much louder?
  - Ballpark 12-14 dB
- When does this work?
  - Depends on the radio hardware
  - Louder packet first almost always works
  - Louder packet second *sometimes* works

# MAC protocol categorization



# CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

- First listen for a duration and determine if anyone is transmitting
  - If idle, you can transmit
  - If busy, wait and try again later
- “listen before send”
- Can be combined with notion of slotting
  - If current slot is idle, transmit in next slot
  - If current slot is busy, follow some algorithm to try again later

# CSMA/CD – CSMA with Collision Detection

- Detect collisions during your own transmission
  - Works great on wired mediums (Ethernet, I2C)
- Very challenging for wireless systems
  - Transmit and receive are usually the same antenna
  - Receiving while transmitting would be drowned out by transmission
    - Remember: TX at 8 dBm and RX at -95 dBm
- Area of active research!

2017 18th Annual Conference on Wireless On-demand Network Systems and Services (WONS)

## On the Feasibility of Collision Detection in Full-Duplex 802.11 Radio

Michele Segata, Renato Lo Cigno

Dept. of Information Engineering and Computer Science, University of Trento, Italy  
{msegata, lo.cigno}@disi.unitn.it

**Abstract**—Full-duplex radios are becoming a feasible reality thanks to recent advances in self-interference cancellation. Switching from half- to full-duplex requires a major re-design of many network features and characteristics, including the MAC layer. The literature provides several new proposals or improvements that are applicable in different topologies; the notion of channel itself becomes blurred, as there is no intrinsic spatial reuse and stations very far from one another hidden with respect to stations in between. Still, the possibility of detecting collisions and avoid the waste of channel is appealing and has only partially been investigated [5].

2014 IEEE 22nd International Conference on Network Protocols

## Concise Paper: Semi-Synchronous Channel Access for Full-Duplex Wireless Networks

Xiaofeng Xie and Xinyu Zhang

University of Wisconsin-Madison

Email: {xiufeng,xyzhang}@ece.wisc.edu

## Throughput Analysis of CSMA With Imperfect Collision Detection in Full Duplex-Enabled WLAN

Megumi Kaneko

**Abstract**—As an alternative to carrier sense multiple access (CSMA) with collision avoidance in half-duplex wireless local area network (WLAN) that incurs heavy control overhead, full-duplex WLANs enabling wireless collision detection (WCD) by simultaneous carrier sensing and data transmission are gaining attention.

Although CSMA with perfect collision avoidance, actual performance in a wireless environment, user patterns. Hence, we derive a throughput analysis for imperfect WCD, that can be expected from conventional random access

multiple access, wireless collision detection, full duplex.

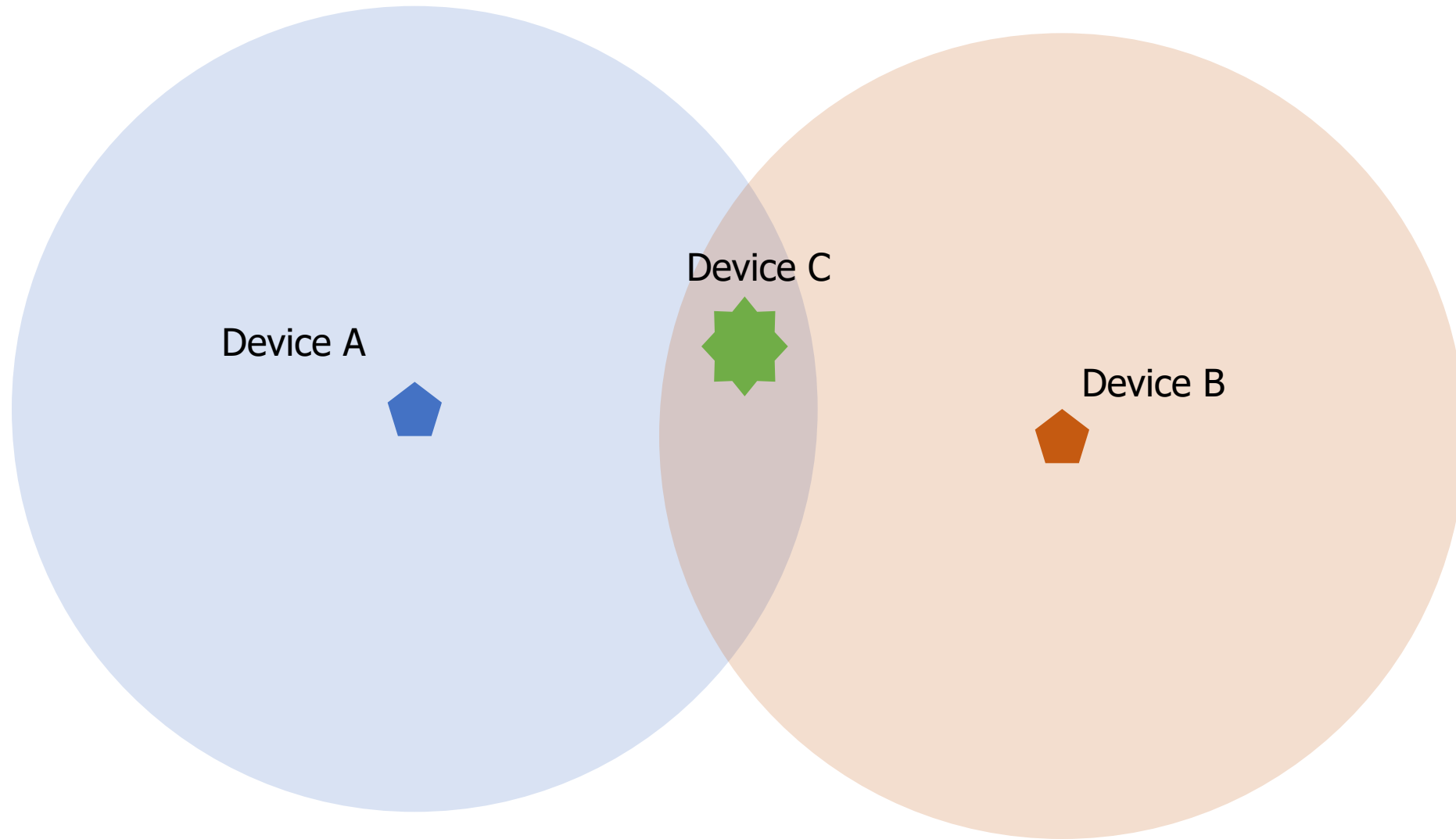
**INDEX**

work (WLAN) systems are problems due to the error.

main reasons. Firstly, a collision detected at the transmitter does not necessarily imply a collision at the receiver due to the nature of wireless channels such as large/small-scale fading. Secondly, detecting simultaneous transmissions during one's own transmission is very challenging, as the transmitter's self-interference signal power is several orders of magnitudes higher than that of collision signals to be detected.

Thus, a number of PHY layer WCD schemes have been proposed [7], [8]. A MIMO-based scheme is designed in [7] for detecting an interfering preamble signal at one of the transmit antennas, and a self-interference canceller is designed in [8] which enables the transmitter to detect simultaneous transmissions even under very high self-interference. Such schemes allow the UTs to detect potential collisions during transmission, and hence to immediately revert to the transmission process without any delay, leading to large throughput improvements compared to CSMA/CA [5]. Note that [3] assumed an ideal WCD where any collision can be perfectly detected at the transmitter. In [9], the impact of interference on full-duplex transmitter-receiver pairs in ad-hoc

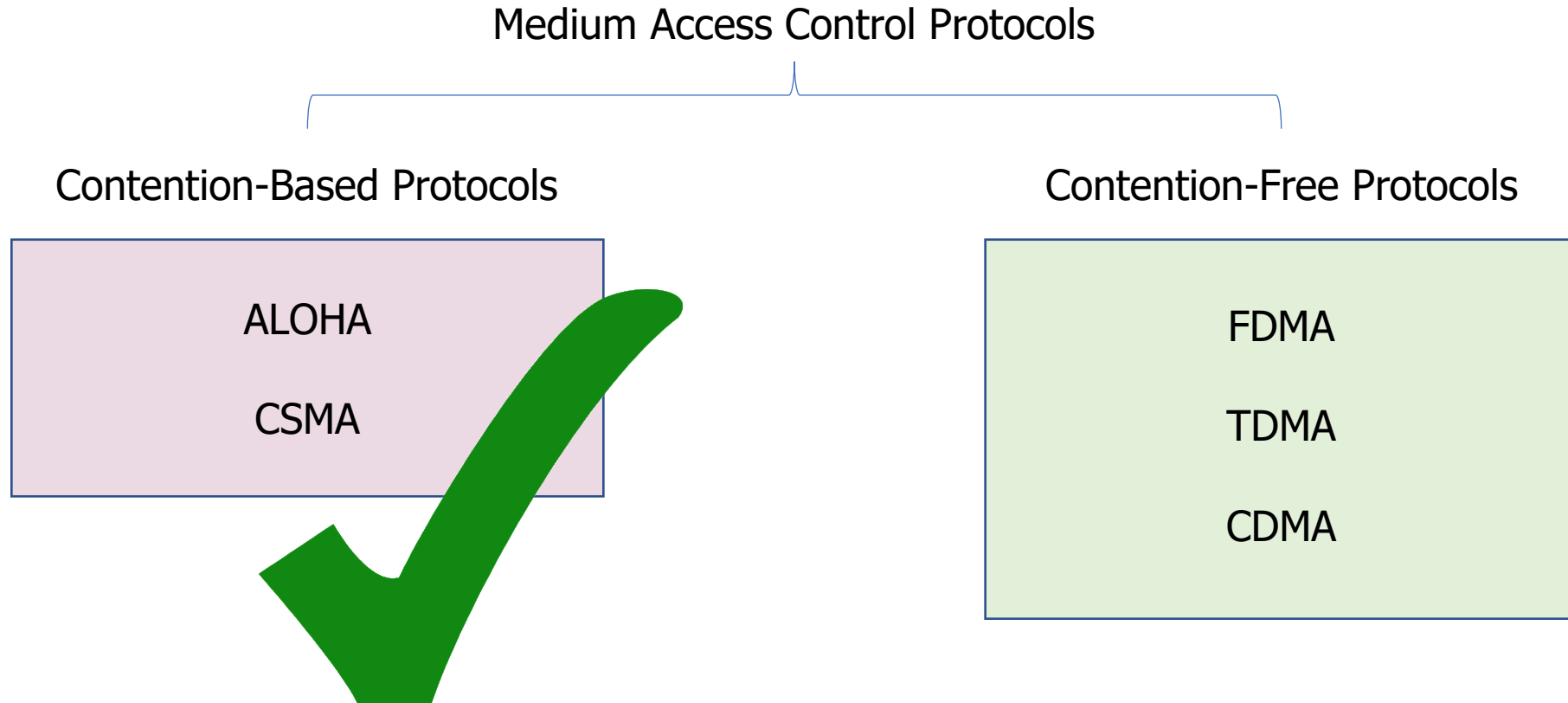
# Hidden terminal problem



# CSMA with RTS/CTS

- Hidden terminal problem means that two transmitters might never be able to detect each other's transmissions
- A partial solution
  - When channel is idle, transmitter sends a short Request To Send (RTS)
  - Receiver will send a Clear To Send (CTS) to only one node at a time
  - RTS collisions are faster and less wasteful than hidden terminal collisions
  - Downside: overhead is high for waiting for CTS when contention is low
    - Not always worth it

# MAC protocol categorization



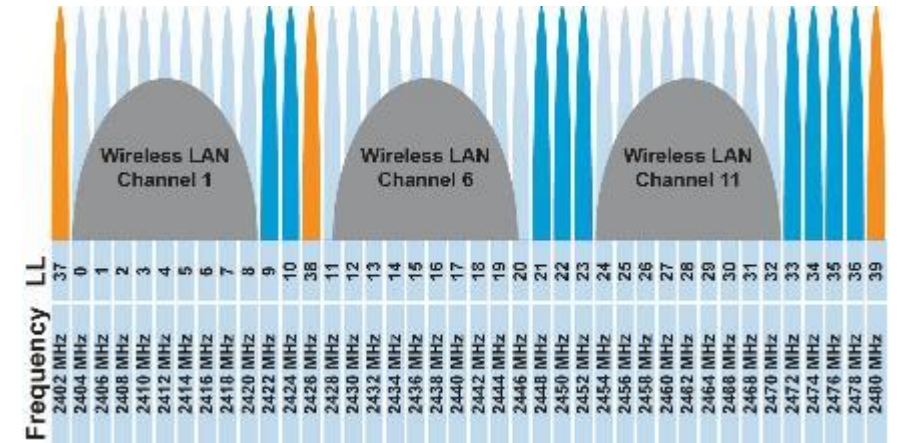
# Contention-free access control protocols

- Goal: split up communication such that devices will not conflict
- Can be predetermined or reservation-based
  - Devices might request to join the schedule and be given a slot
    - Devices lose their slot if it goes unused for some amount of time
    - Reservations often occur during a dedicated CSMA contention slot
  - Assignment of schedules can be complicated
- Really efficient at creating a high-throughput network
  - Assuming they are all following the same protocol
  - Otherwise, interference can be very problematic



# FDMA – Frequency Division Multiple Access

- Split transmissions in frequency
  - Different carrier frequencies are independent
  - Fundamentally how RF spectrum is split
  - Usually in conjunction with another scheme (but not always)
- Technically, each device uses a separate, fixed frequency
  - Walkie-talkies
- Conceptually, how RF channels work
  - WiFi networks pick different bands
  - 802.15.4 picks a channel to communicate on



# TDMA – Time Division Multiple Access

- Split transmissions in time
  - Devices share the same channel
- Splits time into fixed-length windows
  - Each device is assigned one or more windows
  - Can build a priority system here with uneven split among devices
- Requires synchronization between devices
  - Often devices must listen periodically to resynchronize
  - Less efficient use of slots reduce synchronization
    - Large guard windows. E.g. 1.5 second slot for a 1 second transmission

# CDMA – Code Division Multiple Access

- Split transmissions in 'codes'
  - Not new; original applications in radar and early satellite communications
- Analogy: Multiple speakers in the same room all in different languages
  - [The human brain is crazy good at ignoring what it doesn't understand 😊]
- Requires signal power coordination
  - [everyone needs to speak ~the same volume]
  - Can be hard in uncontrolled / dynamic environments
- Also can be more performant with highly synchronized clocks
  - i.e. if the code clock is known to both devices

## Break + Question

- What is an advantage of Aloha over TDMA?

# Break + Question

- What is an advantage of Aloha over TDMA?
  - Simplicity! It's really easy to implement Aloha
  - No required centralization
    - TDMA time schedule needs to be decided by something
    - That thing is "in charge"
    - Aloha can be entirely distributed

# Real-world protocol access control

- ALOHA
  - BLE advertisements
  - Unlicensed LPWANs: Sigfox, LoRaWAN
- CSMA
  - WiFi (slotted, CSMA/CA)
- TDMA
  - BLE connections
  - Cellular LPWANs: LTE-M and NB-IoT

# Outline

- Physical Layer
  - Overview
  - Signal Strength
  - Signal Frequency and Bandwidth
  - Signal Modulation
- Data Link Layer
- **BLE Background**

# Bluetooth Low Energy Resources

- Good walkthrough of BLE:
  - <https://www.silabs.com/documents/public/user-guides/ug103-14-fundamentals-ble.pdf>
- [[5.2 specification](#)] [[4.2 specification](#)] (link to PDF download)
  - Also: [[Supplement v9](#)]
- I used a mix of 5.2 and 4.2 for this
  - Will talk about BLE 5 differences as part of next lecture



# Basics of Bluetooth Low Energy (BLE)

- Direct device-to-device communication
  - Usually: Computer to Thing
  - Smartphone to device, Laptop to device, etc.
- Focus on making the “Thing” really low energy
  - Push energy-intensive requirements onto “Computer”
- Devices (Computer or Thing) are servers with accessible fields
  - Not the traditional send-explicit-packets interface you might be expecting
  - Lower layers are still exchanging packets to make it work



# A note on outdated notation

- Master/Slave paradigm
  - Master is the “Computer” and is in charge of interaction
  - Slave is the “Device” and has little control over interaction parameters
  - Really common notation in EE side of the world.
    - Not intended to be harmful, but also literally inconsiderate.
- Field is changing for the better. It’s going to take some time.
  - **Central/Peripheral**
  - Device/Peripheral
  - Controller/Peripheral
  - Master/Minion
  - Primary/Secondary

# BLE development

- Protocol development
  - Research product
  - Specification
  - Hardware support
  - Usefulness and iteration
- Bluetooth Low Energy
  - Research in early 2000s: Bluetooth Low End Extension and Wibree
  - Specification in 2009: Bluetooth version 4.0
  - Hardware support in 2011/12: iPhone 4s, nRF51 series
  - 4.1 and 4.2 (2014), 5.0 (2016, first in phones 2017, really 2019 though)

# Bluetooth has a long history — the IoT is near-exclusively BLE (Bluetooth 4.0+) as opposed to Bluetooth Classic (<4.0)

Year	Bluetooth Standard	Data Rate	Modulation	Notes
1999	V1.0	1 Mb/s	GFSK	<ul style="list-style-type: none"> <li>The Bluetooth 1.0 Specification is released by the Bluetooth SIG</li> </ul>
2003	V1.2	1 Mb/s	GFSK	<ul style="list-style-type: none"> <li>First FDA-approved Bluetooth medical system. Bluetooth product shipments grow to 1 million/week</li> </ul>
2004	V2.0 + EDR	1 Mb/s 2 Mb/s 3 Mb/s	GFSK $\pi/4$ -DQPSK 8-DPSK	<ul style="list-style-type: none"> <li>Introduction of Enhanced Data Rate (EDR) for faster data transfer.</li> <li>Bluetooth product shipments surpasses to 3 million/week</li> </ul>
2007	V2.1 + EDR	1 Mb/s 2 Mb/s 3 Mb/s	GFSK $\pi/4$ -DQPSK 8-DPSK	<ul style="list-style-type: none"> <li>Introduction of secure simple pairing (SSP) and extended inquiry response (EIR) for Bluetooth devices</li> </ul>
2009	V3.0+HS	1 Mb/s 2 Mb/s 3 Mb/s	GFSK $\pi/4$ -DQPSK 8-DPSK	<ul style="list-style-type: none"> <li>Introduction of AMP (Alternative MAC/PHY) and the addition of 802.11 as a high-speed transport with data transfer speeds up to 24 Mbit/s.</li> </ul>

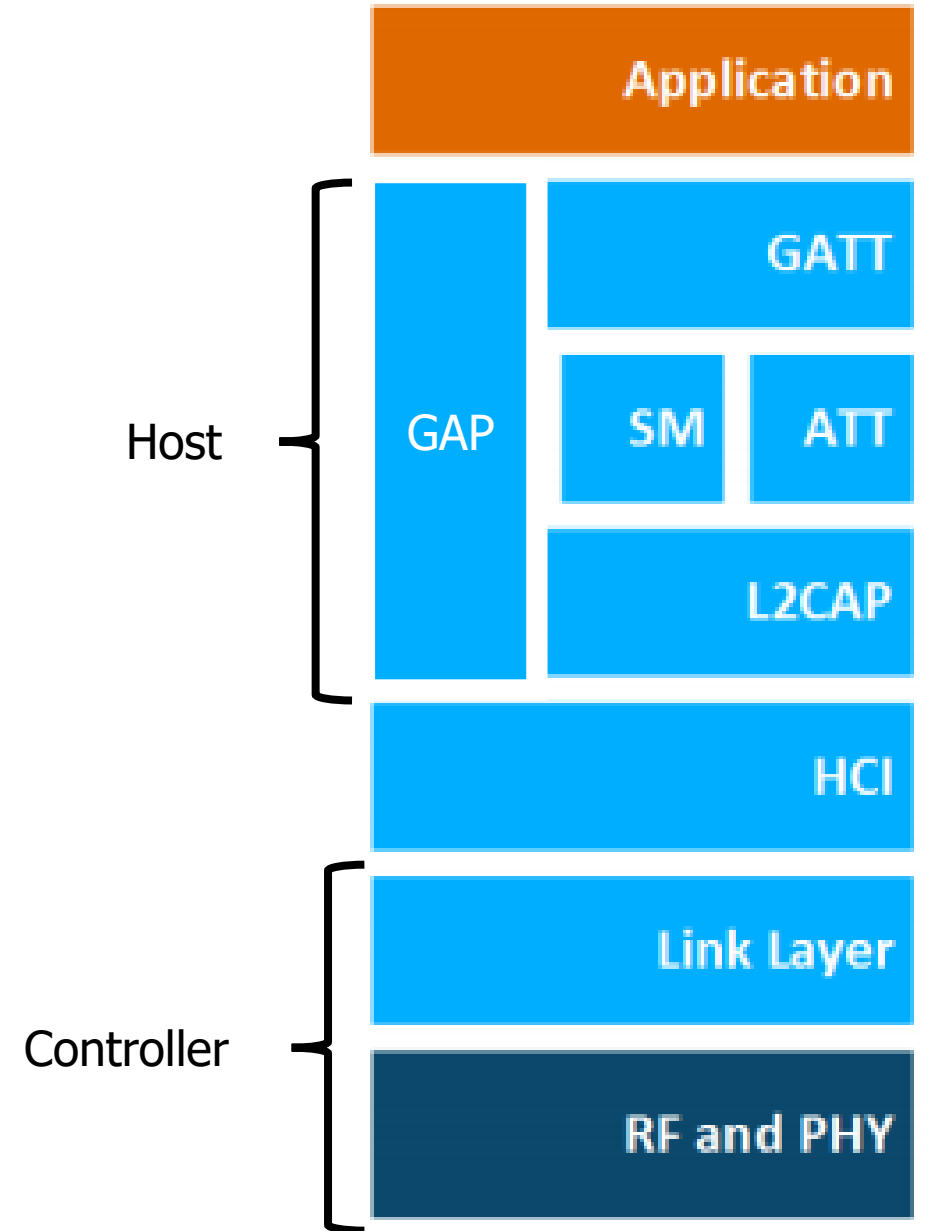
2009	V3.0+HS	1 Mb/s 2 Mb/s 3 Mb/s	GFSK $\pi/4$ -DQPSK 8-DPSK	<ul style="list-style-type: none"> <li>Introduction of AMP (Alternative MAC/PHY) and the addition of 802.11 as a high-speed transport with data transfer speeds up to 24 Mbit/s.</li> </ul>
2010	V4.0 (Smart)	1 Mb/s 2 Mb/s 3 Mb/s	GFSK $\pi/4$ -DQPSK 8-DPSK	<ul style="list-style-type: none"> <li>Introduction of Bluetooth Low Energy protocol and AES encryption</li> </ul>
2013	V4.1	1 Mb/s 2 Mb/s 3 Mb/s	GFSK $\pi/4$ -DQPSK 8-DPSK	<ul style="list-style-type: none"> <li>MWS (Mobile Wireless Standard) Coexistence</li> <li>SIG membership surpasses 20,000 companies</li> </ul>
2014	V4.2	1Mb/s 2Mb/s 3Mb/s	GFSK $\pi/4$ -DQPSK 8-DPSK	<ul style="list-style-type: none"> <li>Smart sensor allows flexible internet connectivity</li> <li>Increased privacy (Le Privacy 1.2 and LE Secure Connections)</li> <li>LE Data Length Extension increases data throughput with packet capacity increase of 10x compared to previous versions.</li> </ul>

# Bluetooth Specification

- Problem: a bit overwhelming...
  - 5.2 spec: **3256 pages**
  - We only care about Vol 6: Low Energy Controller
    - Part A: Physical Layer Specification
    - Part B: Link Layer Specification
    - CSS: Part A: Data Types Specification
    - So ~250 pages
- Tip: be willing to just ignore things when skimming specs
  - 5.2 spec covers BLE and Bluetooth Classic and a bunch of upper layer stuff that we never have to care about

# BLE Layers

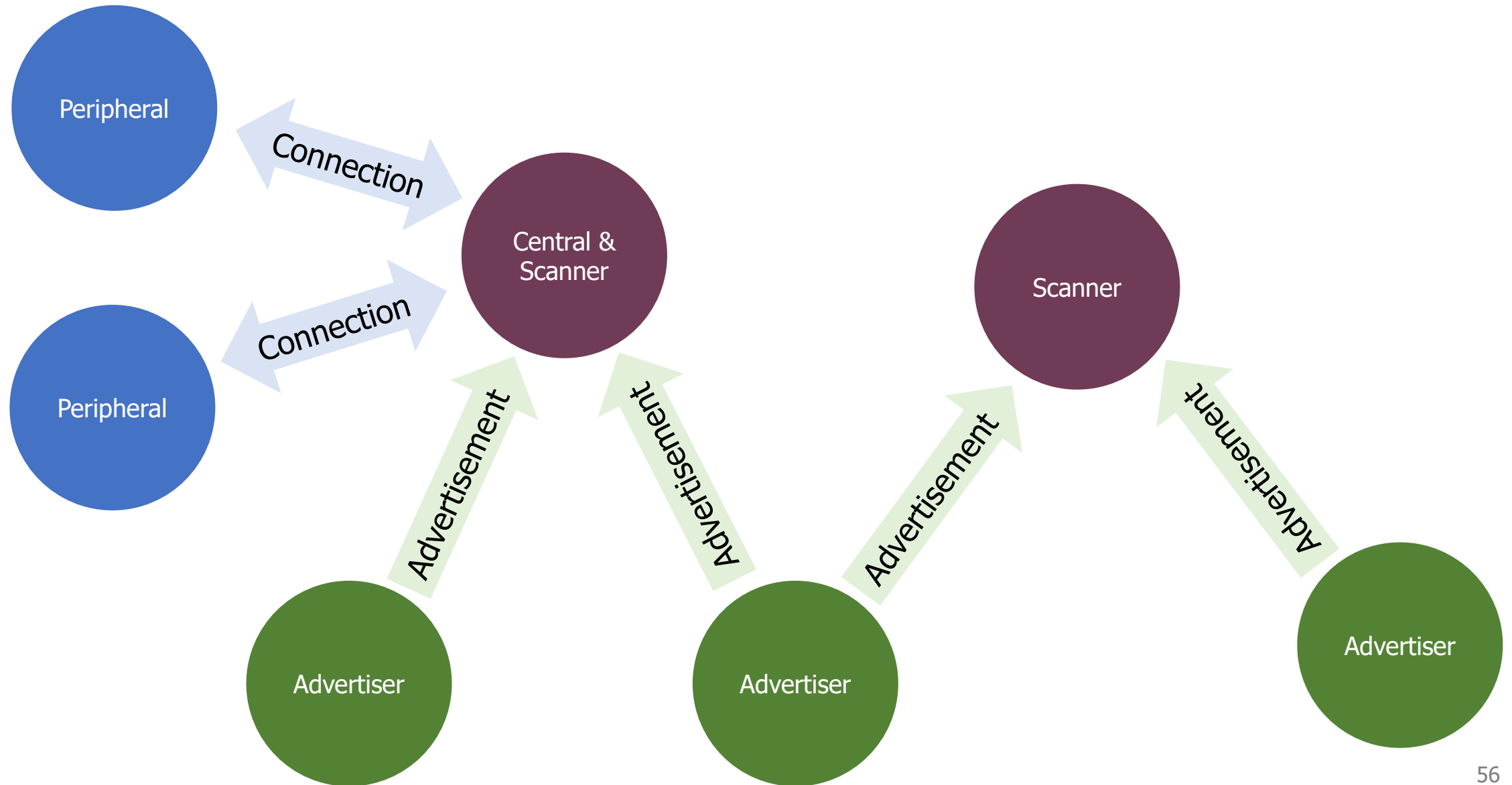
- Host – Configuration and Server
  - GAP – Generic Access Profile
    - Configure advertising
  - GATT – Generic ATtribute profile
    - Configure connections
- HCI - Host Controller Interface (sigh)
- Controller - Communication
  - Link Layer – send packets
  - RF and PHY – send bits



# BLE mechanisms

- Advertising
  - Discovery
  - Advertisements – broadcast messages indicating device details
  - Ephemeral, uni-directional communication from Advertiser to Scanner(s)
  - ALOHA access control
- Connections
  - Interaction
  - Bi-directional communication between Peripheral and Central
  - Maintained for some duration
  - TDMA access control

# BLE network topology





# Multiple roles at the same time

- Topology picture is a simplification of roles
- A single device can have multiple roles simultaneously
  - Scanning and Advertising simultaneously
  - Peripheral and Scanner and Advertiser simultaneously
  - Peripheral and Scanner and Central and Advertiser simultaneously
    - Getting a bit out of hand though
- One Peripheral can even be connected to multiple Centrals
  - Not in the original design though: you'll find old docs saying you can't
  - And it's not a normal use-case for BLE

# Break + Check your understanding

- Which roles is each device likely to have?
  - Keyboard
  - Laptop
  - Smartphone

# Break + Check your understanding

- Which roles is each device likely to have?
  - Keyboard
    - Advertiser and Peripheral
  - Laptop
    - Scanner and Central
  - Smartphone
    - Advertiser, Peripheral, Scanner, and Central

# Outline

- Physical Layer
  - Overview
  - Signal Strength
  - Signal Frequency and Bandwidth
  - Signal Modulation
- Data Link Layer
- BLE Background