Lecture 03
Data Link Layer + BLE Introduction

CS397/497 – Wireless Protocols for IoT
Branden Ghena – Winter 2023

Materials in collaboration
with Pat Pannuto (UCSD)

Northwestern

Administrivia

- Hw: Background
  - Goal: brush up on some embedded systems and networks background
  - Due by Wednesday end-of-day
  - Submit on Gradescope

- Lab: Wireless
  - Goal: familiarize yourself with Wireshark
    - Install it, do some basic scanning, explore a little

  - Writeup:
    - Due next Friday by end-of-day
    - Submit on Gradescope

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:
  - https://forms.gle/wDvSngsSvJ2hWL56A

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?

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

Outline

- **Data Link Layer**

- BLE Background

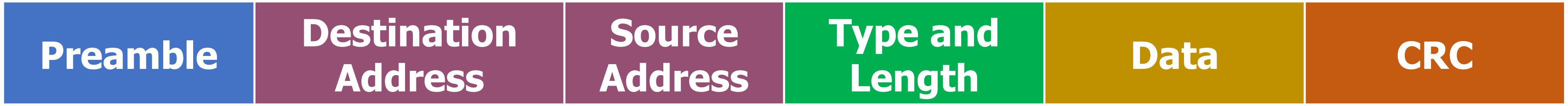
- BLE Layers
  - Physical Layer
  - Link Layer

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



Preamble	Destination Address	Source Address	Type and Length	Data	CRC

- 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: in one minute you will have to recite the alphabet
  - We’ll jump by tables, one person per letter
  - You all fail if two people speak at the same time
  - I will ban any strategy that two tables use

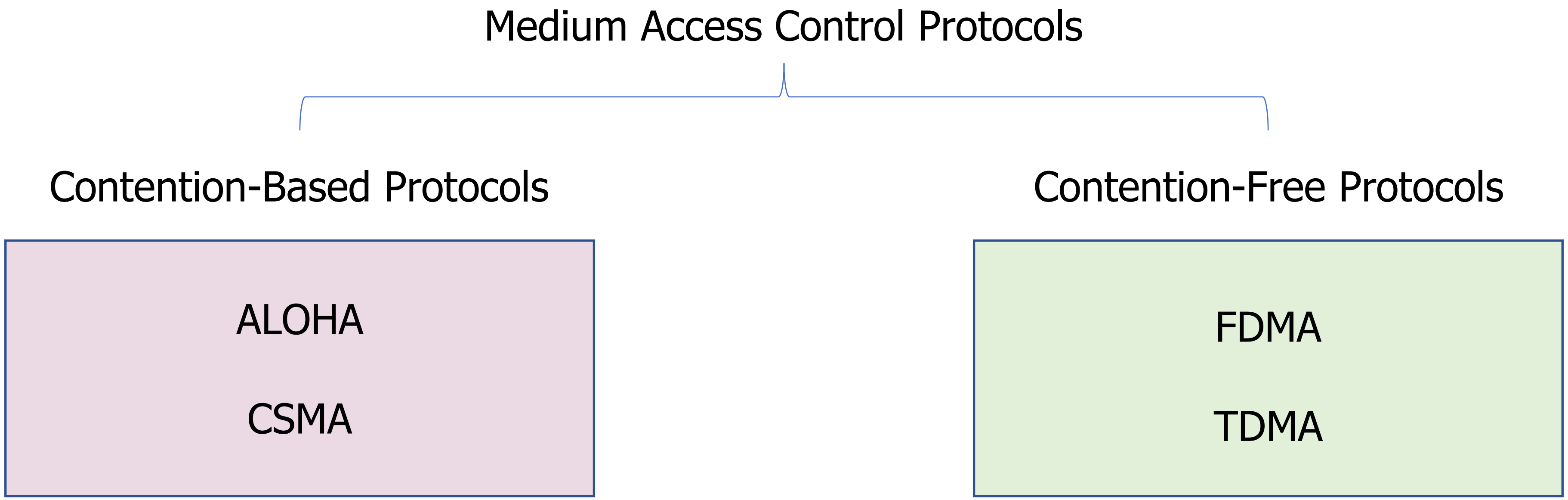
Analogy: wireless medium as acoustic

- 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

- Others?

MAC protocol categorization



Medium Access Control Protocols

Contention-Based Protocols

ALOHA

CSMA

Contention-Free Protocols

FDMA

TDMA

Also, CDMA

ALOHA

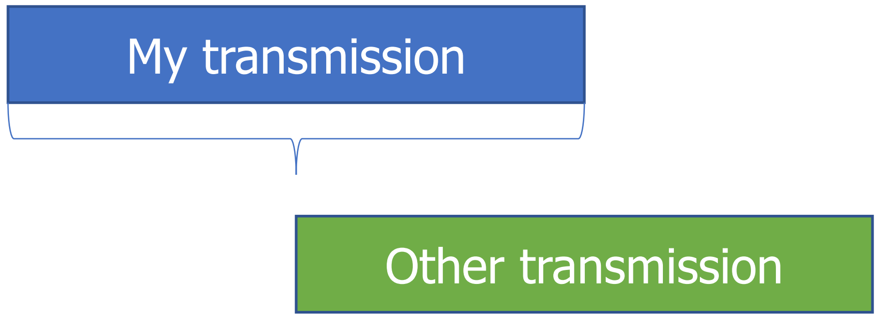
- ALOHAnet (1971)
  - University of Hawaii – Norman Abramson
  - First demonstration of wireless packet network

- Rules
  1. If you have data to send, send it

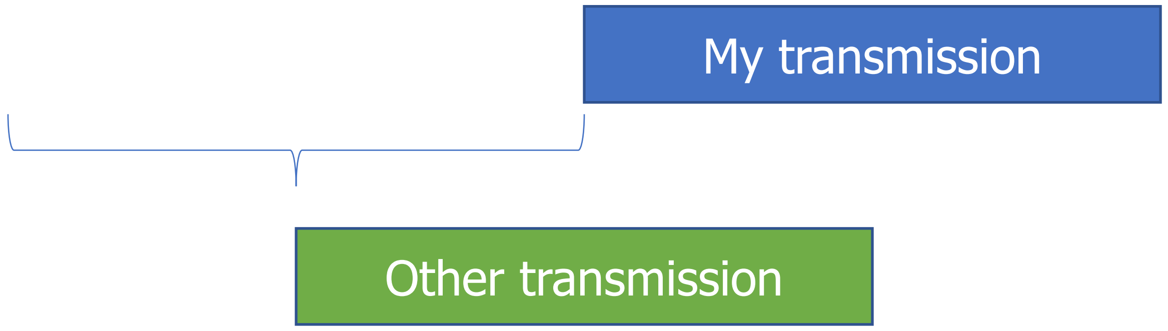
- Two (or more) simultaneous transmissions will collide and be lost
  - Wait a duration of time for an acknowledgement
  - If transmission was lost, try sending again “later”
    - Want some kind of exponential backoff scheme here

Packet collisions

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

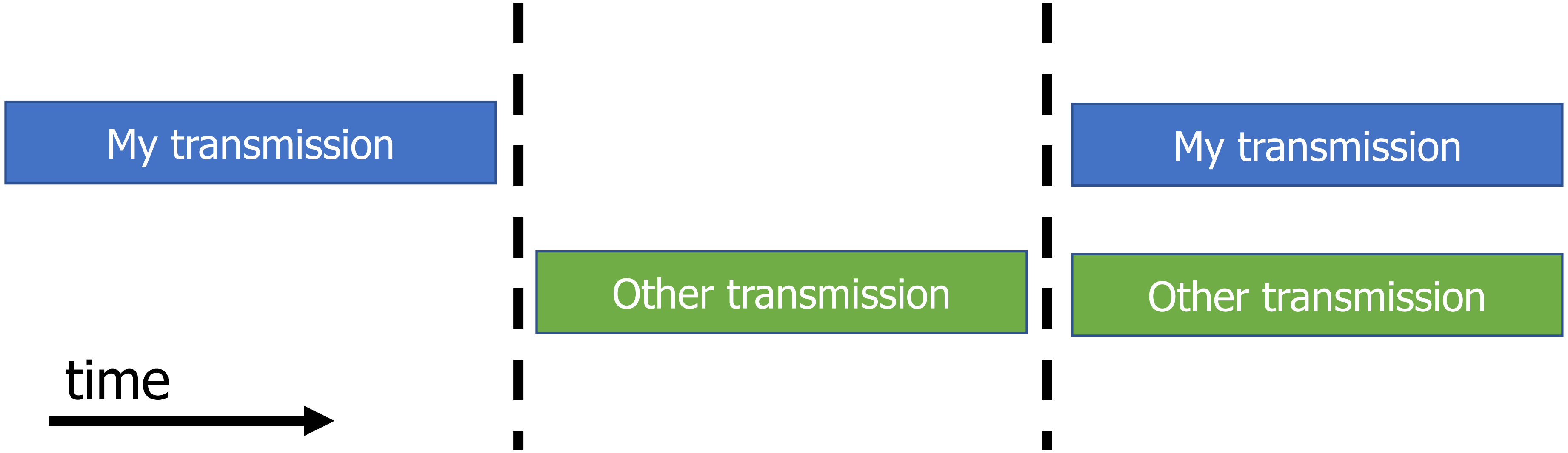


  - Transmissions before packet can also be bad



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

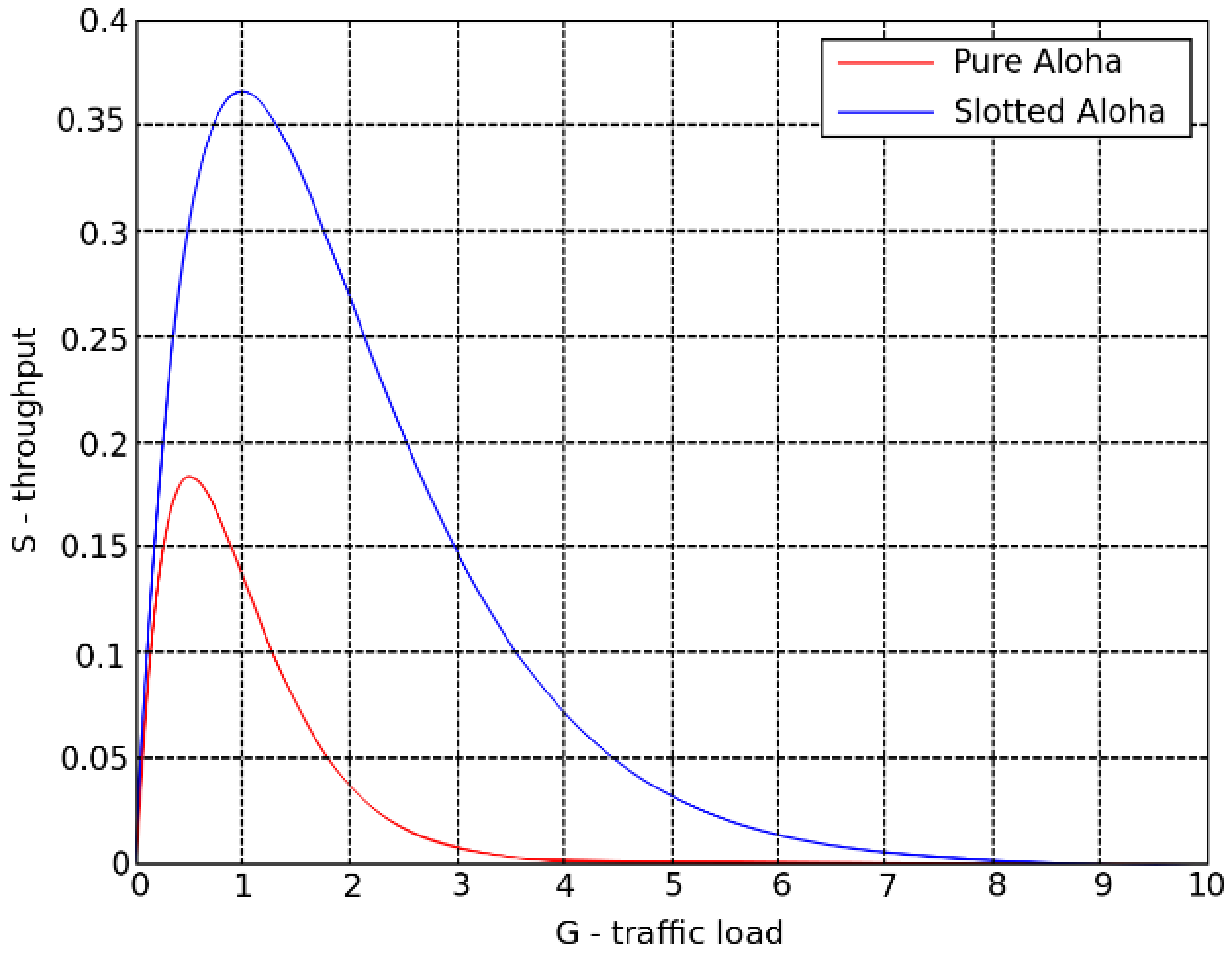


ALOHA throughput

- 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



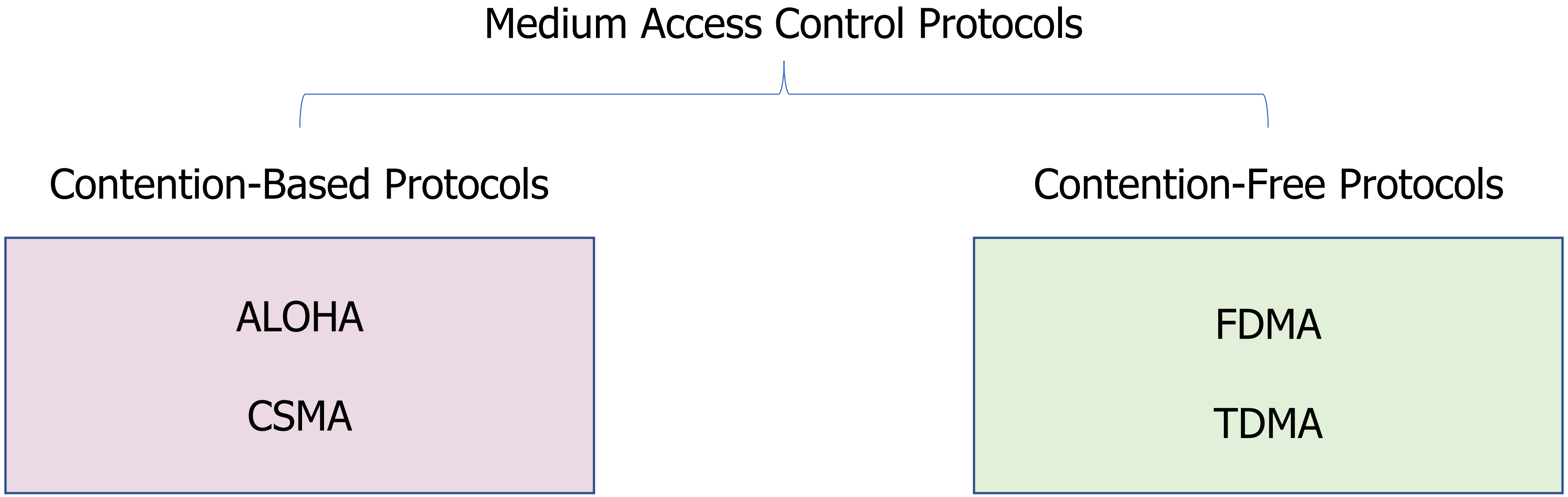
Capture effect

- 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



Medium Access Control Protocols

Contention-Based Protocols

- ALOHA
- CSMA

Contention-Free Protocols

- FDMA
- TDMA

Also, CDMA

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

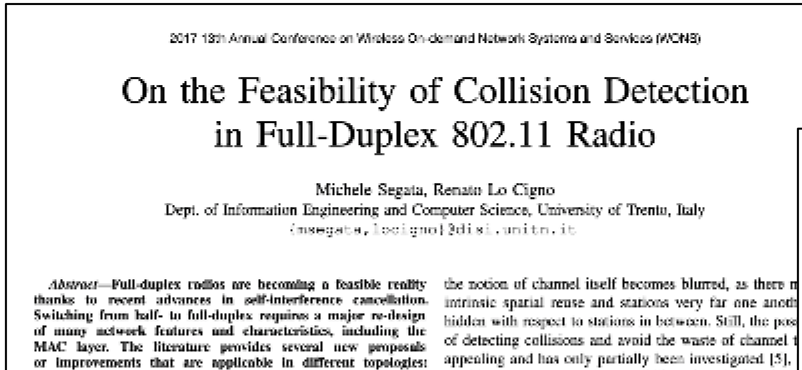
- First listen for a duration and determine if anyone is transmitting
    - If idle, you can transmit
    - If busy, wait and try again later
- “listen before send”
- Can be combined with notion of slotting
    - If current slot is idle, transmit in next slot
    - If current slot is busy, follow some 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 13th 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,locigno}@disi.unitn.it

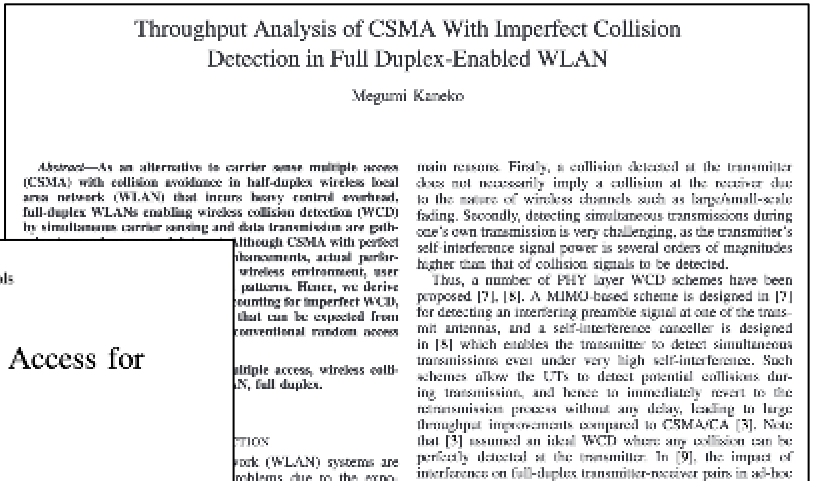
Abstract—Full-duplex radios are becoming a feasible reality thanks to recent advances in self-interference cancellation. Switching from half- to full-duplex requires a major re-design of many network features and characteristics, including the MAC layer. The literature provides several new proposals or improvements that are applicable in different topologies:

the notion of channel itself becomes blurred, as there m intrinsic spatial reuse and stations very far one anoth hidden with respect to stations in between. Still, the pos of detecting collisions and avoid the waste of channel t 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

Xiufeng 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 gath- lthough CSMA with perfect hancements, actual perfor- wireless environment, user patterns. Hence, we derive counting for imperfect WCD, that can be expected from conventional random access

ultiple access, wireless colli- AN, full duplex.

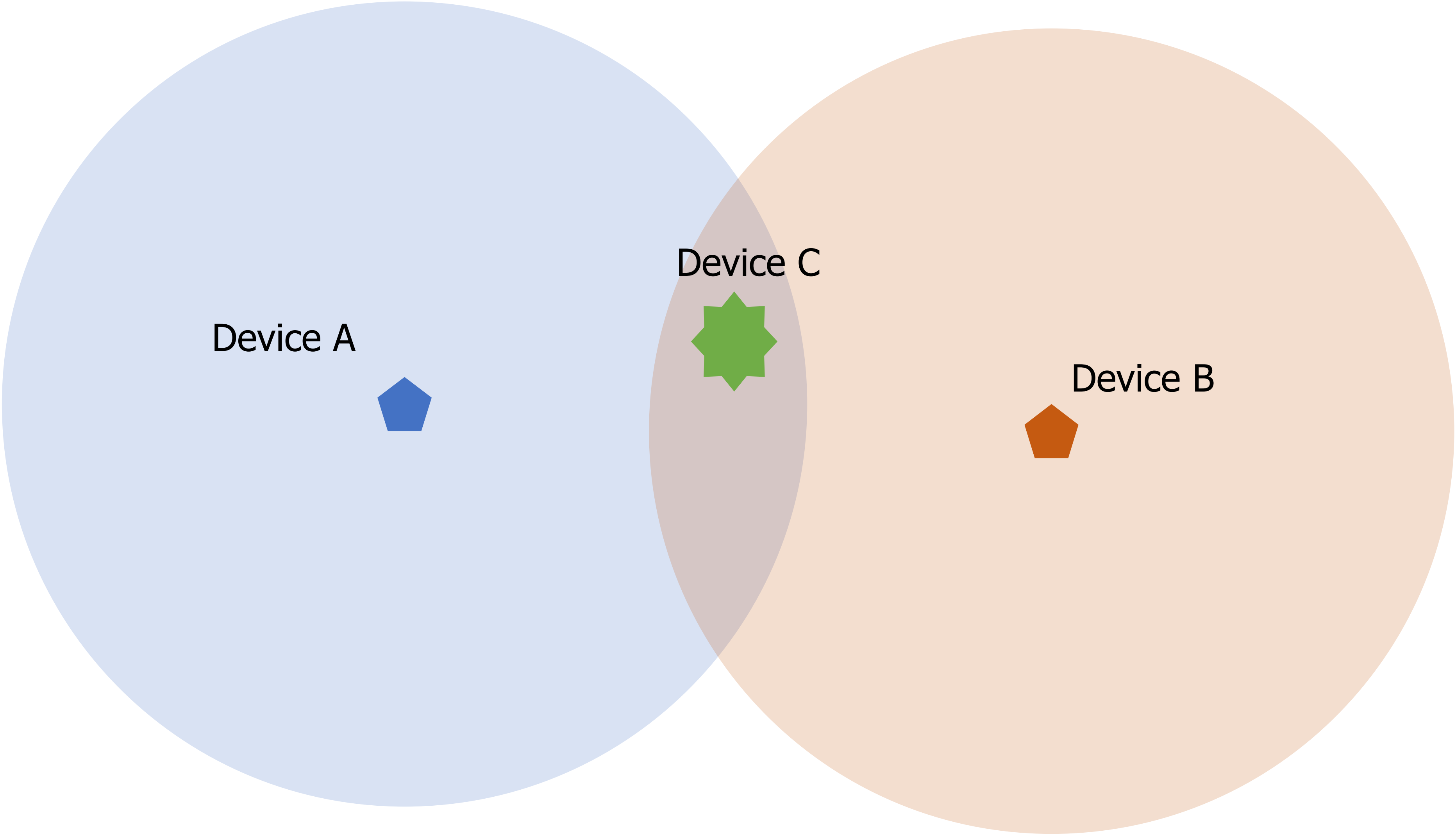
TION

work (WLAN) systems are roblems due to the asyno-

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 retransmission process without any delay, leading to large throughput improvements compared to CSMA/CA [3]. 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

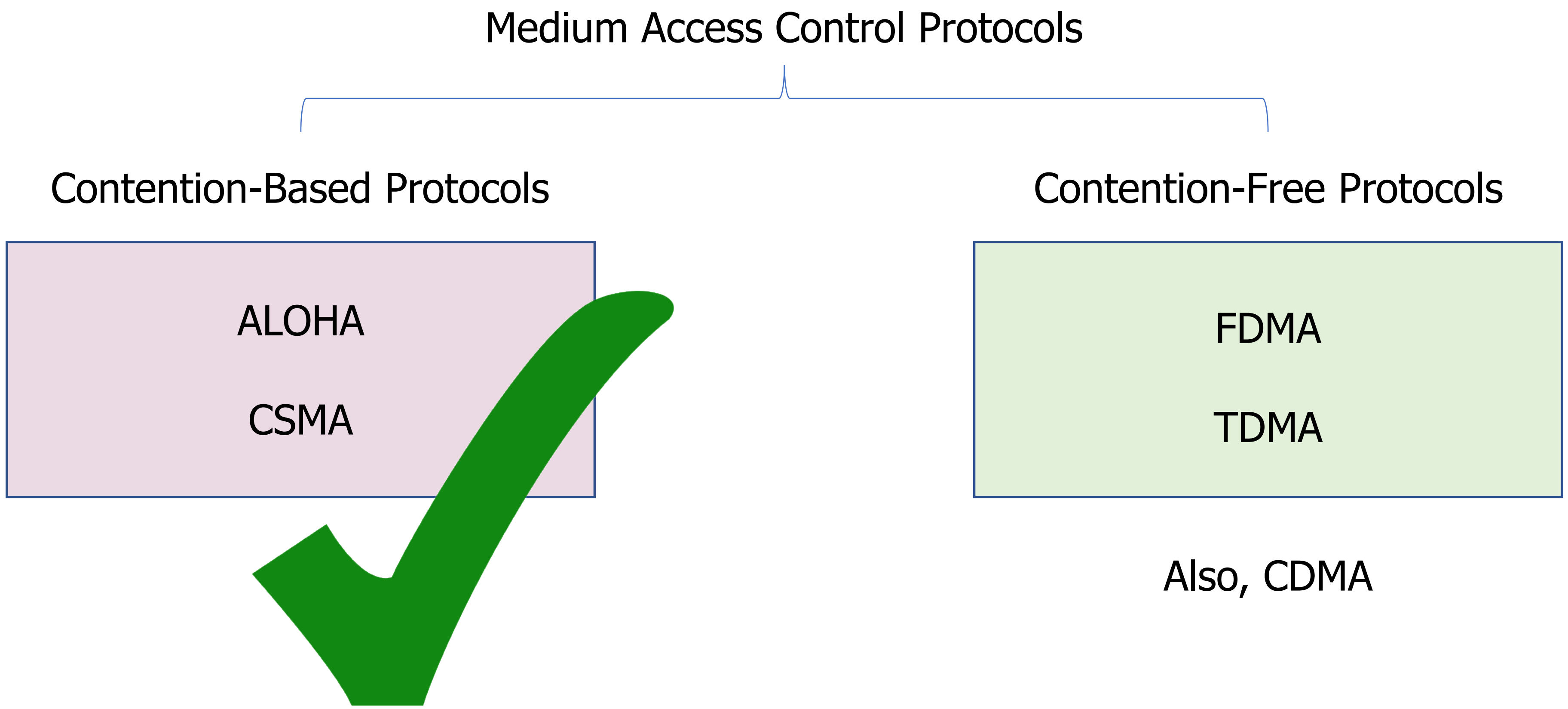


CSMA with RTS/CTS

- 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

MAC protocol categorization



Medium Access Control Protocols

Contention-Based Protocols

ALOHA

CSMA

Contention-Free Protocols

FDMA

TDMA

Also, CDMA

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

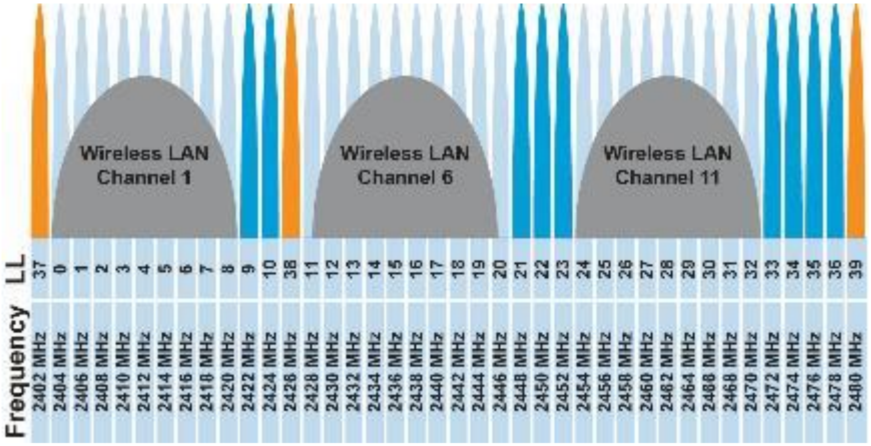
- Really efficient at creating a high-throughput network
    - Assuming they are all following the same protocol
    - Otherwise, interference can be very problematic

FDMA – Frequency Division Multiple Access

- Split transmissions in frequency
  - Different carrier frequencies are independent
  - Fundamentally how RF spectrum is split

- 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



LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

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

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

Break + Say hi to your neighbors

- Things to share
    - Name

    - Major

    - One of the following
        - Favorite Candy
        - Favorite Pokemon
        - Favorite Emoji

Break + Say hi to your neighbors

- Things to share
  - Name -Branden

  - Major -EE, CE, and CS

  - One of the following
    - Favorite Candy - Twix
    - Favorite Pokemon - Eevee
    - Favorite Emoji - 🍢

Outline

- Data Link Layer
- **BLE Background**
- BLE Layers
  - Physical Layer
  - Link Layer

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.

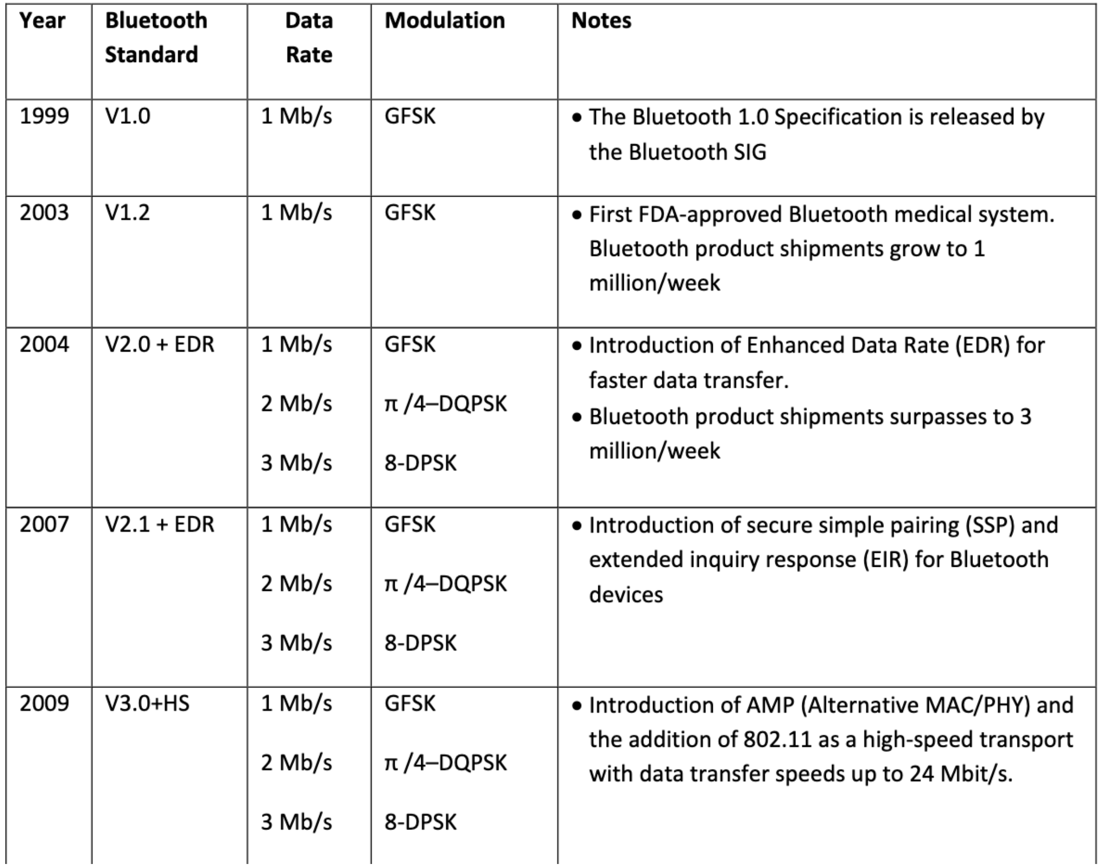
- Field is changing for the better. It’s going to take some time.
  - **Central/Peripheral**
  - Device/Peripheral
  - Controller/Peripheral
  - Master/Minion
  - Primary/Secondary

BLE development

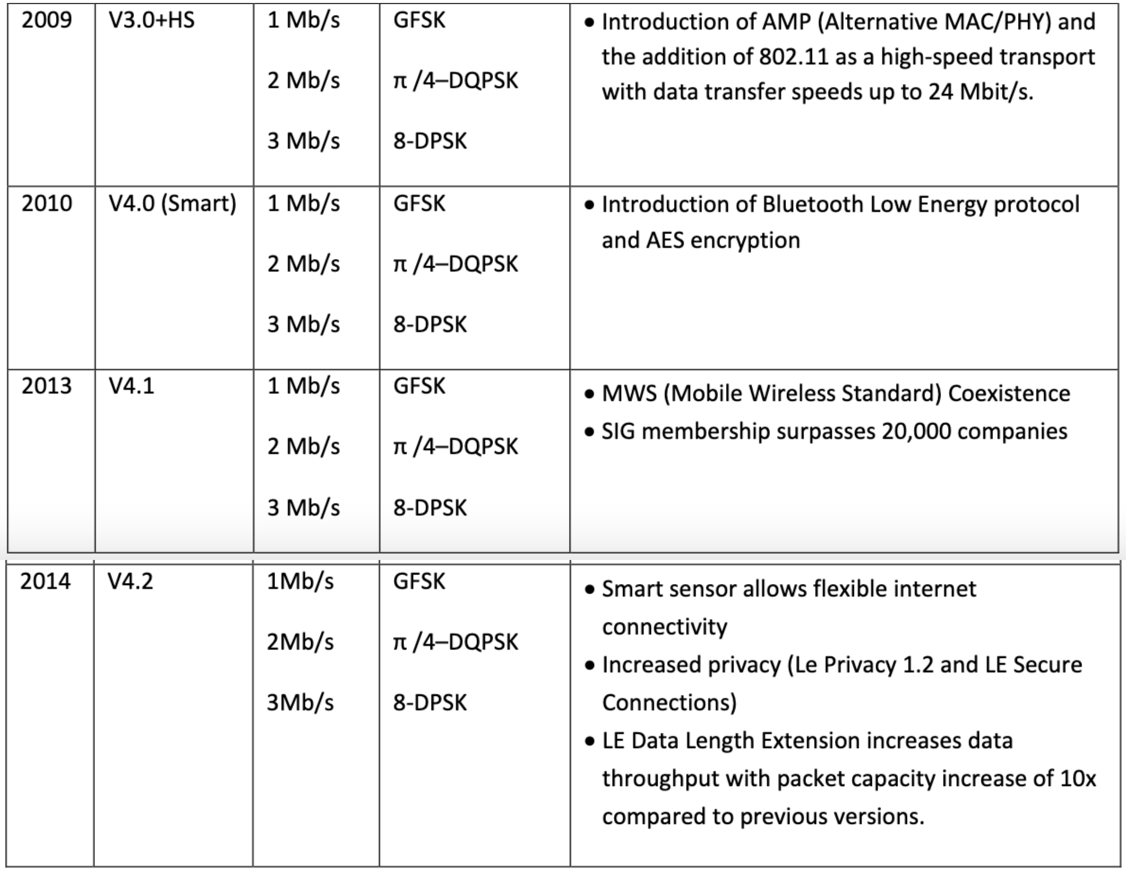
- Protocol development
  - Research product
  - Specification
  - Hardware support
  - Usefulness and iteration

- 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	• The Bluetooth 1.0 Specification is released by the Bluetooth SIG
2003	V1.2	1 Mb/s	GFSK	• First FDA-approved Bluetooth medical system. Bluetooth product shipments grow to 1 million/week
2004	V2.0 + EDR	1 Mb/s 2 Mb/s 3 Mb/s	GFSK π /4–DQPSK 8-DPSK	• Introduction of Enhanced Data Rate (EDR) for faster data transfer. • Bluetooth product shipments surpasses to 3 million/week
2007	V2.1 + EDR	1 Mb/s 2 Mb/s 3 Mb/s	GFSK π /4–DQPSK 8-DPSK	• Introduction of secure simple pairing (SSP) and extended inquiry response (EIR) for Bluetooth devices
2009	V3.0+HS	1 Mb/s 2 Mb/s 3 Mb/s	GFSK π /4–DQPSK 8-DPSK	• 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.



2009	V3.0+HS	1 Mb/s 2 Mb/s 3 Mb/s	GFSK π /4–DQPSK 8-DPSK	• 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.
2010	V4.0 (Smart)	1 Mb/s 2 Mb/s 3 Mb/s	GFSK π /4–DQPSK 8-DPSK	• Introduction of Bluetooth Low Energy protocol and AES encryption
2013	V4.1	1 Mb/s 2 Mb/s 3 Mb/s	GFSK π /4–DQPSK 8-DPSK	• MWS (Mobile Wireless Standard) Coexistence • SIG membership surpasses 20,000 companies
2014	V4.2	1Mb/s 2Mb/s 3Mb/s	GFSK π /4–DQPSK 8-DPSK	• Smart sensor allows flexible internet connectivity • Increased privacy (Le Privacy 1.2 and LE Secure Connections) • LE Data Length Extension increases data throughput with packet capacity increase of 10x compared to previous versions.

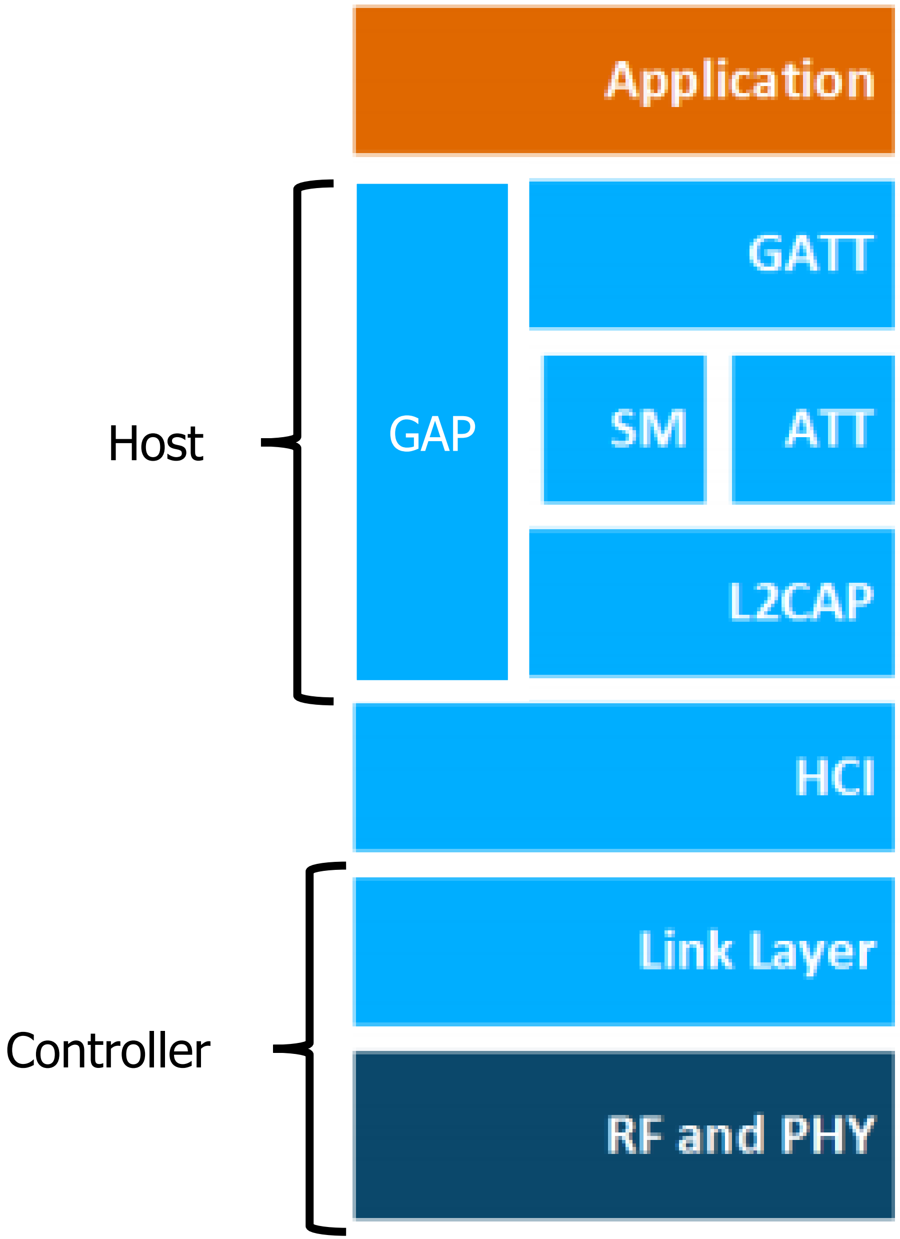
Bluetooth Specification

- 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

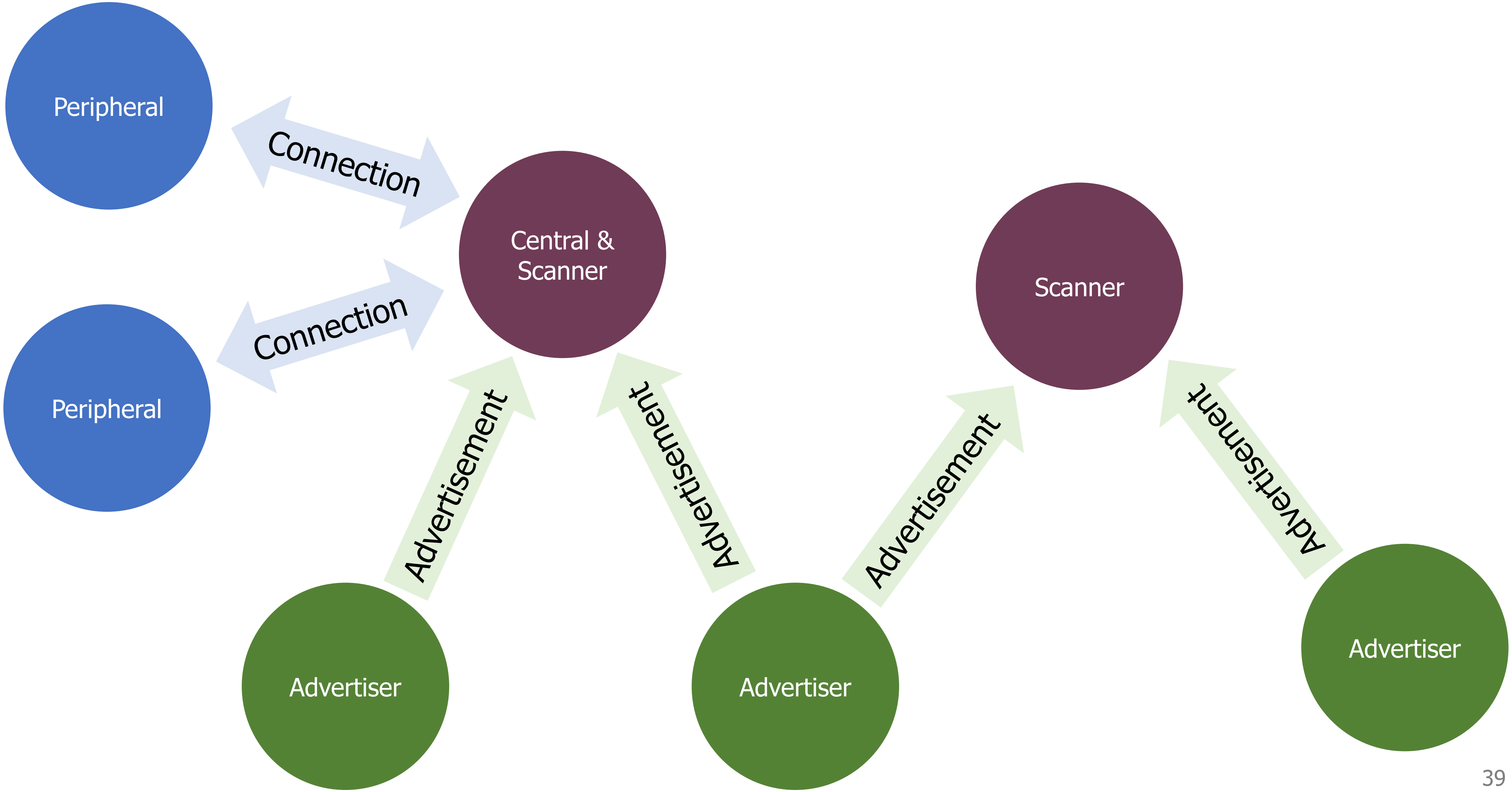


BLE mechanisms

- 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

- Also possible:
  - One Peripheral can be connected to multiple Centrals
    - This is relatively new in BLE still, you’ll find old docs saying you can’t

Break + Check your understanding

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

Break + Check your understanding

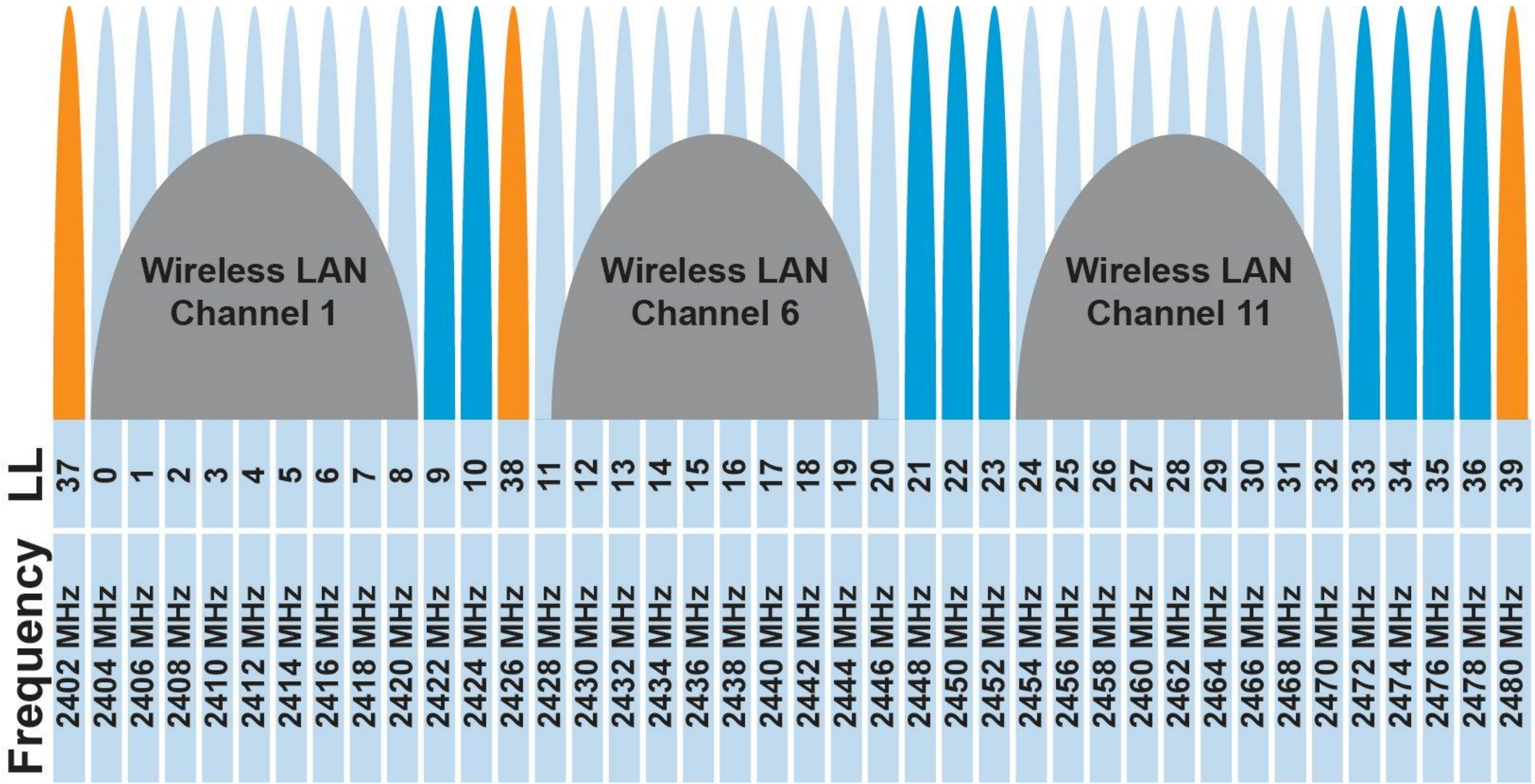
- Which roles is each device likely to have?
  - Keyboard
    - Advertiser and Peripheral
  - Laptop
    - Scanner and Central
  - Smartphone
    - Advertiser, Peripheral, Scanner, and Central

Outline

- Data Link Layer
- BLE Background
- **BLE Layers**
  - **Physical Layer**
  - Link Layer

BLE frequency

- 2.4 GHz carrier, Forty 2-MHz channels, 1 Mbps data rate
  - 37, 38, 39 for advertising
  - 0-36 for connection (FHSS)

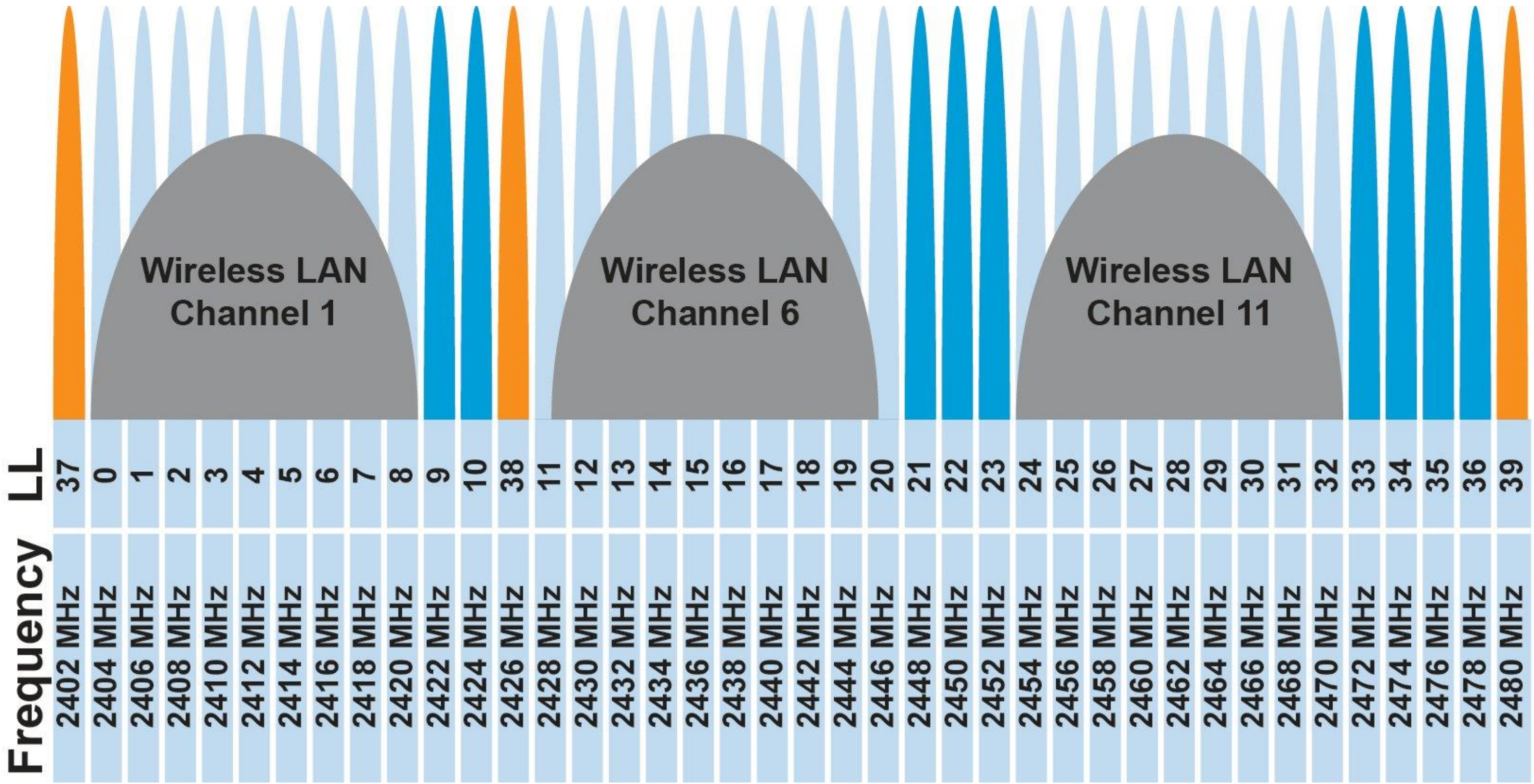


LL	37	0	1	2	3	4	5	6	7	8	9	10	38	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	39
Frequency	2402 MHz	2404 MHz	2406 MHz	2408 MHz	2410 MHz	2412 MHz	2414 MHz	2416 MHz	2418 MHz	2420 MHz	2422 MHz	2424 MHz	2426 MHz	2428 MHz	2430 MHz	2432 MHz	2434 MHz	2436 MHz	2438 MHz	2440 MHz	2442 MHz	2444 MHz	2446 MHz	2448 MHz	2450 MHz	2452 MHz	2454 MHz	2456 MHz	2458 MHz	2460 MHz	2462 MHz	2464 MHz	2466 MHz	2468 MHz	2470 MHz	2472 MHz	2474 MHz	2476 MHz	2478 MHz	2480 MHz

Why doesn't BLE avoid WiFi altogether?

BLE frequency

- 2.4 GHz carrier, Forty 2-MHz channels, 1 Mbps data rate
    - 37, 38, 39 for advertising
    - 0-36 for connection (FHSS)



LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

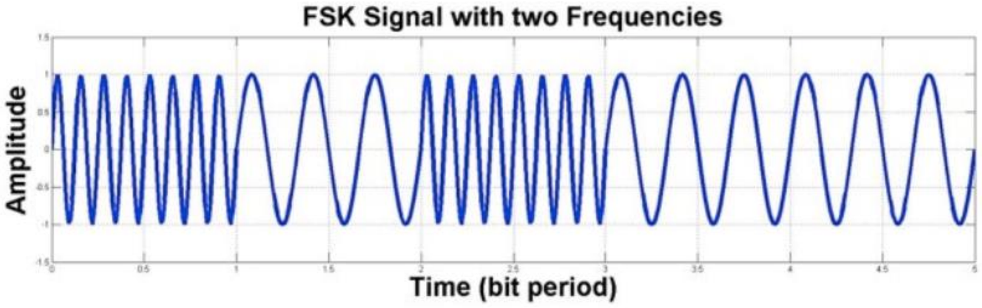
Why doesn’t BLE avoid WiFi altogether?

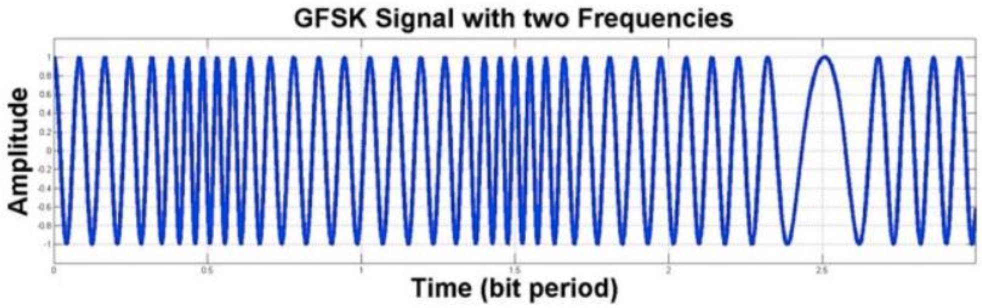
Can’t on 2.4 GHz

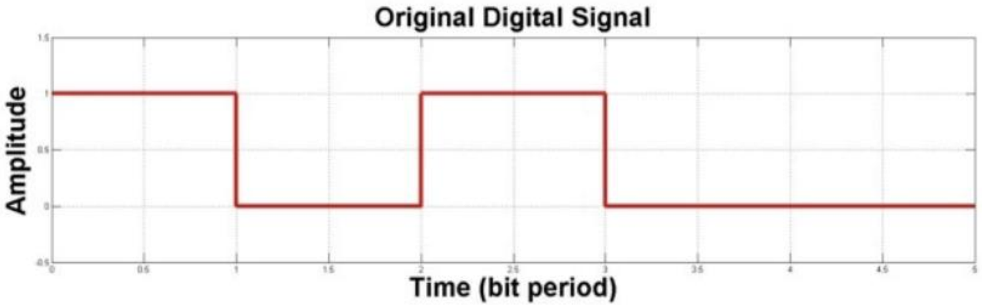
Wants 2.4 GHz for technology improvements

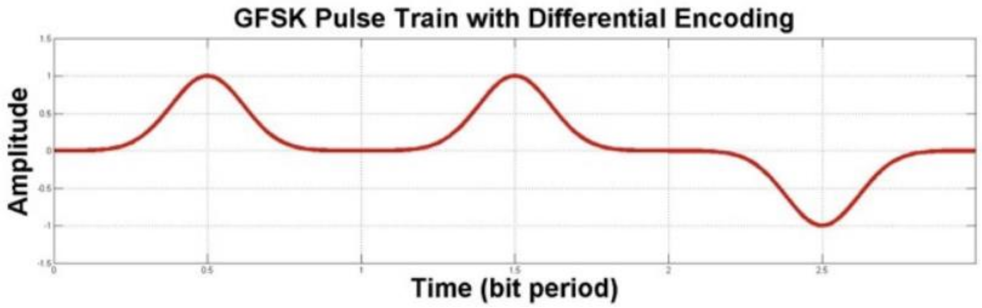
BLE modulation

- Gaussian Frequency-Shift Keying (GFSK)
  - Improvement on base Frequency-shift Keying
  - Smoother transitions between bits -> reduces nearby interference

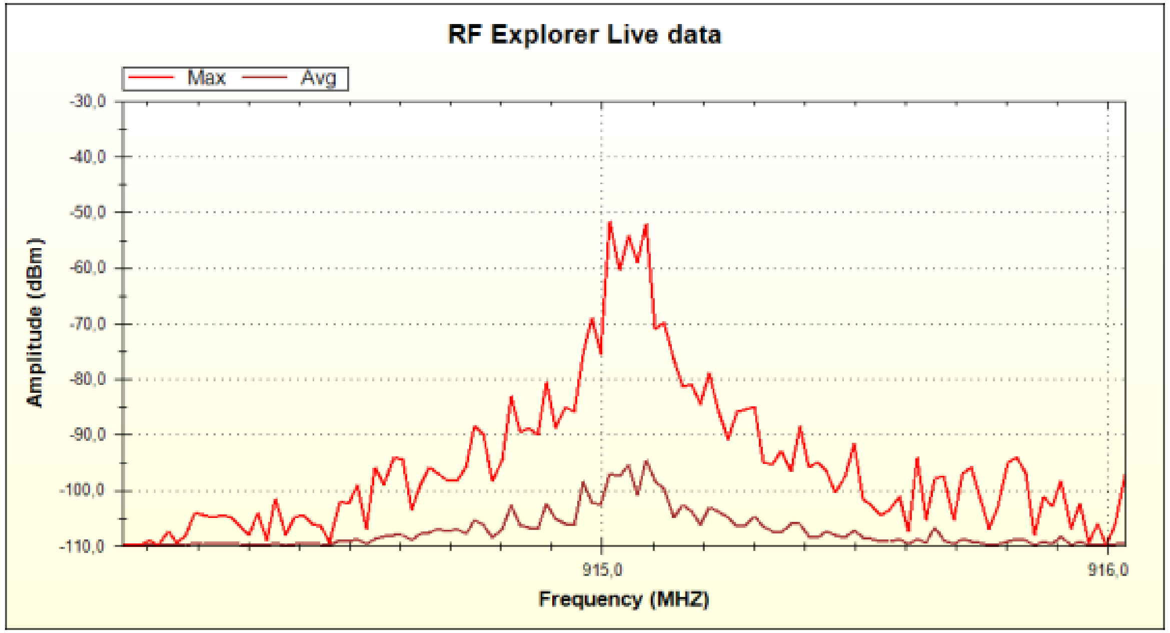

FSK Signal with two Frequencies

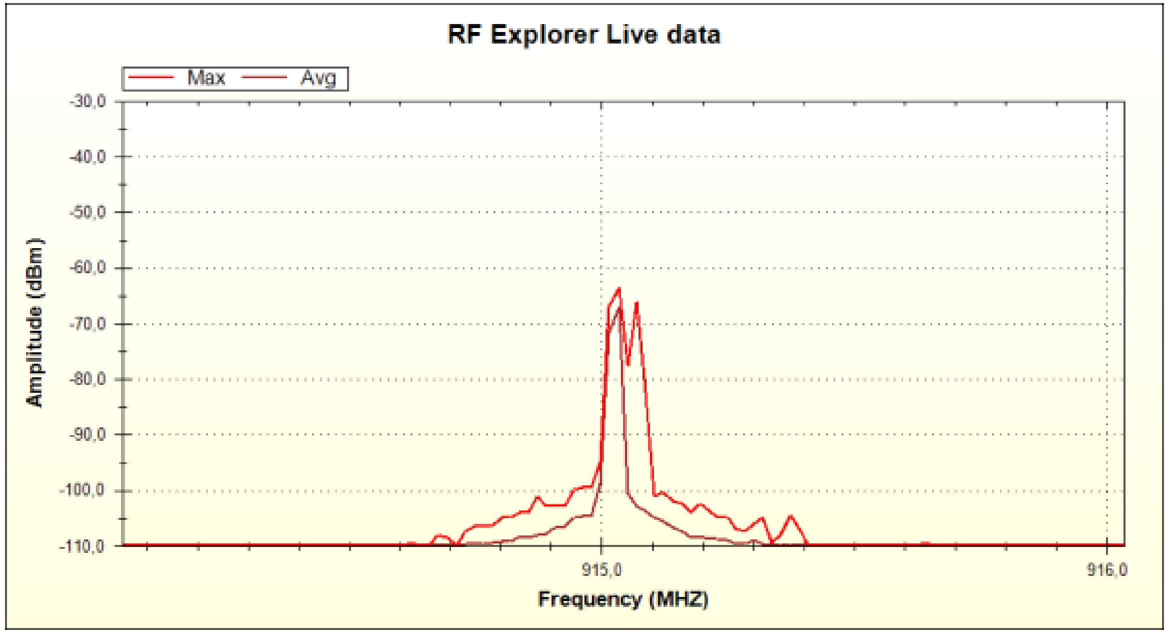

GFSK Signal with two Frequencies


Original Digital Signal

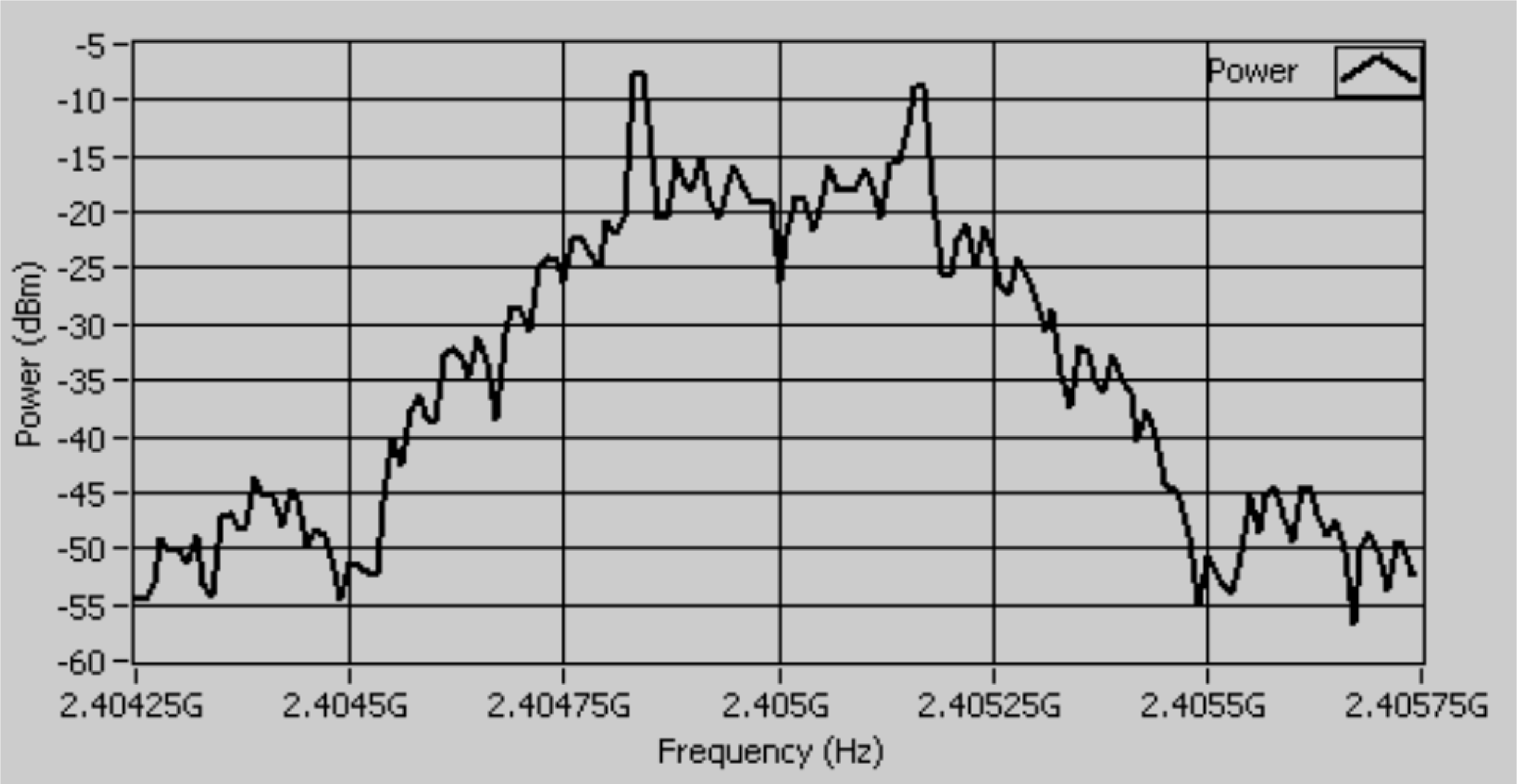

GFSK Pulse Train with Differential Encoding

Gaussian FSK lessens spectral leakage at the expense of some loss in intersymbol discriminability

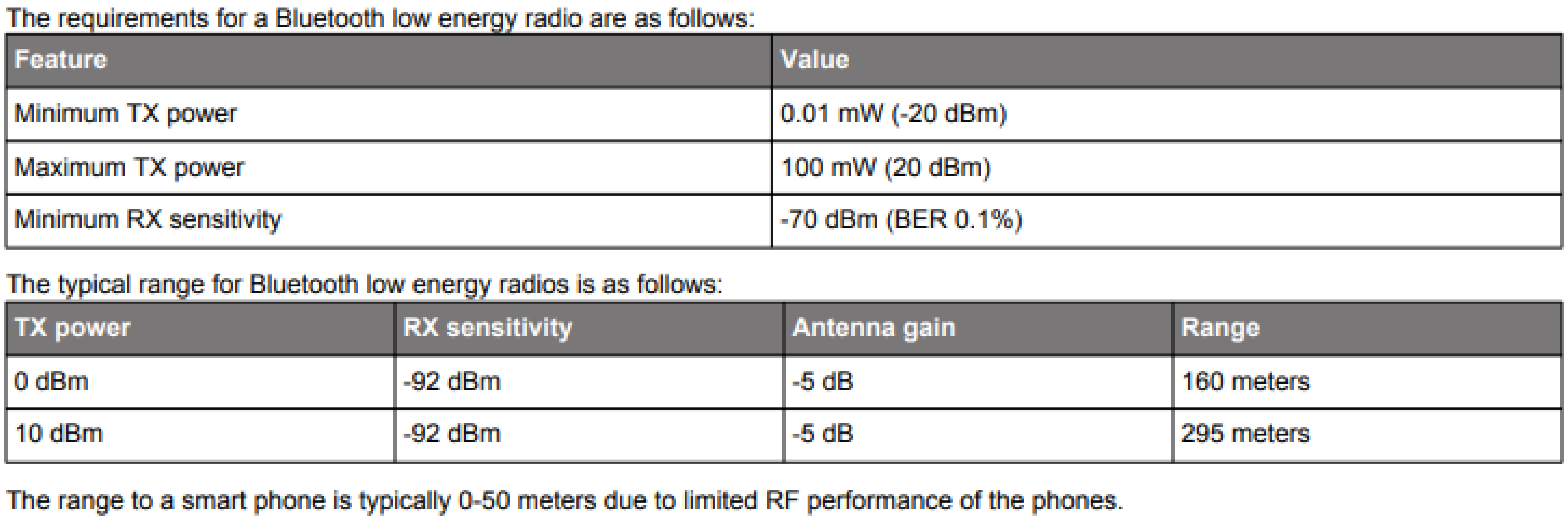




An example from `good case` BLE hardware



BLE signal strength



The requirements for a Bluetooth low energy radio are as follows:

Feature	Value
Minimum TX power	0.01 mW (-20 dBm)
Maximum TX power	100 mW (20 dBm)
Minimum RX sensitivity	-70 dBm (BER 0.1%)

The typical range for Bluetooth low energy radios is as follows:

TX power	RX sensitivity	Antenna gain	Range
0 dBm	-92 dBm	-5 dB	160 meters
10 dBm	-92 dBm	-5 dB	295 meters

The range to a smart phone is typically 0-50 meters due to limited RF performance of the phones.

- Remember nRF52840 capabilities
  - Transmit: up to 8 dBm
  - Receive sensitivity: -95 dBm

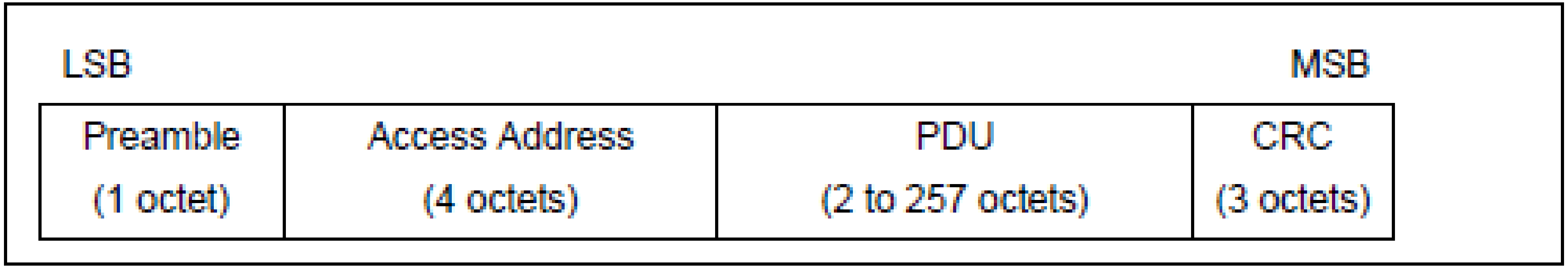
Outline

- Data Link Layer

- BLE Background

- **BLE Layers**
  - Physical Layer
  - **Link Layer**

Packet structure



LSB | | | MSB

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

Figure 2.1: Link Layer packet format

- Same packet structure for both advertisements and connections
  - Fields are filled in little endian (the opposite of network byte order 😠)
- Access address unique for each connection (randomly chosen)
  - In Advertising always set to 0x8E89BED6

Device addresses

- Public and private address forms
- Public
  - 48 bits: 24-bits of company ID, 24-bits of company assigned number
  - Literally the same MAC address scheme as Ethernet and WiFi
- Private
  - Top two MSbs specify type
    - 46 bits of random
    - 46 bits of hash of an identity key
- **Why have the two types?**

Device addresses

- Public and private address forms
- Public
    - 48 bits: 24-bits of company ID, 24-bits of company assigned number
    - Literally the same MAC address scheme as Ethernet and WiFi
- Private
    - Top two MSbs specify type
        - 46 bits of random
        - 46 bits of hash of an identity key
- **Why have the two types?** **Privacy**

Data whitening

- Avoid long series of repetitive bits (all zeros or all ones)
  - Would cause RF noise to be more focused in one direction
  - Radio hardware desires output to have zero DC-bias (or close to that)
  - Great example of the PHY and MAC being interwoven in wireless

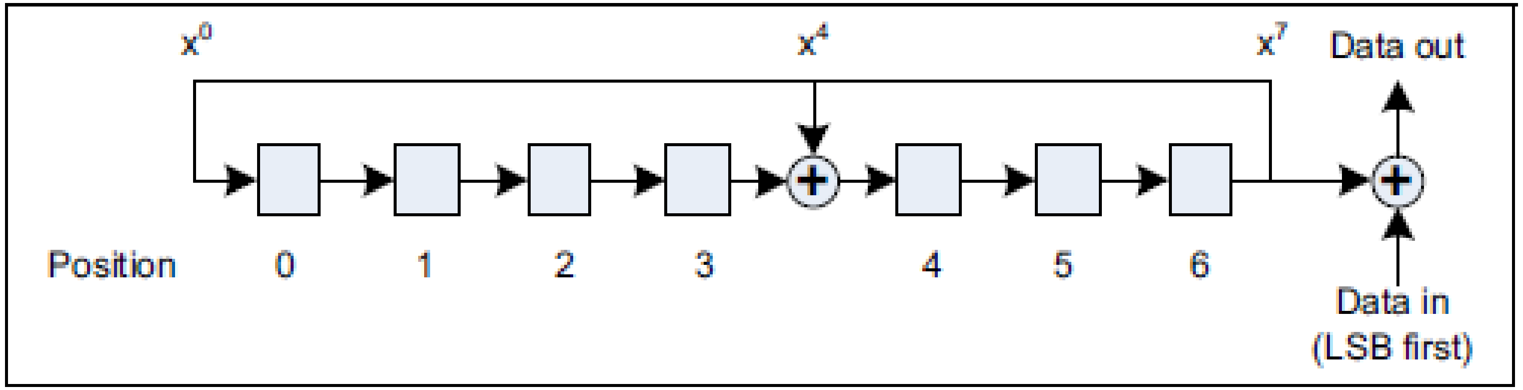


Figure 3.3: The LFSR circuit to generate data whitening

- I always forget this exists, since hardware usually handles it automatically

Bit processing pipeline

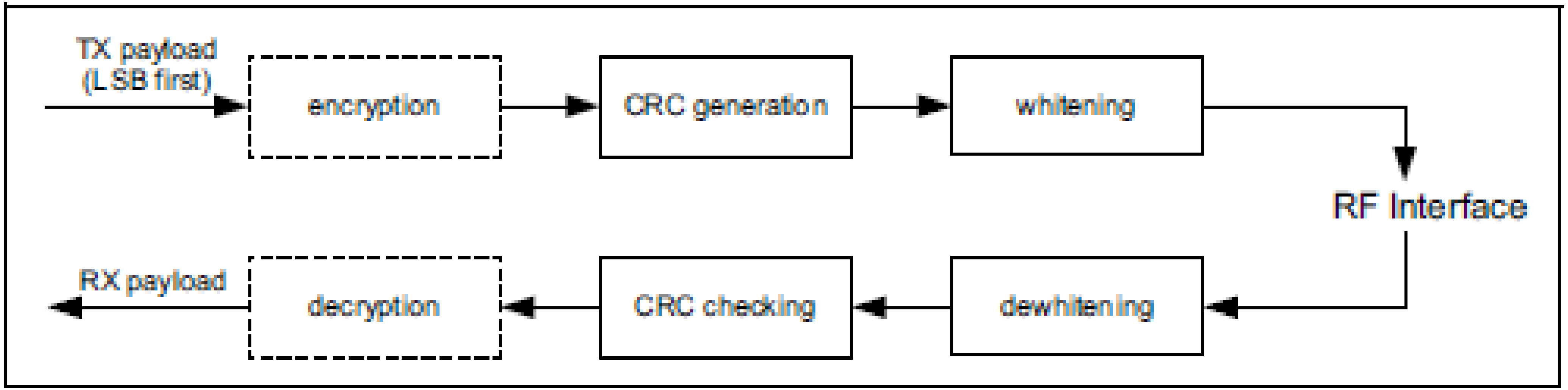


Figure 3.1: Payload bit processes for the LE Uncoded PHYs

Break + Question

- With enough scanners, could you track BLE devices as they move?

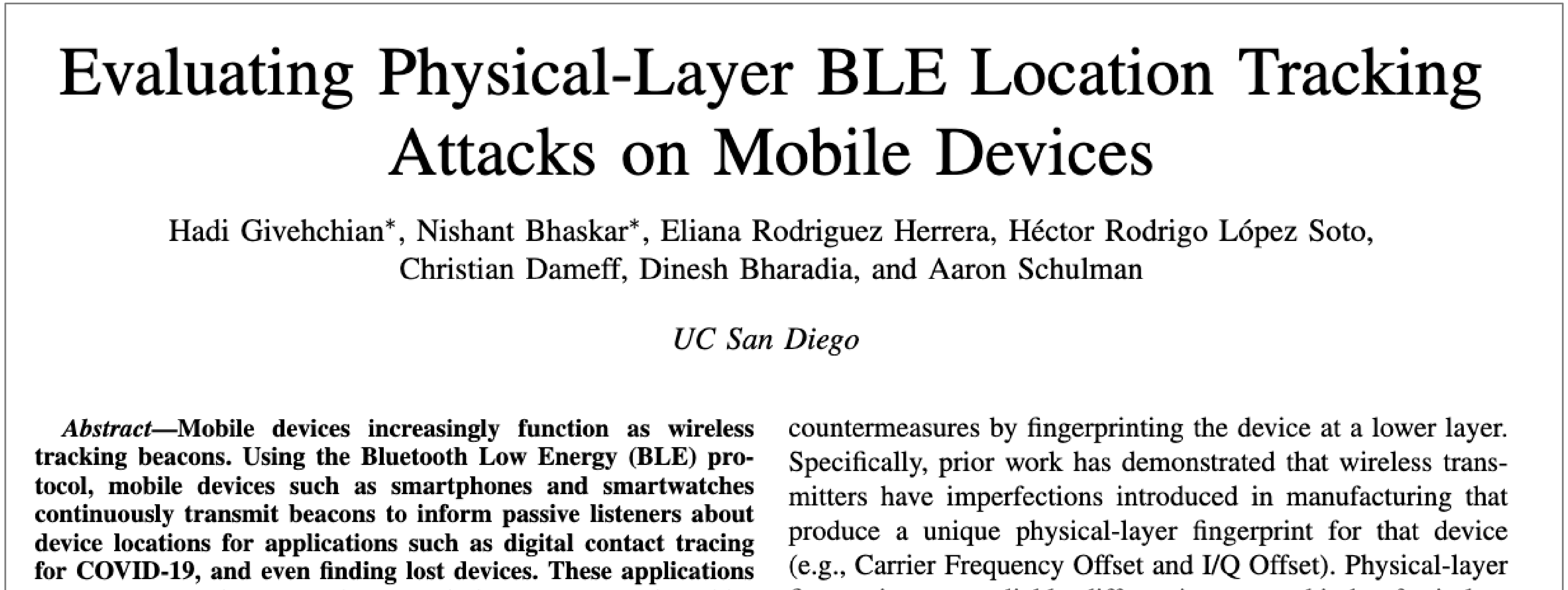
Break + Question

- With enough scanners, could you track BLE devices as they move?

    - Link Layer
        - Depends on how long they use a device address for
        - You can do a scan of BLE transmissions to find device addresses
        - Scans at multiple locations can detect when a device moves throughout an area
        - But if the device re-randomizes between two scanners, you can’t follow it anymore
            - Re-randomizing at a scanner could be detectable…
            - Or if the user has more than one device with unsynchronized rotation schedules

Break + Question

- With enough scanners, could you track BLE devices as they move?
  - Physical Layer
    - Fingerprint unique physical-layer imperfections in signals
    - Looking at things like amplitude and timing
    - 2022 paper out of UCSD explores this



Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices

Hadi Givehchian*, Nishant Bhaskar*, Eliana Rodriguez Herrera, Héctor Rodrigo López Soto,
Christian Dameff, Dinesh Bharadia, and Aaron Schulman

UC San Diego

***Abstract*—Mobile devices increasingly function as wireless tracking beacons. Using the Bluetooth Low Energy (BLE) protocol, mobile devices such as smartphones and smartwatches continuously transmit beacons to inform passive listeners about device locations for applications such as digital contact tracing for COVID-19, and even finding lost devices. These applications**

countermeasures by fingerprinting the device at a lower layer. Specifically, prior work has demonstrated that wireless transmitters have imperfections introduced in manufacturing that produce a unique physical-layer fingerprint for that device (e.g., Carrier Frequency Offset and I/Q Offset). Physical-layer

Outline

- Data Link Layer

- BLE Background

- BLE Layers
  - Physical Layer
  - Link Layer