CSE 122/222C ; WES 269

BLE Advertising Deep Dive

Pat Pannuto, UC San Diego

ppannuto@ucsd.edu

BLE Advertising Deep Dive Goals

- Refresh Major Concepts in Bluetooth
- Investigate some questions of real-world performance!
  - What are real-world use cases of advertisements?
  - How much energy do advertisements take?
  - What is the probability of receiving a packet?
    - Of receiving data?

Outline

- **Recap**

- Communicating with Advertisements
  - Advertisement Use Cases
  - Energy Use
  - Packet Collisions

Bluetooth Classic and BLE co-exist & have different use cases

Bluetooth Classic (around since 1999)

- Continuous data communication
- Can afford higher battery power requirements

Bluetooth Low Energy (introduced in v4.0)

- Small amounts of data transfer
- Low power requirements
  - “months or years” on small batteries
- Ideal for IoT devices

Headphones

Car BT Audio

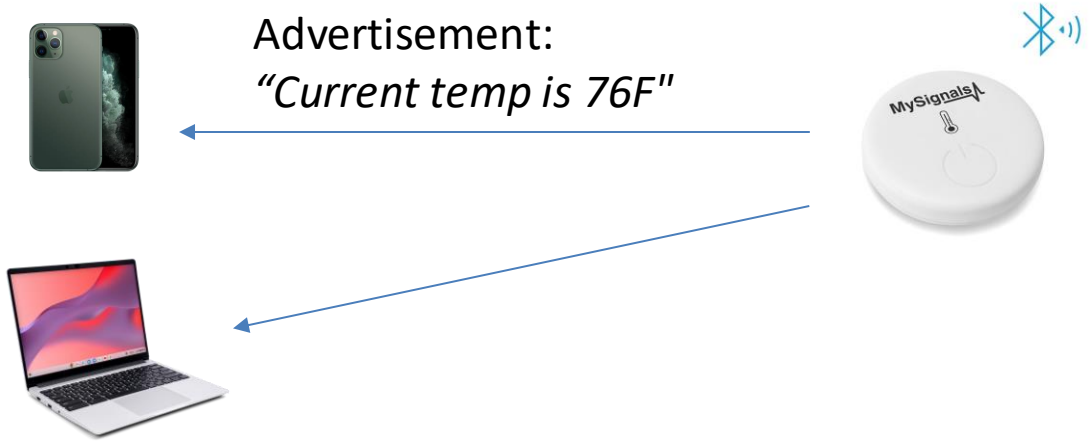
Mobile Photo Printers

Fitness Trackers

Tracking Devices (eg: Apple AirTag)

Switches and Sensors

Bluetooth Low Energy Roles: Scanner, Advertiser



BLE Central and Peripheral roles are for connections

Central

Advertisement:
"I'm the Living Room Light"

Connection Request

Connected (stops advertising)

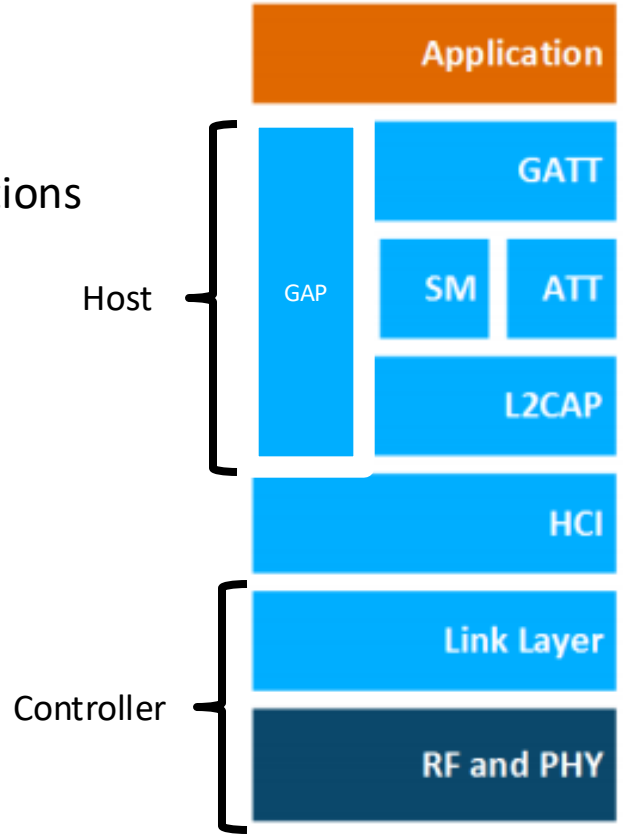
"Set light brightness to 50%"

Peripheral

(note: this is highly simplified)

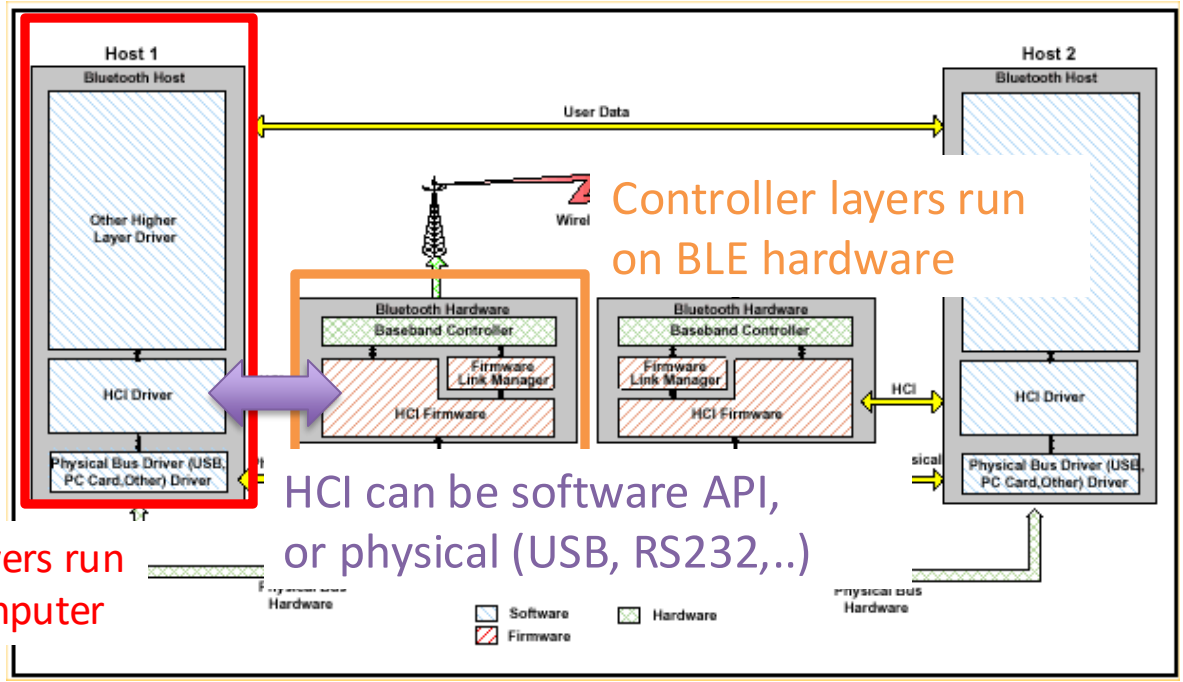
BLE Layers

- Host – Configuration for advertisements, connections
  - GAP – Generic Access Profile
    - Configure advertising
  - GATT – Generic ATTribute profile
    - Configure connections
- HCI - Host Controller Interface
- Controller - Communication
  - Link Layer – send packets
  - RF and PHY – send bits



What's the need for the HCI Layer?

- BT Classic envisioned separate implementations for Host and Controller



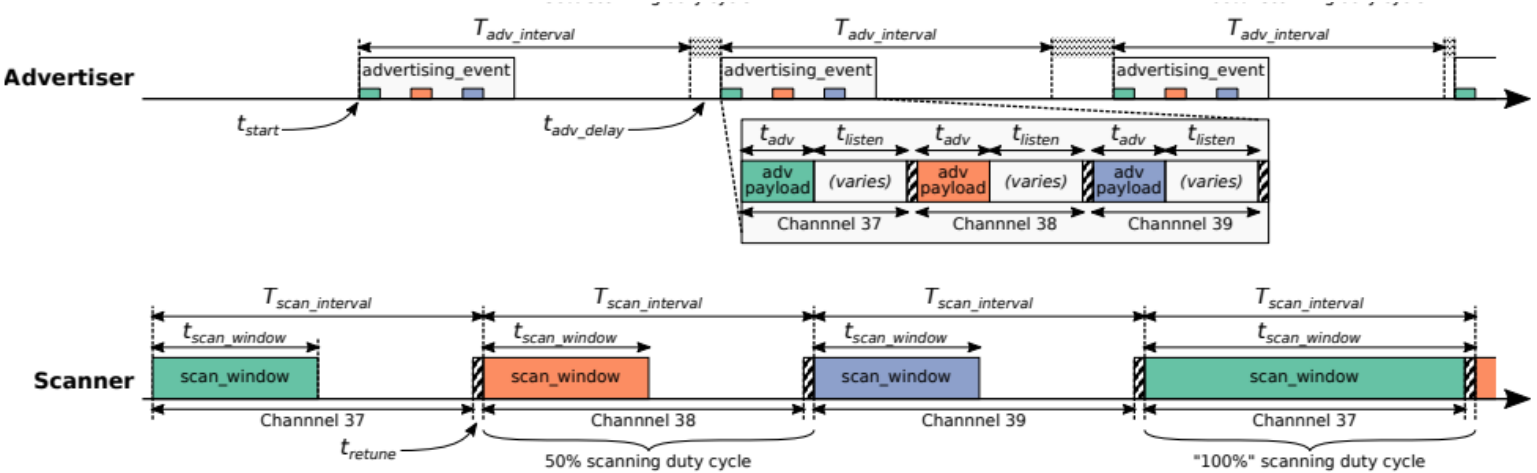
Controller layers run on BLE hardware

HCI can be software API, or physical (USB, RS232,..)

Host layers run on computer

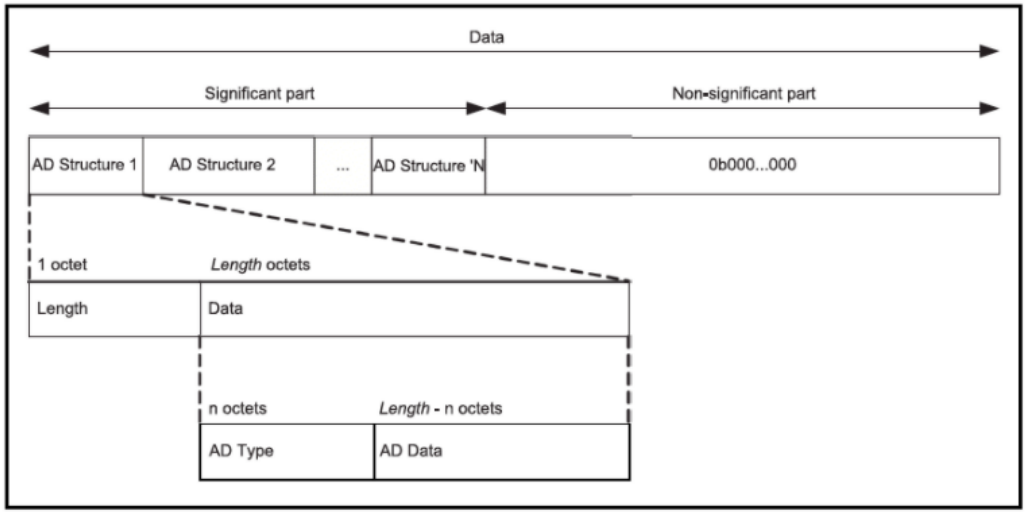
Advertisement and Scanning in Action

- Advertisements are received when the channel of the scan window and the channel of the advertisement overlap in time (and space)



Advertisement payloads are in Length – Type – Value Format

- Scanner hops through length/type pairs to find what interests it



- Name
- Service UUID
- TX Power Level
- Manufacturer-specific data
- And about twenty others
- Flags

Outline

- Recap

- **Communicating with Advertisements**
  - **Advertisement Use Cases**
  - Energy Use
  - Packet Collisions

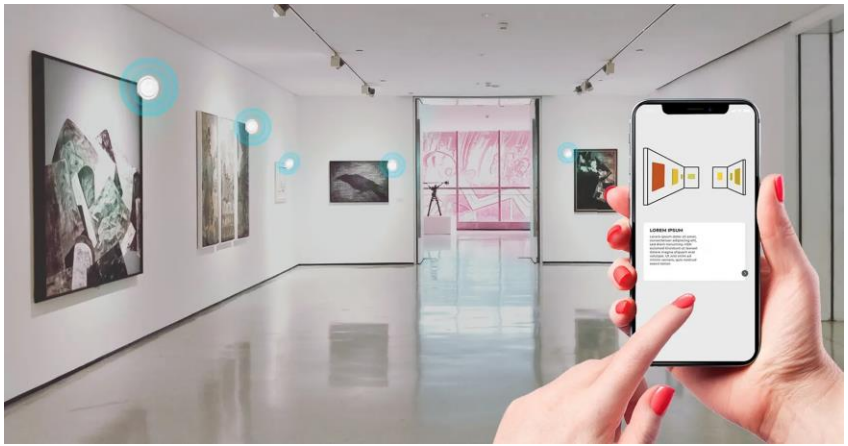
Advertisements alone can be used for communication

Recall: BLE advertisements are uncoordinated, broadcast messages designed for discovery

- Yet some devices, applications use *only* advertisements:
  1. Beacons – iBeacon, Eddystone
  2. Tracking – Tile, Apple AirTag
  3. Local communication – Apple Continuity
  4. Sensor deployments – PowerBlade

Beacons to advertise presence and send out useful information

- iBeacon and Eddystone
  - Popular formats for sending URLs and device identifiers
  - Use existing BLE fields (Service Data and Manufacturer-Specific Data)



Self-guided tours at museums

BLE signals can be used to track distance to items

- Find my X
  - Tile, AirTag: find my keys
  - Apple: find my device

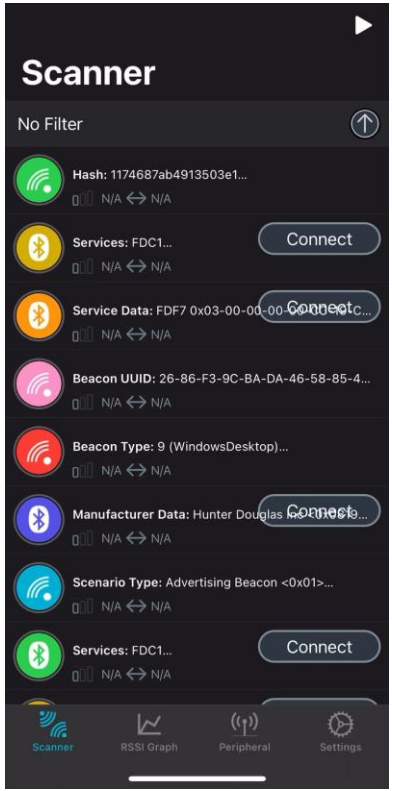
- Find devices nearby
  - Get a sense of distance to the device

nRF Connect Activity

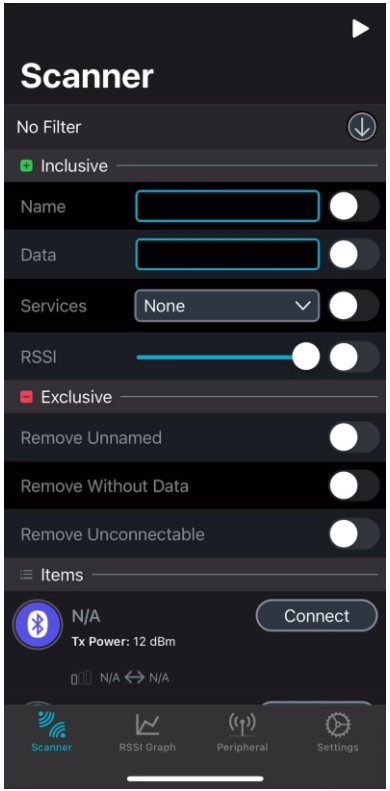
- Work in pairs with your neighbor
- Open nRF Connect app on both smartphones
- 1 person becomes Advertiser
- Other person becomes Scanner

- Advertiser:
  - Go to Peripheral
  - Set a name for your Advertiser
  - Start Advertising

- Scanner:
  - Start scan (Play button on top right)
  - Filter by Advertiser's name
  - Go to RSSI viewer



Advertiser



Scanner

RSSI and some questions

- **RSSI (Received Signal Strength Indicator)**: Strength of beacon's signal as seen on receiving device

- What's the highest RSSI value you notice?
  How close to the advertiser is this?

- What do you notice about RSSI when moving away from the advertiser?

RSSI Experiments

- Can you get different RSSI readings at the same distance?
- Can get the same RSSI readings at different distances?

Intuition on using signal strength to find distance

- **RSSI (Received Signal Strength Indicator)**: Strength of beacon's signal as seen on receiving device

Measured Power: -20 dBm
factory-calibrated, read-only constant

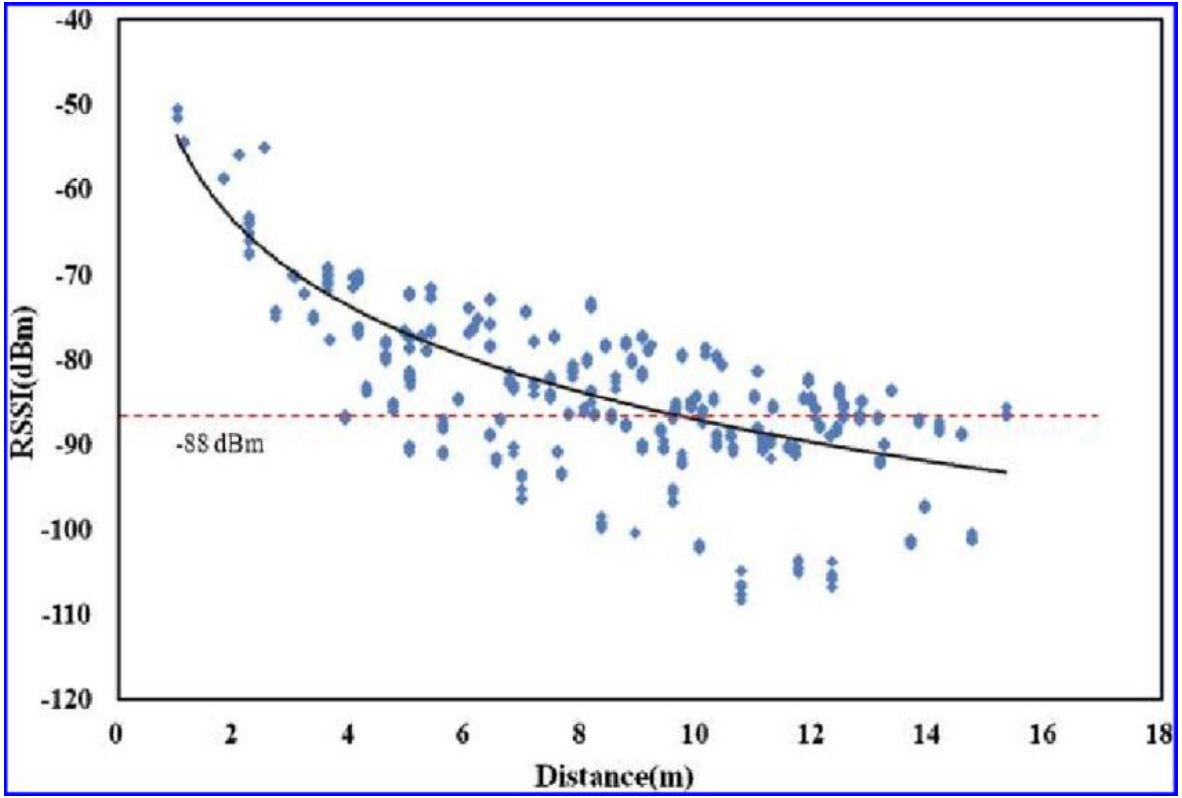
RSSI from received signal

"Hey you should be getting an RSSI of -20 dBm at 1 m distance from me"

Can roughly figure out how far the beacon is

Problem with RSSI-based distance – not accurate

- Pathloss is NOT only due to distance
- RSSI is way worse at this than you hope it would be



Apple uses BLE on its devices to implement “Continuity”

- Key part of Apple’s “ecosystem”, including:

- Handoff
  - start tasks on one device and continue on another device
- Universal Clipboard,
  - copying of data from one Apple device and pasting on another
- iPhone Cellular Calls
  - make calls using iPhone’s cellular connection on Mac or iPad

Uses BLE "Manufacturer Specific Data" to communicate

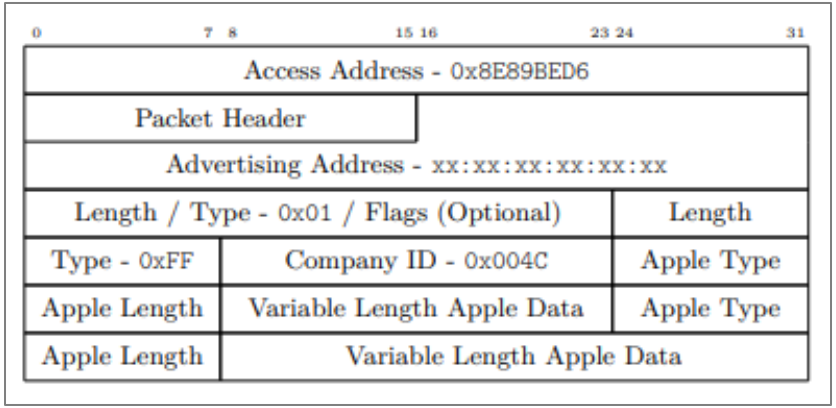
- Communication with only *nearby* devices

Table 1. Advertisement Frames

		Test 1	Test 2
		Count	
Address Type	Public	26	57
	Random	726	1,518
Company ID†	Apple	692	1296
	Microsoft	30	201
	Garmin	2	9
	Samsung	0	3
	All Others	2	9

† Randomized Devices Only

Martin, Jeremy, et al. "Handoff all your privacy–a review of apple's bluetooth low energy continuity protocol." *Proceedings on Privacy Enhancing Technologies* 2019.4 (2019): 34-53.



Type	Value
Watch Connection	11
Handoff	12
Wi-Fi Settings	13
Instant Hotspot	14
Wi-Fi Join Network	15
Nearby	16

Table 3. Action Codes

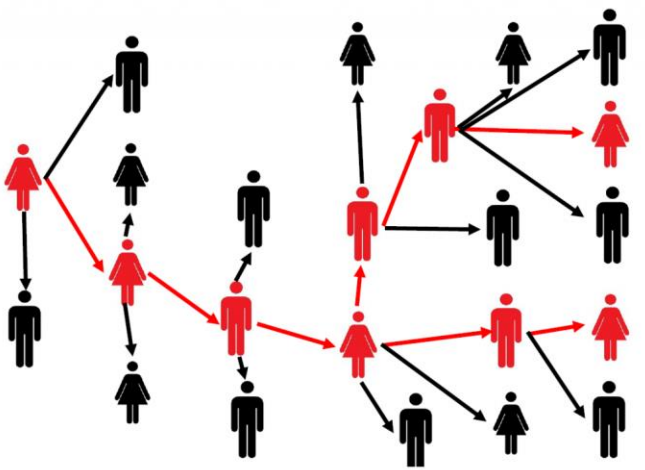
Type	Description
1	iOS recently updated
3	Locked Screen
7	Transition Phase
10	Locked Screen, Inform Apple Watch
11	Active User
13	Unknown
14	Phone Call or Facetime

Local Communication: Exposure Notifications

- Apple and Google collaboration to use phones for contact tracing
  - Smartphone constantly broadcasts identifier.
  - Periodically, each smartphone listens for broadcasts around it.
  - Check list of identifiers to see if you've been around someone who is sick.

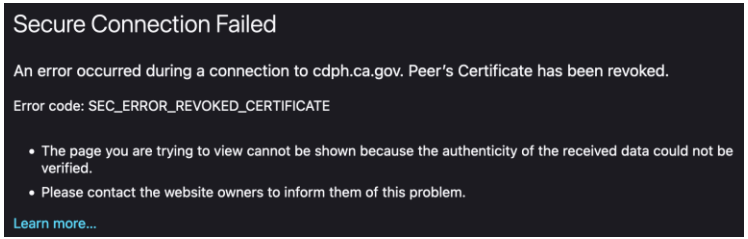
- Requires government/healthcare system interactions to determine when an identifier should be flagged as sick
  - 24 states adopted this

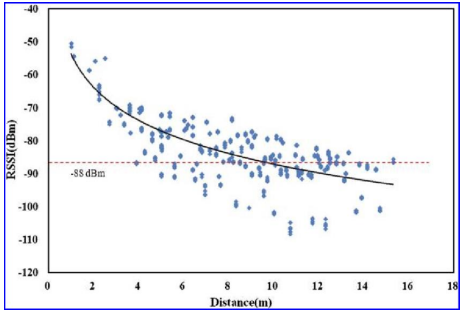
- Implemented at OS level in background



Cautionary Tale:
Technology cannot solve all the world's problems

- What was the state of CA Notify on October 4, 2022?





- More seriously, advertisement-only was always going to be limited
- **Bad/imperfect technology is not neutral — this caused measurable harm**
  - Post-hoc analyses show contact-tracing apps reduced trust in government, reduced willingness to use future apps (independent of source)

Contact-tracing apps and alienation in the age of COVID-19

Frantz Rowe, Ojelanki Ngwenyama &

Pages 545-562 | Received 25 Jun 2020, Accepted 26 Ju

Citizens' Attitudes to Contact Tracing Apps

Published online by Cambridge University Press: **02 September 2020**

Laszlo Horvath, Susan Banducci and Oliver James

One for all, all for one: Social considerations in user acceptance of contact tracing apps using longitudinal evidence from Germany and Switzerland

Olga Abramova [a], Amina Wagner [b], Christian M. Olt [b], Peter Buxmann [b]

Outline

- BLE roles
  - Advertising
  - Scanning

- **Advertisement-based Networking?**
  - Advertisement Use Cases
  - **Energy Use**
  - Packet Collisions

Paper: power measurements of BLE advertisements

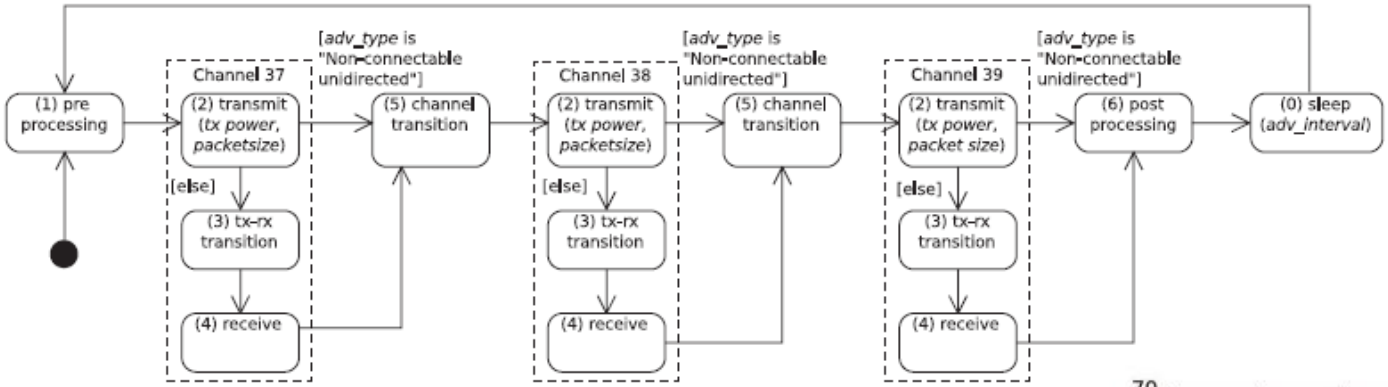
Schrader, Raphael, et al. "Advertising power consumption of bluetooth low energy systems." *2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*. IEEE, 2016.

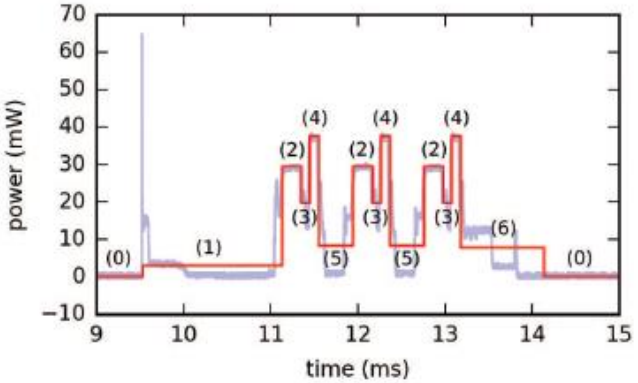
The 3rd IEEE International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems
26-27 September 2016, Offenburg, Germany

Advertising Power Consumption of Bluetooth Low Energy Systems

Raphael Schrader, Thomas Ax, Christof Röhrig, Claus Fühner
Fachhochschule Dortmund
Fachbereich Informatik
Email: claus.fuehner@fh-dortmund.de

Energy model for BLE advertisements





Power measured for BLE adv states for hardware

- Power use and duration energy measured on
  - nRF51 Development Kit (nRF51822 System-on-Chip)
  - nRF52 DK (nRF52832 SoC)

nRF51 DK

nRF51822 SoC

TABLE II
SoC-Dependent Model Parameters from Measurements

Phase	Nordic nRF51		Nordic nRF52	
	T_i (σ) (µs)	$\overline{P_i}$ (mW)	T_i (σ) (µs)	$\overline{P_i}$ (mW)
preprocessing	951.8 (9.1)	2.9	321.4 (8.9)	2.7
tx (4 dBm)	72.4 (0.5) + $n_{\text{Bit}} \cdot 1/\text{Bit}$	45.4	13.2 (1.8) + $n_{\text{Bit}} \cdot 1/\text{Bit}$	46.2
tx (0 dBm)		29.5		33.2
tx (-4 dBm)		25.8		27.5
tx (-8 dBm)		23.2		25.3
tx (-12 dBm)		21.1		23.6
tx (-16 dBm)		19.8		22.6
tx (-20 dBm)		18.9		21.6
tx-rx transit.	94.7 (0.6)	19.6	130.6 (2.0)	15.9
rx	104.3 (1.5)	37.6	73.0 (3.9)	32.4
channel transit.	390.4 (0.9)	8.4	432.3 (4.47)	7.3
postprocessing	961.8 (156.9)	7.7	321.4 (32.2)	10.2
sleep	T_{advSleep}	0.0114	T_{advSleep}	0.0058

Exercise: How much energy does one advertising cycle consume?
(for the peripheral / advertising device)

- nrf52 chip
- 0 dBm TX power
- 30 byte advertisement (total)
- Receive window is 100 µs
- 500 ms advertisement interval
- Ignore startup, transition, and processing energy use

TABLE II
SoC-Dependent Model Parameters from Measurements

Phase	Nordic nRF51		Nordic nRF52	
	T_i (σ) (µs)	$\overline{P_i}$ (mW)	T_i (σ) (µs)	$\overline{P_i}$ (mW)
preprocessing	951.8 (9.1)	2.9	321.4 (8.9)	2.7
tx (4 dBm)	72.4 (0.5) + $n_{Bit} \cdot 1/Bit$	45.4	13.2 (1.8) + $n_{Bit} \cdot 1/Bit$	46.2
tx (0 dBm)		29.5		33.2
tx (-4 dBm)		25.8		27.5
tx (-8 dBm)		23.2		25.3
tx (-12 dBm)		21.1		23.6
tx (-16 dBm)		19.8		22.6
tx (-20 dBm)		18.9		21.6
tx-rx transit.	94.7 (0.6)	19.6	130.6 (2.0)	15.9
rx	104.3 (1.5)	37.6	73.0 (3.9)	32.4
channel transit.	390.4 (0.9)	8.4	432.3 (4.47)	7.3
postprocessing	961.8 (156.9)	7.7	321.4 (32.2)	10.2
sleep	$T_{advSleep}$	0.0114	$T_{advSleep}$	0.0058

How much energy does one advertising cycle consume?

- Energy = TX + RX + sleep
- TX:
  - 30 bytes @ 1 Mbps
  - 3 channels
  - 240 us * 3 = 720 us
  - 720 us * 33.2 mW = 23.9 µJ
- RX:
  - RW = 100 us
  - 3 channels
  - 300 us * 32.4 mW = 9.7 µJ
- Sleep
  - 500 ms interval
  - Radio active = 720 us + 300 us
  - Sleep = 500 ms – 1.02 ms
  - 498.98 ms * 0.0058 mW = 2.9 µJ
- Energy = 23.9 µJ + 9.7 µJ + 2.9 µJ = 36.5 µJ

TABLE II
SoC-Dependent Model Parameters from Measurements

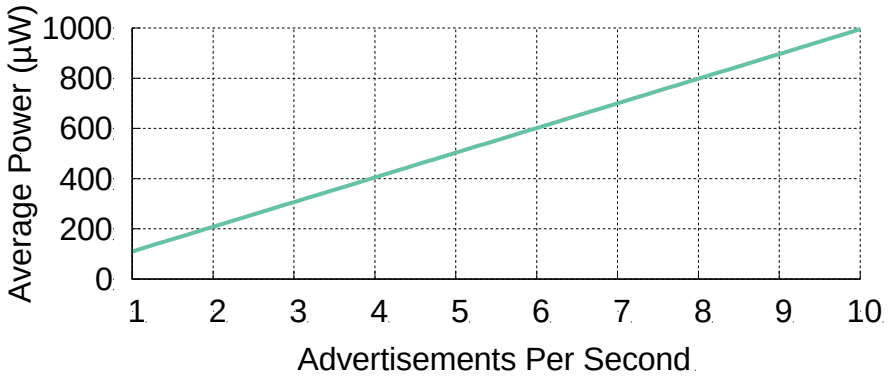
Phase	Nordic nRF51		Nordic nRF52	
	T_i (σ) (µs)	$\overline{P_i}$ (mW)	T_i (σ) (µs)	$\overline{P_i}$ (mW)
preprocessing	951.8 (9.1)	2.9	321.4 (8.9)	2.7
tx (4 dBm)	72.4 (0.5) + $n_{Bit} \cdot 1/Bit$	45.4	13.2 (1.8) + $n_{Bit} \cdot 1/Bit$	46.2
tx (0 dBm)		29.5		33.2
tx (-4 dBm)		25.8		27.5
tx (-8 dBm)		23.2		25.3
tx (-12 dBm)		21.1		23.6
tx (-16 dBm)		19.8		22.6
tx (-20 dBm)		18.9		21.6
tx-rx transit.	94.7 (0.6)	19.6	130.6 (2.0)	15.9
rx	104.3 (1.5)	37.6	73.0 (3.9)	32.4
channel transit.	390.4 (0.9)	8.4	432.3 (4.47)	7.3
postprocessing	961.8 (156.9)	7.7	321.4 (32.2)	10.2
sleep	$T_{advSleep}$	0.0114	$T_{advSleep}$	0.0058

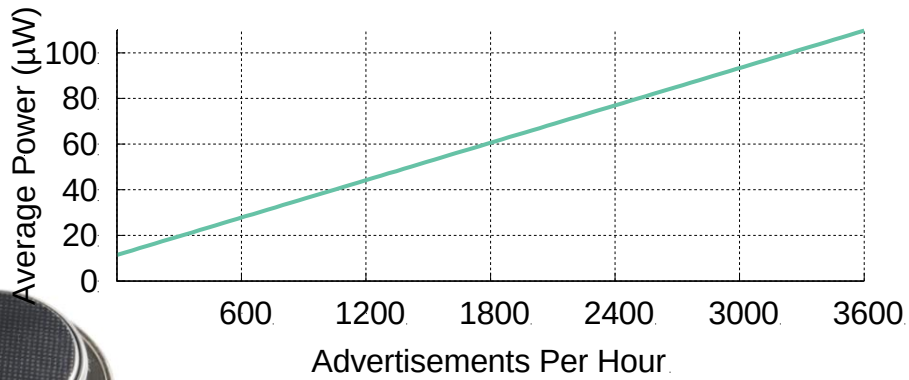
How much energy does it cost to send data over advertisements?

- Configuration
  - nRF51822 microcontroller
  - Maximum payload size
  - +4 dBm transmit power
  - Connectable advertisement
  - Sleep power 11 µW

- One packet per second example:
  - 110 µW average
  - **~270 days** on a CR2032

- One packet per minute example:
  - 13 µW average
  - **~2250 days (6 years)** on a CR2032





Outline

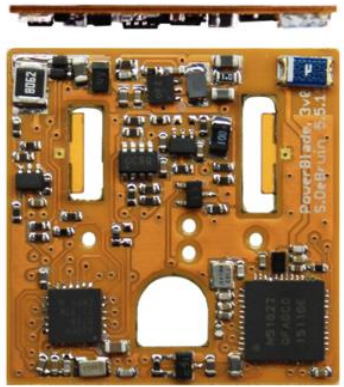
- BLE roles
  - Advertising
  - Scanning

- **Advertisement-based Networking?**
  - Advertisement Use Cases
  - Energy Use
  - **Packet Collisions**

Example of real-world research:

Sensor data collection via BLE advertisements

- Motivation:
  - Very resource-constrained device
  - Diverse environments (“quick-deploy”)
- Requirements:
  - Report data so gateways and users can retrieve it simultaneously
  - Easy introspection during a deployment
- Idea: Ignore difficult questions about networking
  - Just broadcast the data!
  - **Will it work?**



DeBruin, Samuel, et al. "Powerblade: A low-profile, true-power, plug-through energy meter." *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. 2015.

Questions about network capability

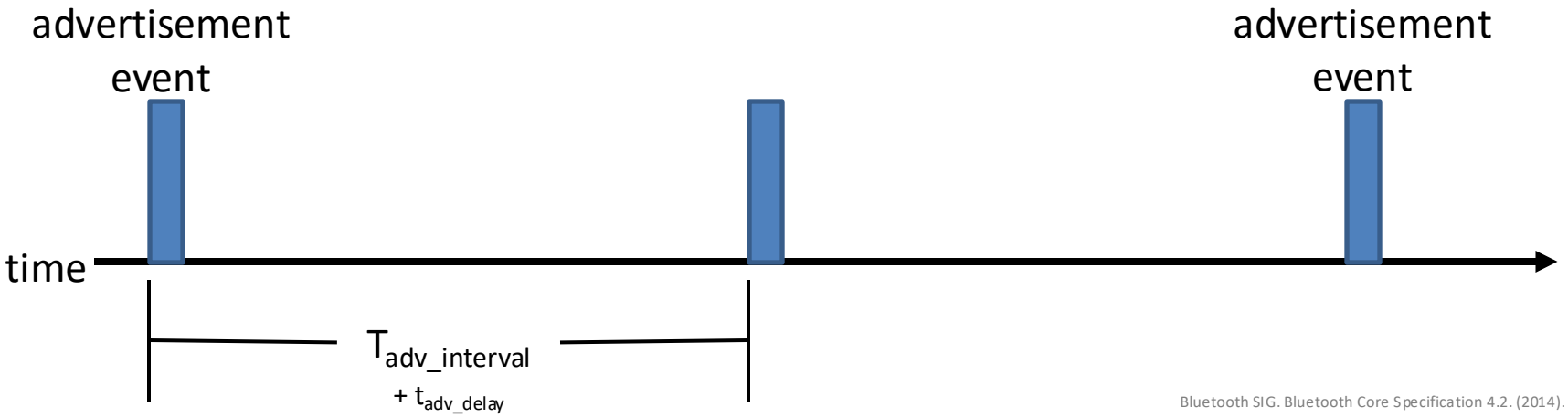
- What are the odds that a transmitted advertisement will be received?
  - **Packet reception rate**

- If M redundant advertisements are sent instead, what are the odds that at least one are received?
  - **Data reception rate**

- How do these odds vary with number of devices, advertising interval, and packet size?

BLE advertisements are periodic, broadcast transmissions.

- Advertisement events occur periodically ($T_{adv\_interval}$: 20 ms–10 s).
- Random delay appended before each transmission (t_{adv_delay}: 0–10 ms).
- Data payload of up to 31 bytes.

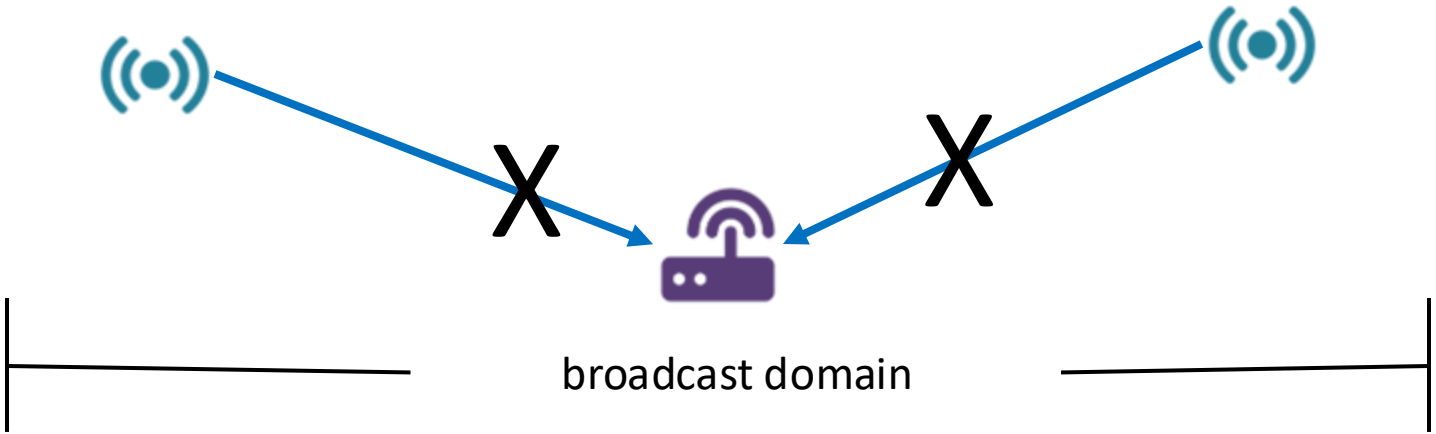


Bluetooth SIG. Bluetooth Core Specification 4.2. (2014).

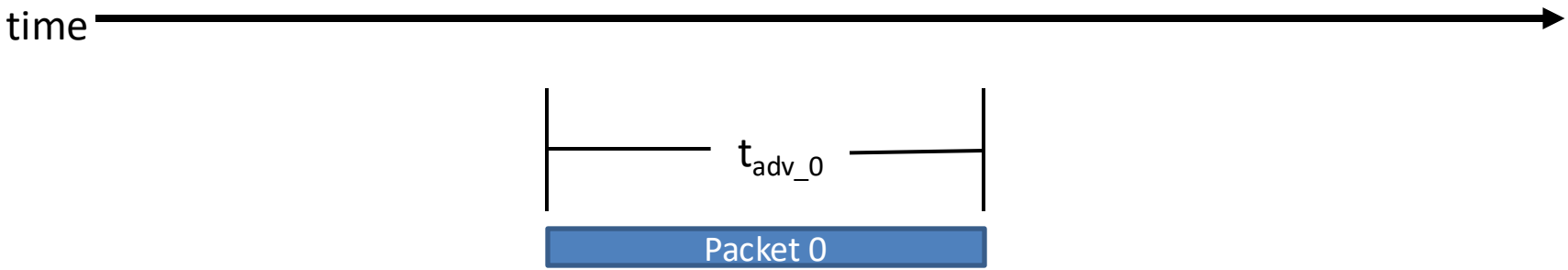
What causes transmissions not to be received?

1. Not within range of the gateway
   - Or various other losses within the gateway itself

2. Two devices try to send at the same time (packet collision)

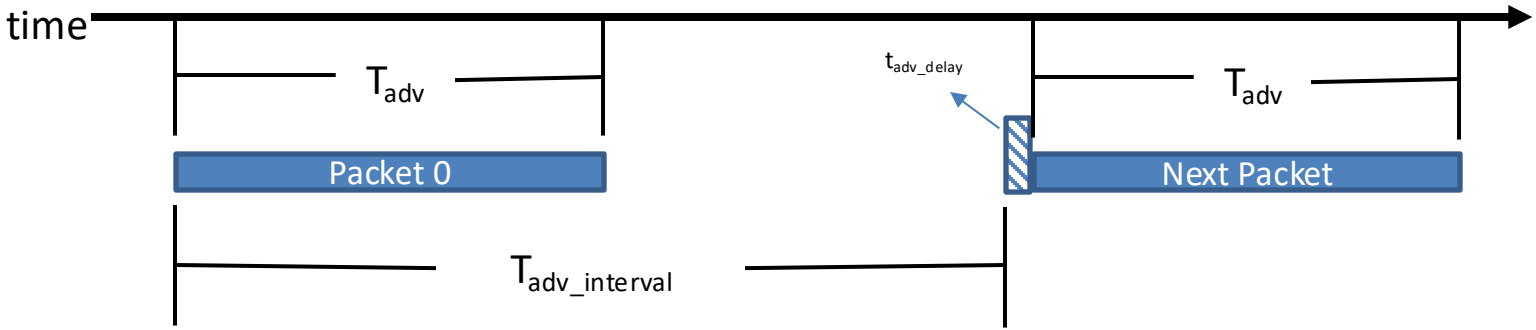


What is the probability of a packet collision?



Jeon, Wha Sook, et al. "Performance analysis of neighbor discovery process in bluetooth low-energy networks." (IEEE Transactions on Vehicular Technology, 2016).
Perez-Diaz de Cerio, David, et al. "Analytical and experimental performance evaluation of BLE neighbor discovery process including non-idealities of real chipsets." (Sensors, 2017).

Let's define some terms for a single advertiser



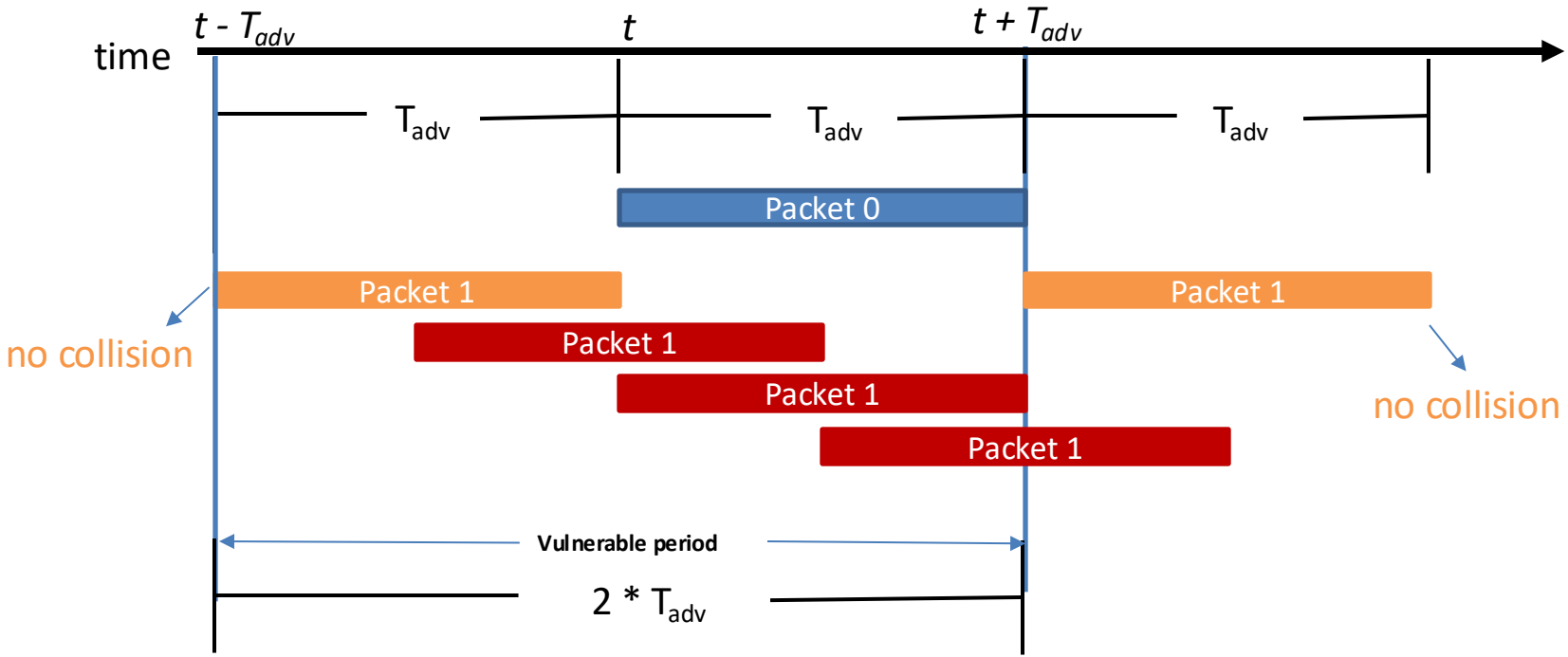
T_{adv}: Transmission Time for packet

t_{adv_delay}: Random advertisement delay

$T_{advInterval}$: Advertisement interval

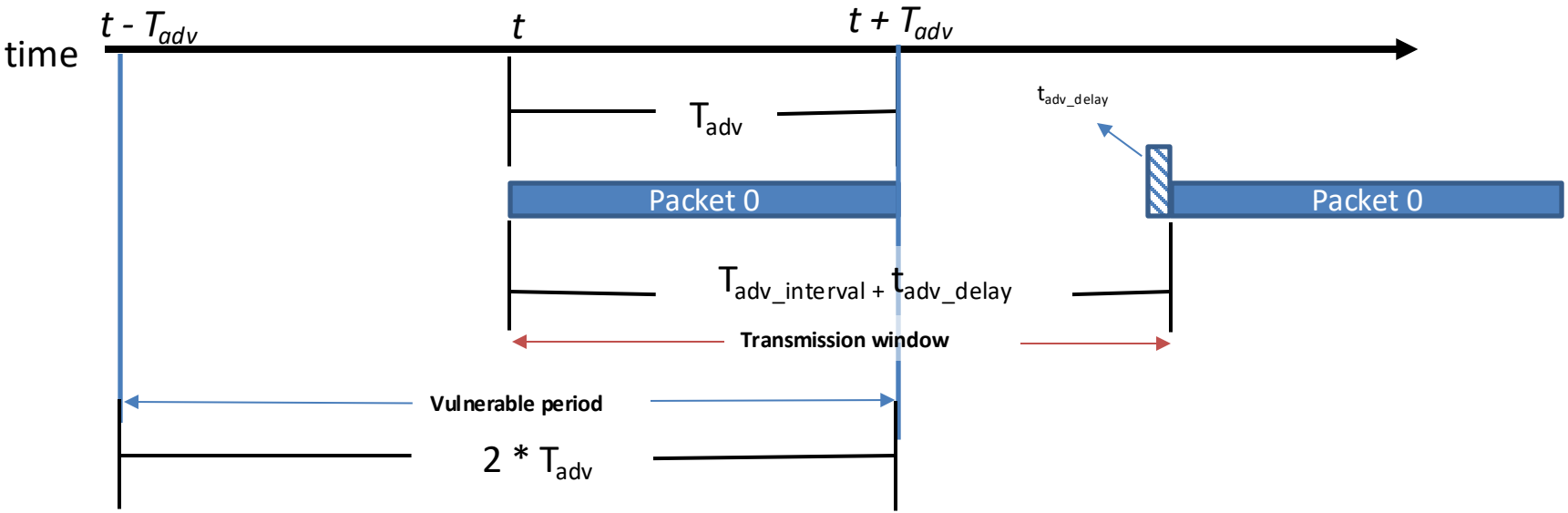
Jeon, Wha Sook, et al. "Performance analysis of neighbor discovery process in bluetooth low-energy networks." (IEEE Transactions on Vehicular Technology, 2016).
Perez-Diaz de Cerio, David, et al. "Analytical and experimental performance evaluation of BLE neighbor discovery process including non-idealities of real chipsets." (Sensors, 2017).

Collisions occur if any part of the two packets overlap



Jeon, Wha Sook, et al. "Performance analysis of neighbor discovery process in bluetooth low-energy networks." (IEEE Transactions on Vehicular Technology, 2016).
Perez-Diaz de Cerio, David, et al. "Analytical and experimental performance evaluation of BLE neighbor discovery process including non-idealities of real chipsets." (Sensors, 2017).

Computing probability of collision from vulnerable period and Tx window



$$\text{Probability of Collision} = \frac{Vulnerable\ Period}{Transmission\ Window} = \frac{2 * T_{adv}}{T_{adv\_interval} + avg(t_{adv\_delay})}$$

Easy way to combat inevitable collisions: Just say it twice!
(…or three times, or four times, …)

With redundancy, we care about data reception instead of packet reception.

Naïve model:

- $Packet\ Reception\ Rate = 1 - (Probability\ of\ Collision)$
- $Data\ Reception\ Rate = 1 - (Probability\ of\ Collision)^{Number\ of\ Packets}$

Data Reception Assumption: repeat packet collisions are independent.

- True for any arbitrary selection of two BLE devices
- Close enough to true for two devices that have recently collided

Determine Probability of Multiple Failures
(How many times should we say the same thing?)

- Given:
  - Probability of collision of 1 packet with reference packet

$$\text{Probability of Collision} = \frac{Vulnerable\ Period}{Transmission\ Window} = \frac{2 * T_{adv}}{T_{adv\_interval} + avg\ (t_{adv\_delay})}$$

- Determine:
  - Probability of Reception for data sent redundantly across **M** packets
  - i.e., what are the odds that **at least one** of the packets doesn't collide
  - 1 – (Probability of Collision^M)
    - $(P_c)^M$ = Probability that all of them collide
    - 1-that = Probability that NOT all of them collide

Equations for modeling data transmissions

- Packet Reception Rate
  - Probability that at the transmitted packet does not have a collision with any of N transmitting devices

$$\mathrm{PRR} = (1 - \frac{2 * tadv}{T_{adv\_interval} + \mathrm{E}[tadv_{\_delay}]})^{N-1}$$

- Data Reception Rate
  - Probability that at least one of M redundant packets does not have a collision with any of N transmitting devices

$$\mathrm{DRR} = 1 - \left(1 - \left(1 - \frac{2 * t_{adv}}{T_{adv\_interval} + \mathrm{E}[tadv_{\_delay}]}\right)^{N-1}\right)^{M}$$

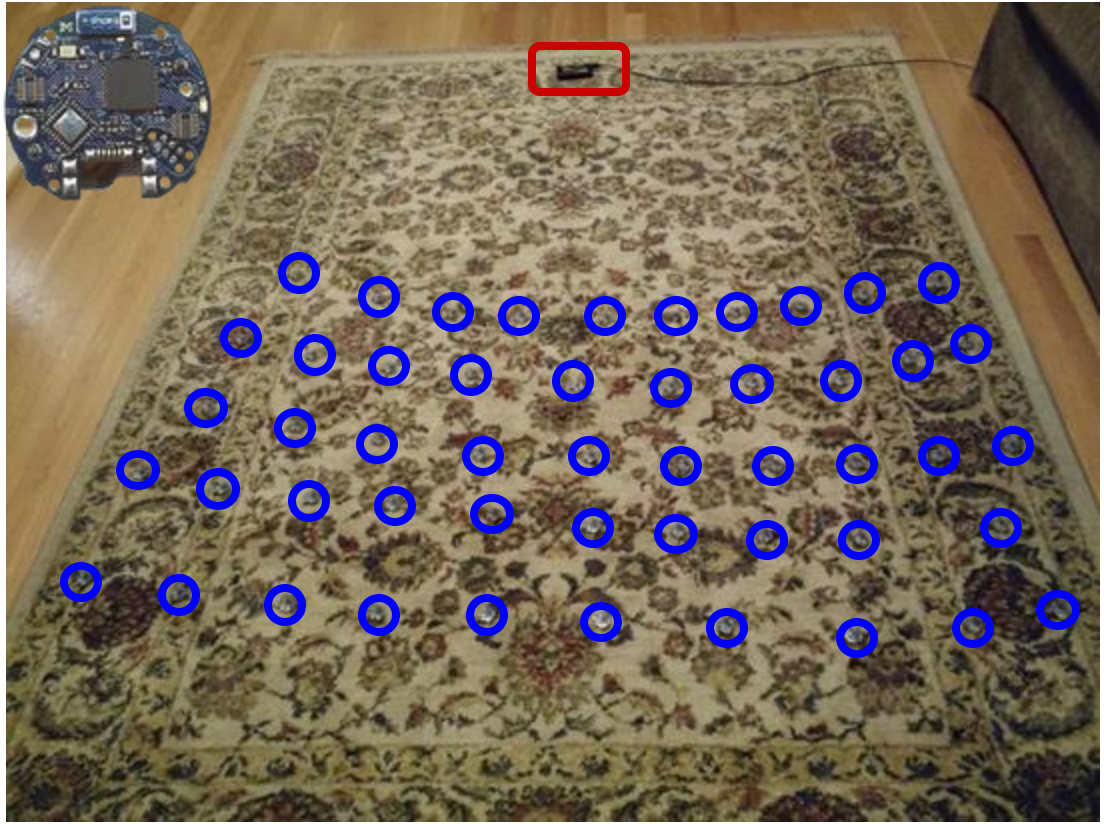
Is the model valid?

Empirical testing setup:

- 50 devices
- 1 meter from scanner
- 5-10 cm apart

Transmit monotonically increasing sequence numbers.

Sweep number of devices and advertising intervals.

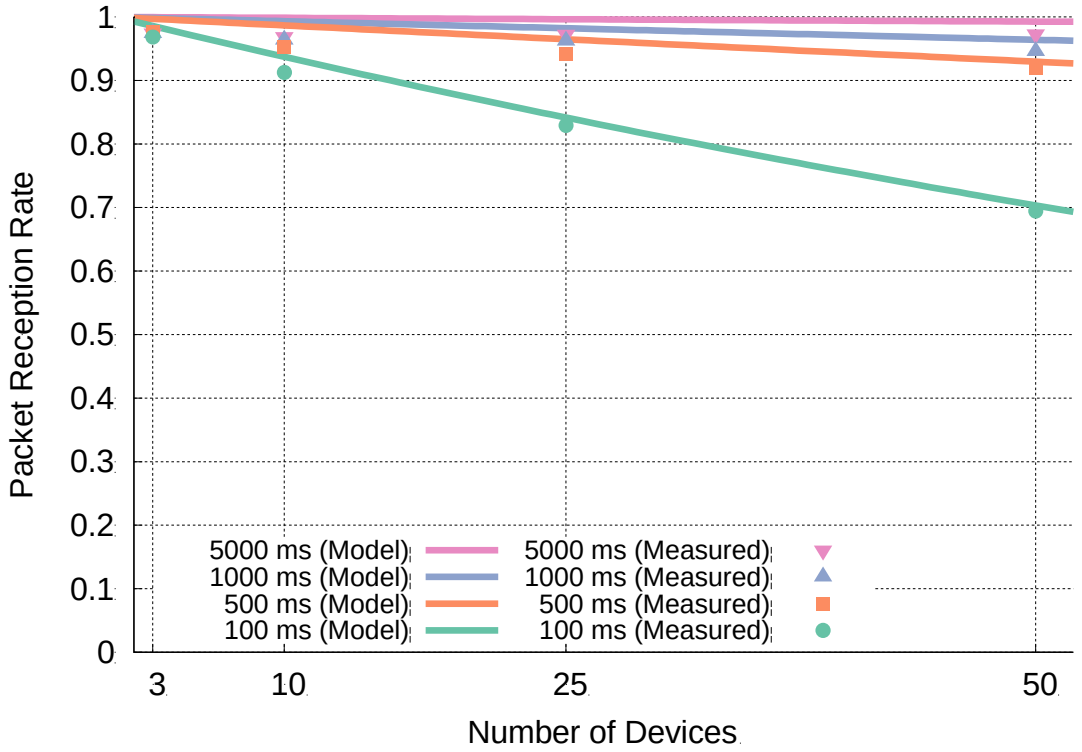


The model is accurate across advertisement rates and deployment sizes.

Accuracy is fairly consistent across intervals.

The model consistently overestimates the measured PRR values.

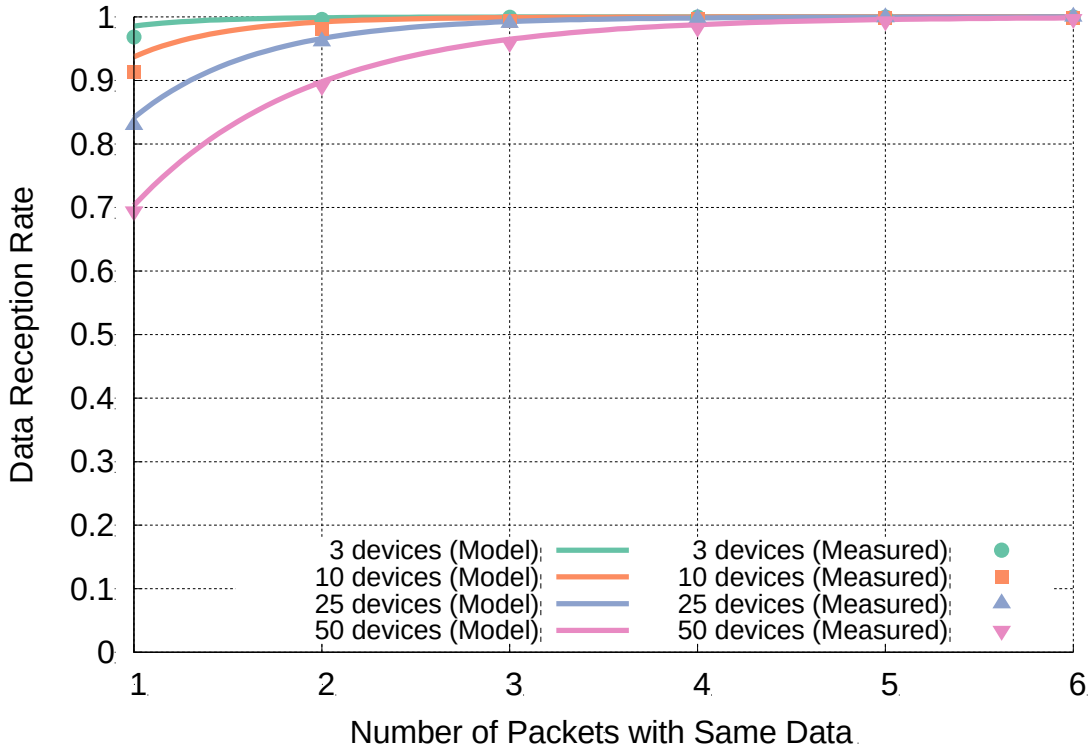
The effect could be due to RF interference.



The model accurately accounts for redundancy as well.

The same dataset can be used to measure the effect of redundancy by grouping sets of sequence numbers.

The model again slightly overestimates, but error reduces quickly as DRR approaches 100%.



What questions can we answer with a collision model?

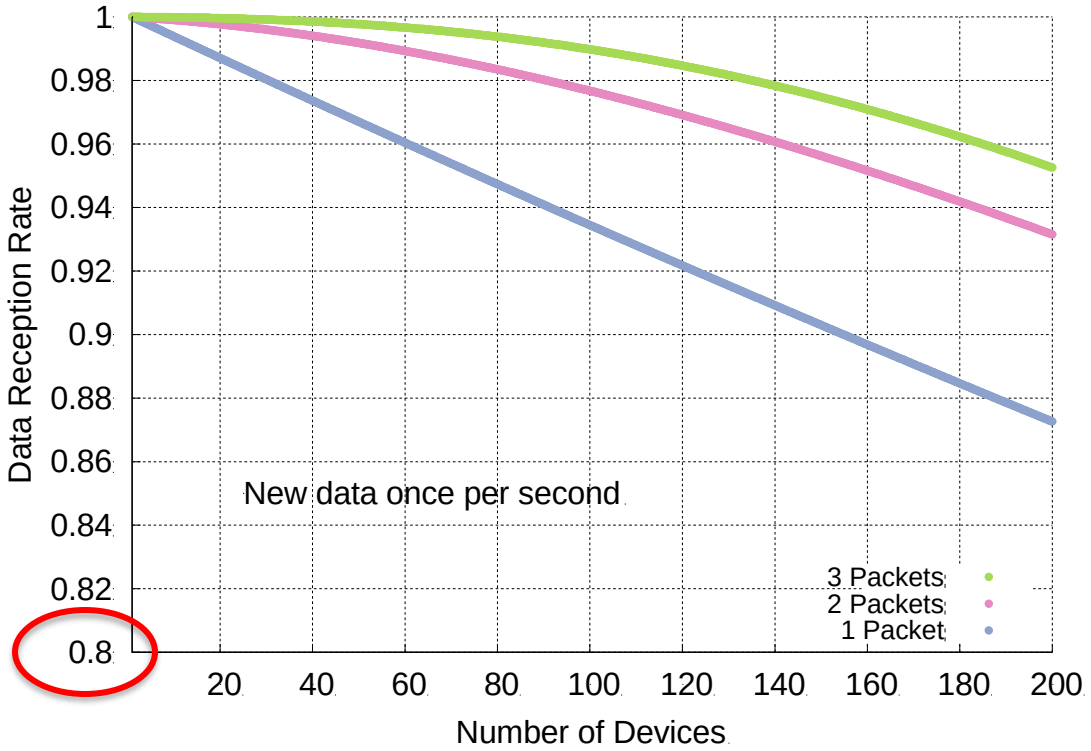
- Original questions
  - What are the odds that a transmitted advertisement will be received?
  - If M redundant advertisements are sent instead, what are the odds that at least one are received?
  - How do these odds vary with number of devices, advertising interval, and packet size?

- Additional questions
  - Can redundancy make advertisements reliable?
  - Is it better to transmit often for high redundancy or rarely for less congestion?

Redundancy results in high DRR even with many devices.

In this example, a sensor has new data once per second and sends it in 1-3 packets.

Even without redundancy, data reception rates never fall below 87% even with 200 devices in a deployment, assuming no interference.



Redundancy is (normally) better than less congestion.

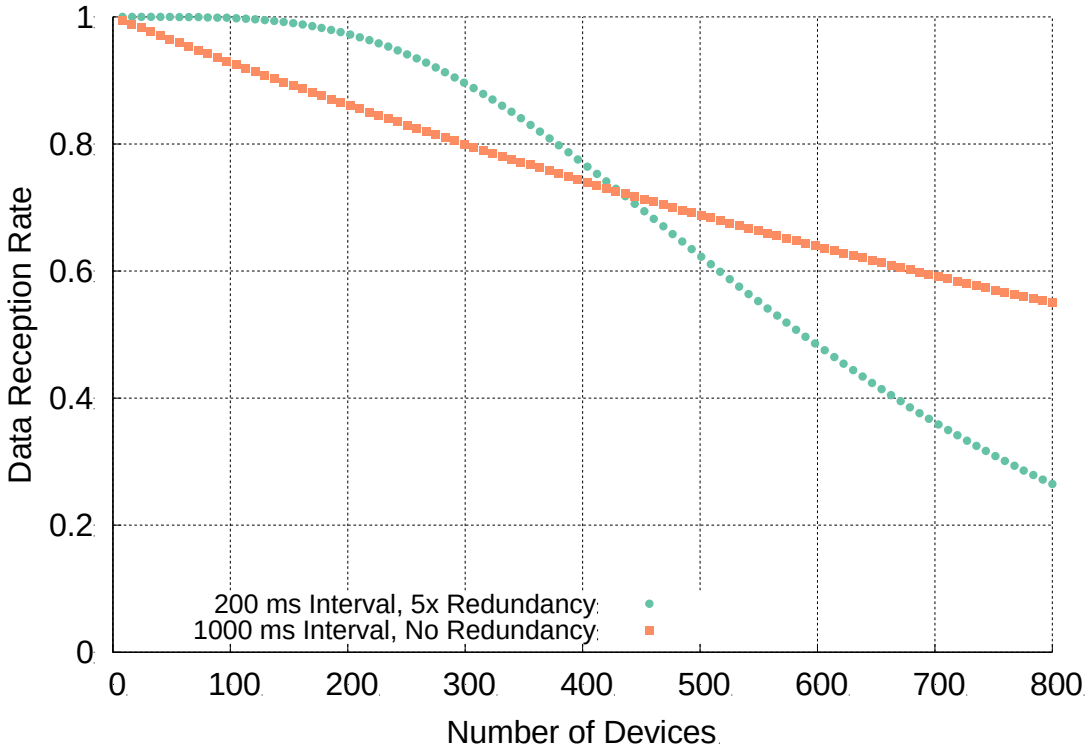
Design question:

- Send more packets to gain from redundancy?

  OR

- Send less packets to reduce congestion?

The answer changes, but only with many devices.



Outline

- BLE roles
  - Advertising
  - Scanning

- **Advertisement-based Networking?**
  - Advertisement Use Cases
  - Energy Use
  - Packet Collisions
  - **What about Scan Requests & Responses?**

Scan requests/responses seem intriguing

- Why not send most data in scan responses instead of advertisements?
  - Theoretically could reduce energy costs
- Can we use scan requests as a form of acknowledgement?
  - Could relieve need for redundant transmissions
- Problem: scan requests/responses don't work all that well

Scan Requests and Responses don't work for data use case

- Goal: provide a little extra advertisement data on demand

- Problem: exponential backoff for lost messages
  - If there is a request without a response, scanners assume collision with another scanner and exponentially back off from requesting
  - But collisions are far more likely between a device and a scanner, which should not have back off
  - Result is that scan requests will occur far less frequently than expected
  - Instead, better just send additional advertisements with different data

Kravets, Robin, Albert F. Harris III, and Roy Want. "Beacon trains: blazing a trail through dense BLE environments." *Proceedings of the Eleventh ACM Workshop on Challenged Networks*. 2016.

Next up: BLE Connections