Lecture 01
Introduction

CS397/497 – Wireless Protocols for IoT

Branden Ghena – Winter 2023

Materials in collaboration
with Pat Pannuto (UCSD)

Welcome to CS397/497!

- Goal: get a **feel** for wireless communication and protocols
  - How are they used?
  - Why are they different and in what ways?
  - Which applications are they most useful for?

- ~35 students (22 undergrad, 13 grad)
  - Lots of different backgrounds and interests

- This course is based on discussion and questions
  - Expect to attend classes, ask questions, and interact with others
  - You're hopefully here because you want to be and want to learn

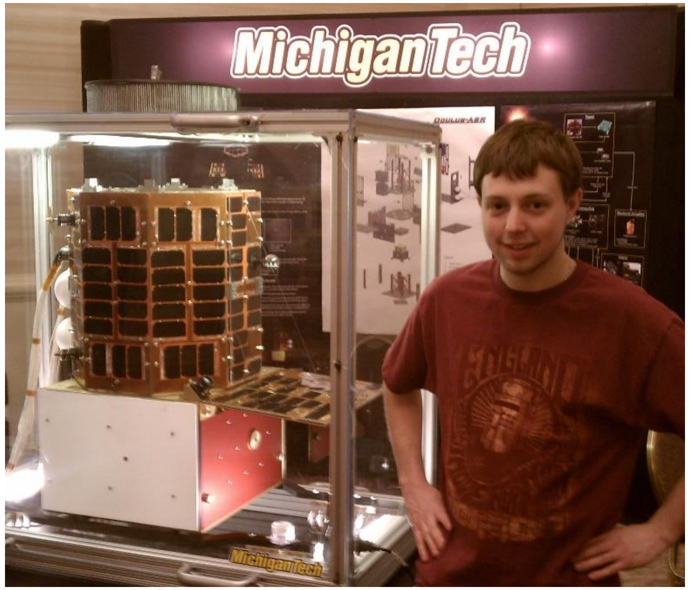
Branden Ghena (he/him)

- Assistant Faculty of Instruction
- Education
  - Undergrad: Michigan Tech
  - Master's: University of Michigan
  - PhD: University of California, Berkeley
- Research
  - Resource-constrained sensing systems
  - Low-energy wireless networks
  - Embedded operating systems
- Teaching
  - Computer Systems
    - CS211: Fundamentals of Programming II
    - CS213: Intro to Computer Systems
    - CS343: Operating Systems
    - CE346: Microprocessor System Design
    - CS397: Wireless Protocols for the IoT

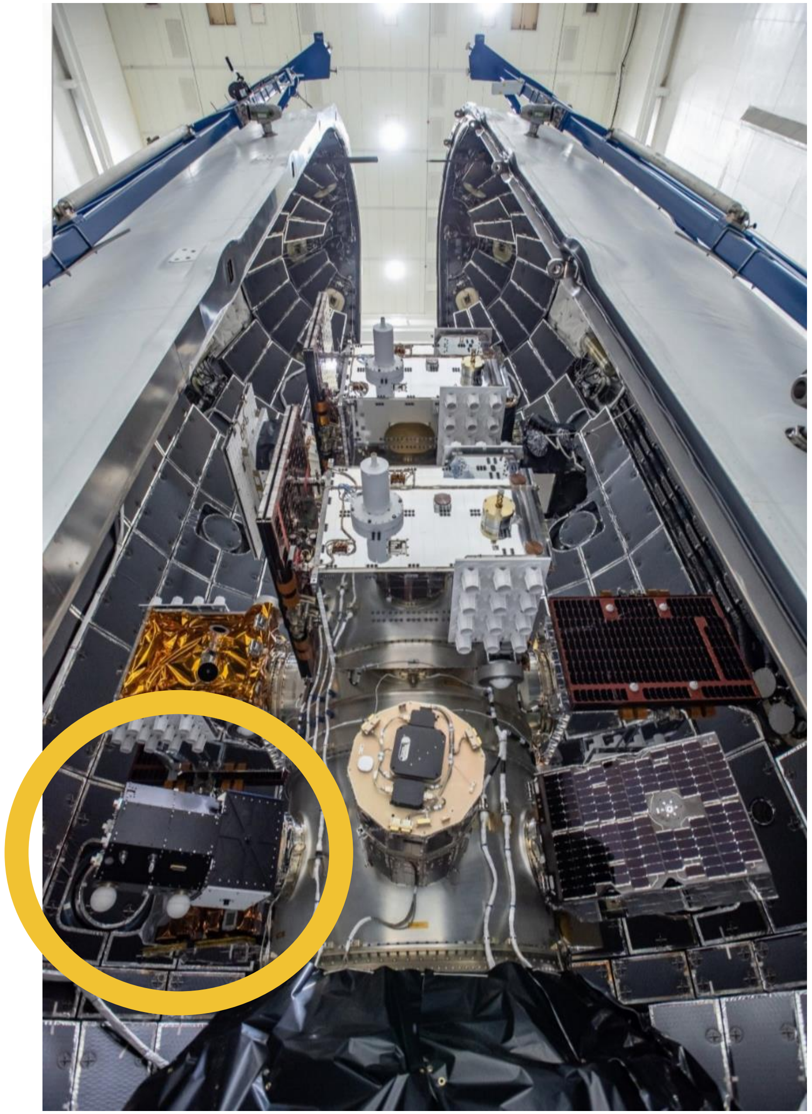
Things I love

Undergraduate: satellite radios and computers

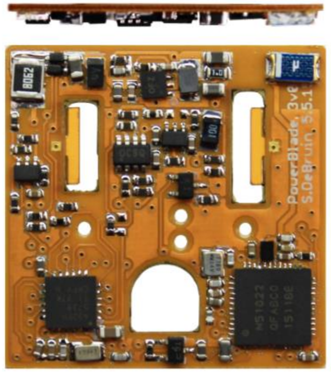
Oculus -Sat Uplink Command Budget:	NOTE:		Oculus -Sat Version: 2.4.1	Date Data Last Modified: 2011 October 12
Parameter:	*Value:*	*Units:*	*Comments:*	
Ground Station:				
Ground Station Transmitter Power Output:	50.0	watts	This value is transferred from "Transmitters" W/S, Cell [E15].	
In dBW:	17.0	dBW	Transmitter power expressed in dB above one watt	
In dBm:	47.0	dBm	Transmitter power expressed in dB above one milliwatt	
Ground Stn. Total Transmission Line Losses:	3.3	dB	This value is transferred from "Transmitters" W/S, Cell [I33]	
Antenna Gain:	16.3	dBi	This value is selected at "Antenna Gain" W/S, Cell [E11]	
Ground Station EIRP:	30.0	dBW	Ground Station Effective Isotropic Radiated Power (EIRP) [EIRP=Pt x Ltl x Ga]	
Uplink Path:				
Ground Station Antenna Pointing Loss:	0.3	dB	This value is calculated in the "Antenna Pointing Losses" W/S, and transferred f	
Gnd-to-S/C Antenna Polarization Losses:	3.0	dB	This value is calculated in the "Polarization Loss" W/S and is transferred from C	
Path Loss:	141.5	dB	Lp = 22 + 20LOG(D/l); Transferred from "Orbit & Frequency" W/S	
Atmospheric Losses:	1.1	dB	This value is transferred from "Atmos. & Ionos. Losses" W/S, Cell [D23]	
Ionospheric Losses:	0.7	dB	This value is transferred from "Atmos. & Ionos. Losses" W/S, Cell [D47:D50]	
Rain Losses:	0.0	dB	This value should be estimated by the link model operator and place into Cell [	
Isotropic Signal Level at Spacecraft:	-116.6	dBW	This is the signal level received in space in the vacinity of the spacecraft using	

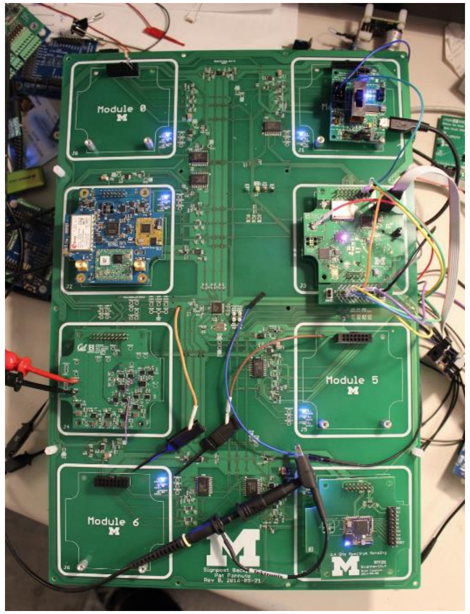


- How the heck are you supposed to learn this stuff?

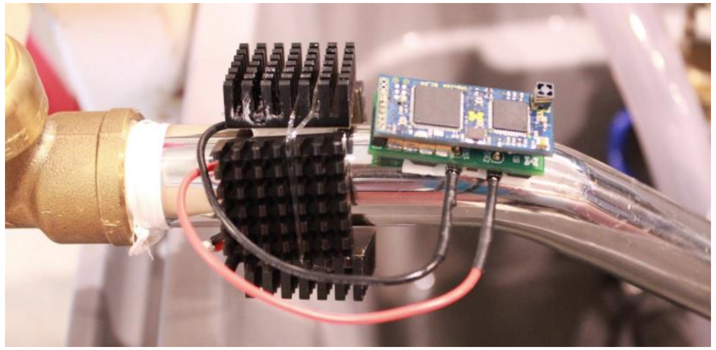


Grad school: resource-constrained embedded systems






- Most interesting to me: the interfaces
  - Hardware and software
  - Applications and OS
  - Communication
- Again: learn by doing
  - With significant assistance from my peers



Faculty: now I can choose what to teach!

- Goal: provide classes that teach more advanced embedded systems topics
  - Overlaps strongly with CS and ECE, but hopefully useful to other engineering and sciences domains too

- Result: this course!
  - Course goals: make students familiar with a number of different wireless protocols and their tradeoffs
    - Practical hands-on experience with as many networks as possible
    - Open-ended design for final, chance to delve deeply into materials

Today's Goals

- Introduction to the Internet of Things

- Overview of the course

- Introduction to wireless communication

Outline

- Who and Why
- **Internet of Things**
- Embedded Systems
- Course Overview
- Overview of wireless networks

Perspective of this course

- This class is about wireless protocols
    - For a specific domain: the Internet of Things

- So we'll spend some amount of time discussing the Internet of Things and embedded systems

Discussion: what is the Internet of Things?

1. Name a few Internet of Things devices

2. What are the qualities that designate those devices at “IoT”?

Discussion: what is the Internet of Things?

1. Name a few Internet of Things devices

2. What are the qualities that designate those devices at “IoT”?

Thought experiment on capabilities

- What if a smart speaker was battery powered and meant to be kept in your pocket?

- Would that still count as IoT?

Thought experiment on capabilities

- What if a smart speaker was battery powered and meant to be kept in your pocket?

- Would that still count as IoT?

    - Feels to me like a personal device rather than infrastructure
    - Something important about having many users

Thought experiment on capabilities

- What if the Nest thermostat was powered by an entire desktop?
  - 8-core x86-64 processor, 32 GB RAM, 1 TB SSD
- Would that still count as IoT?
- Why don’t we see that in practice?

Thought experiment on capabilities

- What if the Nest thermostat was powered by an entire desktop?
  - 8-core x86-64 processor, 32 GB RAM, 1 TB SSD

- Would that still count as IoT?

- Why don't we see that in practice?

Cost

Thought experiment on energy

- The origins of IoT are battery-powered sensing systems
  - And energy-harvesting devices

- Why do we put so much focus on systems with batteries?
  - Why do they need batteries?

Thought experiment on energy

- The origins of IoT are battery-powered sensing systems
  - And energy-harvesting devices

- Why do we put so much focus on systems with batteries?
  - Why do they need batteries?

Deployability

Largest IoT challenges: *power* and *communication*

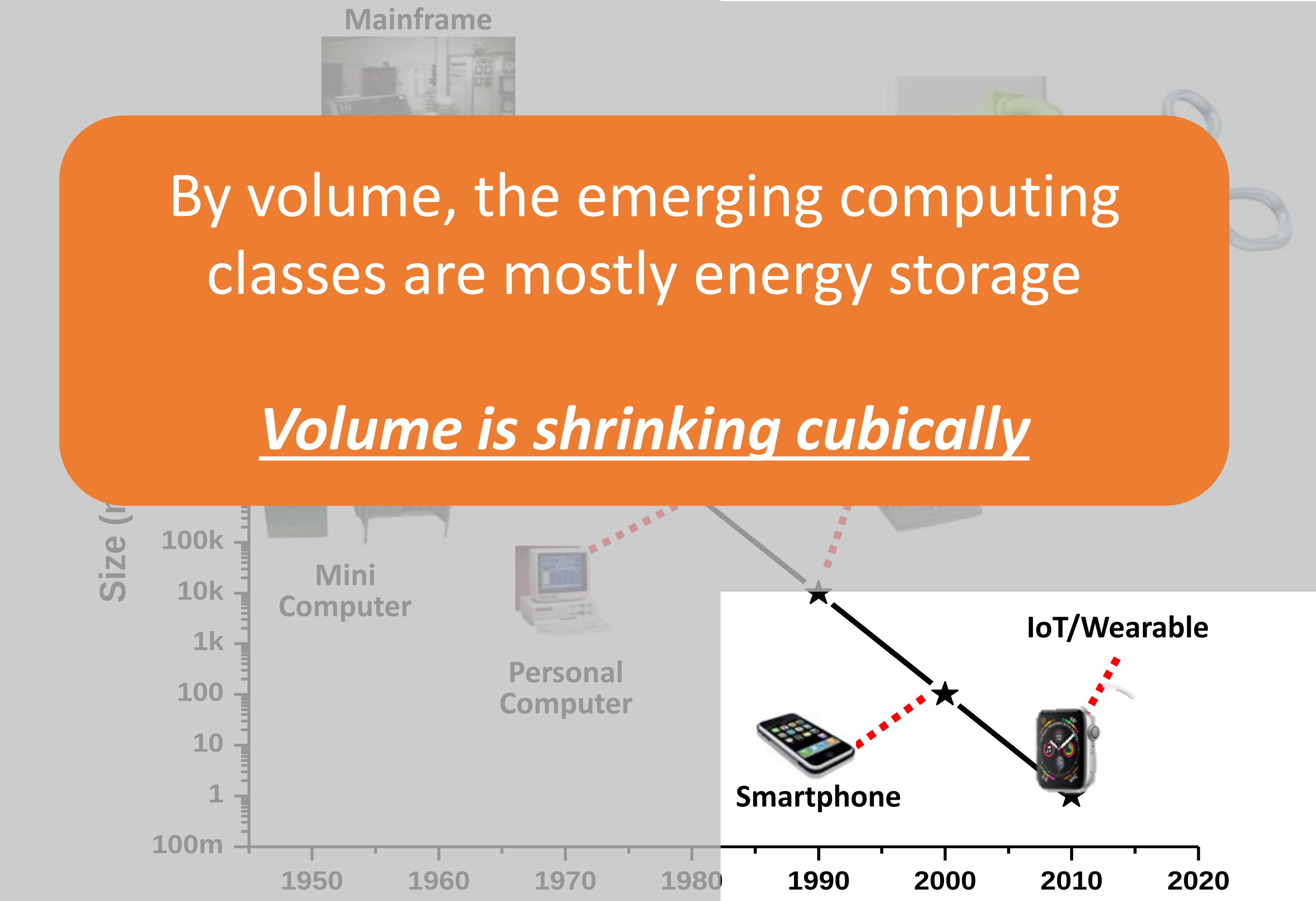
- This class is about wireless technologies
  - For resource-constrained systems, such as the IoT

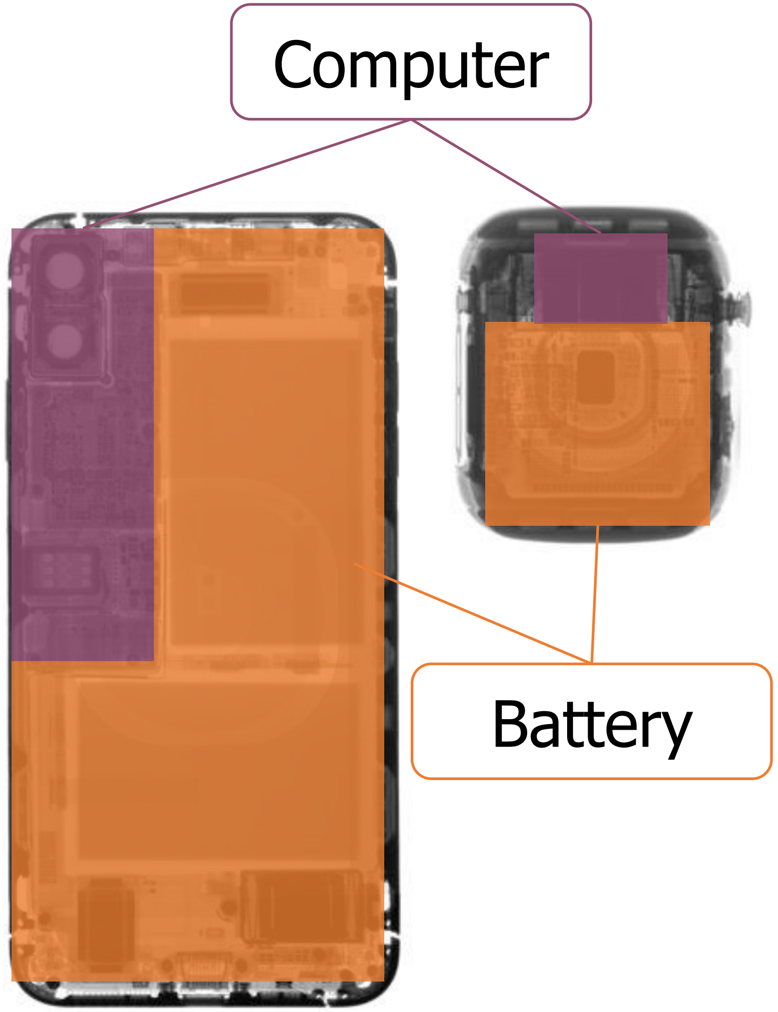
- We will focus on the tradeoffs between technologies
  - How they balance differing constraints
    - Power, spectrum, complexity, etc.
  - And the technical foundations of these designs and differences

Energy is *the* defining constraint of emerging technologies

By volume, the emerging computing classes are mostly energy storage

Volume is shrinking cubically





Branden's take on the Internet of Things

- Key features
  - Computation
    - Local to the device
    - With some capability for arbitrary compute and storage
  - Connectivity
    - Almost certainly wireless
    - Likely Internet, possibly local
  - Interaction
    - Sensing or Actuation
- Secondary features
  - Low energy
  - (Relatively) Low cost

Pat Pannuto’s take on the Internet of Things

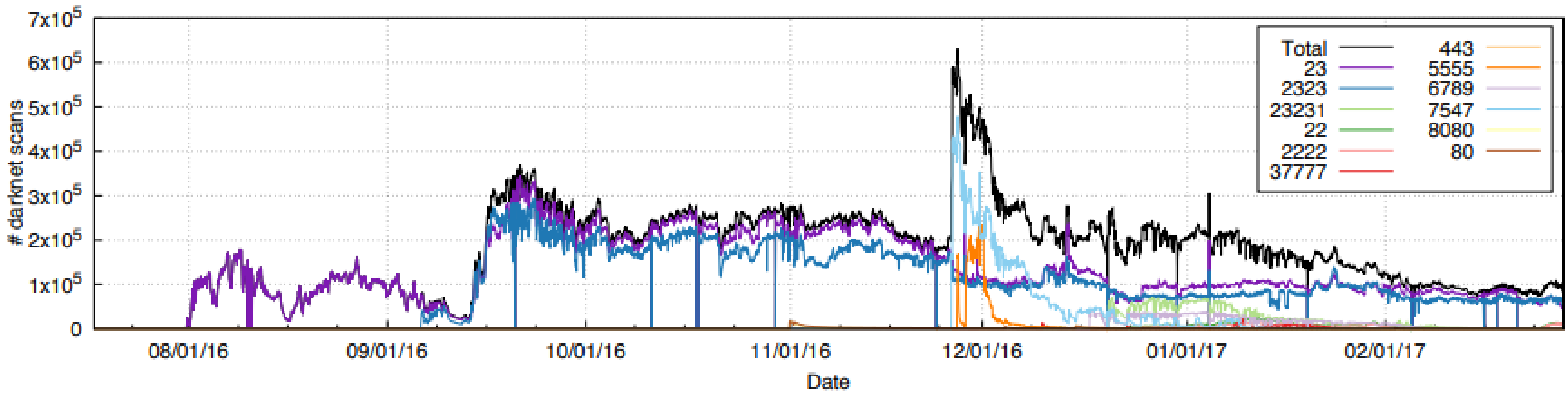
- His early grad school essays described the “last inch” problem
  - Now he often says “expanding the reach of digital world”
- For him, it is about ‘networked’ ‘things’
  - Which implicitly adds some computational capacity
    - [Though not always? Backscatter sensors break this definition…]

Assistant Professor, UC San Diego
https://patpannuto.com/

He teaches a version of this course there, and we share materials back-and-forth!

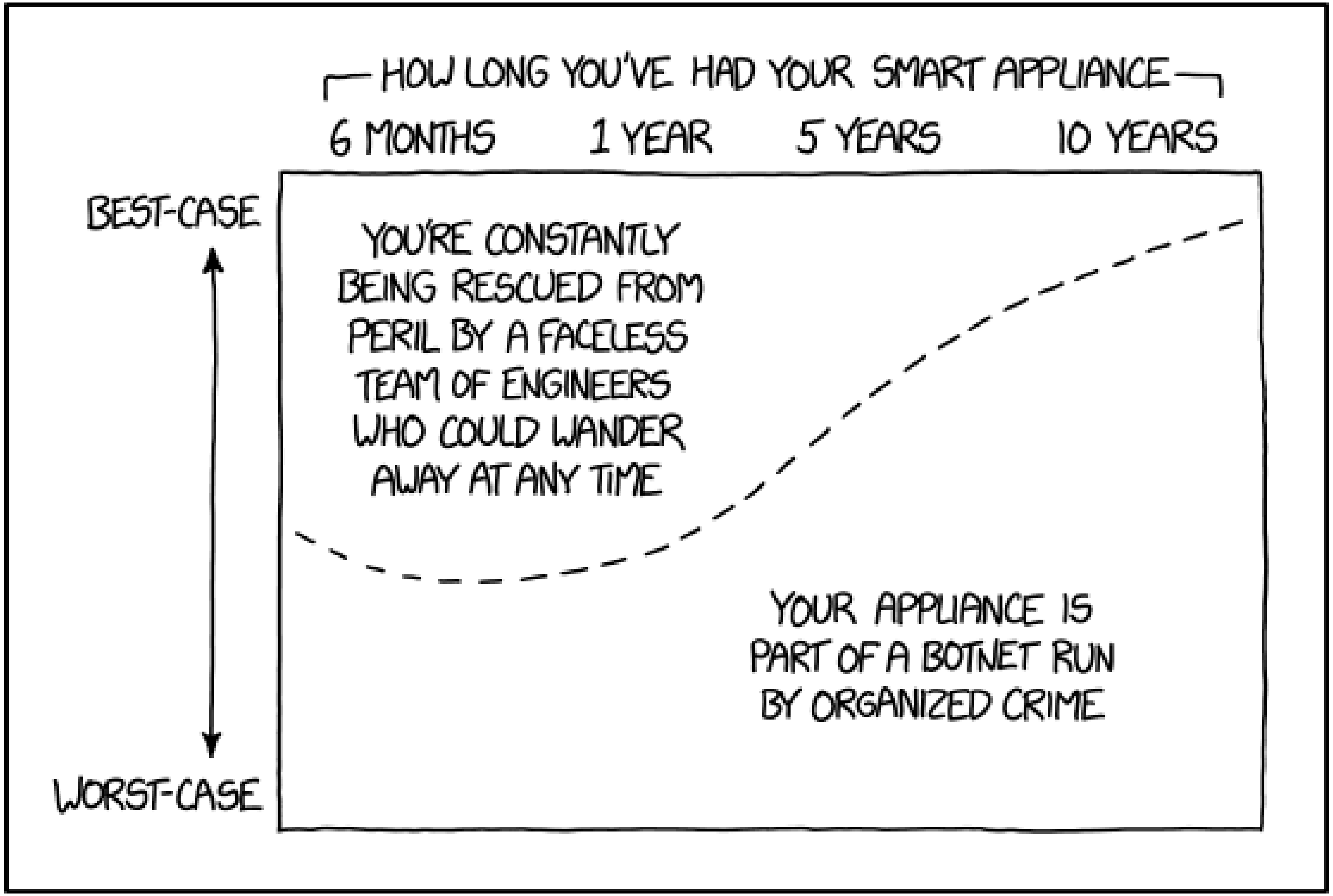
Warning: Internet of Crap

Internet of Insecure Crap



- Mirai botnet (2016)
- Takes control of up to 600,000 insecure connected devices
  - IP-attached cameras, DVRs, routers, printers
- Used to DoS websites

Break + xkcd



https://xkcd.com/1966/

Outline

- Who and Why
- Internet of Things
- **Embedded Systems**
- Course Overview
- Overview of wireless networks

What are embedded systems

- Embedded systems are devices containing computers that are used as a **device** rather than as a **computer**
  - Computers are **embedded** into the device

- Internet of Things devices are embedded devices

- But there are embedded systems that are not IoT
  - Smart vehicles and Robotics
  - Personal devices (embedded systems inside laptops/smartphones)

- Example: USB-C power brick has more compute than Apollo 11 did

https://forrestheller.com/Apollo-11-Computer-vs-USB-C-chargers.html

Microcontrollers drive most embedded systems

- Microcontroller: entire computer in a single chip
  - Processor
  - Working memory: SRAM (like RAM)
  - Nonvolatile memory: Flash (like SSD)
  - Peripherals
    - I/O pins
    - Analog Inputs and Outputs
    - Timers
    - Wireless radios
    - Cryptography accelerators
    - Buses
      - UART
      - I2C
      - SPI
      - USB
  - Power management

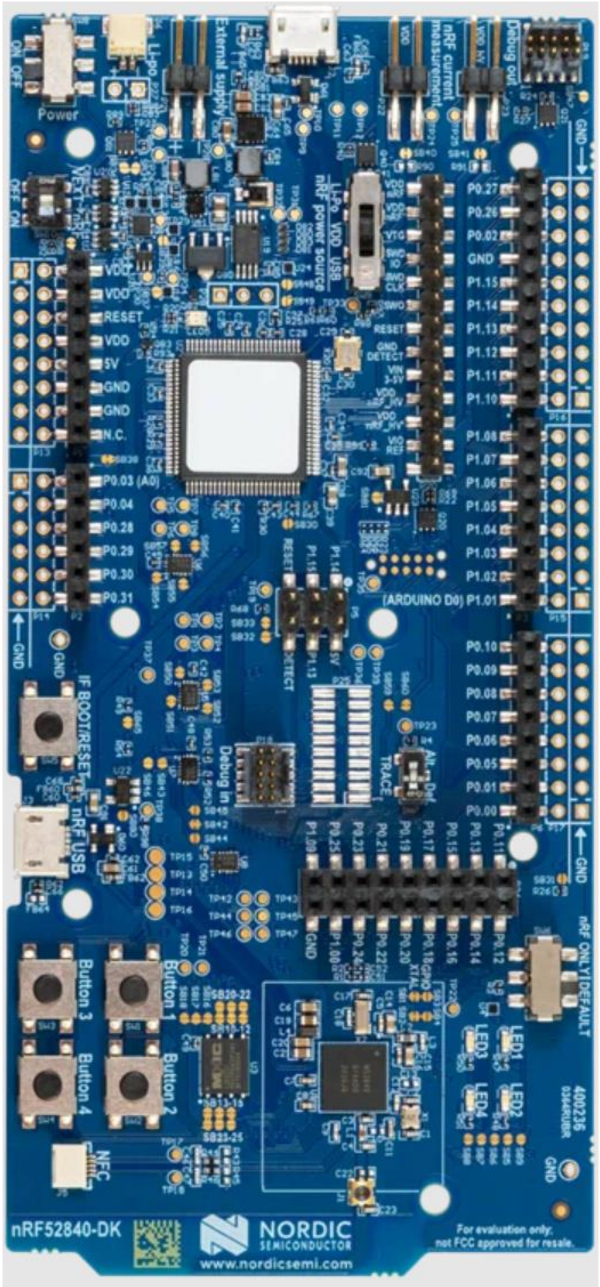
How is a microcontroller different?

- A very constrained computer
  - Simple processor
    - 16 or 32 bits (usually 32-bit these days)
    - Processor speed in MHz
    - Single core, pipelined processor
    - No cache, or maybe a very small instruction cache
  - Memory measured in kB
    - Code executes right from read-only Flash (which is part of the address space)
  - Often no OS support
    - “bare-metal” programming

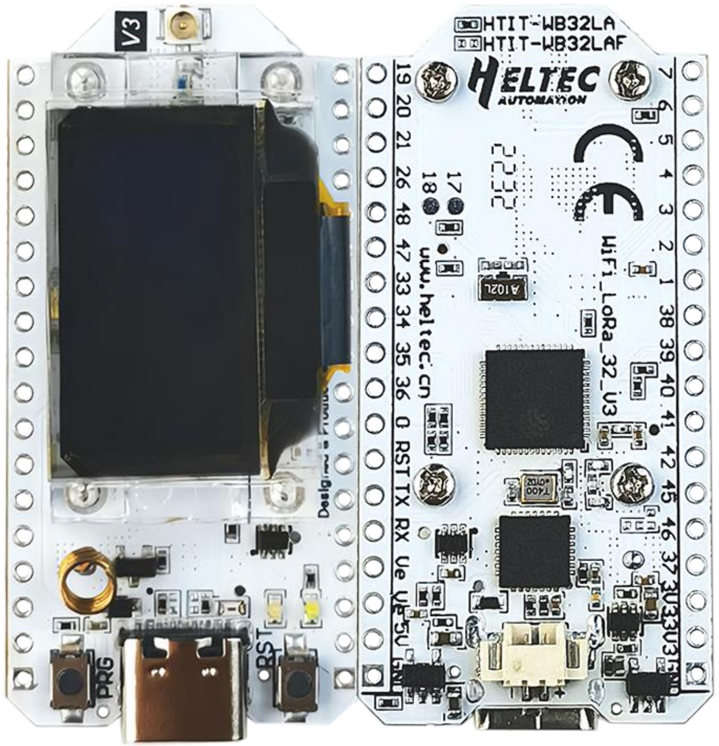
Nordic nRF52840DK - BLE & Thread

- nRF52840 microcontroller dev kit
  - Microcontroller is the bottom chip
  - Everything else is just to program it, measure power, and connect to external things

- nRF52840
  - 64 MHz, 32-bit ARM Cortex-M4F
  - 1 MB Flash, 256 KB RAM
  - A bunch of peripherals
  - Bluetooth Low Energy and 802.15.4 communication



Heltec WiFi LoRa 32 v3 - WiFi & LoRa



- ESP32 microcontroller
  - 240 MHz, 32-bit custom architecture
  - 384 kB Flash, 512 kB RAM
  - A bunch of peripherals
  - WiFi and Bluetooth Low Energy communication
- SX1262
  - LoRa transceiver (connected over SPI)
- OLED display

Embedded systems are programmed in C

- C++ also used
  - Occasionally assembly
  - Rarely other things (Rust, Lua, Python)

- But even the few things C gives you aren't necessarily available
  - Heap space possibly nonexistent
    - You have to choose some space in RAM to save as a heap
    - And then include the algorithm for allocating that memory

  - Printf may be nonexistent too
    - There's no STDIN/STDOUT/STDERR because there is no shell
    - Might be able to do serial output though

How do I load code onto microcontrollers?

- JTAG (Joint Test Action Group)
  - Hardware built into the microcontroller for testing purposes
  - Can arbitrarily read/write memory
  - Can single step process too, at runtime!
    - GDB can connect to it! (sort of)
  - RTT (Real Time Transfer) makes printf work over JTAG

- Serial bootloaders
  - Software runs on the microcontroller at boot that waits a short time for someone to contact it and upload code
  - Convenient, but sometimes flaky

Embedded software

- There are a multitude of embedded software systems
  - Every microcontroller vendor has their own
  - Popular platforms like Arduino

- Embedded OSes
  - Contiki, Riot, Zephyr, Mynewt, FreeRTOS, Tock

- nRF52840DK has support across all of these
- WiFi LoRa 32 v3 should work with some
  - Best support likely in Arduino

Outline

- Who and Why
- Internet of Things
- Embedded Systems
- **Course Overview**
- Overview of wireless networks

Asking questions

- Class and office hours are always an option!
  - Office hours by demand. I promise to meet!!
- Piazza: (similar to Campuswire)
  - Post questions
  - Answer each other’s questions
  - Find lab partners
  - Information from the course staff
  - Post private info just to course staff
- Please do not email me! Post to Piazza instead!
  - I’ll be updating roster again a few times

Grading

- 50% Lab projects - hands-on semi-guided activities
  - Likely 5 of these, divided equally
  - Small groups of three students
- 25% Homeworks - pencil-on-paper practice
  - Likely 4 of these, with the last worth double
  - Individual work
- 25% Final design project - paper writeup
  - One of these due during exam week
  - Individual work

Labs

- Practice interacting with and considering networks

- Should all include real hardware and real wireless communication
  - Wireshark
  - Bluetooth
  - Thread
  - WiFi
  - LoRaWAN

- Note: WiFi/LoRa hardware shipping from China now, we'll see how that goes and adjust if needed

Homeworks

- Analysis, designing, calculating
  - Background
  - BLE packets
  - Mesh
  - Cellular (worth double)

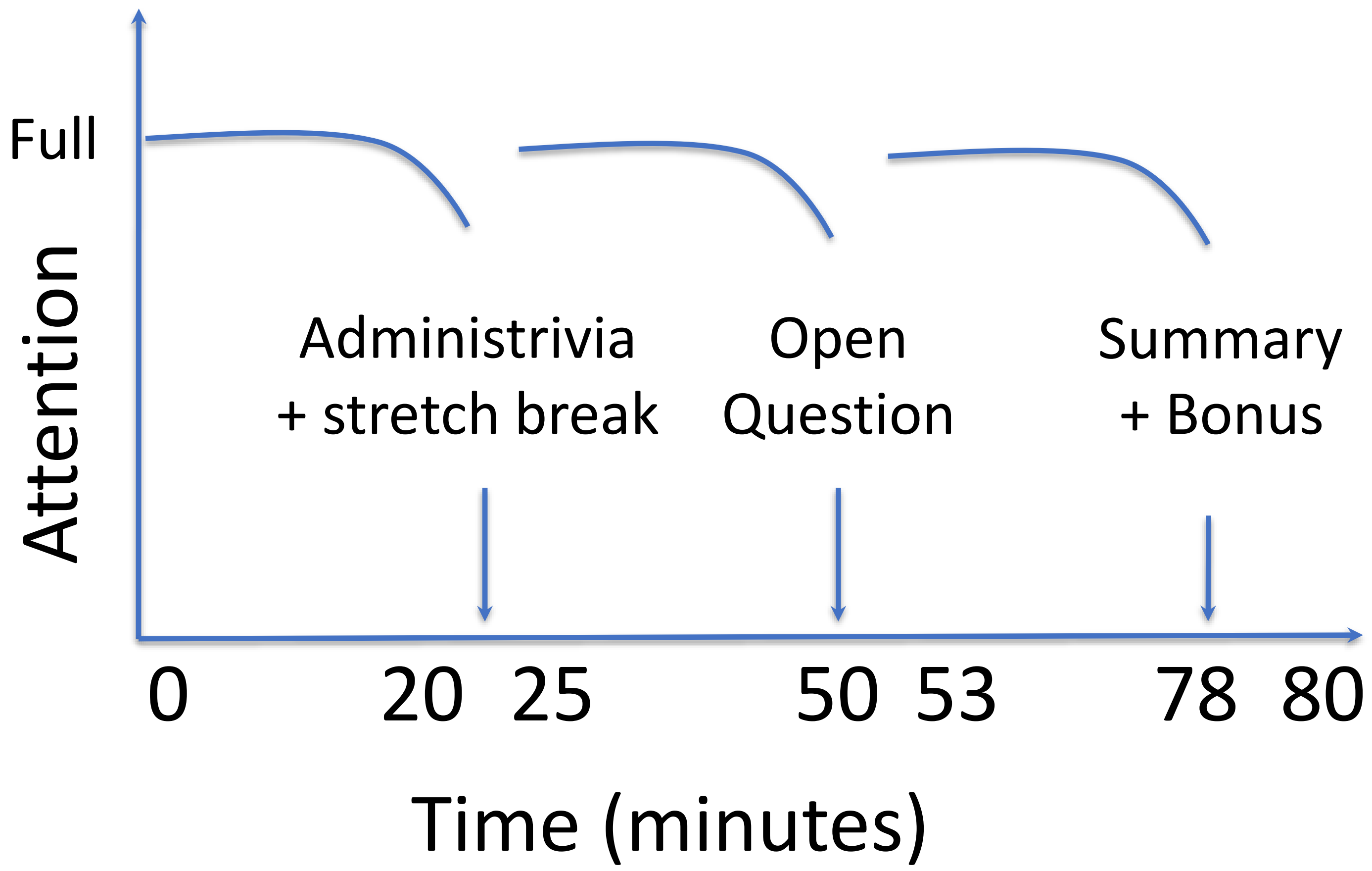
Final design project

- Design a communication plan for an application of your choice
- Explain application and determine what its constraints are
  - Cost, power, scale, data, reliability
- Actually think through how it will work, citing real-world capabilities
  - Research and cite data you find
  - Explain and consider tradeoffs
- This is the “final project” for the course
  - Design rather than real hardware

On upper-level, special-topics courses

- Something this class does **not** include is exams or quizzes
- The point is to be here because you’re actually interested in the material
  - So show up to lecture because it’s interesting to you and so you can discuss with your classmates
  - But the class itself isn’t going to force you to learn anything
- You can help guide the course
  - It’s okay to derail lecture (sometimes) with interesting tangents
  - I’m happy to add material on other topics if you ask

Break + Architecture of a lecture



Outline

- Who and Why
- Internet of Things
- Embedded Systems
- Course Overview
- **Overview of wireless networks**

Bluetooth Low Energy (BLE)

- Bluetooth Classic was good for enabling device to device communication
  - But not particularly fast or low energy
- Bluetooth Low Energy was developed to improve this
  - Focuses on low-energy interactions
  - Much lower throughput that Bluetooth
- Supported by hardware devices already in smartphones
  - Humans can interact directly with nearby devices!!

802.15.4 & Thread

- 802.15.4 is a low-energy physical layer
  - Radio chips have been widely available for 15-20 years

- *Significant* amounts of sensor network research have focused on building layers on top of 802.15.4
  - Access control layers
  - Network layers

- Thread is a selection of these possibilities to make a network
  - Uses IPv6 networking!!

WiFi (802.11)

- Ubiquitous wireless communication
  - High energy requirements for high throughput communication

- Now accessible through relatively low power radios
  - ESP32 is dominant here
  - Still significantly more effort than BLE or Thread

- IoT devices can use the same WiFi that’s already available
  - No need for additional infrastructure!!

LPWANs (Low-Power Wide-Area Networks)

- How do we collect data from city-scale deployments?
  - There's an unmet need for long-range, but low-throughput networks
  - Existing cellular technologies focus on human requirements

- Still a brand new space (relatively)
  - Unlicensed-band technologies in last 5 years: Sigfox and LoRaWAN
  - Cellular technologies in last 2 years: LTE-M and NB-IoT

- Focus on long-range, low-energy, low-throughput
  - One gateway can cover an entire city!!

Extra topics

- Matter
  - Interoperability standard for the Internet of Things
  - First public spec released in October 2022
- Backscatter
  - Insanely low-energy communication
  - Enables energy-harvesting indoor devices
- Localization
  - How do we find all this stuff?
  - And how do devices determine where they are relative to each other?
- Other topics are possible if desired! (seriously!)
  - Reach out and tell me what you want to learn about

Why use wireless?

- There are no wires!

- No need to install and maintain wires
  - Reduces cost
  - Simplifies deployment – place devices wherever makes sense

- Supports mobile users
  - Move around office, campus, city
  - Move devices around home

What is hard about wireless?

- There are no wires!

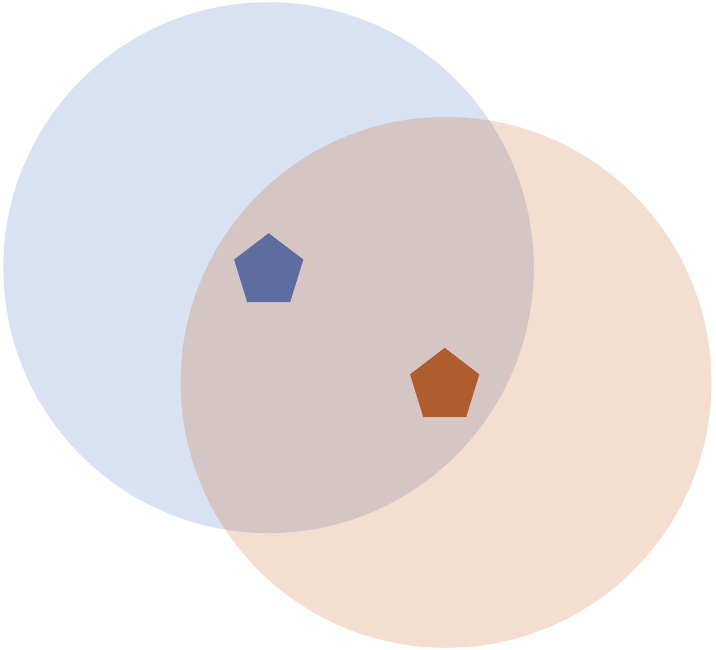
- Wired networks are constant, reliable, and physically isolated
  - Ethernet has the same throughput minute-to-minute
  - Bits sent through Ethernet or USB are (usually) received

- Wireless networks are variable, error-prone, and shared
  - WiFi throughput changes based on location and walls
  - Signals from nearby devices interfere with your signals
  - Individual bits might flip or never be heard at all

Wireless is a shared medium

- Wired communication has signals confined to a conductor
  - Copper or fiber
  - Guides energy to destination
  - Protects signal from interference

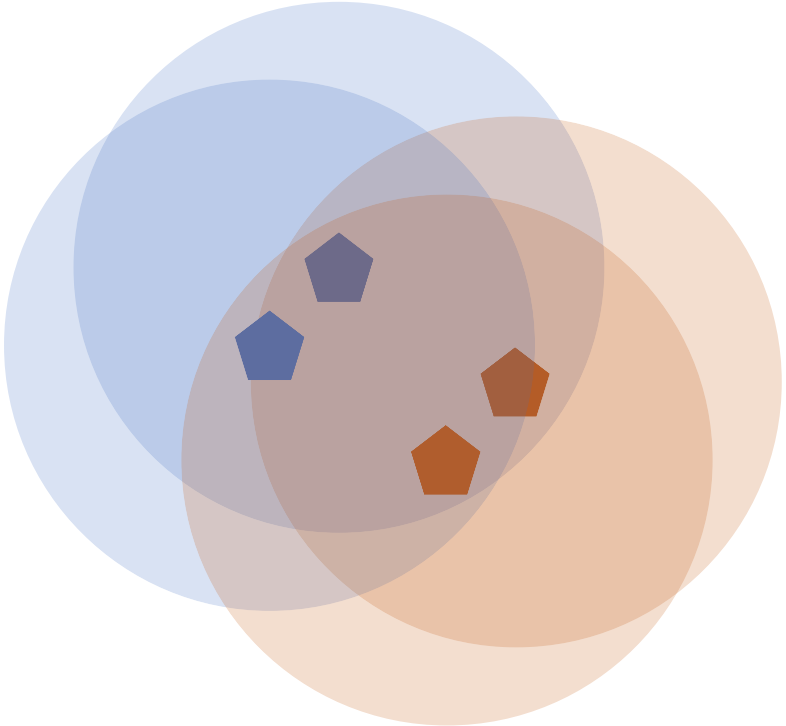
- Wireless communication is inherently broadcast
  - Energy is distributed in space
  - Signals must compete with other signals in same frequency band



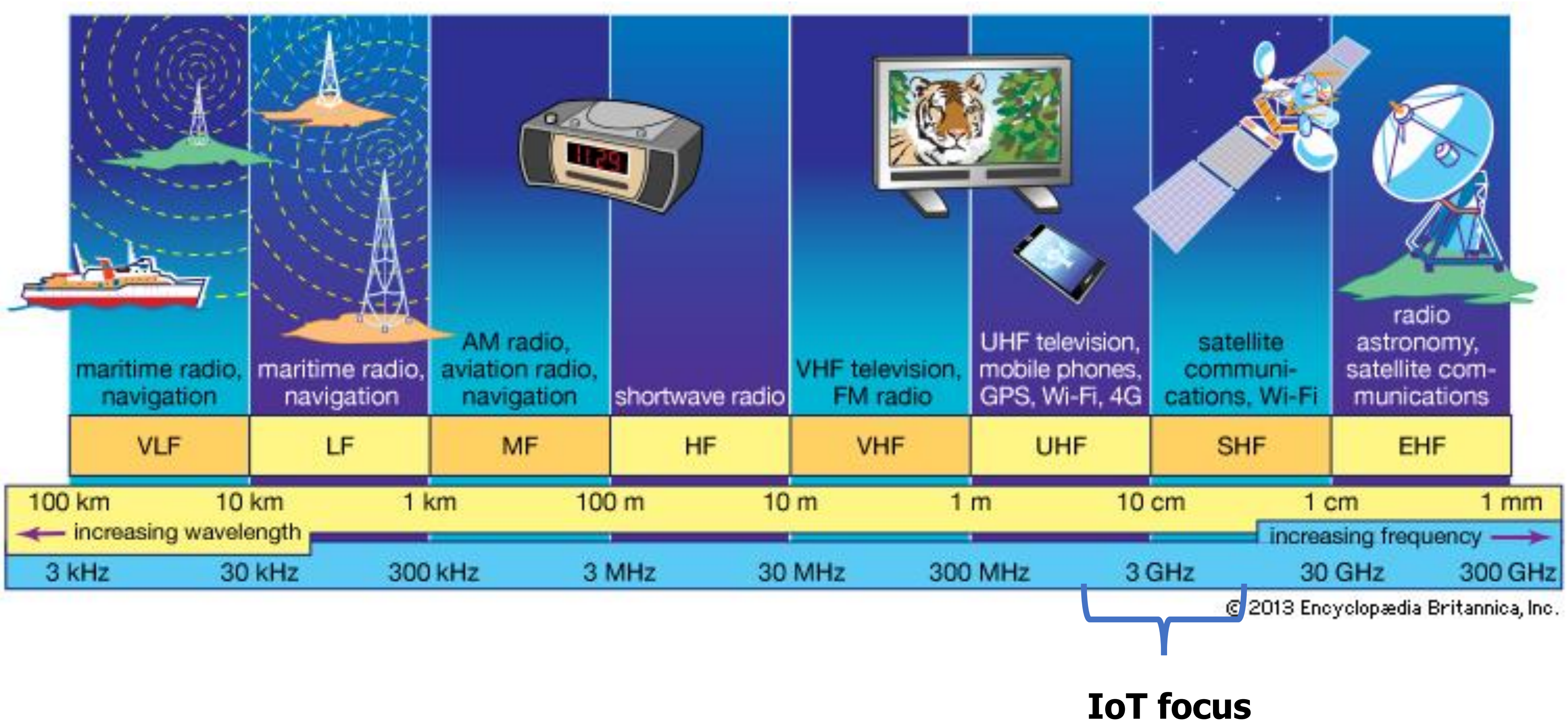
Increasing network capacity is challenging

- Wired networks just add more wires
  - Buses are many signals in parallel to send more data

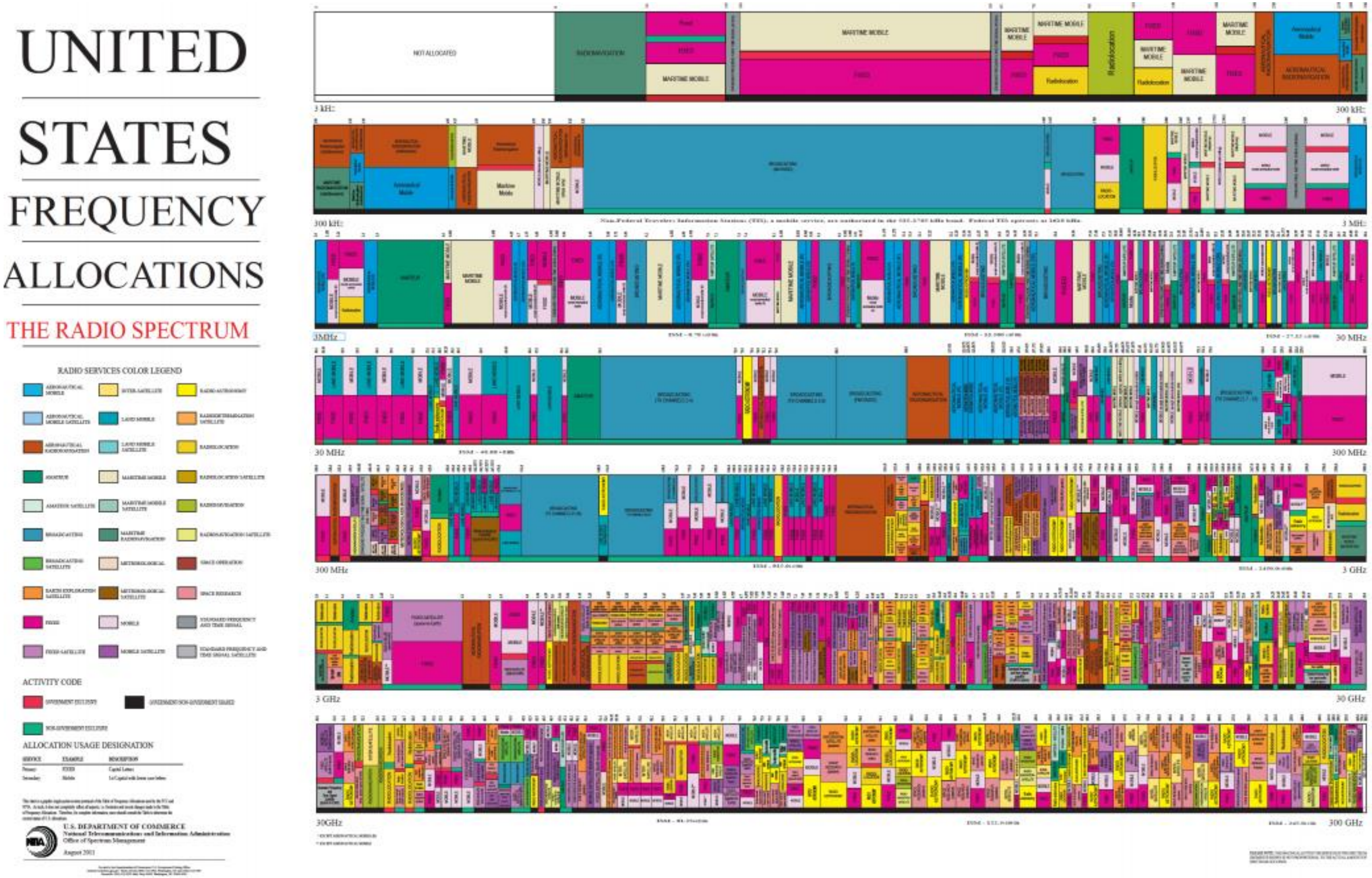
- Wireless networks are harder
  - Adding more links just increases interference
  - Need to expand to different frequencies



RF communication

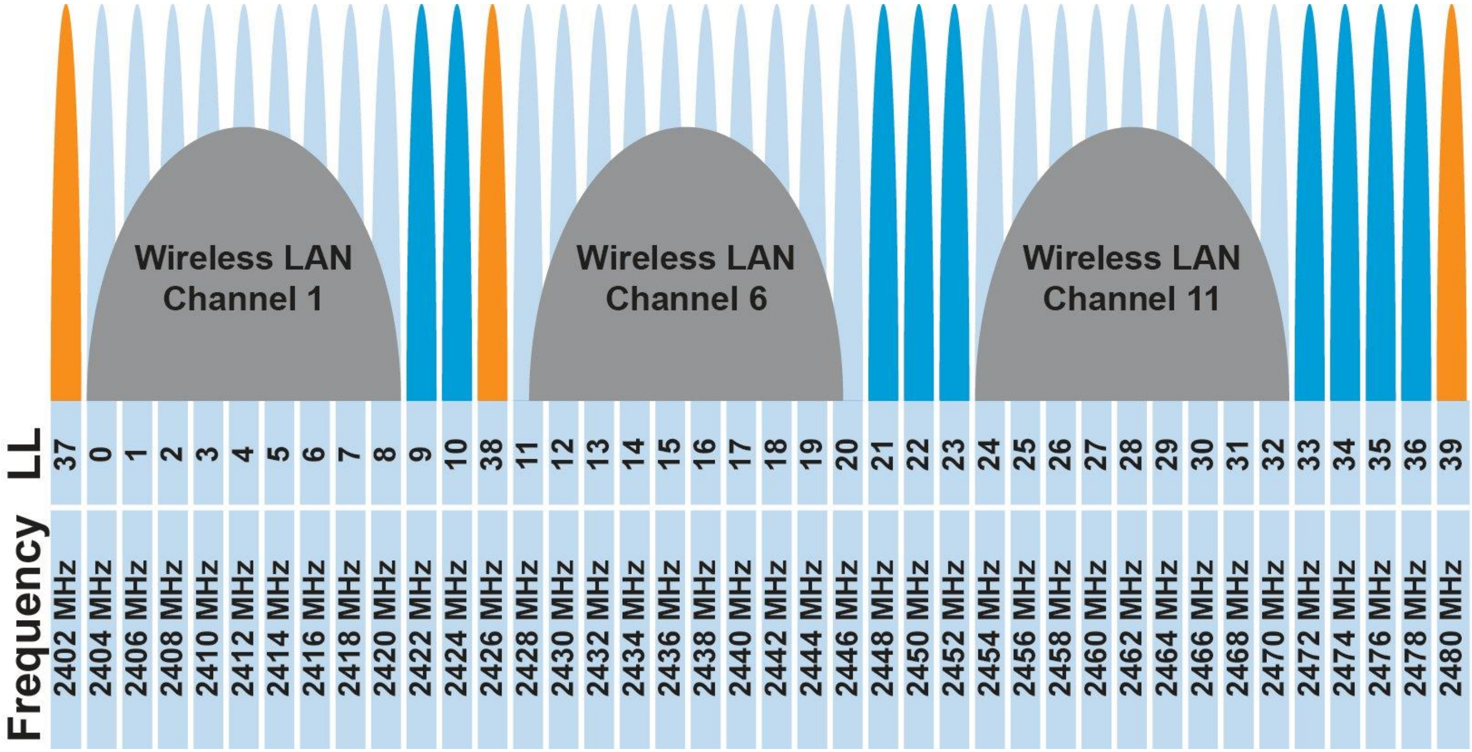


Wireless spectrum is allocated to specific uses



Unlicensed bands are where IoT thrives

- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi
- Cellular uses licensed bands

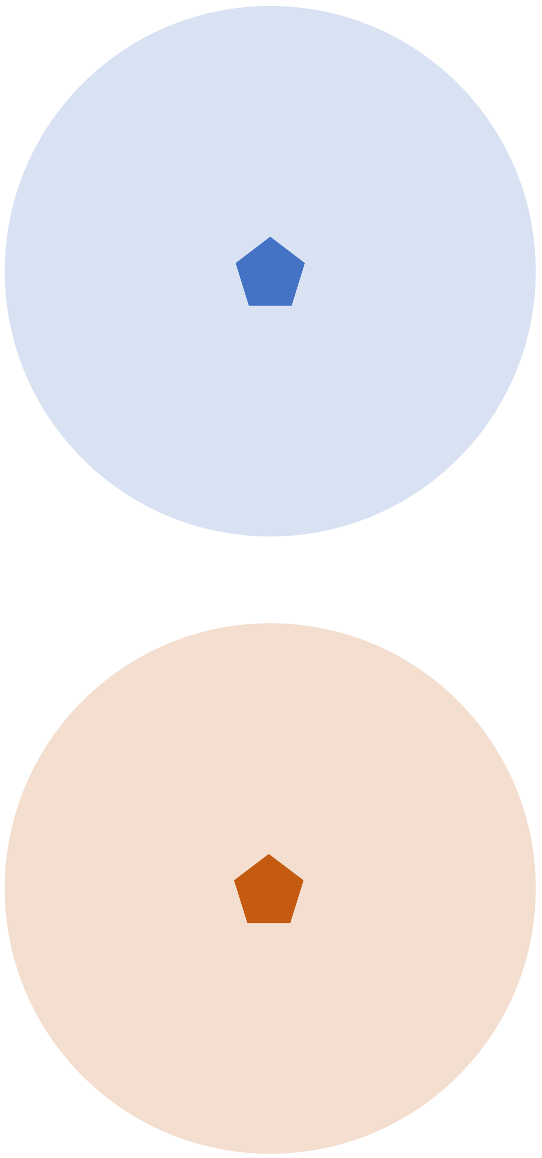


Model of RF communication

- Energy that radiates spherically from an antenna

- Attenuation with distance
  - Density of energy reduces over time, distance
  - Signal strength reduced, errors go up

- Two key features
  - Error rates depend on distance
  - Spatial reuse of frequencies



Outline

- Who and Why
- Internet of Things
- Embedded Systems
- Course Overview
- Overview of wireless networks