Lecture 14
Unlicensed LPWANs

CS433 – Wireless Protocols for IoT

Branden Ghena – Spring 2025

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

Administrivia

- WiFi Lab due today
- Lab: LoRa on Friday

- Cellular Homework due next week Thursday
  - Last homework
  - Counts as double points
  - About half of you have made a reservation already
    - No duplicates, No MVNOs

- Final Project out now

- Only other graded item: Quiz3 on Tuesday, June 3rd

Today’s Goals

- Overview of unlicensed-band LPWAN approaches
  - LoRaWAN
  - Sigfox
  - 802.11ah
  - TV Whitespaces

Resources

- LoRaWAN
  - LoRaWAN Specification version 1.1
  - LoRaWAN Regional Parameters version 1.0.2

- Sigfox
  - Sigfox Technical Overview
  - IETF Descriptions
    - https://www.ietf.org/proceedings/97/slides/slides-97-lpwan-25-sigfox-system-description-00.pdf
    - https://tools.ietf.org/html/draft-zuniga-lpwan-sigfox-system-description-04

Outline

- **Wide-Area Network Background**

- Unlicensed LPWANs
  - LoRaWAN
  - Sigfox
  - 802.11ah
  - TV Whitespaces

Wide area networks

- Communication at the region/city scale rather than the building/residence scale
  - Throughout cities
  - Agricultural deployments
  - Industrial facilities

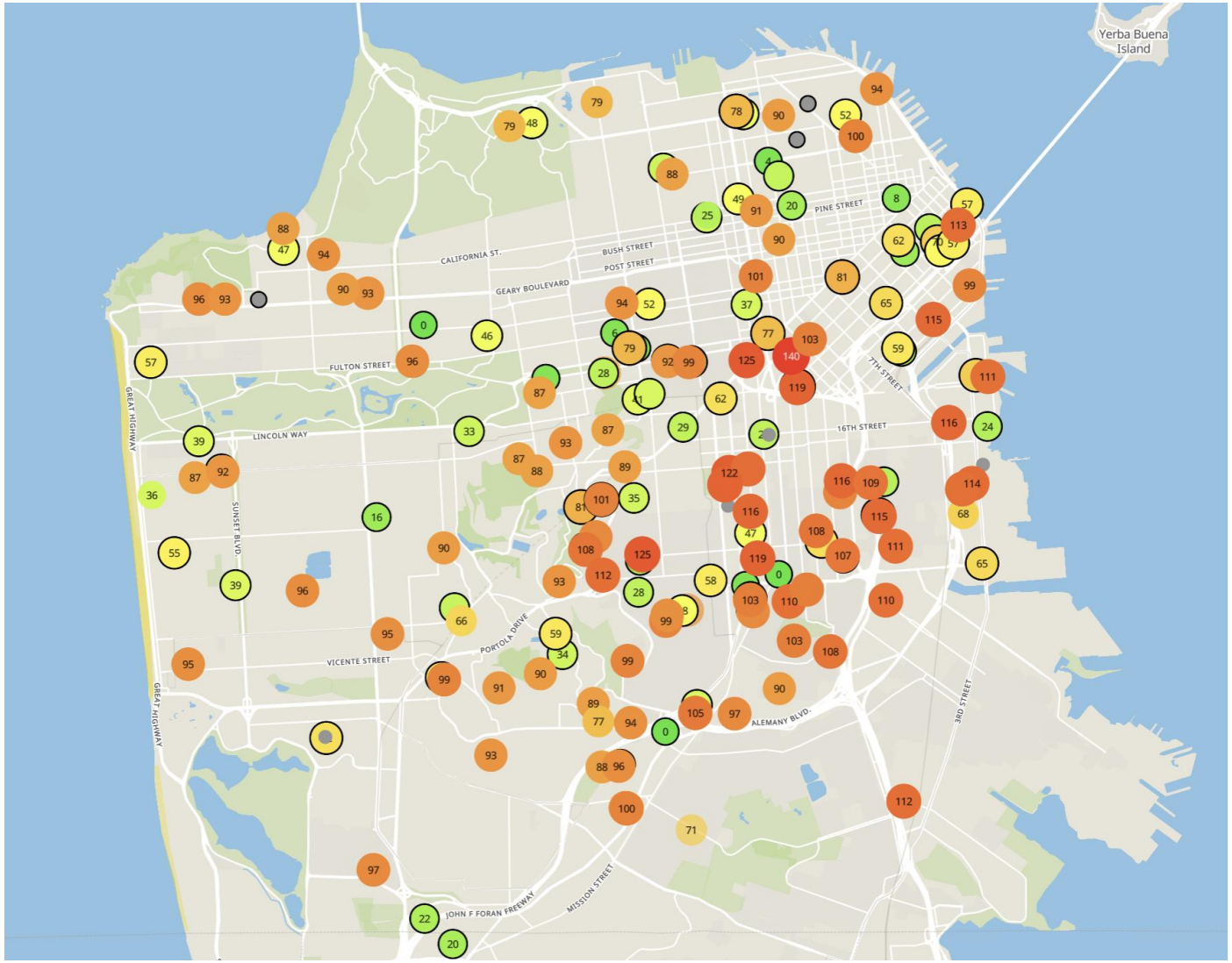
- City-scale sensing is one very popular domain
  - What might we want to sense throughout a city?

Example application: air quality monitoring

[1]

[2]

[2]



[1] Cheng et al. AirCloud: a cloud-based air-quality monitoring system for everyone. 2014.

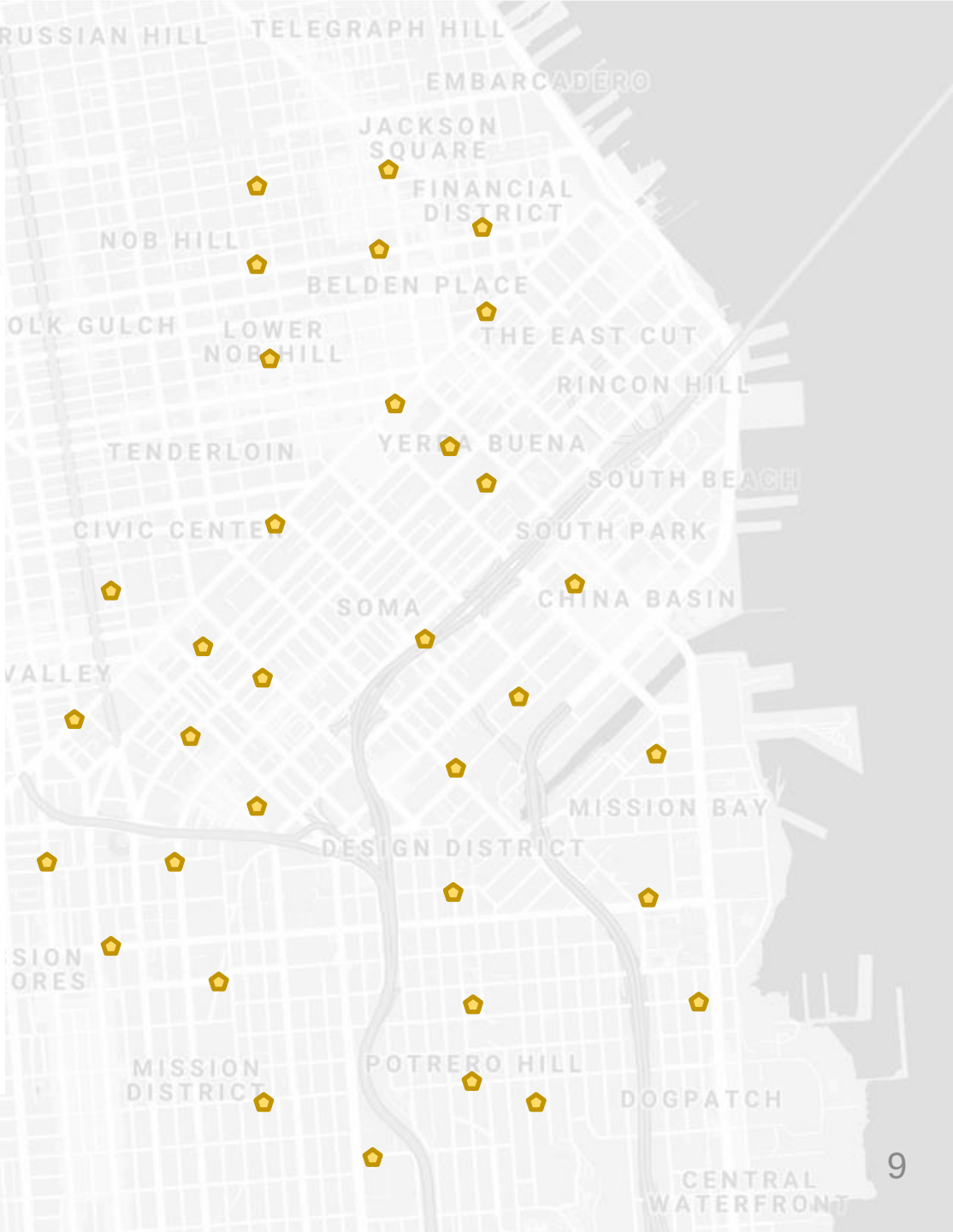
[2] Purple Air. 2019.

How do we collect data from a sensor?

- Manually collect measurements
- Connect it to WiFi (or Ethernet)
- Pay for cellular access

How do we collect data from MANY sensors?

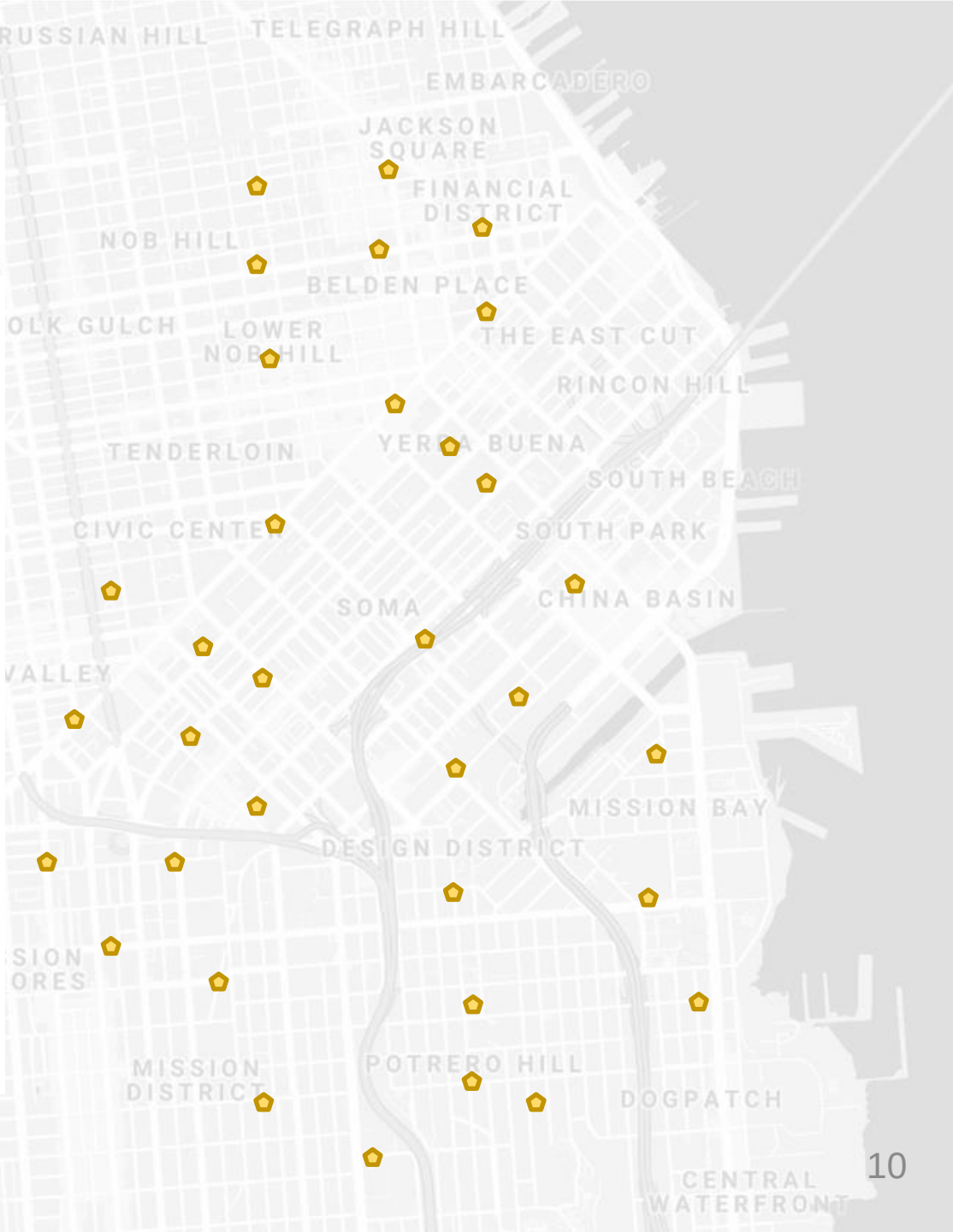
- Manually collect measurements
  - Too much work
- Connect it to WiFi (or Ethernet)
  - Too many separate networks
- Pay for cellular access
  - Too expensive for many devices



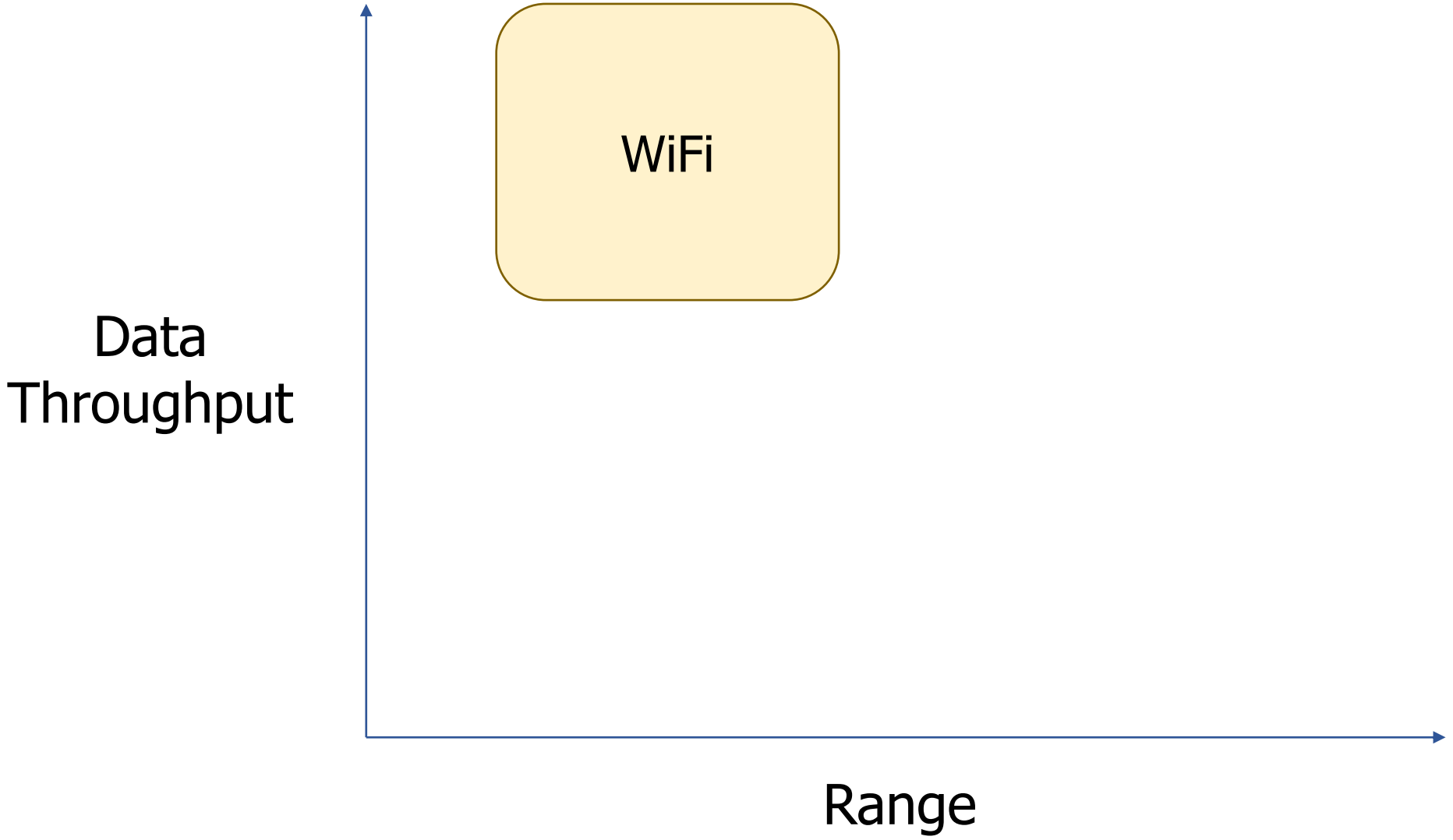
We need another network option

Requirements:

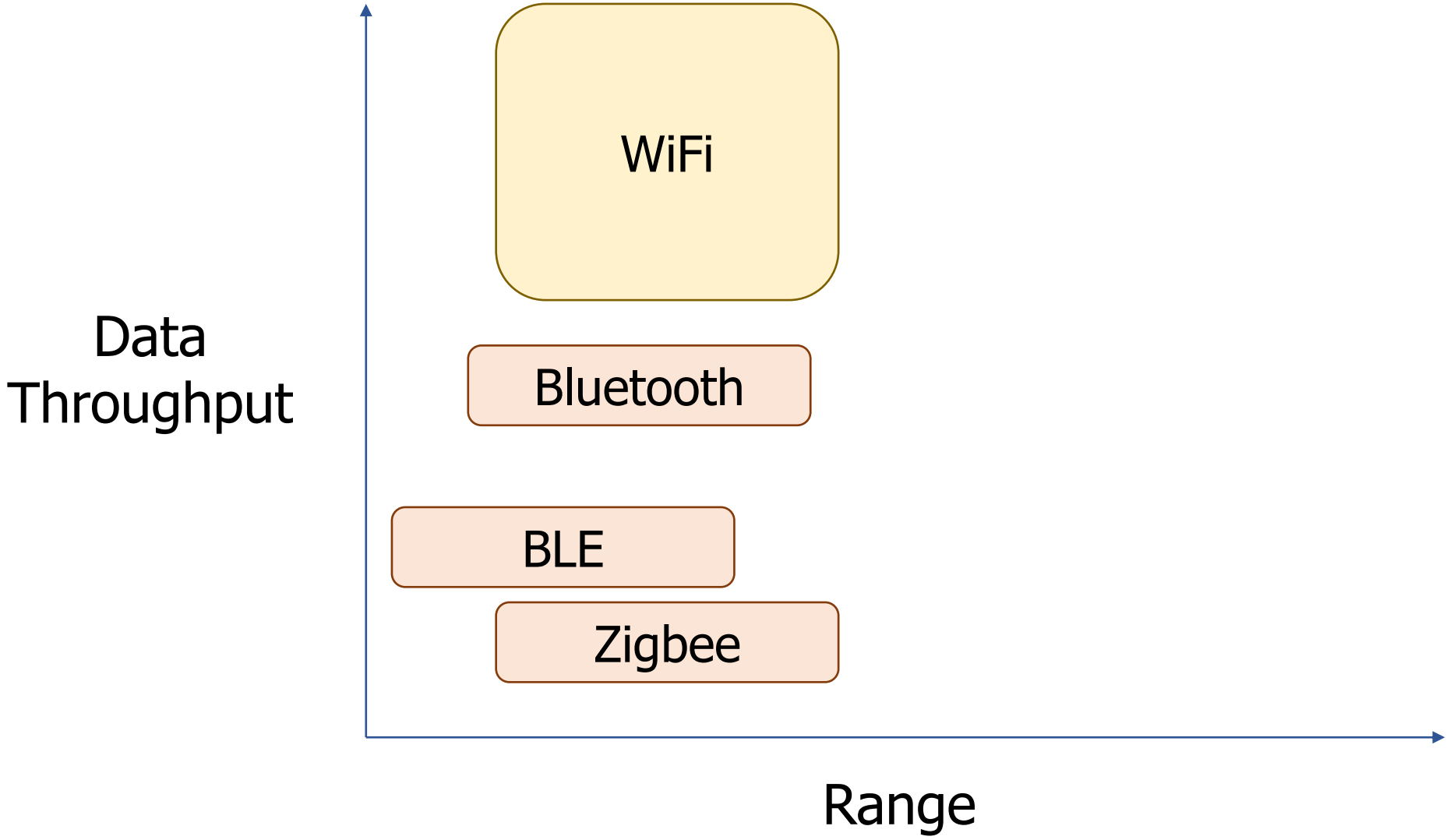
- Wide area of coverage
  - Deploy fewer gateways
- Low power
  - So we can deploy on batteries
- Doesn’t need high throughput
  - Sensor data is relatively small



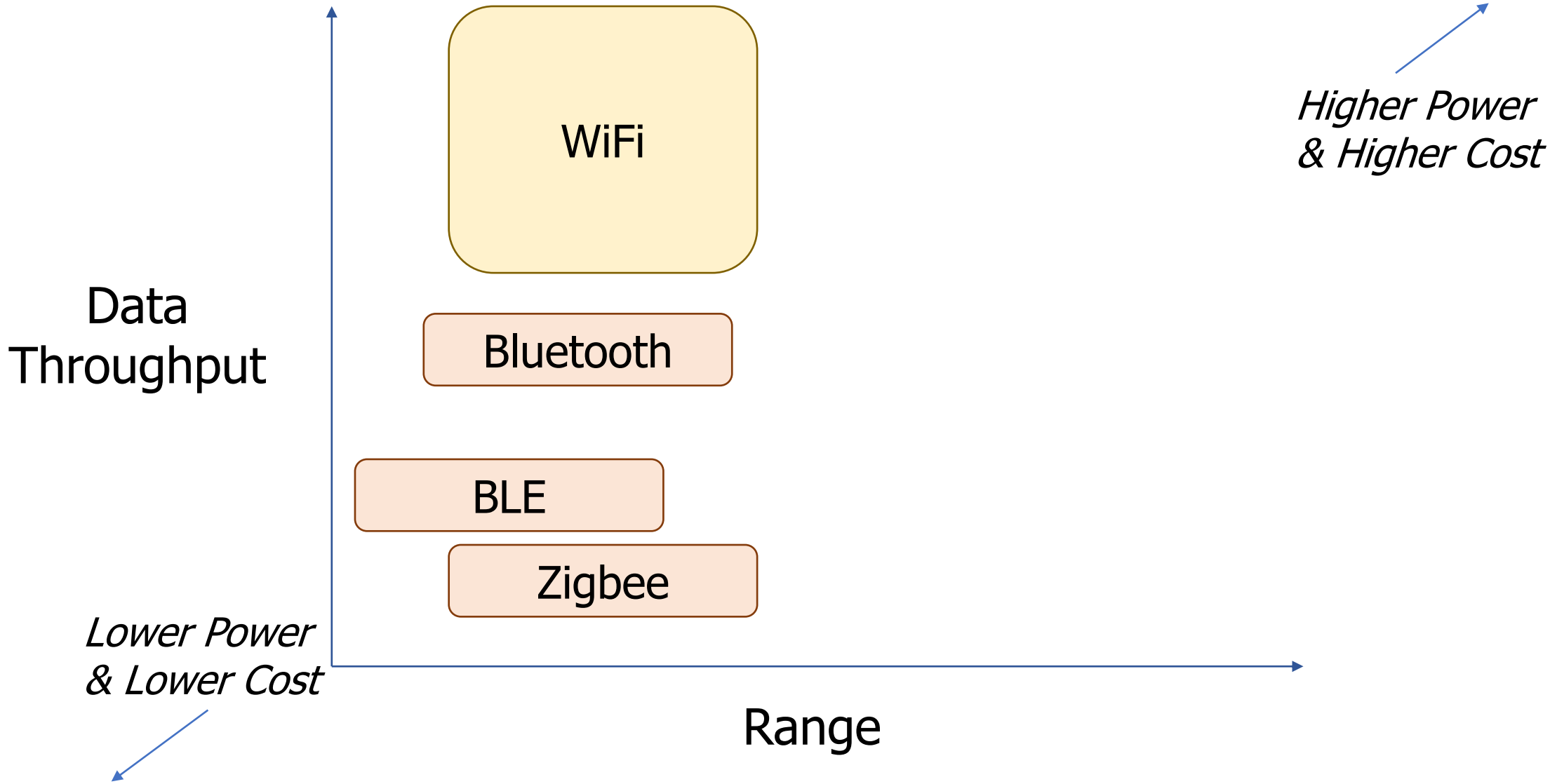
Long-range, low-data needs haven’t historically been met



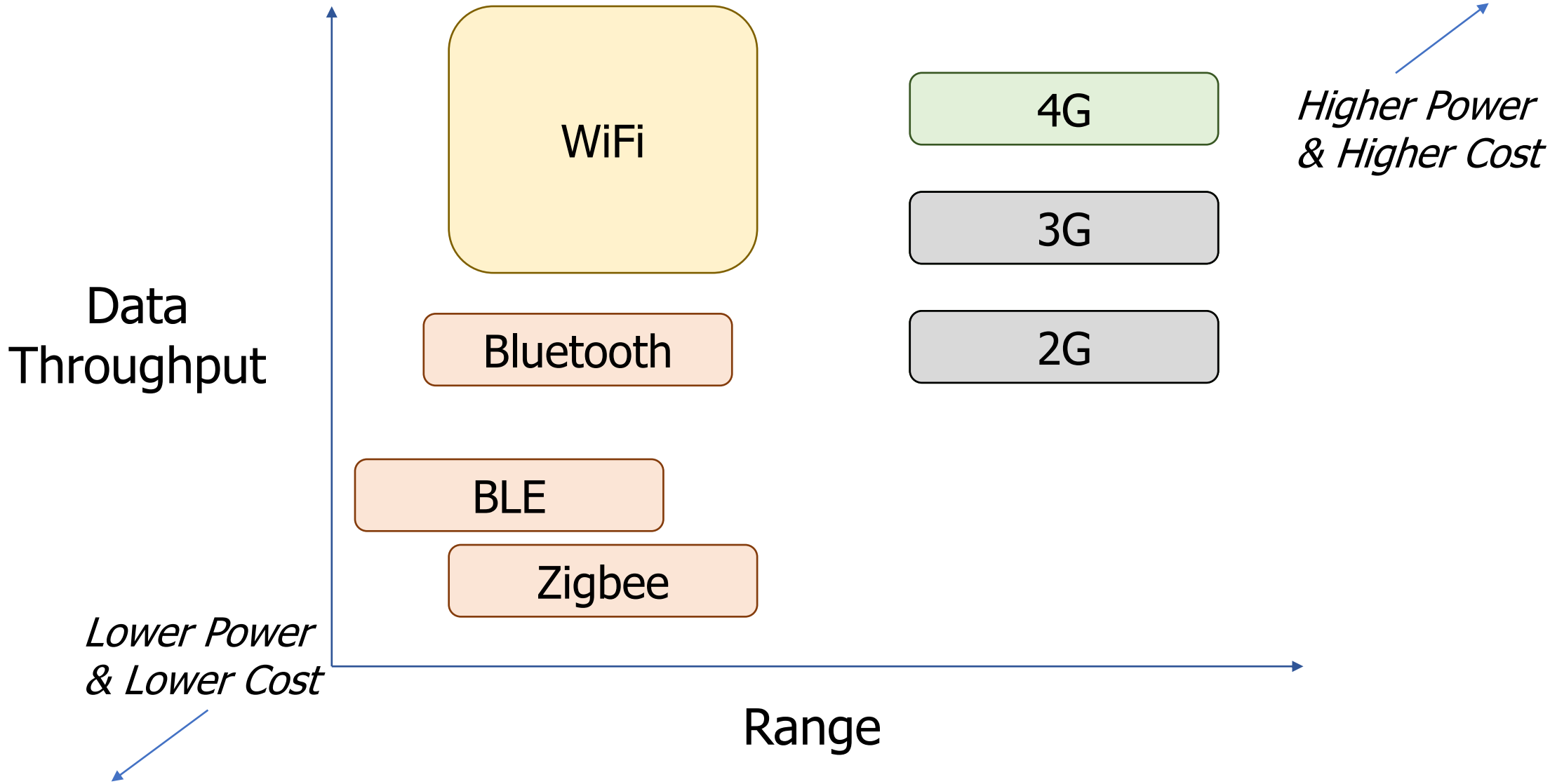
Long-range, low-data needs haven’t historically been met



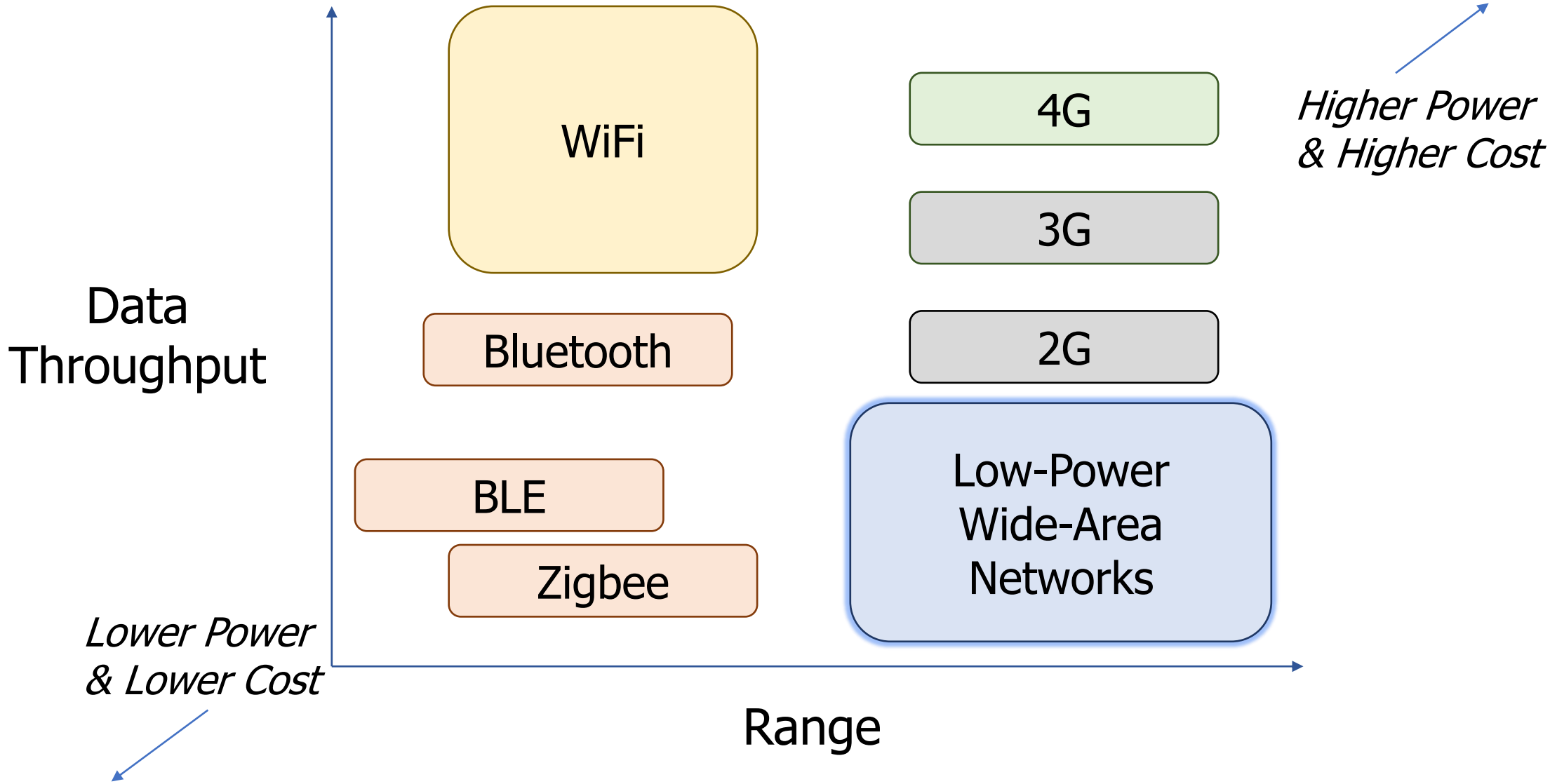
Long-range, low-data needs haven't historically been met



Long-range, low-data needs haven't historically been met



Long-range, low-data needs haven't historically been met



LPWANs overview (common qualities)

- Unlicensed 915 MHz band (902-928 MHz in North America)
  - EU: 863-870 MHz (notably less bandwidth)
  - China: 779-787 MHz
- Higher power transmissions: ~20 dBm (100 mW)
- Low data rate 100 kbps or less
- Range on the order of multiple kilometers
- Simple Aloha access control

Outline

- Wide-Area Network Background

- **Unlicensed LPWANs**
  - **LoRaWAN**
  - Sigfox
  - 802.11ah
  - TV Whitespaces

LoRaWAN

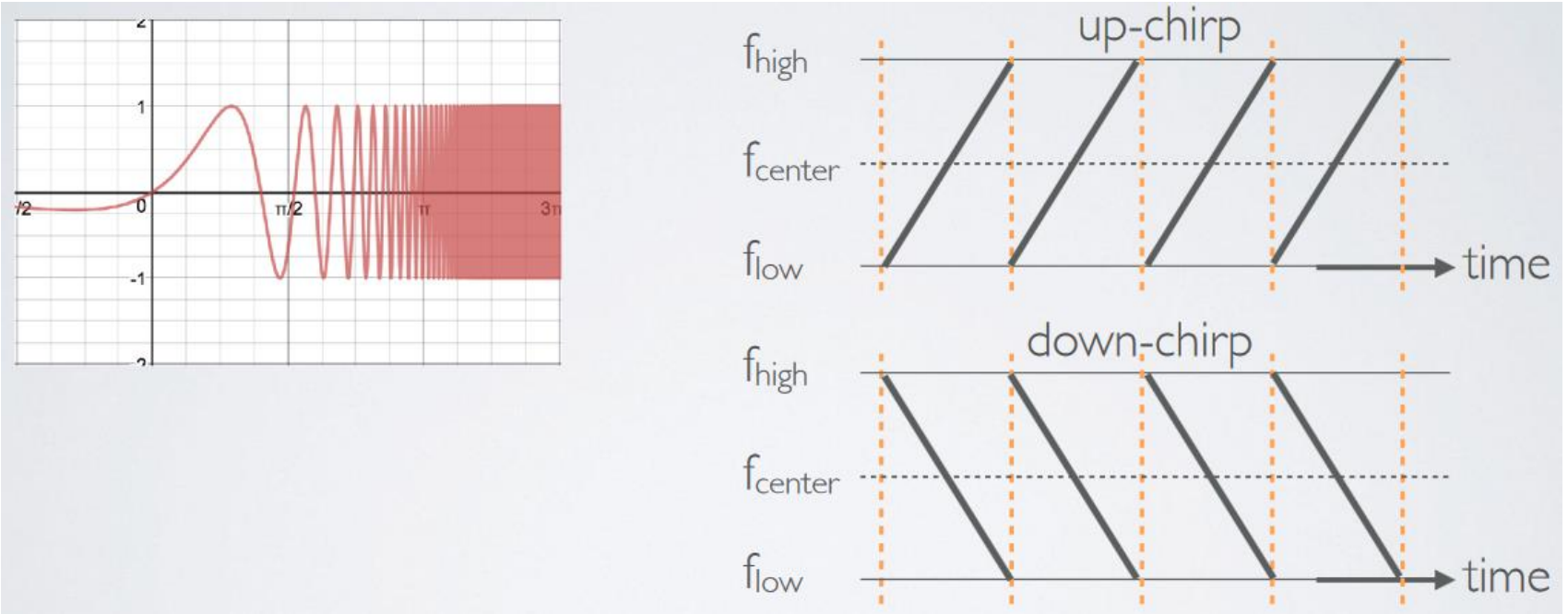
- Open communication standard built with proprietary LoRa PHY

- Low rate (1-20 kbps) and long range (~5 km)
  - Shorter range than Sigfox but much higher bit rate

- Most popular LPWAN protocol
  - Target of academic research
  - Industry involvement in hardware and deployments

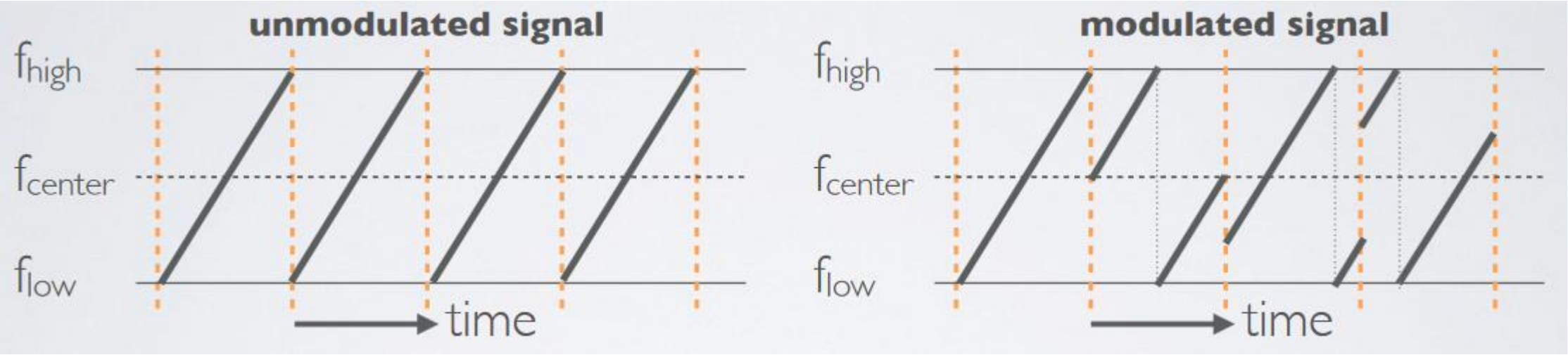
LoRa PHY uses a different modulation

- Chirp Spread Spectrum (CSS)
  - Modulation technique where frequency is varied linearly from lowest to highest within a channel



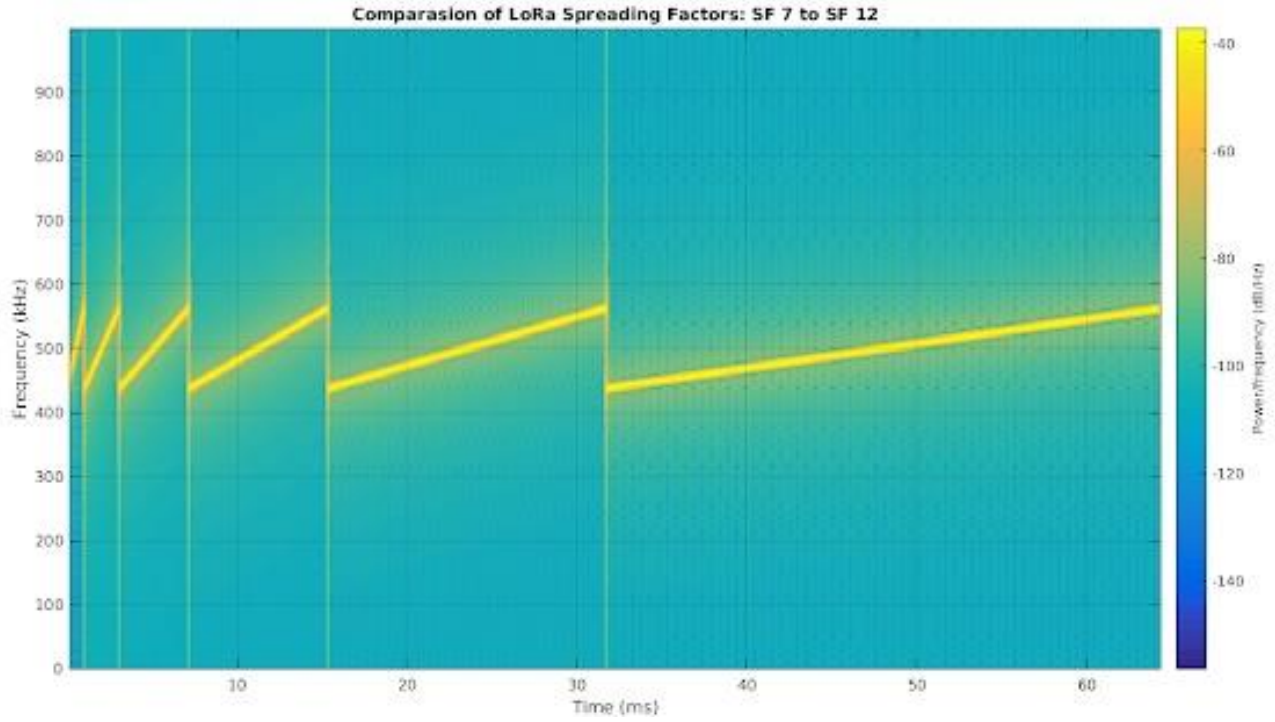
Chirp Spread Spectrum

- Data is modulated in the starting and ending points of chirp
  - Frequency increases linearly, modulo bounds of the channel



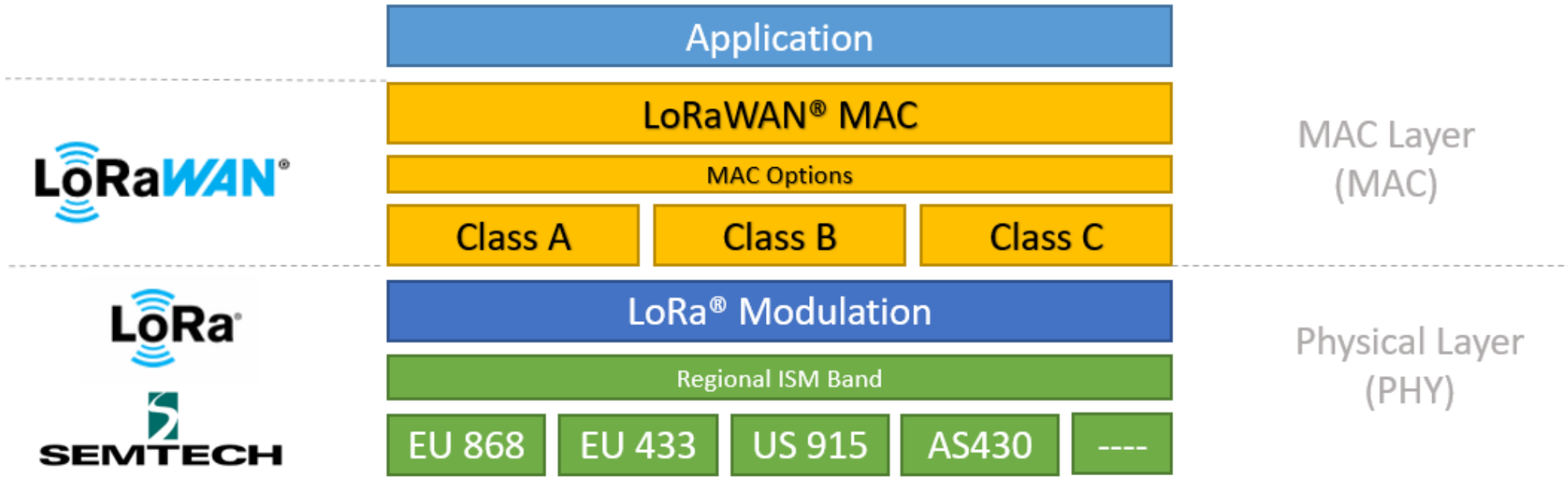
CSS has a Spreading Factor which determines bit rate

- Spreading Factor is essentially the rate-of-change of frequency
  - Slope of the line
  - Lower values of spreading factor (steeper slope) are faster data rate
- Important: different spreading factors are (mostly) orthogonal!
  - Two can overlap in time, space, and channel without a collision



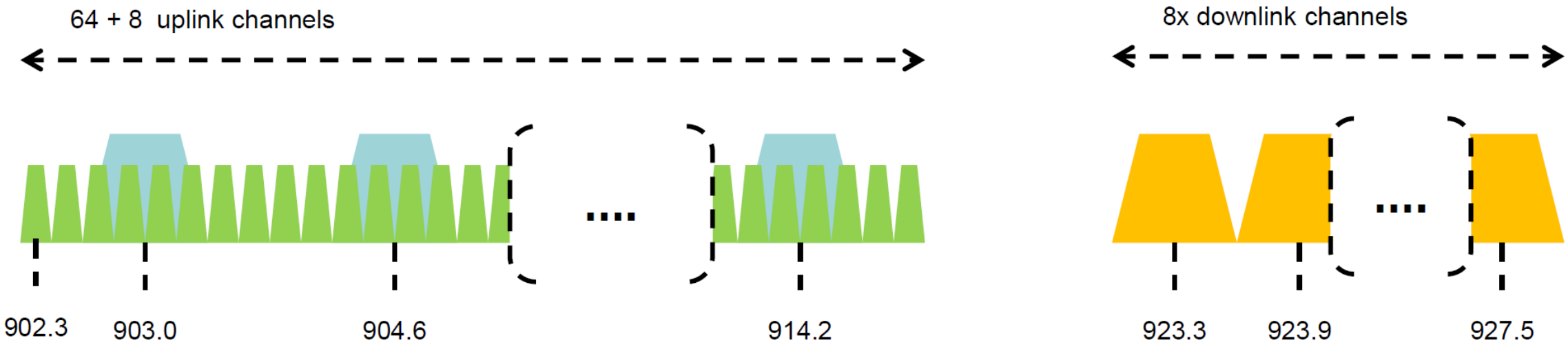
LoRa vs. LoRaWAN

- LoRa: physical layer protocol
- LoRaWAN: MAC and network layer
- (In practice we often conflate LoRa and LoRaWAN.)



https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

LoRaWAN channels (in the US)



- Sixty-four, 125 kHz uplink channels
  - Frequency Hopping over the 64 uplink channels
  - Plus eight, 500 kHz overlapping uplink channels (not very used in practice)

- Eight, 500 kHz downlink channels

LoRaWAN data rates

- Data rate options depend on channel in use
  - Unbalanced uplink and downlink
- 64-channel uplink
  - 1-5 kbps data rate
- Allowable rates based on US dwell time restriction (400 ms)
  - Different in different regions

Data Rate Index	**Spreading Factor**	**Bit Rate**
125 kHz Uplink Rates		
0	SF10, 125 kHz	980 bps
1	SF9, 125 kHz	1760 bps
2	SF8, 125 kHz	3125 bps
3	SF7, 125 kHz	5470 bps
500 kHz Uplink Rates		
4	SF8, 500 kHz	12500 bps
500 kHz Downlink Rates		
8	SF12, 500 kHz	980 bps
9	SF11, 500 kHz	1760 bps
10	SF10, 500 kHz	3900 bps
11	SF9, 500 kHz	7000 bps
12	SF8, 500 kHz	12500 bps
13	SF7, 500 kHz	21900 bps

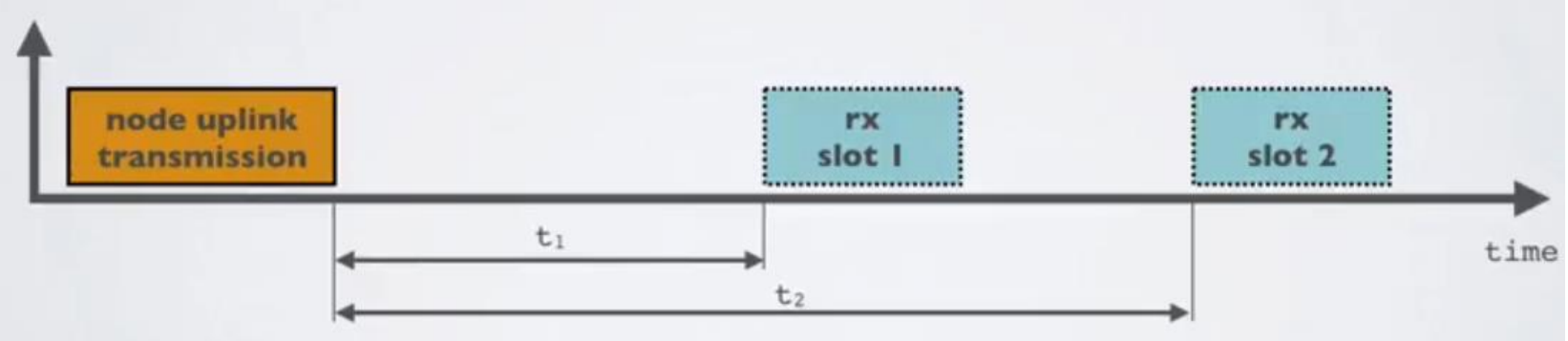
LoRaWAN link budget

- Typical TX power 20 dBm
  - Up to 30 dBm for 64-channel hopping
  - Up to 26 dBm for 8-channel hopping
- Receive sensitivity -119 dBm
  - Compare to -100 dBm for 802.15.4 and -95 dBm for BLE
- Resulting range is about a kilometer in urban environments

LoRaWAN MAC

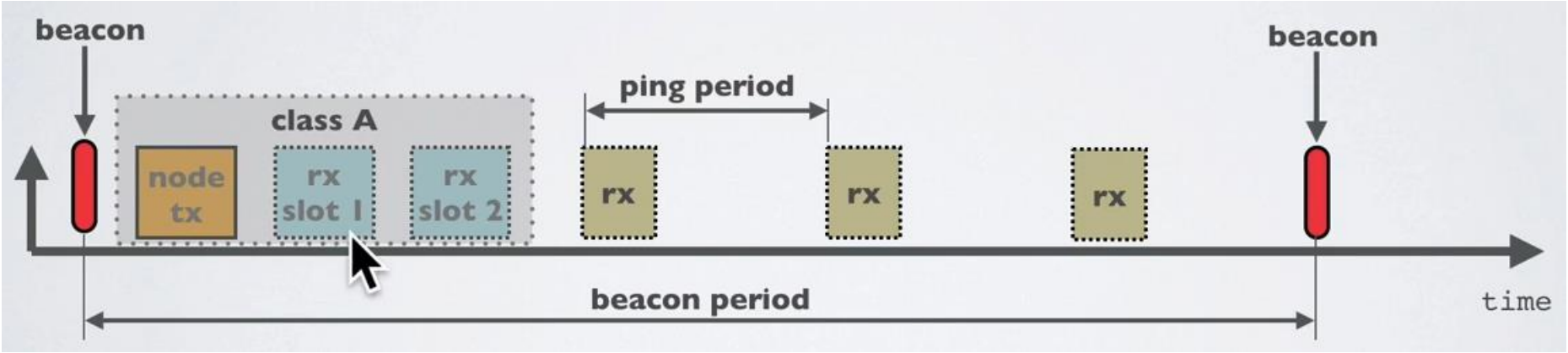
- Uplink: Aloha - transmit whenever
  - Randomly split across 64 uplink channels (reduced odds of collision)
  - Devices a different spreading factors also do not collide
  - Packets are very long though: up to 400 ms in duration

- Downlink: listen-after-send (class A device)
  - Two windows for RX on different channels



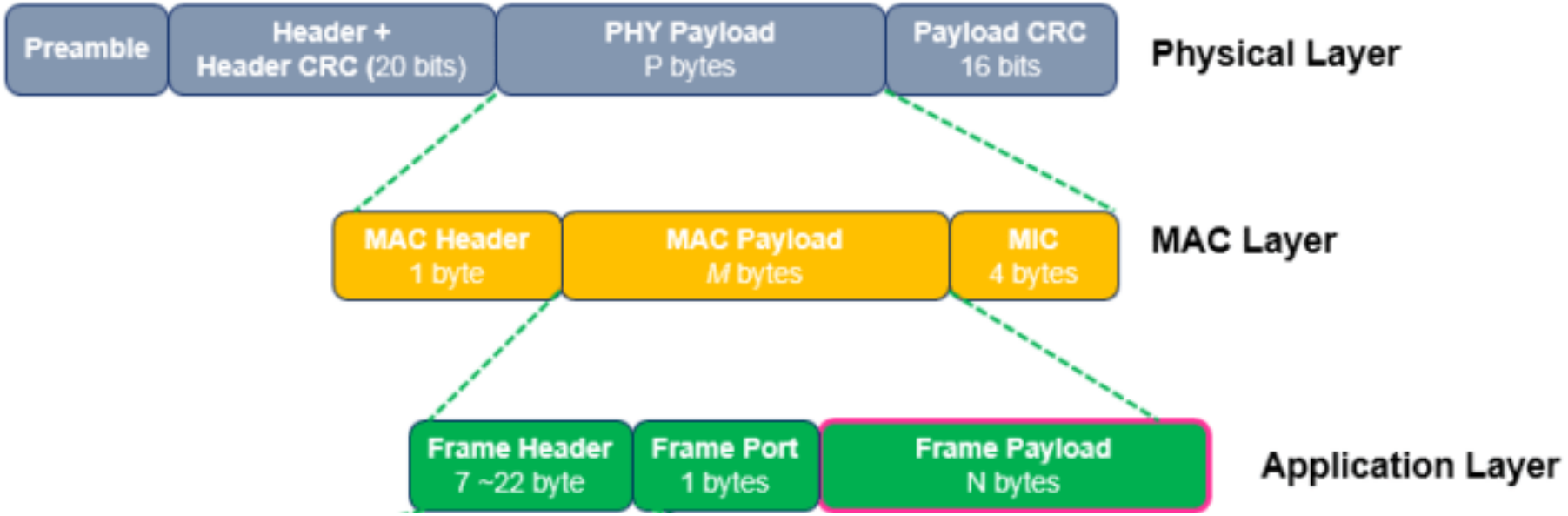
Optional downlink mechanisms

- Periodic listening (class B device)
  - Synchronized with periodic beacons
    - TX still unsynchronized Aloha
  - Mostly unused



- Continuous listening (class C device)
  - Always-on receivers

LoRaWAN packet format



- Frame header includes device address
- MAC Payload maximum size depends on data rate
  - Again based on dwell time in the US

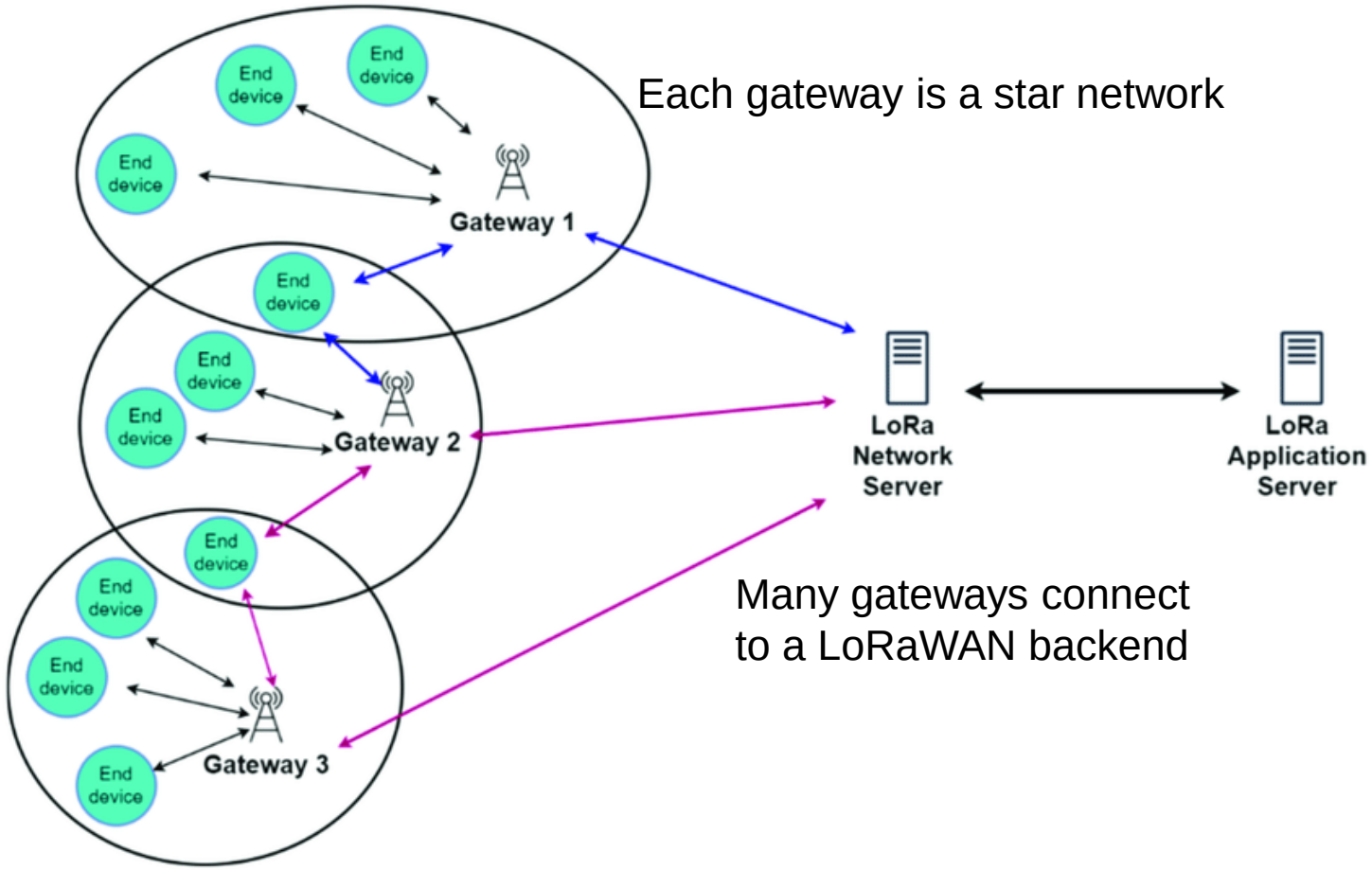
Data Rate Index	MAC Payload Size
0	19 bytes
1	61 bytes
2	133 bytes
3	250 bytes
4	250 bytes

LoRaWAN gateways

- No synchronization with end devices

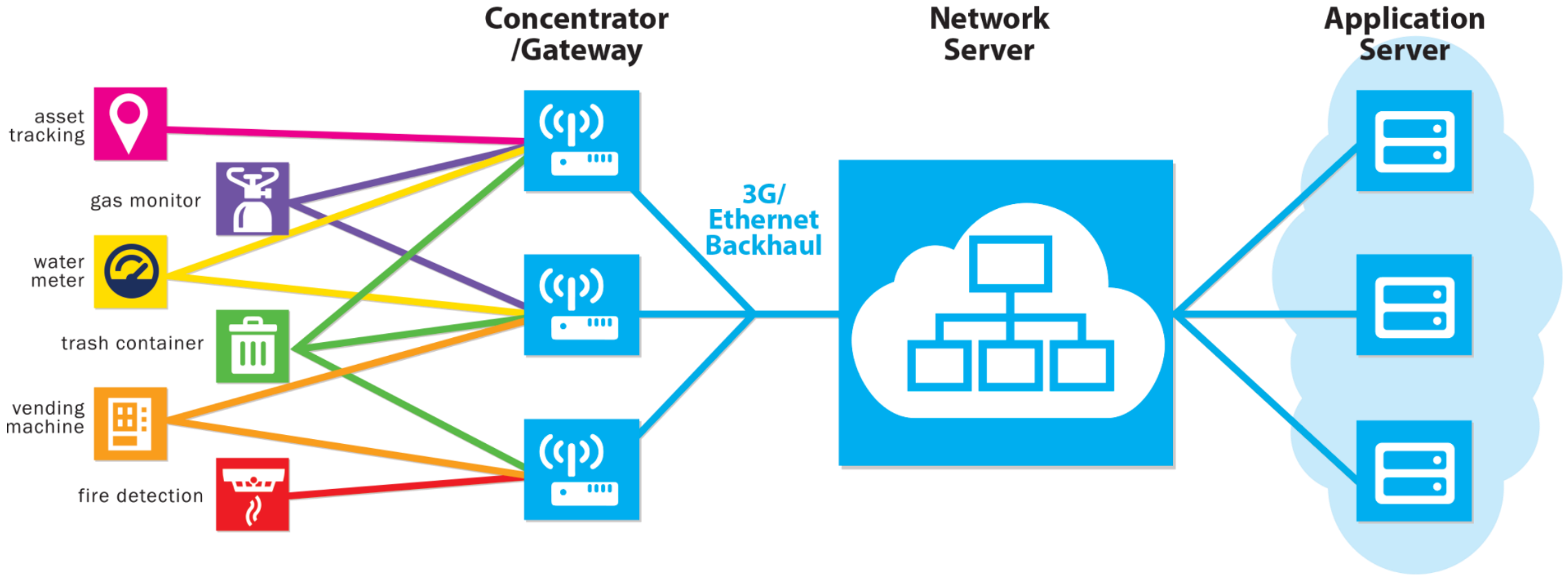
- Instead listen to entire bandwidth simultaneously
  - Only 12 MHz total
  - Recognize preambles and allocate hardware to decode packet
  - Number of simultaneously decoded packets depends on decoders
    - Cheap gateways: 8 decoders
    - Good gateways: 64 decoders

LoRaWAN star-of-stars topology



https://www.researchgate.net/publication/360965985_LoRaWAN_Communication_Protocols_A_Comprehensive_Survey_under_an_Energy_Efficiency_Perspective

LoRaWAN network details



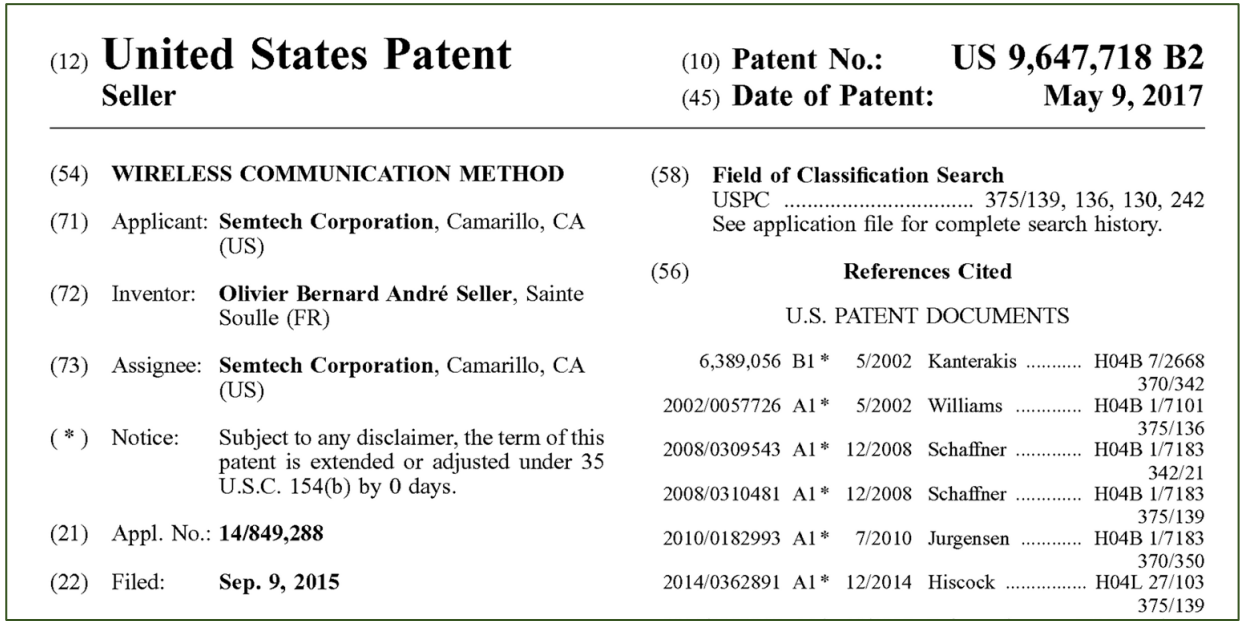
LoRaWAN hardware

- Numerous hardware modules and development kits
  - Almost all use Semtech radio chips (Semtech owns LoRa PHY)

- Recent addition: STM32WLE5 LoRa SoC
  - Cortex-M4 + LoRa radio (analogous to nRF52840)

Note about LoRa hardware

- LoRa PHY is patented
- Hardware controlled by Semtech
  - Good for interoperability
- Openness? Innovation?
  - Less good



(12) **United States Patent**
Seller

(10) **Patent No.: US 9,647,718 B2**
(45) **Date of Patent: May 9, 2017**

(54) **WIRELESS COMMUNICATION METHOD**

(71) Applicant: **Semtech Corporation**, Camarillo, CA (US)

(72) Inventor: **Olivier Bernard André Seller**, Sainte Soulle (FR)

(73) Assignee: **Semtech Corporation**, Camarillo, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/849,288**

(22) Filed: **Sep. 9, 2015**

(58) **Field of Classification Search**
USPC 375/139, 136, 130, 242
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,389,056	B1 *	5/2002	Kanterakis	H04B 7/2668 370/342
2002/0057726	A1 *	5/2002	Williams	H04B 1/7101 375/136
2008/0309543	A1 *	12/2008	Schaffner	H04B 1/7183 342/21
2008/0310481	A1 *	12/2008	Schaffner	H04B 1/7183 375/139
2010/0182993	A1 *	7/2010	Jurgensen	H04B 1/7183 370/350
2014/0362891	A1 *	12/2014	Hiscock	H04L 27/103 375/139

Joining a LoRaWAN Network

- Two modes:
  - OTAA (Over the air activation): Dynamic join procedure that sets up security keys
  - ABP (Activation By Personalization): Legacy approach with pre-shared security keys

- OTAA Joining: two packets
  - Join-request: from end device to the Network Server
  - Join-accept: from Network Server to the end device

OTAA Join Procedure

Device knows three things:

- AppEUI: Identifier for the application the device uses on the application server
- DevEUI: Device ID
- AppKey: AES-128 bit secret registered with the network server

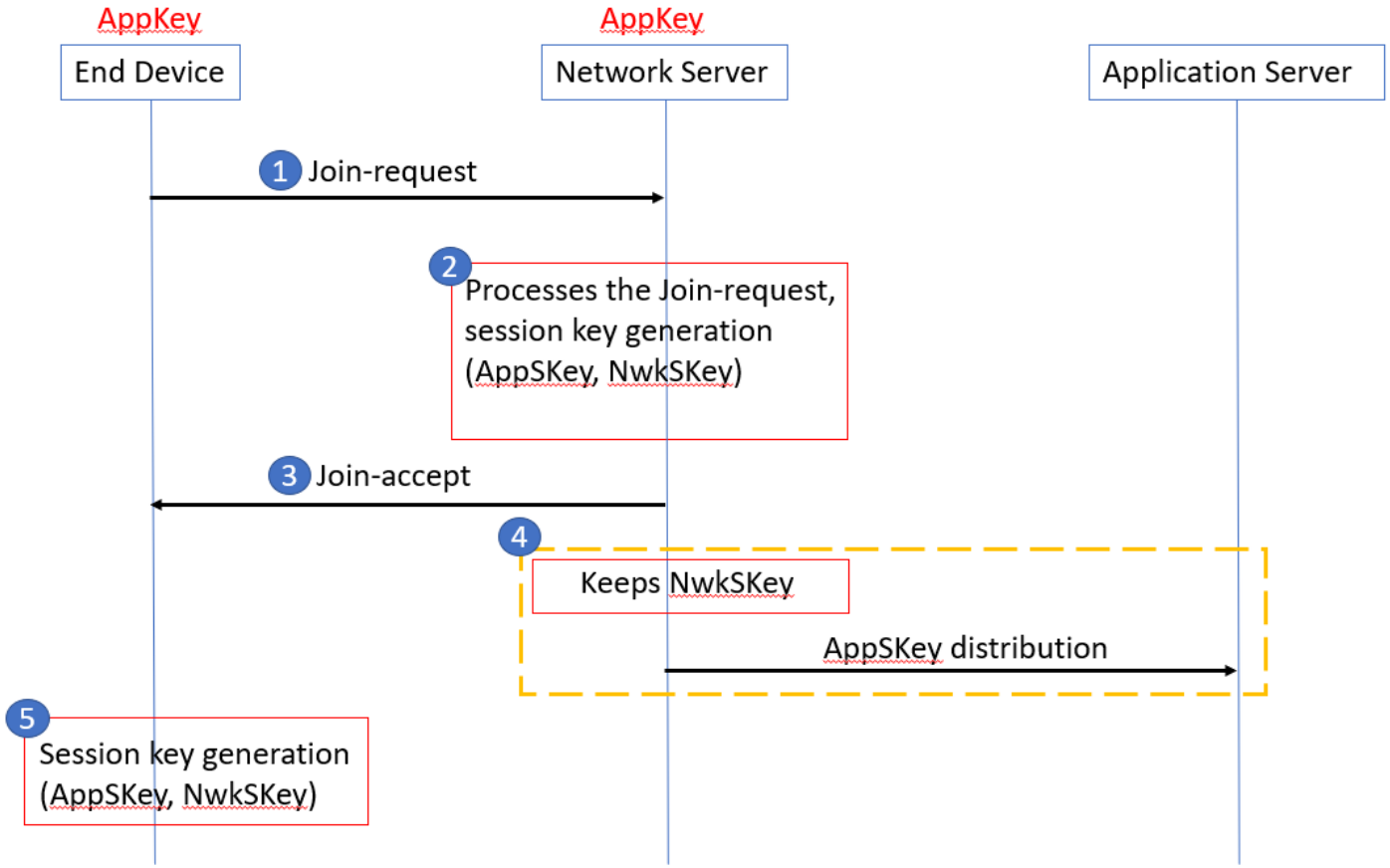
Join Request

- Device sends (AppEUI, DevEUI, Nonce) and MIC using AppKey

Join Accept

- Network server responds with AppNonce encrypted with AppKey

Device and network server compute the same AppSKey to encrypt all future payloads

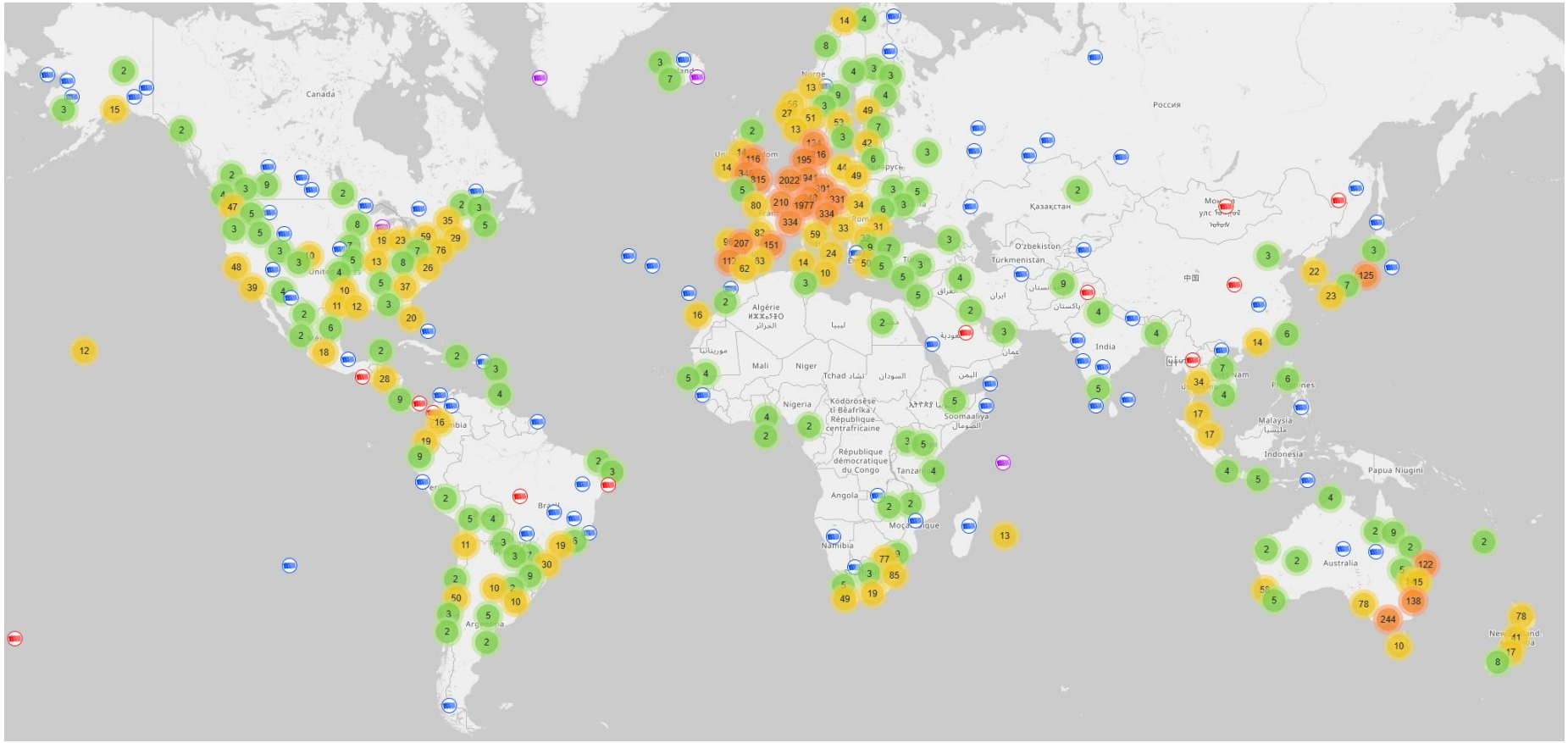


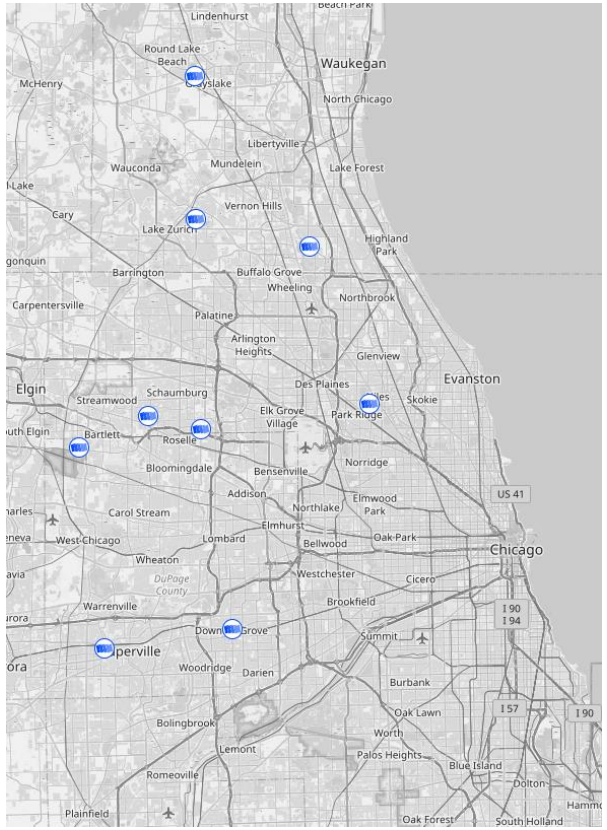
LoRaWAN network providers

- You can always manage your own network
  - Buy a gateway and run whatever backend software you want

- Somewhat-managed network providers
  - The Things Network (predominantly in Europe)
    - But available in the US too!
  - Helium
    - Anyone can buy and install their own gateway, which serves everyone
    - Microtransactions to pay for communication

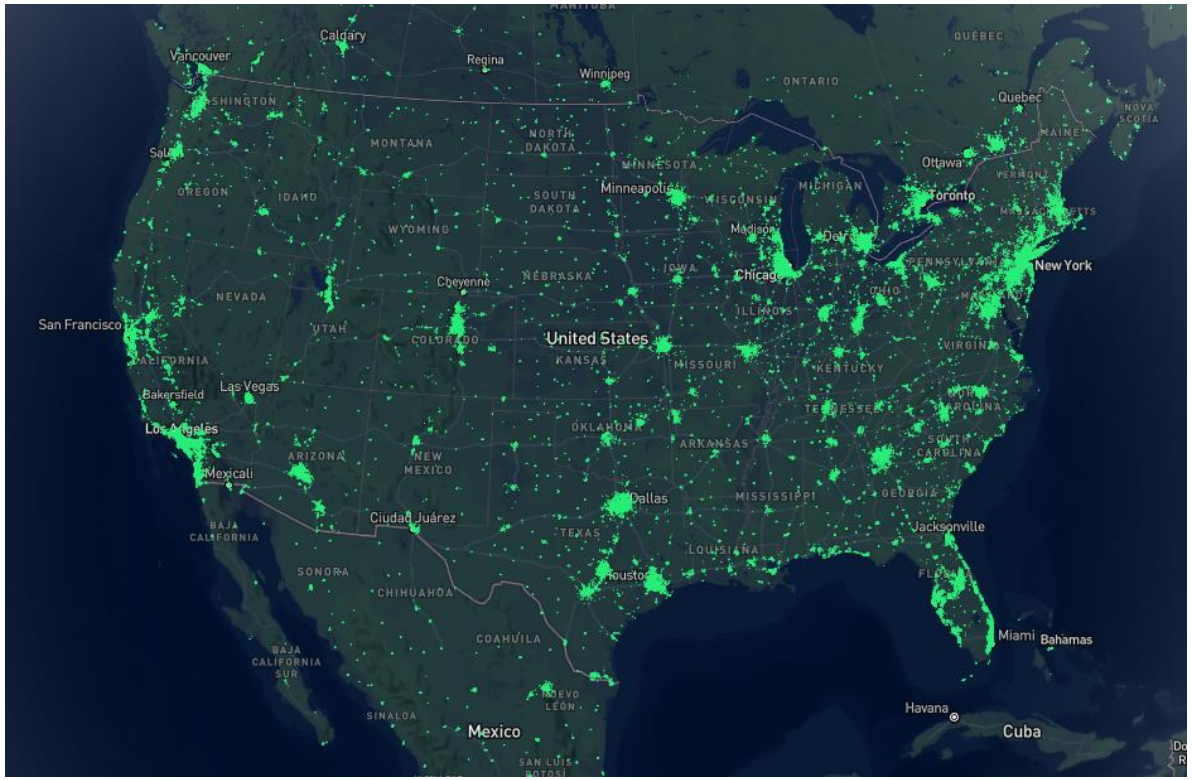
The Things Network gateways (Spring 2025)

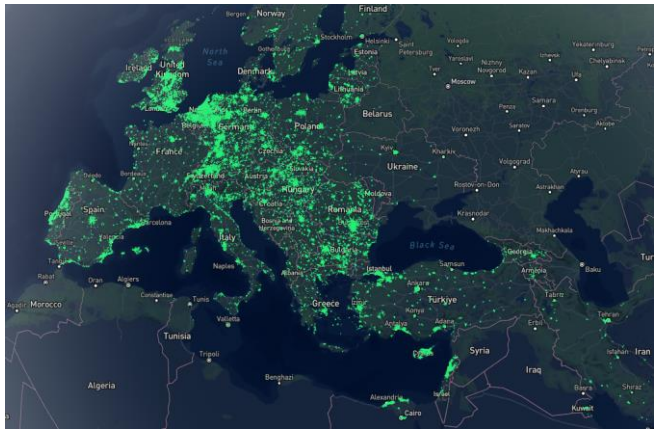


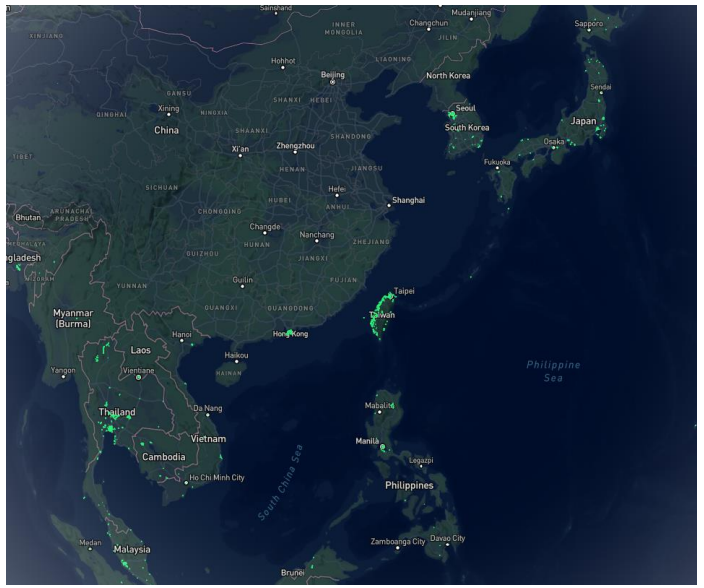


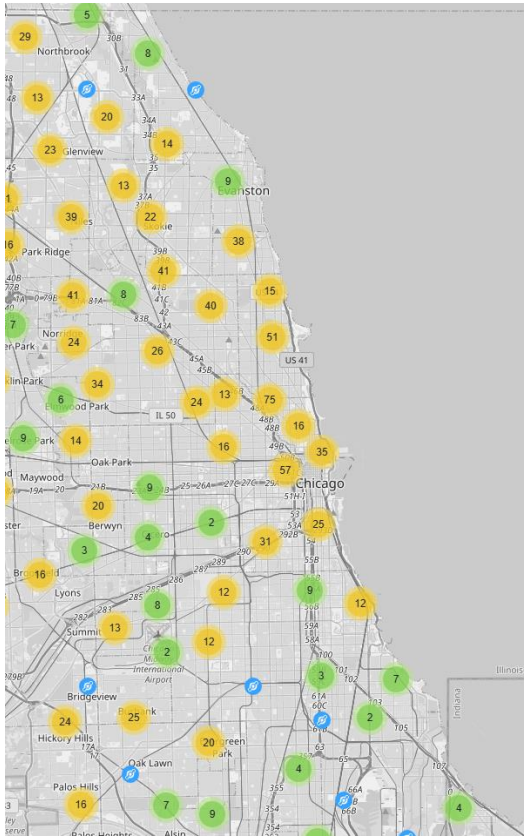
- 21000 gateways active in last two weeks (May 2025)
- Closest to Evanston is in Niles ~10 miles away

Helium gateways (Spring 2025)







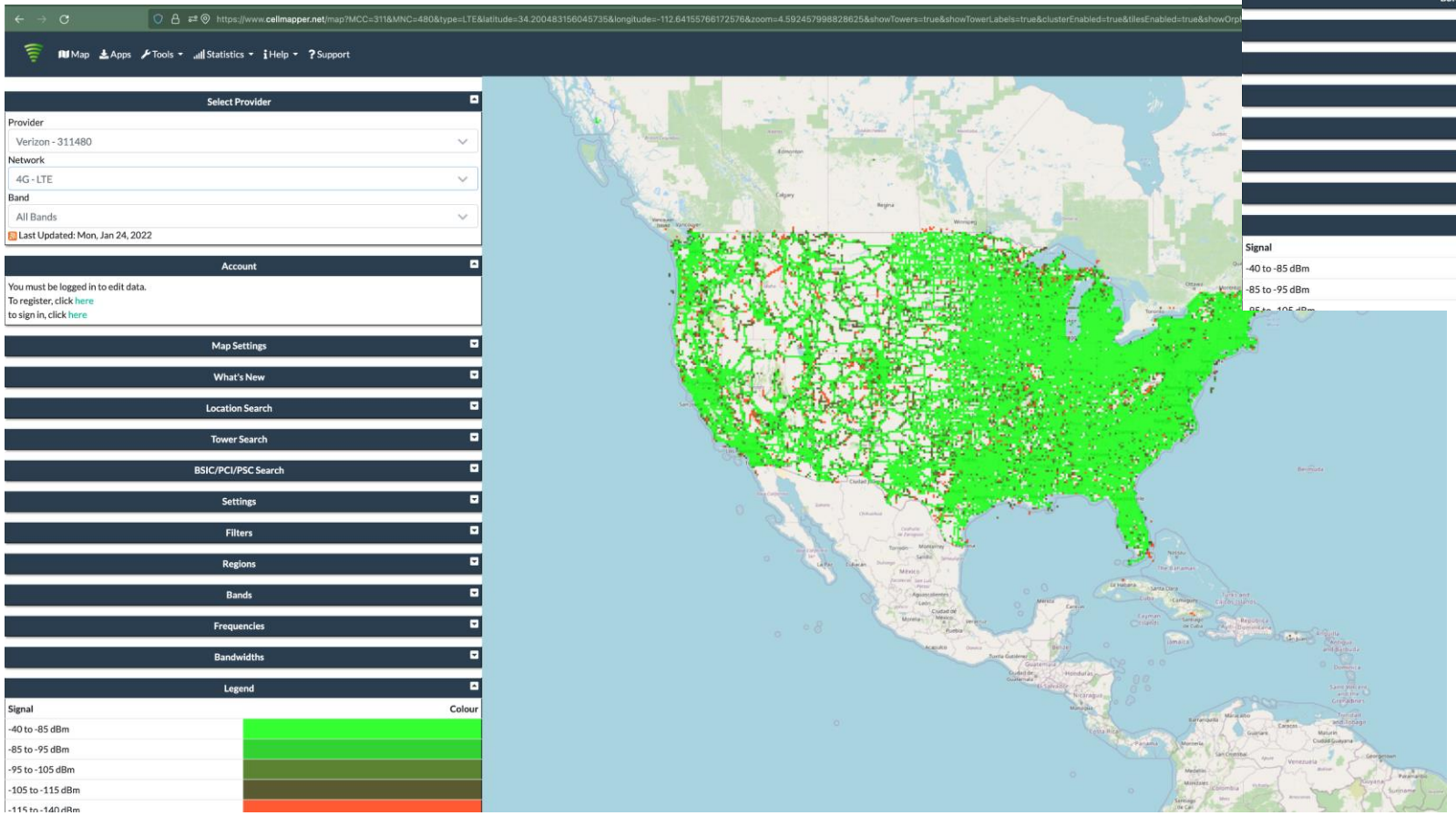


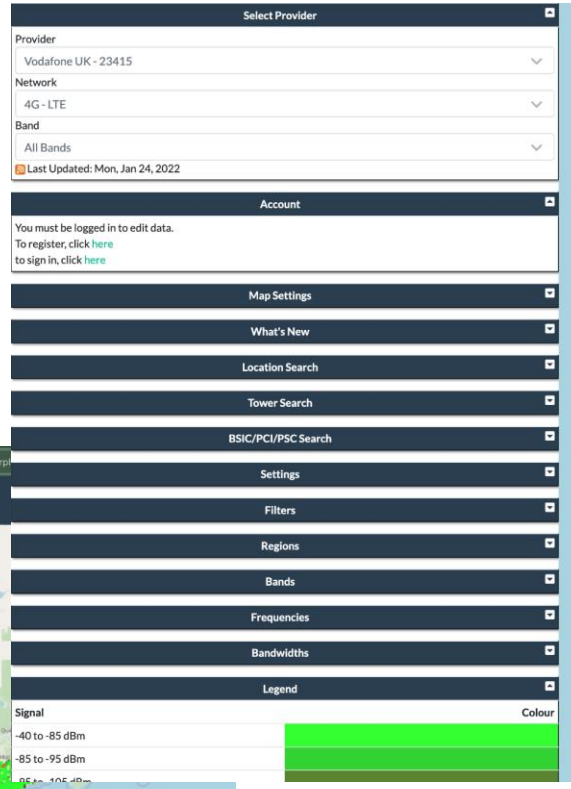
May 2022: 800,000 hotspots, with +80K in last 30 days
Feb 2023: 980,000 hotspots, with +3K in last 30 days
May 2025: 285,000 hotspots… I think they pruned dead gateways, but also rewards seem to be reduced lately

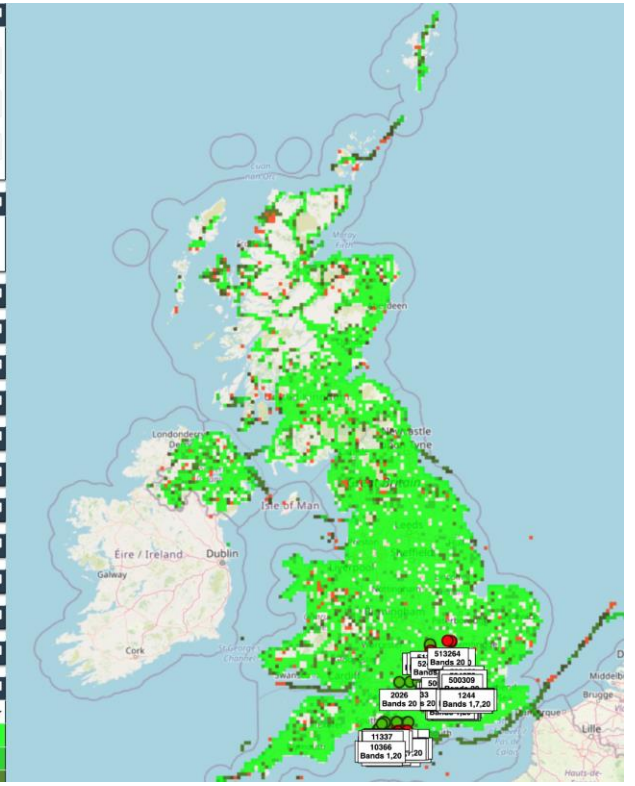
- Several gateways in Evanston, including one on far south side of campus

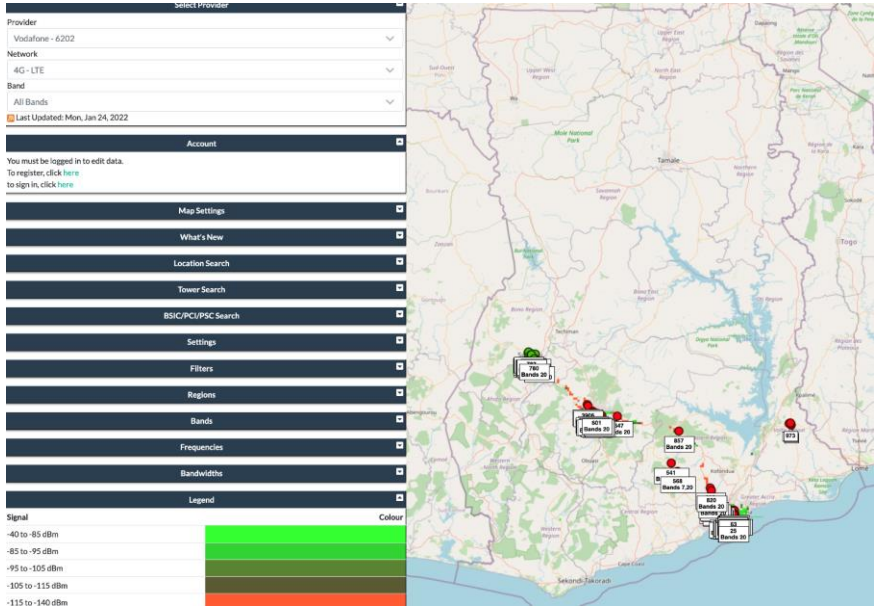
Quick reality check: Cellular?

- ~350,000 sites across ~150,000 towers
  - In the just US









Break + Open Question

- What kinds of use cases exist for LoRaWAN?
  - What can you do with 1-5 kbps uplink, 1-22 kbps downlink?
  - Multiplied by 64 channels uplink, 8 channels downlink

Break + Open Question

- What kinds of use cases exist for LoRaWAN?
  - What can you do with 1-5 kbps uplink, 1-22 kbps downlink?
  - Multiplied by 64 channels uplink, 8 channels downlink
- Outdoor small-sized sensing seems possibly achievable!
  - With a low enough rate, it could support **many** devices
- Code updates on devices could be tough

Outline

- Wide-Area Network Background

- **Unlicensed LPWANs**
  - LoRaWAN
  - **Sigfox**
  - 802.11ah
  - TV Whitespaces

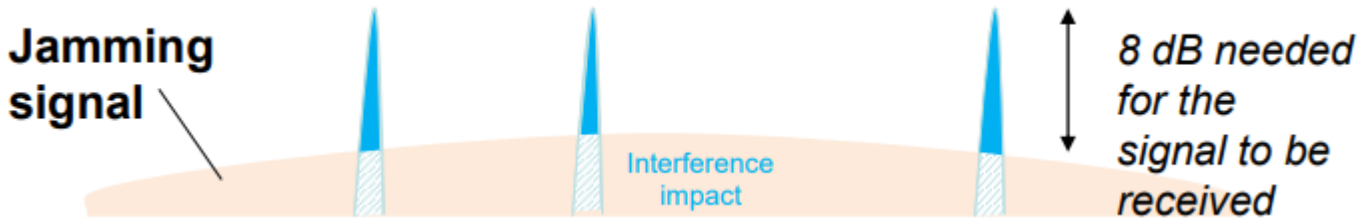
Sigfox

- Very low-rate (600 bps), very long-range (10+ km) communication
- Star-topology networks, with always-listening gateways
  - Any number of low-power end devices
- Uplink-focused communication
- Applications: very low-rate metering

Sigfox PHY

- Unlicensed-band communication
  - Europe 868 MHz. US 902-928 MHz (915 MHz band)

- Ultra-narrowband 600 Hz (100 Hz Europe) channel bandwidth
  - Detection only needs to occur at very specific frequency
  - Helps improve signal-to-noise ratio



Sigfox unbalanced uplink and downlink

- Uplink
  - 600 Hz bandwidth, 600 bps, DBPSK
- Downlink
  - 1.5 kHz bandwidth, 600 bps, GFSK

- Particularly designed for Europe
  - Uplink on 1% duty cycle channel, up to 14 dBm
  - Downlink on 10% duty cycle channel, up to 27 dBm

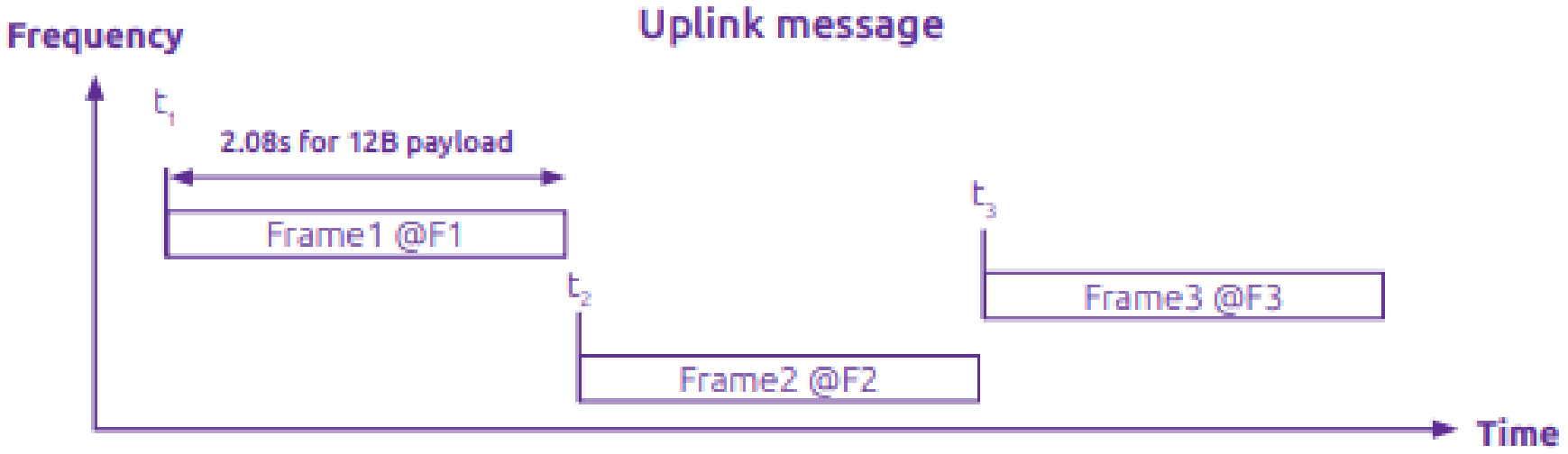
- Works fine in US too
  - Gets more power (24 dBm up is typical, up to 32 dBm down) and more range

Sigfox link budget

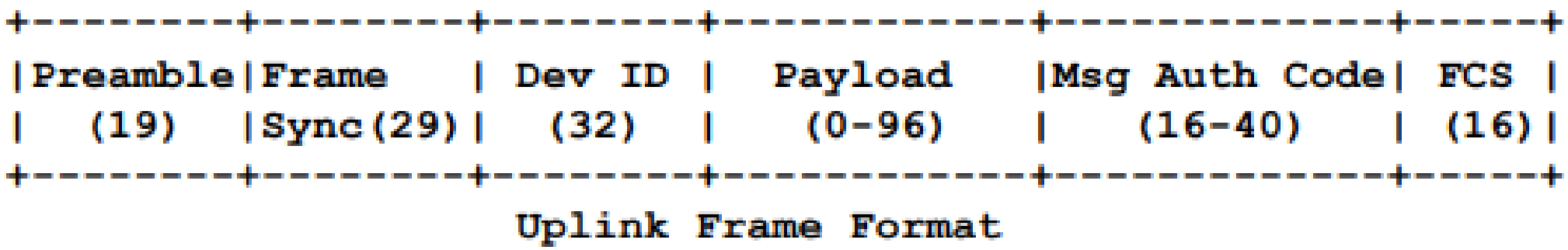
- Why transmit at 100-600 bps?
  - For greatly increased link budget
- Link budget: 150-160 dBm
  - Assuming Tx at ~20 dBm
  - Means Rx Sensitivity of -130 dBm (10 dBm better than LoRaWAN)
- Resulting range: 10-15 km in urban environments
  - Except that buildings lead to dead spots in range

Sigfox MAC

- Aloha-style access control (send whenever)
  - No acknowledgements!
- Send message three times for increased reliability
  - Then listen for downlink at a set period later on a known frequency



Sigfox uplink packet



Uplink Frame Format

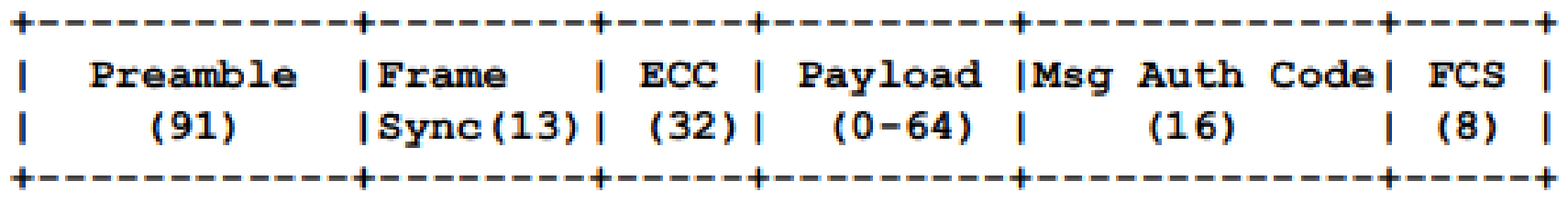
- Up to 29 bytes total per packet
  - Payload: up to **12 bytes** 😱
- Other fields
  - Preamble + Frame Sync are really a 6 byte field for radio sync
  - Authentication: 2-5 bytes
  - Frame Check Sequence: 16-bit CRC

Aside: why faster bitrate in the US?

- Packet size up to 29 bytes (232 bits)
  - At 100 bps: 2.32 seconds on air
  - At 600 bps: 0.387 seconds on air

- Maximum dwell time for 915 MHz band: 400 ms

Sigfox downlink packet



Downlink Frame Format

- Similar structure, 28 bytes total
  - Payload: up to 8 bytes
- Larger preamble + frame sync of 13 bytes
- Error Correcting Code for increased reliability

Sigfox deployments

- Proprietary network with managed deployment
  - Like cellular networks
  - Sigfox deploys networks and transports data
  - 140 uplink messages plus 4 downlink message per day

- Connectionless communication
  - Devices are registered with the networks
  - Keys are provided in the software image
  - Any deployed Sigfox gateway can collect transmitted data
    - Enables mobile applications

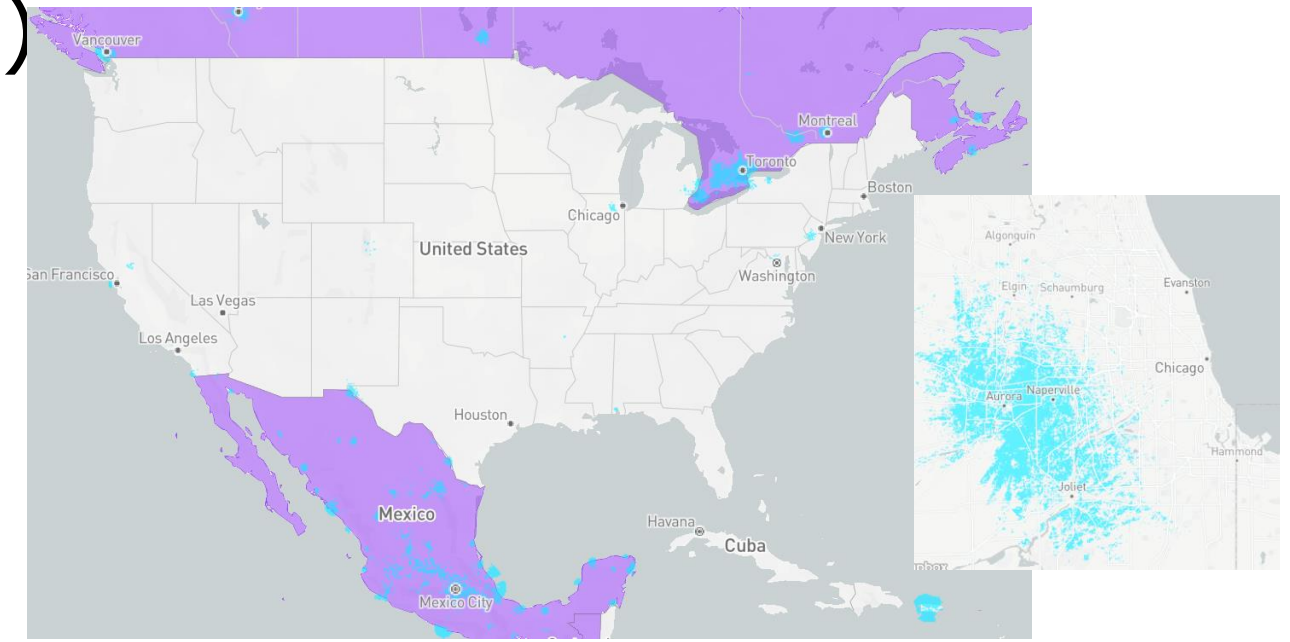
Sigfox coverage (Spring 2025)

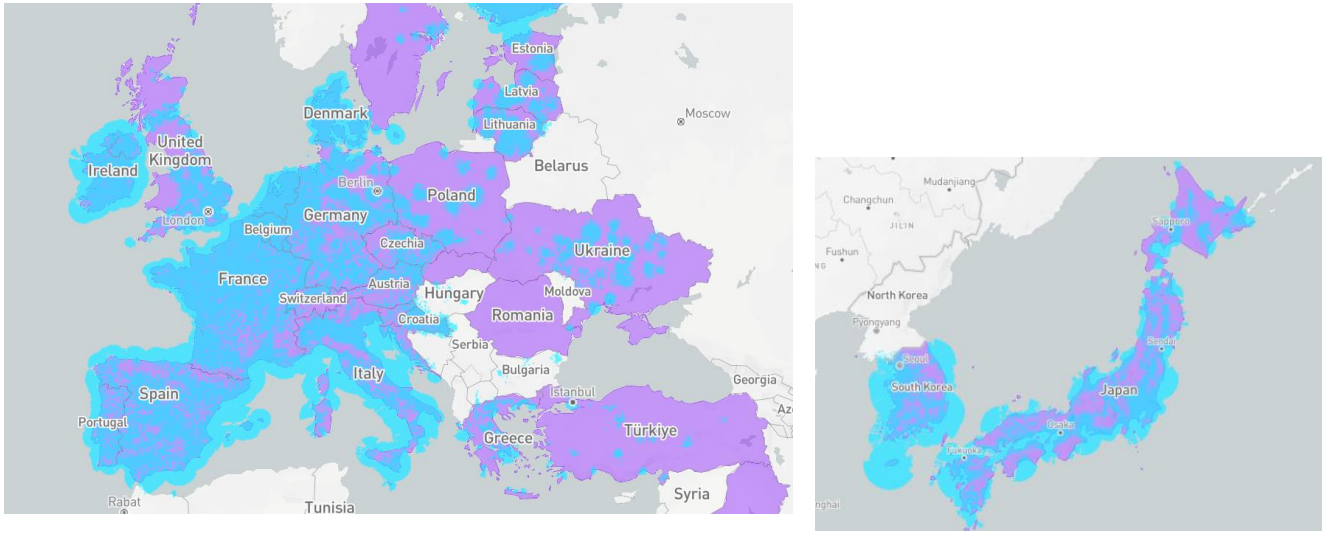
- Not focused on US coverage right now (coverage is blue)
  - Much higher availability in Europe
  - No longer planned rollout in US (purple)

- January 2022
  - Sigfox filed for bankruptcy

- April 2022
  - Sigfox purchased by UnaBiz
  - Renamed: Sigfox "0G" Technology

- December 2024
  - Reports 14 million connected devices worldwide





Break + Open Question

- What kinds of use cases exist for Sigfox?
  - What can you do with 600 bps uplink, 600 bps downlink?
  - Multiplied by ?hundreds? of channels (~400 in Europe)

Break + Open Question

- What kinds of use cases exist for Sigfox?
  - What can you do with 600 bps uplink, 600 bps downlink?
  - Multiplied by ?hundreds? of channels (~400 in Europe)

- **Many** devices that aren't doing very much
  - Simple status monitoring (water, electric, etc.)
    - Not metering necessarily, but activity detection
    - Did a breaker trip?, is water flowing?, etc.

- Definitely no code updates

Outline

- Wide-Area Network Background

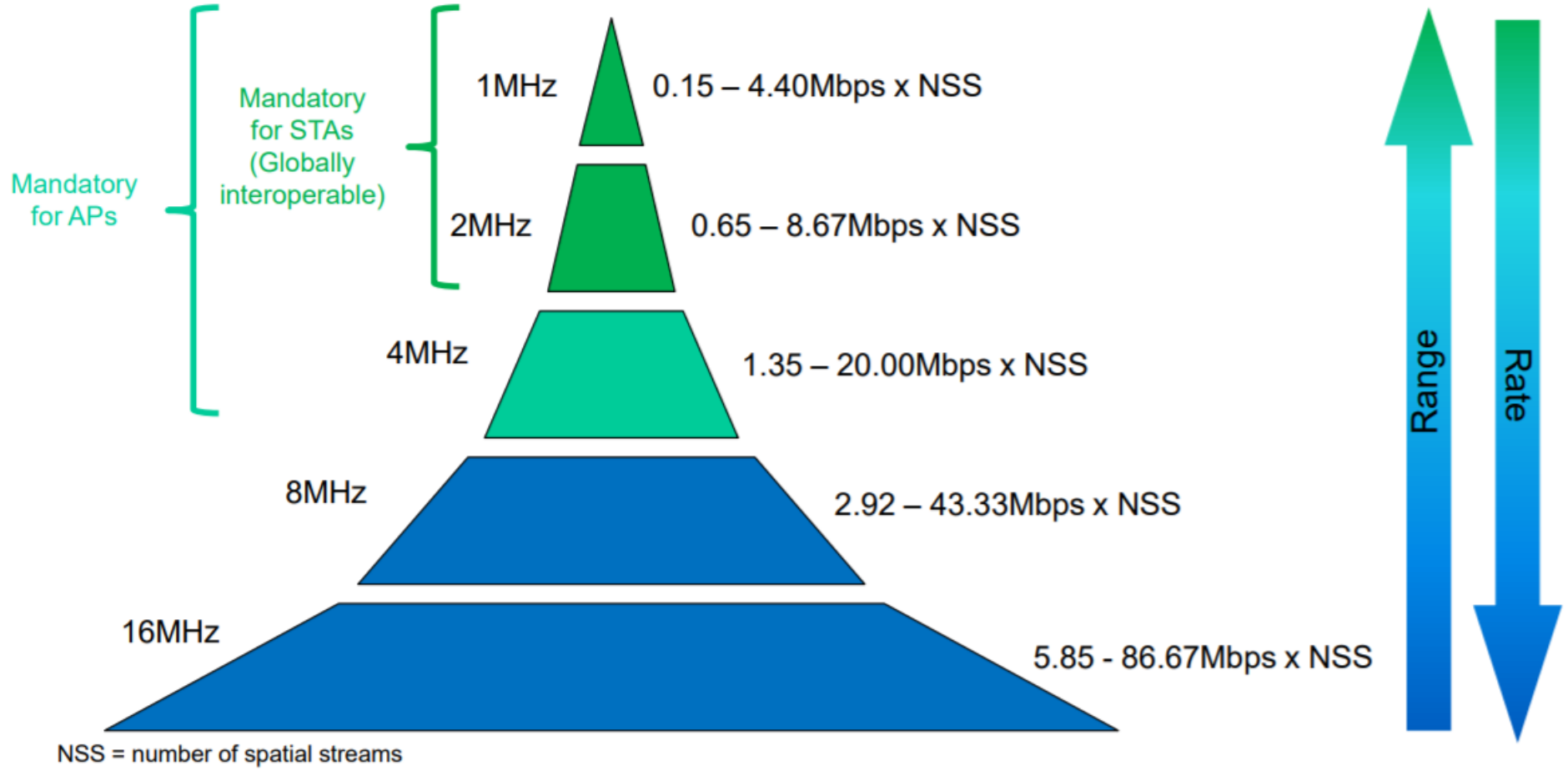
- **Unlicensed LPWANs**
  - LoRaWAN
  - Sigfox
  - **802.11ah**
  - TV Whitespaces

IEEE standard for LPWANs

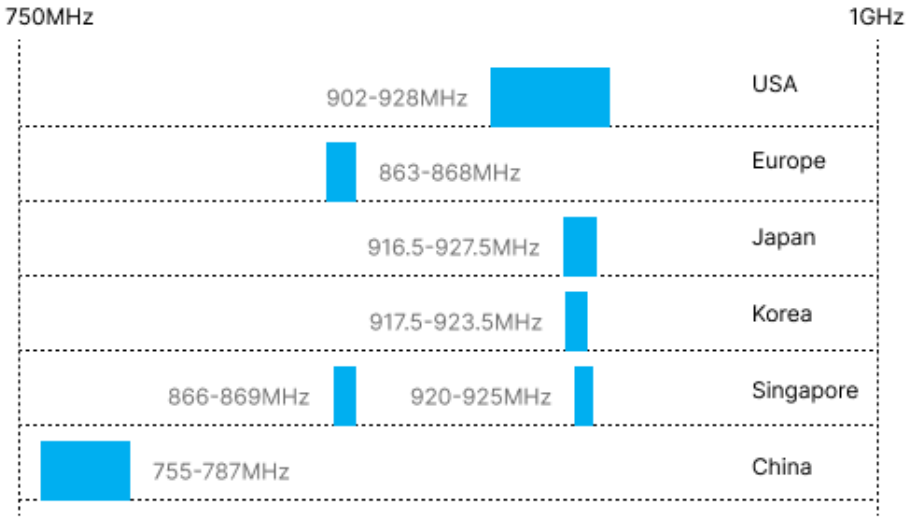
- 802.11ah (HaLow) standard in 2016
  - First real hardware in 2020
  - Hardware and dev kits available (Heltec makes one)
  - Unclear if there are real-world devices, but things are improving
- Focus on the indoor-to-outdoor scenario
  - Medium range (maximum 1 km, so expect 100s of meters)
- 915 MHz communication
  - **NOT** interoperable with other 802.11 access points and devices
- Theoretically up to 356 Mbps
  - Practically, most devices are expected to implement 150 kbps to 8 Mbps

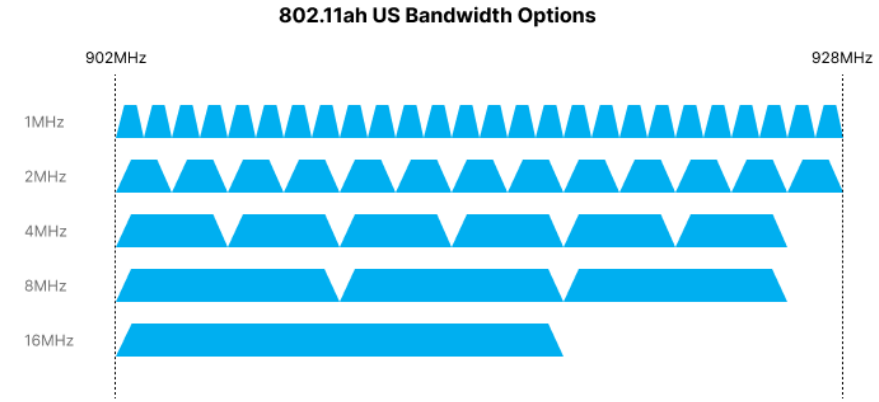
802.11ah allows multiple bandwidth allocations

- Expected throughput vs. coverage



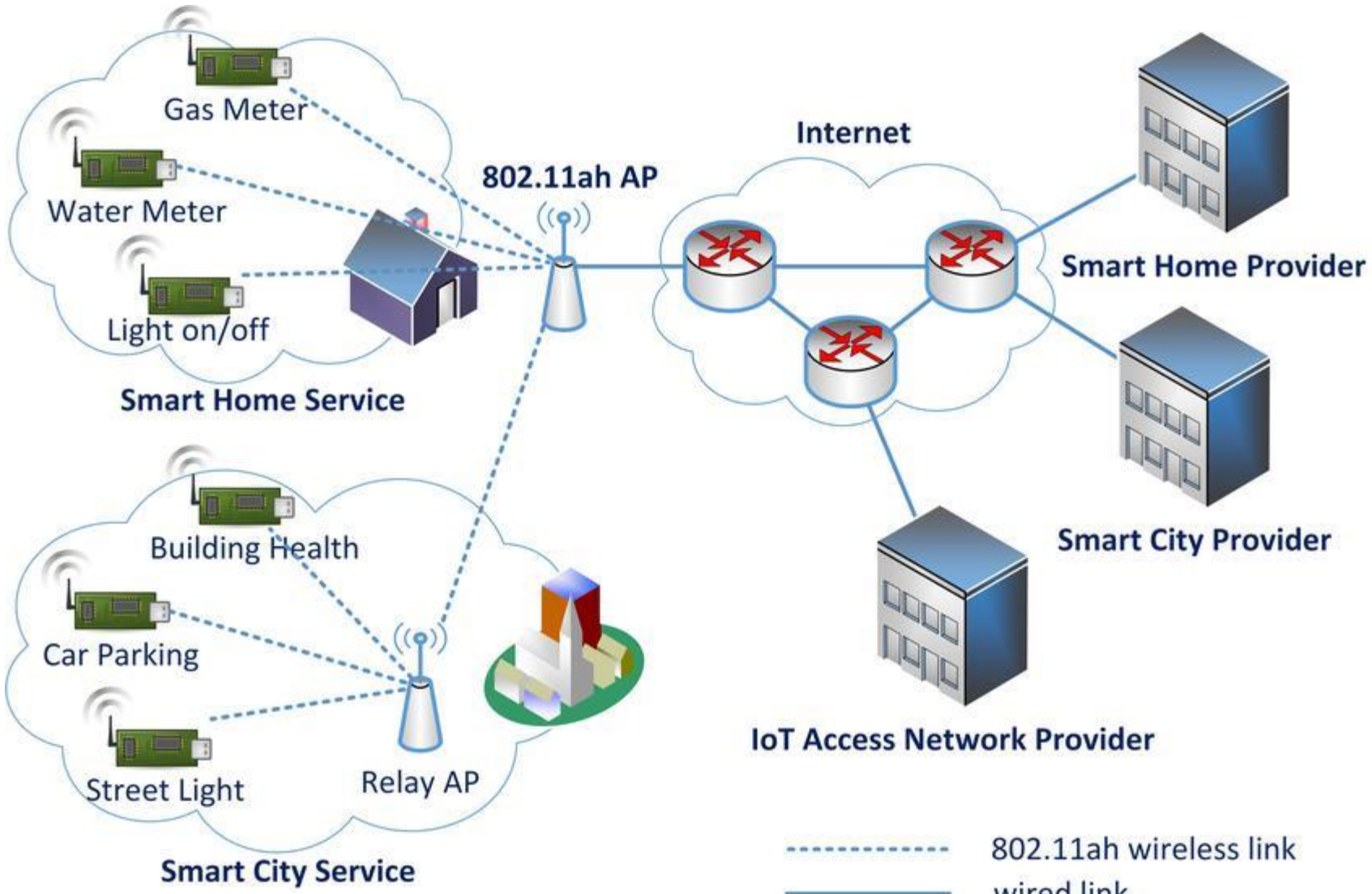
802.11ah frequency bands





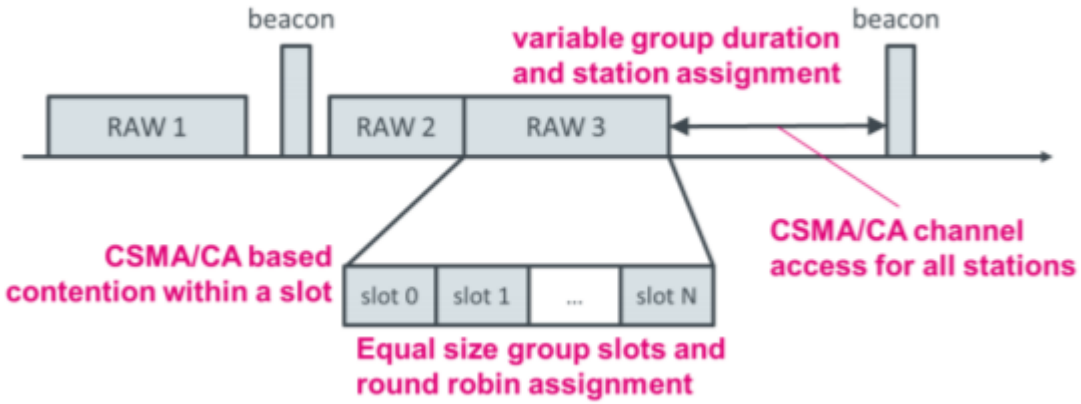
- Frequency and available bandwidth vary by region
  - 16 MHz allocation possible in US/China
  - 4 MHz max in Europe
- Given range, probably want more smaller allocations to avoid contention
  - Twenty-six 1 MHz bands up to 4 Mbps

HaLow Network Model



802.11ah architecture

- Star topology
  - Up to 8191 devices per access point



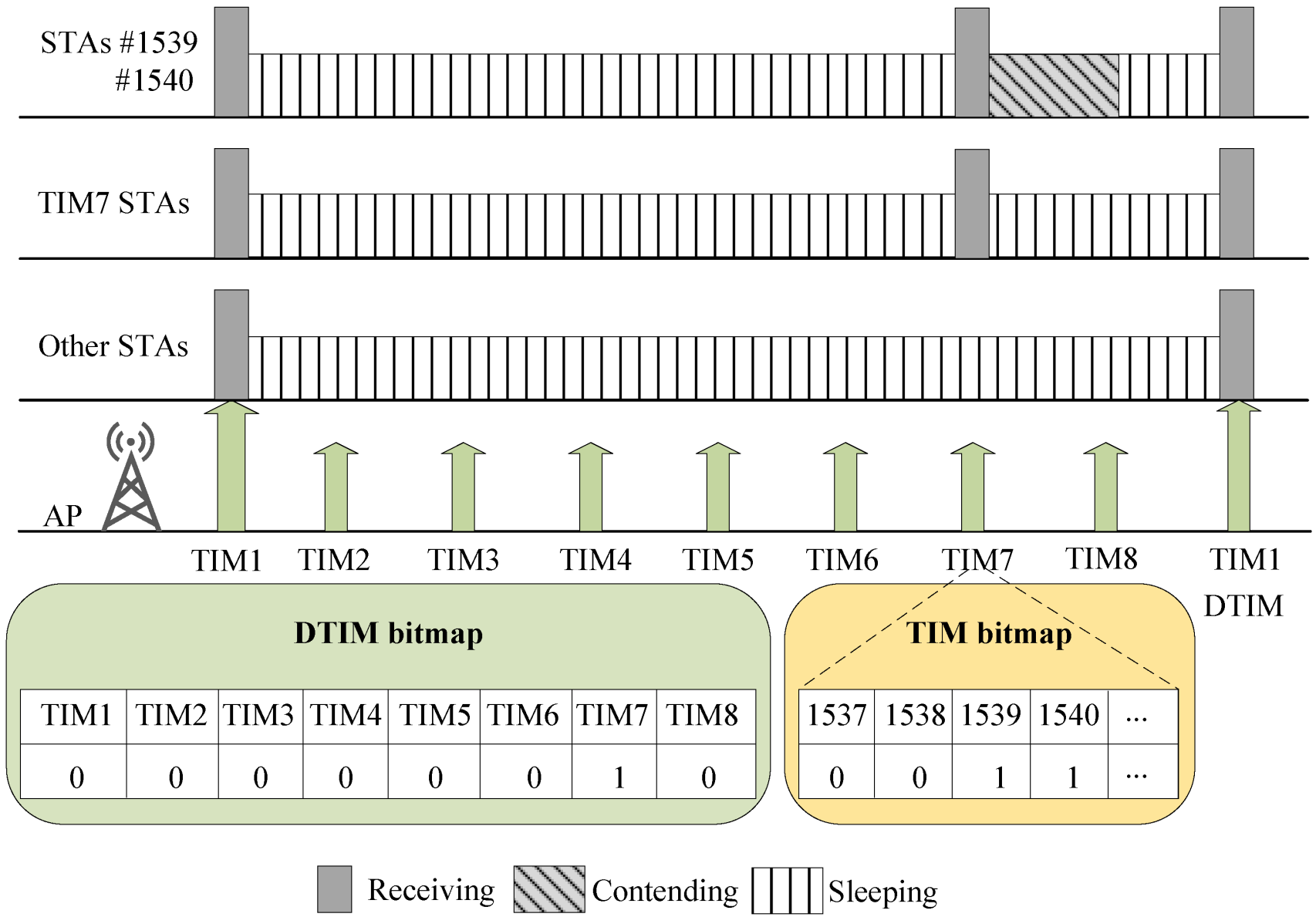
- Devices are assigned to a group
  - Groups are scheduled slots with TDMA
  - Within a slot CSMA/CA is used for contention among devices
  - Devices not in the group can sleep until their slot
  - Groups can be assigned by location to avoid hidden-terminal problem

- Traditional IP communication on top of that
  - And traditional 802.11 security mechanisms (WPA2/TLS)

Example group scheduling

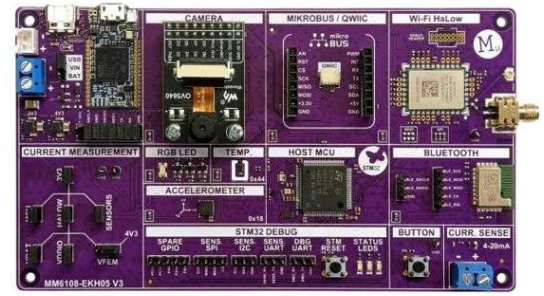
- For low-power communication, reduce the amount of time devices might need to listen

- Hierarchical
  - Entire groups are indicated if any traffic exists for any of them
  - Then additional indication of which device when that group starts



802.11ah hardware

- Morse Micro developer of HaLow radio chip
  - $30 for the MM6108 soc
  - Morse Micro dev board - $150



- Heltec sells hardware
  - 802.11ah access point - $80
  - Dev board with ESP32 + HaLow radio - $45
  - Radio module - $13
    - Built around MM6108
    - (not sure how it's so much cheaper…)

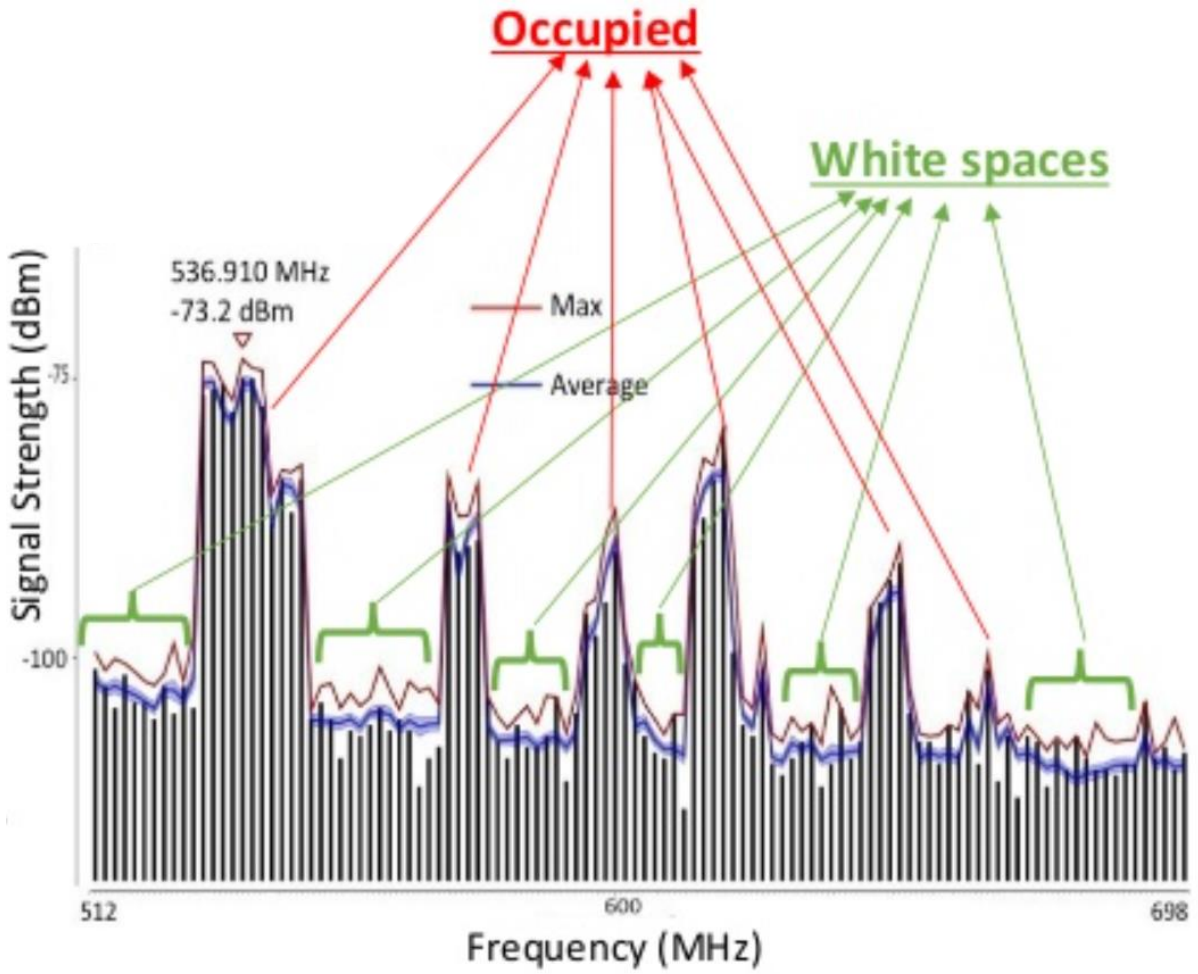
Outline

- Wide-Area Network Background

- **Unlicensed LPWANs**
  - LoRaWAN
  - Sigfox
  - 802.11ah
  - **TV Whitespaces**

TV whitespaces

- Unused TV channels between 54 MHz and 698 MHz
  - VHF (54-216 MHz)
  - UHF (470-698 MHz)
  - 6 MHz channel width
- Allocated but unused
  - FCC allows unlicensed use
  - **IF** you do not interfere with primary users



Sensing channel use

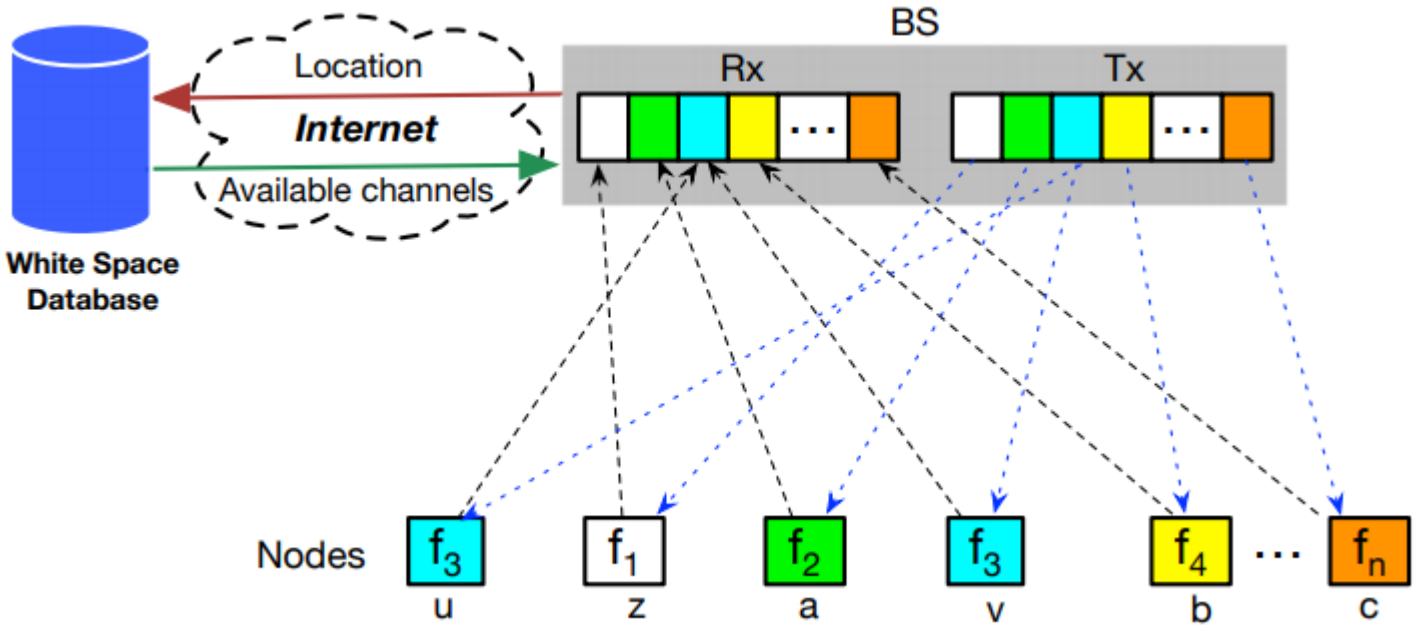
- Variation in use
  - Spatial: Cannot assume same channel will be free everywhere
  - Temporal: Cannot assume channel will be free at all times
- Cognitive radio approach
  - Dynamically identify unused portions of spectrum
- Database approach
  - Let someone else do the scanning. Consult database based on location and time

802.11af

- IEEE standard for whitespaces circa 2014
  - Not much (any?) use to date
- US/Canada-specific
  - Limits general-purpose product appeal
- Requires infrastructure about whitespace availability
  - People are figuring this out, but not really available yet
  - [n.b. very active area of research]

Sensor Networks Over tv Whitespaces (SNOW)

- A design for sensor networks over whitespaces
  - Base Station manages channel for deployment
  - Frequency division for devices. Each uplinks on separate subcarrier
  - Downlink is one OFDM transmission. Each device hears its frequency



Outline

- Wide-Area Network Background
- Unlicensed LPWANs
  - LoRaWAN
  - Sigfox
  - 802.11ah
  - TV Whitespaces