Lecture 14
Deep-Dive into LPWANs

CS397/497 – Wireless Protocols for IoT
Branden Ghena – Winter 2021

Northwestern

Today's Goals

- Overview of other unlicensed LPWAN approaches
  - Sigfox
  - 802.11ah
  - TV Whitespaces

- Discuss Cellular IoT protocols

- Deep-dive into challenges LPWANs face

Outline

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

- Cellular IoT

- LPWAN Challenges

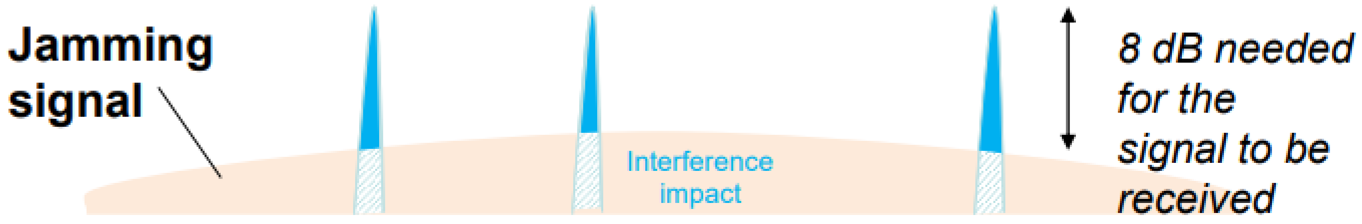
Sigfox

- 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 optimized 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

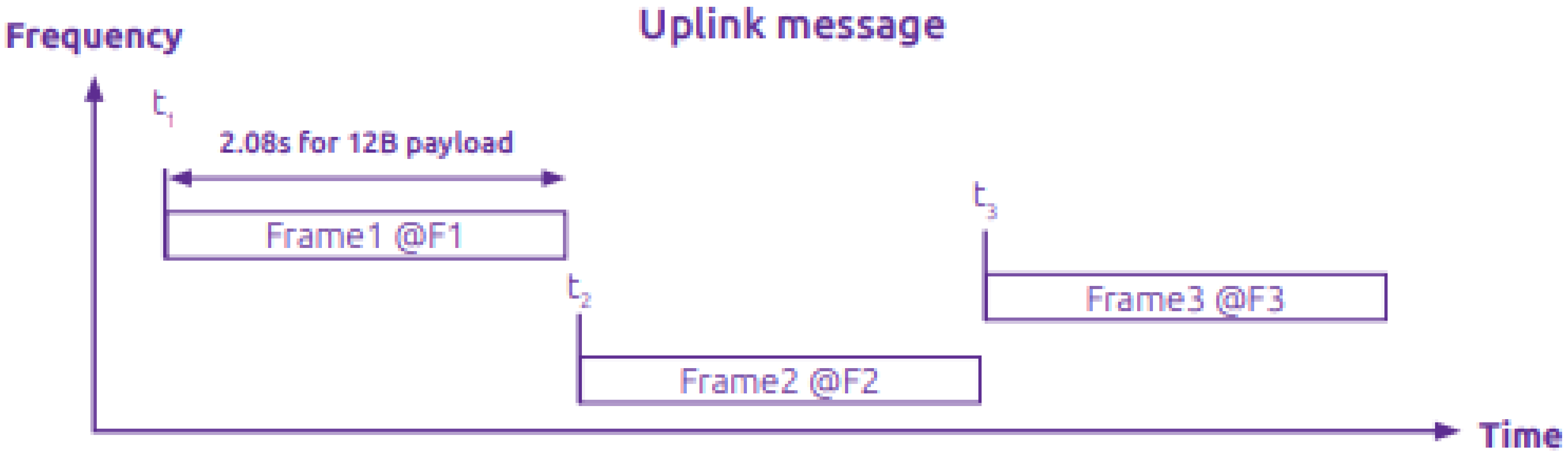
- Why transmit at 100-600 bps?
  - For greatly increased link budget

- Link budget: 150-160 dBm
  - Assuming Tx at ~20 dBm
  - Means Rx Sensitivity of -130 dBm (10 dBm better than LoRaWAN)

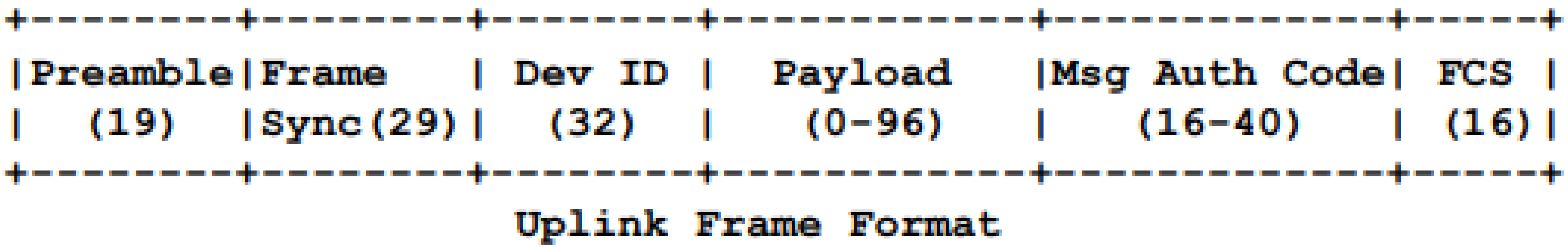
- Resulting range: 10-15 km in urban environments
  - Except that buildings lead to dead spots in range

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



```
+--------+---------+---------+-------------+--------------+-----+
|Preamble|Frame    | Dev ID  |   Payload   |Msg Auth Code| FCS |
|  (19)  |Sync(29)|  (32)   |   (0-96)    |    (16-40)   | (16)|
+--------+---------+---------+-------------+--------------+-----+
                    Uplink Frame Format
```

- Up to 29 bytes total per packet
  - Payload: up to **12 bytes** 😱

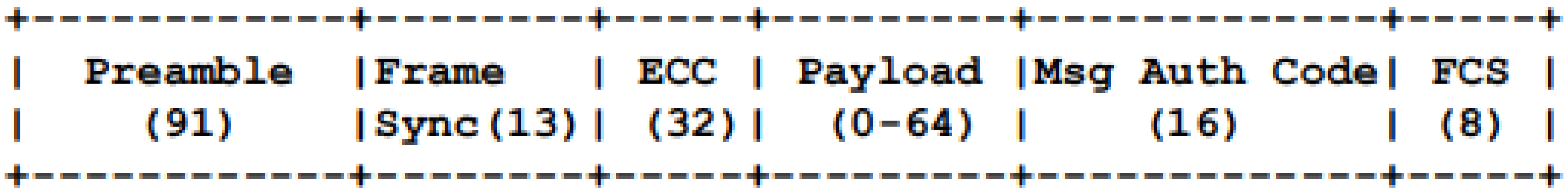
- Other fields
  - Preamble + Frame Sync are really a 6 byte field for radio sync
  - Authentication: 2-5 bytes
  - Frame Check Sequence: 16-bit CRC

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



```
+------------+--------+-----+---------+-------------+-----+
|  Preamble  |Frame   | ECC | Payload |Msg Auth Code| FCS |
|    (91)    |Sync(13)| (32)|  (0-64) |     (16)    | (8) |
+------------+--------+-----+---------+-------------+-----+
```

Downlink Frame Format

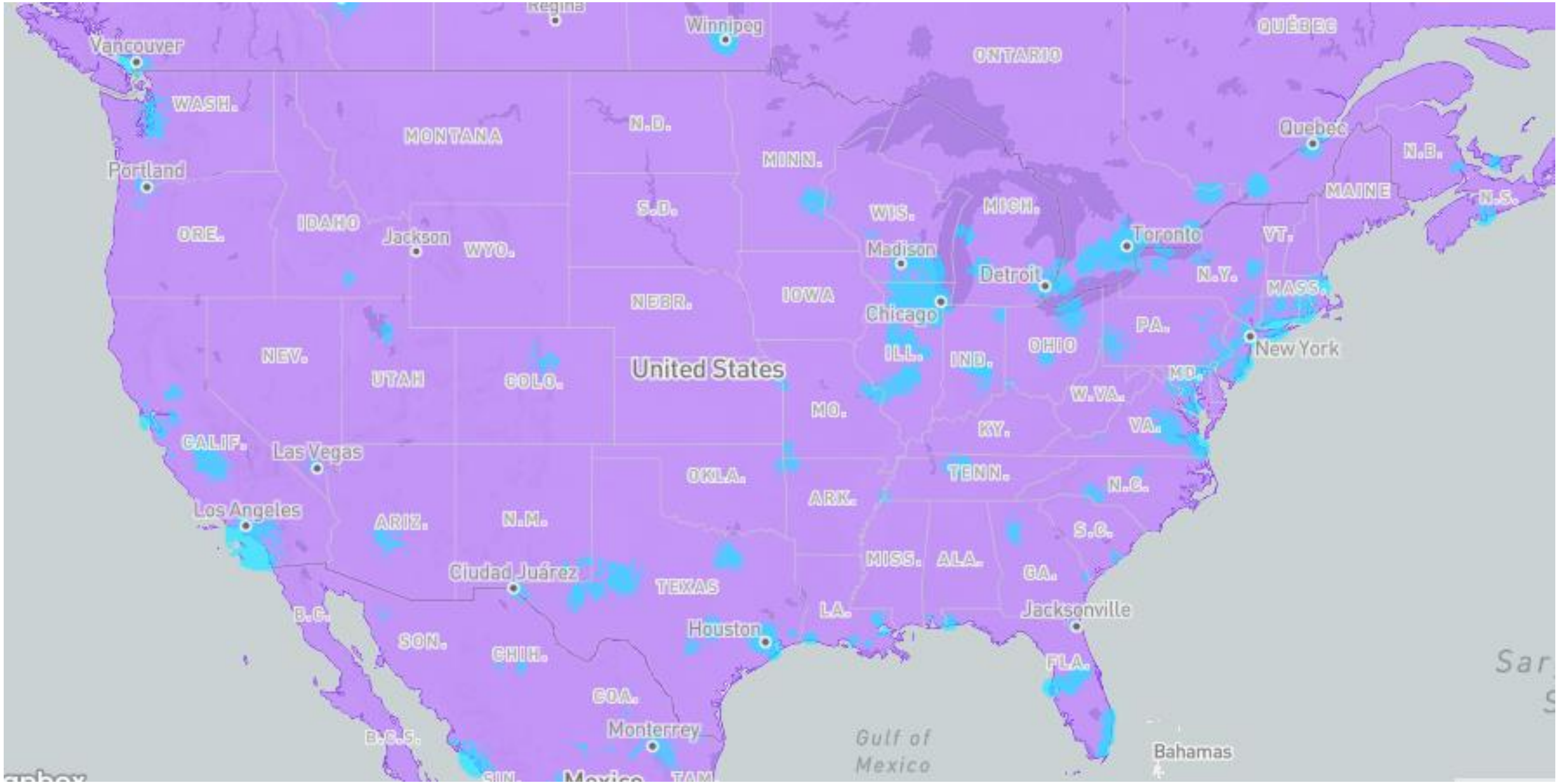
- Similar structure, 28 bytes total
  - Payload: up to 8 bytes
- Larger preamble + frame sync of 13 bytes
- Error Correcting Code for increased reliability

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 (Winter 2021)



Outline

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

- Cellular IoT

- LPWAN Challenges

IEEE standard for LPWANs

- 802.11ah (HaLow) standard in 2016
  - First real hardware in 2020
  - Still not in real-world use yet

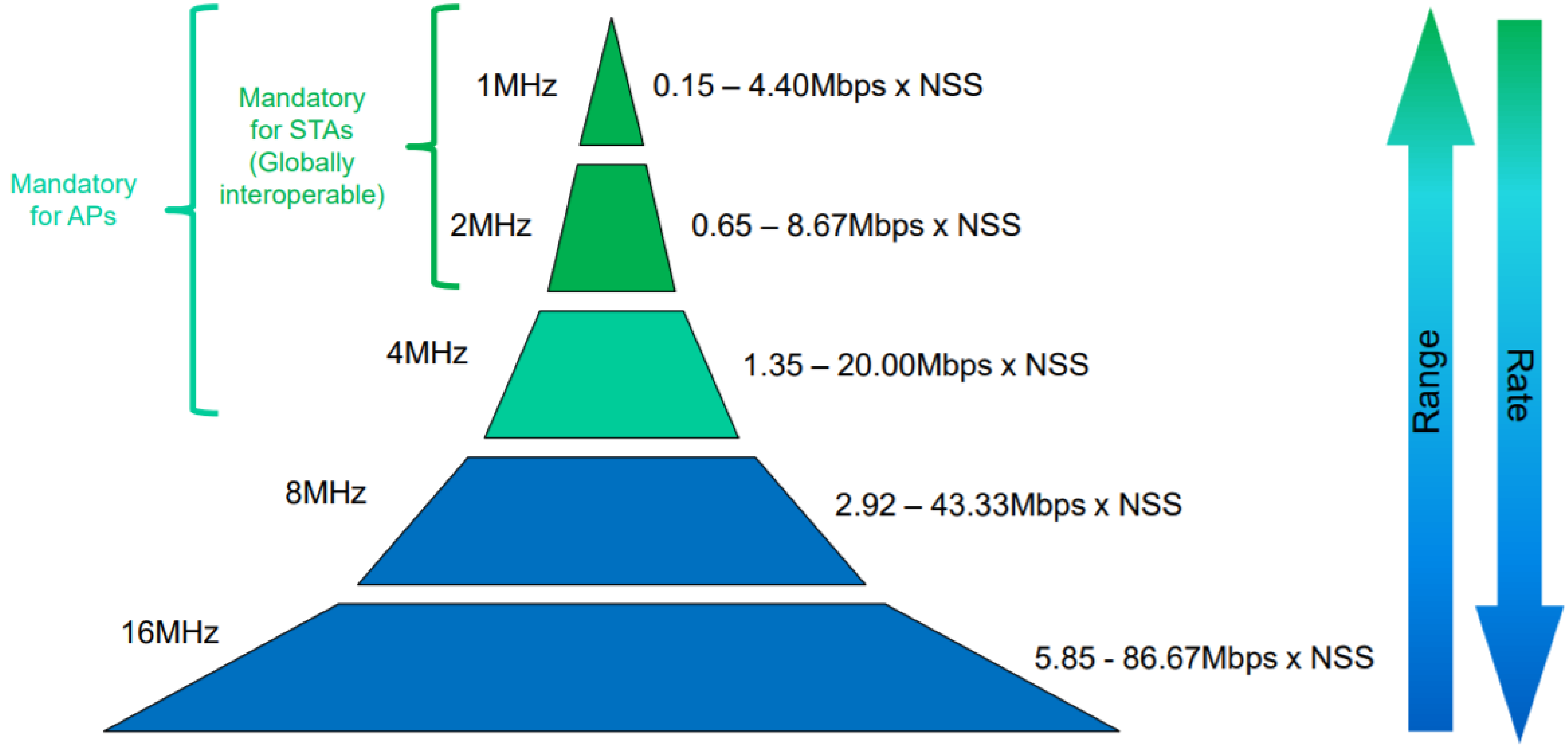
- Focus on the indoor-to-outdoor scenario
  - Medium range (maximum 1 km)

- 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



Mandatory for APs

Mandatory for STAs (Globally interoperable)

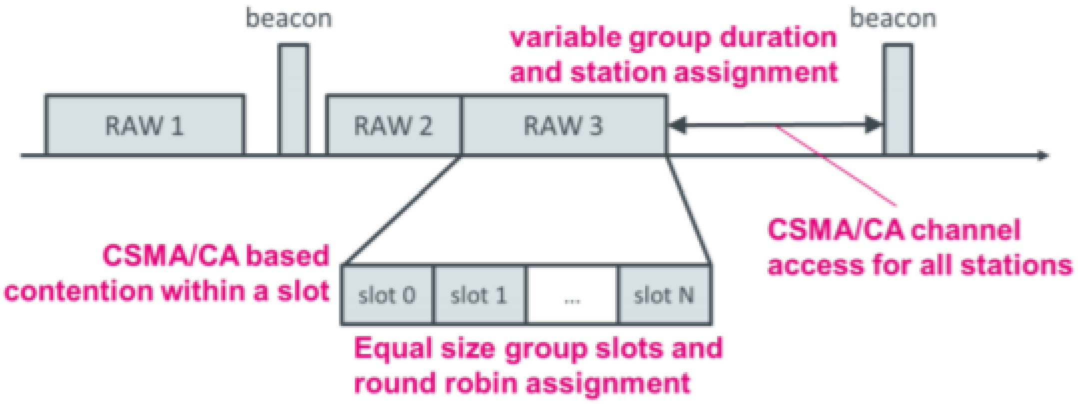
1MHz	0.15 – 4.40Mbps x NSS
2MHz	0.65 – 8.67Mbps x NSS
4MHz	1.35 – 20.00Mbps x NSS
8MHz	2.92 – 43.33Mbps x NSS
16MHz	5.85 - 86.67Mbps x NSS

Range

Rate

NSS = number of spatial streams

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

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

Outline

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

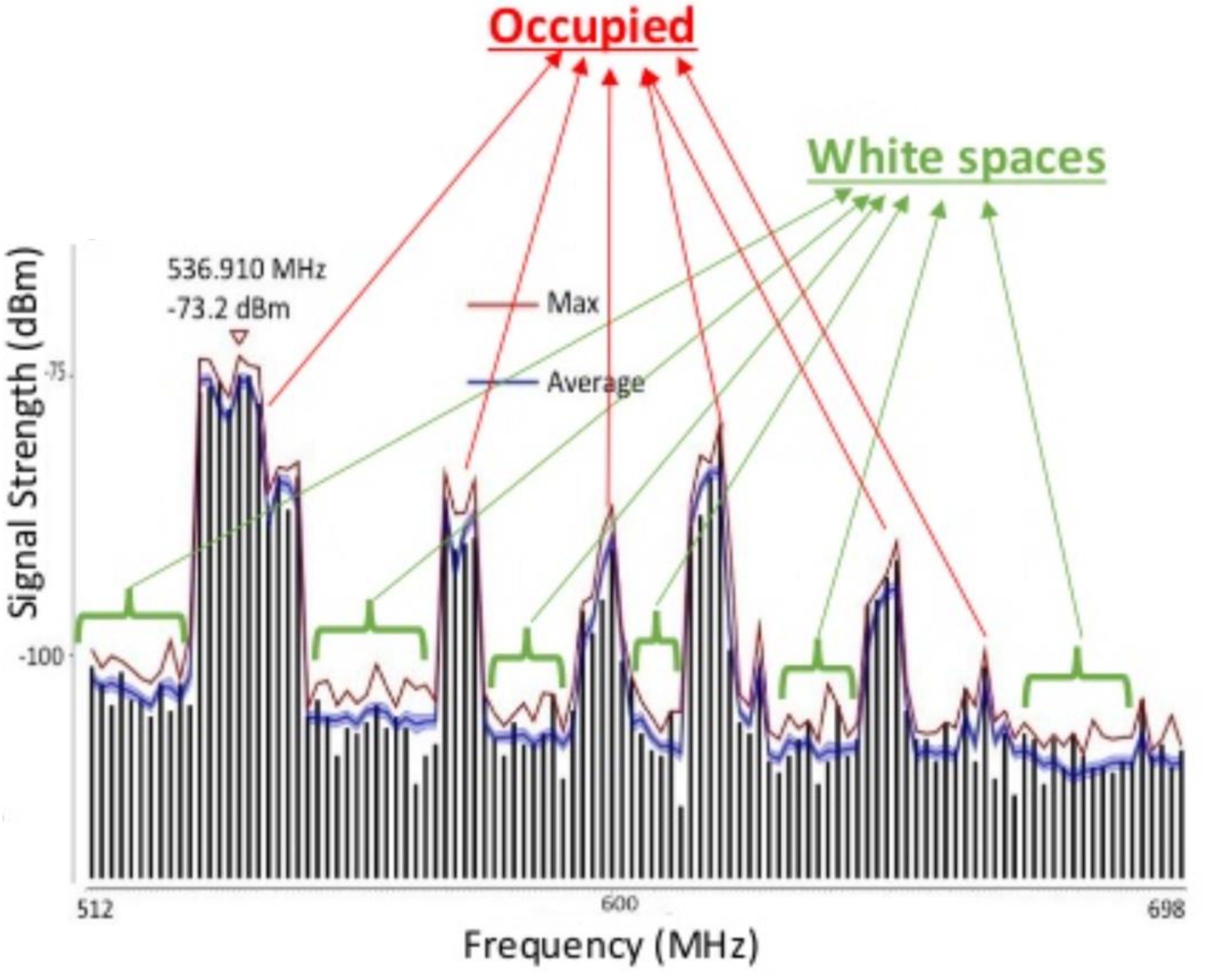
- Cellular IoT

- LPWAN Challenges

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

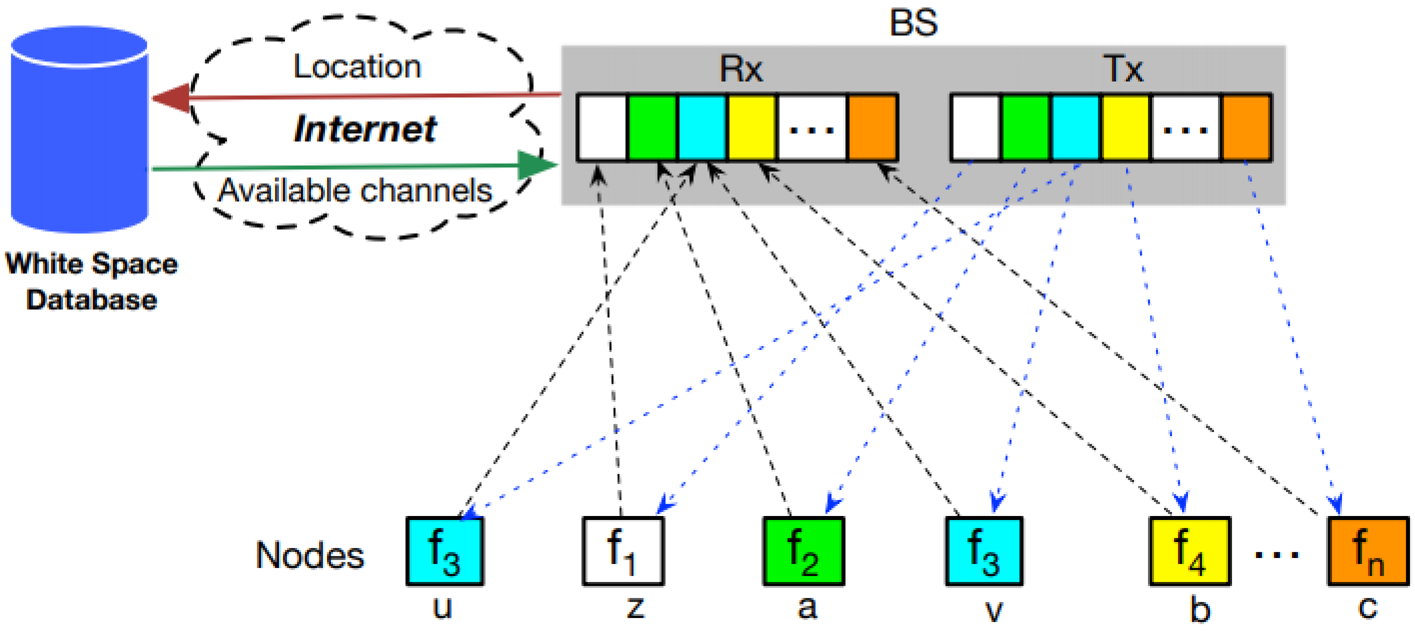
- Variation in use
  - Spatial: Cannot assume same channel will be free everywhere
  - Temporal: Cannot assume channel will be free at all times

- Cognitive radio approach
  - Dynamically identify unused portions of spectrum

- Database approach
  - Let someone else do the scanning. Consult database based on location and time

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

- Unlicensed LPWANs
  - Sigfox
  - 802.11ah
  - TV Whitespaces

- **Cellular IoT**

- LPWAN Challenges

3GPP

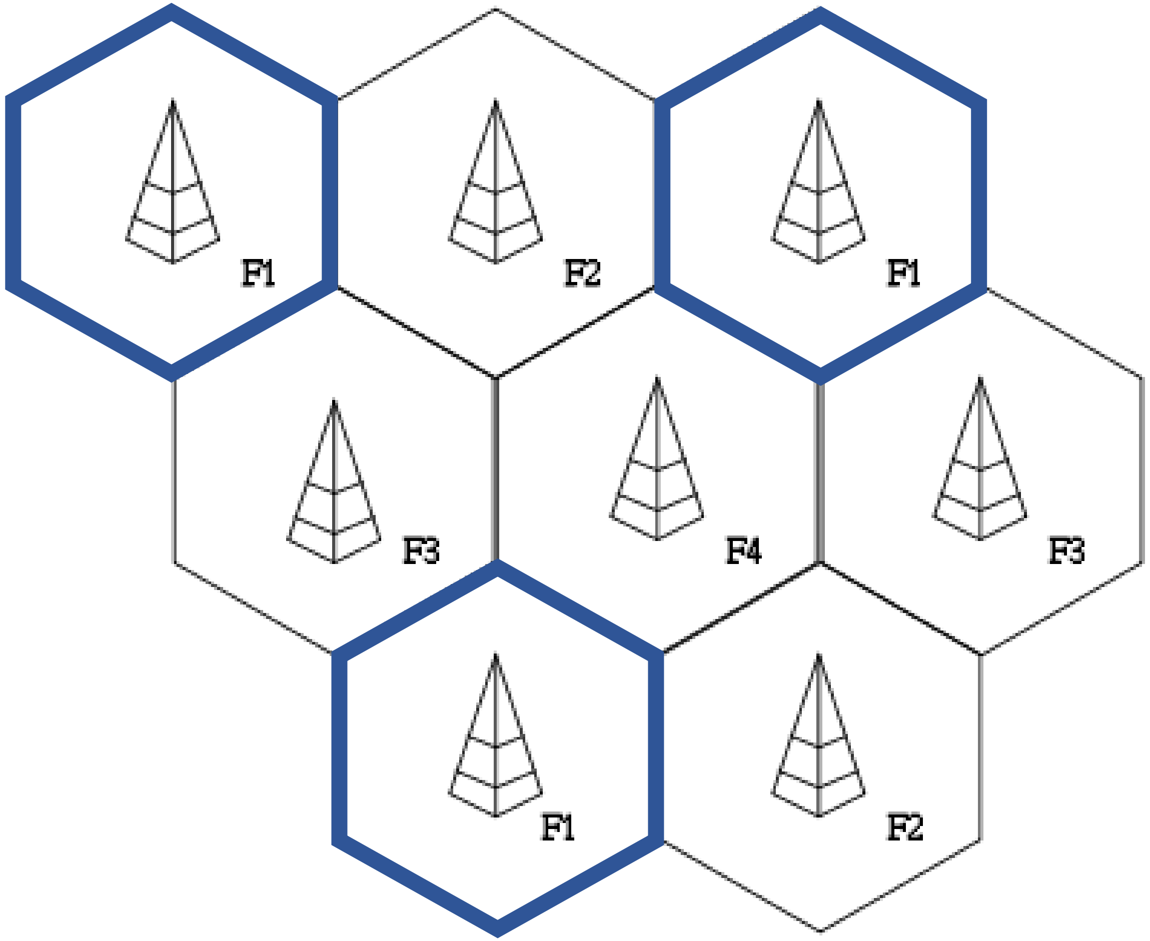
- 3rd Generation Partnership Project (3GPP)
  - Developed 3G, 4G, 5G

- Industry alliance for development of telecoms standards
  - Established around 1998
  - Makes “Releases” which are roughly analogous to IEEE standards/versions
    - Release 8 (2008) LTE ~4G
    - Release 15 (2018) NR (New Radio) ~5G

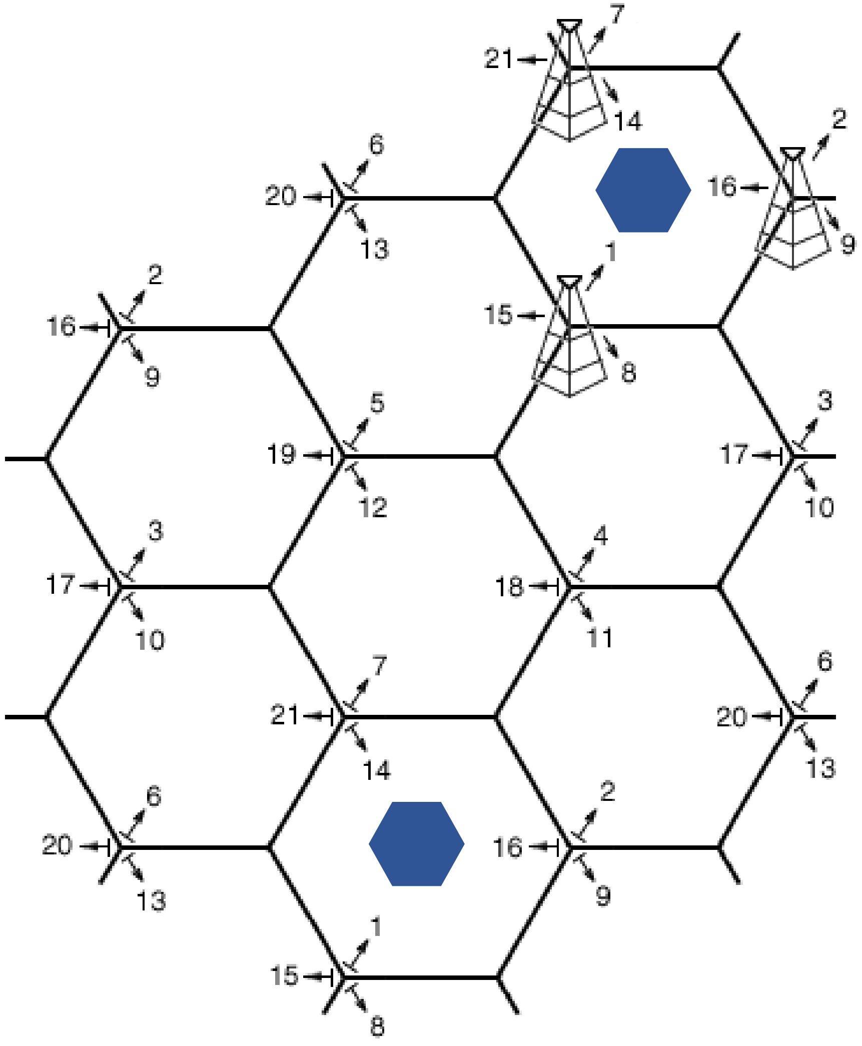
- Focused on the practical
  - Different group actually defined 4G (ITU). 3GPP made LTE

Cells in a cellular network

- Split a physical area into a number of non-overlapping cells
  - Each cell gets a cell tower and a frequency band assigned to it
  - Apply frequency bands so nearby cells use different frequencies

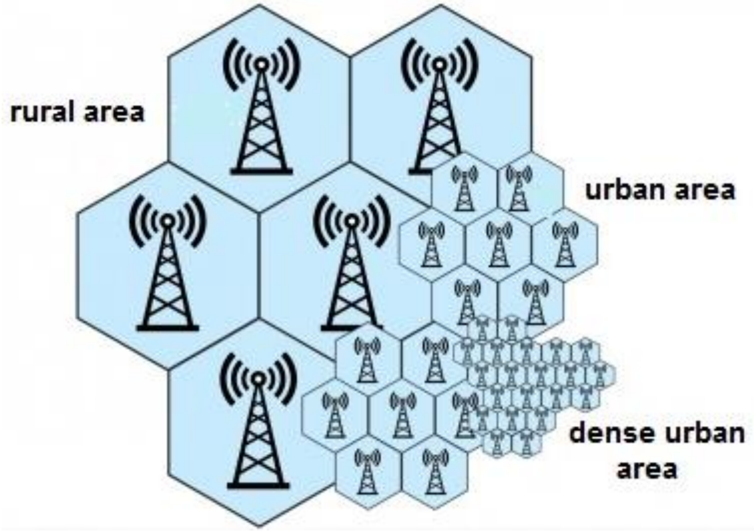


More complicated real-world cells



- Place towers at corners of cells
  - Directional antennas send three different frequency bands, one per cell
  - Each cell gets three tower and three bands

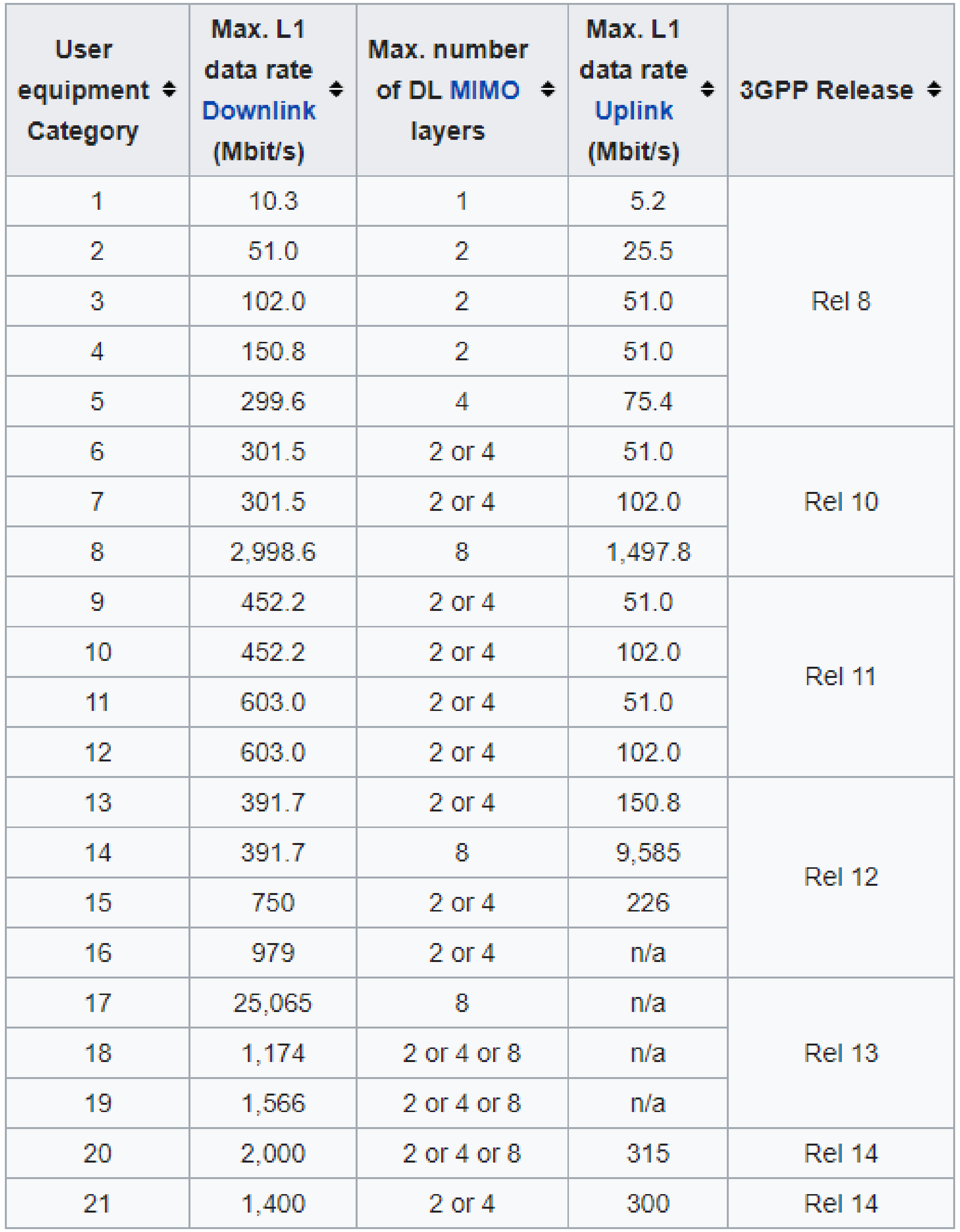
- Density of cells varies based on expected number of users
  - Change cell size using Power Control



LTE Categories

- Different equipment supports different “categories” of LTE
  - Maximum MCS index supported

- Examples
  - iPhone 6 (2015): Cat 4
  - Pixel 3 (2018): Cat 16



User equipment Category	Max. L1 data rate Downlink (Mbit/s)	Max. number of DL MIMO layers	Max. L1 data rate Uplink (Mbit/s)	3GPP Release
1	10.3	1	5.2	Rel 8
2	51.0	2	25.5	
3	102.0	2	51.0	
4	150.8	2	51.0	
5	299.6	4	75.4	
6	301.5	2 or 4	51.0	Rel 10
7	301.5	2 or 4	102.0	
8	2,998.6	8	1,497.8	
9	452.2	2 or 4	51.0	Rel 11
10	452.2	2 or 4	102.0	
11	603.0	2 or 4	51.0	
12	603.0	2 or 4	102.0	
13	391.7	2 or 4	150.8	Rel 12
14	391.7	8	9,585	
15	750	2 or 4	226	
16	979	2 or 4	n/a	
17	25,065	8	n/a	Rel 13
18	1,174	2 or 4 or 8	n/a	
19	1,566	2 or 4 or 8	n/a	
20	2,000	2 or 4 or 8	315	Rel 14
21	1,400	2 or 4	300	Rel 14

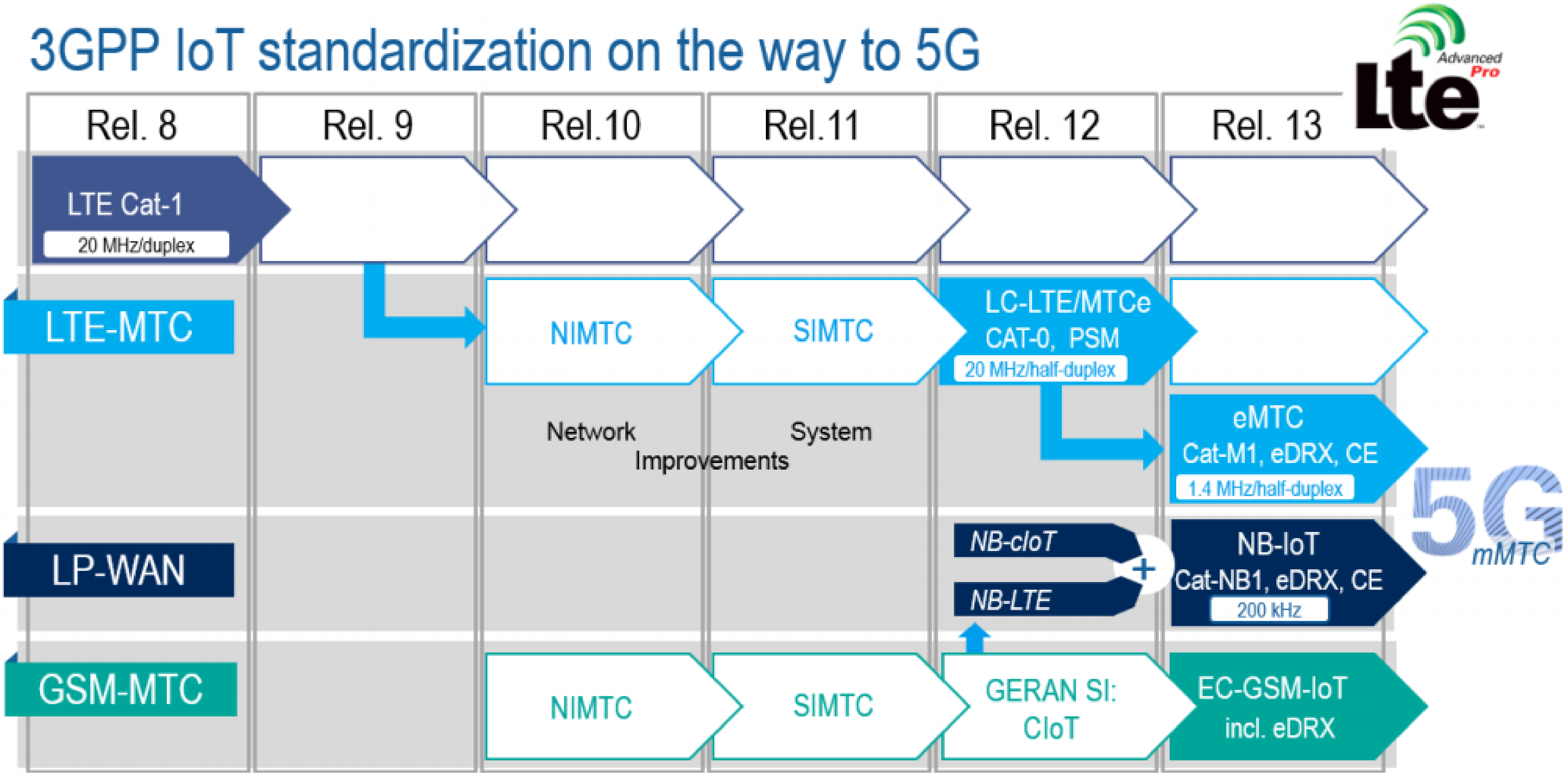
Additional low-end categories for IoT

- LTE Cat 0
  - Traditional LTE, but focused on the really low end

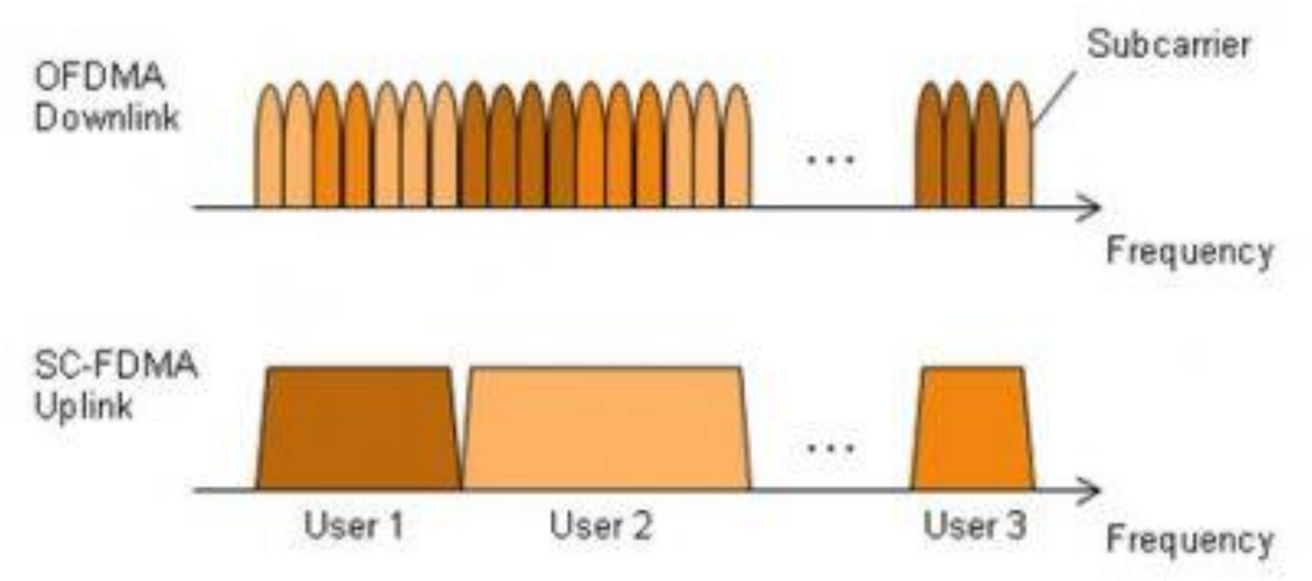
- LTE-M (LTE Cat M1)
  - 375 kbps uplink, 300 kbps downlink (for the actually implemented mode)
  - Reduced power and maximum bandwidth
  - Increased range

- NB-IoT (LTE Cat NB1)
  - 65 kbps uplink, 26 kbps downlink
  - Reduced power and greatly reduced bandwidth
  - Greatly increased range

LTE-M and NB-IoT were developed in parallel



LTE-M and NB-IoT downlink and uplink

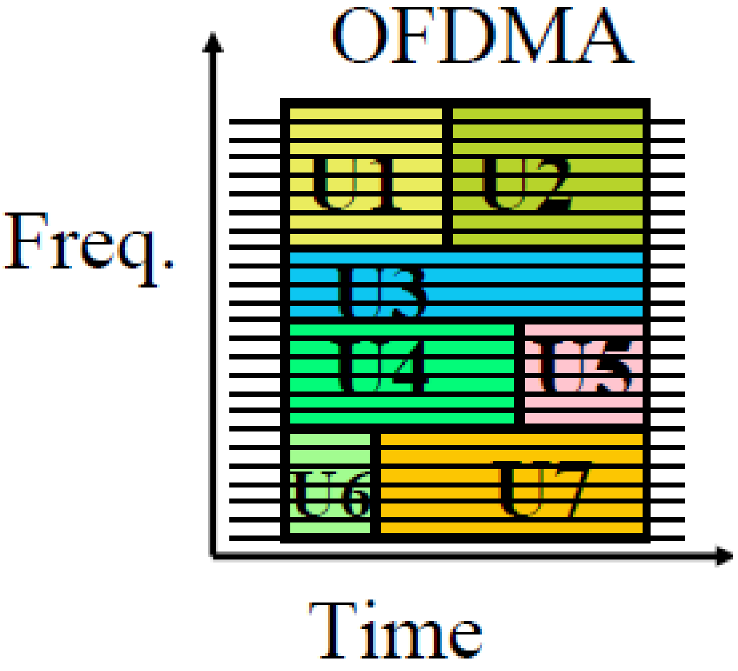


- OFDMA downlink
  - Put the more complicated hardware in the cell tower

- SC-FDMA (single carrier FDMA) uplink
  - Blocks of subchannels combined into one signal
  - Similar concept, but simpler for end devices to implement

LTE resource allocation

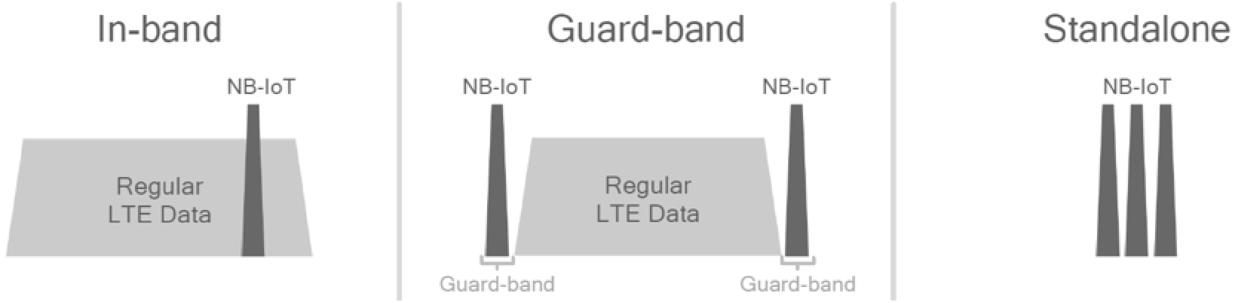
- Cellular uses OFDMA to schedule
  - Time + Frequency -> “2D Scheduling”
- Cellular uses single channels up to 20 MHz
  - Further divides these into 100 Resource Blocks
- Resource Block
  - 12 subcarriers for OFDM in frequency (15 kHz each)
  - 7 symbols in time (0.5 ms)
    - Remember, better modulation can pack many bits into a symbol
- Devices are allocated frequency and time based on what they are sending
  - Allocated in units of Resource Blocks



Resources used by LTE-M and NB-IoT

- LTE-M uses up to 6 resource blocks
  - 1.4 MHz of bandwidth (1.080 MHz)
  - Can co-exist with other normal LTE traffic, scheduled by cell tower
  - Limited to only some capability of LTE

- NB-IoT uses up to 1 resource block
  - 200 kHz of bandwidth (180 kHz)
  - Multiple deployment options
    - Guard-band in practice



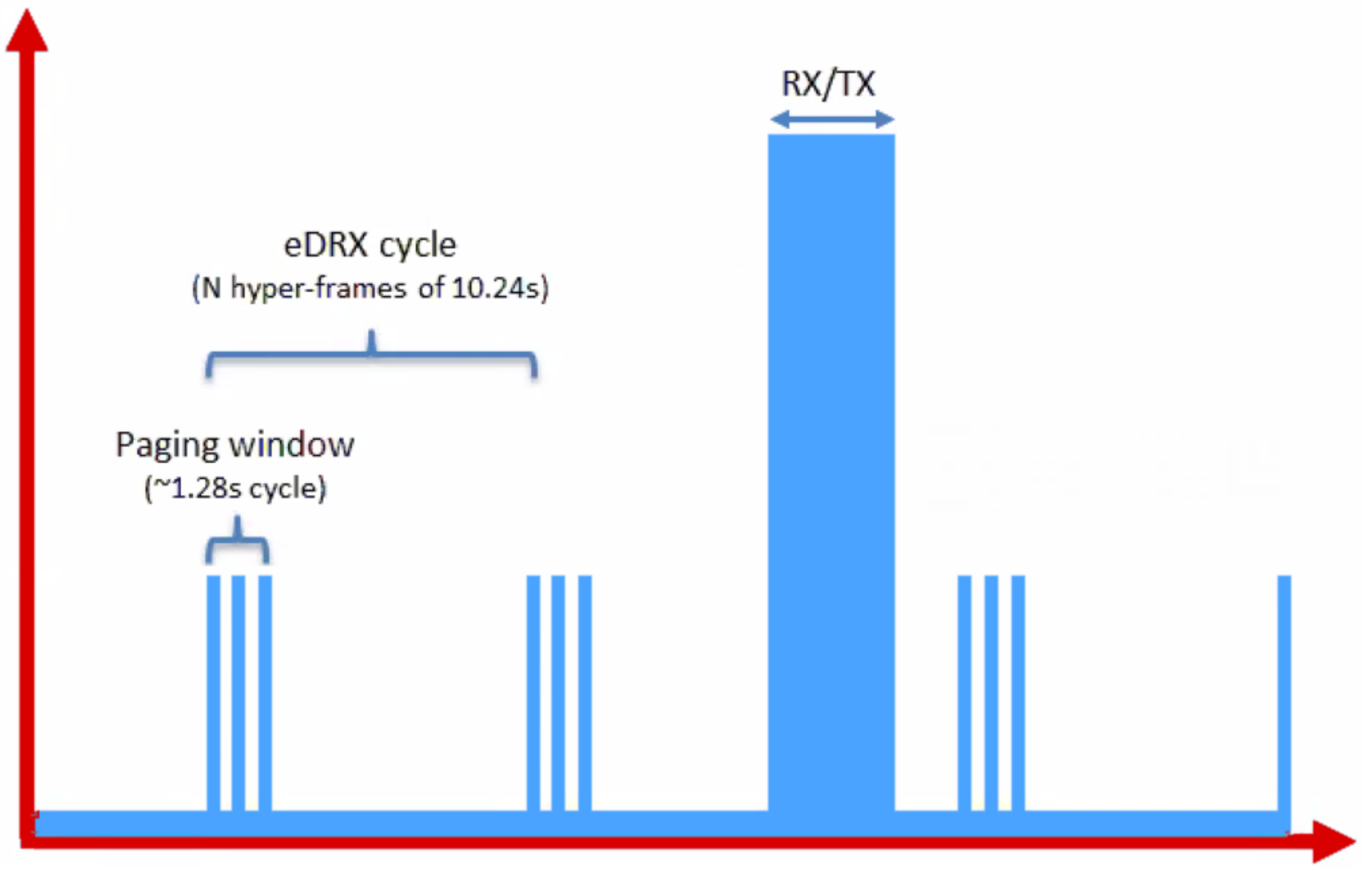
Utilizing single resource block (180kHz) within an LTE carrier

Utilizing unused resource blocks within an LTE carrier guard-band

Utilizing stand-alone 200 kHz carrier

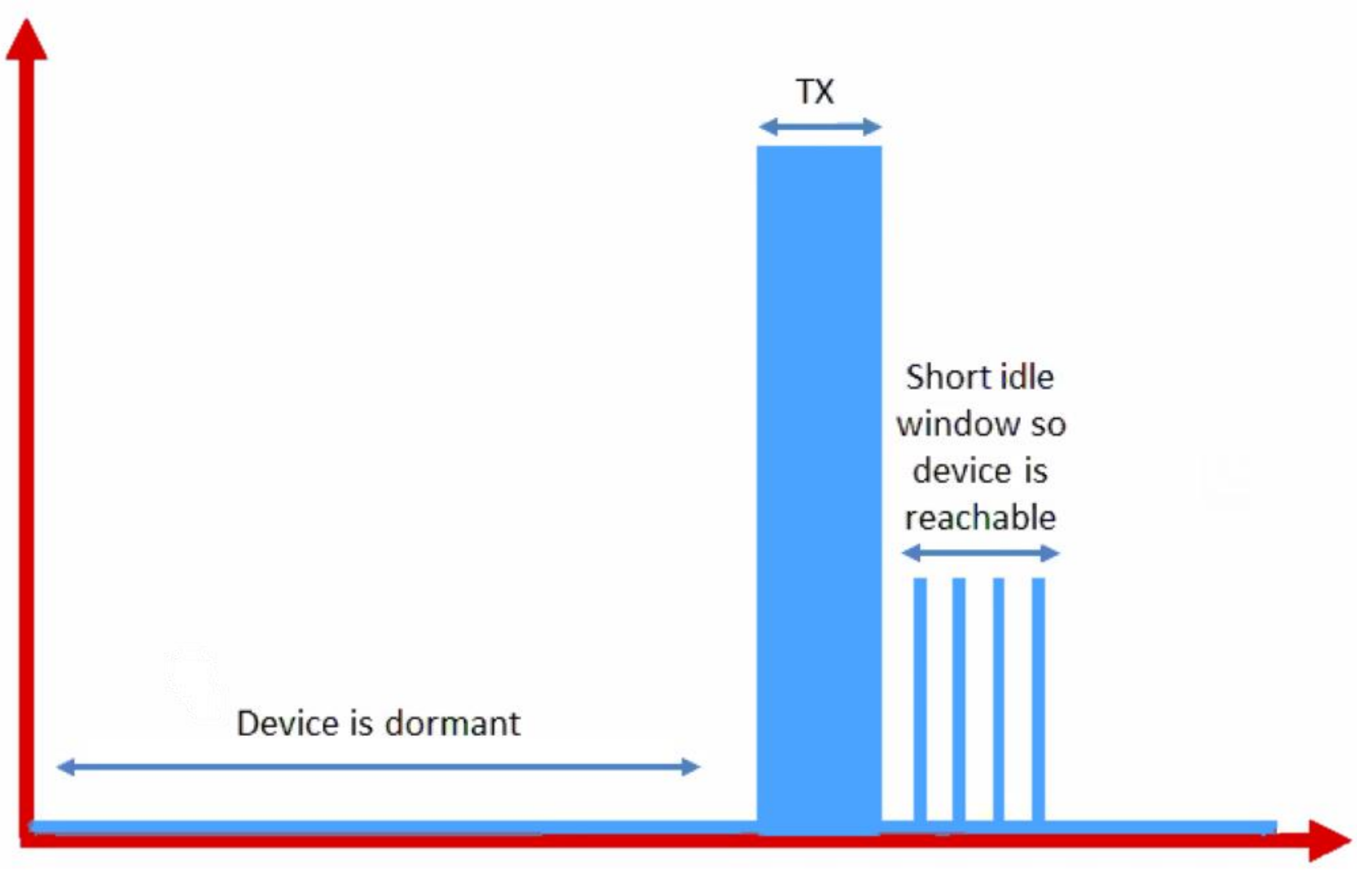
Reducing power for IoT devices

- Reduce maximum Tx power to 20 dBm
  - Increased receive sensitivity will cover it
- Extended Discontinuous Reception
  - Allow devices to reduce paging period and still stay on network
  - Cell tower will hold messages



Further power reduction for simple devices

- Power Saving Mode
  - For very simple, uplink-focused devices allow them to turn off entirely but stay connected
  - Minutes to days in duration
  - Notify tower before sleeping, listen for packets after each transmission



Improved range for LTE-M and NB-IoT

- LTE defines a Maximum Coupling Loss (MCL) a.k.a Link Budget
  - Traditional cellular: 144 dB (~2.5 km)
  - LTE-M: 160 dB (~5 km)
  - NB-IoT: 164 dB (~10 km)

  - Sigfox: ~155 dB
  - LoRaWAN: ~143 dB

- Note that cellular networks are on higher frequencies
  - Example: 1900 GHz

Cellular deployments

- Originally unclear which would be dominant
  - Verizon and AT&T focused on LTE-M
  - T-Mobile focused on NB-IoT
  - All rolled out services nationwide in the 2018-2019 timeframe

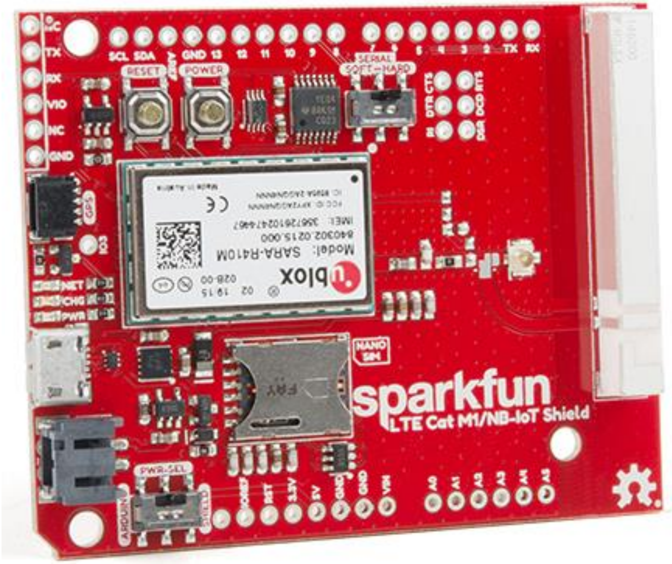
- Networks are expanding to provide both capabilities
  - LTE-M: AT&T, T-Mobile, US Cellular, Verizon
  - NB-IoT: AT&T, T-Mobile

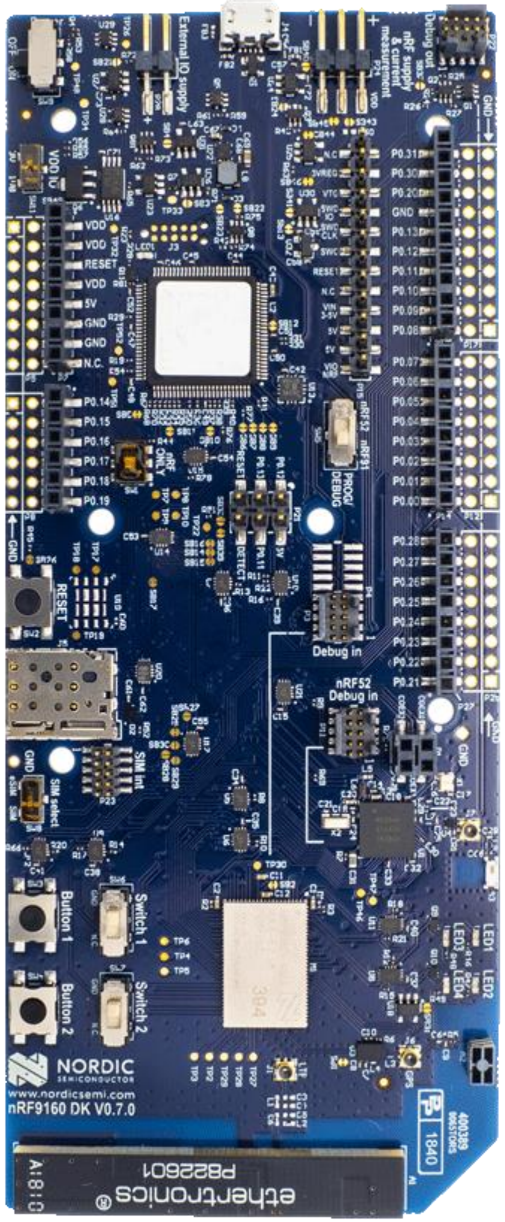
- Pricing models still very uncertain
  - NB-IoT example: $5 per device per year up to 12 MB, 10 packets per hour
  - Future adoption will greatly depend on these

Microcontroller support

- Devices need to be certified
  - Hardware and software
  - Tend to be modules or dual-core systems

- Add a SIM card to connect to network





Outline

- Unlicensed LPWANs
    - Sigfox
    - 802.11ah
    - TV Whitespaces
- Cellular IoT
- **LPWAN Challenges**

Do novel networks meet application needs?

- How do we compare varied requirements and capabilities?
  - Networks have throughput per gateway and range of gateway.
  - Applications have throughput per device and deployment area.

- Each gateway must support throughput for all devices in its coverage area.
  - Deployment areas are often wider than a single gateway’s range.

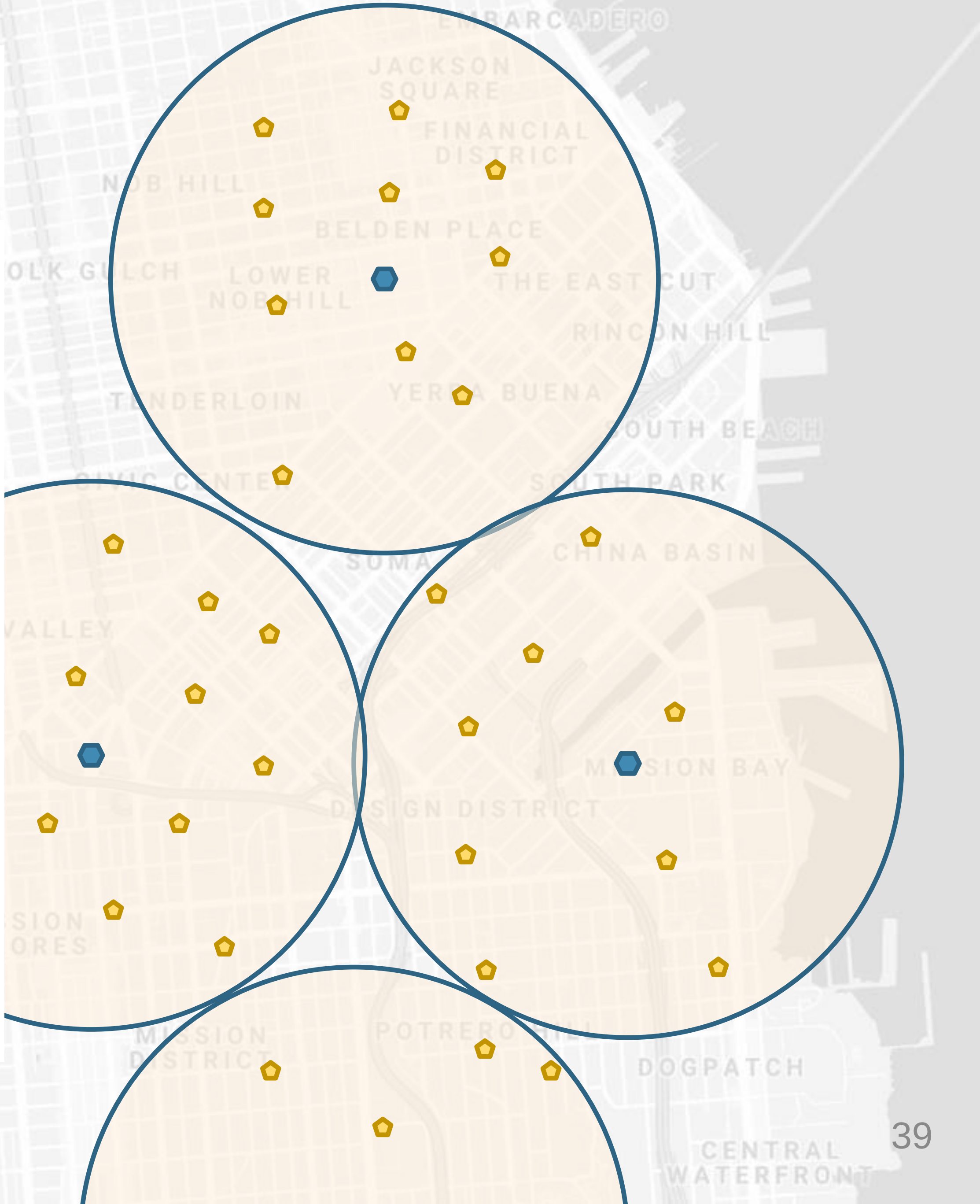
- Solution: compare the density of communication.
  - Data communication rate per unit area.

New metric for wide-area communication.

Our proposed metric: **bit flux**

- $$bit\ flux = \frac{network\ throughput}{coverage\ area}$$
- Units: bit per hour / m^2
- First suggested by Mark Weiser

Branden Ghena, et al. "Challenge: Unlicensed LPWANs Are Not Yet the Path to Ubiquitous Connectivity." *MobiCom'19*

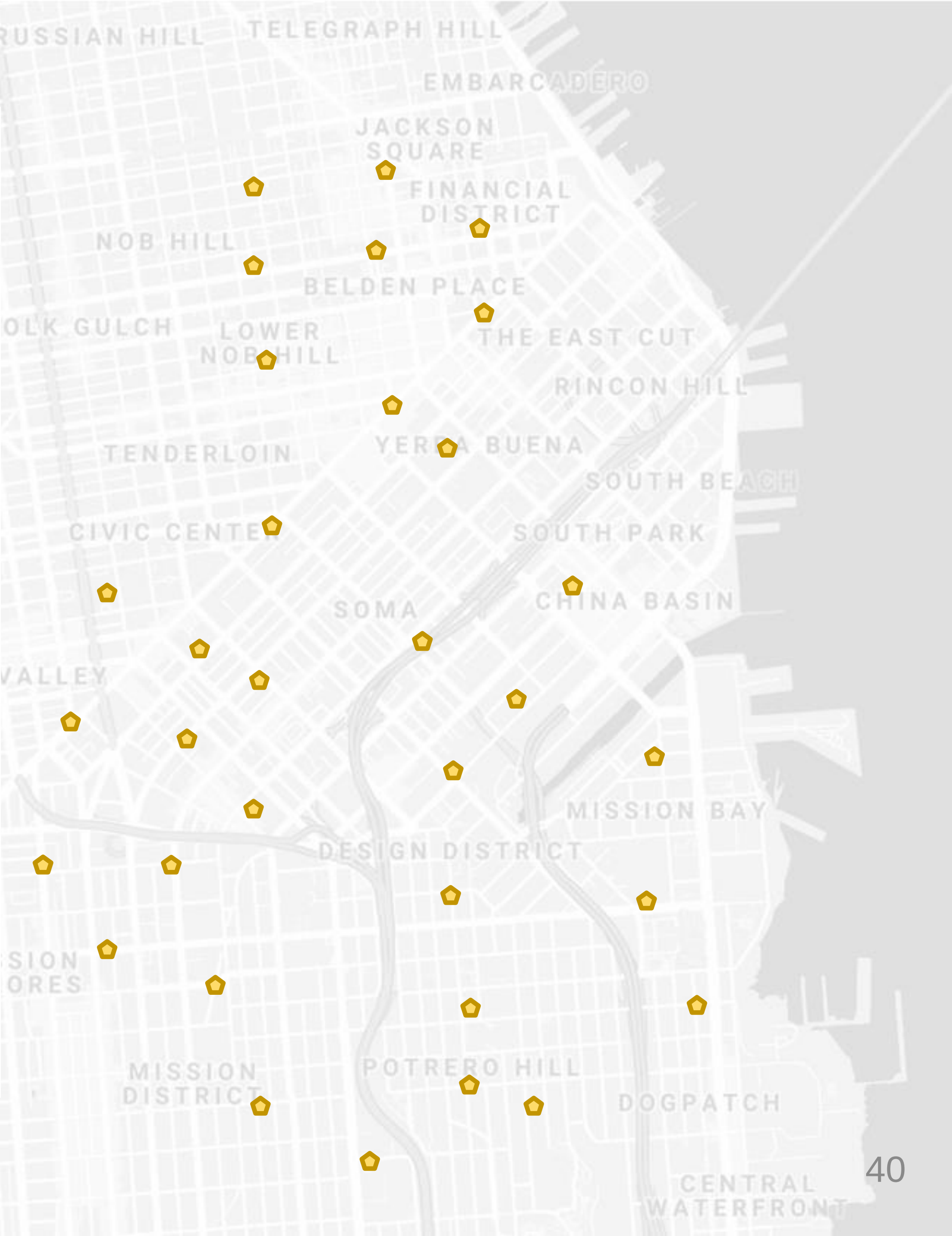


Bit flux can measure application needs.

For an application:

$$bit\ flux = \frac{\sum each\ device's\ uplink}{deployment\ area}$$

- Assumes a relatively homogeneous distribution.

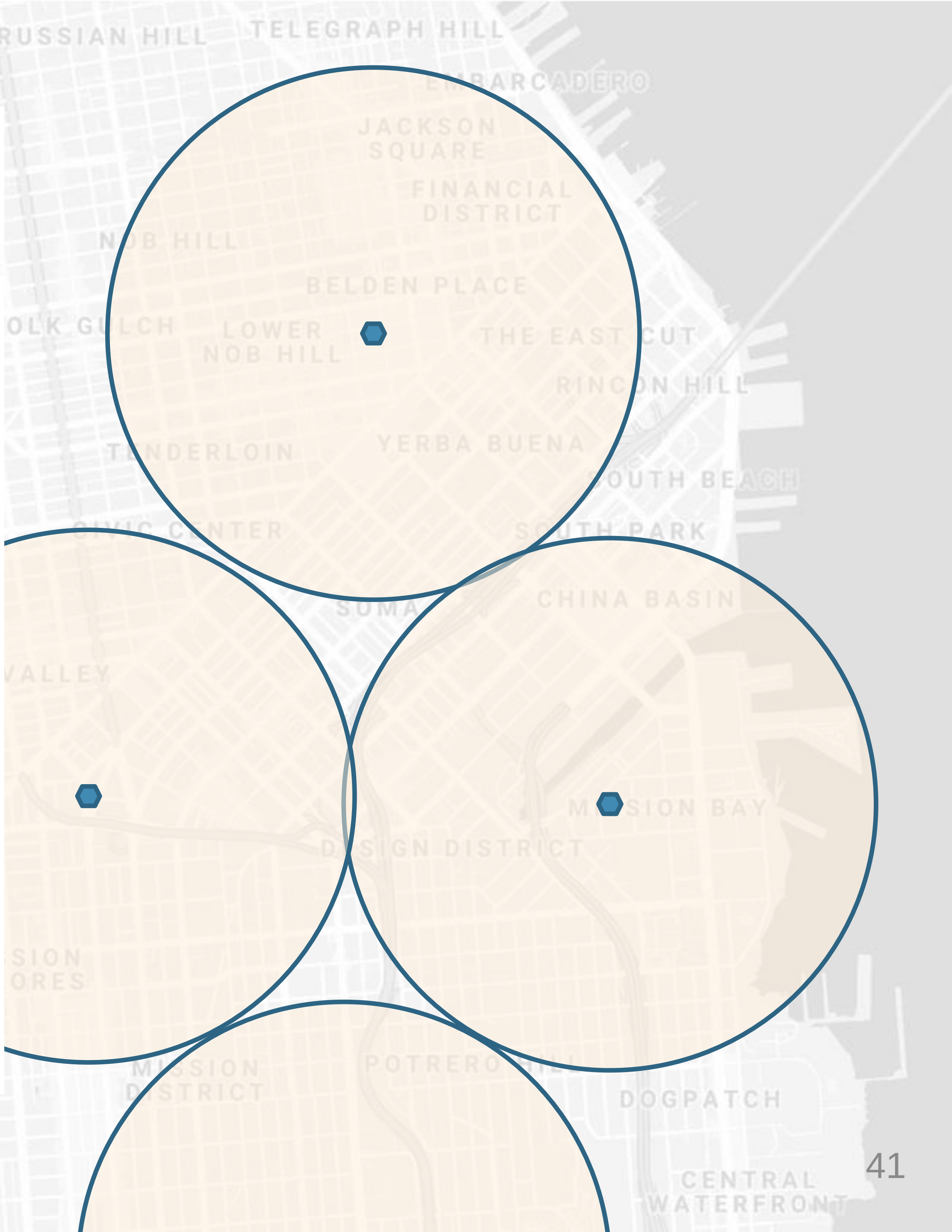


Bit flux can measure network capabilities.

For a network:

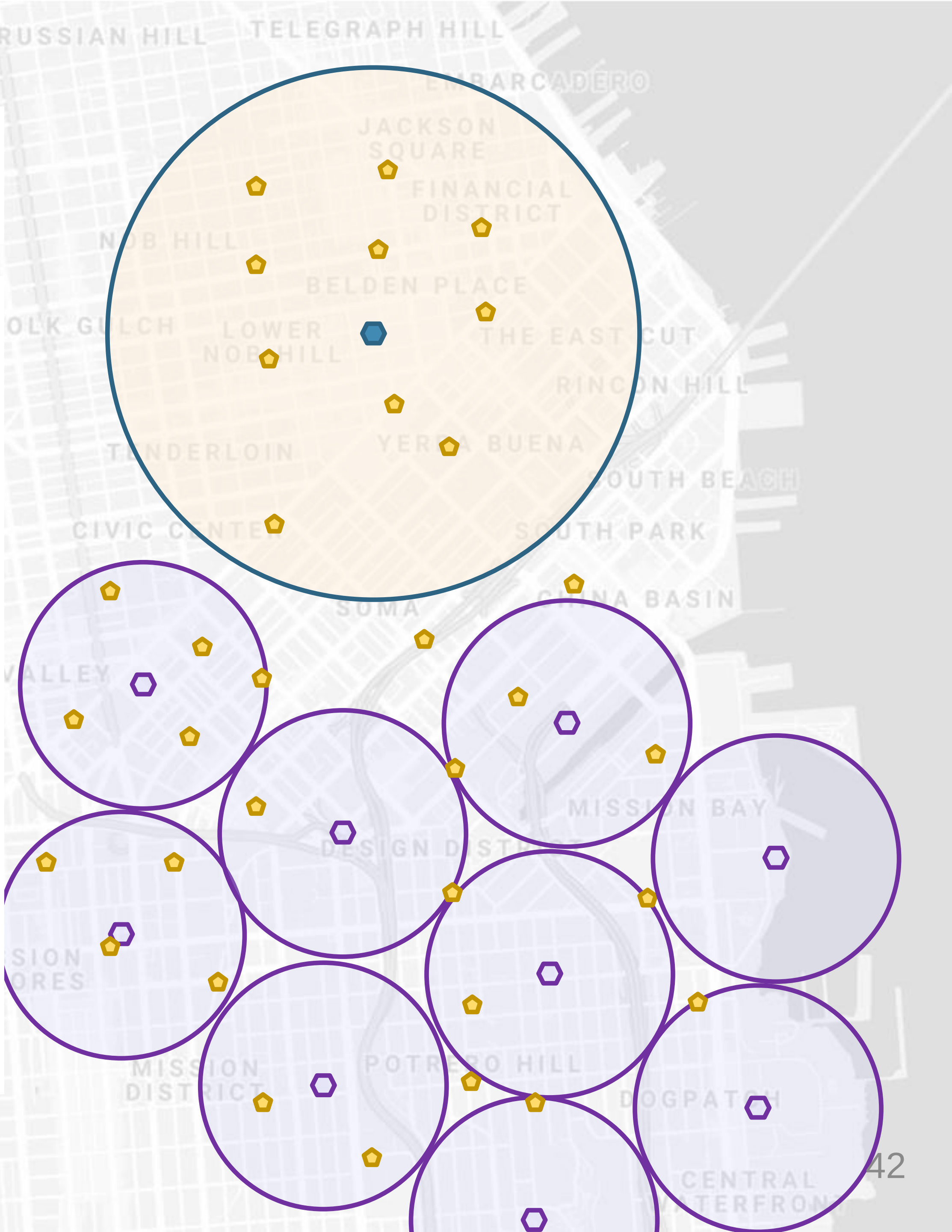
$$bit\ flux = \frac{gateway\ goodput}{gateway\ coverage\ area}$$

- Assumes a non-overlapping deployment of gateways.
- Note that bit flux alone ignores the total number of gateways required.

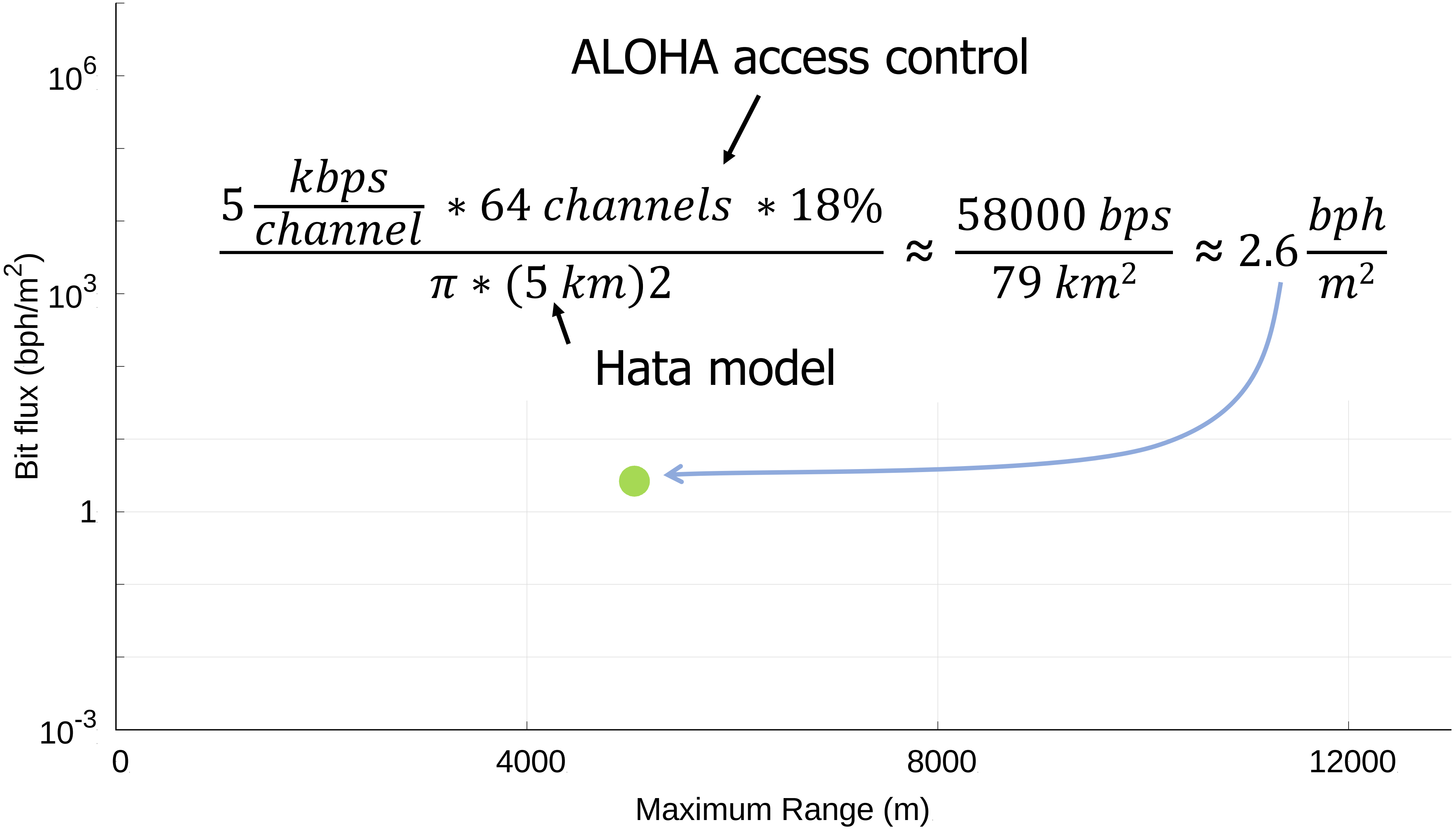


Bit flux accounts for spatial reuse.

- Reducing coverage area and deploying additional gateways improves capacity.
- $bit\ flux \uparrow = \dfrac{gateway\ goodput}{coverage\ area \downarrow}$



Bit flux measurement for LoRaWAN.

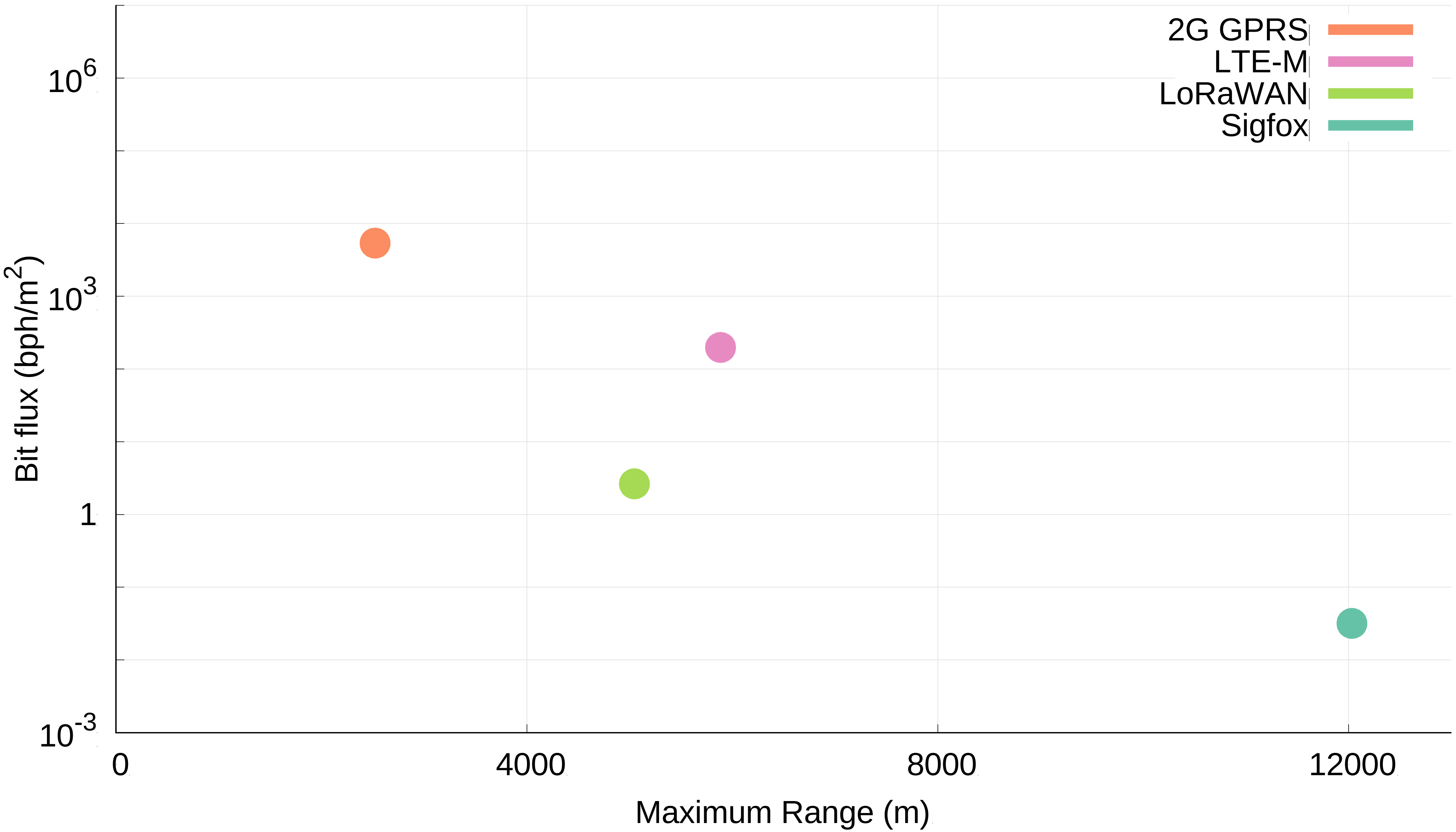


ALOHA access control

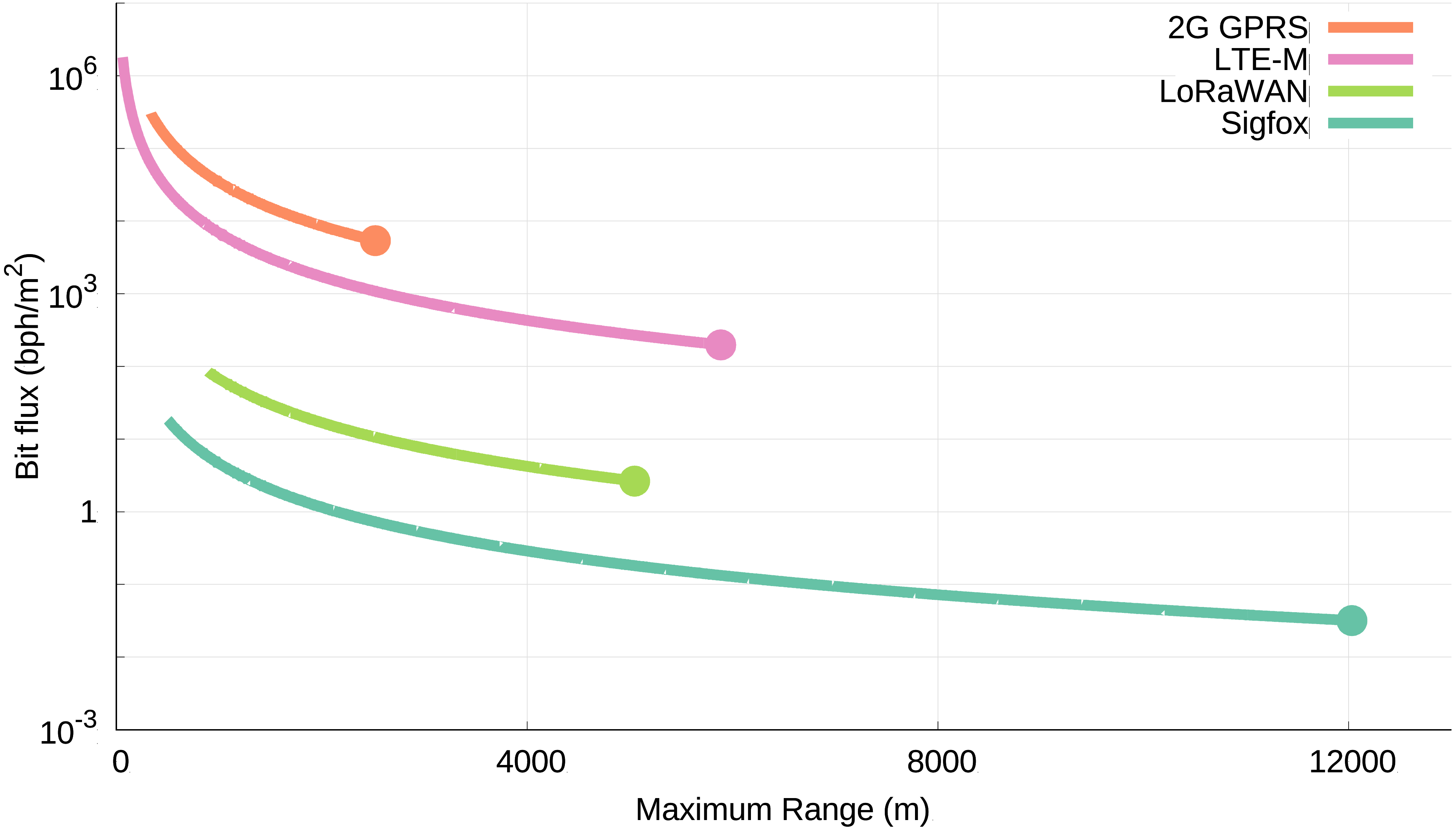
$$\frac{5\,\frac{kbps}{channel} * 64\ channels * 18\%}{\pi * (5\ km)2} \approx \frac{58000\ bps}{79\ km^2} \approx 2.6\,\frac{bph}{m^2}$$

Hata model

Networks differ in capability by orders of magnitude.



Range reduction results in a bit flux curve for each network.



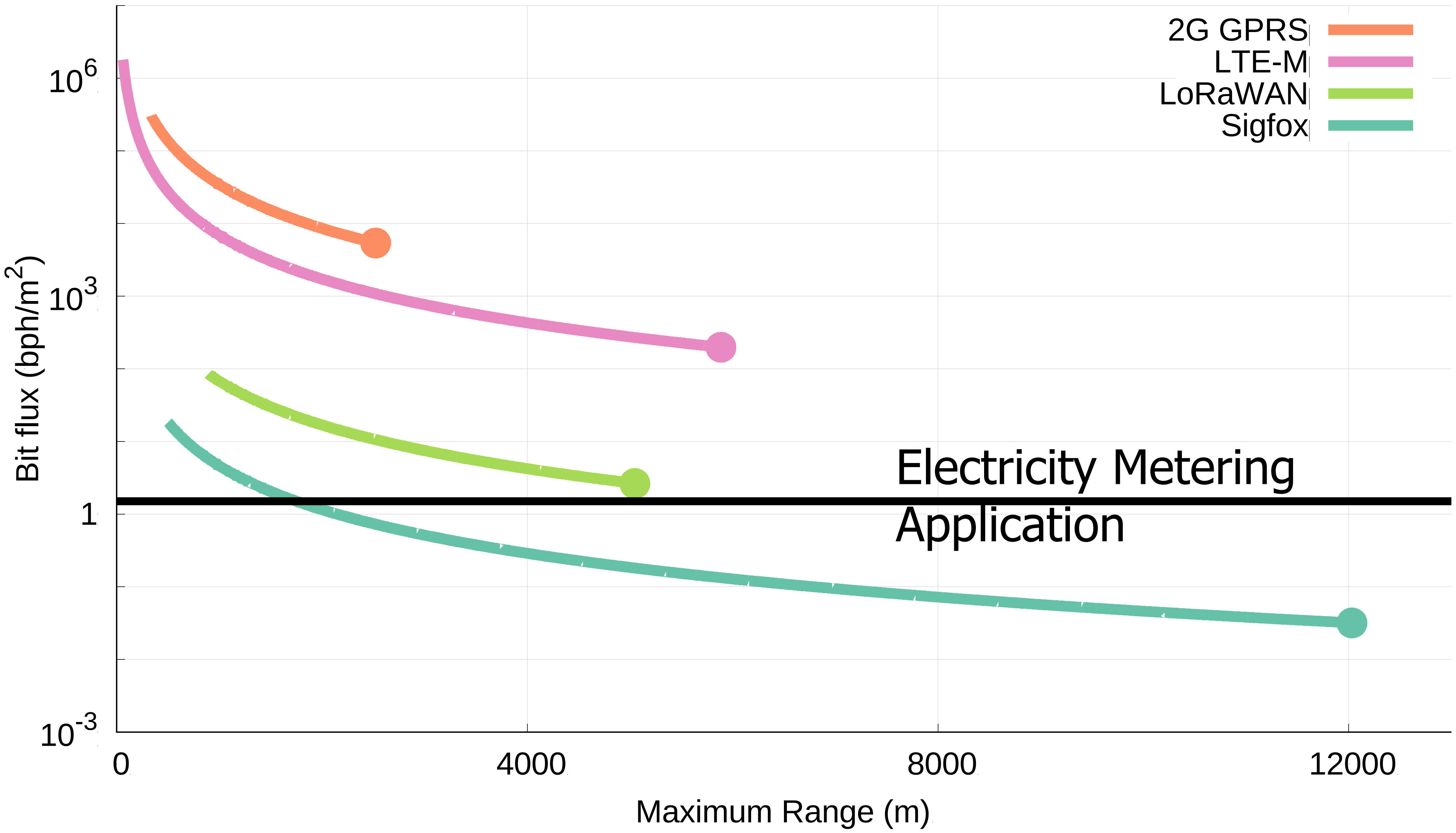
Let’s compare network capabilities to a real-world application.

Smart household electric meters.

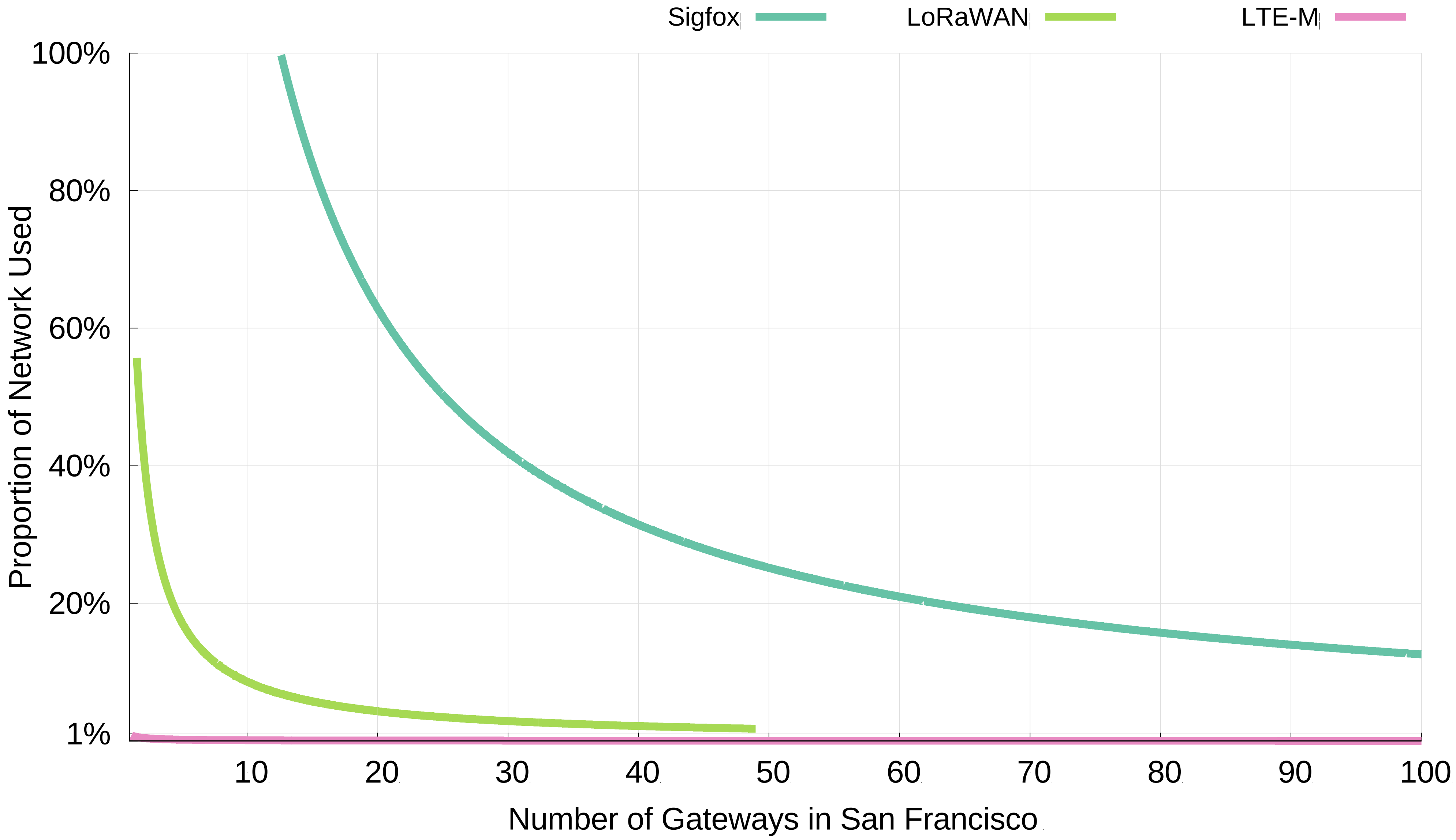
- ~250 bytes of data every 4 hours
- ~370000 electric customers in San Francisco

$$\frac{\frac{250\ bytes}{4\ hours} * 370000\ devices}{120\ km^2} \approx \frac{51000\ bps}{120\ km^2} \approx 1.5\,\frac{bph}{m^2}$$

All networks are capable of meeting the data needs of electricity metering.

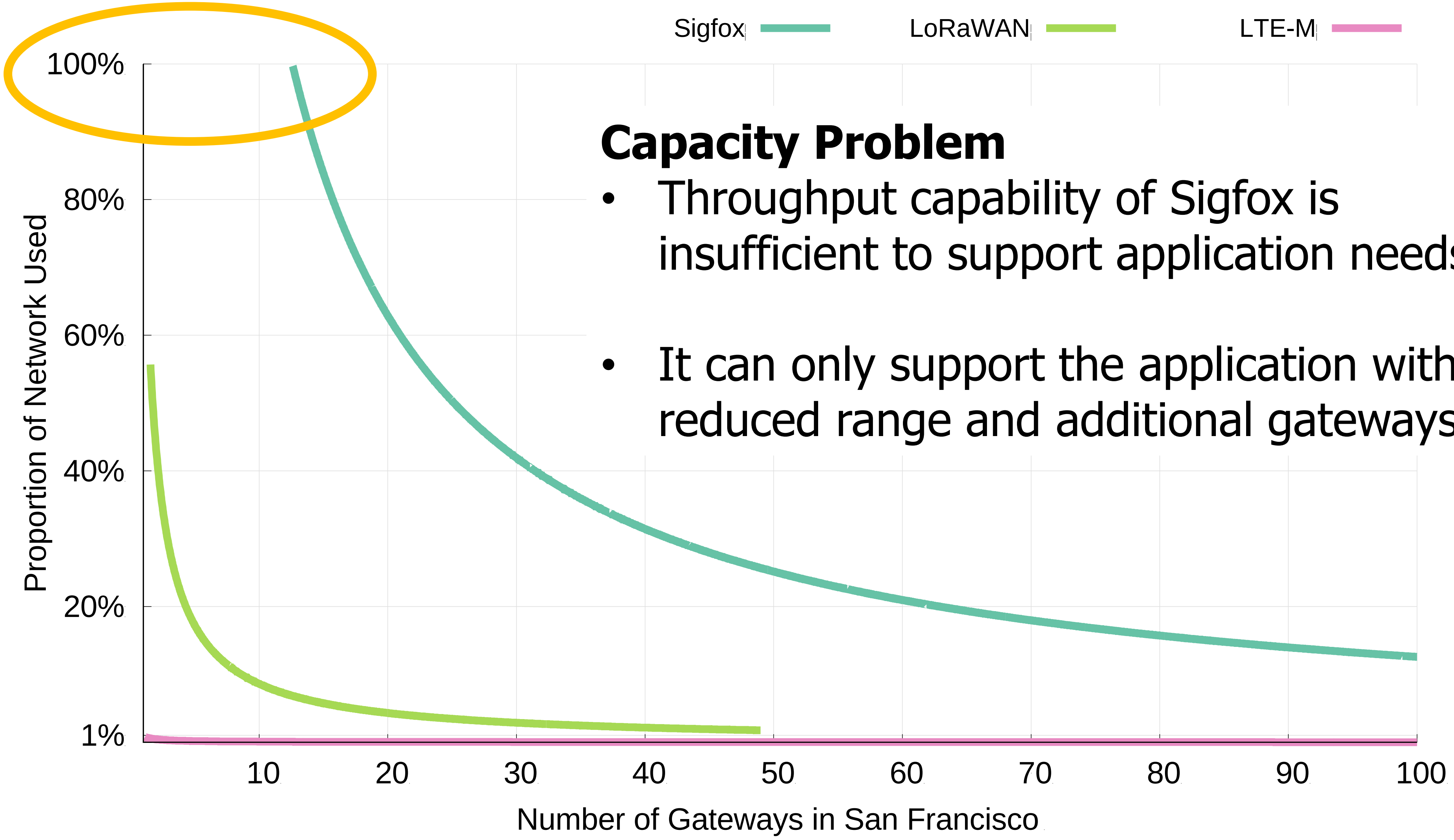


Unlicensed LPWANs lag behind Cellular IoT in ability to support applications.



2G < 0.03% utilized

Sigfox requires range reduction to meet application needs.



Capacity Problem

- Throughput capability of Sigfox is insufficient to support application needs
- It can only support the application with reduced range and additional gateways

Capacity solutions are relatively straightforward.

- Better access control mechanisms.
- Recover simultaneous transmissions (Choir and Charm).
- Increase bandwidth (TV white spaces).

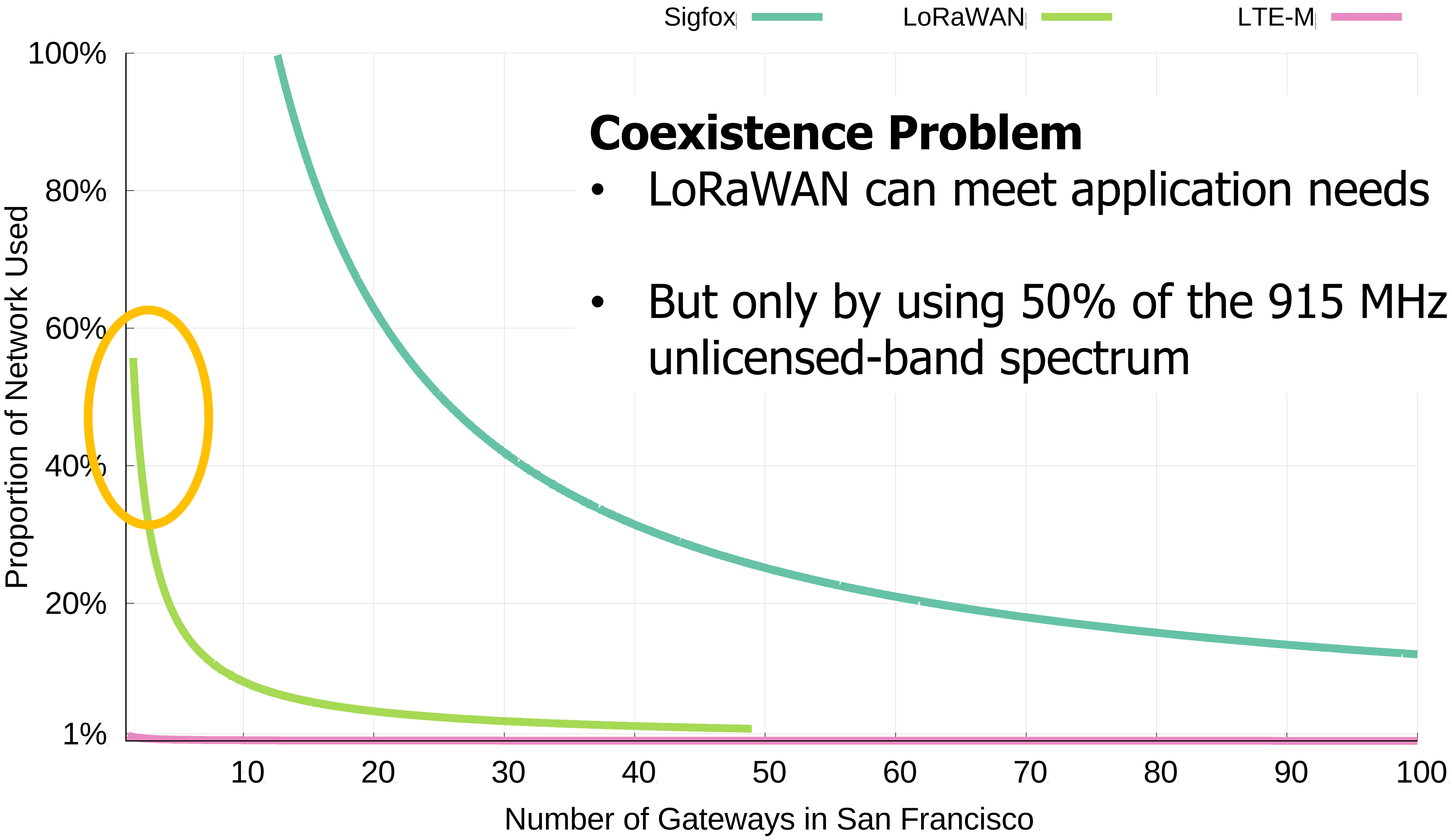
- All likely come at the cost of increased energy usage…
  - Results in a protocol that looks pretty similar to cellular…

Adwait Dongare, et al. "Charm: exploiting geographical diversity through coherent combining in low-power wide-area networks.“ *IPSN’18*

Rashad Eletreby, et al. "Empowering low-power wide area networks in urban settings." *SIGCOMM’17*

Abusayeed Saifullah, et al. "SNOW: Sensor network over white spaces." *SenSys’16*

LoRaWAN devotes most of its network capacity to a single application.

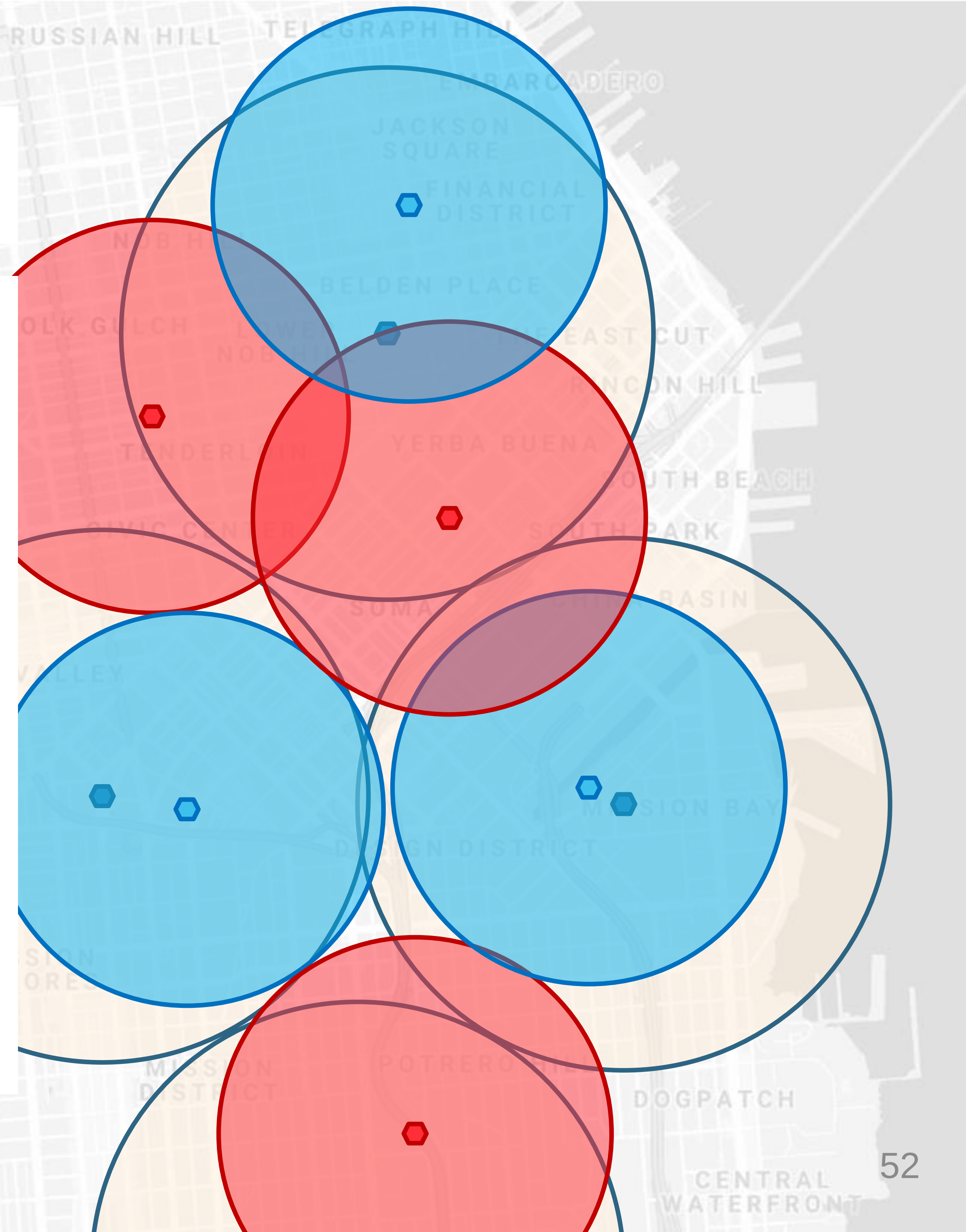


Coexistence Problem

- LoRaWAN can meet application needs
- But only by using 50% of the 915 MHz unlicensed-band spectrum

Coexistence is inevitable in urban areas.

- Urban environments and long range lead to many overlapping deployed networks.
- Capacity problems worsen coexistence by devoting more bandwidth to one application.
- It’s not just electricity metering…



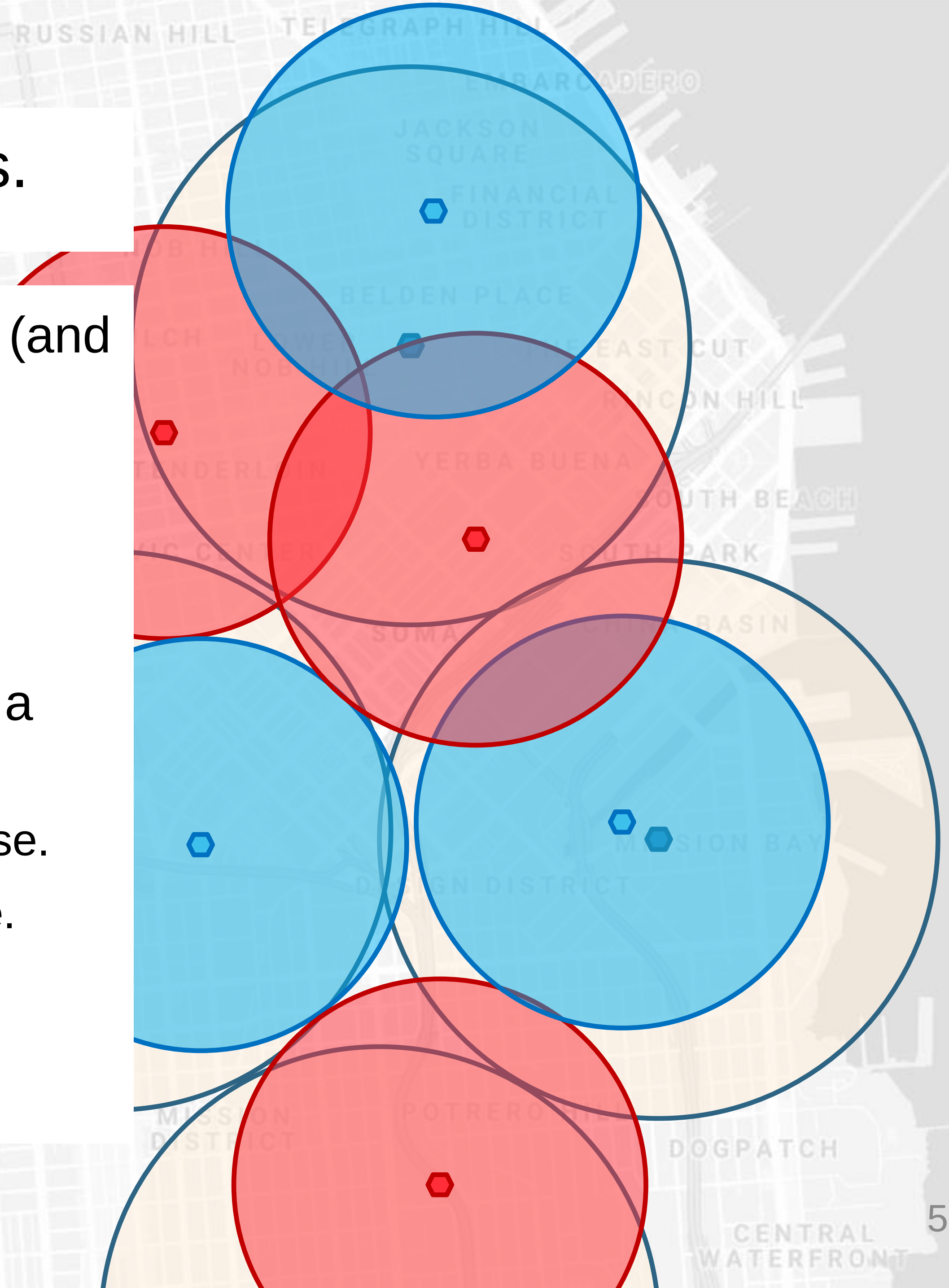
Coexistence in unlicensed bands is a more difficult problem.

- No methods for inter-network negotiation so far.
- Without buy-in from most deployments, all access control becomes uncoordinated.

- **Cellular IoT does not have this problem**

Cellular may dominate future deployments.

- LTE-M and NB-IoT are now deployed in the US (and worldwide).
- Licensed bandwidth avoids the coexistence problem.
- Cellular may solve many applications but is not a perfect solution.
    - Still has higher energy and monetary costs for use.
    - Also limited to where service is already available.



Unlicensed LPWANs are still useful for some scenarios.

- Controlled or unoccupied regions have reduced coexistence concerns.
  - Industrial factories, farms, parks and forests.

- Unlicensed networks are very exciting for research.
  - Anyone can deploy a network wherever they want.
  - Much easier to explore protocol modifications and new technologies.

- Research suffers without real-world applications.
  - Problem areas are strong recommendations for new research.
  - New research is only useful if they will have real-world impacts.

Implications – Low-Power Wide-Area Networks.

- Existing unlicensed LPWANs face significant challenges in supporting urban applications.
    - Best suited for industrial or agricultural uses in controlled environments.

- Research directions for unlicensed LPWANs:
    - improve network capacity,
    - and enable coexistence.

- Cellular IoT networks (LTE-M and NB-IoT) are positioned to solve the needs of city-scale sensing.
    - If the money and energy costs are there.

Outline

- Unlicensed LPWANs
  - Sigfox
  - 802.11ah
  - TV Whitespaces

- Cellular IoT

- LPWAN Challenges