Lecture 13
Cellular IoT & LPWAN Design

CS433 – Wireless Protocols for IoT

Branden Ghena – Spring 2025

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

Administrivia

- Hw: Cellular
  - Be sure to claim your countries soon
  - Only two students per country

- Final Design Project
  - Writeup, due early exam week
  - A few big parts
    - A: Explain some application
    - A: Consider the constraints on the application
    - A: Choose wireless technologies that seem to best work for it
    - B: Model and compare energy/battery life
    - C: Compare other aspects of performance
    - C: Choose a best option for your system

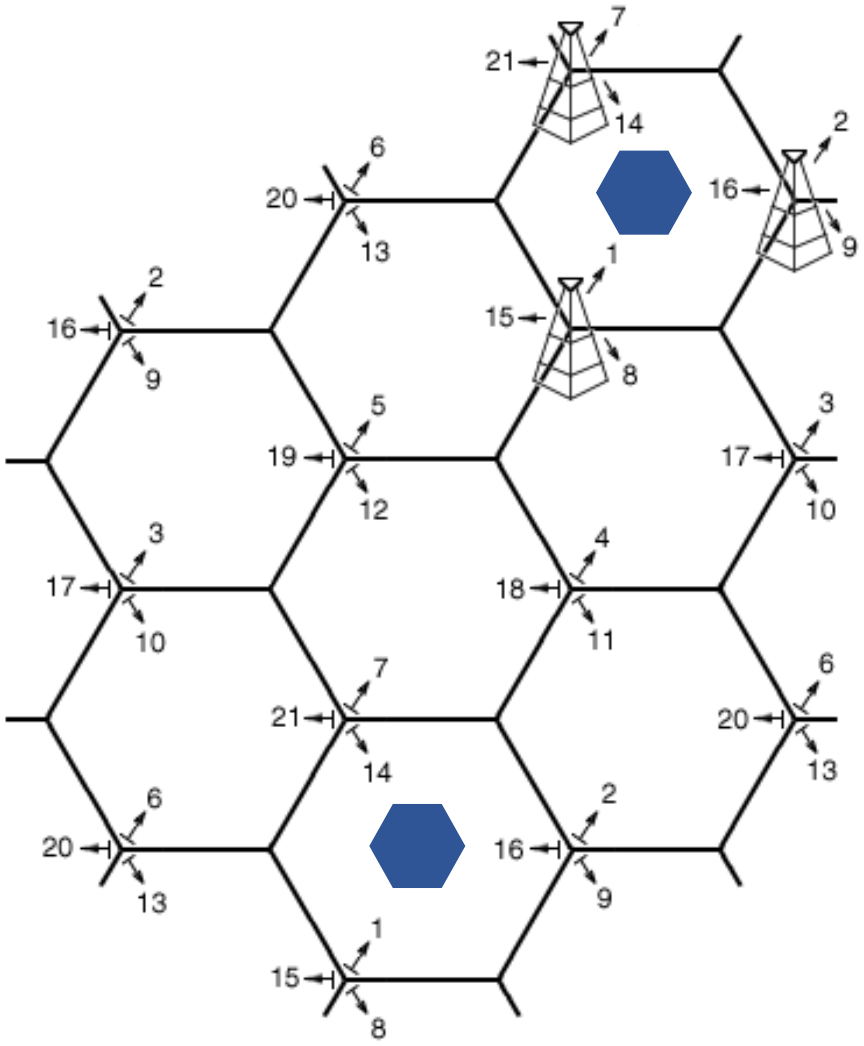
Today’s Goals

- Understand how modern “Cellular for IoT” fit into the existing cellular infrastructure, and what they do at a technical level to suit IoT needs
- Discuss real-world concerns with cellular device deployments
- Apply knowledge from the course to understand LPWAN design

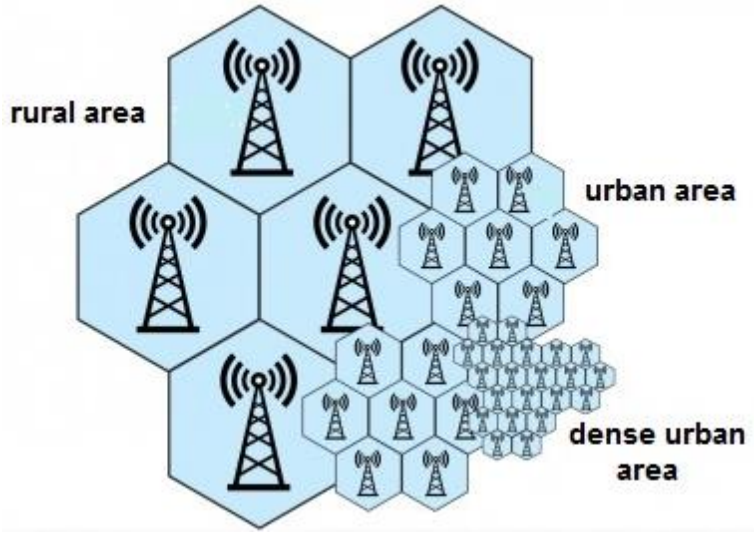
Outline

- **Cellular IoT**
- IoT on Global Cellular
- LPWAN Design

Reminder: the **cell** in cellular technologies



- 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



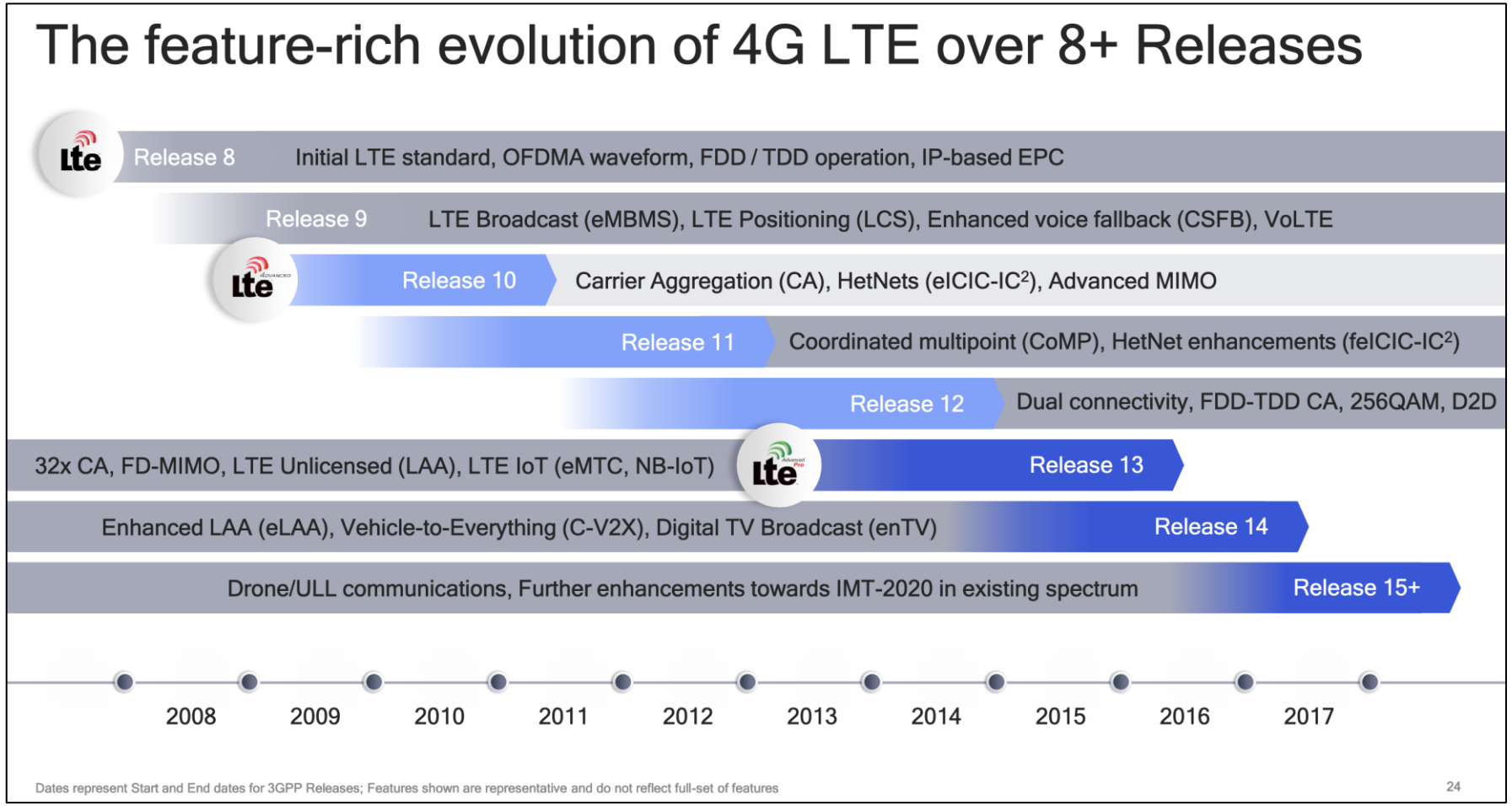
3GPP *(aka: the actual answer for what stuff is really doing)*

- 3rd Generation Partnership Project (3GPP)

- 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
  - ITU post-hoc defined "4G", 3GPP defined LTE

Mapping ”4G”, “LTE”, “LTE Advanced”, etc onto actual technologies



This Qualcomm presentation is great: https://www.qualcomm.com/media/documents/files/demystifying-3gpp-and-the-essential-role-of-qualcomm-in-leading-the-expansion-of-the-mobile-ecosystem.pdf

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

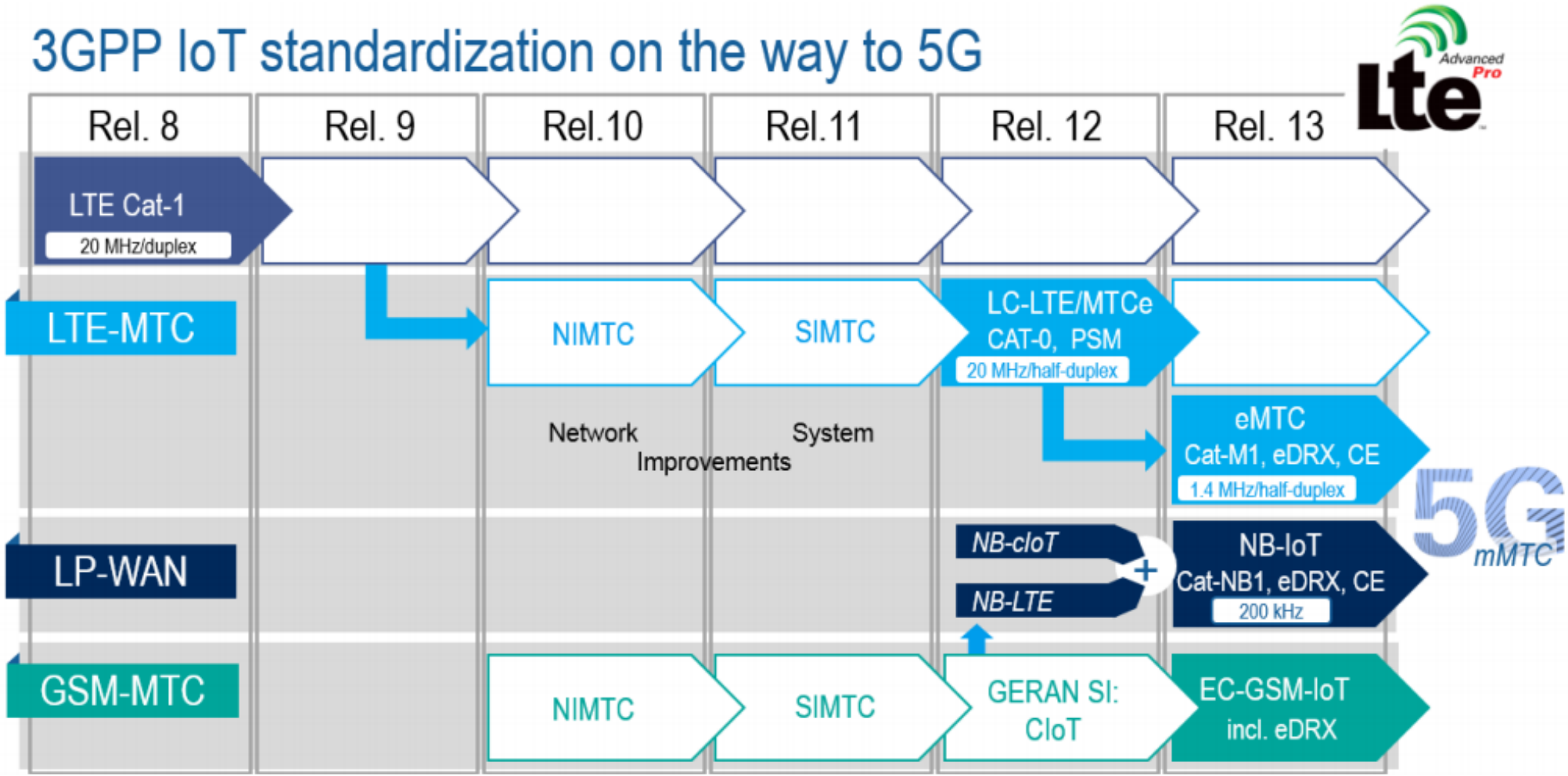
Additional low-end categories for IoT

- LTE Cat 0
  - Traditional LTE, but focused on the really low end
  - 1 Mbps for uplink and downlink

- LTE-M (LTE Cat M1)
  - 375 kbps uplink, 300 kbps downlink (for the commonly 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



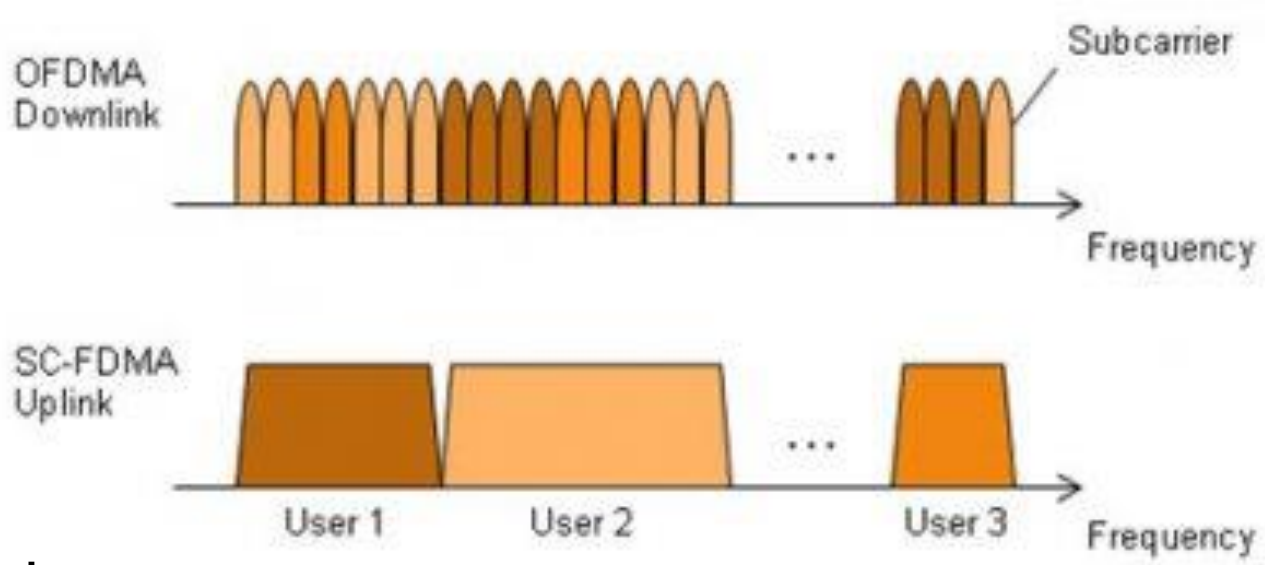
Why do we need “special categories” for IoT on cell?

- We can treat IoT devices differently than human-centric devices

- Pragmatic for the end device
  - Lower power
  - Allow for long-off periods

- Pragmatic for network operators
  - *Allows for scale*– network no longer needs to assume that devices could always be on in each cell or that they all possibly need a lot of throughput

LTE-M and NB-IoT downlink and uplink

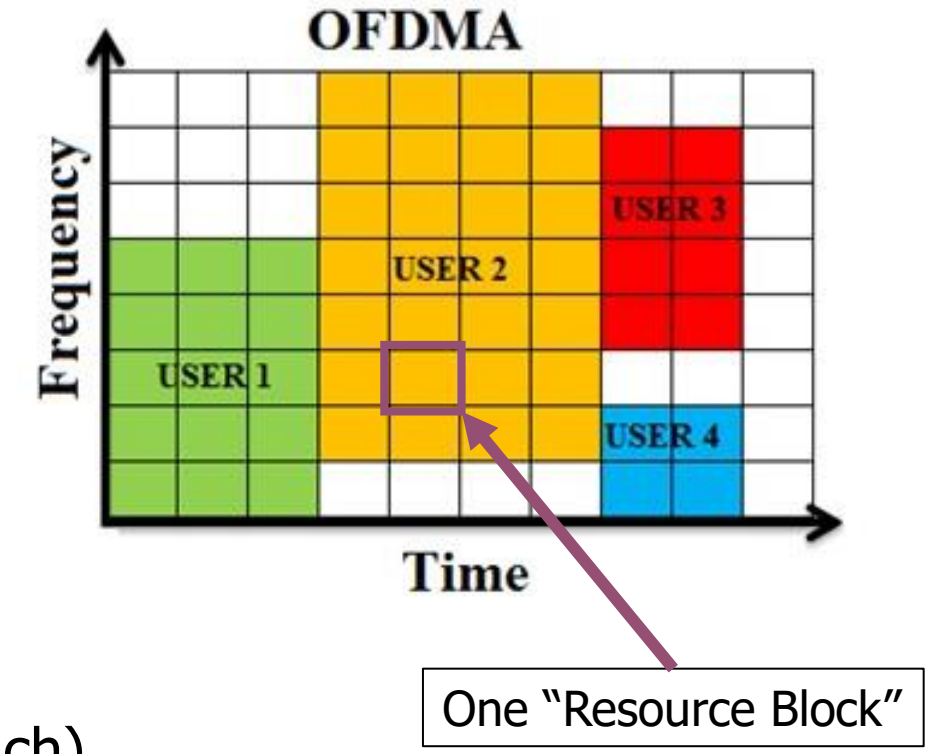


- OFDMA downlink
  - Put the more complicated hardware in the cell tower [simple FFT demodulator]

- SC-FDMA (single carrier FDMA) uplink
  - Blocks of subchannels combined into one signal
  - Essentially just send a single signal, with increased bandwidth.
    - Simpler for end devices to implement

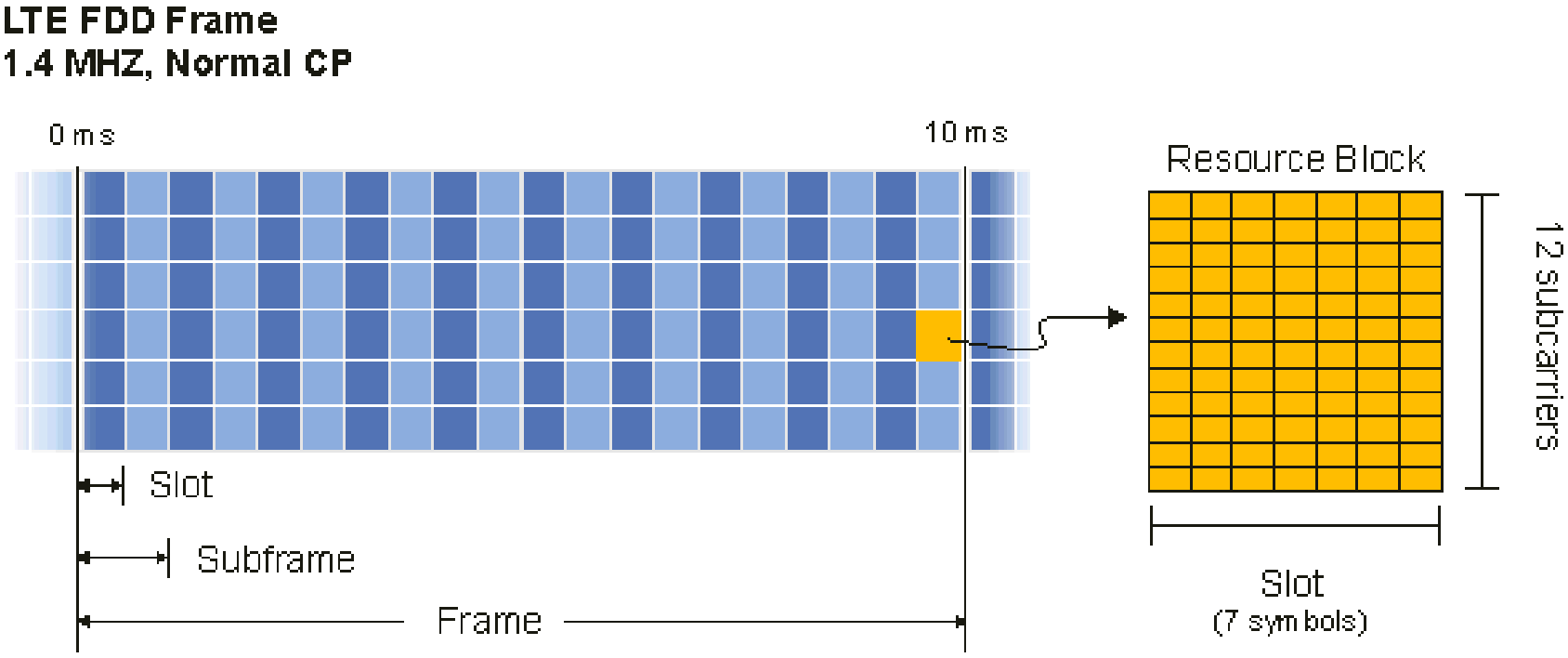
LTE resource allocation

- 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)
- Devices are allocated frequency and time based on what they are sending
  - Allocated in units of Resource Blocks



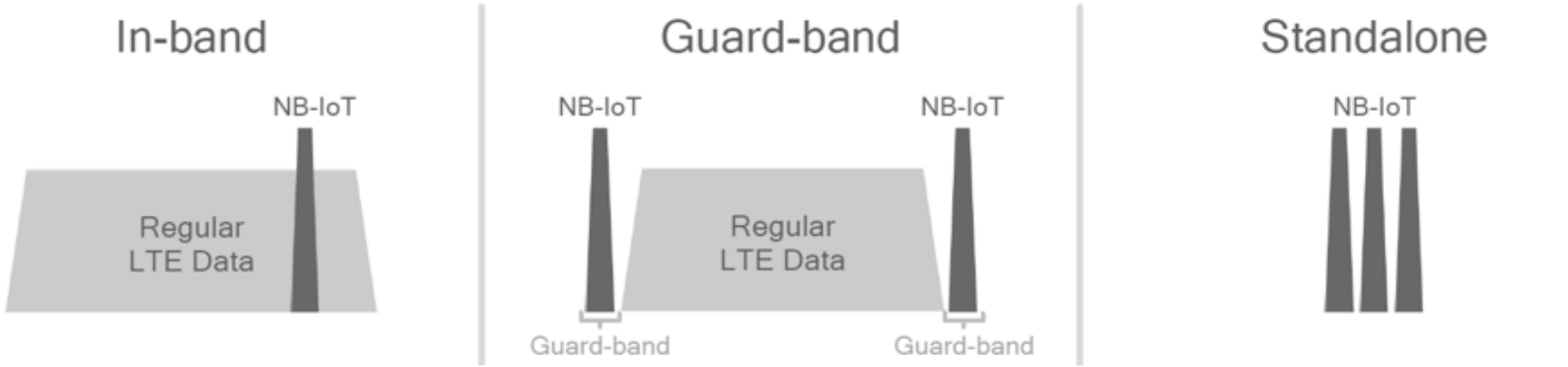
Resources used by LTE-M and NB-IoT

- 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 (**much** less throughput)



Resources used by LTE-M and NB-IoT

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



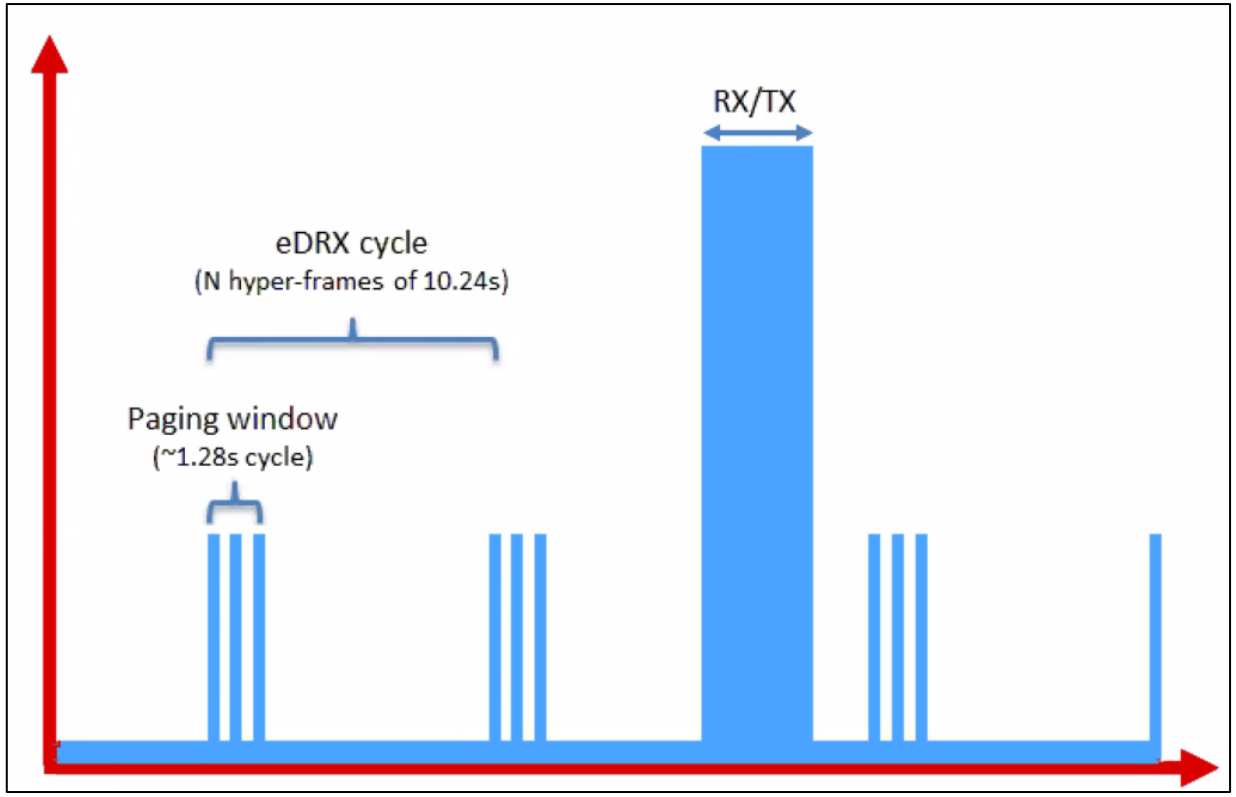
Utilizing single resource block (180kHz) within an LTE carrier

Utilizing unused resource blocks within an LTE carrier guard-band

Utilizing stand-alone 200 kHz carrier

Reducing energy use for IoT devices

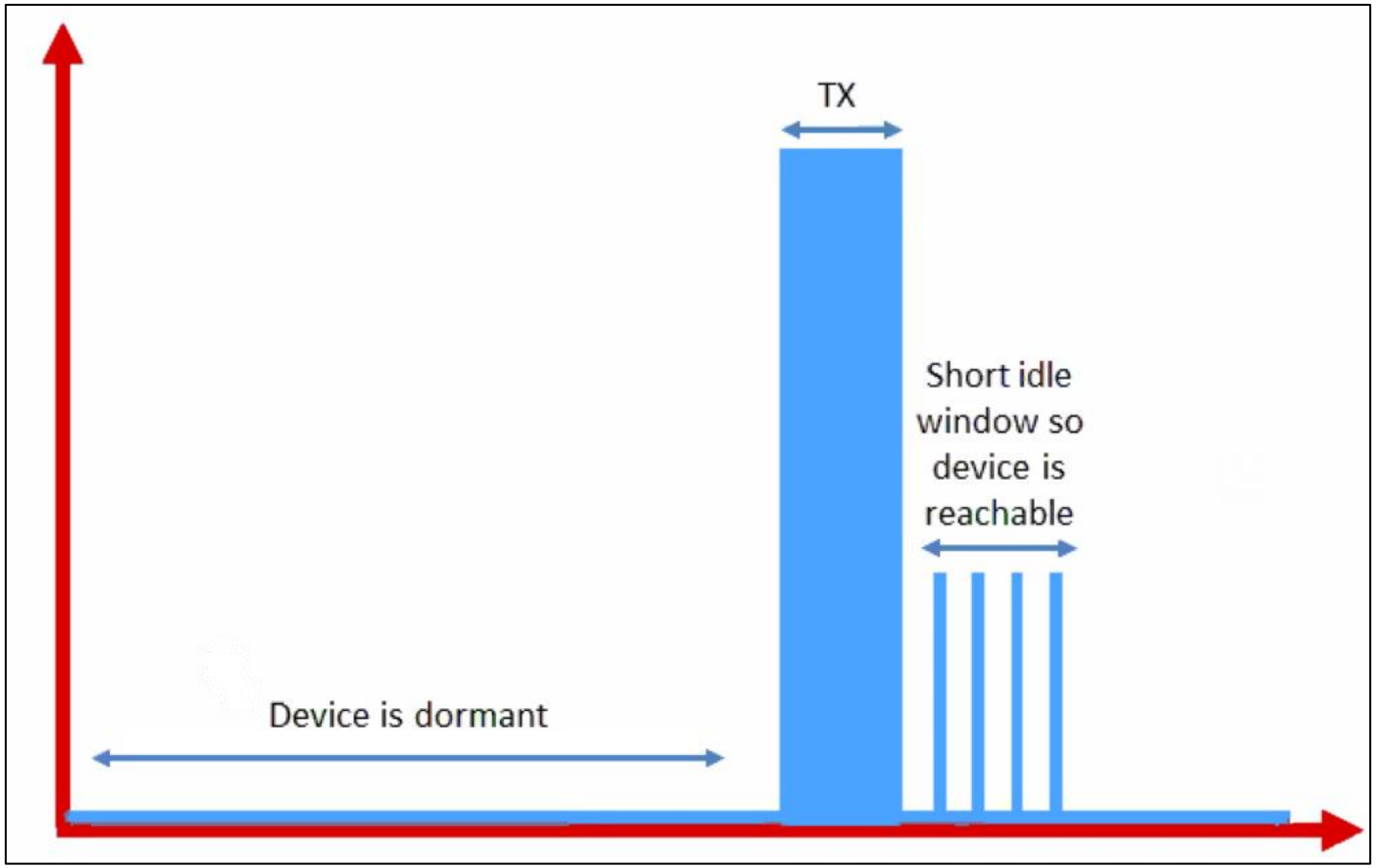
- Reduce max Tx power to 20 dBm
  - Increased receive sensitivity at tower will cover it
- Extended Discontinuous Reception (eDRX)
  - Allow devices to reduce paging period and still stay on network
  - Cell tower will hold messages
- What does this get to?
  - "For a LTE-M1 device that transmits data once per day, and wakes up every 60 hyper frames to check for commands (this would be about every 10 minutes), **a life of 4.7 years is achievable on 2 AA batteries**."



Graphics, quote from https://www.link-labs.com/blog/lte-e-drx-psm-explained-for-lte-m1

Further power reduction for simple devices

- Power Saving Mode (PSM)
  - 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



Graphics from https://www.link-labs.com/blog/lte-e-drx-psm-explained-for-lte-m1

Some numbers from an actual telecom: Aeris
[n.b. Aeris has been a leader in cellular M2M since the 90's]

- PSM has two timers, devices *request* values, *tower chooses* actual:
  - Extended Timer ("sleep" timer)
    - 3GPP max is 35,712,00s [413.33 days]
    - Aeris timer range: Min 240m [4h]; Max 413 days
    - "Aeris Fusion" timer range: Max: 12.9 days
  - Active Timer (how long will the device stay in idle after communication?)
    - Seconds or minutes

Active Timer – T3324

The requested active timer value is a single binary string byte value defined by octet 3 of the GPS Timer 2 specification (see section 10.5.7.4 of 3GPP TS 24.008) as follows:

- Bits 5 to 1 represent the binary coded timer value.
- Bits 6 to 8 define the timer value unit (table):

Timer 3 Value	Timer Value Incremented
000xxxxx	2 seconds
001xxxxx	1 minute
010xxxxx	1 decihour (6 minutes)
111xxxxx	Timer is deactivated

Numbers from https://aeriscom.zendesk.com/hc/en-us/articles/360049848254-Understanding-LTE-M-Power-Management-Modes

Variety of features supported in real-world

Features & Features configuration	PSM PSM Activity Timer T3324			eDRX					Data Packet Buffering		SMS support	Power Classes (3, 5, 6)	CE Level (0, 1, 2)
	No/static/ dynamic	min value	max value	No/static/ dynamic	T eDRX Min value	T eDRX Max value	T PTW Min value	Max value	Yes/No	Nb of Packets			
Telekom Deutschland	Dynamic	0 sec	11.160 s	Dynamic	20,48s	10485,76 s	2,56 s	40,96 s	Yes	10	No	Yes (3&5)	Yes
Magenta Telekom	Dynamic	0 sec	11.160 s	Dynamic	20,48 s	10485,76 s	2,56 s	40,96 s	Yes	10	No	Yes (3&5)	Yes
T-Mobile Netherlands	Dynamic	0 sec	11.160 s	Dynamic	20,48 s	10485,76 s	2,56 s	40,96 s	Yes	10	No	Yes (3&5)	Yes
T-Mobile Czech Republic	Dynamic	0 sec	11.160 s	Dynamic	20,48 s	10485,76 s	2,56 s	40,96 s	Yes	10	No	Yes (3&5)	Yes
Slovak Telekom	Dynamic	0 sec	11.160 s	Dynamic	20,48 s	10485,76 s	5,12 s	40,96 s	Yes	10	No	Yes (3&5)	Yes
Magyar Telekom	Dynamic	0 sec	11.160 s	No	N/A	N/A	N/A	N/A	Yes	10	No	Yes (3&5)	Yes
OTE / Cosmote	Dynamic	0 sec	11.160 s	No	N/A	N/A	N/A	N/A	No	NA	Yes	Yes (3&5)	Yes
T-Mobile Poland	Dynamic	0 sec	11.160 s	No	N/A	N/A	N/A	N/A	Yes	Dynam.	Yes	Yes (3&5)	Yes
Hrvatski Telekom	Dynamic	4 sec	50 s	No	N/A	N/A	N/A	N/A	Yes	10	No	Yes (3&5)	Yes

- Probably out-of-date details for NB-IoT networks
  - PSM 0-11 seconds (or 4-50)
  - eDRX 20 seconds – 3 hours (or not supported at all)
  - Packet buffering none to 10 packets (or dynamic)

https://docs.iotcreators.com/docs/nb-iot-network-information

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 many cellular bands are often on higher frequencies
  - Example: 1900 GHz
  - Coarsely, lower frequency is longer range, but it's ***complicated***

Cellular deployments

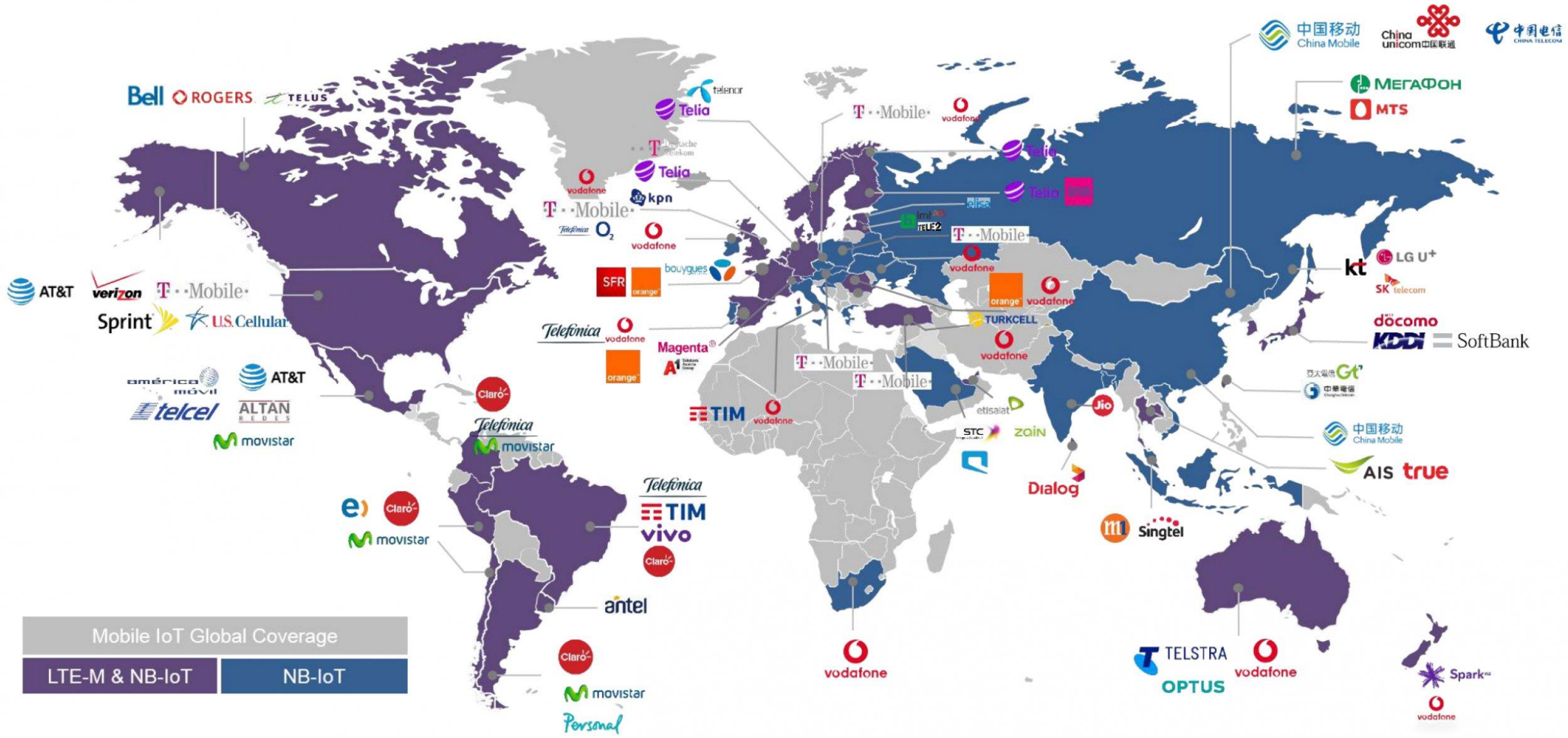
- Originally unclear which would be dominant
  - Verizon and AT&T focused on LTE-M
  - T-Mobile focused on NB-IoT
  - All rolled out services nationwide in the 2018-2019 timeframe

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

- 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

Kotonlink
Your Reliable IoT Partner

LPWA Network Deployment (Based on GSMA Data up to Nov. 1, 2020)



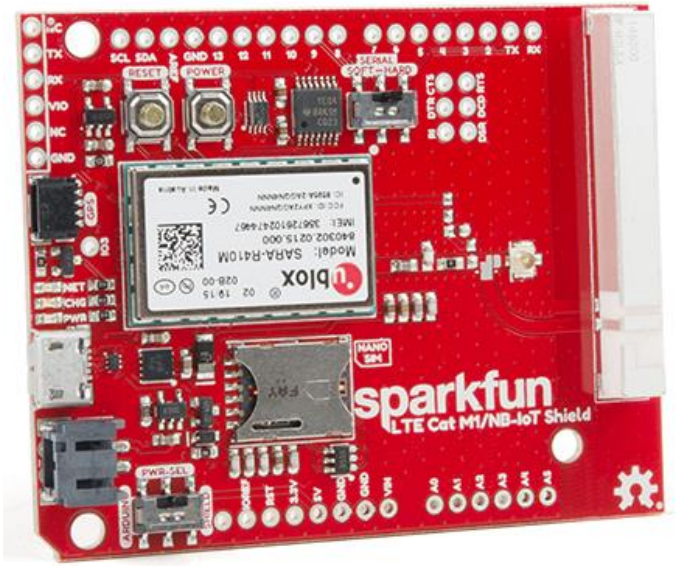
Mobile IoT Global Coverage

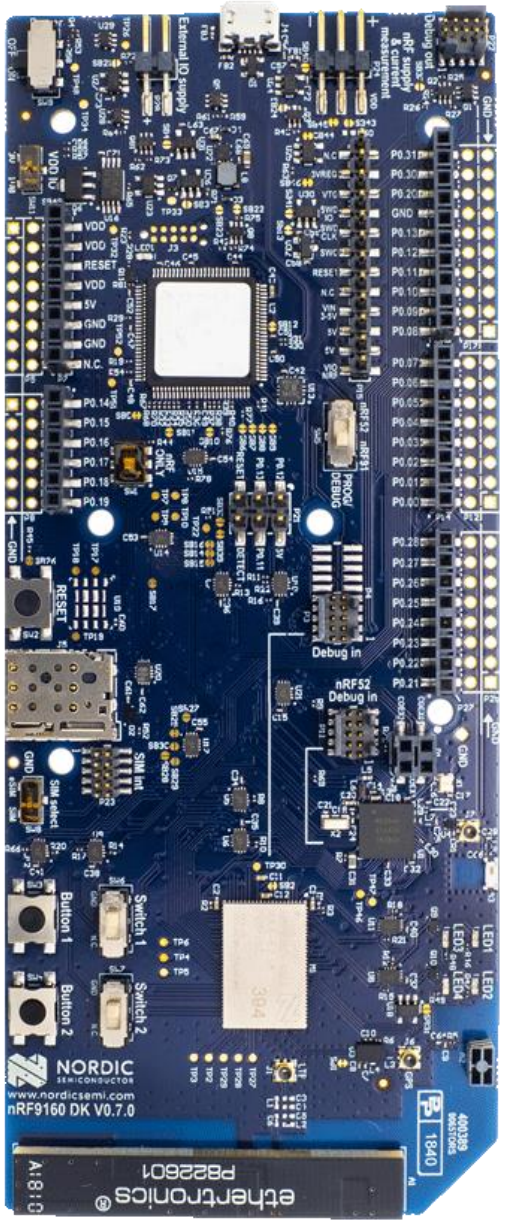
LTE-M & NB-IoT | NB-IoT

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





Break + Open Question

- Cellular hardware almost always requires certified radio modules where you can’t change the code at all. Why?

Break + Open Question

- Cellular hardware almost always requires certified radio modules where you can’t change the code at all. Why?
  - Otherwise you could cheat at the protocols!!
  - Or just generally not follow them fairly.
  - Avoids “tragedy of the commons” by allowing specific trusted devices only

What about 5G?

- NB-IoT and LTE-M *are* the low-power, wide-area 5G solutions
  - Intent is to coexist with 5G solutions for human-centric devices

> - 3GPP has agreed that the NB-IoT and LTE-M technologies will continue evolving as part of the 5G specifications, meaning that mobile operators can leverage LPWA investments already today and continue as part of the 5G evolution.

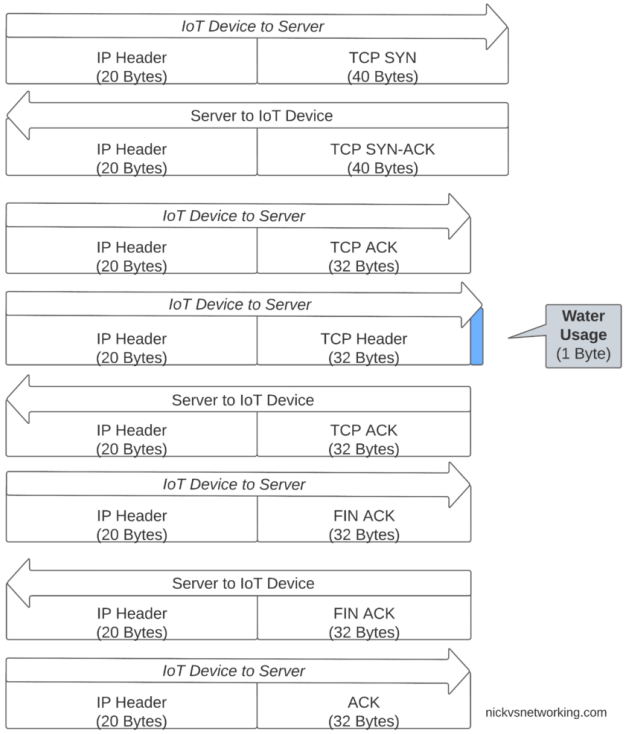
- Even if 4G sunset occurs, LTE-M and NB-IoT will still be around

https://www.ericsson.com/en/reports-and-papers/nb-iot-and-lte-m-in-the-context-of-5g-industry-white-paper

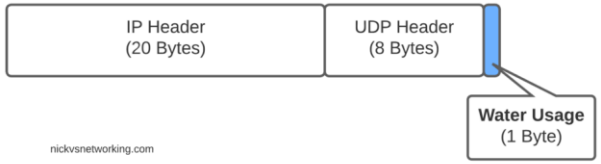
Support for IoT - Non-IP Data Delivery (NIDD)

- Reduce the amount of data necessary to transmit
  - Registers device with a single "destination IP"
  - Device just transmits data payload, network handles sending it to server

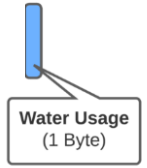
TCP Data Transmission



UDP Data Transmission



NIDD Data Transmission



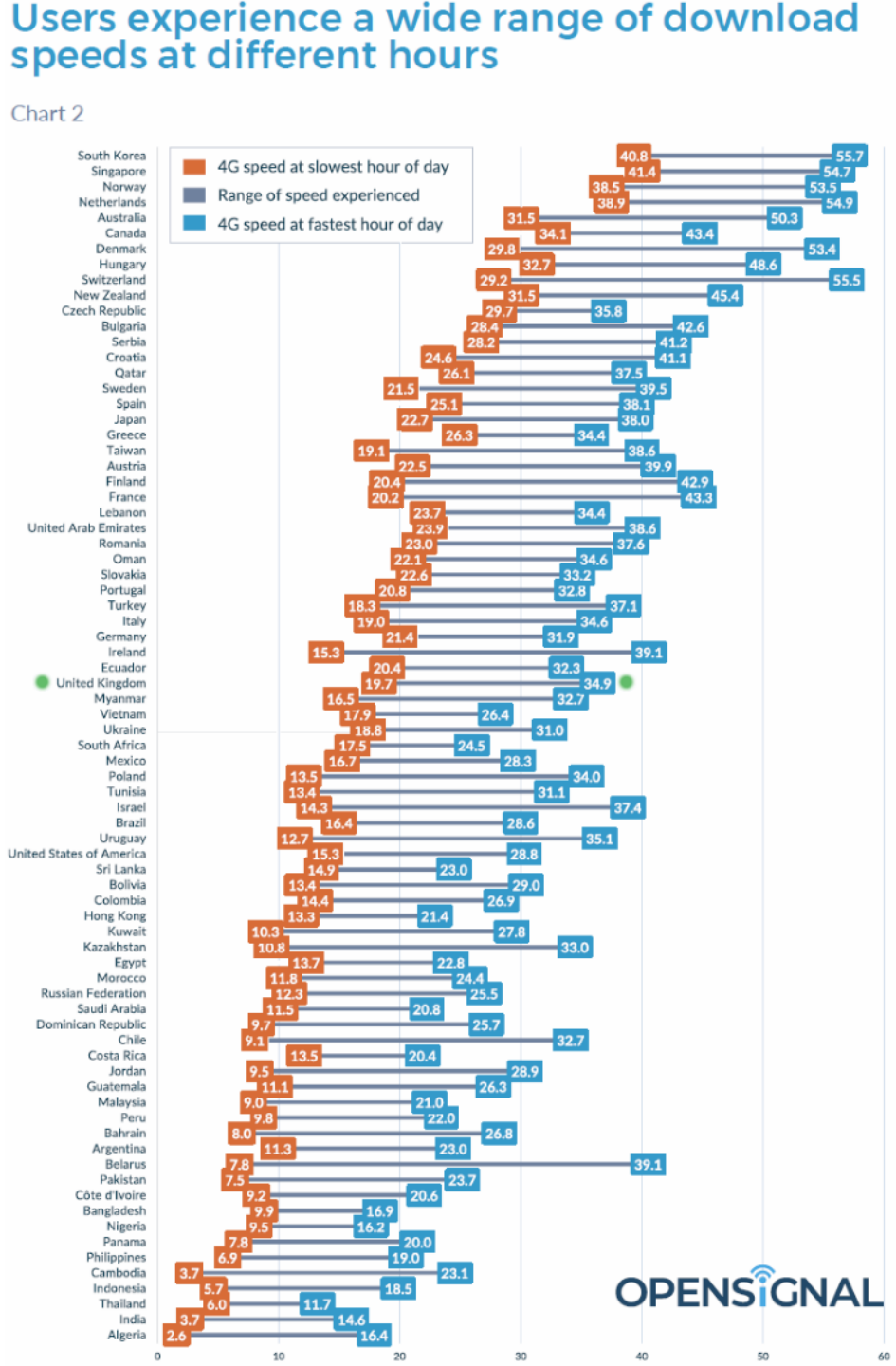
https://nickvsnetworking.com/nb-iot-nidd-basics/

Outline

- Cellular IoT
- **IoT on Global Cellular**
  - Story by Pat Pannuto & nLine
- LPWAN Design

Sizing networks is hard

- Sometimes you just lose performance..



Traffic fluctuates in all networks, for cellular it becomes a function of both when and where you are

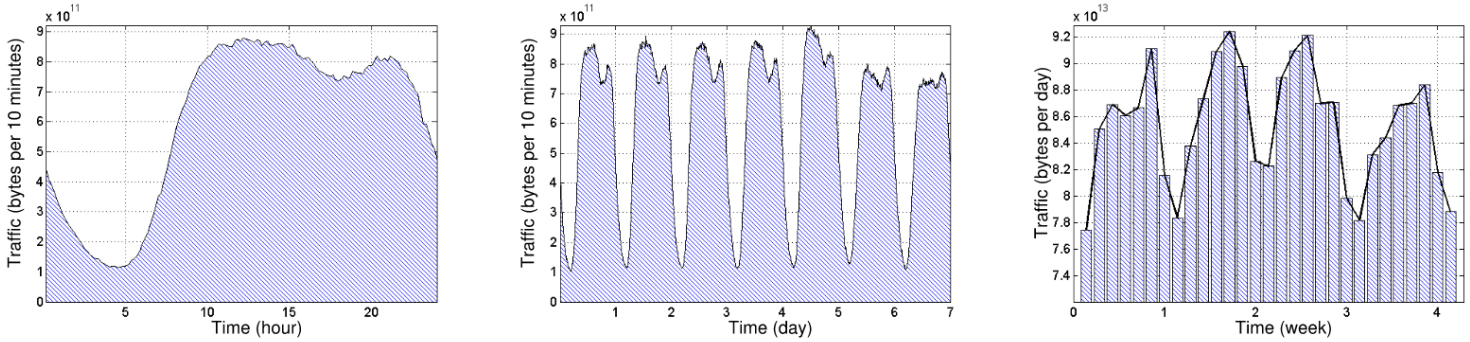


Fig. 1. The temporal distribution of cellular traffic at different time scales. (a) Hourly. (b) Daily. (c) Weekly.

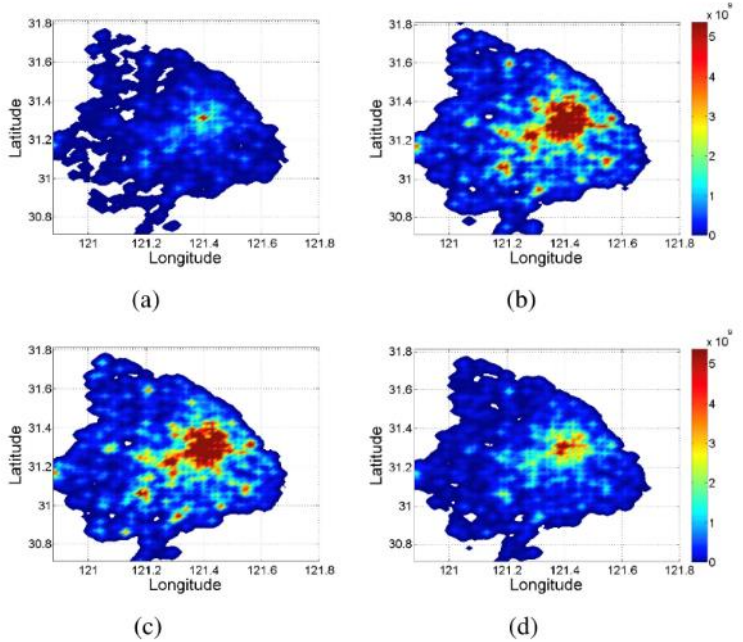


Fig. 2. The spatial distribution of cellular traffic at different time. (a) 4AM. (b) 10AM. (c) 4PM. (d) 10PM.

Understanding Mobile Traffic Patterns of Large Scale Cellular Towers in Urban Environment; Xu, Li, Wang, Zhang, Jin; IEEE ToN

What is an MVNO
“Mobile Virtual Network Operator”

- Decoupling the builders of infrastructure from the sellers
- Not a new concept, but seeing aggressive growth
  - MetroPCS; Cricket; Boost Mobile; etc
  - GoogleFi; Xfinity Cellular

Why does this matter for IoT Deployments?

- Say you're building a power grid sensor you want to deploy globally…

PARTICLE ELECTRON: CELLULAR

The Electron is a tiny development kit for creating 3G cellular-connected electronics projects and products. It comes with a Particle SIM card with service in more than 100 countries worldwide.

Device Cloud

Access to the Device Cloud includes: 3MB of cellular data per device/mo (additional data $0.40/MB for most countries) First 3 months of Device Cloud FREE ($2.99 per device/mo after) Device Cloud Features:

- Device Management
- Over the Air Firmware Updates
- Fully Managed Connectivity
- Developer Tools
- Integrations

So how does Particle, a small IoT platform startup, provide global cellular coverage?

- We deployed some Electrons in Accra, Ghana sending a message once per minute 24/7 for a few weeks
  - PRR [POST Reception Rate] changes over time
  - Almost zero PRR from ~7-9am and ~4-7pm daily

- Introducing traffic priority
  - Call Particle: “What gives?”
    - Particle buys from T-Mobile
    - T-Mobile buys from Deutsche-Telekom [didn’t own them yet]
    - DT buys from Vodafone
    - Vodafone buys from MTN
    - MTN has 5 tiers of traffic priority on their network [guess which tier we were in?]

So how do you get higher on the priority list?

- You buy from MTN
- … also not easy
  - Limit of 3 SIMs / person due to fraud
    - Particularly important due to prevalence of SIM-based mobile money

So how do you deploy in Tanzania?

- Not limited in SIMs, but limited in *payment plans*

- Post-paid plans not an option
  - Need to purchase ‘airtime recharges’
  - Which you use by texting from that phone to an SMS shortcode
    - So now you must have in-country staff!

So how do you actually realize this claim?

- Good. Question.

Takeaway: Cellular provides the IoT the only reliable global coverage available today

- If the goal is deploy-today + work-anywhere, cell is the only option
  - (Or arguably satellite)
- That's not to say cell actually works everywhere!
  - Just the best-available
- **Contrast:** What is the insight behind AirTags?
  - Or Tile, Cube, etc.?

Outline

- Cellular IoT
- IoT on Global Cellular
- **LPWAN Design**

LTE-M and NB-IoT design constrained by fitting within existing cellular ecosystem

- What might a fresh design look like?

- *Caveat:* In ISM bands!
  - So it's an unlicensed, shared communication band

Design a wide-area network (ignore low-power for now)

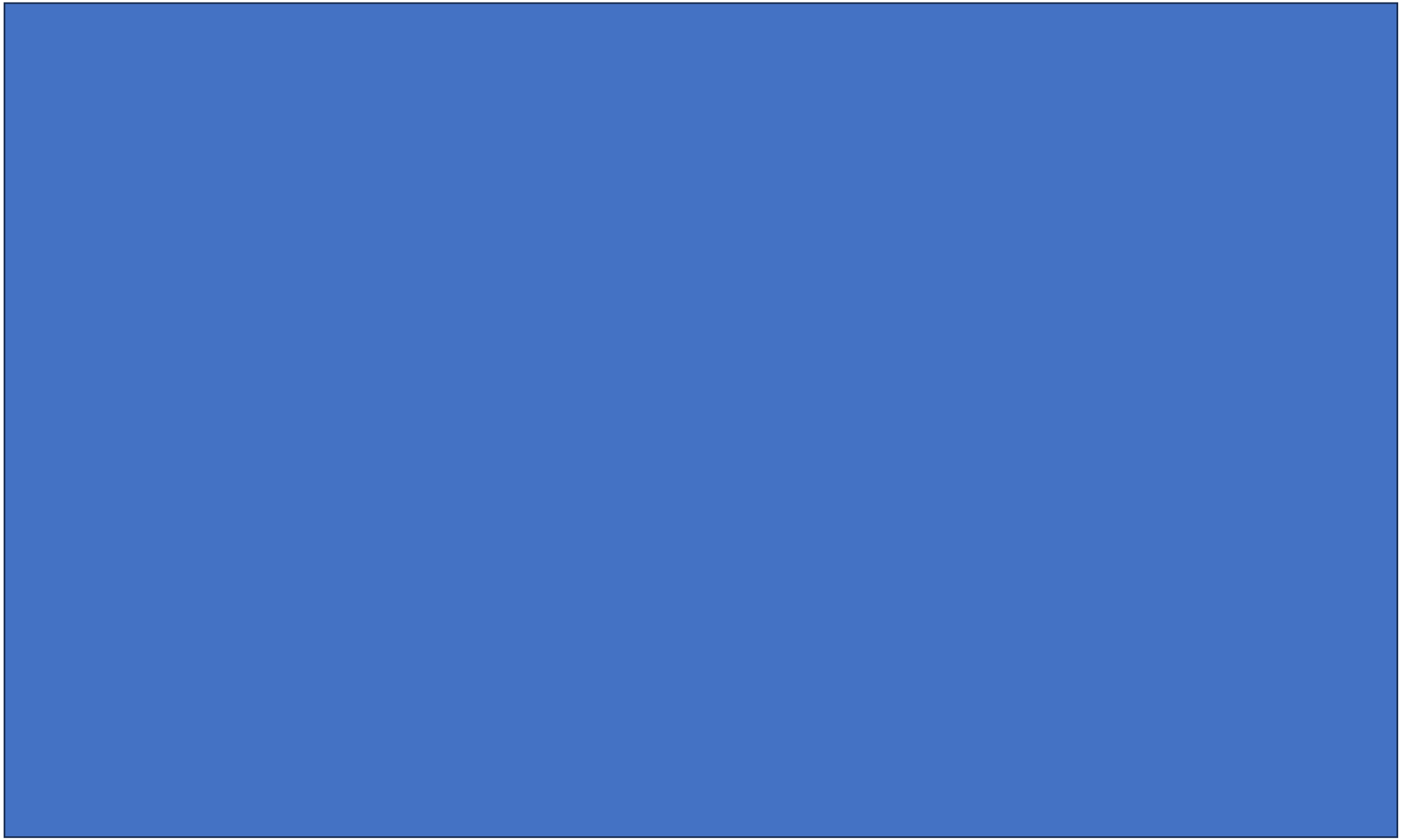
- **What PHY choices would you make?**

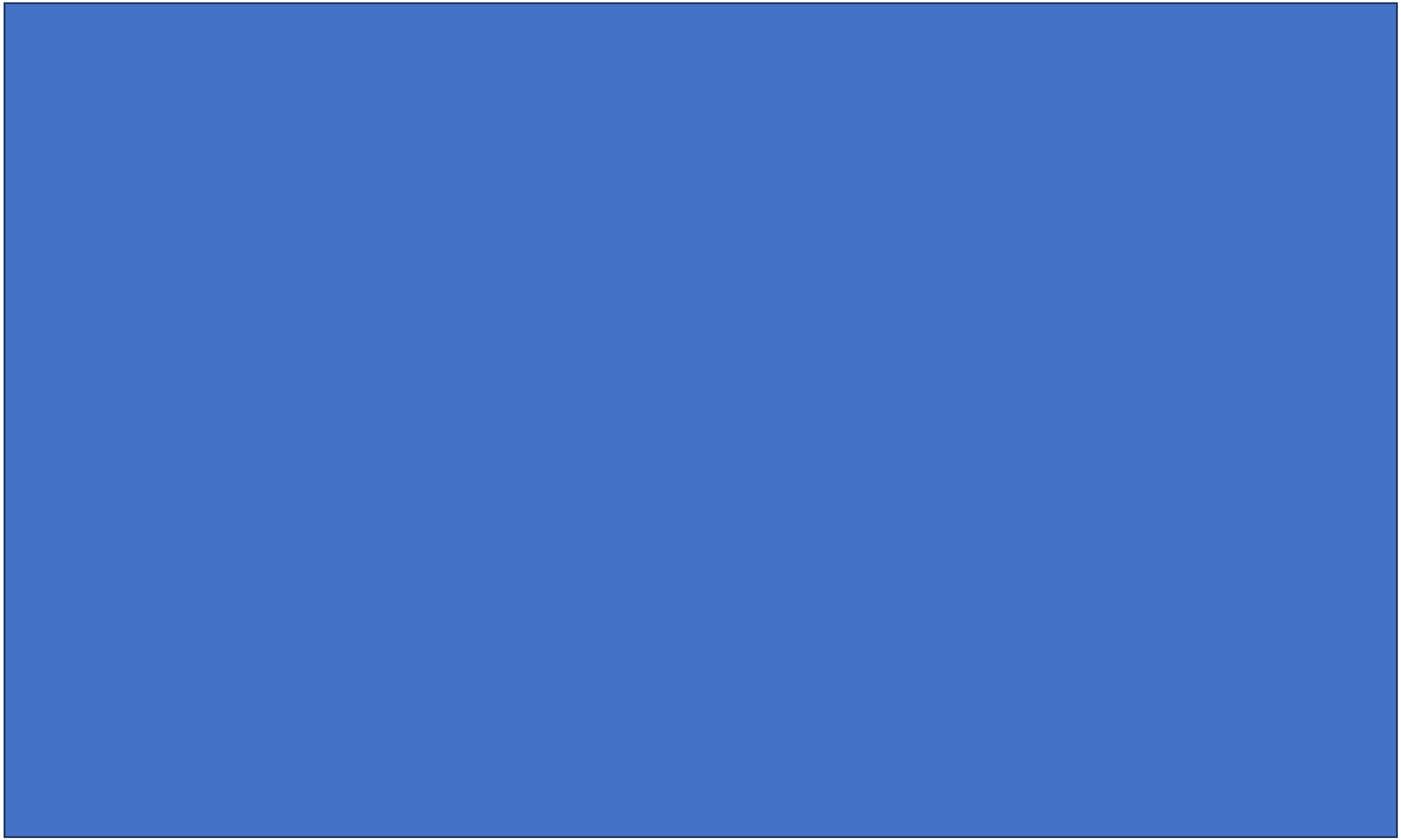
Design a wide-area network (ignore low-power for now)

- **What PHY choices would you make?**
  - Modulation
  - Tx Power
  - Carrier Frequency Band
  - Data Throughput
  - Channel Bandwidth

Design a low-power wide-area network

- **Any particular MAC choices for lower power?**
  - Device Roles
  - When do devices listen?
  - Access Control Mechanism





Outline

- Cellular IoT
- IoT on Global Cellular
- LPWAN Design