Lecture 12
Evolution of Cellular

CS397/497 – Wireless Protocols for IoT

Branden Ghena – Spring 2024

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

Administrivia

- Lab: Thread due Wednesday
- Lab: WiFi due next week Wednesday
  - Get going on this!
- Hardware swap
  - I have more Heltec boards to hand out
  - I will also collect Nordic boards today

Today's Goals

- Introduction to the Wide-area communication space
- Understand fundamentals of cellular technology
- Learn how "older" cellular technology works
  - And why it is relevant to the IoT today

Outline

- **Wide-Area Network Background**

- Cellular Network Technologies
  - 1G
  - 2G
  - 3G/4G and beyond

Wide area networks

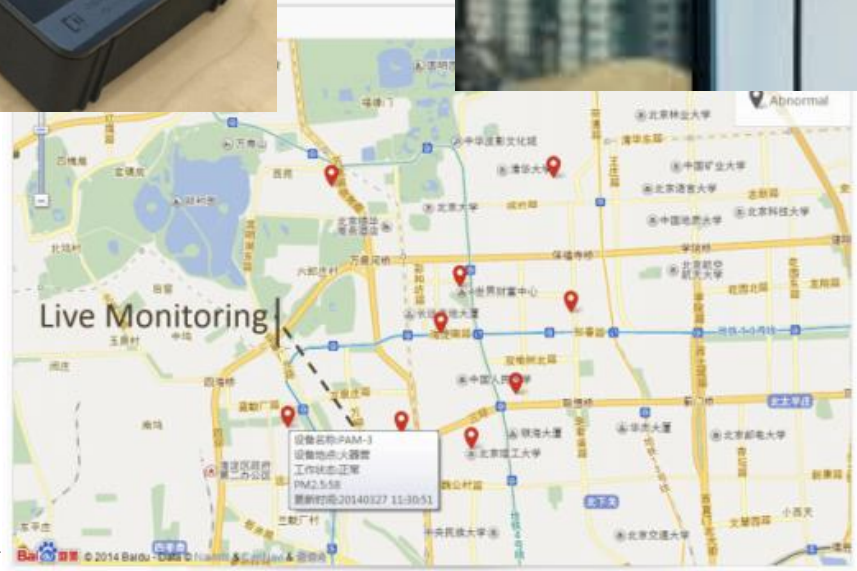
- Communication at the region/city scale rather than the building/residence scale
  - Throughout cities
  - Agricultural deployments
  - Industrial facilities

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

Air quality monitoring

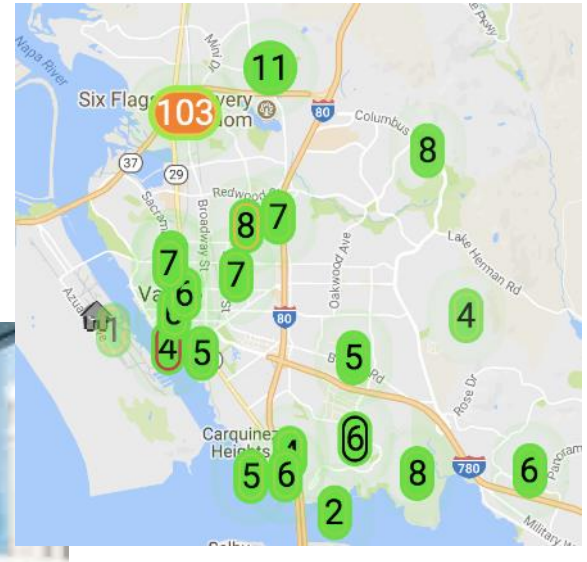
[1]

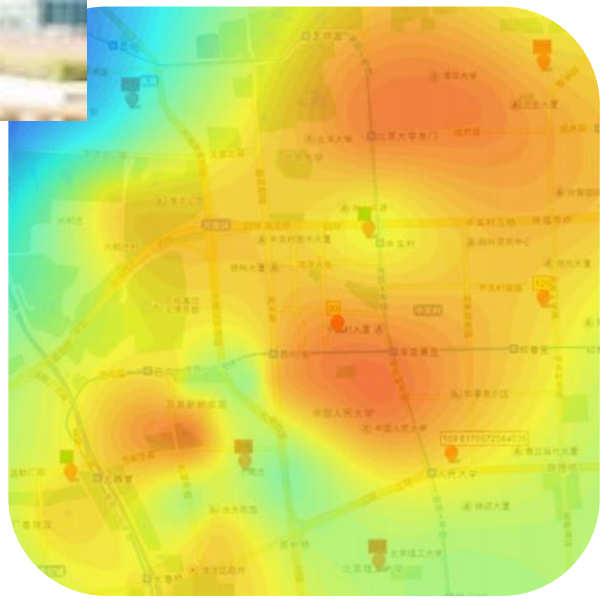
[1]



[2]

[2]

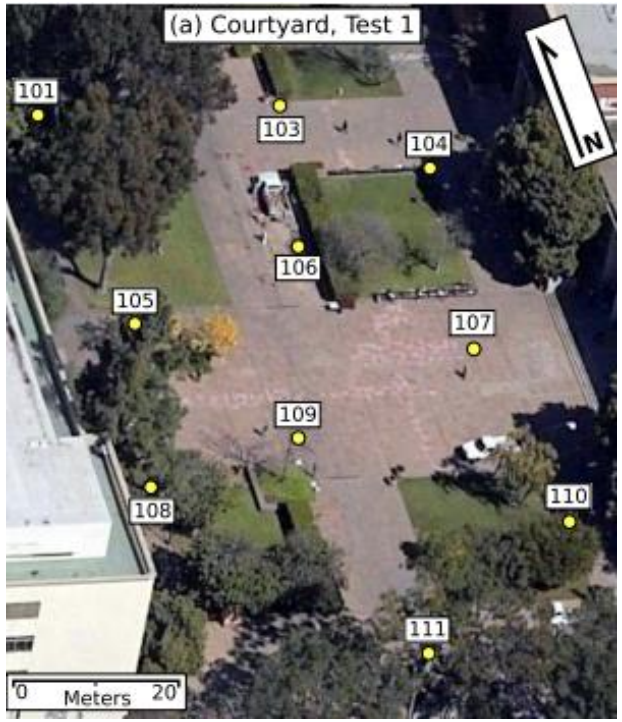




[1] Cheng et al. AirCloud: a cloud-based air-quality monitoring system for everyone. 2014.

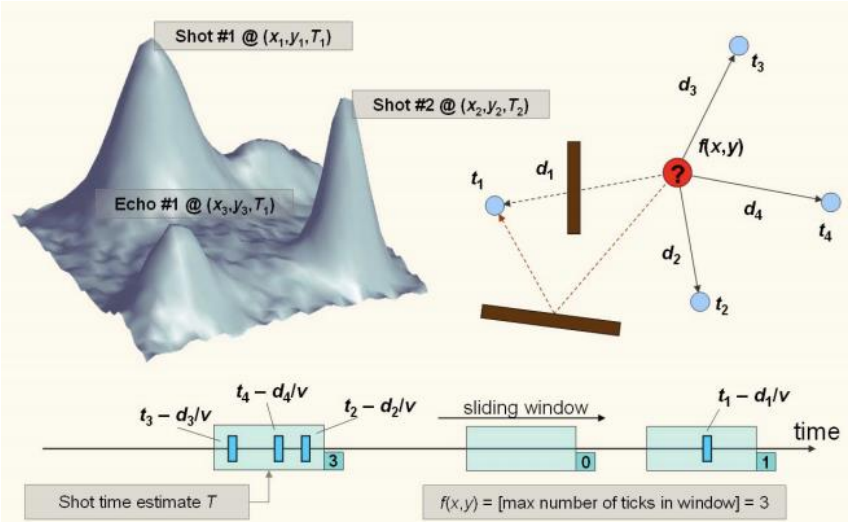
[2] Purple Air. 2018.

Audio detection, classification, and localization

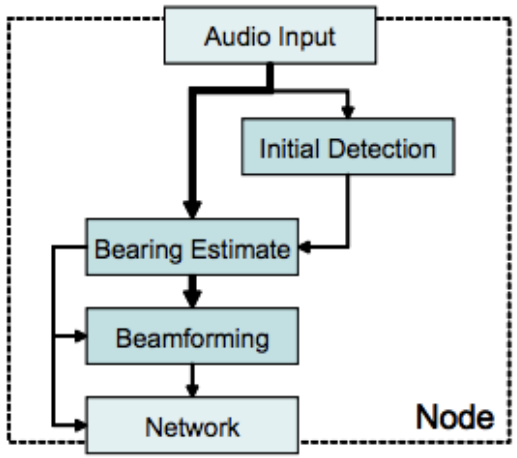


[1]

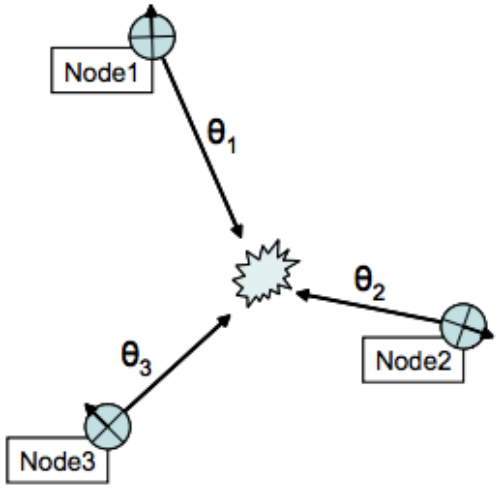
[3]



[2]



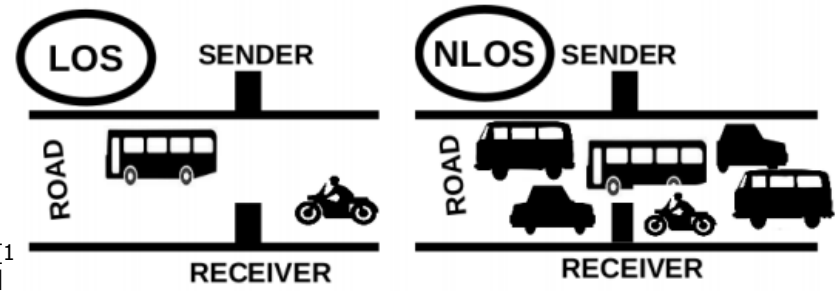
[1]



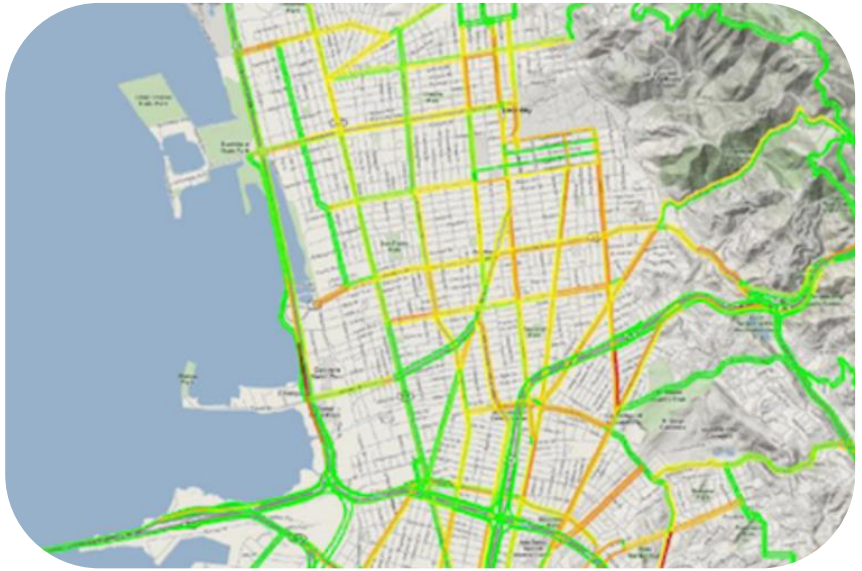
[1] Girod et al. The Design and Implementation of a Self-Calibrating Distributed Acoustic Sensing Platform. 2006.
[2] Lédeczi et al. Multiple Simultaneous Acoustic Source Localization in Urban Terrain. 2005.
[3] Sounds of New York City. 2016.

Traffic queue sensing and congestion control

[1]



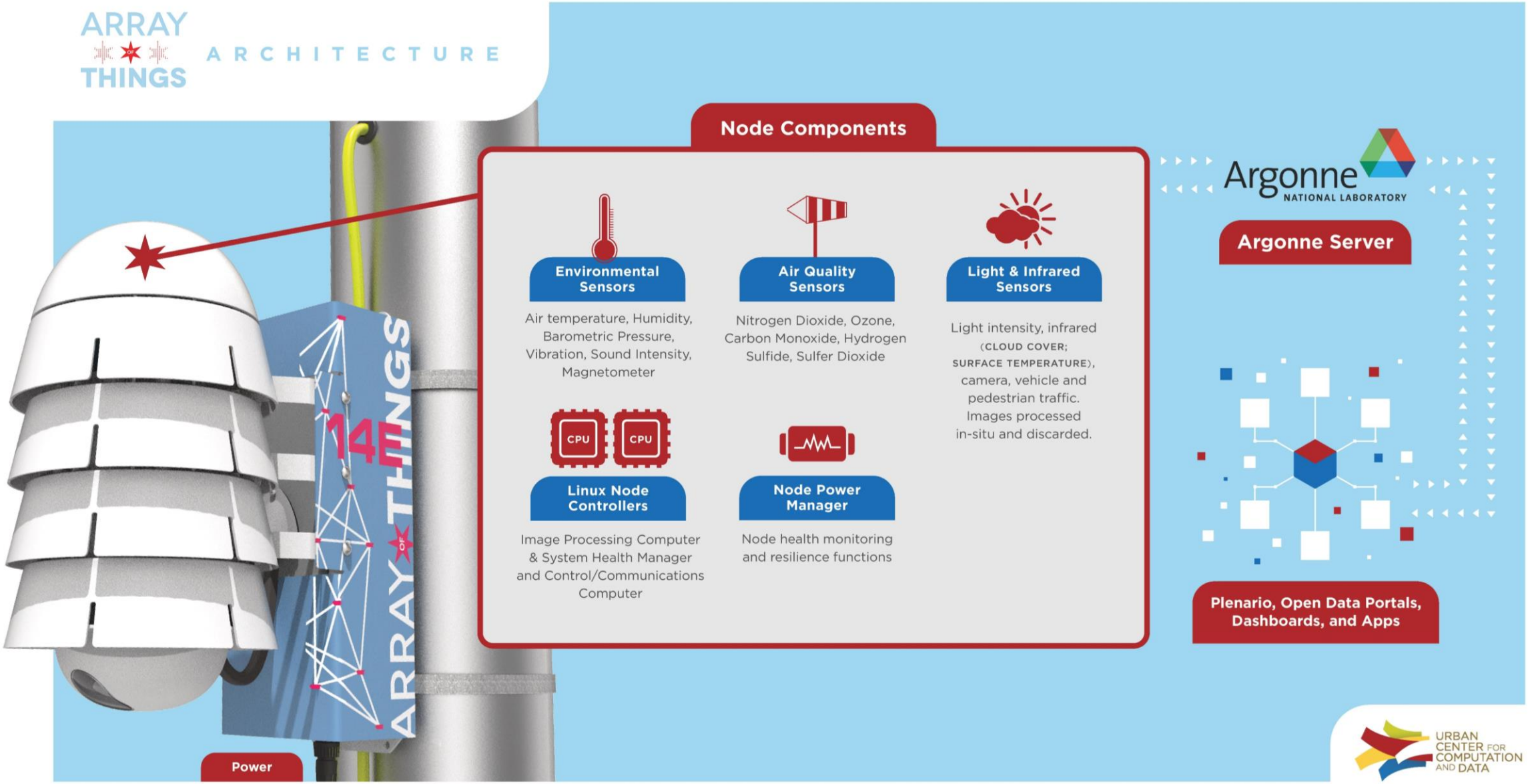
[1]



[1]

[1] Sen et al. Kyun Queue: A Sensor Network System To Monitor Road Traffic Queues, 2012

Array of Things project - Chicago



NIST

THE CITY OF COLUMBUS

Enjoy Jakarta

amsmartterdam city

HUAWEI

SMART DUBLIN

NSF

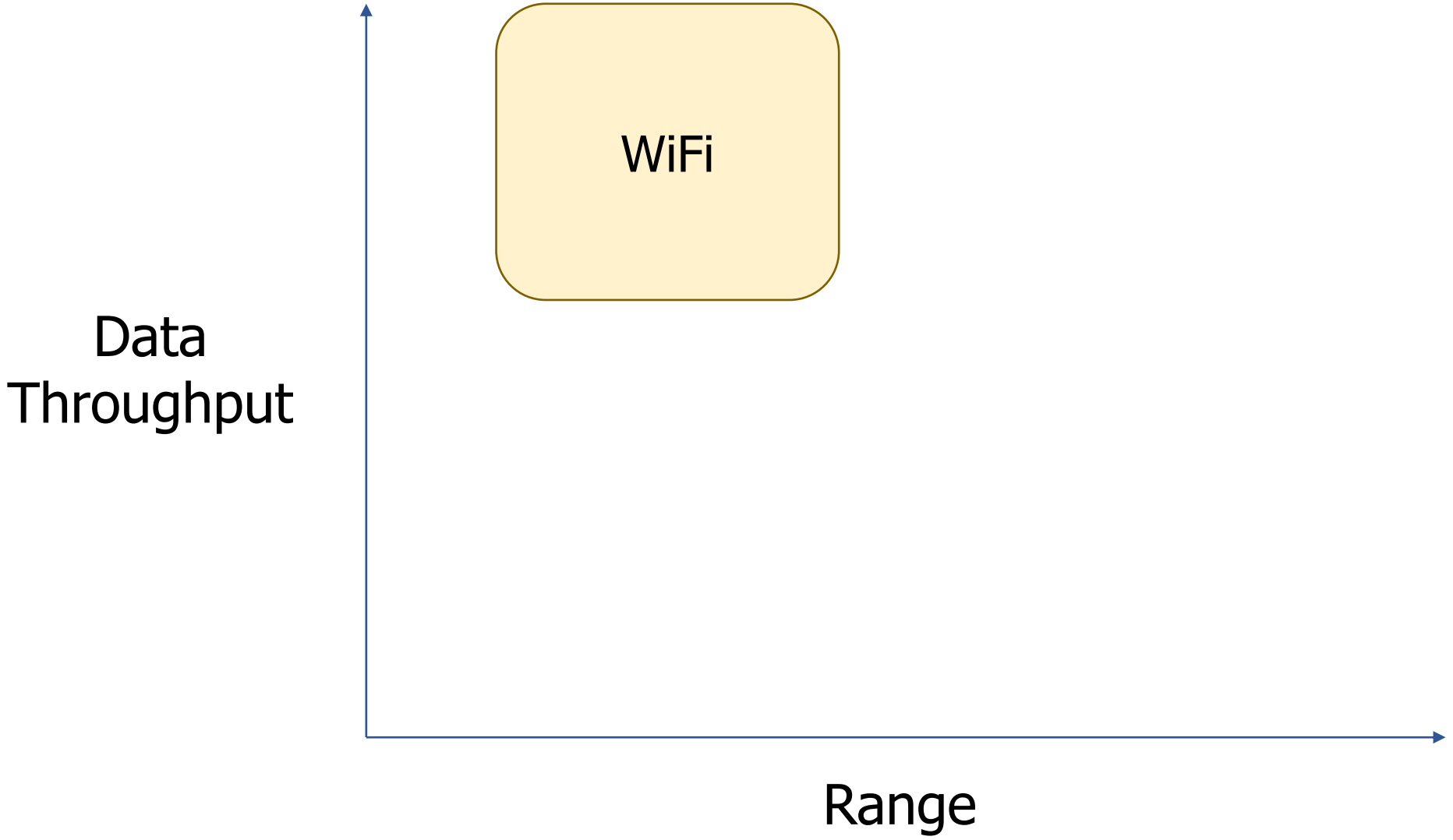
European Commission

Smart Nation SINGAPORE

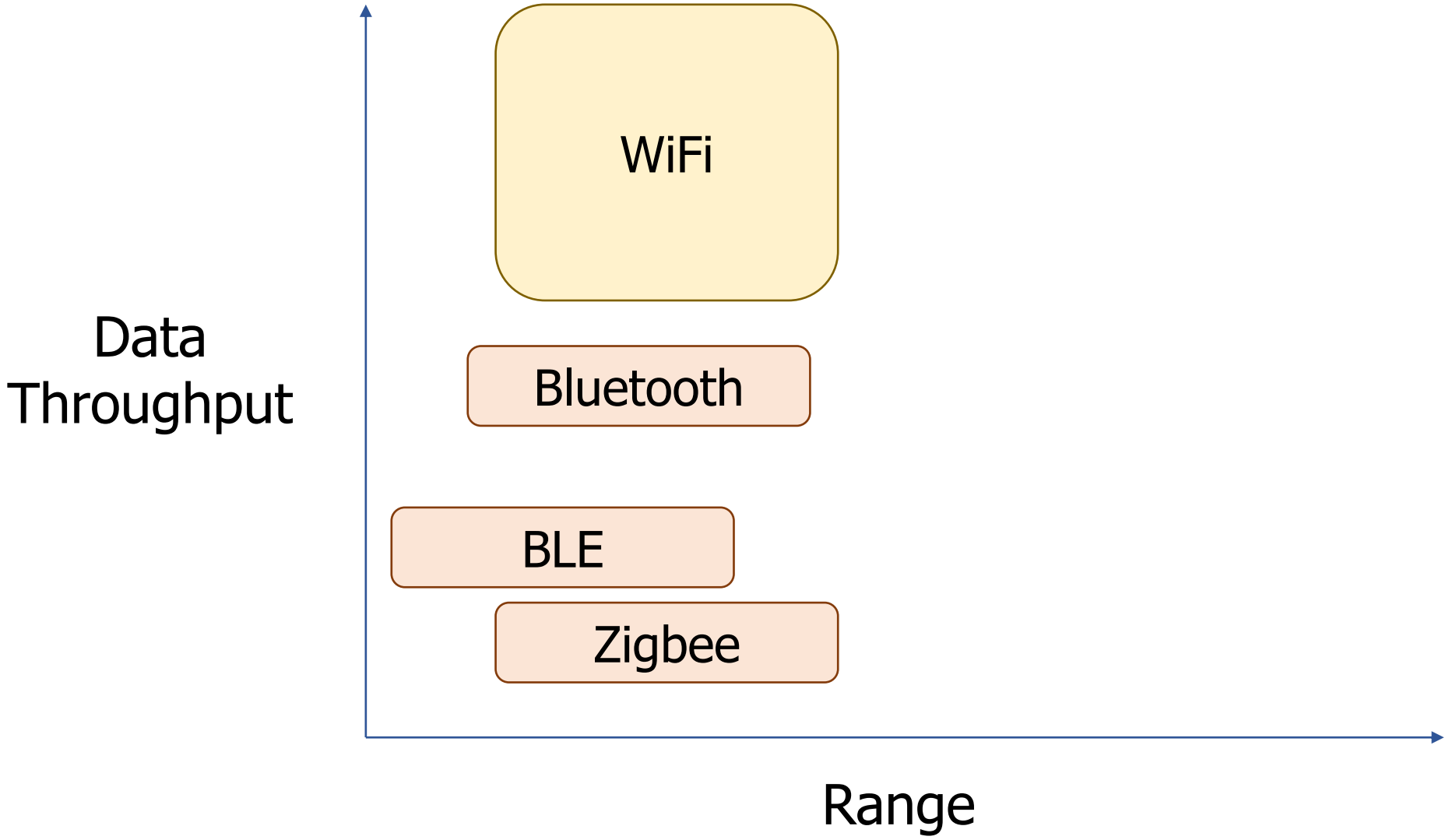
Many Smart Ideas • One Smart Nation

The City of SAN DIEGO

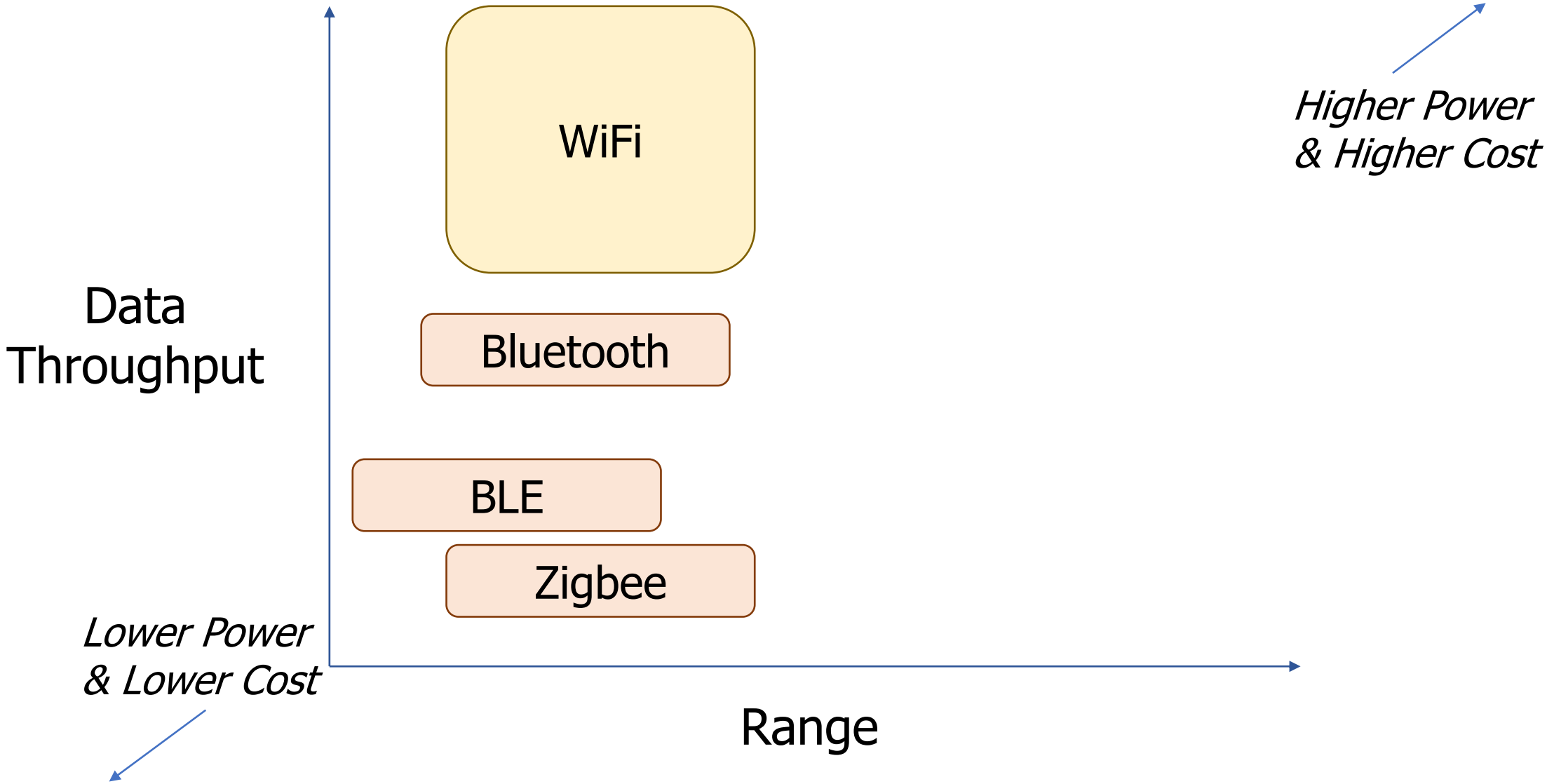
Considering wide-area networks



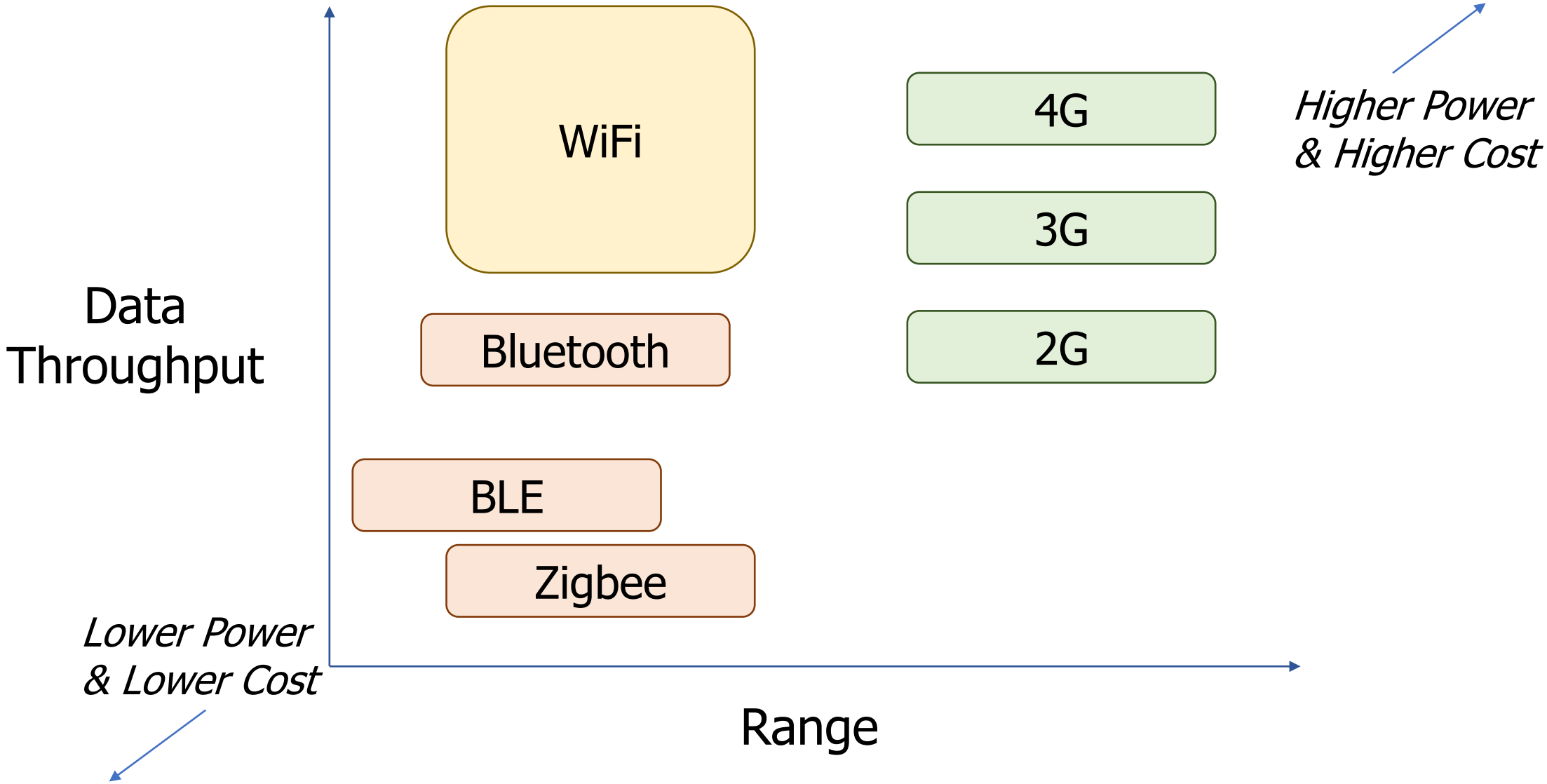
Considering wide-area networks



Considering wide-area networks



Considering wide-area networks



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

Outline

- Wide-Area Network Background

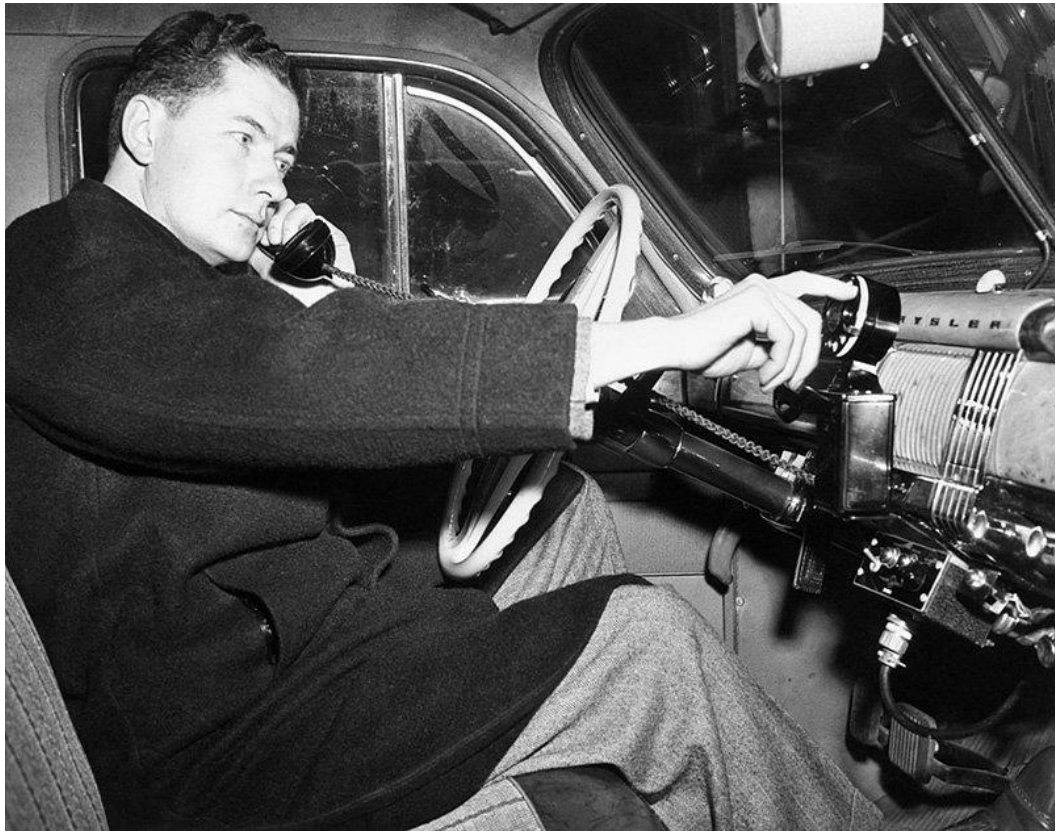
- **Cellular Network Technologies**
  - **1G**
  - 2G
  - 3G/4G and beyond

Poll: What decade was the first commercial mobile phone?

1. 1910-1920
2. 1920-1930
3. 1930-1940
4. 1940-1950
5. 1950-1960
6. 1960-1970
7. 1970-1980
8. 1980-1990
9. 1990-2000
10. 2000-2010

The first commercial mobile phone was in 1946!

- By 1948, 5000 users placing around 30,000 calls weekly



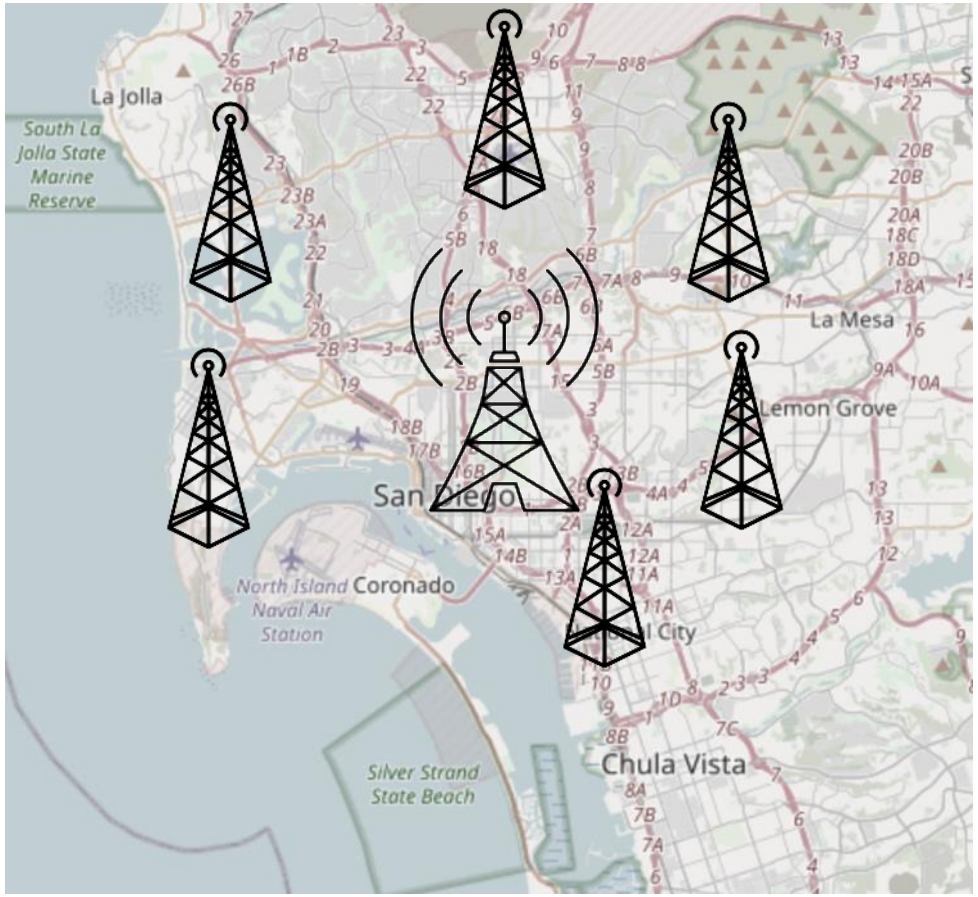
https://www.smithsonianmag.com/innovation/first-mobile-phone-call-was-made-75-years-ago-180978003/

– "The equipment, of course employing vacuum tubes, **weighed eighty pounds, filled much of a vehicle's trunk and drew so much power that it would cause the headlights to dim.** Service cost $15 per month, plus thirty to forty cents per local call, equivalent to $175 2012 dollars, plus $3.50 to $4.65 per call. "

https://ethw.org/The_Foundations_of_Mobile_and_Cellular_Telephony

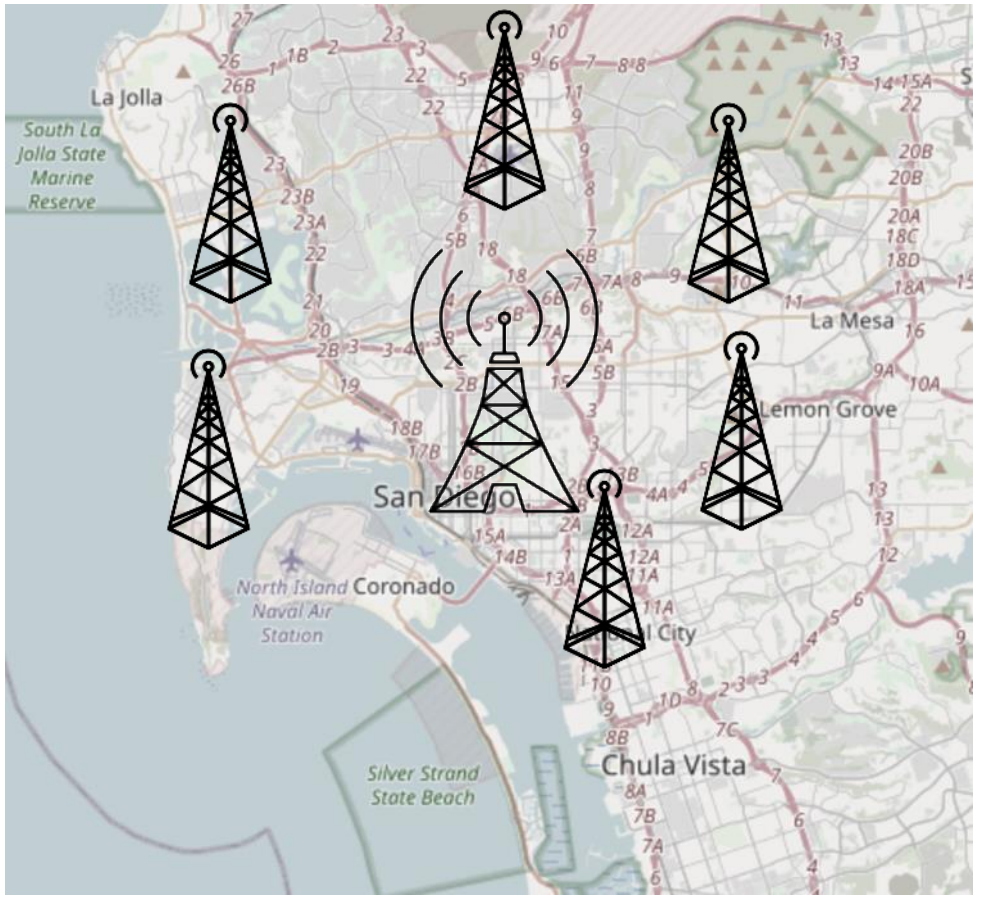
The first `mobile` network architecture

- Single transmitter tower, multiple receiver towers
  - **Why?**



The first `mobile` network architecture

- Single transmitter tower, multiple receiver towers
  - **Why?** Transmission energy of phone!
- Medium Access Control?
  - Push-to-talk [half-duplex]
  - City-wide "party line"
  - Maximum of three concurrent callers



1965: The Improved Mobile Telephone Service

- "More spectrum"
  - Bell: VHF Low (35-44 MHz, 9 channels),
    VHF High (152-158 MHz, 11 channels),
    UHF (454-460 MHz, 12 channels)
  - 7 channels at VHF, and 12 channels at UHF for "RCCs" (Radio Common Carriers)
    - These will end up becoming pagers, mostly
- "Full Duplex"
  - Implemented as channel pairs (two half-duplex)

Phones fit in a briefcase now

- Increased spectrum is still not enough
  - Limited to 40,000 total subscribers
  - E.g. NYC had 2,000 people on 12 channels with a typical wait of 30 minutes to place a call

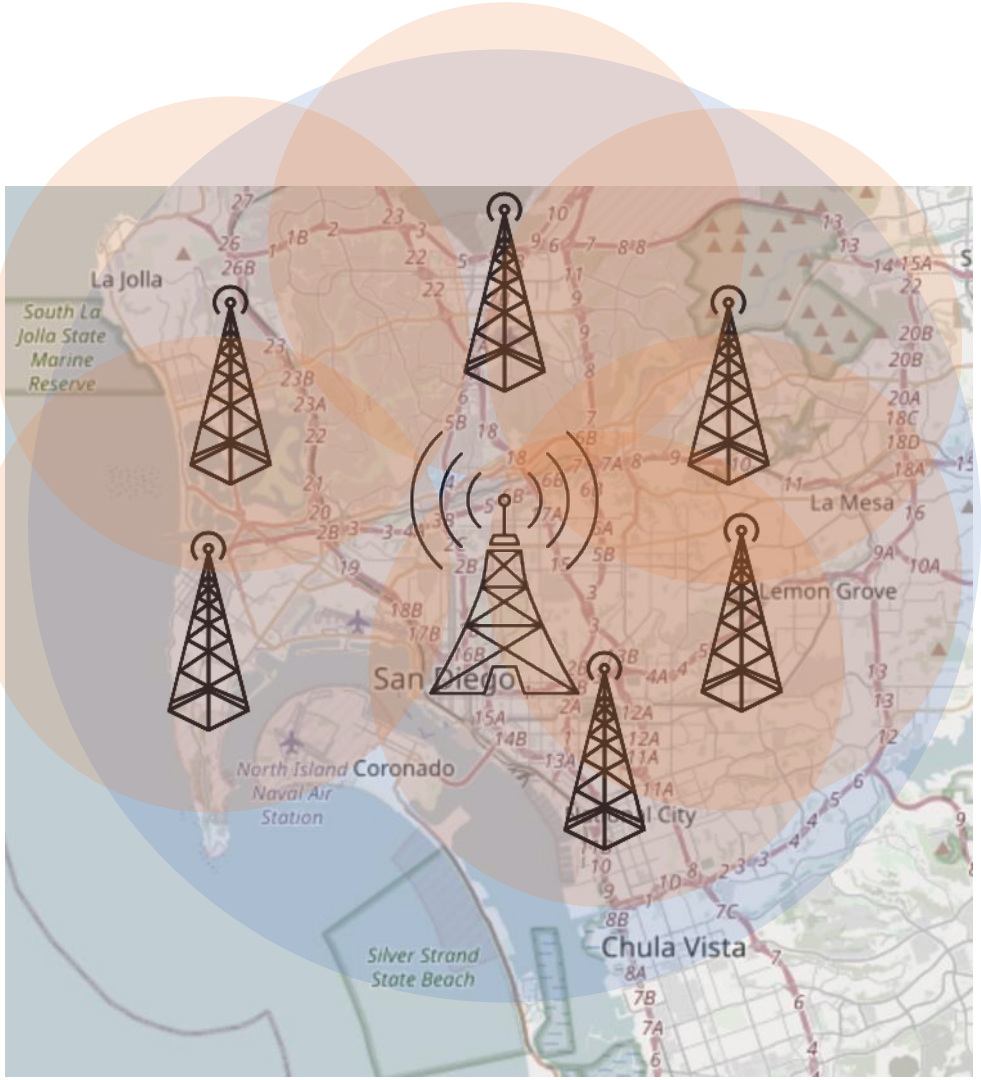
Quick review: How can we share spectrum?

- Frequency division
  - Already doing that
- Time division
  - Already doing that
- Code division
  - Won’t come to [US…] mobile networks until the 80’s

- Spatial division!!

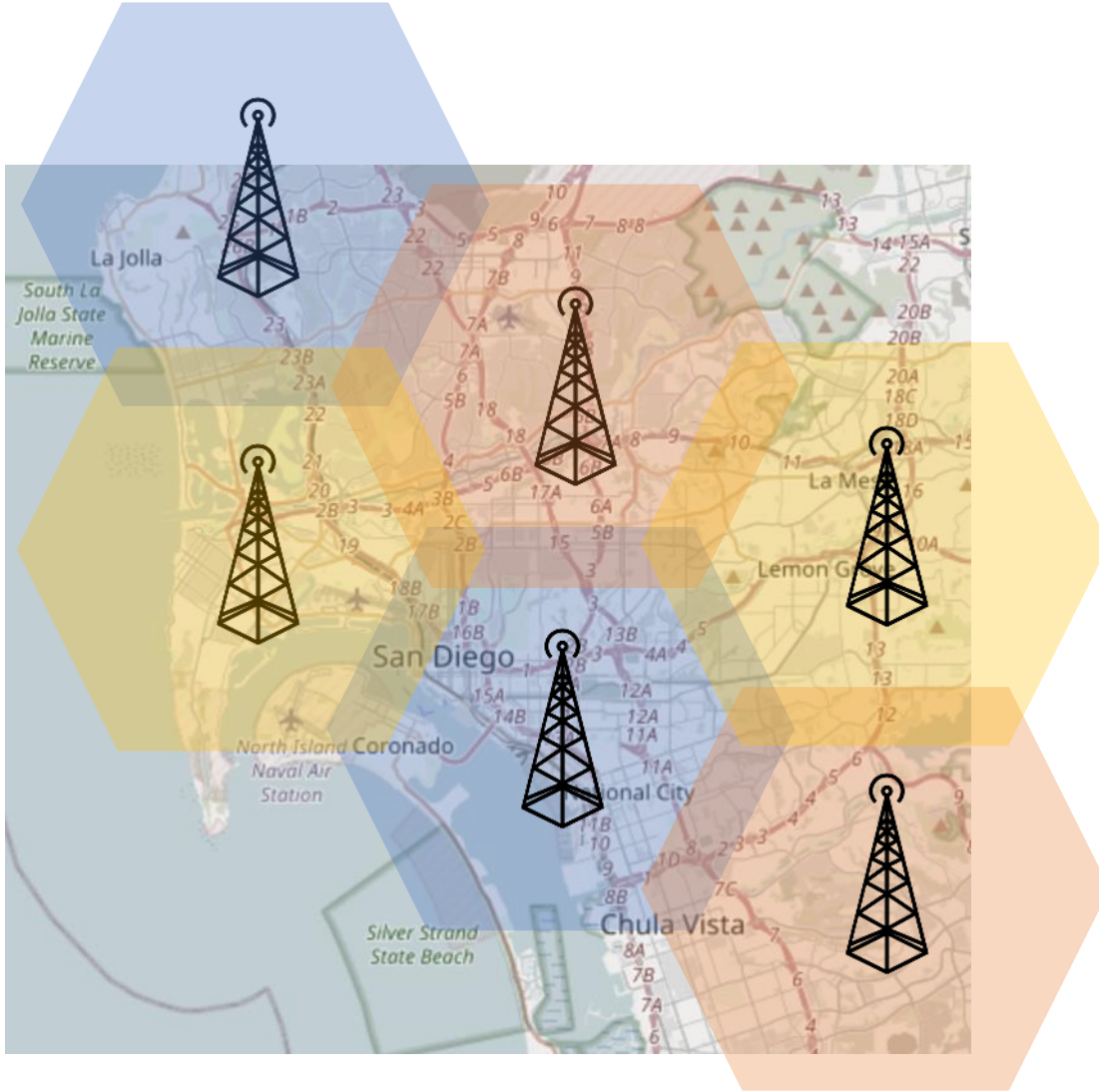
What's ~~wrong~~ inefficient with this picture?

- Early mobile networks handled the mobility challenge with wide-area coverage
- The active user could be anywhere in the 40~60 mile range of the transmit tower
  - So they had exclusive access to that whole area!
- 12 frequency channels → 12 users



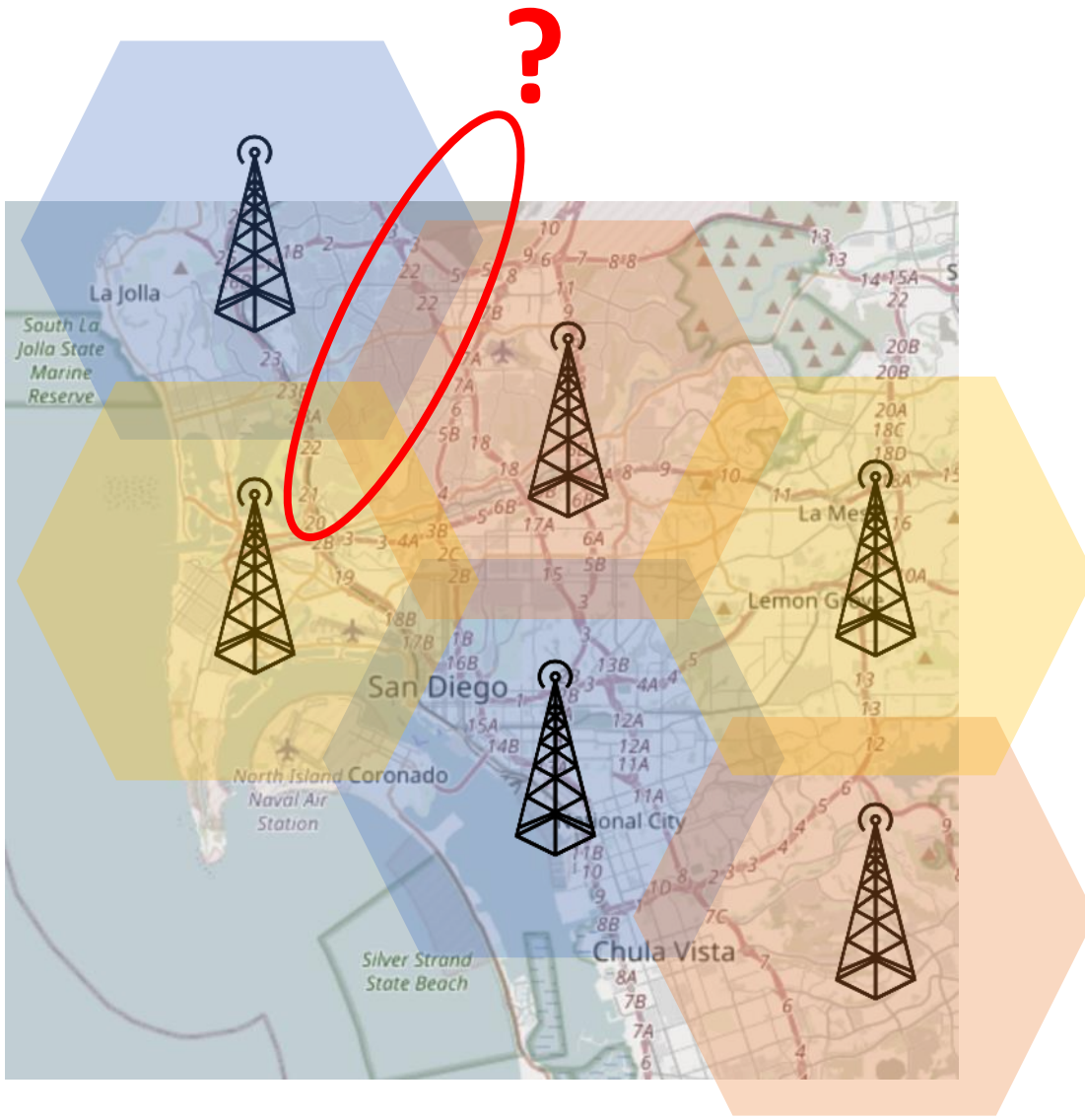
The “cell” in cellular networks

- Cells use *spatial* division
  - Reduce transmit power, smaller area
- Now…
  - 12 / 3 = 4 channels per cell
  - * 6 cells in area
  - = 24 users of same spectrum!
- And we can choose the cell size based on our expected needs



Spatial division tradeoffs

- Need more infrastructure (more towers)
- Need logic to support handoff
  - Cellular concept in Bell labs at 1947 [one year after first mobile], but no handoff solution yet



How often does handoff need to happen anyway?

- Really a question of "how big are cells"

- A back-of-envelope answer for "Handoffs per 3-minute call":

	Speed (mph)	Speed (kph)	Cell Radius (km)	Handoffs
Freeway, rural	65	104	16	0.33
Freeway, urban	65	104	1.6	3.25
Surface streets, urban	30	48	1	2.4
Pedestrian, urban	1.5	2.4	1	0.12
Pedestrian, microcell	1.5	2.4	0.1	1.2

Table data from Arthur H. M. Ross, PhD: http://www.cdg.org/technology/cdma_technology/a_ross/handoff.asp

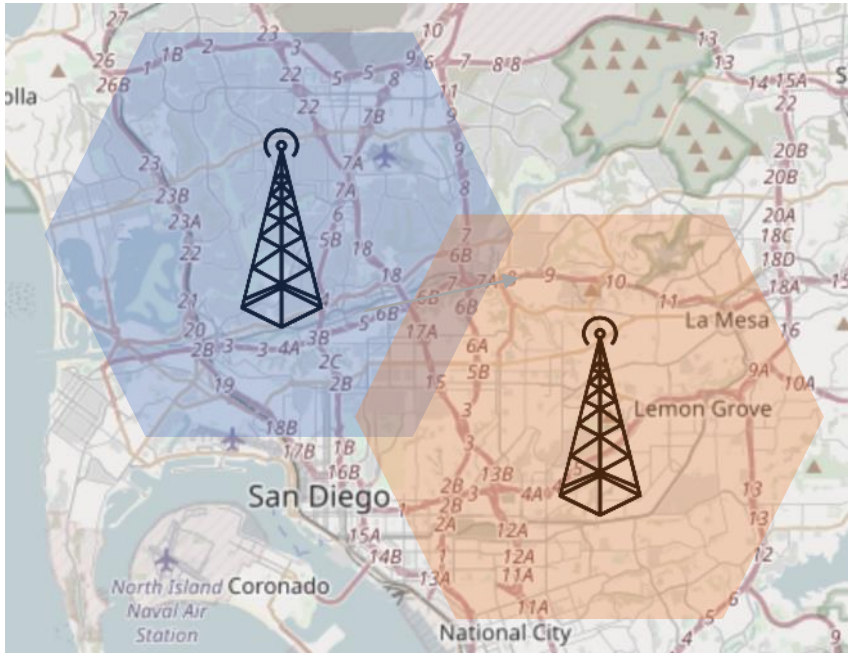
Introducing 1G! (First Generation)

- AMPS — Advanced Mobile Phone Service (circa 1983)
  - Other 1G's:
    - Nordic Mobile Telephone (NMT) — Nordics, Eastern Europe, Russia
    - Total Access Communications System (TACS) — UK, West Germany, Portugal South Africa
    - Radiocom 2000 — France

- 1G is defined by:
  - Analog voice channels
  - Established by digital control channel ← **handoffs**

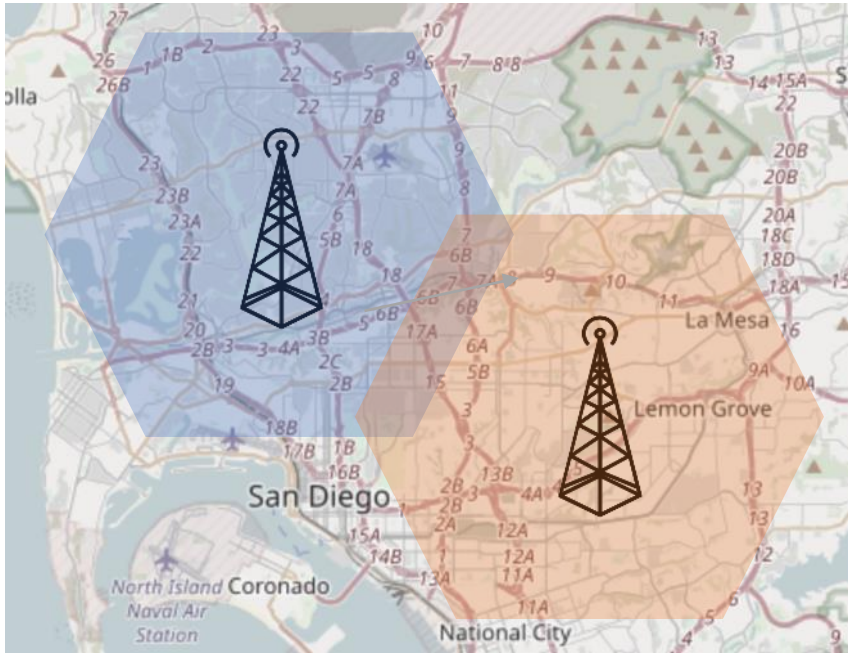
Break + Discussion: How to implement handoff?

- <brainstorm>



How does AMPS implement handoff?

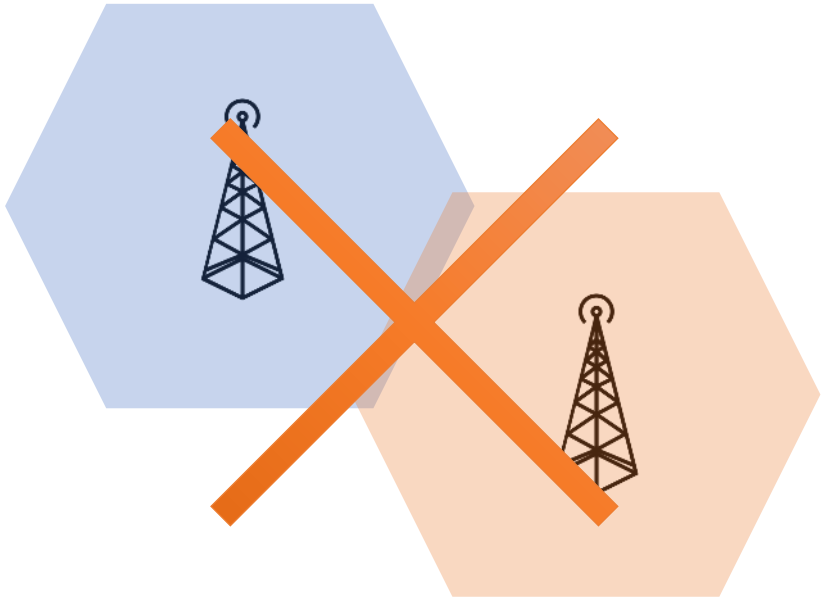
- Base station detects weak signal
- Base station tells mobile about new, better tower
- Base station sends cutover trigger

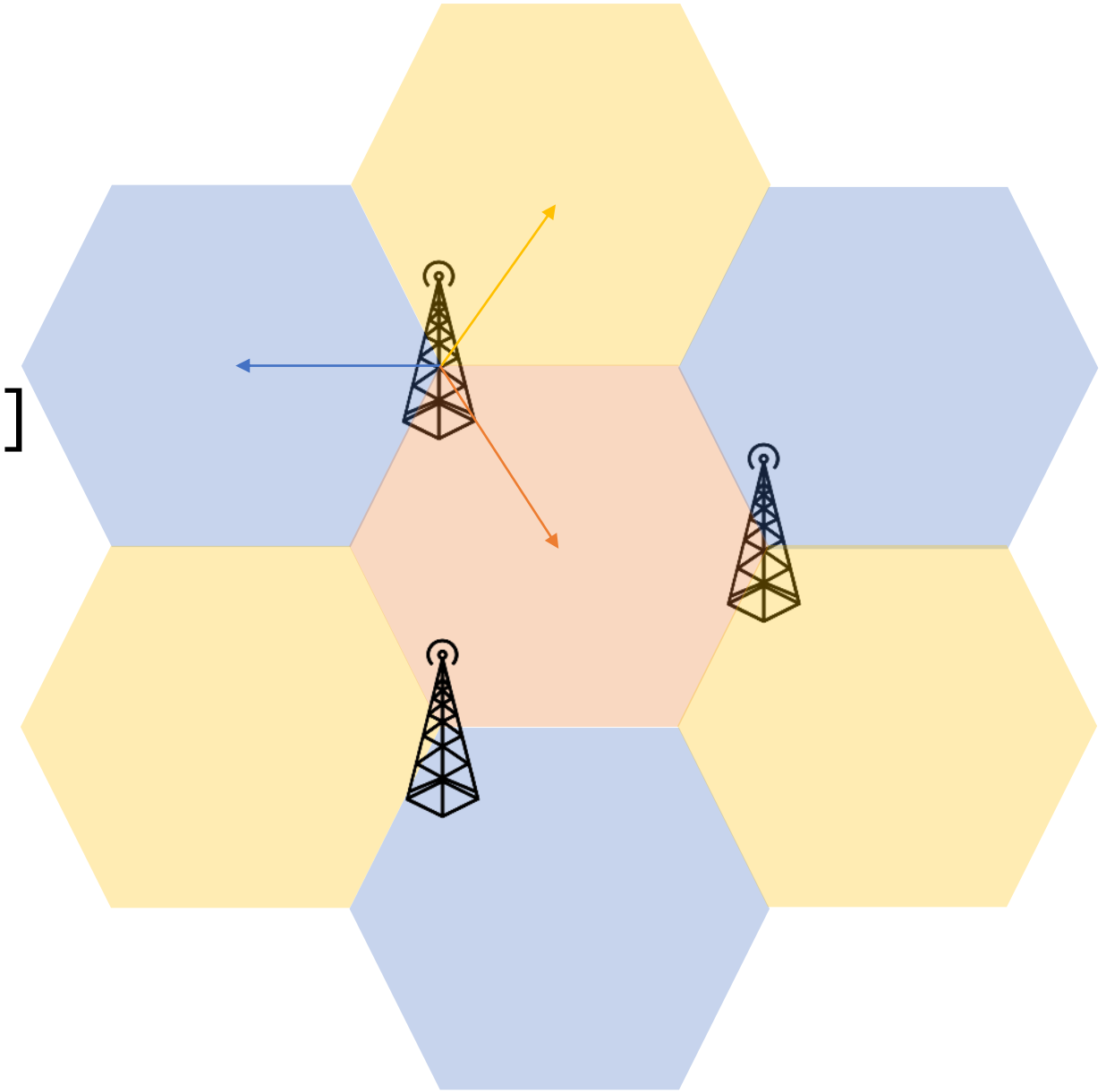


- Lots bad about this:
  - No `make before break` — many drops!
  - Mobile has better estimates than base station

Spatial division in practice

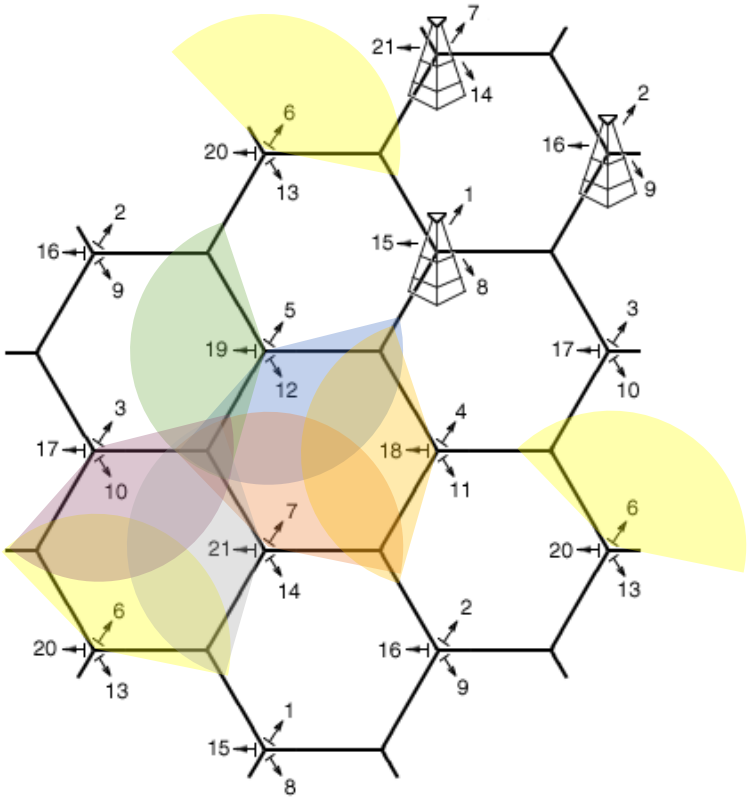
- Directional antennas at tessellation corners provide redundant coverage [robustness!]





Spatial division in practice

- Directional isolation is imperfect, requires many bands in practice
  - ~5-7 cells are within conflict range, so we need to divide channels by ~7



Over time, AMPS did also get more frequencies

- AMPS in the US:
  - 850 MHz band
  - Divided into “A” block and “B” block
    - Granted to local phone company and “wireless company” respectively
  - Each block had 21 control, 395 voice channels
    - Divide by 7 to get voice channels per cell: ~56
    - So ~56 users per cell, rather than 12 for the entire city

- Several expansions of this frequency block
  - Most interesting: in 1989 UHF TV channels 70-83 added 666 more channels

The first "sunset"

- Single-user analog channels is not very efficient
- Wireless carriers want to replace 1G
  - *Key Takeaway:* Spectrum allocation is the most scarce resource, therefore want to maximize efficiency of its use
    [*efficiency:* number of paying customers / spectrum?]

- But many things in the built environment rely on AMPS
  - Because when *they* were built, AMPS was the most reliable
    - OnStar
    - ADT home alarms [got sued!]
  - Some systems made adapters, others just stopped working

- FCC required network support until early 2008 (dropped soon after)

Aside: Super cool hackaday projects

- Building your own 1G network!
  - https://hackaday.com/tag/amps/
  - https://github.com/unsynchronized/gr-amps

  - ⚠ ⚠ ⚠ This uses spectrum you do not own ⚠ ⚠ ⚠
    - **"The FCC can levy fines of up to $11,000, per transmitter, per day, with up to six months in federal prison, for violations of the Code of Federal Regulations."**
    - Could deploy with wired connections though…

Outline

- Wide-Area Network Background

- **Cellular Network Technologies**
  - 1G
  - **2G**
  - 3G/4G and beyond

IS-54 aka 2G aka TDMA aka D-AMPS (Digital AMPS)

- Deployed ~1993

- Used TDMA to share AMPS channels
  - Each AMPS analog channel-pair was 30 kHz
  - Digital compression allowed for 3 time slots per channel — tripled capacity!
    - Later iterations would compress further, 6 time slots per channel
    - Without additional bandwidth: 6*56 = 336 simultaneous devices per cell

- Beat out competing FDMA analog solution from Motorola
  - Narrowband AMPS, "N-AMPS", compressed calls to fit in 10 kHz channels

- Also encrypted [poorly: CMEA broken publicly in 1997]

GSM aka 2G aka TDMA

- Wait, didn't the last slide say 2G was something else?

  IS-54 **aka** 2G **aka** TDMA **aka** D-AMPS **(Digital AMPS)**

- What is "2G" then?
  - Exactly.
  - "2G" isn't one technology, it's a collection of "second generation" protocols
  - This is true for later generations too

The first 2G sunset happened in 2008

- D-AMPS was sunset when AMPS was sunset
- Modern “2G” is all GSM
- And if you think this is confusing, it only gets worse
  - Anecdata: Pat as a Qualcomm intern in 2010 asked everyone I met there “what actually is 4G,” and every engineer just laughed at me

GSM

- So can we just call modern 2G "GSM"?

- "Global System for Mobile Communications"
  - It is a standard [the dominant 2G]
  - GSM meant "phone" for a while in parts of Europe
    - (and apparently still in Belgium?)
  - GSMA is the GSM Association; which a lot of people just call GSM
    - Because GSM made [a] 3G and LTE [which is a 4g?] and 5g [ish! more next time]
  - Yay.

Origins of GSM

- An incredible sweet spot of timing, technology need, and politics?

- 1987: 13 European countries sign accord to use one wireless standard
  - 10 months later: GSM standard ratified
  - Insight: Not a ton new in GSM by '87, just a *lot* of arbitrary design decisions

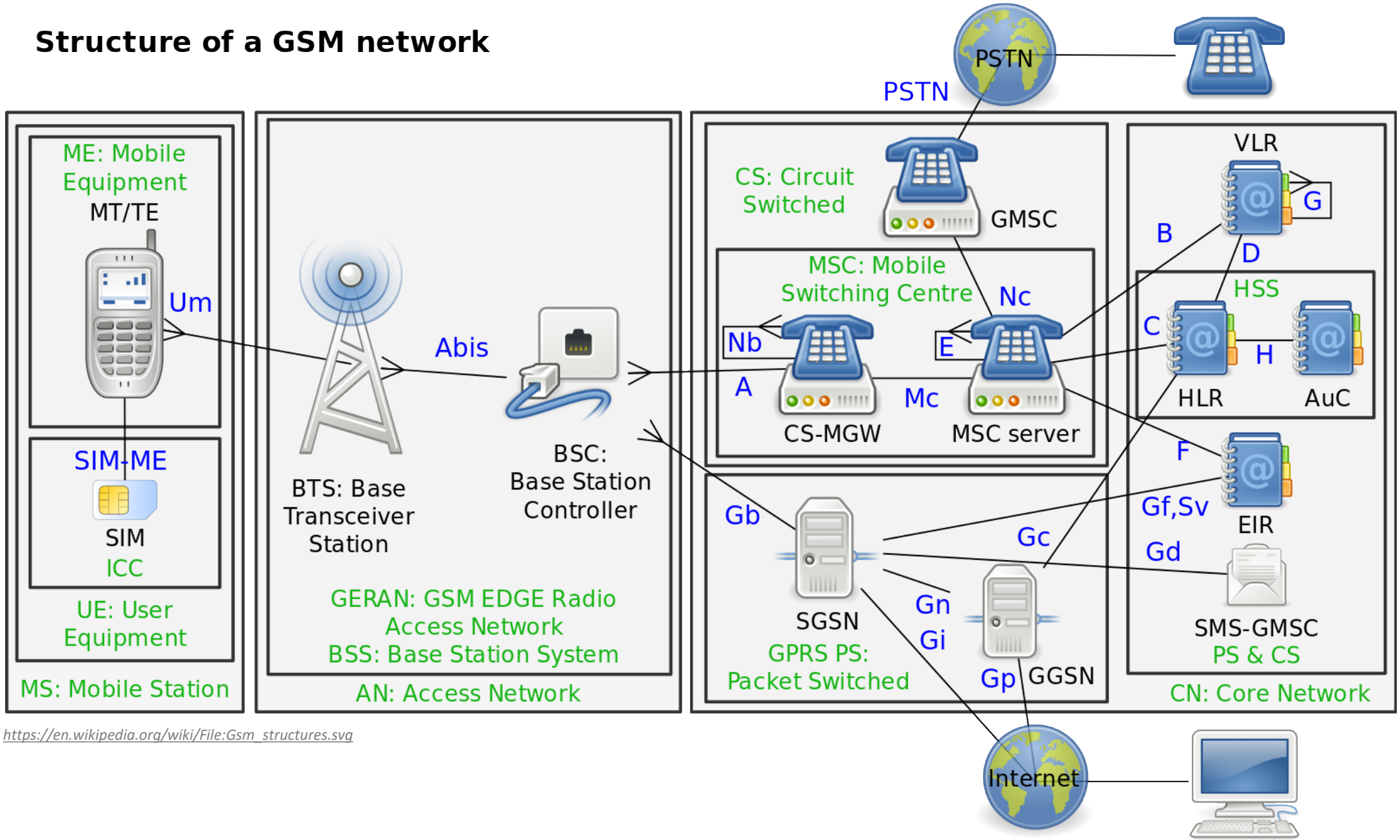
The real innovation of GSM was the indirection and interoperability it enabled

- Europe hit this problem before the US because the US is large
  - (and US telecoms owned/operated subsidiaries in Canada)

- Coincided with major growth in global mobility
  - Mobile devices needed to be able to use other carriers infrastructure

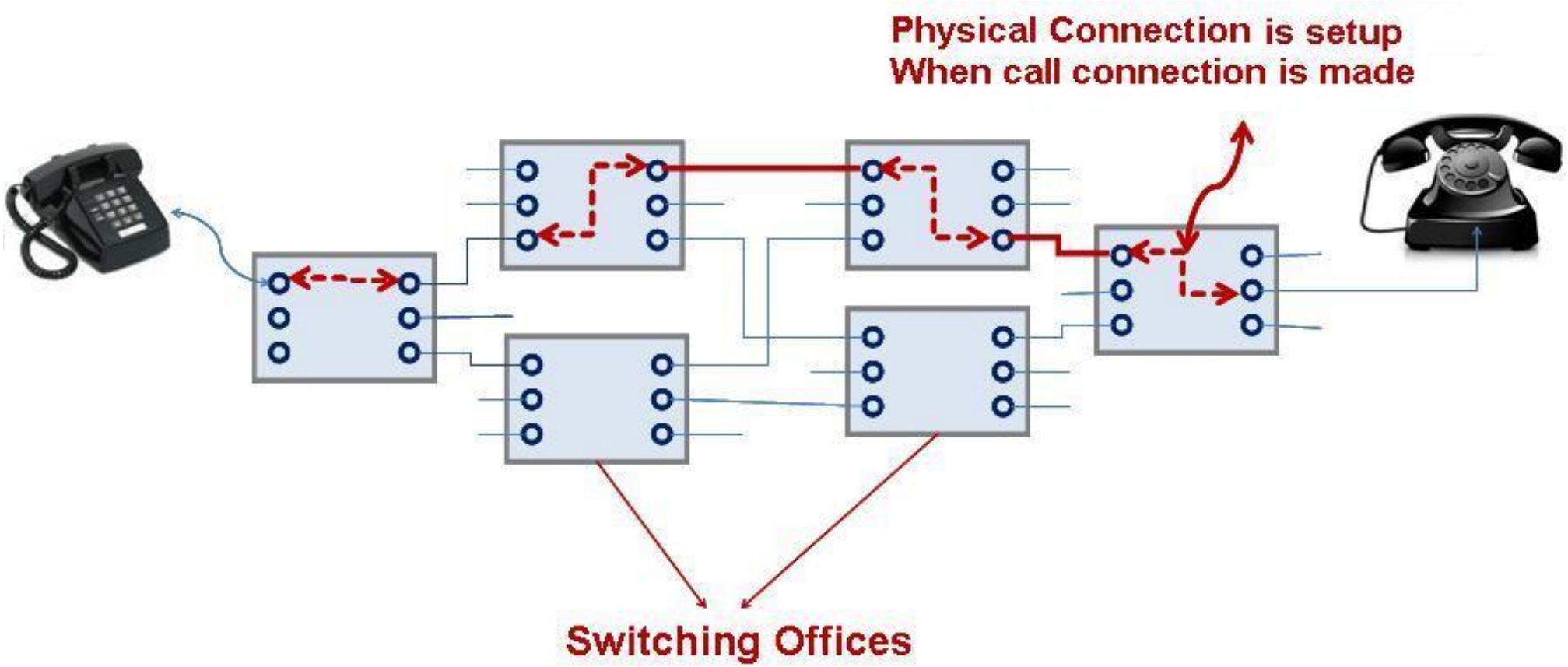
- Early GSM isn’t anything fancy in modulation, data, etc
  - It’s all about the control channels

Structure of a GSM network



https://en.wikipedia.org/wiki/File:Gsm_structures.svg

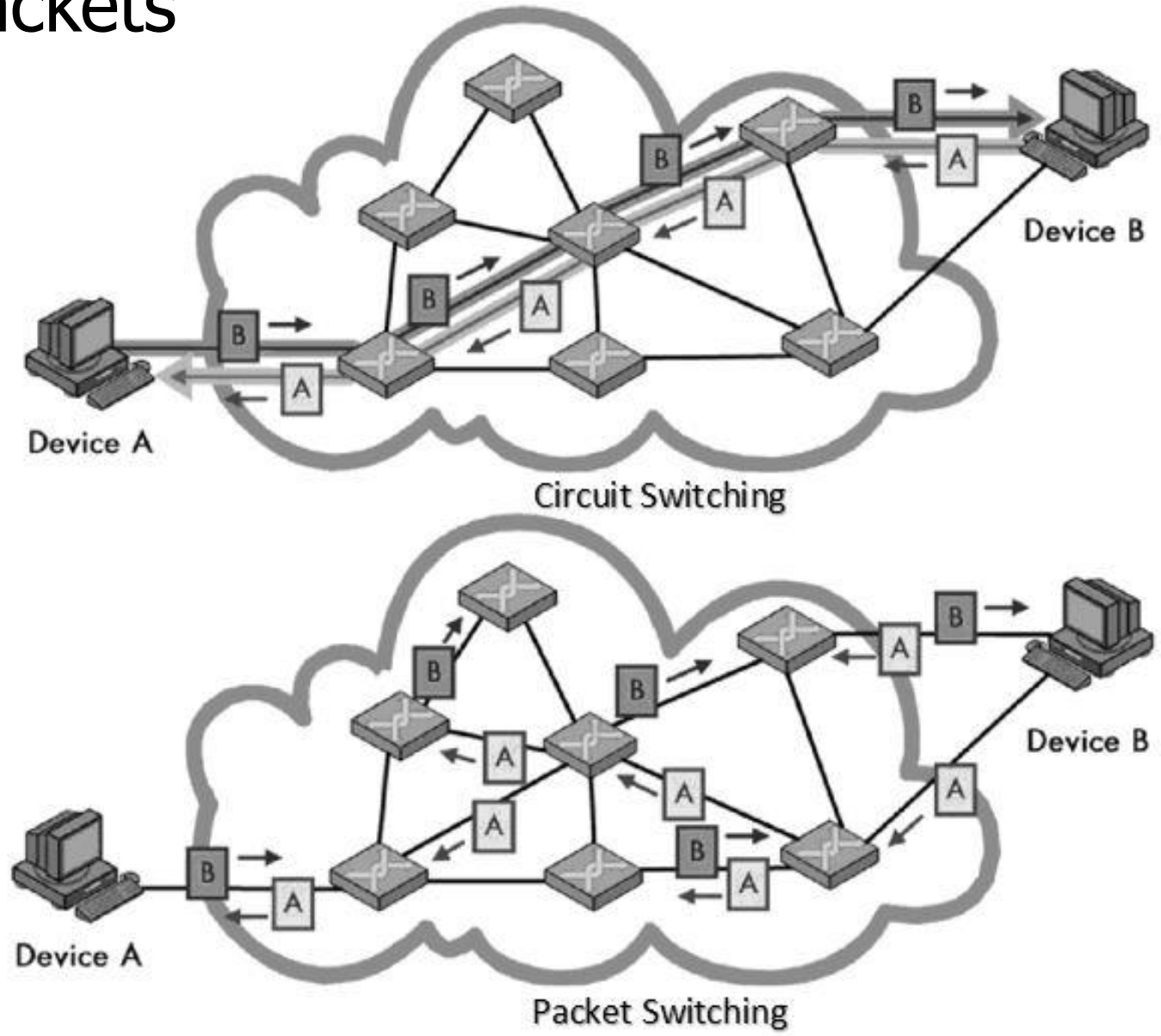
Circuit switching



Comparing circuits vs packets

- Circuit switching
  - Virtual electrical connections between two devices
  - Full capacity is dedicated to only those two devices

- Packet switching
  - Chunks of data get routed between devices
  - Overhead to figure out where they go



GSM evolved over time to add data

- GSM was voice-only at first

- Then overlaid data on the voice channel
  - Circuit Switched Data (CSD)
    - 9.6 — 14.4 kb/s
    - Previous hacks were literally cell phone calling a modem (~3.5 kb/s); same concept

- Then added actual packetized data [“2.5G”]
  - General Packet Radio Service (GPRS)
    - Throughput 9.2 – 21.55 kbit/s/timeslot [goodput 8-20 kbit/s/timeslot]
  - Enhanced Data Rates for GSM Evolution (EDGE)

So why does the IoT care about 2G?

1. It's easy to implement
   - 2G == GMSK, 3G = QPSK [requires linear PA], 4G = …

2. It's cheap
   - Relative to other cellular plans, anyways

3. It's low power*
   - *For select IoT workloads
   - Energy-per-bit of continuous stream improves each generation
   - Energy-per-event of infrequent event is more tricky though

Why might 2G continue to survive [globally]?

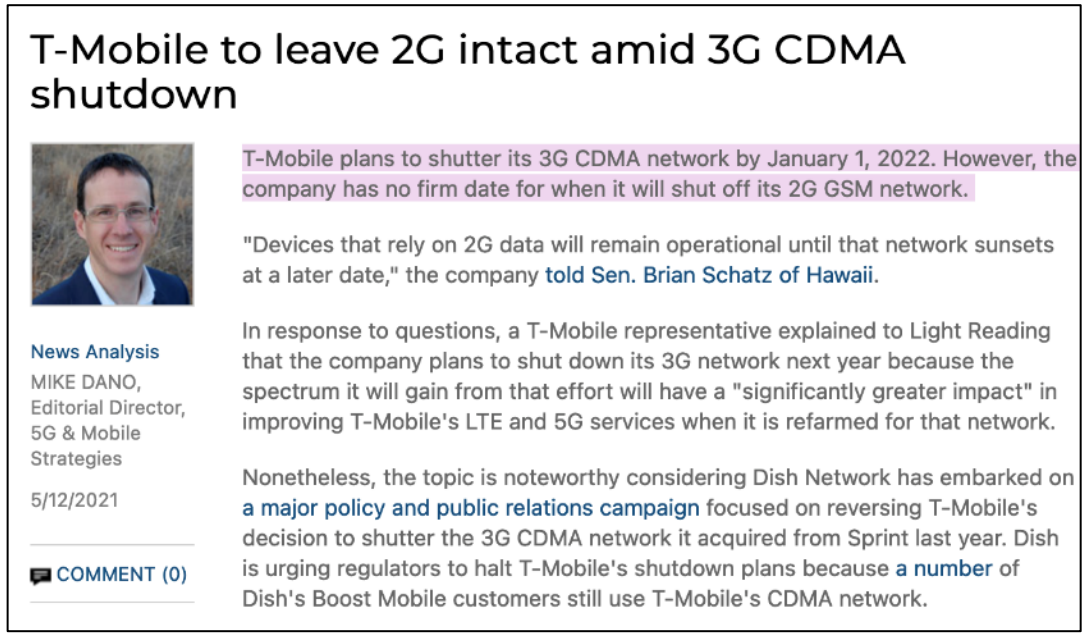
1. More coverage for lower costs
   - 2G has longer range than 3G
2. It fills the legacy niche
   - High performance HW includes fallbacks
     - 2G/3G radios, then 2G/3G/4G radios, now 2G/3G/4G/5G radios
     - Consider the iPhone 13 Pro (2021):
   - Brick phones still popular!

Network

- 5G (600 MHz, 2.5 GHz, mmWave, Standalone (SA))
  - n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79, n258, n260, n261
- 4G LTE
  - 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 34, 38, 39, 40, 41, 42, 46, 48, 66, 71
- 3G / 4G (HSPA / UMTS / HSPA+)
  - 850, 900, 1700/2100, 1900, 2100 MHz
- 2G (GSM, GPRS, and EDGE)
  - 850, 900, 1800, 1900 MHz

2G in the US… [Plans]

- AT&T stopped servicing 2G networks in 2016
- Verizon Wireless also phased out its 2G CDMA network at the end of 2020
- Sprint will shut down their 2G CDMA network in April 2022
  - Unclear if this happened or not
- T-Mobile plans on ~~2023~~ ~~April 2024~~
  No firm date at this time



T-Mobile to leave 2G intact amid 3G CDMA shutdown

News Analysis

MIKE DANO, Editorial Director, 5G & Mobile Strategies

5/12/2021

COMMENT (0)

T-Mobile plans to shutter its 3G CDMA network by January 1, 2022. However, the company has no firm date for when it will shut off its 2G GSM network.

"Devices that rely on 2G data will remain operational until that network sunsets at a later date," the company told Sen. Brian Schatz of Hawaii.

In response to questions, a T-Mobile representative explained to Light Reading that the company plans to shut down its 3G network next year because the spectrum it will gain from that effort will have a "significantly greater impact" in improving T-Mobile's LTE and 5G services when it is refarmed for that network.

Nonetheless, the topic is noteworthy considering Dish Network has embarked on a major policy and public relations campaign focused on reversing T-Mobile's decision to shutter the 3G CDMA network it acquired from Sprint last year. Dish is urging regulators to halt T-Mobile's shutdown plans because a number of Dish's Boost Mobile customers still use T-Mobile's CDMA network.

Does GM ever learn? [Could they have?]

- What would you put in cars if you were the PM of OnStar today?

— What is the 2G network sunset and how does it affect my OnStar service?

As cellular carriers transition to 4G or 5G connectivity, vehicles using a 2G connection will lose OnStar service. In the U.S., most major network providers will complete the transition in December 2022. After the transition, 2G network connectivity will no longer be provided. The decision to sunset these networks was made by the wireless network providers and the need to upgrade to newer technology.

Certain GM vehicles on the road today currently leverage the 2G network for OnStar connectivity. Once the 2G network sunsets, the three-button interface in your vehicle will be deactivated.

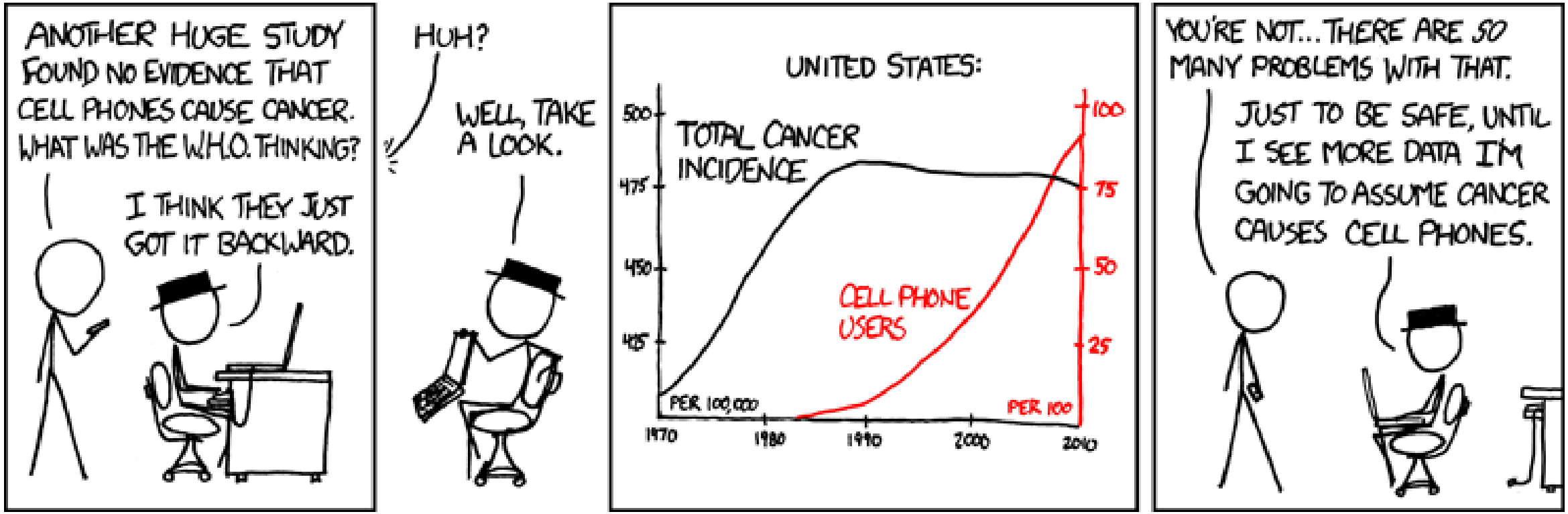
— Which GM vehicles are impacted by the deactivated 2G network?

In the U.S. and Canada, certain 2015 model year and older GM vehicles will be affected when 2G networks are upgraded. This also may include former GM brands, such as Pontiac, Saturn and HUMMER.

— What options are available to Members after the 2G sunset occurs?

GM is actively working to evaluate options for OnStar Members who will be impacted by the 2G network sunset. Due to ongoing semiconductor shortages, GM is discontinuing the previously announced OnStar Link adapter program. Program updates will be announced at a later date.

Break + xkcd



https://xkcd.com/925/

Outline

- Wide-Area Network Background

- **Cellular Network Technologies**
  - 1G
  - 2G
  - **3G/4G and beyond**

Starting with the end: the 3G sunset

- [As of Oct, 2021] announced retirements:
  - Verizon: Dec 2022
  - AT&T: Feb 2022
  - T-Mobile: Finally got there in July 2022 (after months of delays)

- 2G reminder
  - Verizon and AT&T actually did sunset 2G
  - T-Mobile plans on ???

AT&T has experience in this area. The operator discontinued service on its 2G network in 2017. According to AT&T's filings with the SEC around that time, it counted 4 million customers on its 2G network, the bulk of which were IoT devices.

AT&T: 2.7% of customers will be affected by 3G shutdown

Why does 2G have staying power that 3G doesn't?

- T-Mobile's letter to Congress on 2g/3g sunset
  - n.b. Senator Schatz seems to get this stuff

6. How will the 2G and 3G shutdown impact non-cellular devices and other devices and systems that are not mobile phones on your networks? How many of these devices will be impacted in each state?

Non-cellular, data-only devices that rely on 3G data will need to be capable of LTE operation or will need to be upgraded. Devices that rely on 2G data will remain operational until that network sunsets at a later date, but such devices should still be upgraded in the long term.[6] For this response, we interpreted "non-cellular device" to mean any device that is not a feature phone or a smartphone. Non-cellular 2G/GSM and 3G/UMTS active devices accounted for less than 1% of traffic on the T-Mobile network as of the week of April 11, 2021.

[6] Note that all non-cellular 3G/UMTS devices also have 2G/GSM capabilities.

So what did [*]G provide over 2G anyway?

- Biggest thing is throughput
- And a spectrum land-grab
  - Wireless providers advocated [successfully] for [global] release of additional spectrum to support new, faster wireless
  - Lots of [initial] 4G rollout also on new spectrum
    - But no more coming — sunsets only way to get more 4G spectrum
  - 5G is [mostly] on much higher bands, not suited for 4G

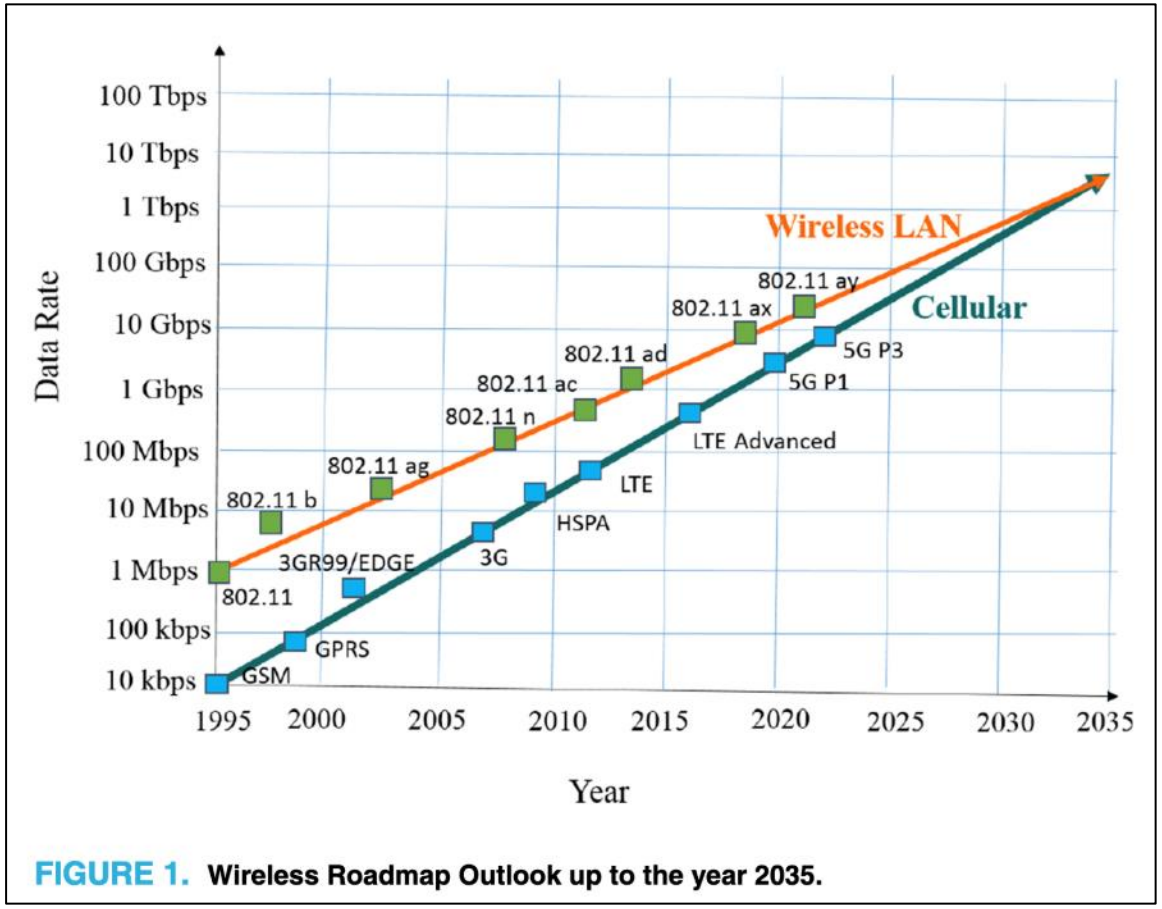


FIGURE 1. **Wireless Roadmap Outlook up to the year 2035.**

Terahertz Band: The Last Piece of RF Spectrum Puzzle for Communication Systems (preprint; Elayan et al.)

Aside: Eventually, the naming thing got annoying, so an international standards body fixed* it

*Yeah, you know how this story will end

- The International Telecommunications Union (ITU) is a UN branch
  - ITU-R set standards for what can be considered "a 4G technology"

- "Generations" are now defined by speed
  - E.g. to qualify as "a 4G technology": 100 Mb/s+ (mobile), 1 Gb/s+ (stationary)

  - Fun game: How fast is LTE?
    - LTE spec maxes out at 300 MB/s down and 75 MB/s up
    - It seems LTE has been retroactively classified as 3.95G
      - [By everyone except the wireless carriers?]

Corollary to improved throughput is improved energy performance

- Same philosophy as high-performance architecture, etc
  - There is always baseline load, which going faster amortizes

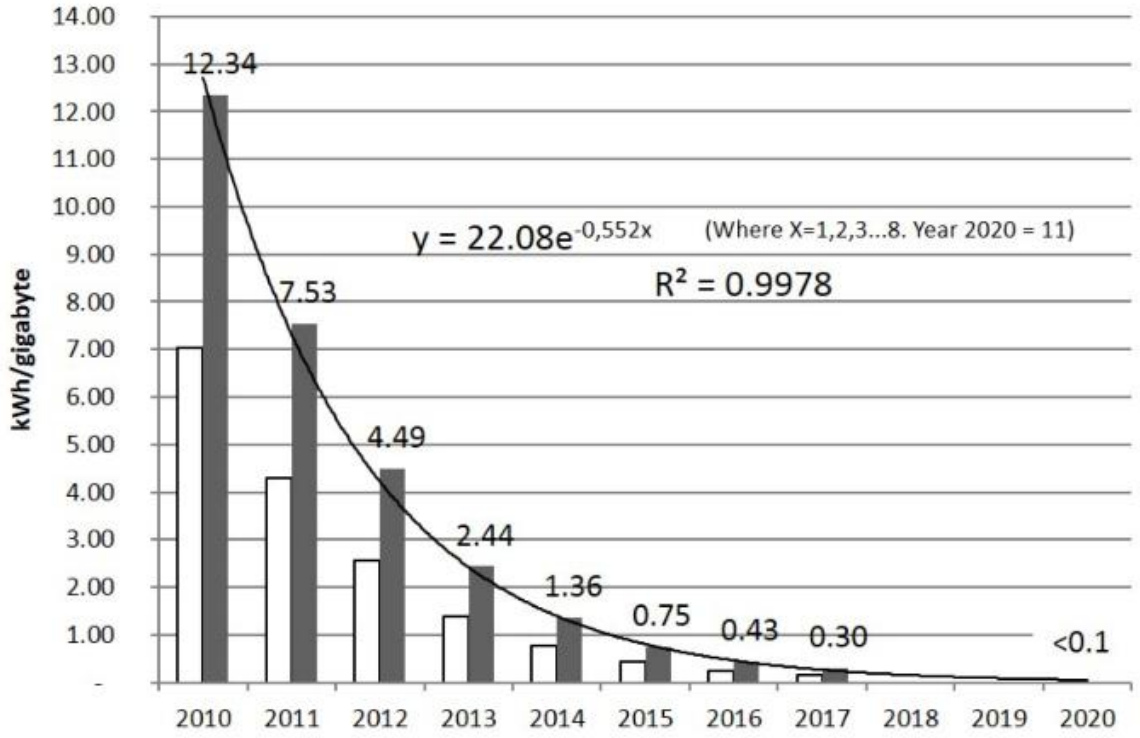


Figure 3. Development of energy efficiency of transmitted mobile data (kWh/gigabyte) in Finland during 2010–2017. Grey bars represent estimated consumption for production networks and white bars for base stations only. Exponential trends (y = y(x)) until 2020 were estimated by means of least squares fit using the data in the grey histogram. X in these equations refers to numbers 1 to 8; and 11 corresponding to years from 2010 through to 2017; and 2020.


sustainability

Evaluating the Energy Consumption of Mobile Data Transfer—From Technology Development to Consumer Behaviour and Life Cycle Thinking

But energy per transaction is complex

- Radios, cellular protocols, and cellular providers have state machines
  - Hard to predict *a priori* and globally ☹

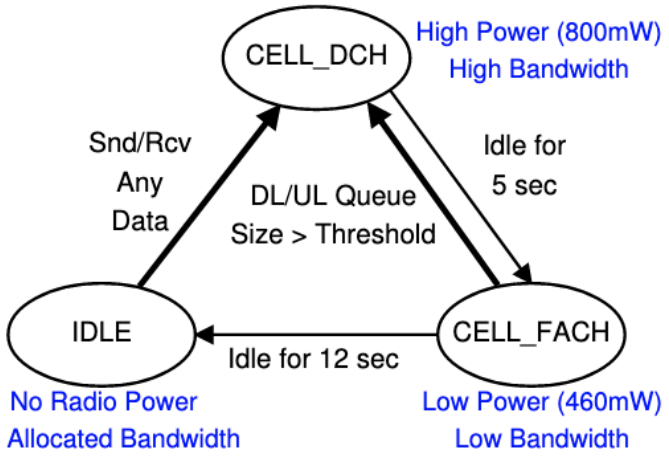


Figure 2: The RRC state machine for the 3G UMTS network of Carrier 1

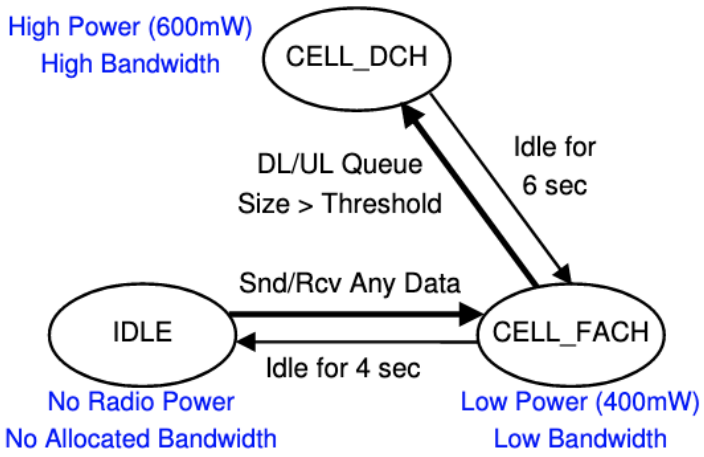


Figure 3: The RRC state machine for the 3G UMTS network of Carrier 2

Characterizing radio resource allocation for 3G networks; Feng Qian, Zhaoguang Wang, Alexandre Gerber, Zhuoqing Morley Mao, Subhabrata Sen, Oliver Spatscheck; SIGCOMM'10

So what is 5G doing differently?

- Largely, 5G is a small(er)-cell technology
  - "Urban optimized"
  - Unlikely to roll out to all geographic areas quickly (because of infrastructure cost)

- This does also allow for higher performance

Outline

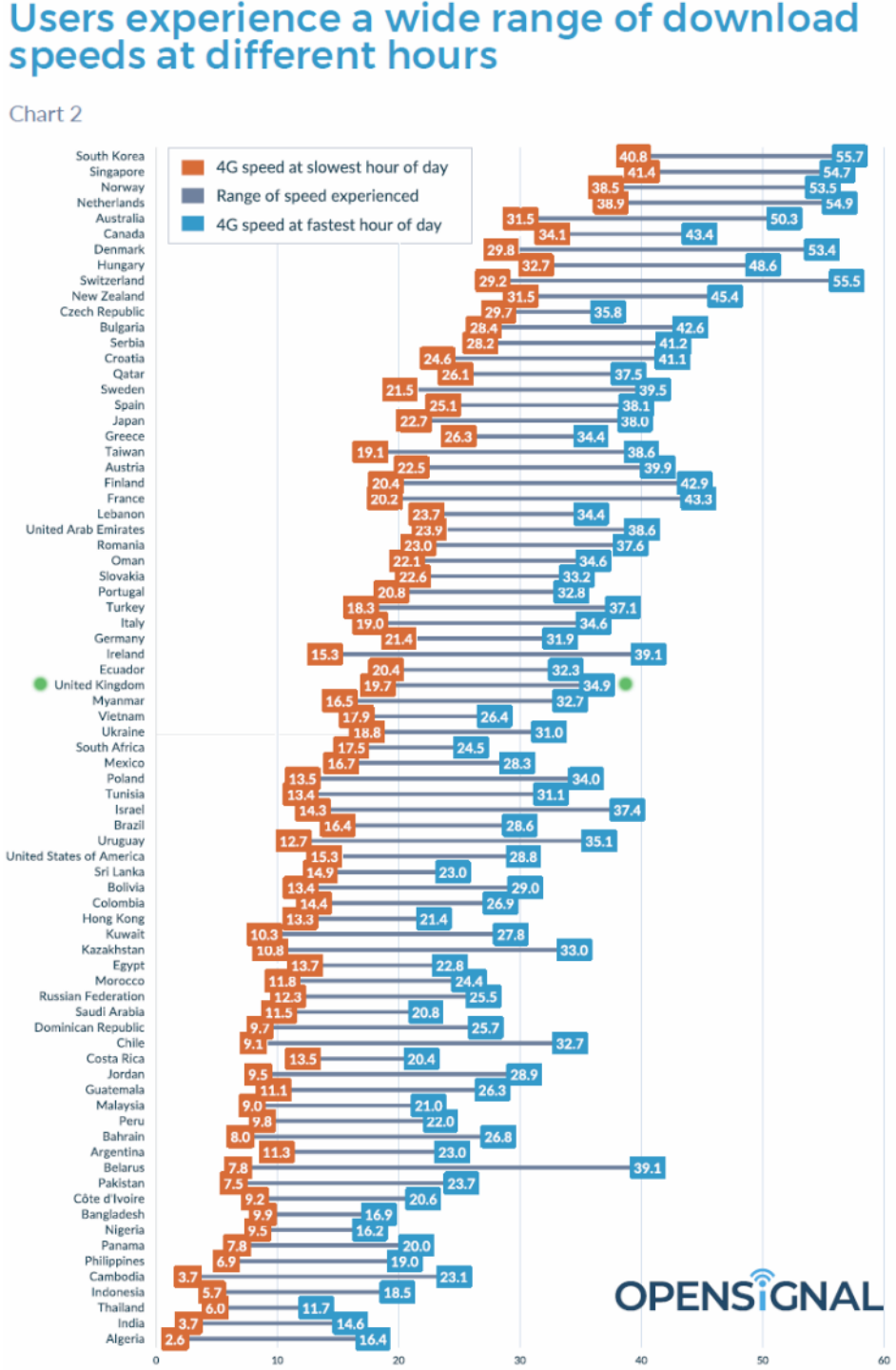
- Wide-Area Network Background
- Cellular Network Technologies
  - 1G
  - 2G
  - 3G/4G and beyond

Outline

- Wide-Area Network Background
- Cellular Network Technologies
  - 1G
  - 2G
  - 3G/4G and beyond
- **Bonus: IoT on Global Cellular**
  - Story by Pat Pannuto & nLine

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

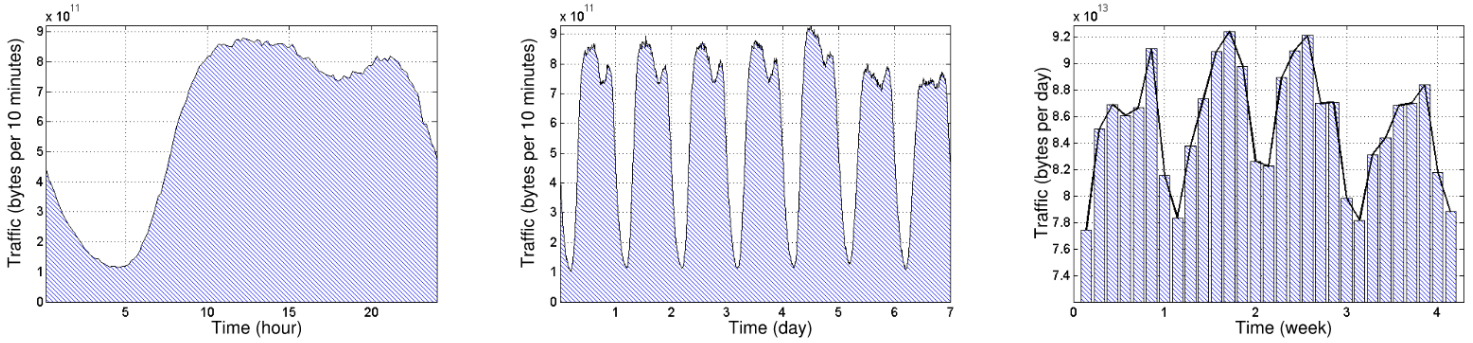


Fig. 1. The temporal distribution of cellular traffic at different time scales. (a) Hourly. (b) Daily. (c) Weekly.

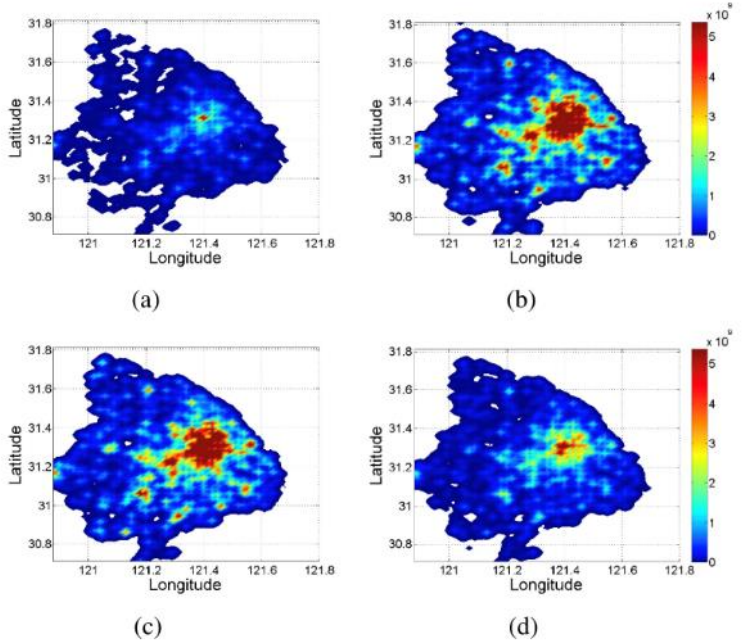


Fig. 2. The spatial distribution of cellular traffic at different time. (a) 4AM. (b) 10AM. (c) 4PM. (d) 10PM.

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

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

What is a 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

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.?