Lecture 15
LPWAN Wrap-up and RFID

CS397/497 – Wireless Protocols for IoT

Branden Ghena – Winter 2021

Some slides borrowed from Ambuj Varshney Uppsala / UC Berkeley

Northwestern

Today’s Goals

- Discuss challenges faced by LPWANs and possible solutions
- Describe RFID communication and backscatter
    - Explore how backscatter techniques can be used for sensor networks

Outline

- **LPWAN Challenges**
    - **Bit flux**
    - **Capacity problems**
    - **Coexistence problems**

- RFID Overview

- Backscatter for Sensors

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.

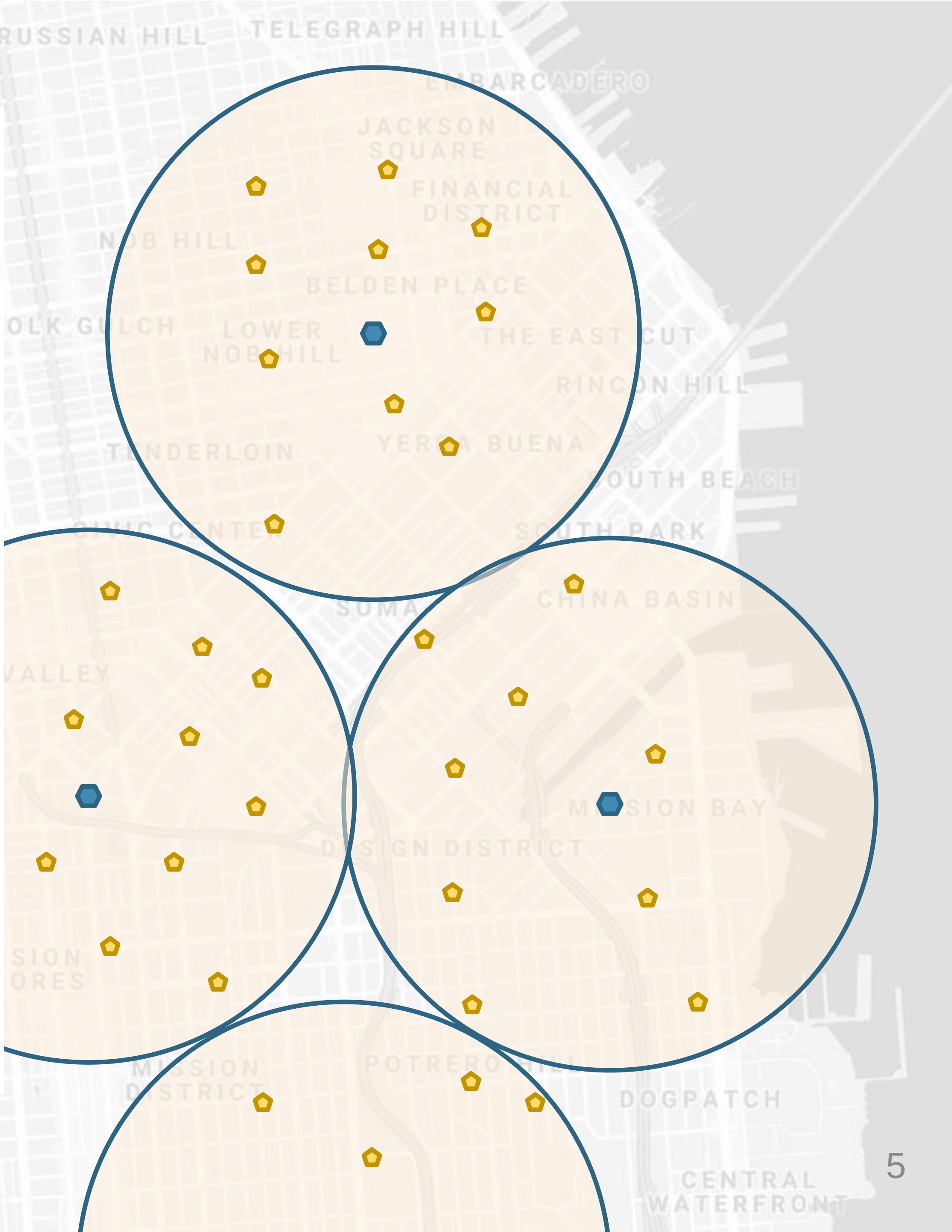
- Solution: compare the density of communication.
  - Data communication rate per unit area.

New metric for wide-area communication.

Our proposed metric: **bit flux**

- $bit\ flux = \dfrac{network\ throughput}{coverage\ area}$
- 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*

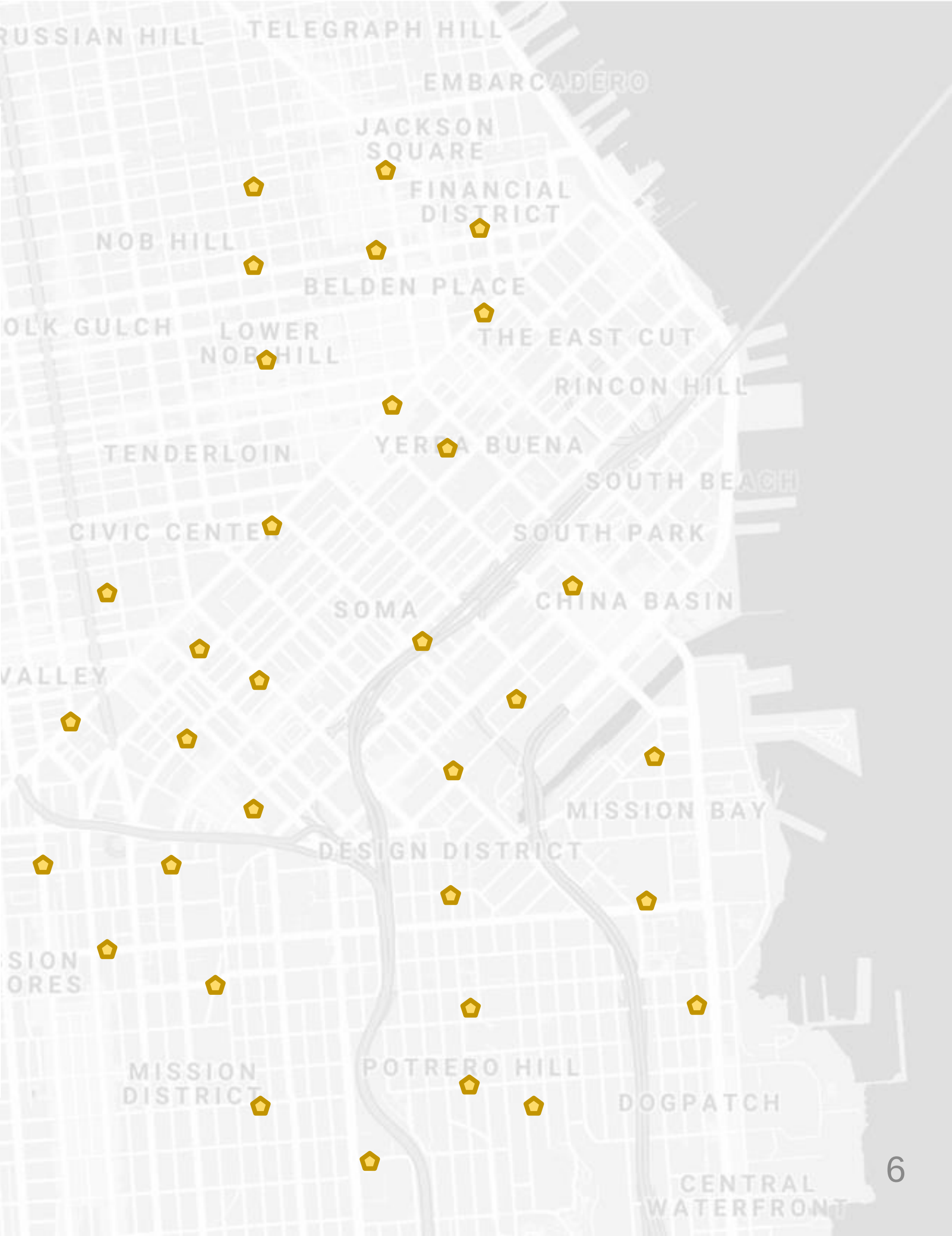


Bit flux can measure application needs.

For an application:

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

- Assumes a relatively homogeneous distribution.

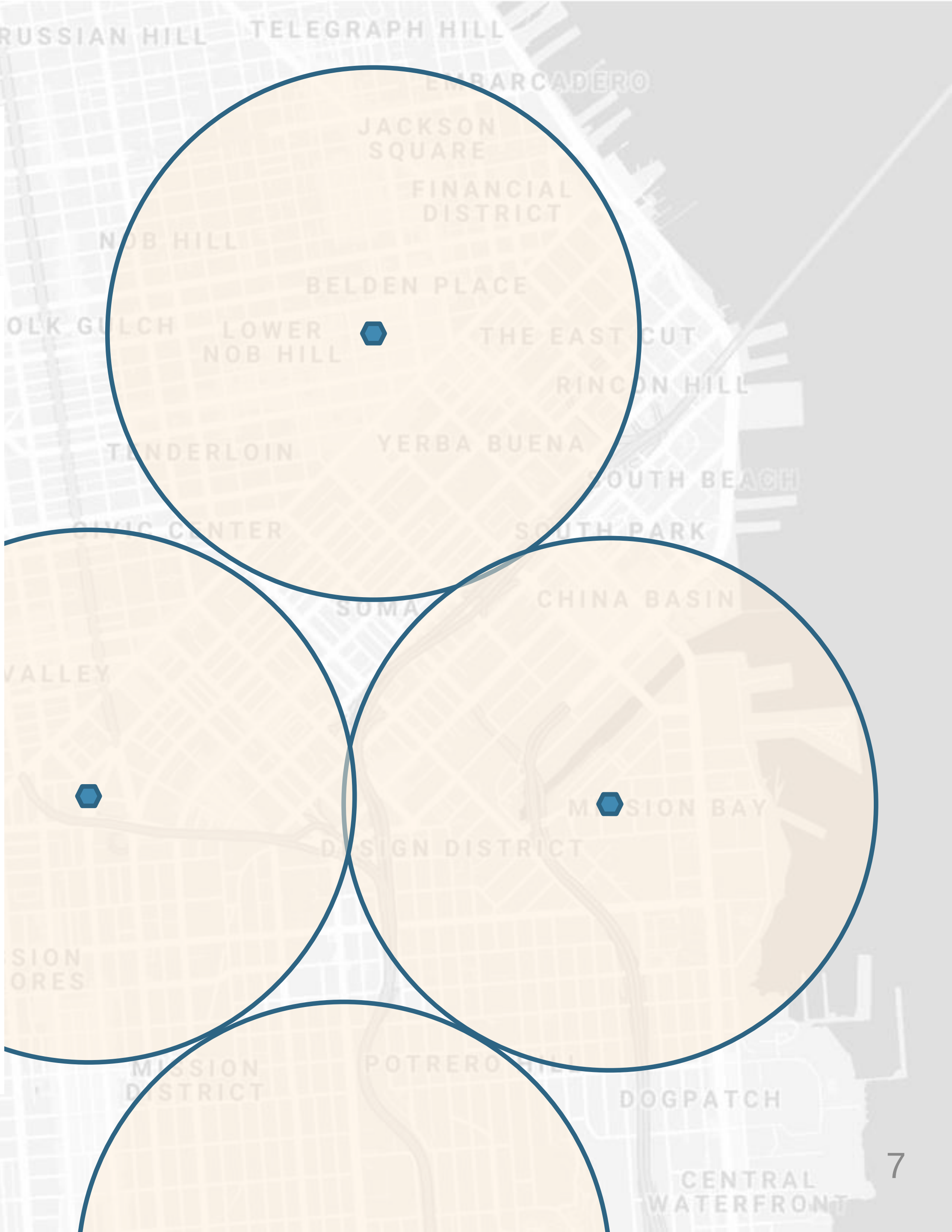


Bit flux can measure network capabilities.

For a network:

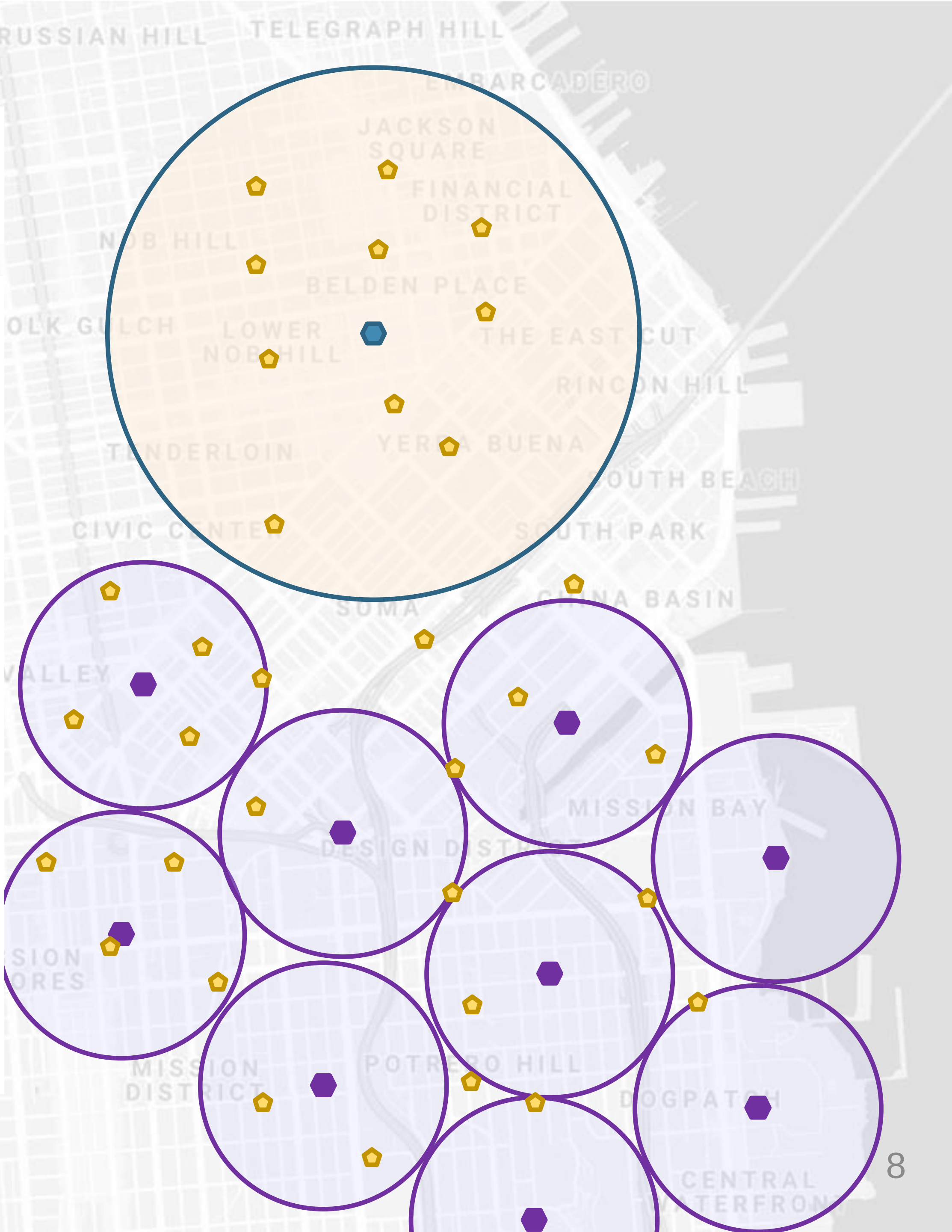
$$\mathit{bit\ flux} = \frac{\mathit{gateway\ goodput}}{\mathit{gateway\ coverage\ area}}$$

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

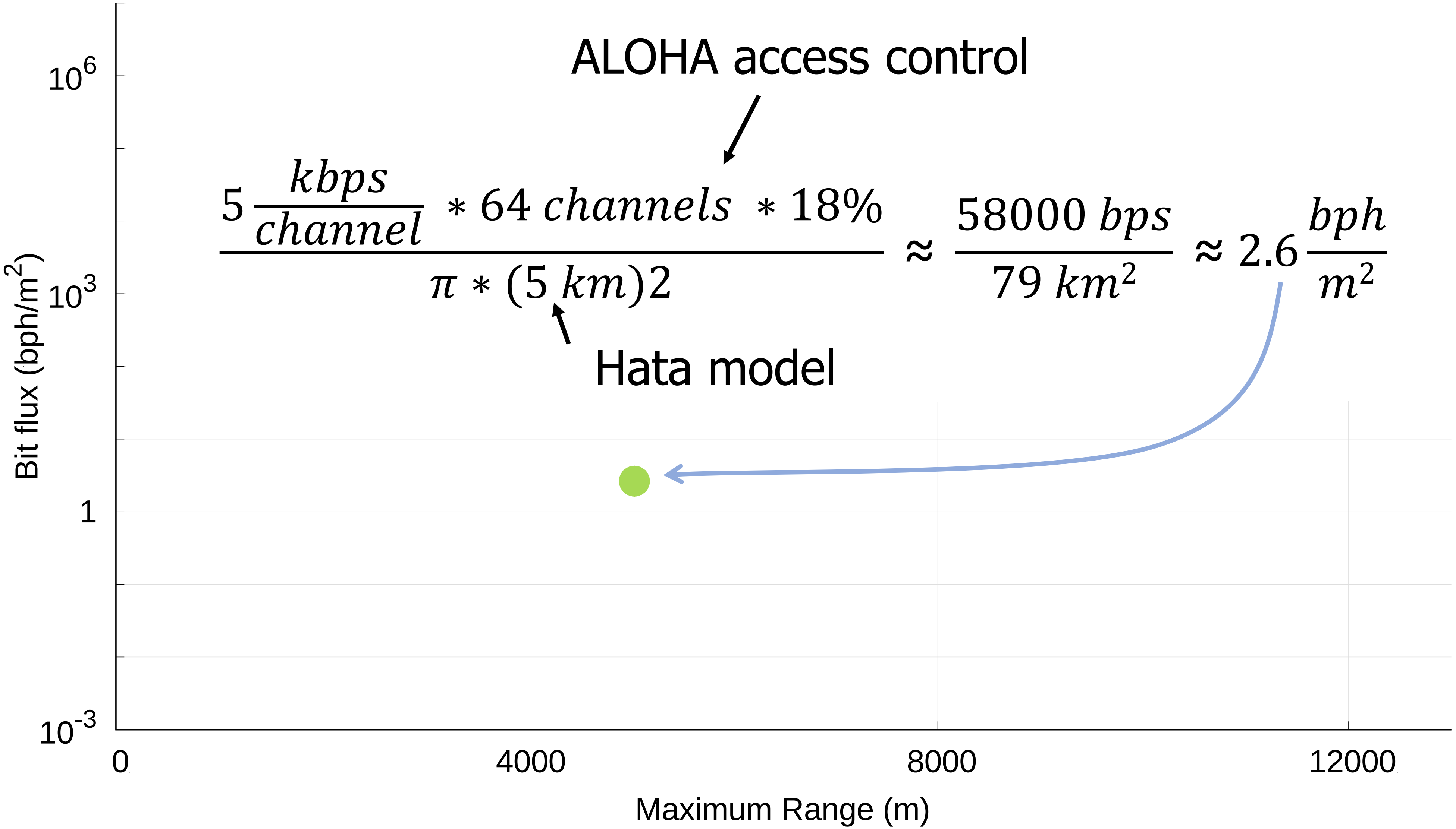


Bit flux accounts for spatial reuse.

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



Bit flux measurement for LoRaWAN.

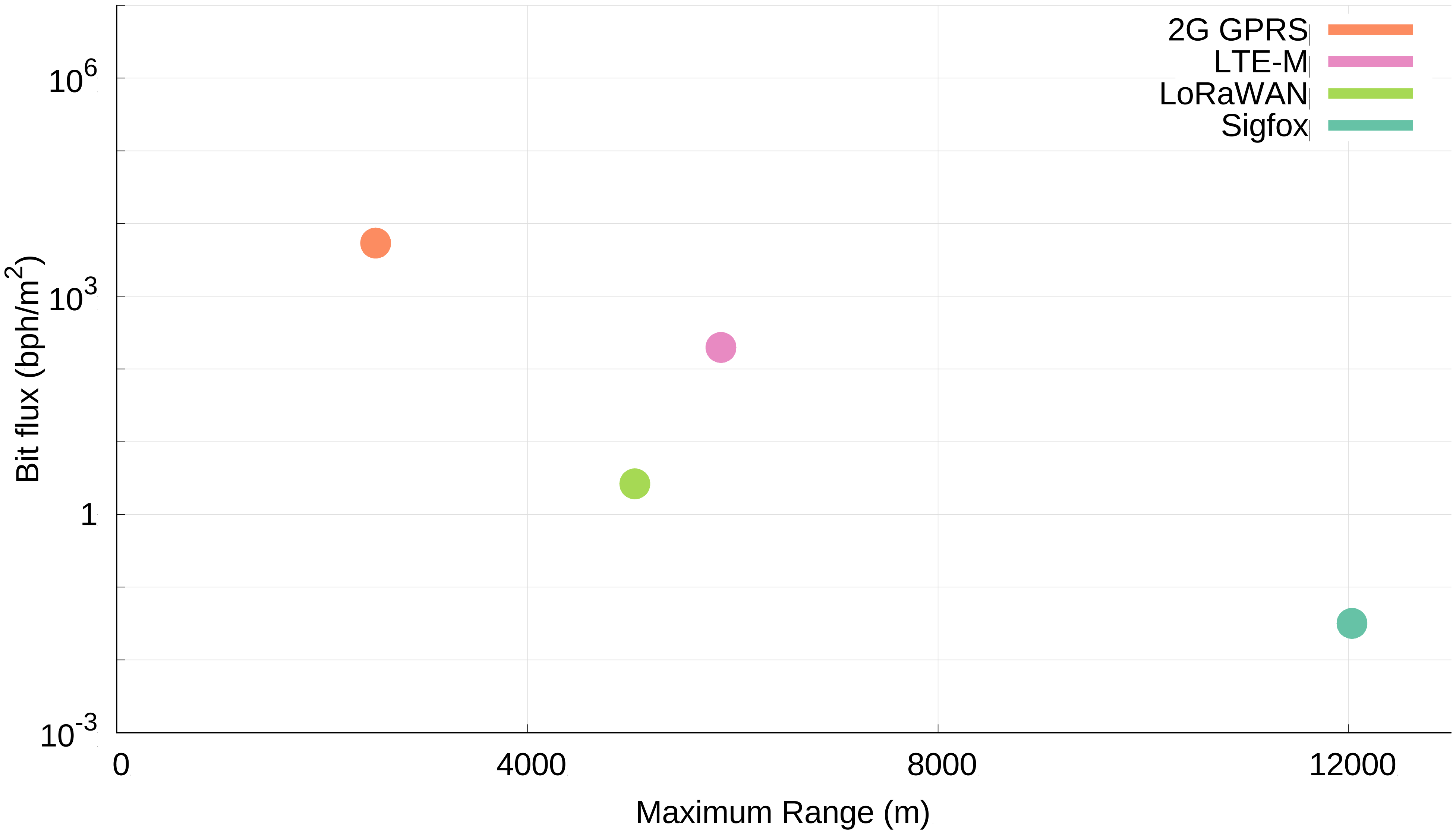


ALOHA access control

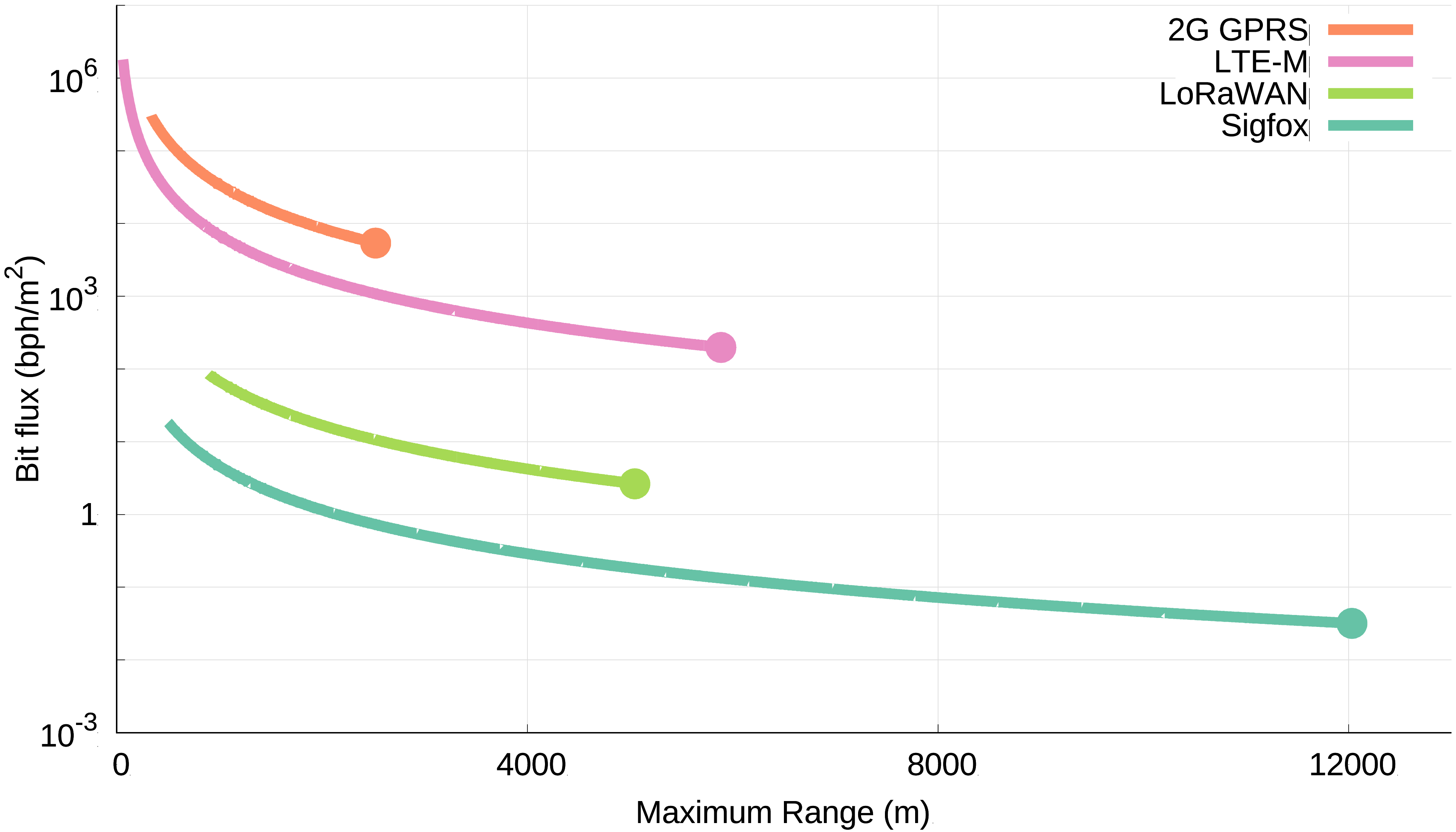
$$\frac{5\,\frac{kbps}{channel} * 64\, channels * 18\%}{\pi * (5\, km)2} \approx \frac{58000\, bps}{79\, km^2} \approx 2.6\,\frac{bph}{m^2}$$

Hata model

Networks differ in capability by orders of magnitude.



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



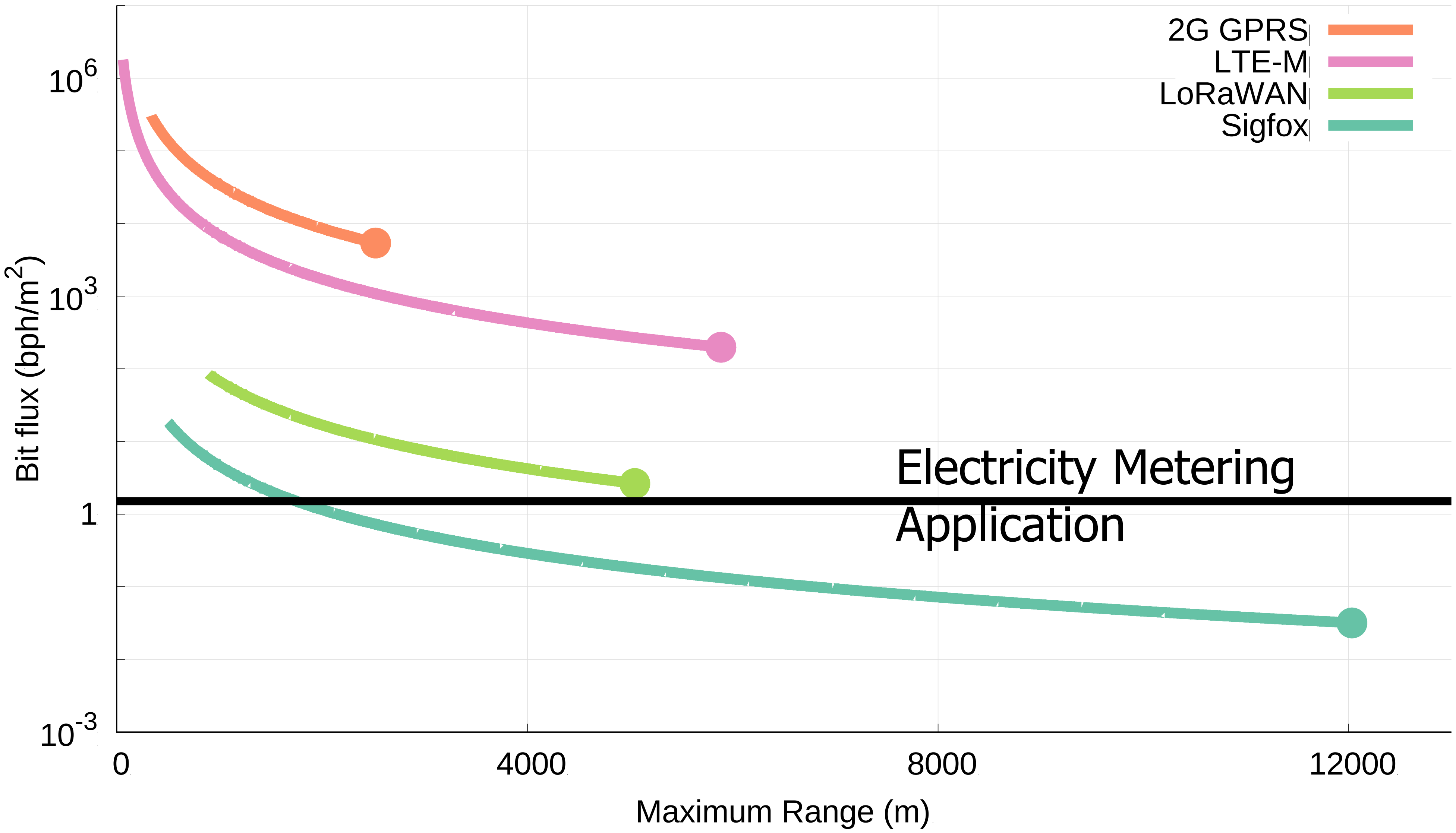
Let’s compare network capabilities to a real-world application.

Smart household electric meters.

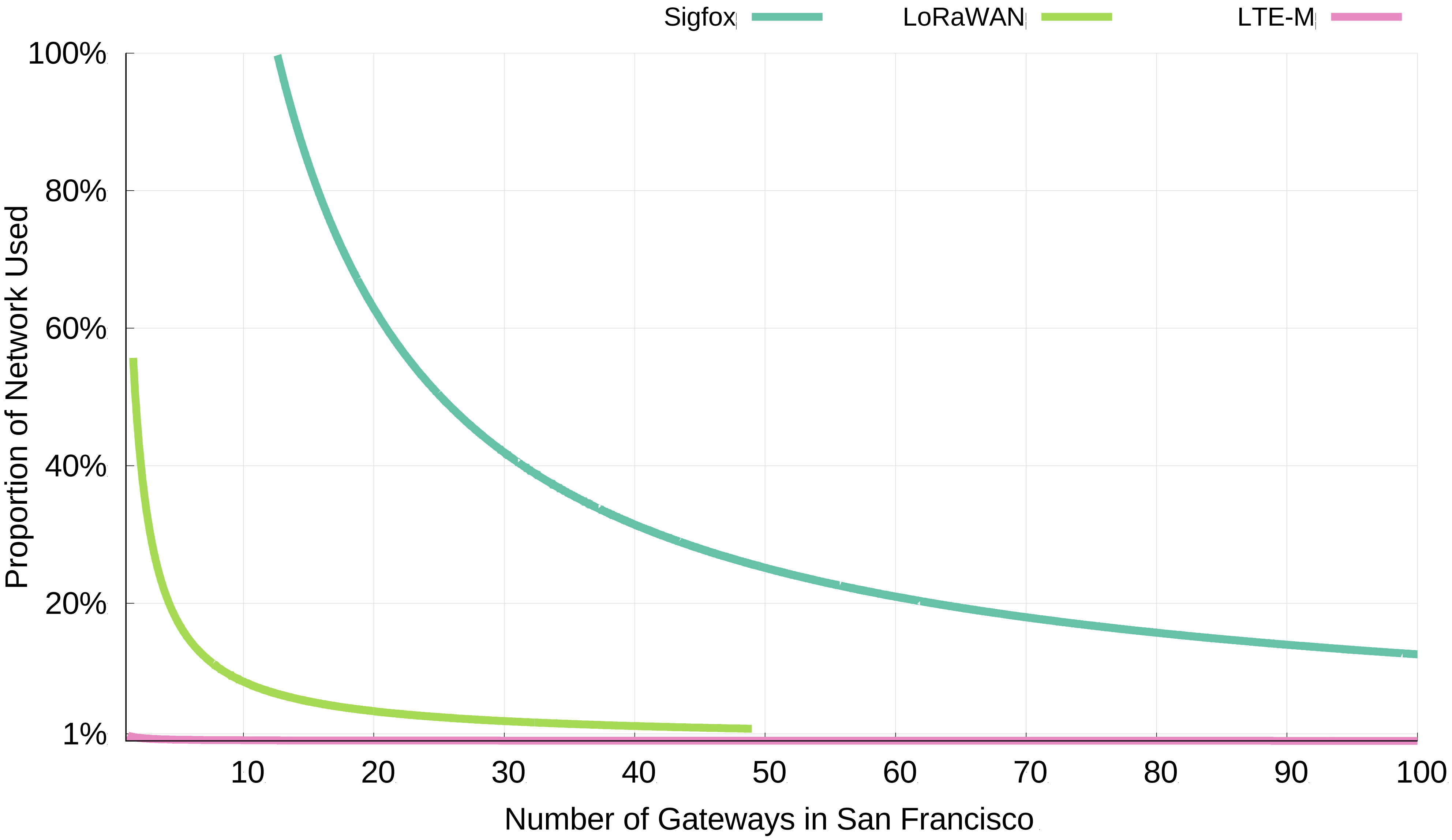
- ~250 bytes of data every 4 hours
- ~370000 electric customers in San Francisco

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

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

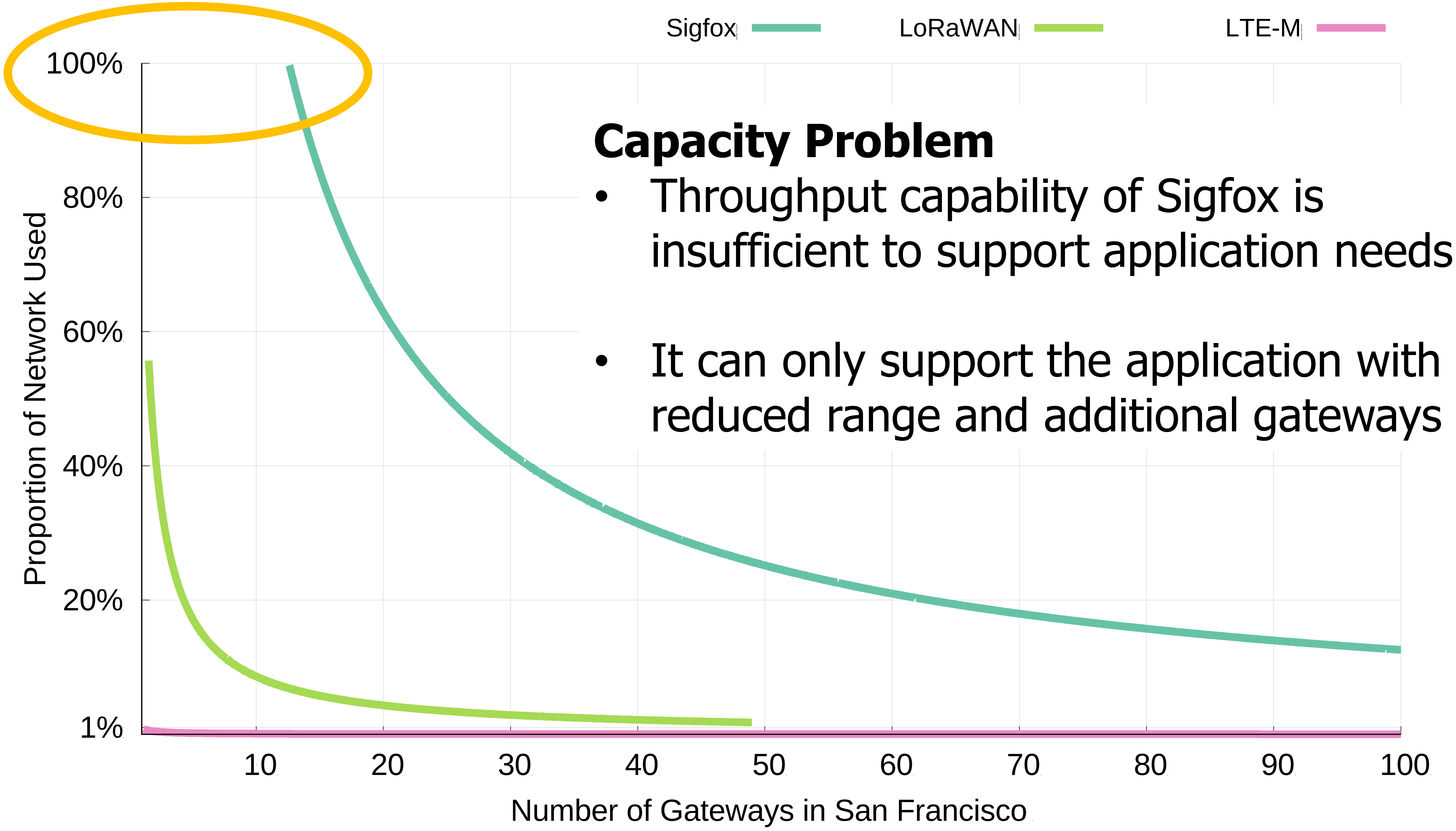


Unlicensed LPWANs lag behind Cellular IoT in ability to support applications.



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 (OFDMA?).
- Recover simultaneous transmissions (Choir and Charm).
- Increase bandwidth (TV white spaces).

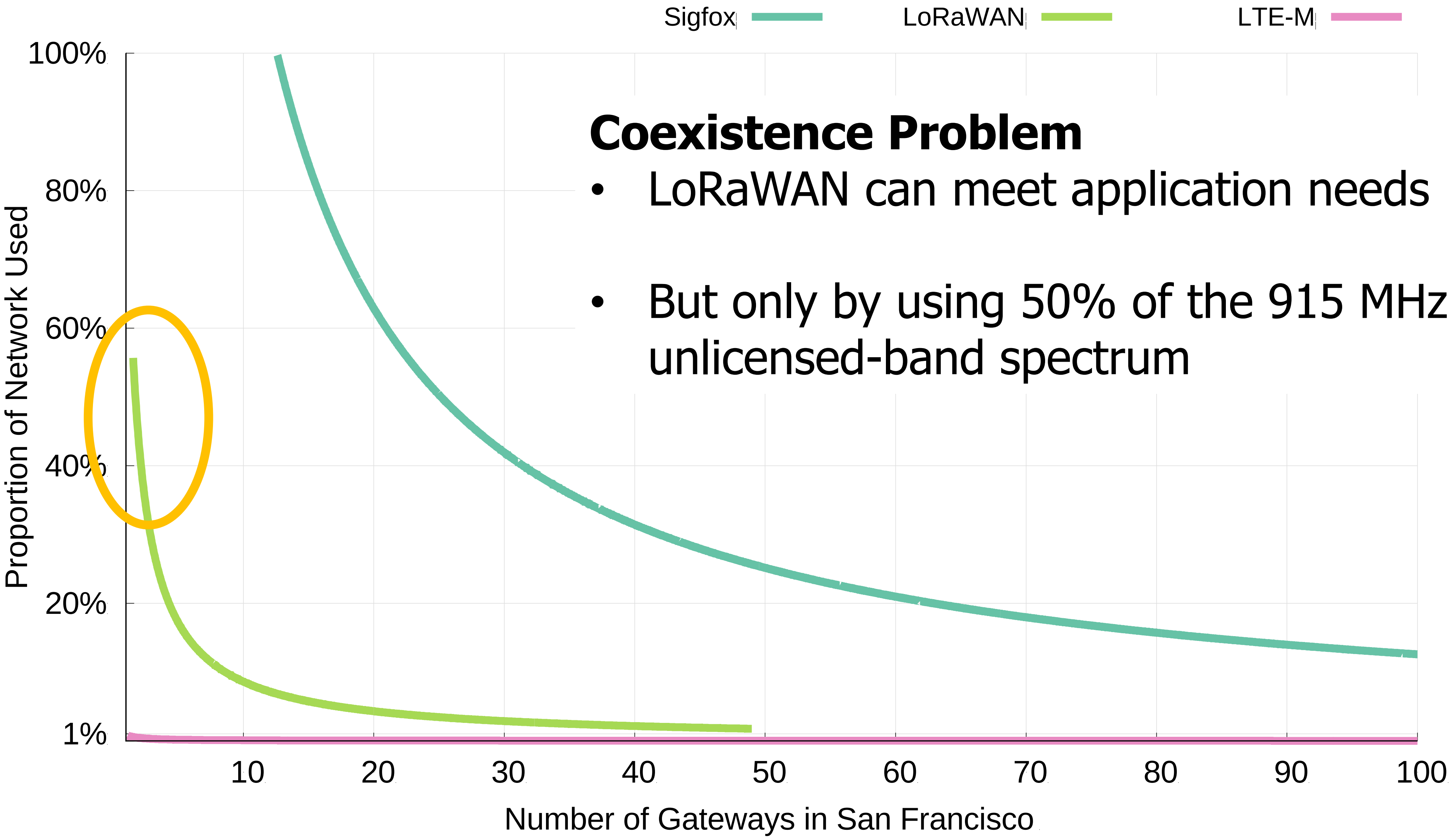
- All likely come at the cost of increased energy usage…
  - Results in a protocol that looks pretty similar to cellular…

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.

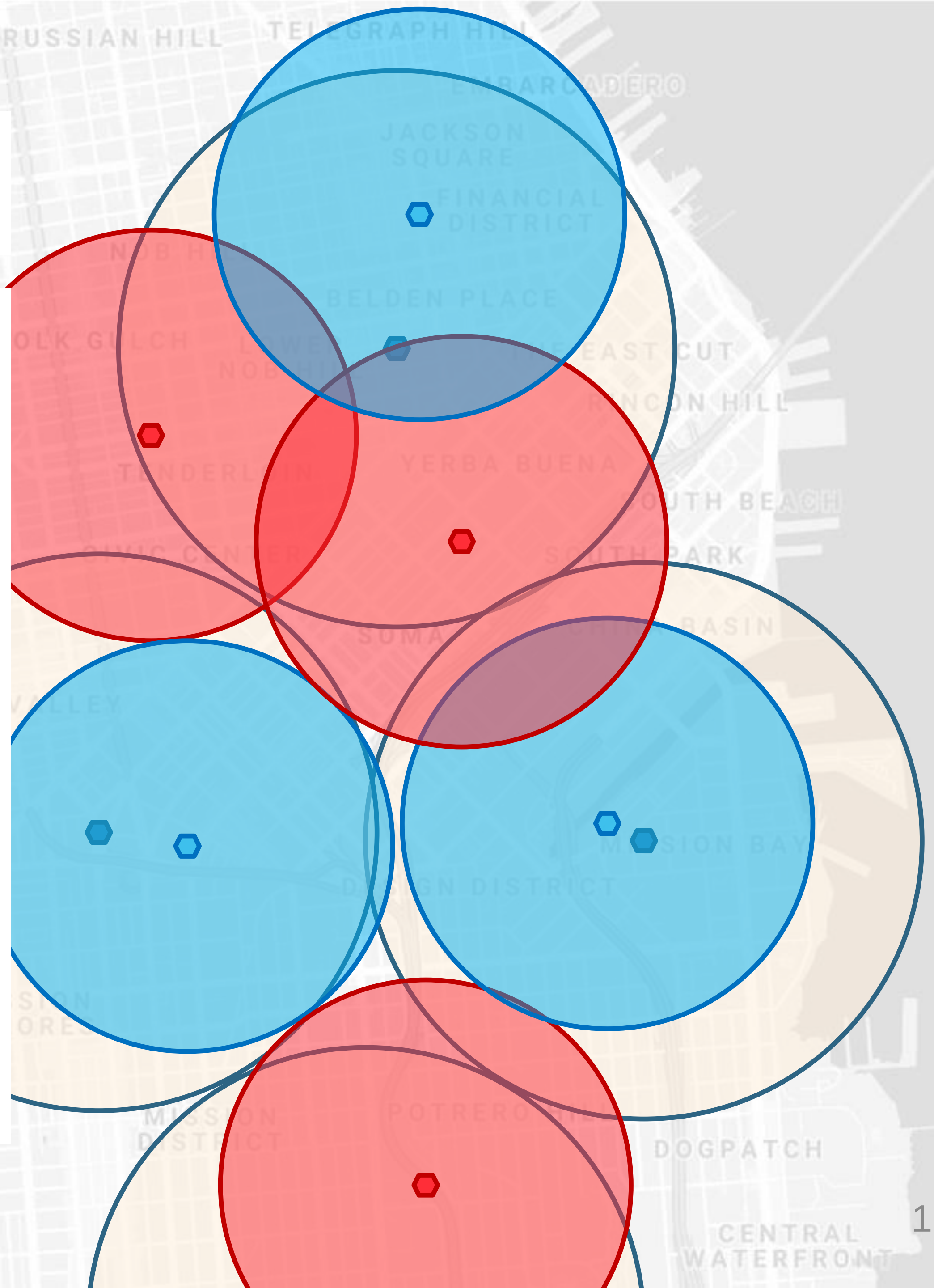


Coexistence Problem

- 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…



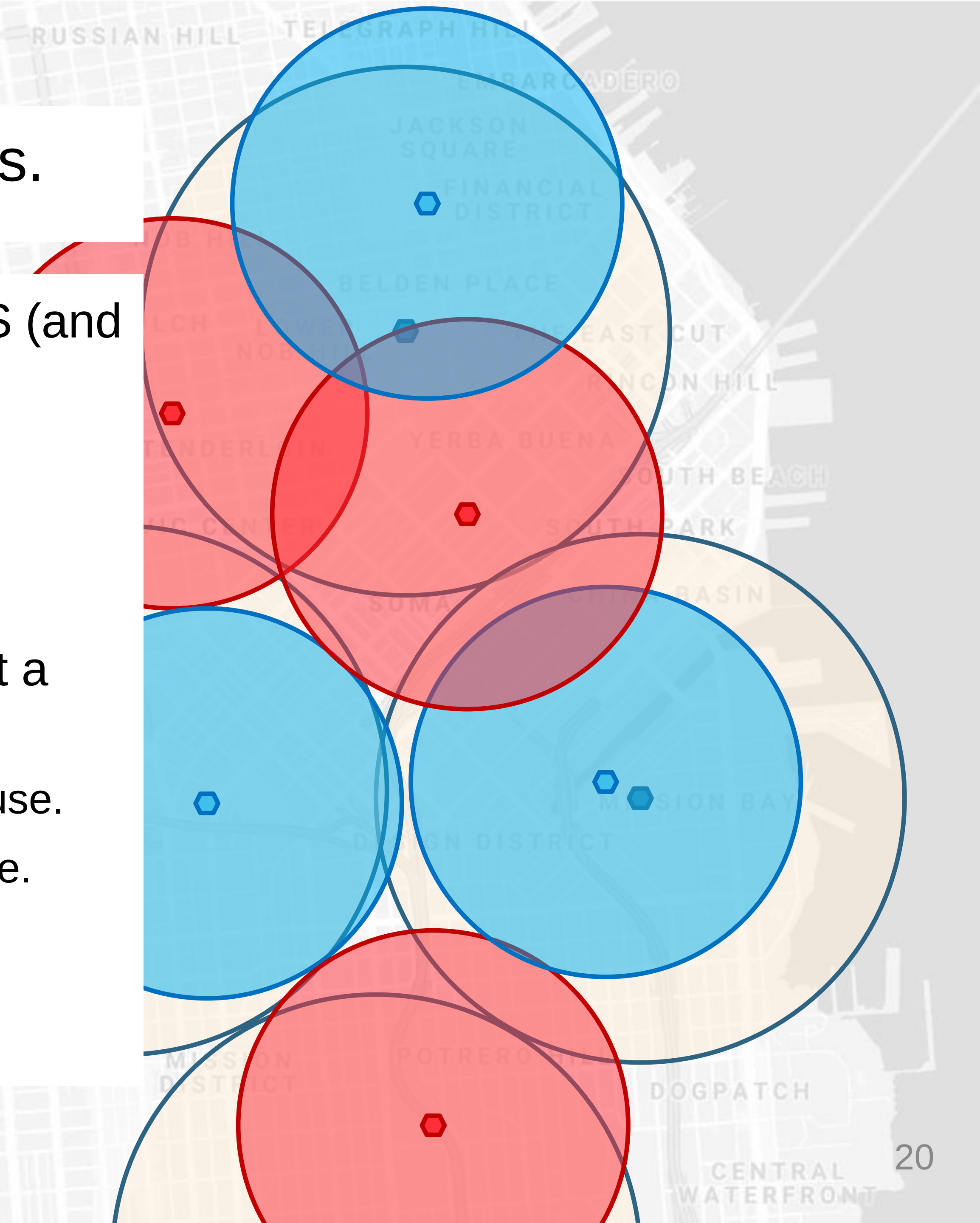
Coexistence in unlicensed bands is a more difficult problem.

- 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

- LPWAN Challenges
  - Bit flux
  - Capacity problems
  - Coexistence problems

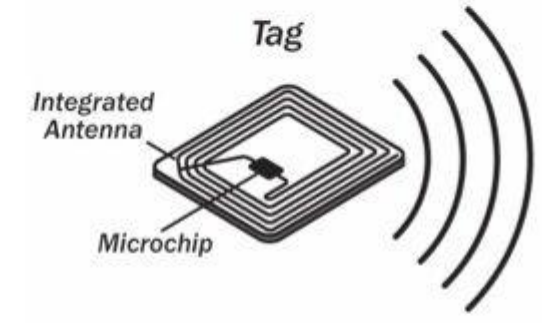
- **RFID Overview**

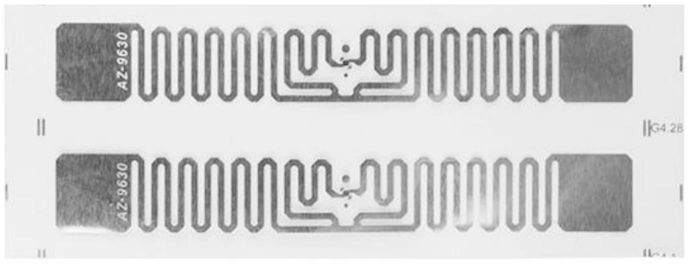
- Backscatter for Sensors

Radio Frequency ID

- Cheap, low-power ubiquitous communication
  - RFID tags on (or in) products
  - NFC communication to/from smartphone

- Requirements
  - Need to transmit small amount of data (ID)
  - Need to operate with little or no energy
    - Most do not have batteries
  - Short interaction time (fast enough bit rate)
  - Range can be extremely limited
    - Meters to centimeters (or millimeters)





Making ultra-low power radios

- How do we make a radio that’s lower power?
- What is the most costly part of the radio?
  - Carrier-frequency generation
  - Modulating bits is comparatively lower energy

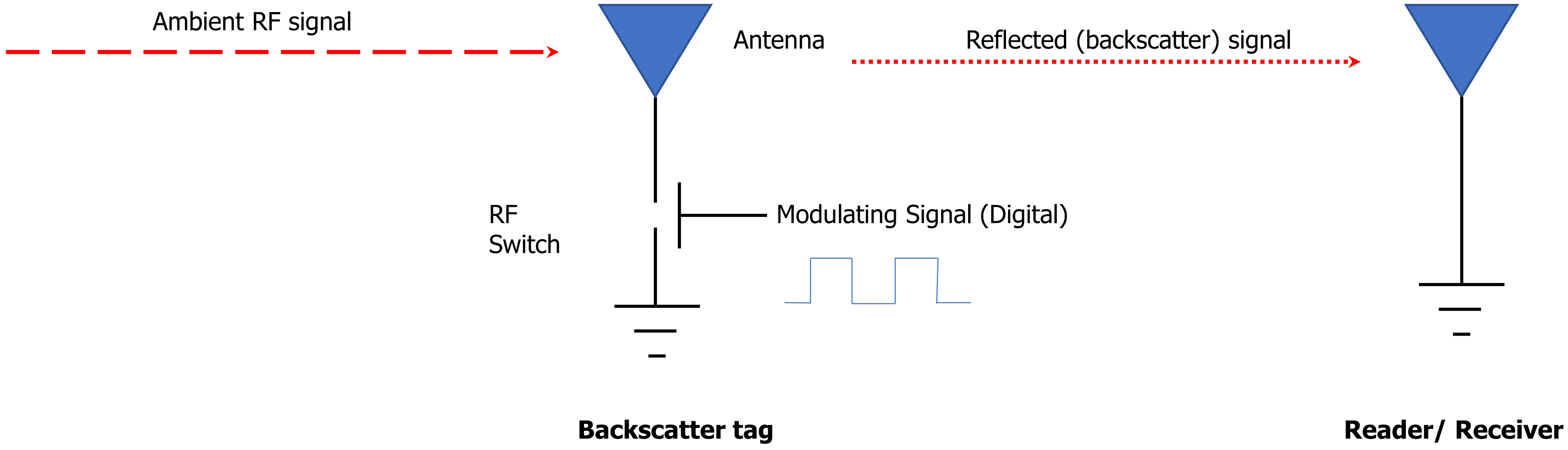
- Solution: do not generate carrier
  - Instead, use existing RF signal transmitted nearby
  - Common case: sent from nearby higher capability device
  - Dream case: use ambient RF signals to communicate

  - Bonus: can harvest energy from the signal being sent

- Two versions in practice: backscatter and inductive coupling

Backscatter theory of operation

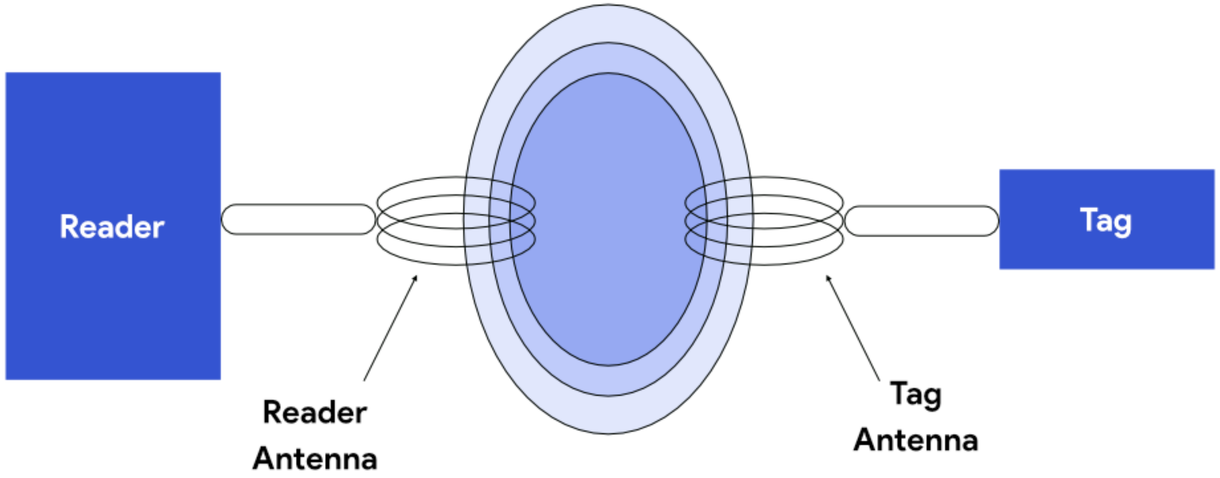
- Vary between absorbing or reflecting signal to modulate data
  - Wireless transmissions at mircowatts of power draw
  - Frequency bands: 400 MHz, 900 MHz, 2.4 GHz
  - These are the really really cheap tags (~$0.15 each)



Inductive coupling theory of operation

- A shared magnetic field is created between the two devices
    - Change in current through one device induces current change through the other
    - Device can vary load to transmit data

- Very low frequency bands (135 KHz, 13.56 MHz)
    - Transmit through materials including skin
    - Sensitive to metal



Power at tag Ptag α 1/d6 Preader

d = tag - reader distance

RFID challenges

- Essentially free communication!
  - What’s the cost (besides having a higher-capability device)

- Difficult to reflect energy when it is already so low
  - Essentially double the path loss (there and back)

- Range is very limited (or transmit power needs to be high)
  - Meters of range, maximum
  - Centimeters for inductive coupling

  - Alternatively, could decouple signal generation from reception

Classes of RFID devices

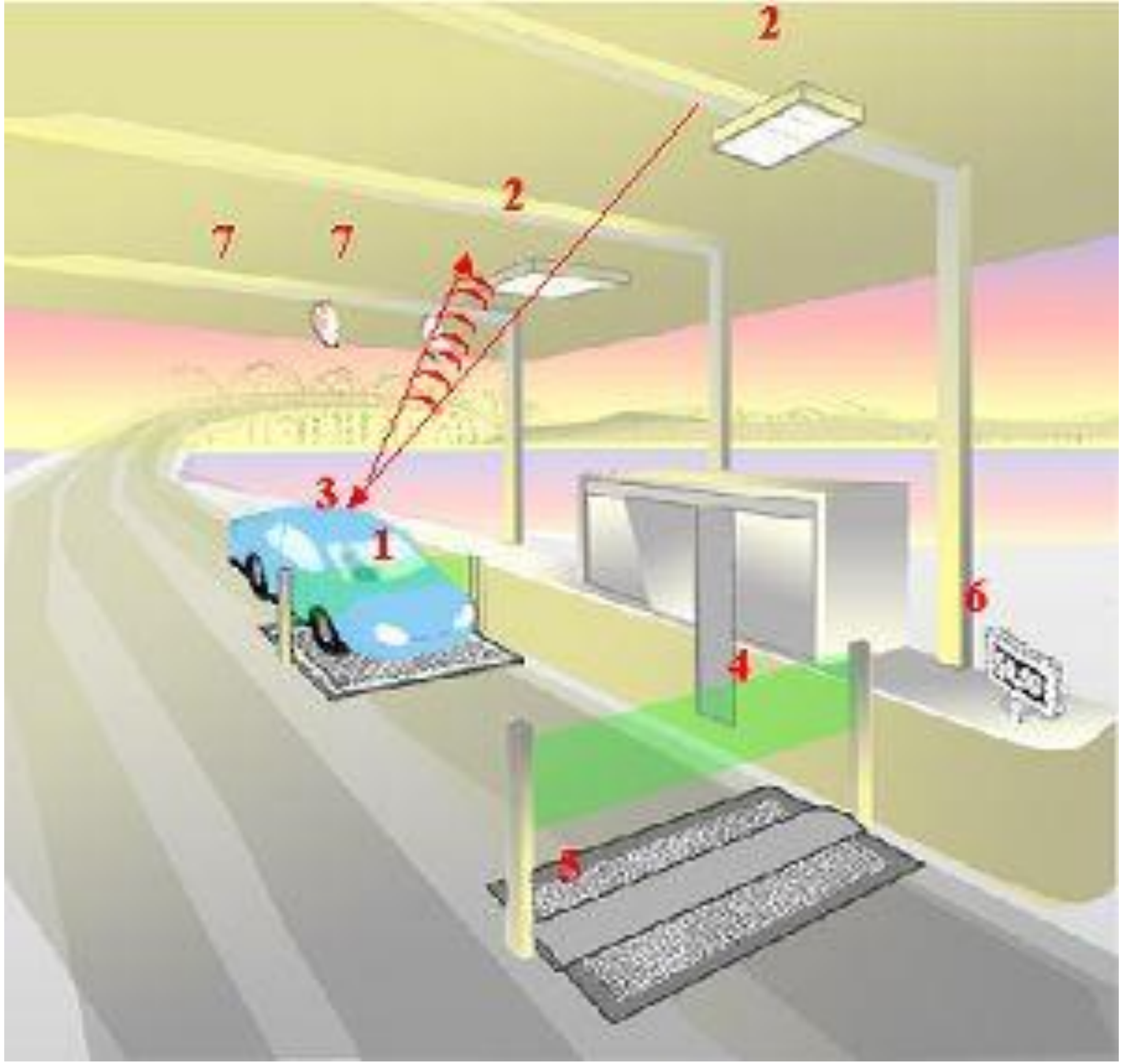
- Passive RFID
  - No battery, harvests energy from RF signals

- Active RFID
  - Contains a battery used to operate
  - Still reflects RF signal to communicate
    - Enables long battery lifetime

Car RFID systems

- Two mounted antennas
    - One broadcasts energy, activating the RFID device
    - The other receives the reflected data

- Devices are battery powered for longer-range operation
    - Don't have to energize themselves with signal
    - Batteries last a decade



MAC layer for RFID tags

- Cards are limited in capability so we can’t do anything fancy
  - But tags are frequently co-located, so some solution is necessary

- Option 1: Aloha with pseudo-random backoff
  - Reader sends out initialization, tags randomly respond back

- Option 2: Adaptive binary tree
  - Reader sends out initialization, along with first bit of ID
  - All cards matching that ID respond
  - Reader sends out a second bit of ID
  - Repeat until CRC is valid, then go back and choose other branches

What data should a card send?

- Let’s think about security for a minute

- **Is just sending ID bits sufficient?**

What data should a card send?

- Let’s think about security for a minute

- **Is just sending ID bits sufficient?**
  - Simple identification, maybe. (e.g. products in a store)
  - For authentication, no. Need to avoid replay attacks.

- Include some kind of challenge and response
  - Probably also encrypted

- May also read/write from an arbitrary memory in the card
  - Up to several hundred bits of storage

Electronic Product Code (EPC)

- Format created by GS1
  - Not-for-profit org that created and standardized barcodes

- 12-byte identifier for products for RFID use

Header	**EPC Manager**	**Object Class**	**Serial Number**
8 bits	28 bits	24 bits	36 bits
(version number)	(Company ID)	(Product type SKU)	(Unique per instance of product)

Near Field Communication (NFC)

- Same Inductive Coupling concept (13.56 MHz)
  - But attached to a powered and capable device (smartphone)

- Can act as a tag or as a reader
  - Allows smartphone to power a tag if needed
  - Alternatively, smartphone could act like a card and respond to a reader
  - Two smartphones can communicate without power transfer

- Data rate 100-400 kbps!
  - nRF52840 capable of 100 kbps communication with attached antenna

Outline

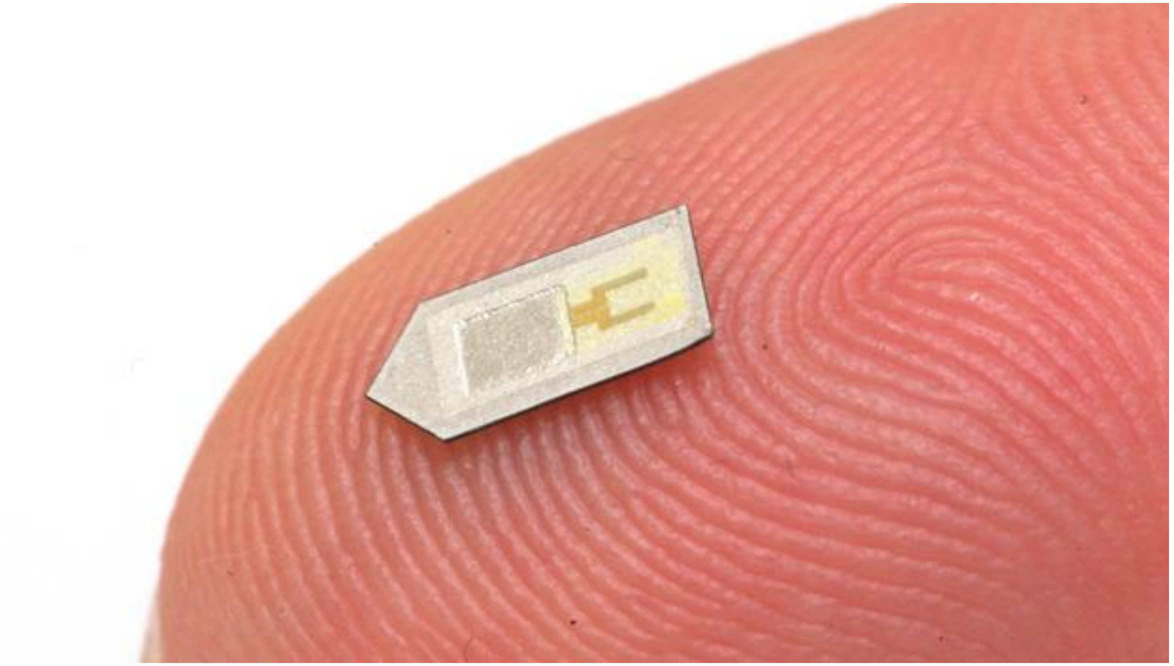
- LPWAN Challenges
  - Bit flux
  - Capacity problems
  - Coexistence problems

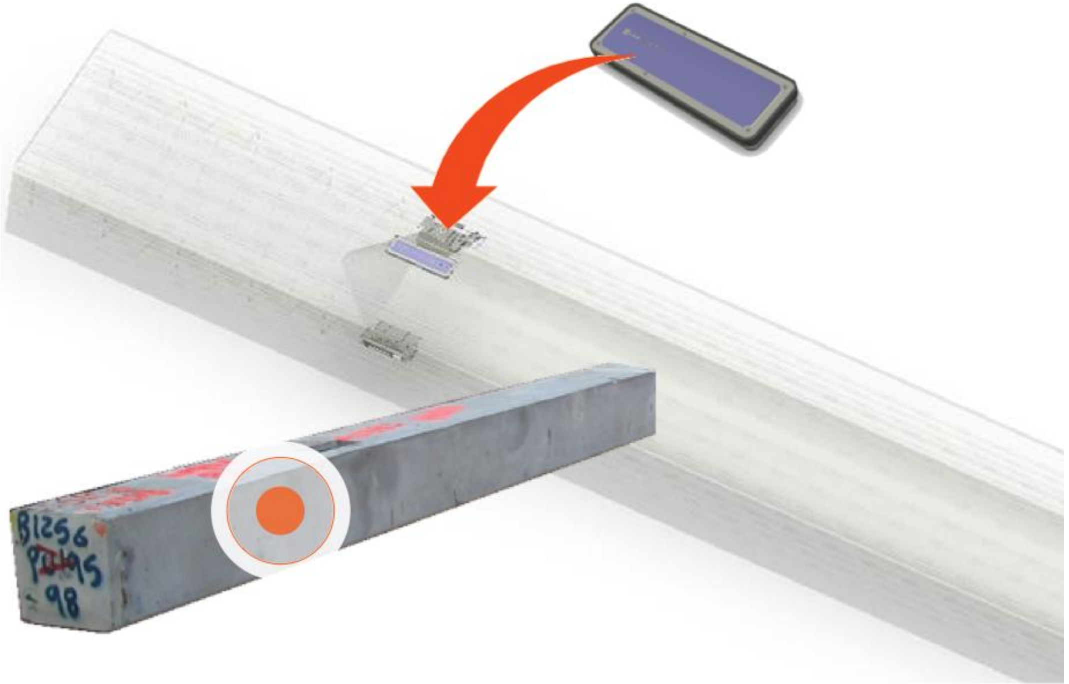
- RFID Overview

- **Backscatter for Sensors**

“Embedded” sensors

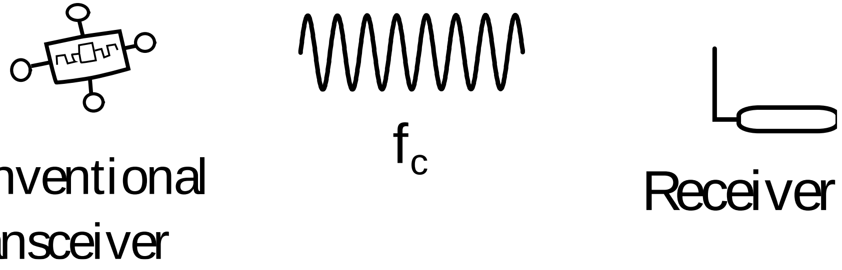
- How do you change batteries in a device that’s inside a wall or inside someone’s body?





Backscatter for sensor networks

Conventional Radio

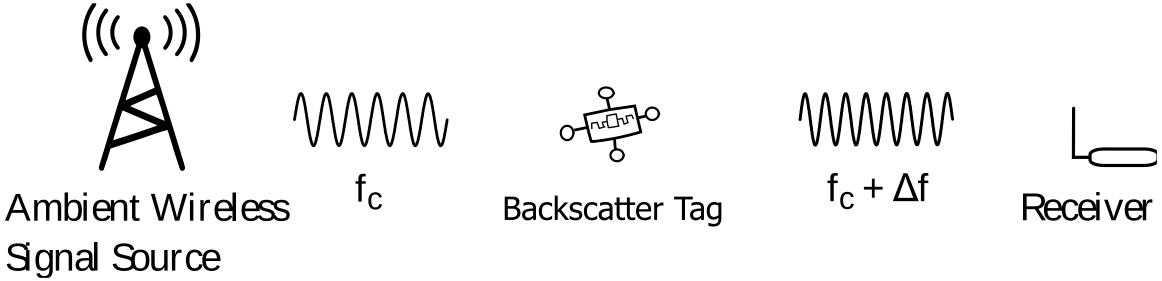


Conventional Transceiver

f_c

Receiver

Backscatter Transmissions



Ambient Wireless Signal Source

f_c

Backscatter Tag

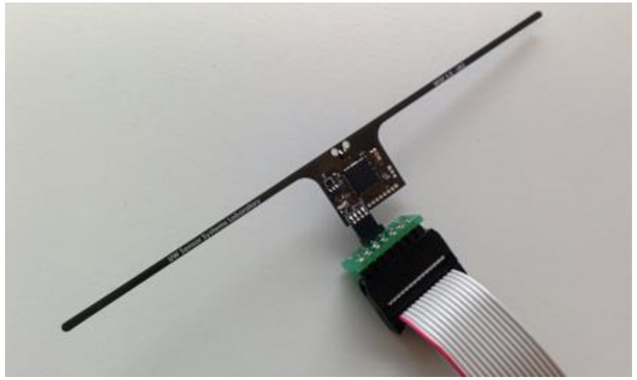
$f_c + \Delta f$

Receiver

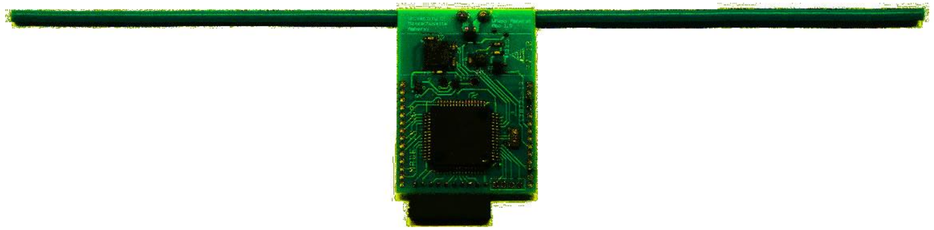
- Backscatter allows transmissions at up to 10000x lower power than conventional radios
  - Makes it very attractive for low-energy sensing devices

RFID sensors

- First iterations were literally RFID sensors
  - Limited by cost and range of RFID readers (only a few meters)



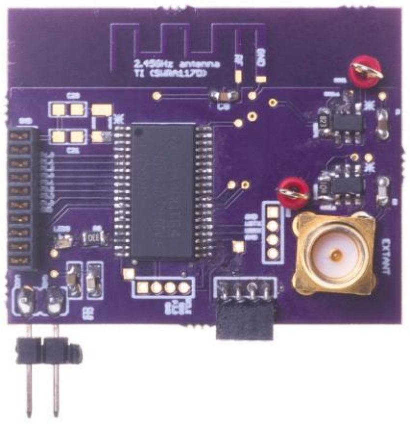
WISP 5.0
University of Washington



Moo 1.0
University of
Massachusetts

Backscatter + LPWAN = usable?

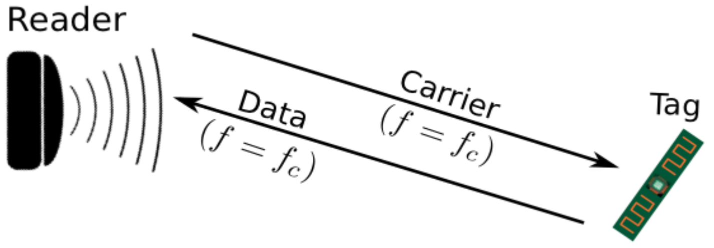
- Idea:
    - Backscatter is about low energy operation
    - LPWANs are about long-range operation
    - Can we combine them for low energy and medium-long range?
- LoRea: long-range transmissions at µW
    - (Next few slides stolen from Ambuj's talks)



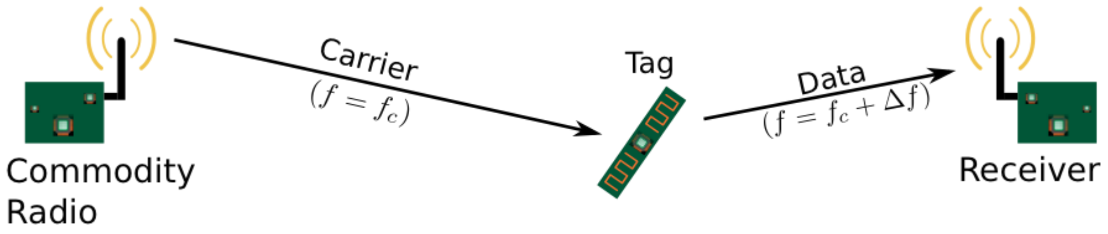
Varshney et al. "LoRea: A Backscatter architecture that achieves a long communication range" SenSys 2017

Design element #1: LoRea decouples the carrier signal generation and reception

- Bi-static setup spatially separates carrier generation from the receiver



Monostatic configuration



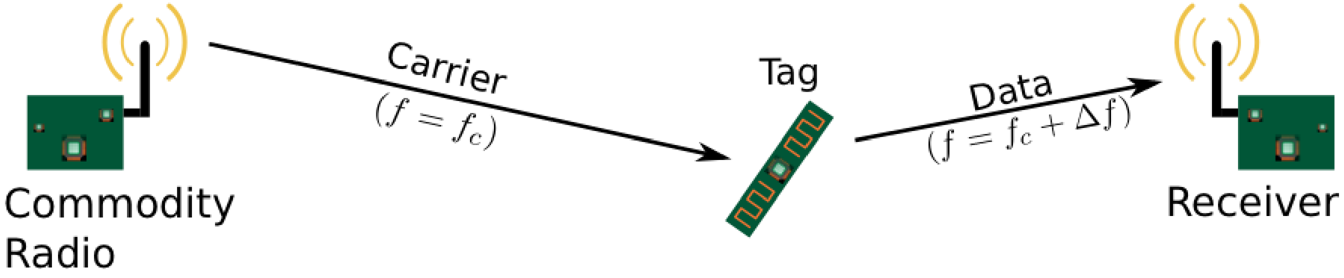
Bi-static configuration

- Use devices that surround us for providing the necessary carrier signal

Self-interference reduced due to path loss suffered by carrier signal

Design element #2: LoRea backscatters at a frequency offset from the carrier signal

- Backscatter is a mixing process



- Transceivers attenuate interference at adjacent frequency channels
- Frequency separation reduces interference from carrier to backscatter signal

No complex self-interference mechanisms required at reader

ambujv@berkeley.edu

We ran out of space while performing experiments

- State-of-art few meters. We achieved kilometers, was difficult to anticipate
- Initial experiments conducted near the university and a river in Uppsala

Experiment Setup

Receiving transmissions 1km away from the setup

ambujv@berkeley.edu

LoRea outperforms state-of-the-art systems

System name	Communication range
LoRea – 868 MHz (SENSYS 2017)	**3400 m**
LoRea – 2.4 GHz (SENSYS 2017)	**225 m**
RFID	< 18 m
BackFi (SIGCOMM 2015)	5 m
Passive WiFi (NSDI 2016)	30 m
HitchHike (SENSYS 2016)	54 m
Interscatter (SIGCOMM 2016)	30 m
LoRa Backscatter (UBICOMP 2017)	2800 m

Range reported are line of sight, with backscatter tag co-located with carrier source

ambujv@berkeley.edu

Future research directions for Backscatter

- Improve capabilities for “ambient” backscatter
  - Reuse existing RF signals rather than relying on carrier generation

- MAC layers for backscatter
  - Need ability to communicate with very low power
  - How do you manage access to the medium?

- Real-world usable backscatter stacks and hardware
  - Needs to be deployable and usable by non-experts

Outline

- LPWAN Challenges
  - Bit flux
  - Capacity problems
  - Coexistence problems

- RFID Overview

- Backscatter for Sensors