Lecture 18
Backscatter & RFID

CS433 – Wireless Protocols for IoT

Branden Ghena – Spring 2025

Some slides borrowed from Ambuj Varshney (NUS)

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

Administrivia

- Lab: LoRa
  - Checkoffs:
    - Today 5-7
    - (late) Friday 1-5pm in Frances Searle 2.370 (our lab room)

- Final Design Project
  - Formal design review of an application
    - Consider energy, costs, etc.
  - Writeup due Tuesday of exam week
    - No late days on this one. Submit it on time.
  - Working on Cellular homework grading
    - Common lost points: no inline citations

Today's Goals

- Describe backscatter communications
- Understand one use of backscatter: RFID
- Explore how backscatter techniques can be used for applications
    - Sensor networks
    - Localization

Outline

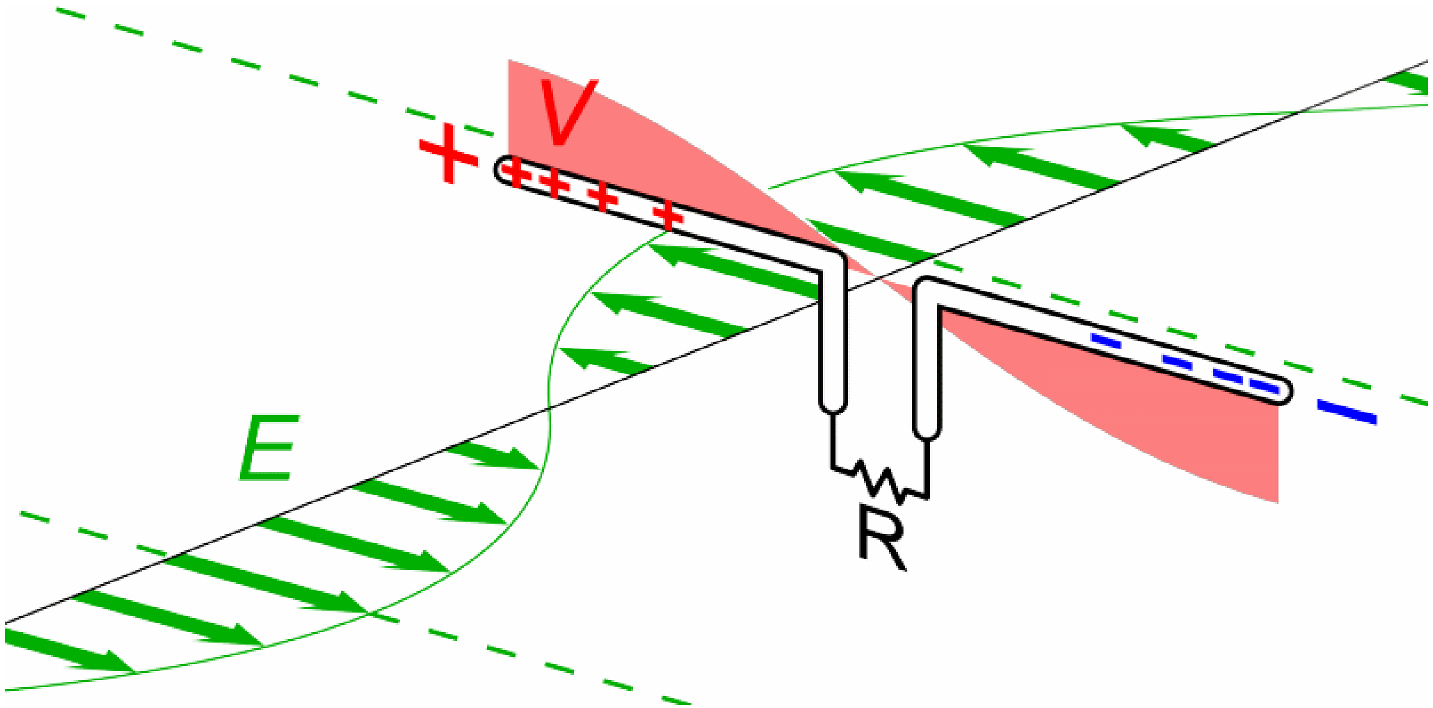
- **Backscatter**

- Backscatter Uses
  - RFID
  - NFC
  - Sensors (Backscatter LoRa)
  - Localization

- Wakeup Radios

What does an antenna *do?*

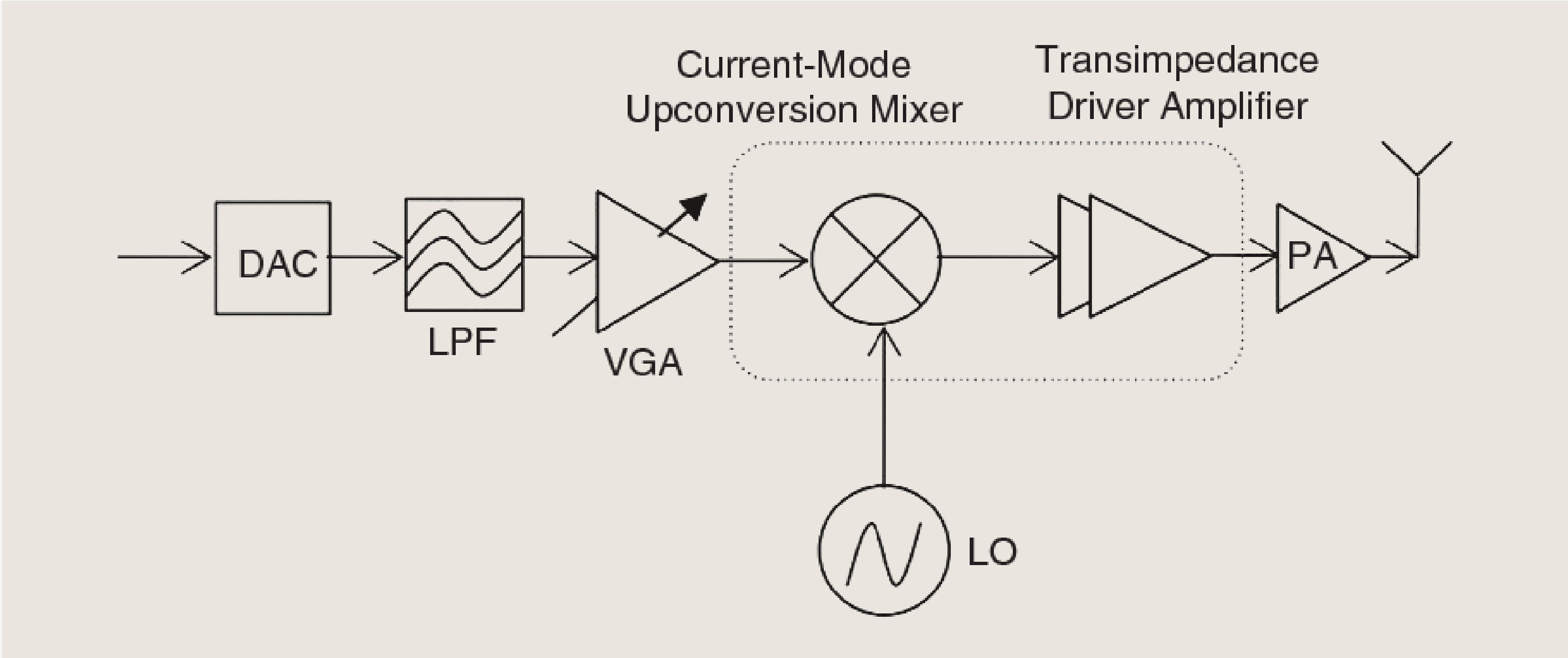
- Loosely: Converts between electric and magnetic waves



Animation by Chetvorno - Own work, CC0, https://commons.wikimedia.org/w/index.php?curid=40789783

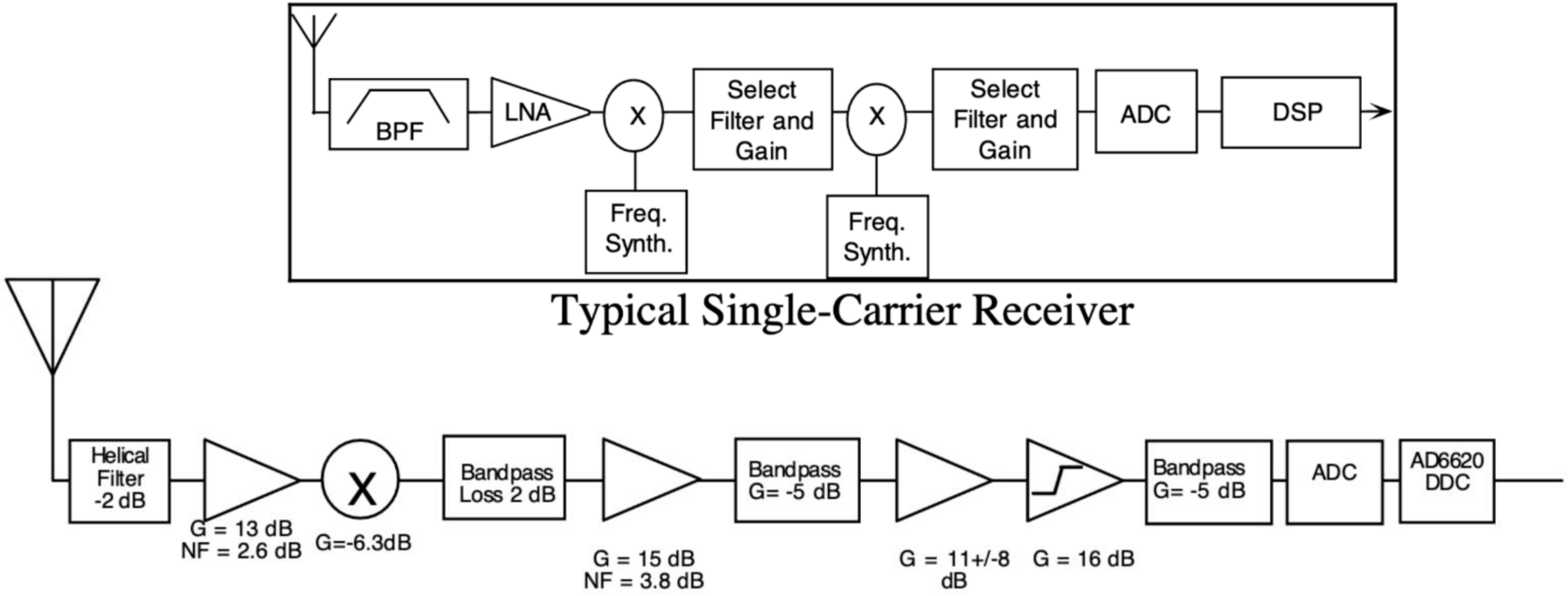
What generates electric waves?

- RF front end
  - can be done with high-speed digital components (e.g. fast DACs)



What receives electric waves?

- Again, lots of stuff nowadays…
  - Could be a high-speed ADC, more often with analog pieces in front:



Typical Single-Carrier Receiver

Graphics from Analog Devices whitepaper: https://www.analog.com/media/en/technical-documentation/tech-articles/480501640radio101.pdf — significantly more detail here

Making ultra-low power radios

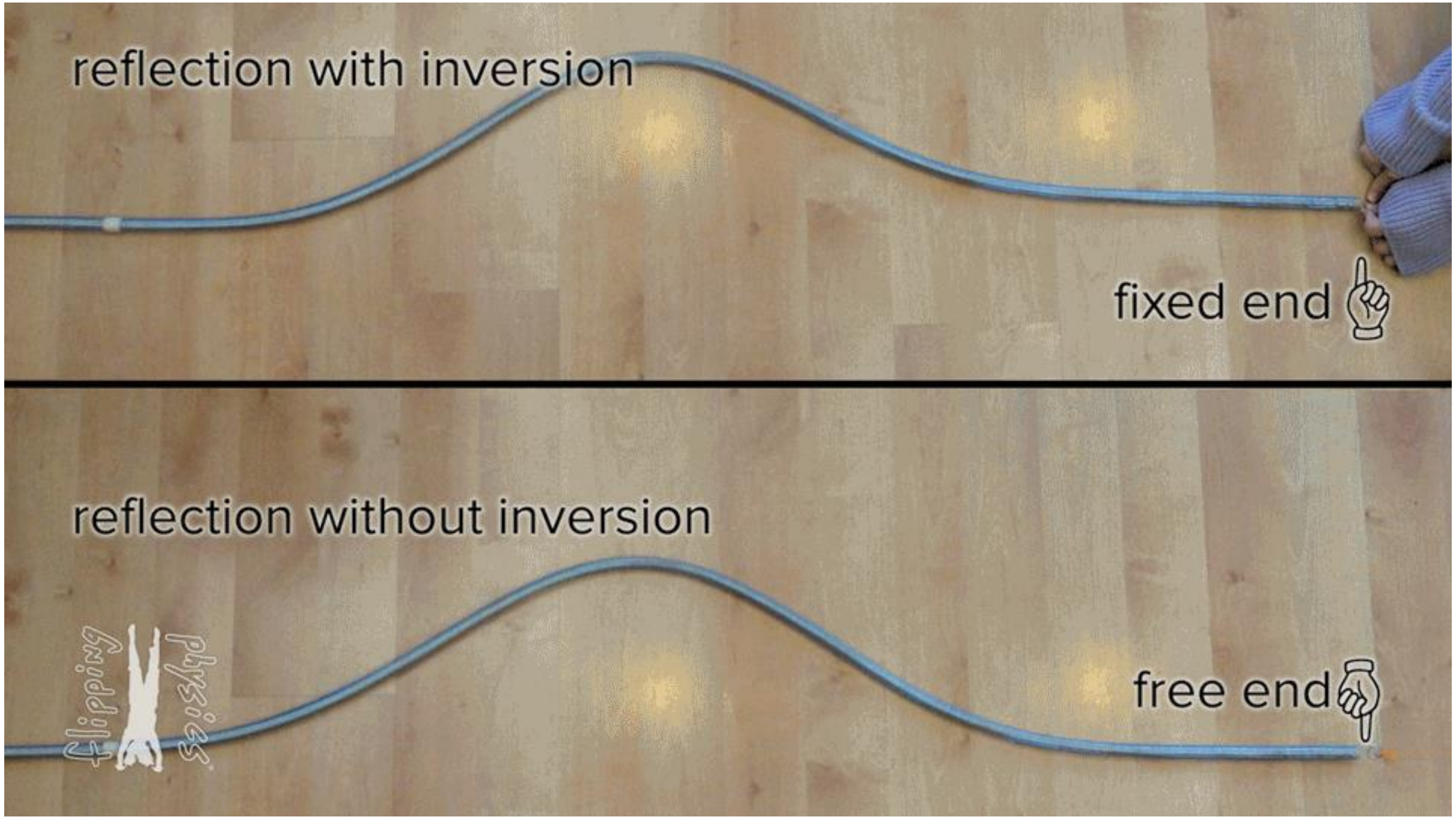
- How do we make a radio that's lower power?
- What is the most costly part of the radio?
  - Carrier-frequency generation is expensive
  - Modulating bits is comparatively lower energy

- 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: could harvest energy from the signal being received

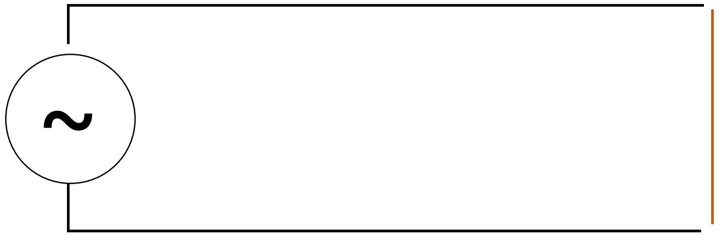
- Two versions in practice: backscatter and inductive coupling

What happens if nothing 'receives' the wave?



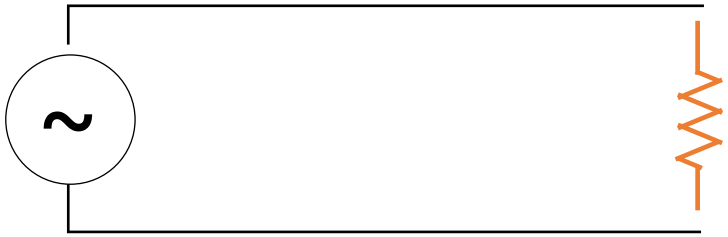
From: https://www.flippingphysics.com/standing-waves.html

”Fixed end” and “Free end” in electronic transmission



Short Circuit = “Free End”
 - Reflects wave

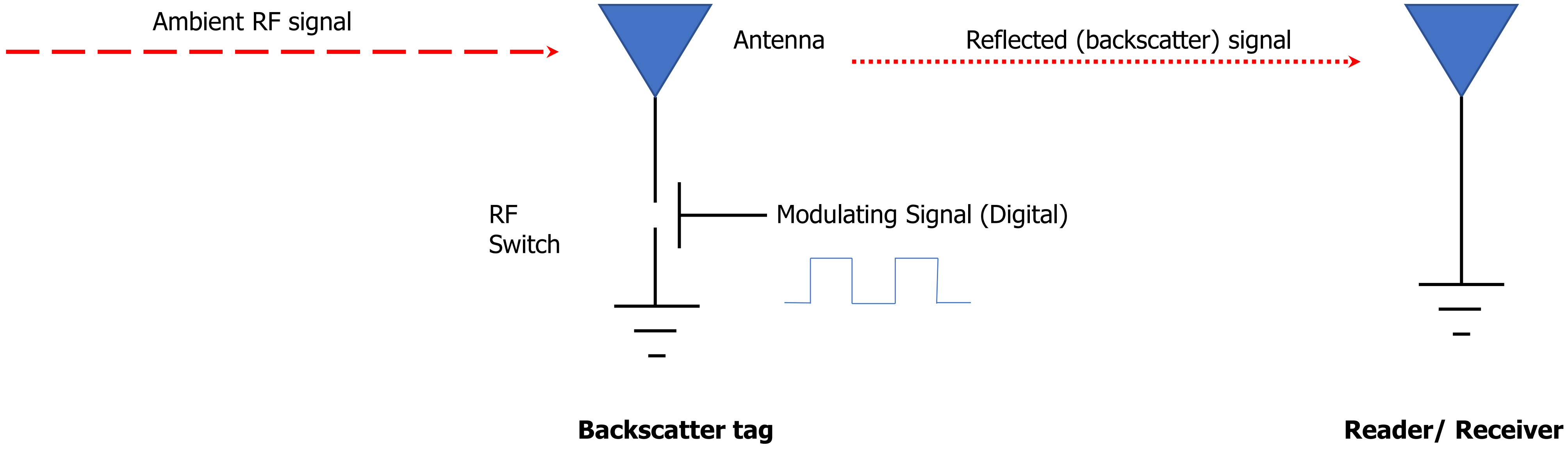
Open Circuit = “Fixed End”
 - Inverts wave



Matched Load
 - Absorbs wave (no reflection)

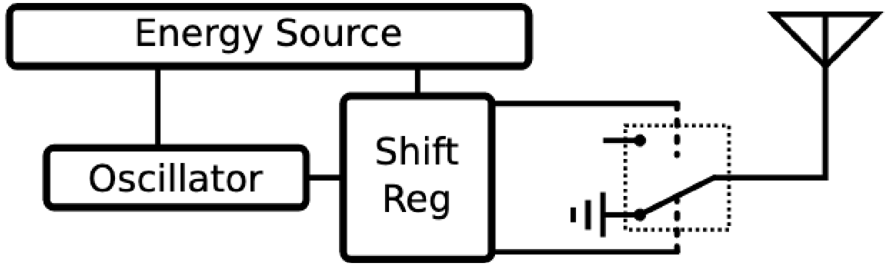
Backscatter theory of operation

- Vary between absorbing or reflecting signal to modulate data
  - Wireless transmissions at microwatts of power draw (10000x savings)
  - Frequency bands: 400 MHz, 900 MHz, 2.4 GHz
  - These are the really really cheap tags (~$0.15 each)

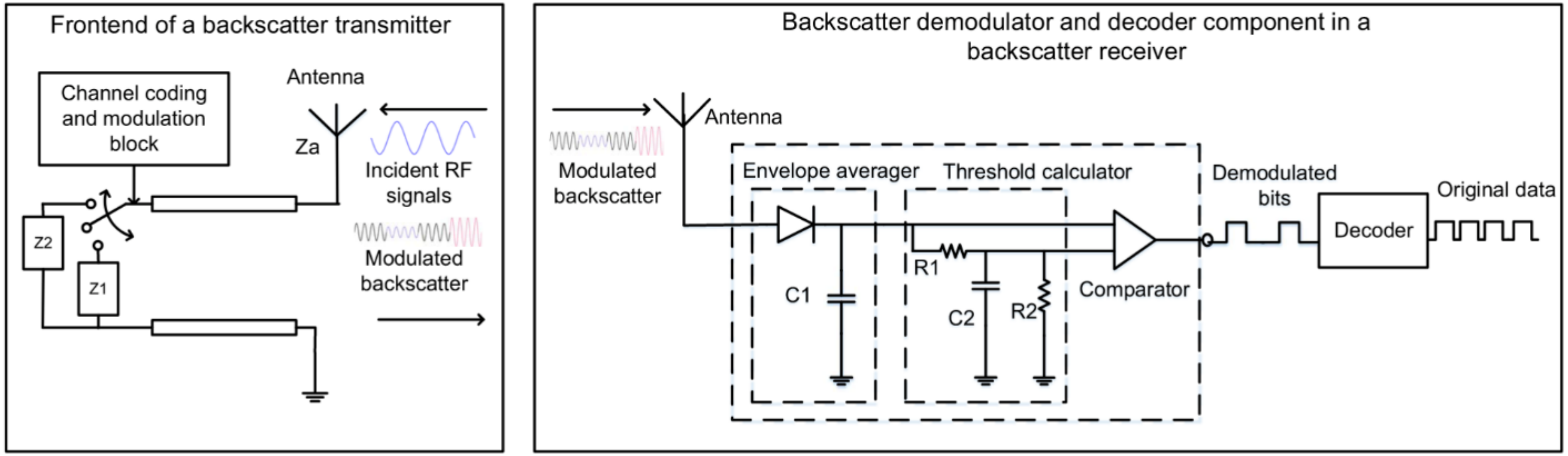


Backscatter radio designs

- Simple versions just 'reflect or don't reflect'



- Modern designs can do more advanced modulation as well



(a) (b)

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8368232

Break + Spycraft

- How could a spy use backscatter for malicious, covert purposes?

Break + Spycraft

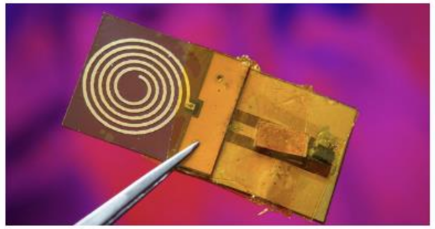
- How could a spy use backscatter for malicious, covert purposes?
  - Use microphone to change if antenna is grounded or not
  - Transmit power at the backscatter tag and collect microphone data from the response

Backscatter is an *old* idea — history in spycraft!

- 1945: Leon Theremin* creates "The Thing" (aka Great Seal Bug)
  - *Yes, same guy who invented the instrument
  - Discovered when a British embassy radio operator heard recorded conversations

Lots of *very active* research in backscatter

- Two broad paths…
  - Passive sensing
    - ”Detune” antennas predictably based on physical phenomenon
  - Cross-technology communication
    - Figure out how to speak “standard” WiFi, BLE, 15.4, etc. with backscattered signals



ForceSticker: Wireless, Batteryless, Thin & Flexible Force Sensors

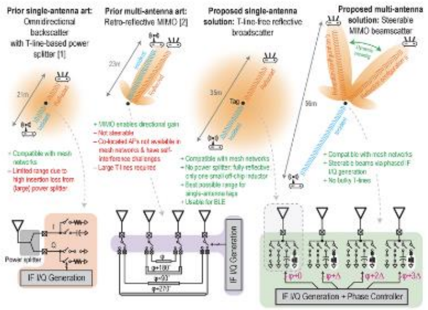
Agrim Gupta, Daegue Park, Shayaun Bashar, Cedric Girerd, Nagarjun Bhat, Siddhi Mundhra, Tania Morimoto, Dinesh Bharadia

ACM IMWUT Vol. 7, No. 1, Article 13/ Ubicomp'23

An LTE-Harvesting BLE-to-WiFi Backscattering Chip for Single-Device RFID-Like Interrogation

Shihkai Kuo, Manideep Dunna, Patrick P. Mercier, Dinesh Bharadia

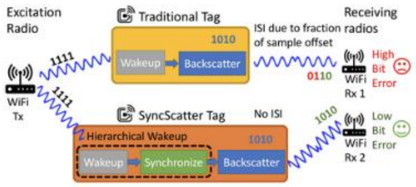
ISSCC 2023



A WiFi and Bluetooth Backscattering Combo Chip Featuring Beam Steering via a Fully-Reflective Phased-Controlled Multi-Antenna Termination Technique Enabling Operation Over 56 Meters

Shihkai Kuo, Manideep Dunna, Patrick P. Mercier, Dinesh Bharadia

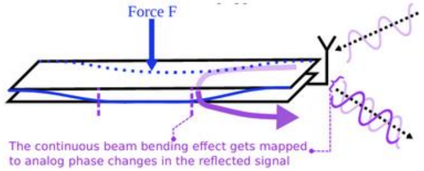
ISSCC 2022



SyncScatter: Enabling WiFi like synchronization and range for WiFi backscatter Communication

Manideep Dunna, Miao Meng, Po-Han Wang, Chi Zhang, Patrick Mercier, Dinesh Bharadia

USENIX NSDI 2021



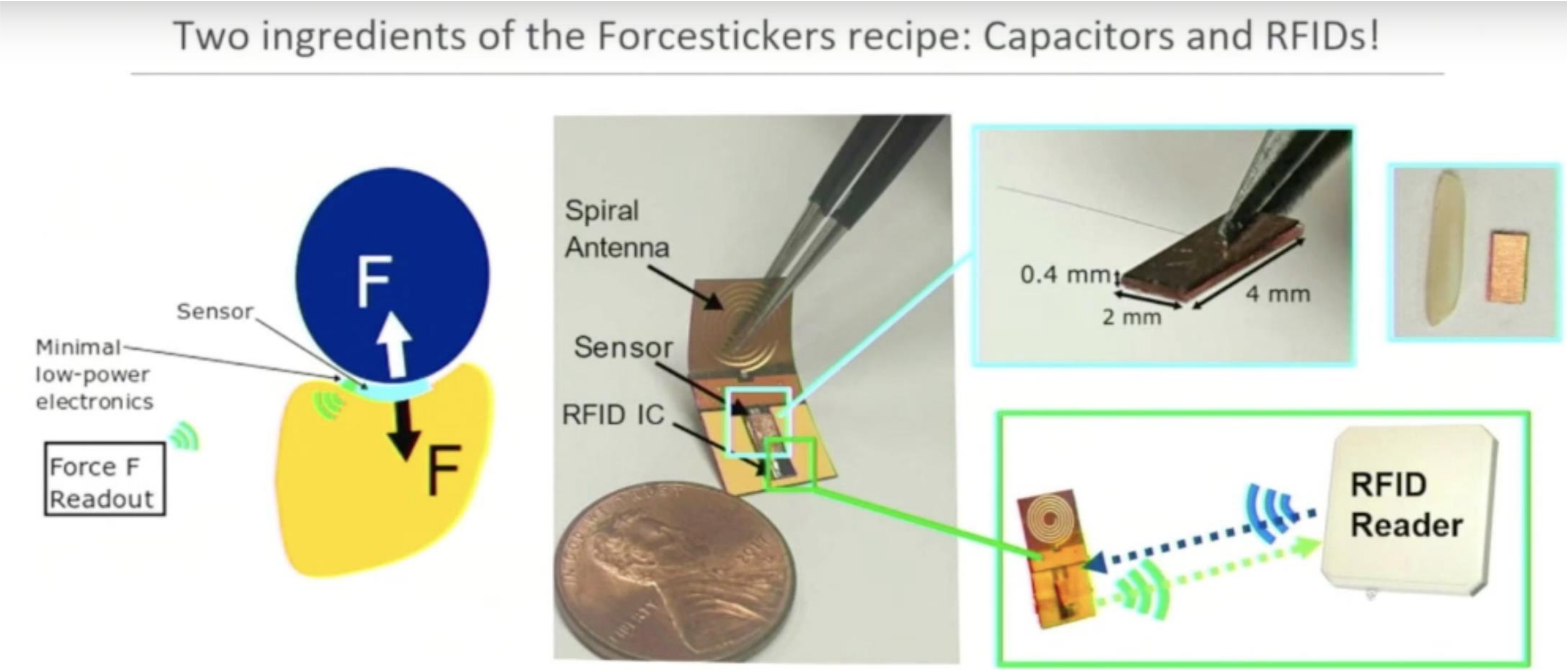
WiForce: Wireless Sensing and Localization of Contact Forces on a Space Continuum

Agrim Gupta, Cédric Girerd, Manideep Dunna, Qiming Zhang, Raghav Subbaraman, Tania Morimoto, Dinesh Bharadia

NSDI 2021

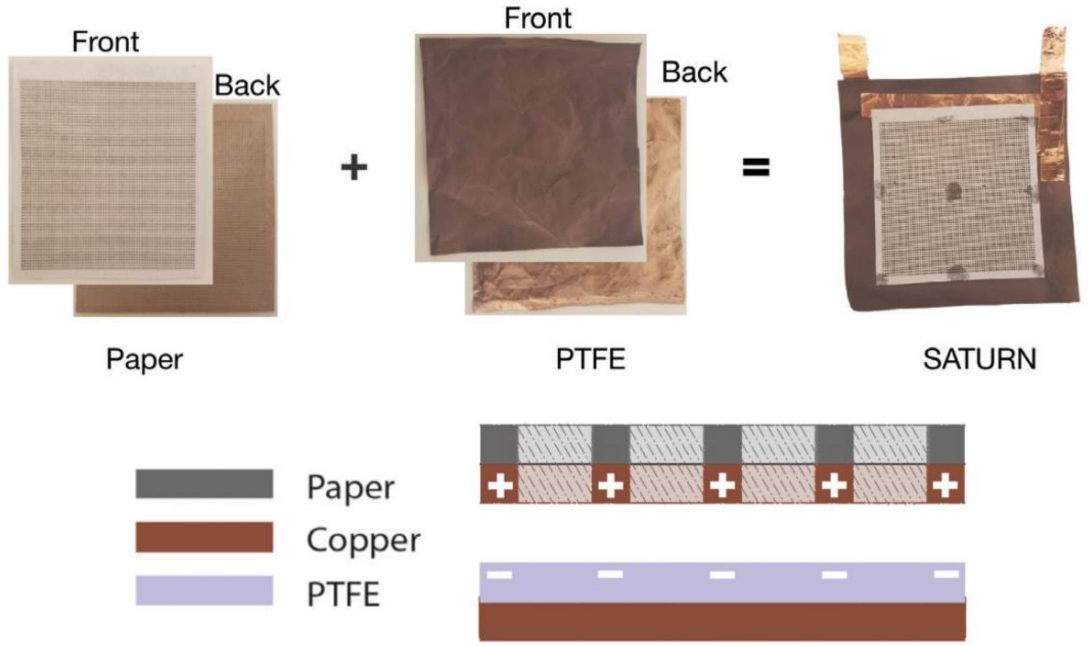
e.g., How much force is applied to a tag?

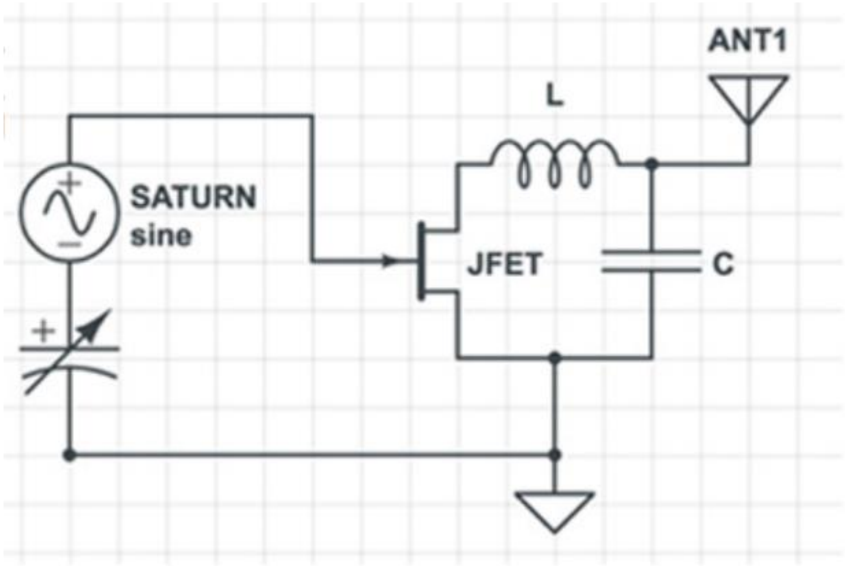
ForceSticker: Wireless, Batteryless, Thin & Flexible Force Sensors



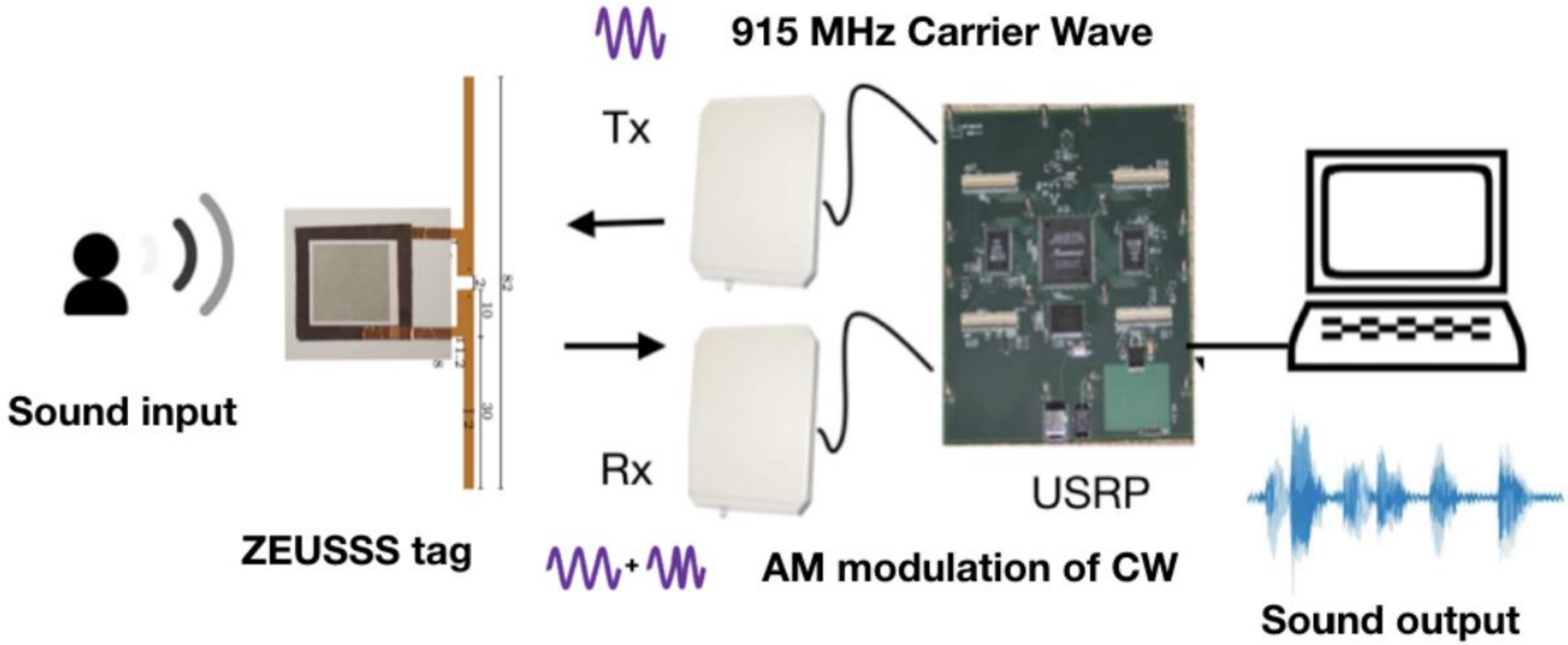
Simple sensors can trigger backscatter

- Backscatter fed directly from a sensor
  - SATURN is an energy-free microphone made of treated paper
  - Use it to trigger transistor for backscattering
  - Nivedita Arora (Northwestern ECE faculty)





Complete transmission path for SATURN audio



Outline

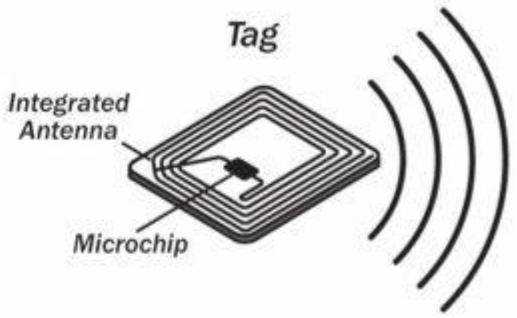
- Backscatter
- **Backscatter Uses**
  - **RFID**
  - NFC
  - Sensors (Backscatter LoRa)
  - Localization
- Wakeup Radios

RFID is *everywhere* nowadays

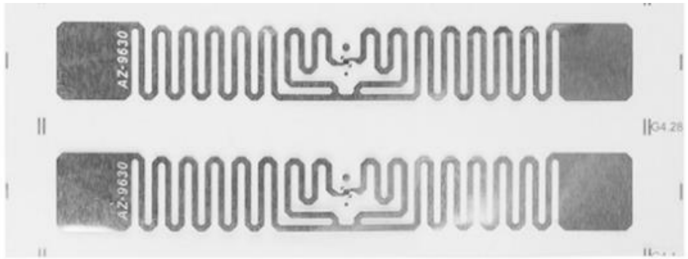
- Fundamental design principle is *asymmetry*
  - Extremely simple, cheap tags
  - Complex readers

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)



A brief digression to be precise in terminology

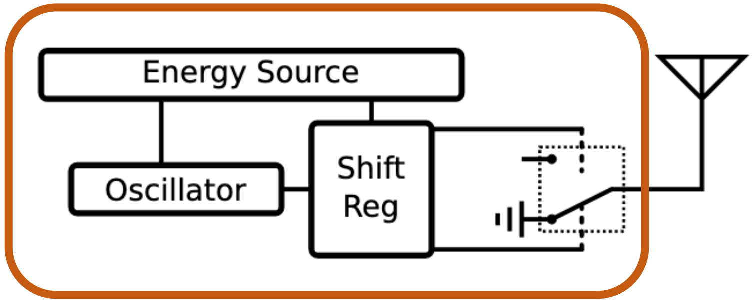
- RFID = Radio Frequency Identification = a communication standard
  - A *ton* of standards through the ~early 90's
  - Most now EPC (Electronic Product Code) Gen2

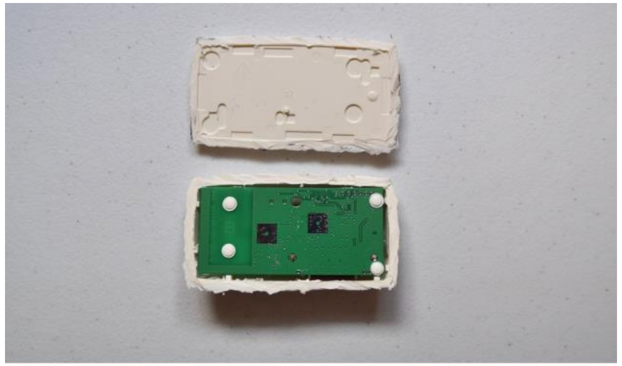
- There are actually three types of "RFID" device
  - Passive Tags - harvest power from reader & reflect
  - Semi-Passive Tags - on-board power, but reflect data
  - Active Tags - on-board power that transmit data

These are "backscatter" — which describes any communication via reflected RF

The meaningful difference is in how the tag devices power themselves

- Even on simple designs, often need some power:
- Let's look at E-ZPass for toll roads:





Let's look at RFID standards to get a sense of the numbers

- Low Frequency (~300 kHz) — mostly legacy
  - ~10cm read range (inductive coupling)

- High Frequency (3~30 MHz; often 13.56 MHz)
  - Passive: 4~7 m max (usually inductive coupling, I think)
  - Semi-Passive: 10~30 m max
  - Active: 30+ m

- Ultra-High Frequency (300 MHz ~ 3 GHz)
  - Passive: Up to 12 m (backscatter)
  - Active: Up to 100 m

RFID challenges

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

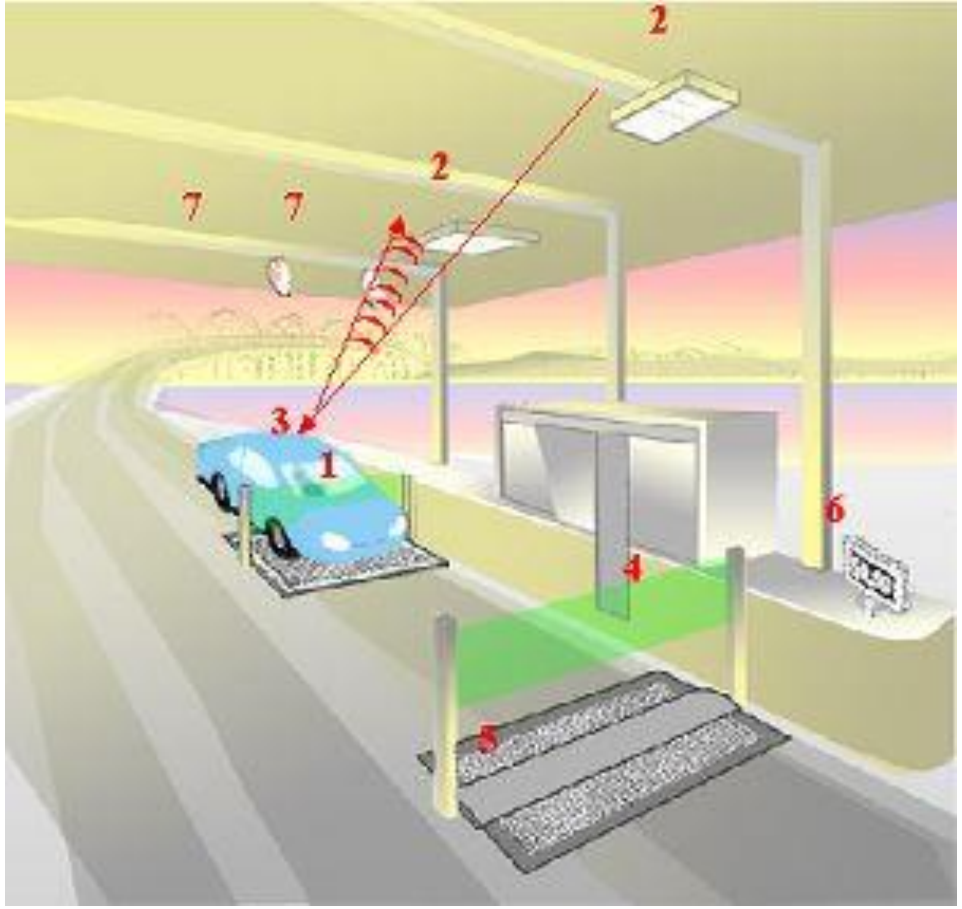
- Difficult to reflect energy when it is already so low
  - Essentially double the path loss (there and back)

- 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

Car RFID systems

- Usually two mounted antennas
  - One broadcasts energy, activating the RFID device
  - The other receives the reflected data
- Devices are often battery powered for longer-range operation
  - Semi-passive
  - 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

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)

Break + Security Consideration

- What data should an ID card send?
  - **Is just sending ID bits sufficient? What problem could occur?**

Break + Security Consideration

- What data should an ID card send?
  - **Is just sending ID bits sufficient? What problem could occur?**

  - 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

How does RFID, Backscatter, etc map back to the IoT?

- Well, as always, "Power and Communication are the hard part"
  - RFID works, but only in the presence of an RFID reader
  - Recent research looks at eliminating that latter clause

- Power: RF Harvesting for general purpose computation
  - WISP
  - Moo

- Communication: Repurposing extant RF signals for other uses
  - Ambient Backscatter
  - Inter-Technology Backscatter

Outline

- Backscatter
- **Backscatter Uses**
  - RFID
  - **NFC**
  - Sensors (Backscatter LoRa)
  - Localization
- Wakeup Radios

Near Field Communication (NFC)

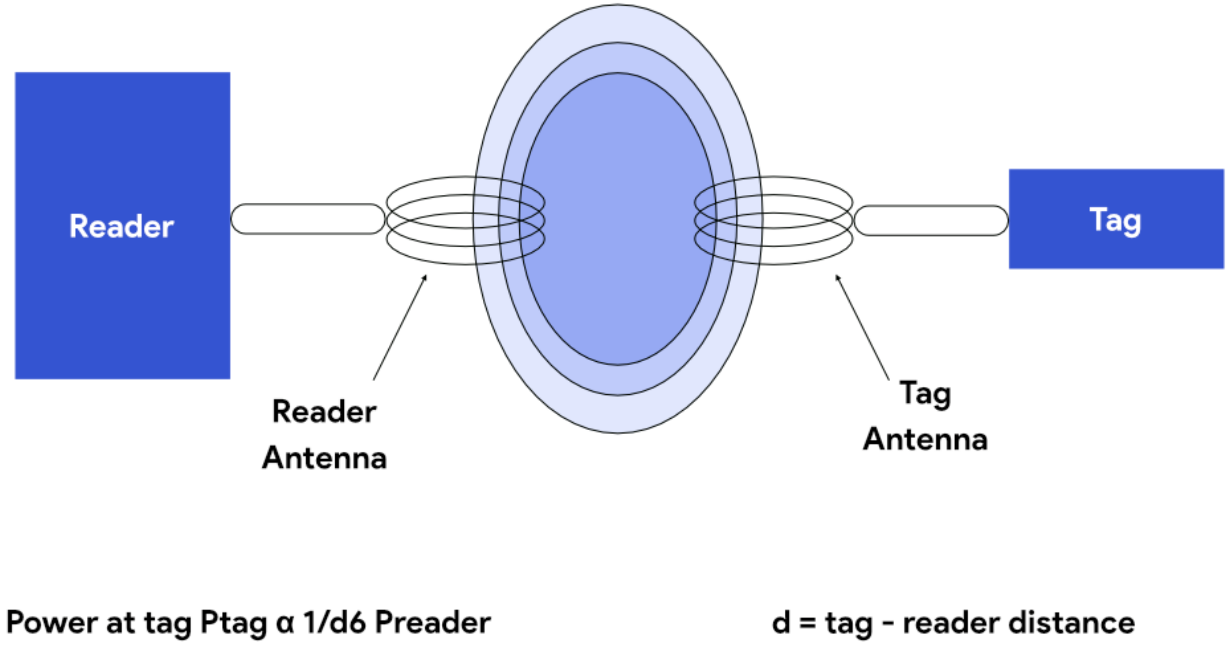
- Inductive Coupling concept (13.56 MHz)
  - But attached to a powered and capable device (smartphone)
  - 10-20 cm range max (usually <10)

- 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

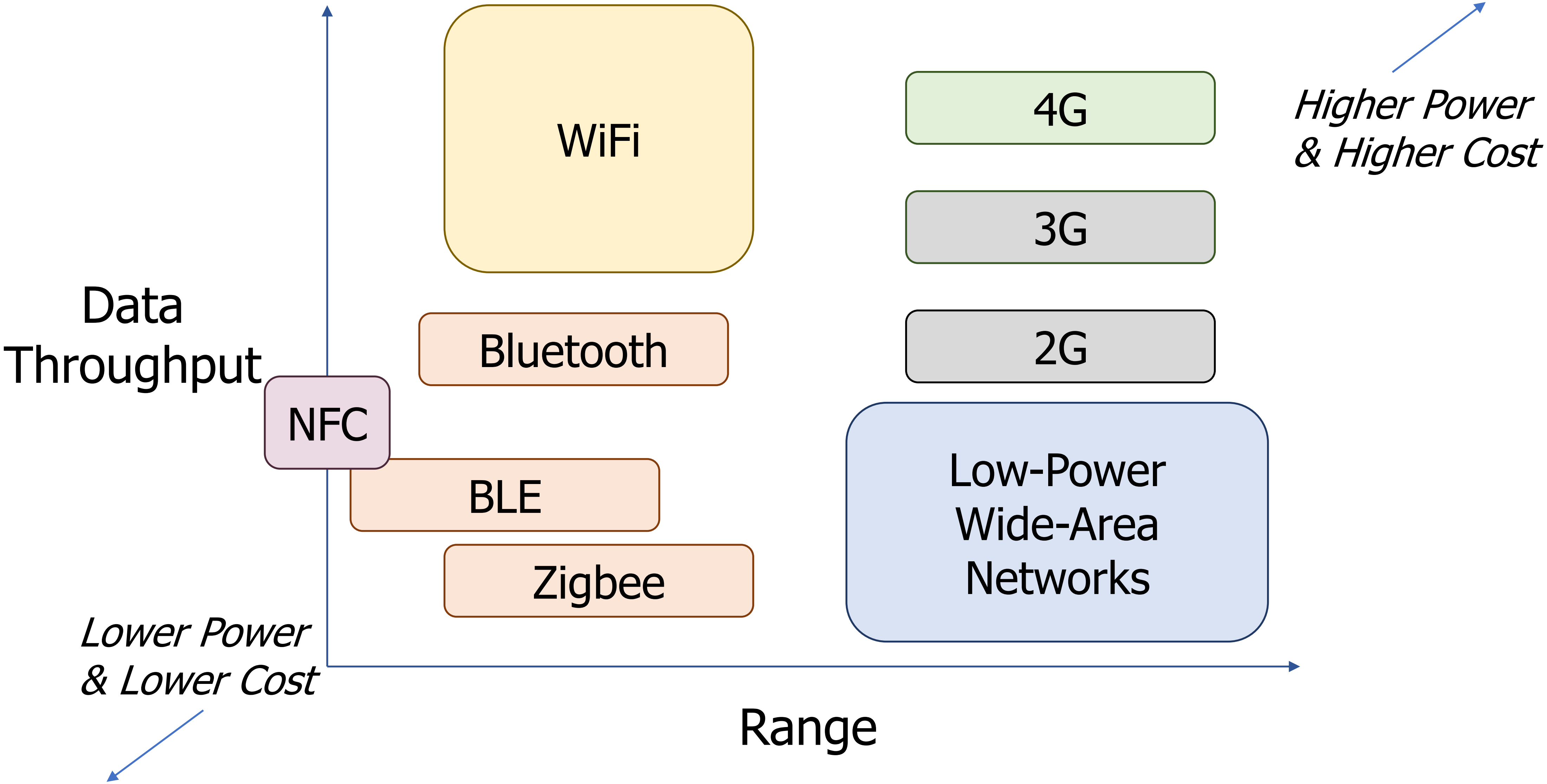
- Data rate 100-400 kbps!
  - nRF52840 capable of 100 kbps communication with attached antenna

Inductive coupling theory of operation

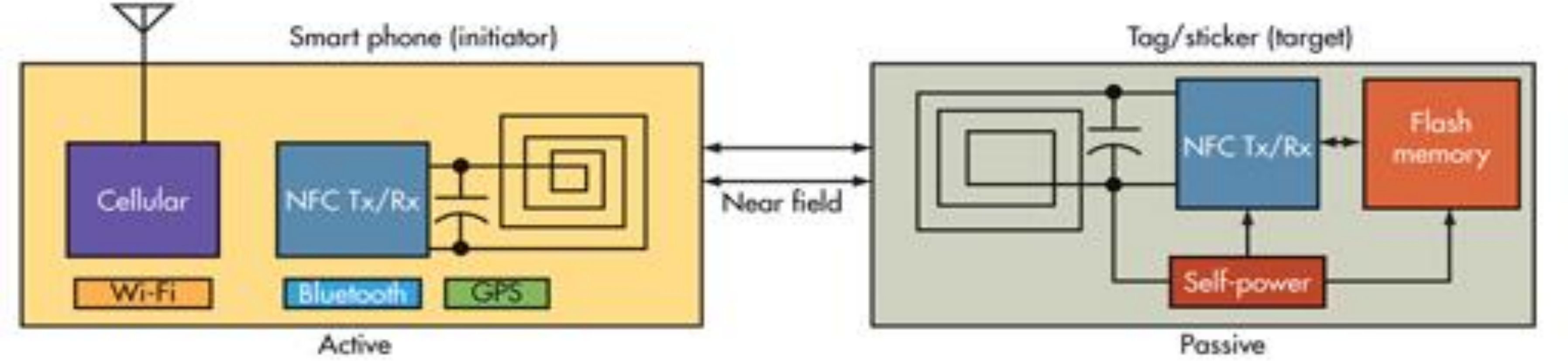
- A shared magnetic field is created between the two devices
  - Change in current through one device induces current change through the other
  - Device can vary load to transmit data
- Very low frequency bands (135 KHz, 13.56 MHz)
  - Transmit through materials including skin
  - Sensitive to metal



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



NFC Active and Passive Devices



- **<u>Active NFC device</u>** is usually microcontroller-based like an <u>NFC enabled smartphone</u>. Can exchange information with other NFC devices. It powers itself.
- **<u>A passive device</u>**, such as an <u>NFC tag</u>, contains information that other devices can read but does not read any information itself. NFC tag does not have its own power source.

NFC Tags – Encoding data

- NDEF (NFC Data Exchange Format) Structure
  - Binary format for data
  - Messages contains records
  - Each record has header
- NFC read returns the NDEF message

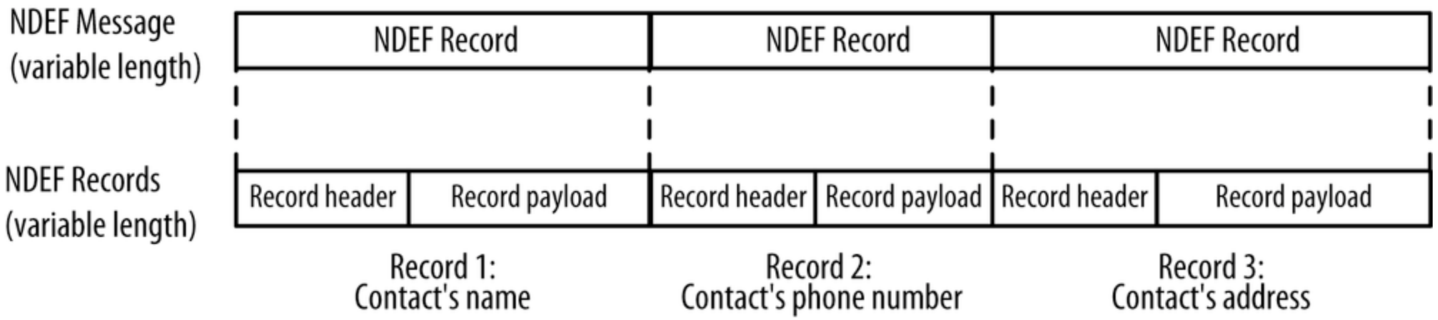
NFC Forum NDEF record types

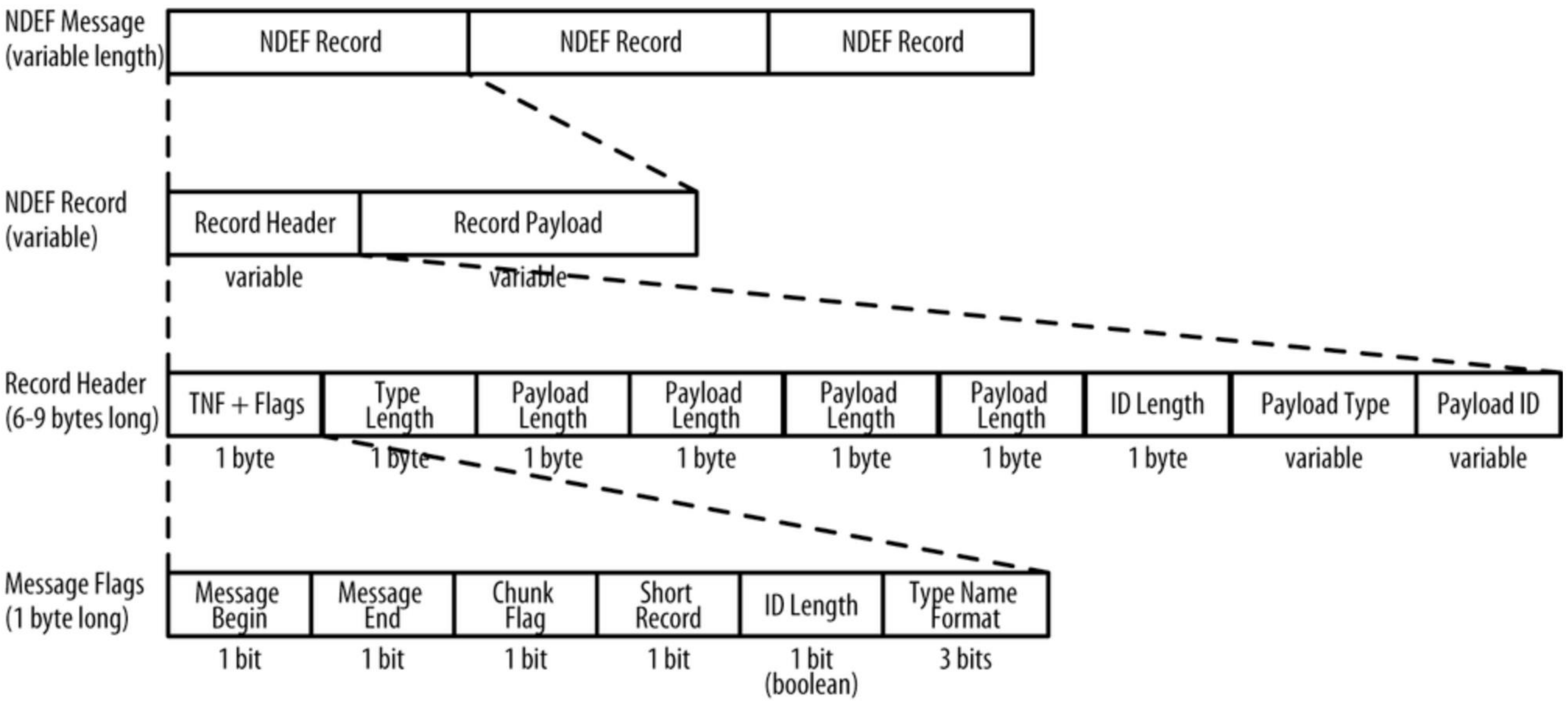
- Record Type Definitions
  - **RTD Technical** - Specifies the format and rules for building standard record types used by NFC Forum application definitions and third parties that are based on the NDEF data format.
  - **Text** - Provides an efficient way to store text strings in multiple languages by using the RTD mechanism and NDEF format. An example of using this specification is included in the Smart Poster RTD.
  - **URI** - Provides an efficient way to store Uniform Resource Identifiers (URI) by using the RTD mechanism and NDEF format. An example of using this specification is included in the Smart Poster RTD.
  - **Smart Poster** - Defines an NFC Forum Well Known Type to put URLs, SMSs or phone numbers on an NFC tag, or to transport them between devices. The Smart Poster RTD builds on the RTD mechanism and NDEF format and uses the URI RTD and Text RTD as building blocks.
  - **Generic Control** - withdrawn
  - **Signature** - Specifies the format used when signing single or multiple NDEF records. Defines the required and optional signature RTD fields, and also provides a list of suitable signature algorithms and certificate types that can be used to create the signature. Does not define or mandate a specific PKI or certification system, or define a new algorithm for use with the Signature RTD.
  - **PHDC** - Addresses a need for an openly-defined standard for the exchange of personal health data between devices using Near Field Communication technology.

Derived types

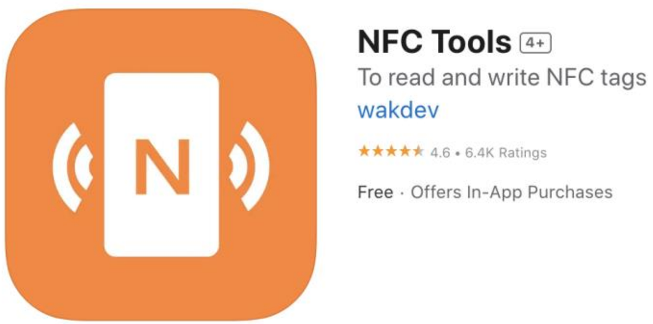
Android Application NDEF Record
Application NDEF Record
Contact NDEF Record
Email NDEF Record
File NDEF Record
Geolocation NDEF Record
Phone NDEF Record
SMS NDEF Record
Website NDEF Record
WiFi NDEF Record

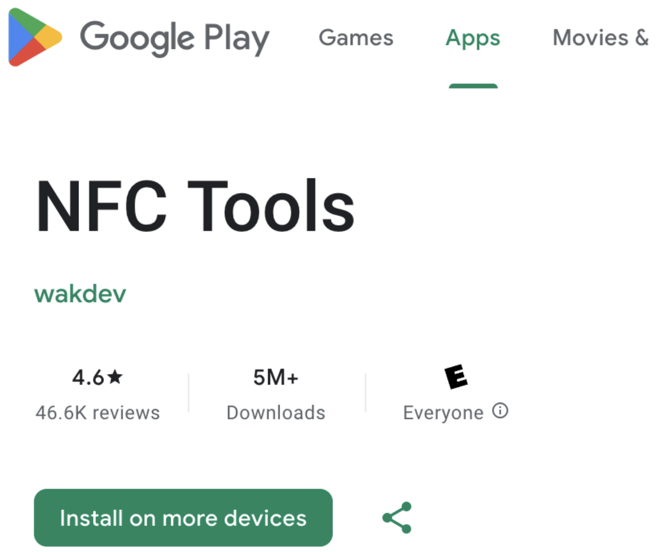
NDEF Format

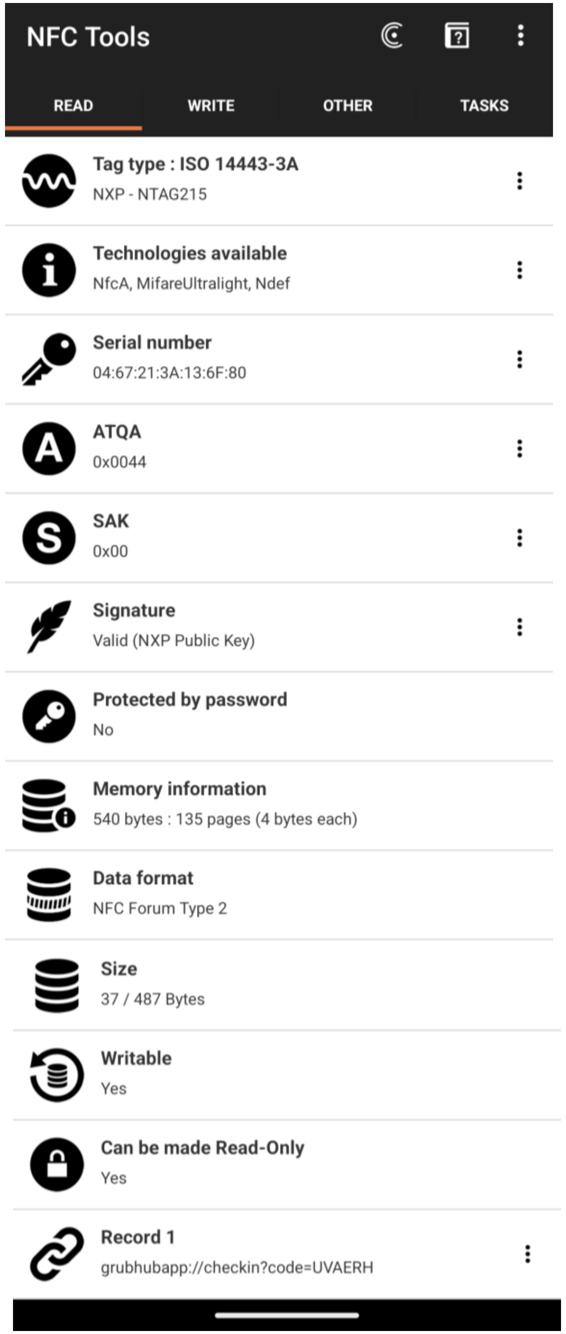

NDEF Message
(variable length)
NDEF Record
NDEF Record
NDEF Record
NDEF Records
(variable length)
Record header
Record payload
Record header
Record payload
Record header
Record payload
Record 1:
Contact's name
Record 2:
Contact's phone number
Record 3:
Contact's address


NDEF Message
(variable length)
NDEF Record
NDEF Record
NDEF Record
NDEF Record
(variable)
Record Header
Record Payload
variable
variable
Record Header
(6-9 bytes long)
TNF + Flags
Type Length
Payload Length
Payload Length
Payload Length
Payload Length
ID Length
Payload Type
Payload ID
1 byte
1 byte
1 byte
1 byte
1 byte
1 byte
1 byte
variable
variable
Message Flags
(1 byte long)
Message Begin
Message End
Chunk Flag
Short Record
ID Length
Type Name Format
1 bit
1 bit
1 bit
1 bit
1 bit
(boolean)
3 bits

Investigating NFC on your own







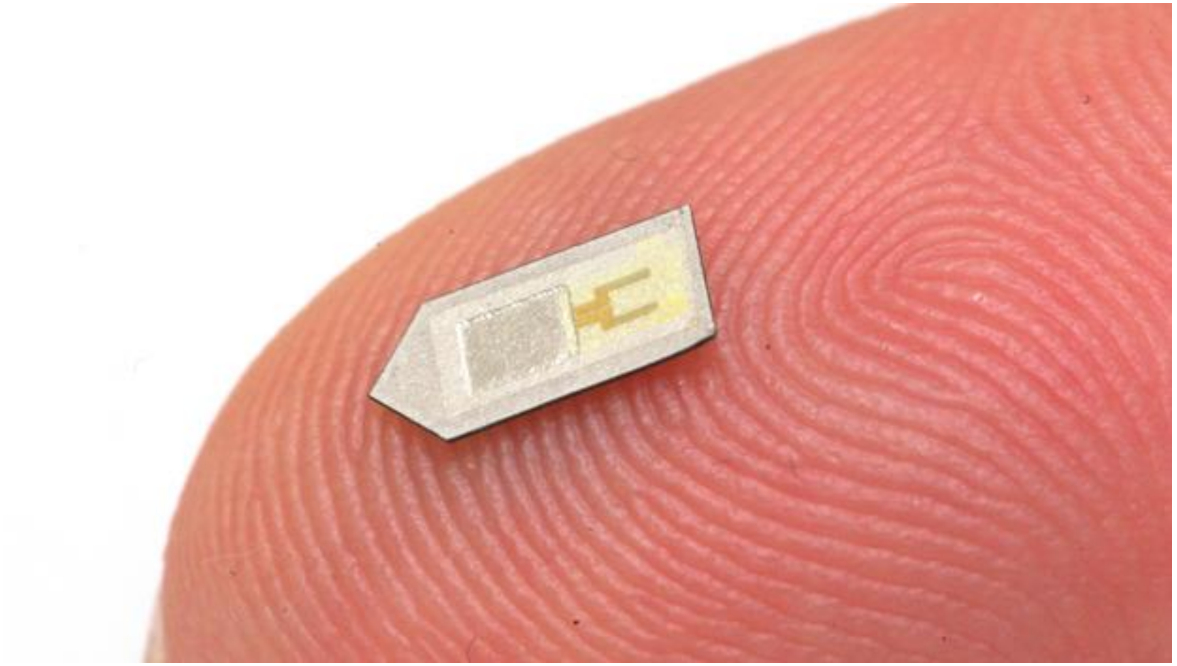
- NFC tools app allows you to inspect NFC tags

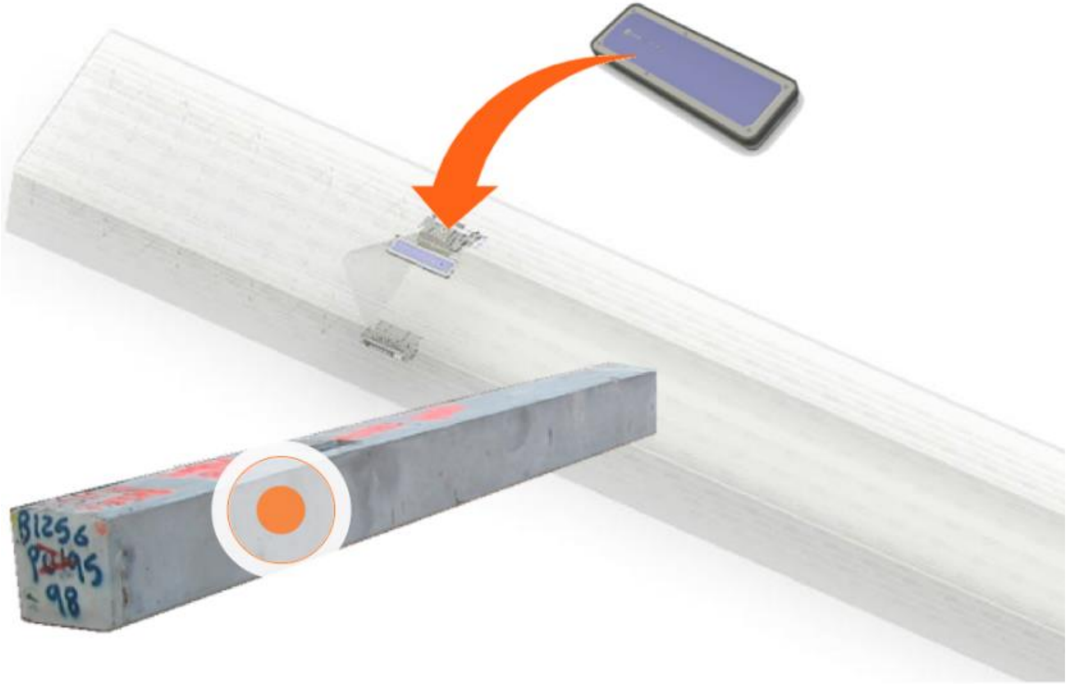
Outline

- Backscatter
- **Backscatter Uses**
  - RFID
  - NFC
  - **Sensors (Backscatter LoRa)**
  - Localization
- Wakeup Radios

“Embedded” sensors

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

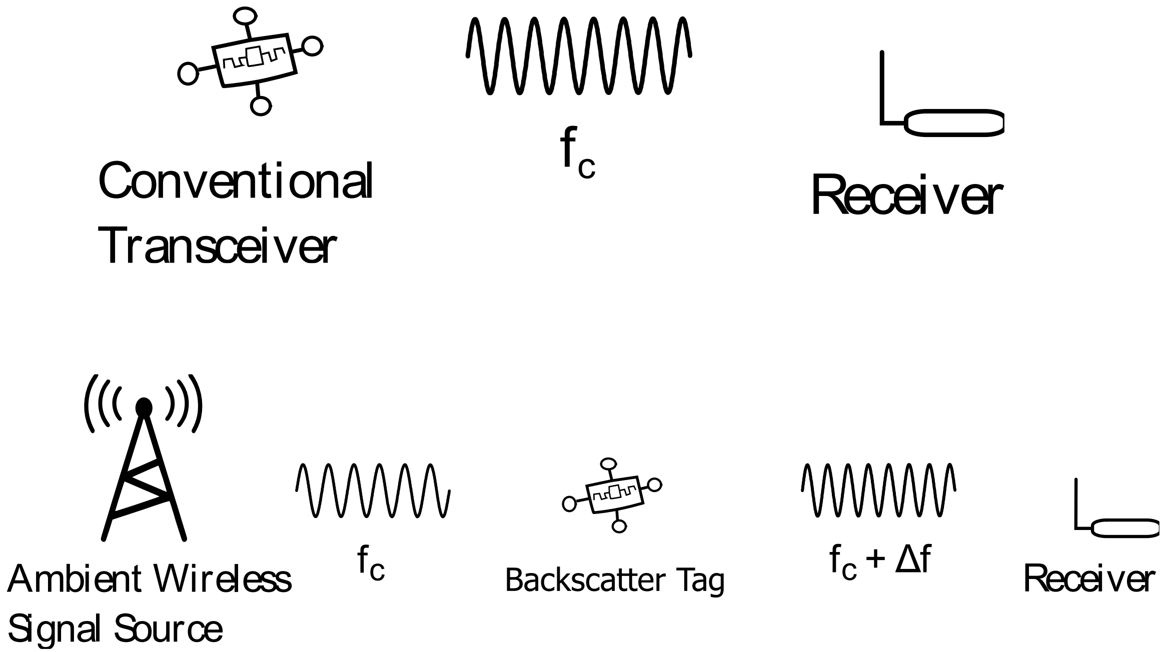




Backscatter for sensor networks

Conventional Radio

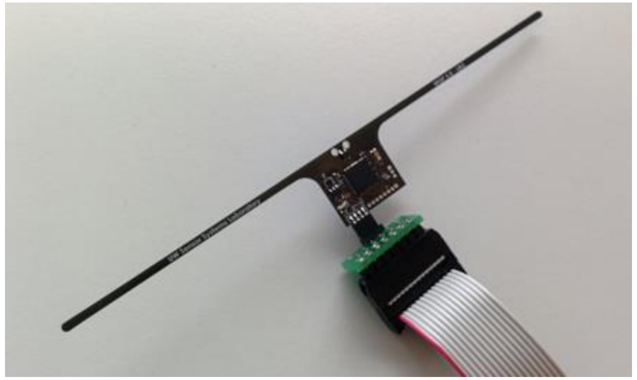
Backscatter Transmissions



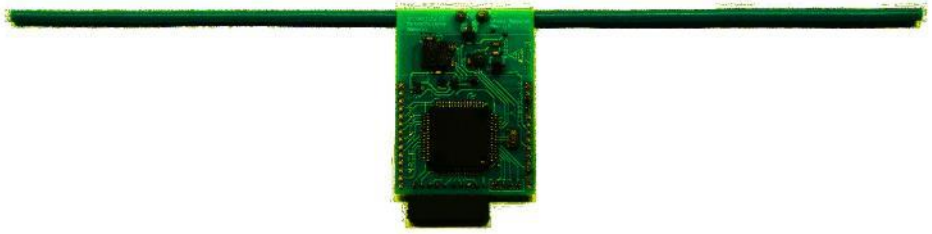
- Backscatter allows transmissions at up to 10000x lower power than conventional radios
  - Makes it very attractive for low-energy sensing devices

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

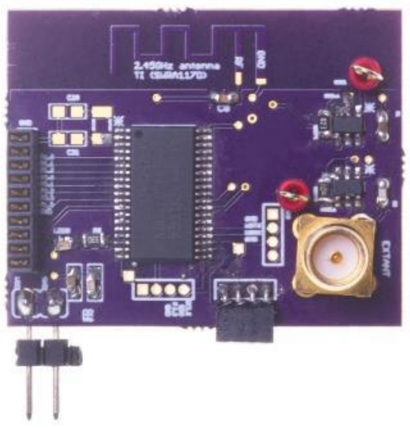


Moo 1.0
University of
Massachusetts

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?

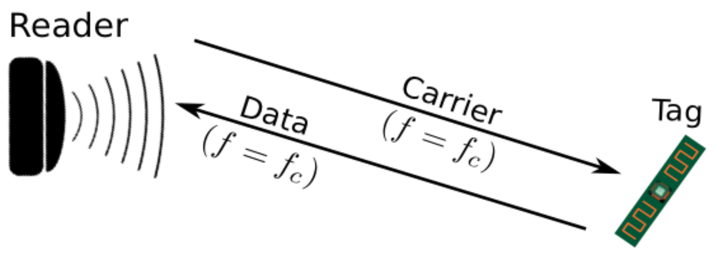
- LoRea: long-range transmissions at µW
  - (Next few slides stolen from Ambuj's talks)



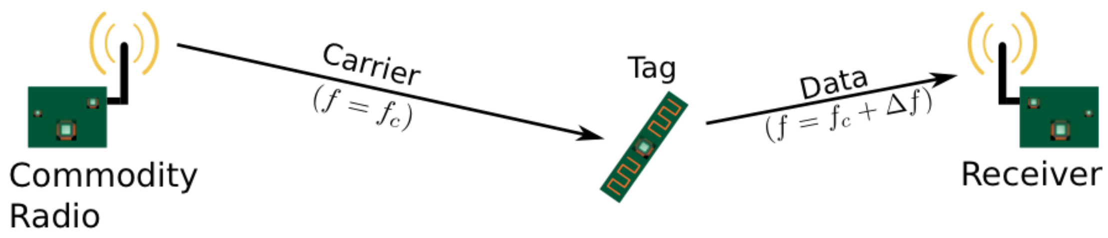
Varshney et al. "LoRea: A Backscatter architecture that achieves a long communication range" SenSys 2017

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

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



Monostatic configuration



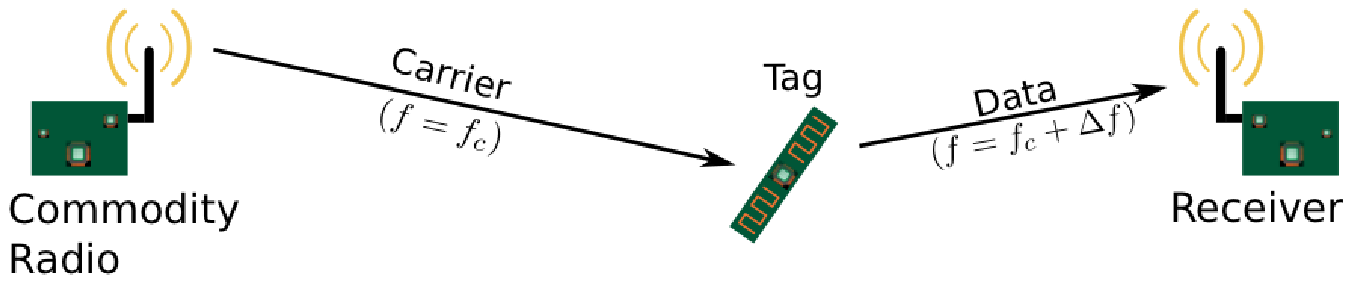
Bi-static configuration

- 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

Ran out of space while performing experiments…

- State-of-art few meters. System 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

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

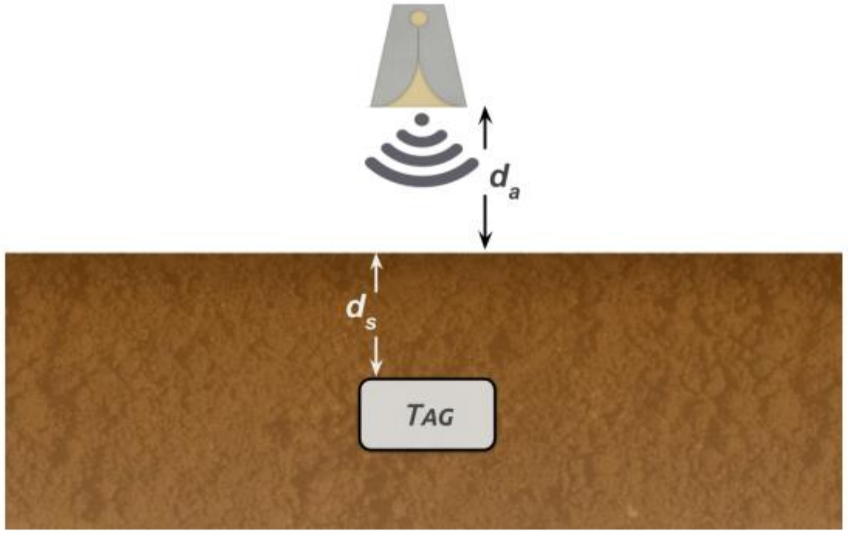
Range reported are line of sight, with backscatter tag co-located with carrier source

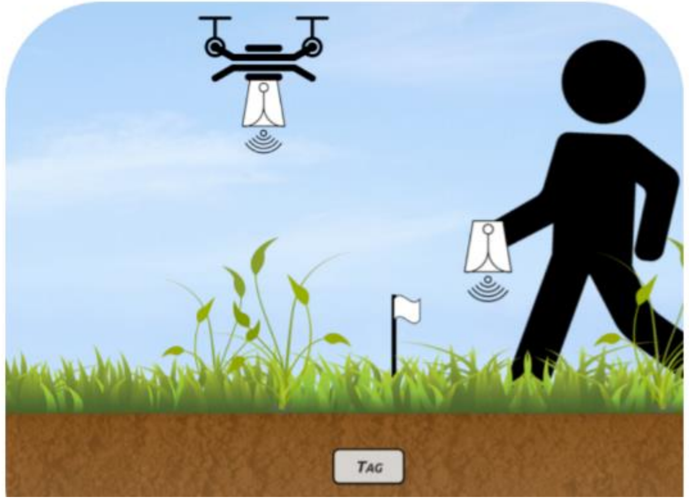
Future research directions for backscatter sensor communication

- 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

Backscatter as a sensor: soil moisture

- Idea: bury backscatter tags in soil
  - Measure round-trip-time for signal to reflect
  - T_s (time signal travels through ground) changes based on the moisture in the soil





Josephson, Colleen, et al. "Low-cost In-ground Soil Moisture Sensing with Radar Backscatter Tags.“ COMPASS 2021

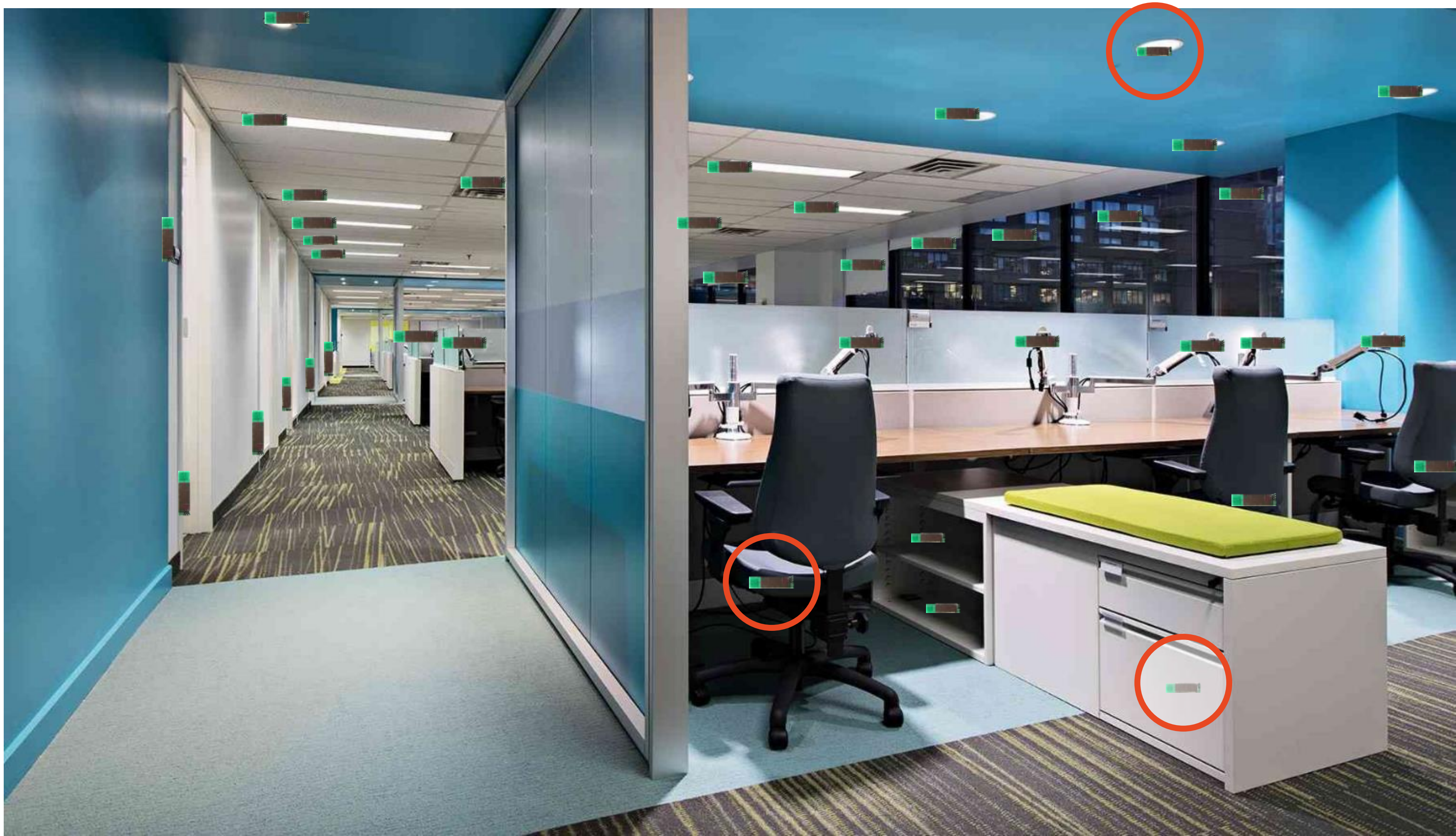
Break + Open Question

- What would you use a backscatter sensor for?
    - Requirement: sensing has to be extremely low power too

Outline

- Backscatter
- **Backscatter Uses**
  - RFID
  - NFC
  - Sensors (Backscatter LoRa)
  - **Localization**
- Wakeup Radios

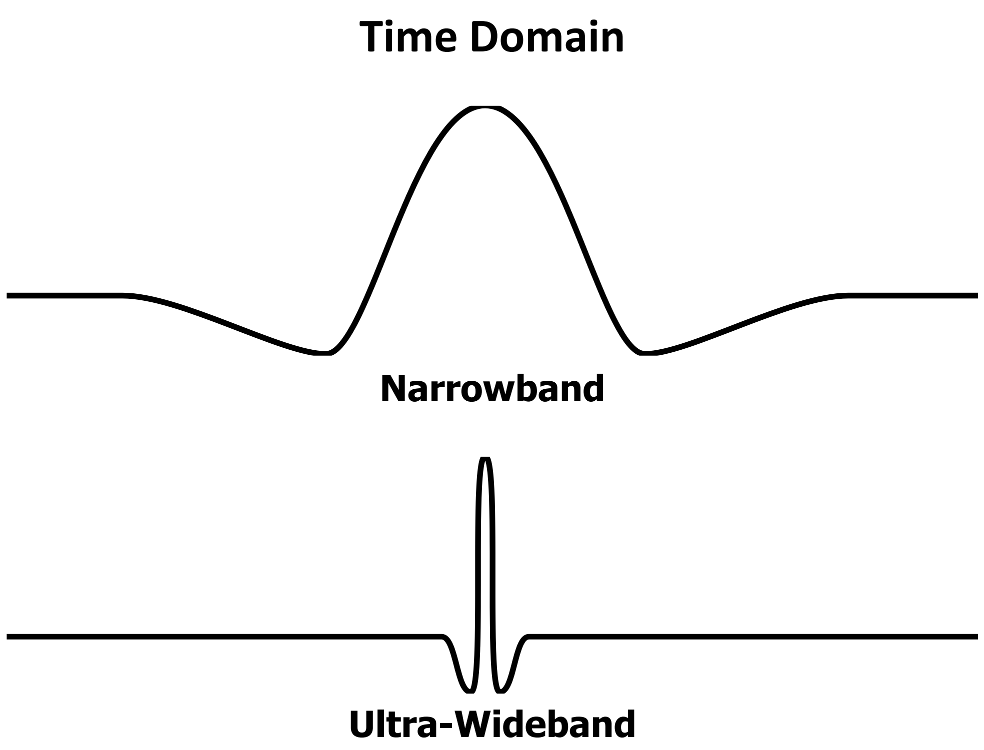
Slocalization: Ultra wideband backscatter localization

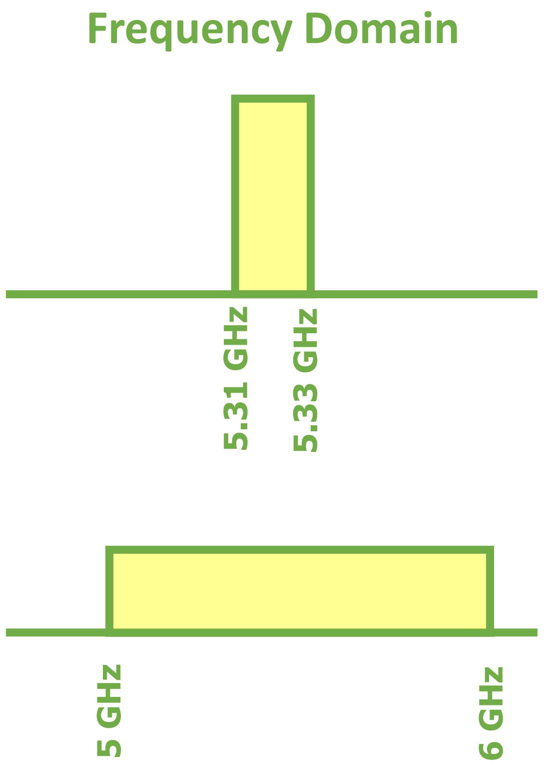


Why RF, why ultra wideband, why backscatter for ubiquitous localization?

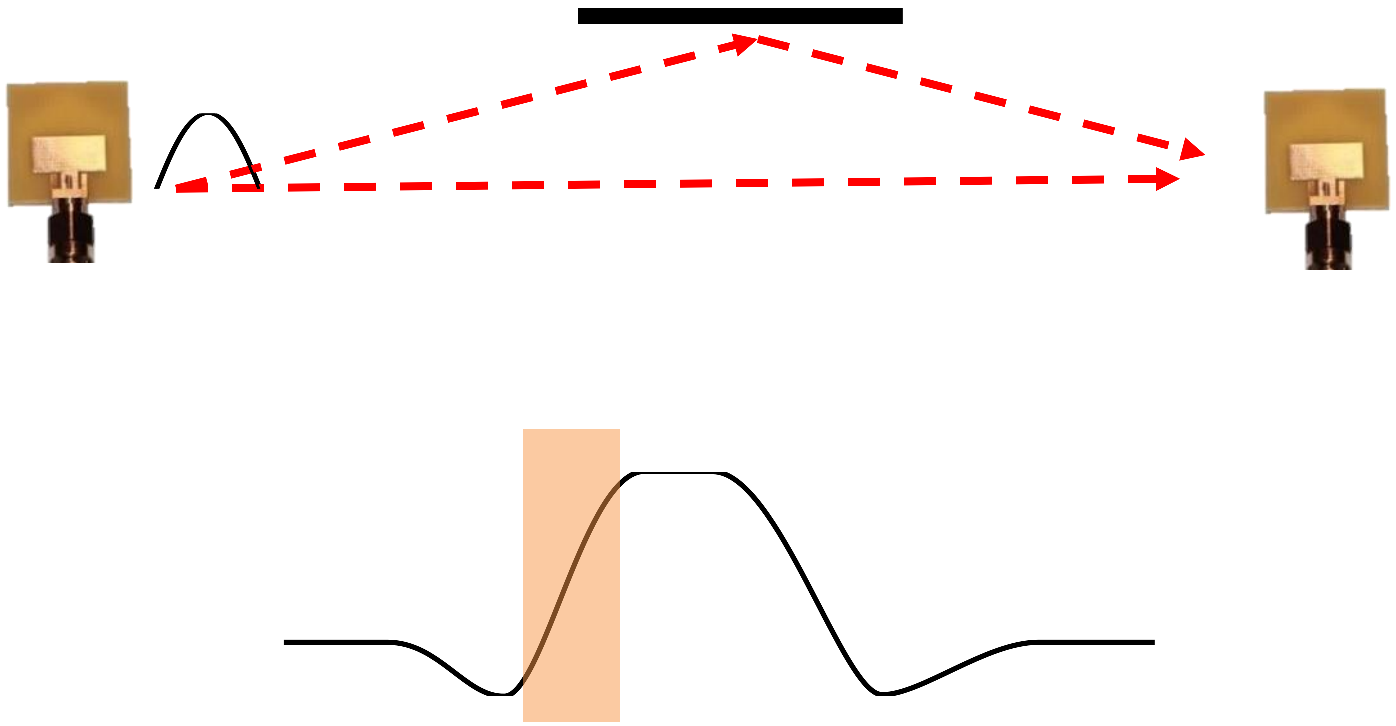
Mautz, Rainer. "Indoor positioning technologies." (2012).

Why RF, why ultra wideband, why backscatter for ubiquitous localization?

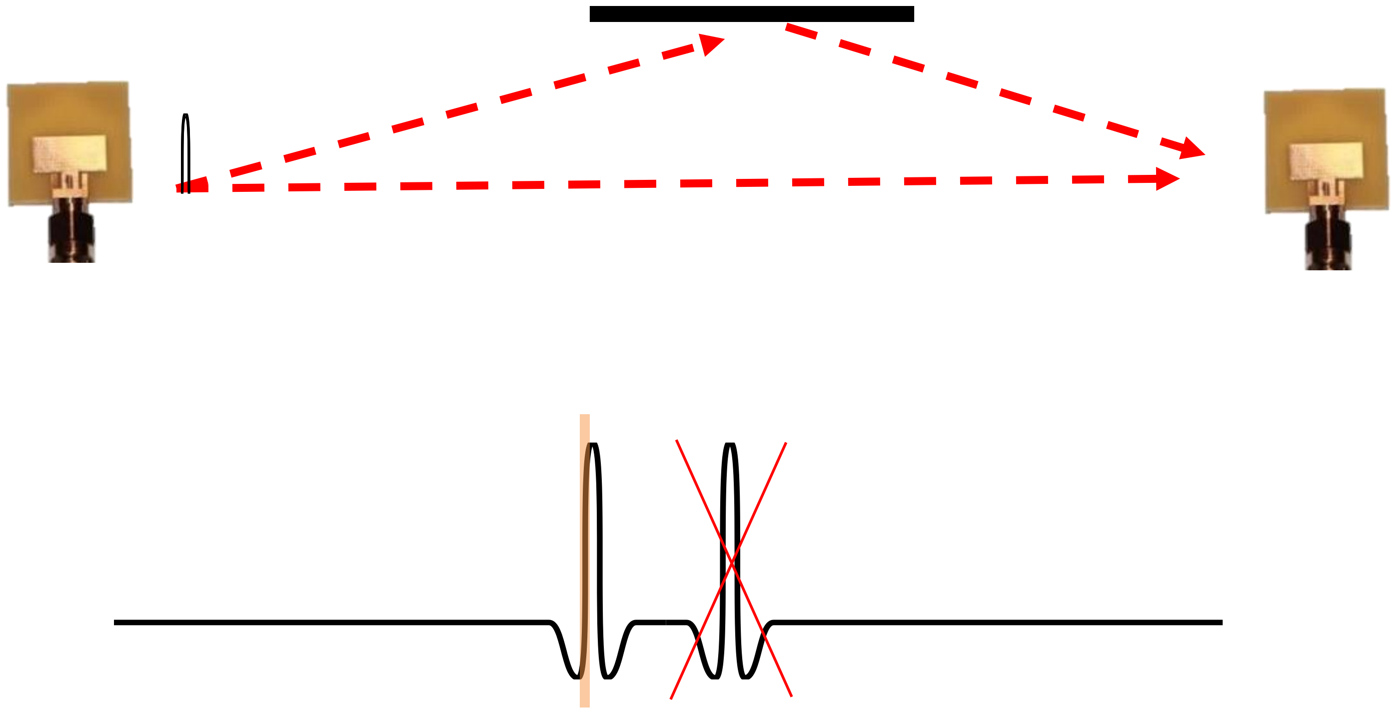




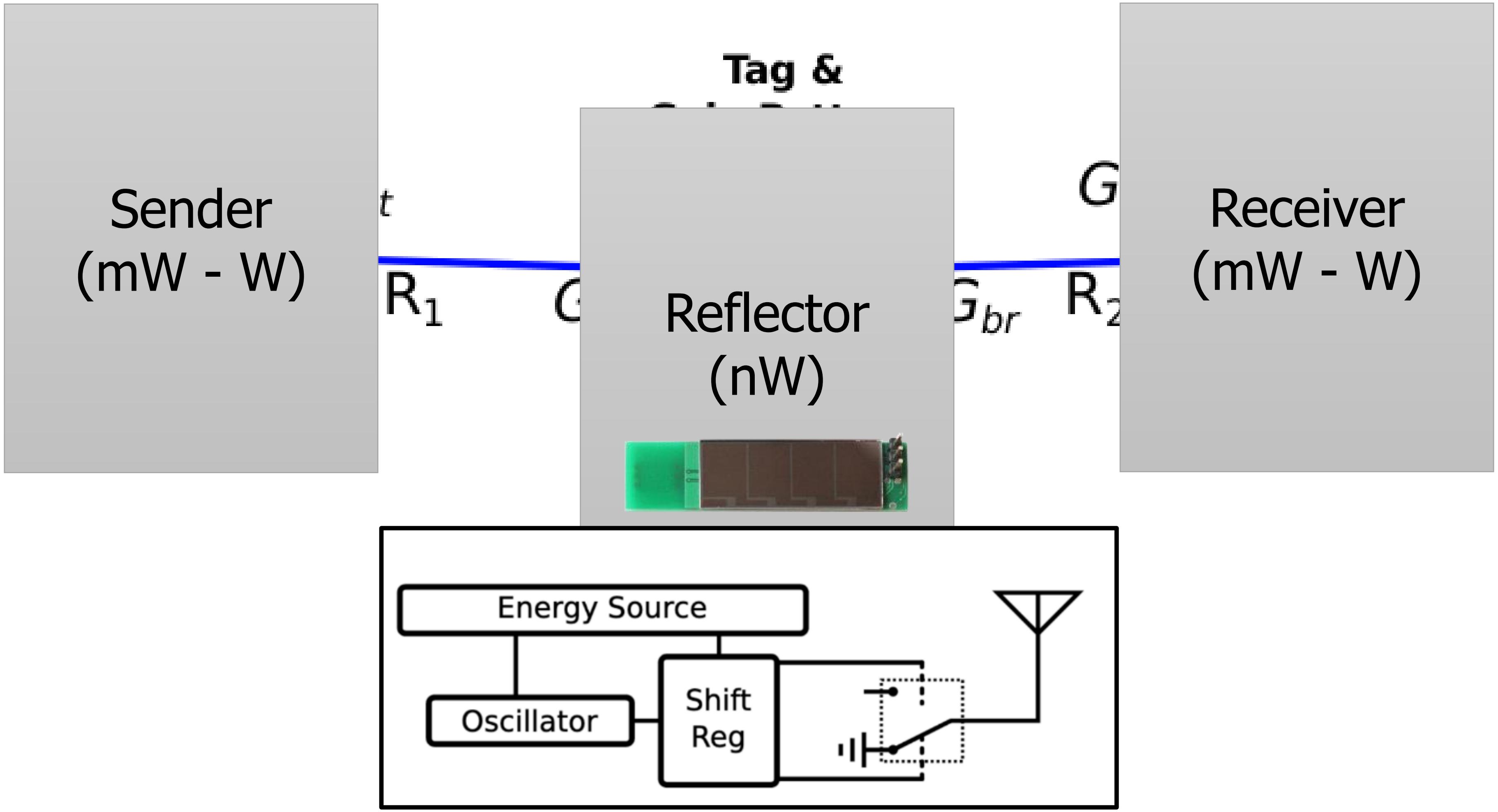
Reflections make time-of-flight estimation difficult and inaccurate



Ultra wideband can better disambiguate multipath and identify signal arrival time



Why RF, why ultra wideband, why backscatter for ubiquitous localization?

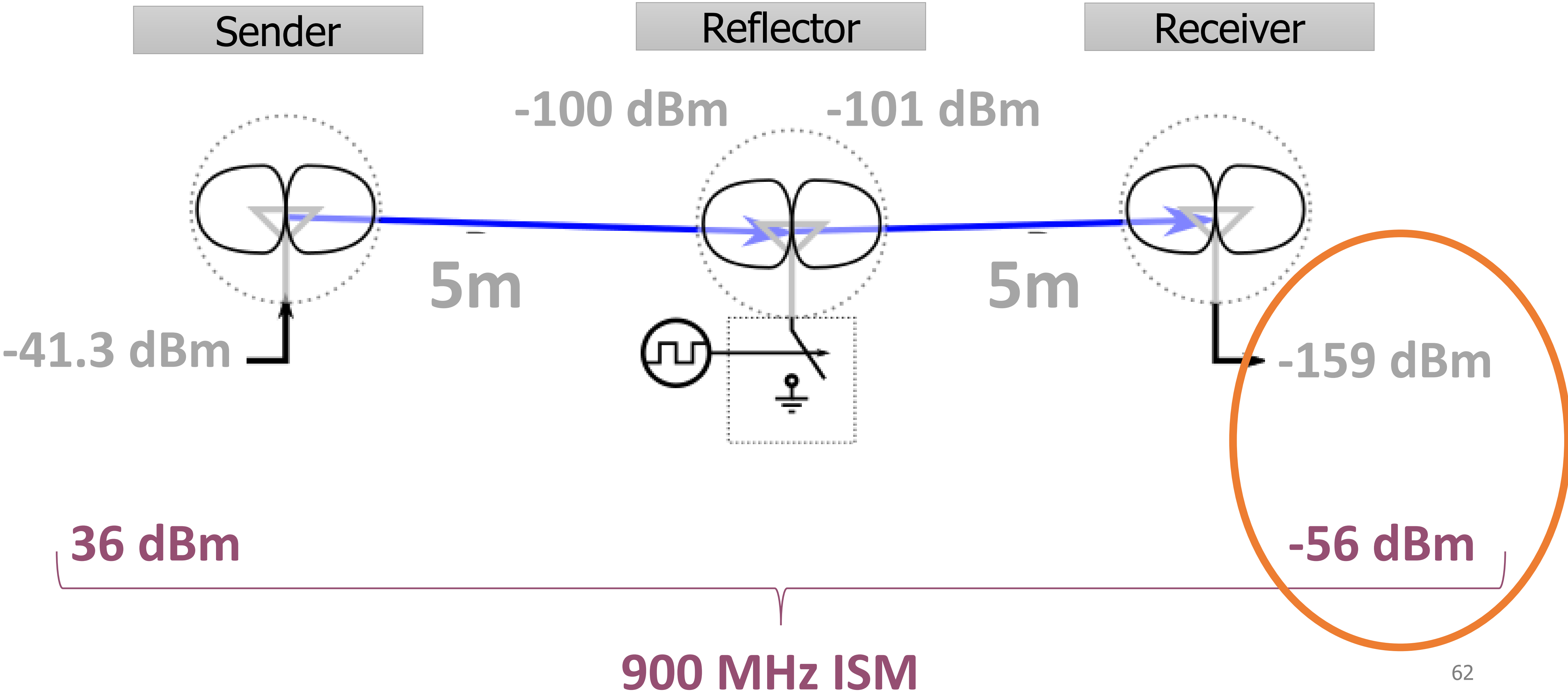


There is a new tradeoff to introduce to enable wide-area ultra-low power, high-quality localization

- Covers areas 30m+
  - “through walls”
- Decimeter accurate
- <1 µW tag
  - (COTS, can do order of magnitude or more better with VLSI)
- (Nearly) unlimited number of concurrent tags
- **Cost: 1-15+ minutes per location fix**
  - **A latency/energy tradeoff for localization**

Slocalization: Sub-µW Ultra Wideband Backscatter Localization
Pat Pannuto, Kempke, Benjamin, and Prabal Dutta
Proceedings of the 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN’18). **Best Paper Finalist.**

UWB Backscatter is passive reflection of a lot less energy than traditional communications



UWB Backscatter is passive reflection of a lot less energy

Packet Error Rate	Data Rate	Typical Receiver Sensitivity	Units
1%	110 kbps	-106	dBm/500 MHz
10%	110 kbps	-107	dBm/500 MHz
	11[illegible] kbps	-102	dBm/500 MHz
1%	850 kbps	-101	dBm/500 MHz
	6.8 Mbps	-93 (*-97)	dBm/500 MHz
10%	110 kbps	-106	dBm/500 MHz
	850 kbps	-102	dBm/500 MHz
	6.8 Mbps	-94 (*-98)	dBm/500 MHz

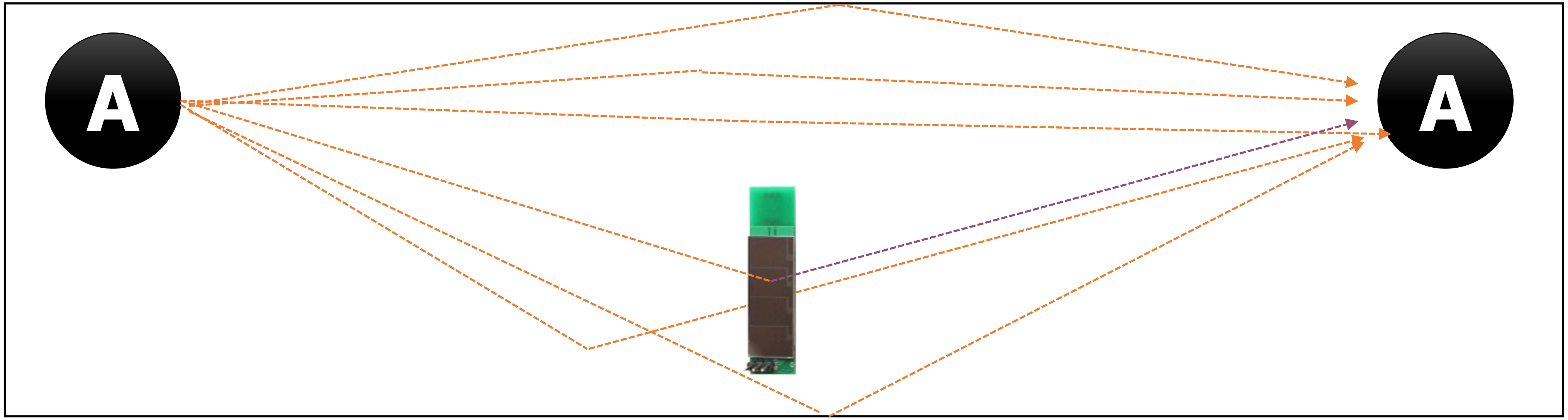
Typical receiver sensitivity ranges from -94 to -106

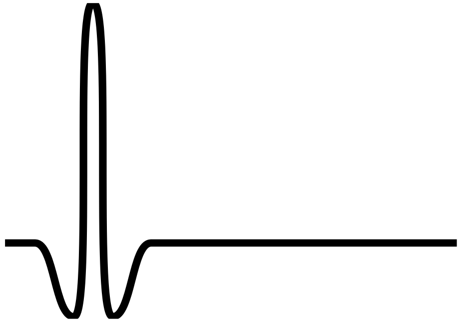
-159 dBm

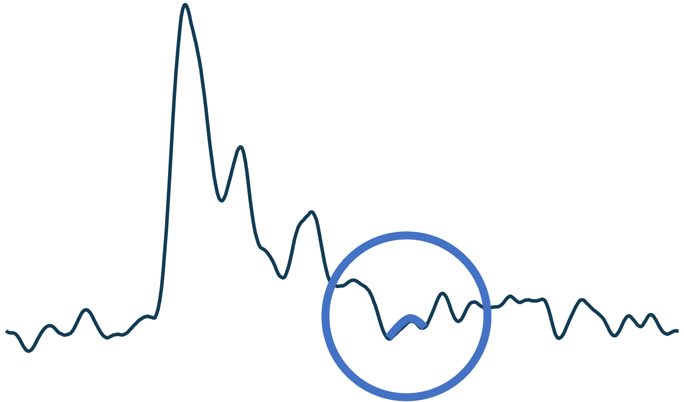
-56 dBm

How do we recover a signal that is way below the noise floor?

- Exploit tag stationarity and environmental stability

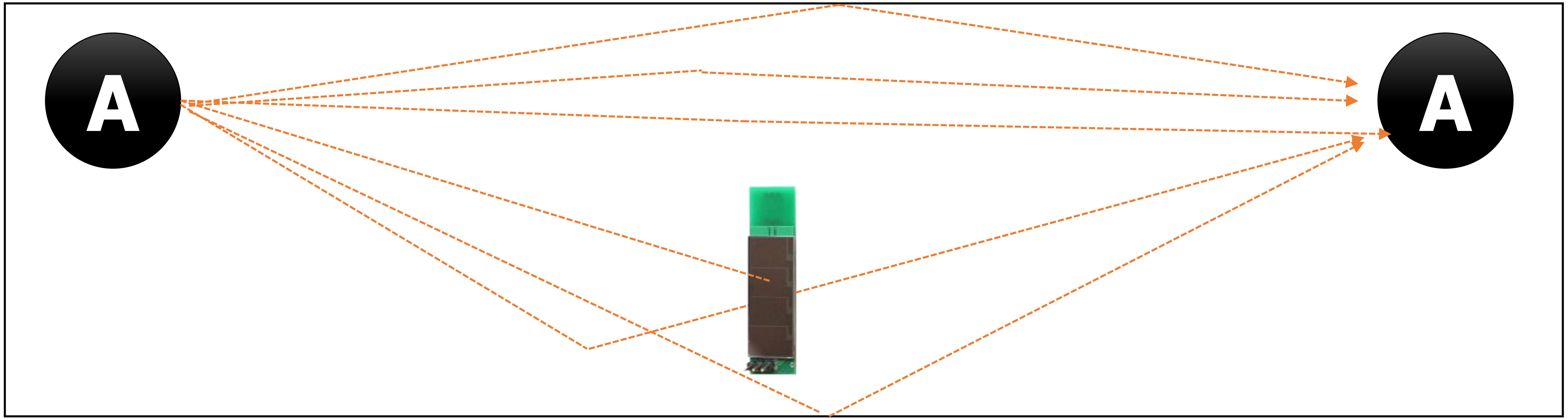


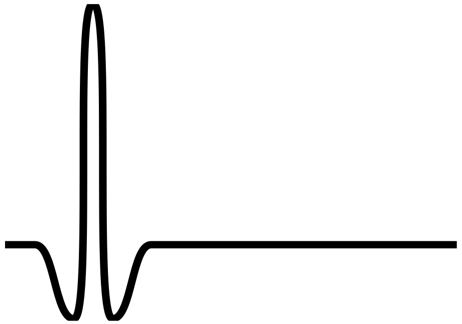


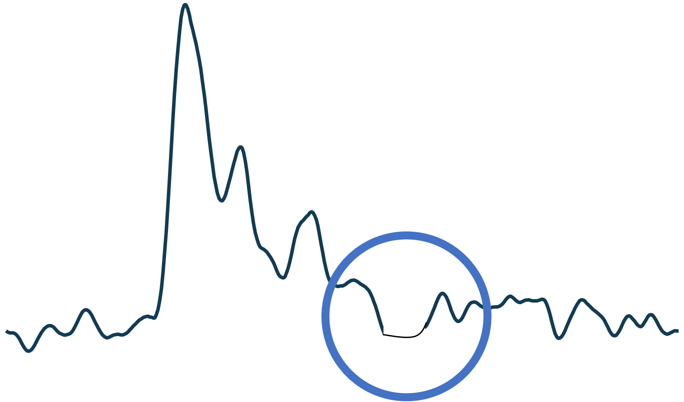


How do we recover a signal that is way below the noise floor?

- Exploit tag stationarity and environmental stability

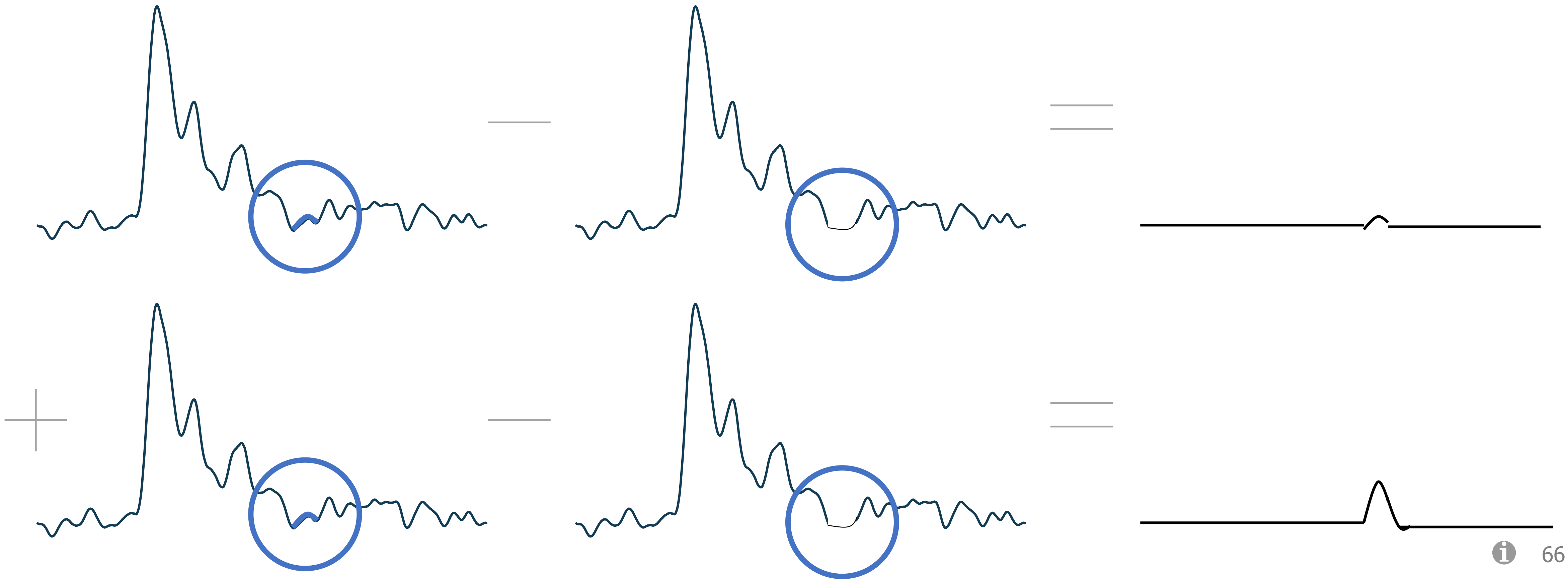




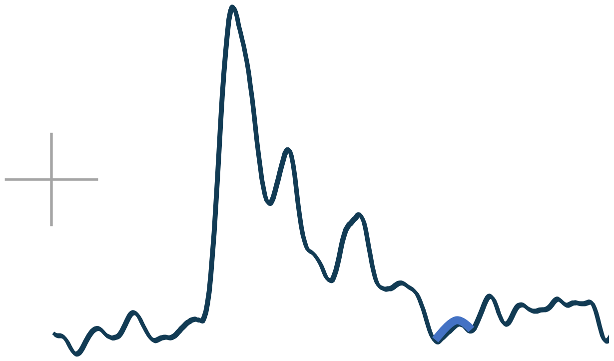


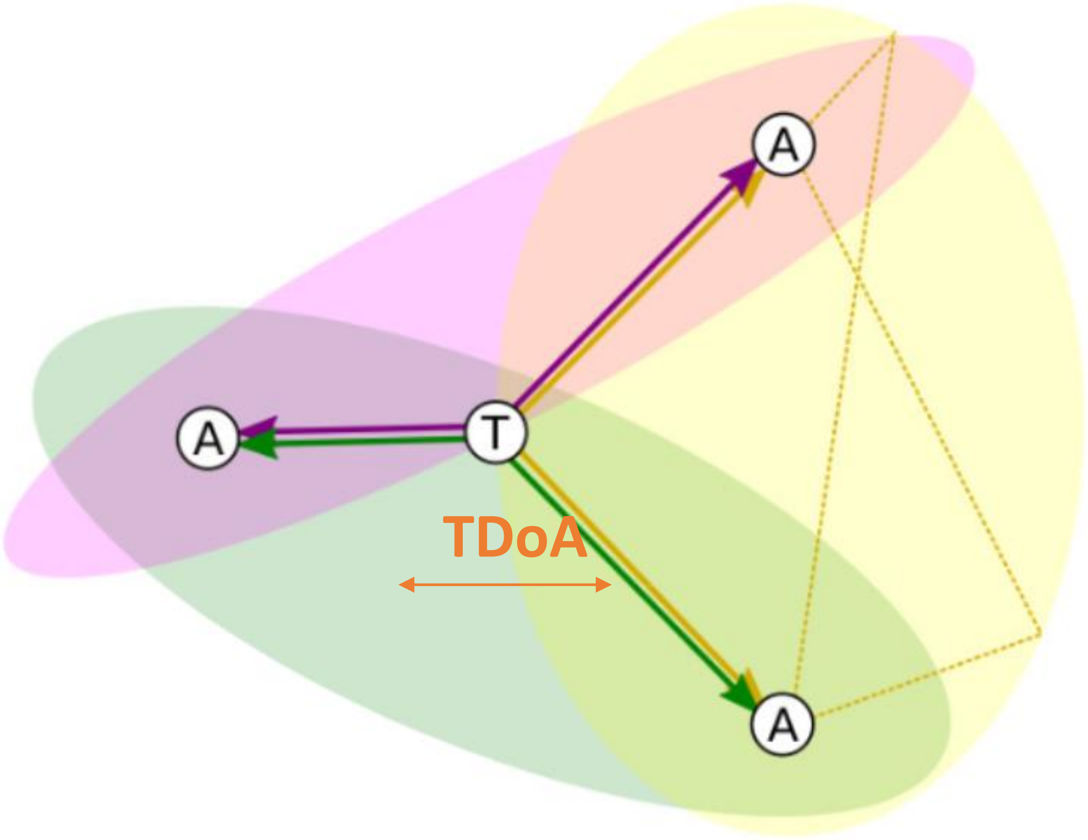
Ideally, the only change in the channel impulse response is the tag reflection

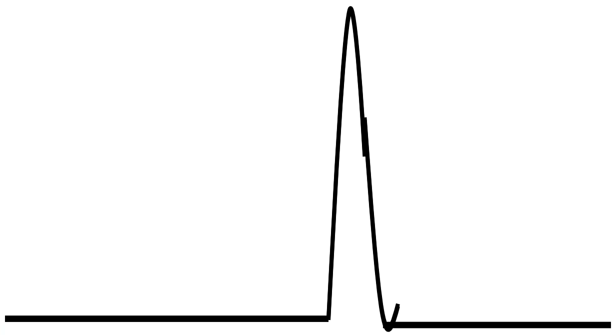
- Subtracting the environment finds the tag



The goal is to estimate the time difference of arrival (TDoA) and trilaterate



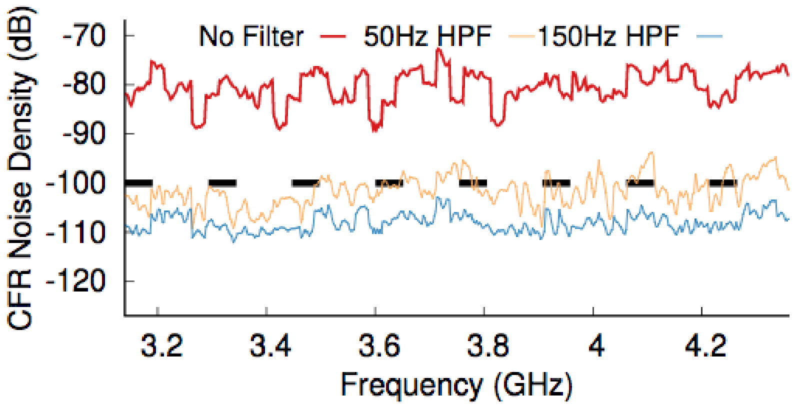




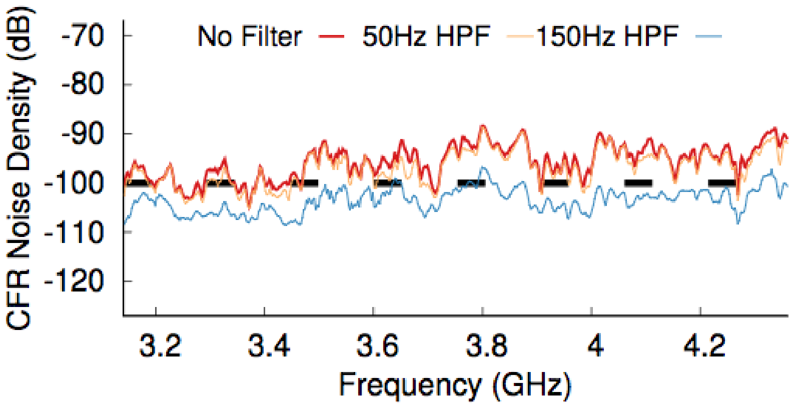
- First peak is anchor—anchor path, then anchor—tag—anchor

Extracting the tag signal in the real world has a few additional challenges

- The environment is not actually static
  - But noise is largely white & Gaussian
  - And we can filter out the rest (sets floor for tag frequency, active power)



(b) CFR Noise Walking

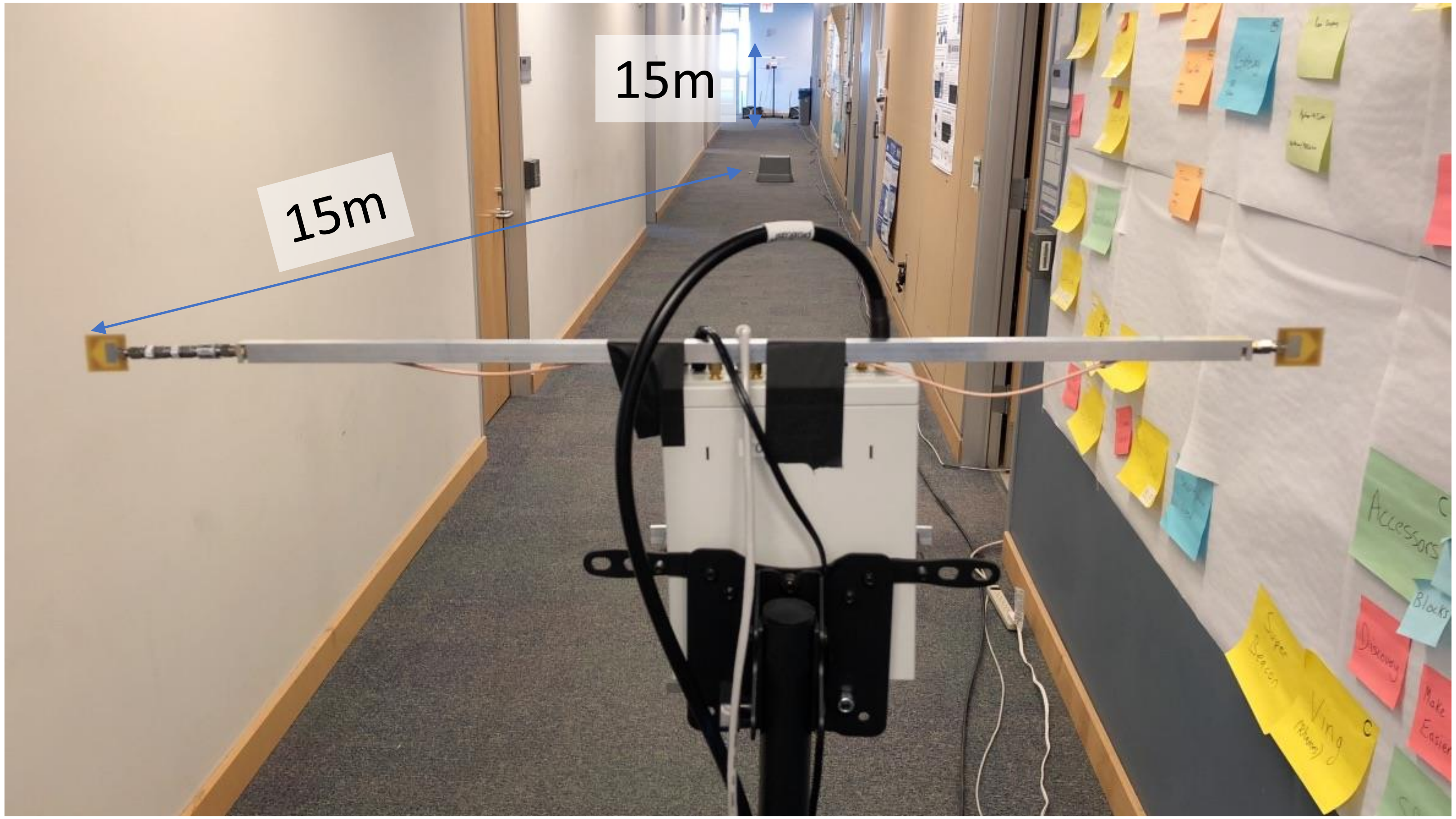


(c) CFR Noise Fluorescents

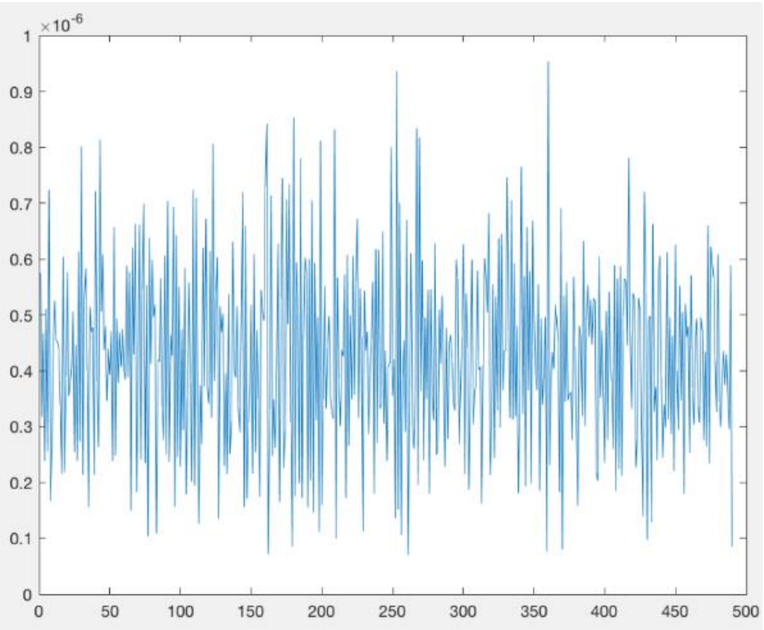
- Finding tag phase offset currently requires brute force search

Does it really work?

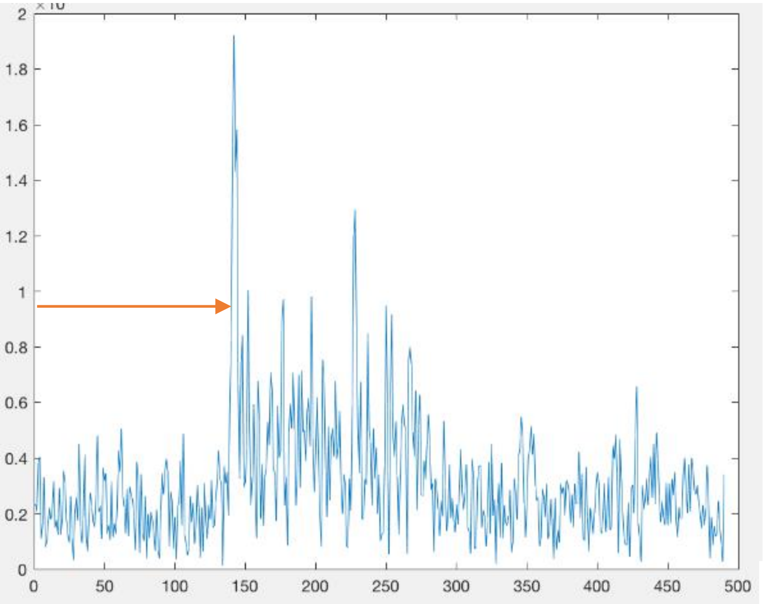
- 15 minutes can cover 30 meters
- 30 cm average error (3D Euclidean distance)



After a few seconds



After a few minutes



Outline

- Backscatter
- Backscatter Uses
  - RFID
  - NFC
  - Sensors (Backscatter LoRa)
  - Localization
- **Wakeup Radios**

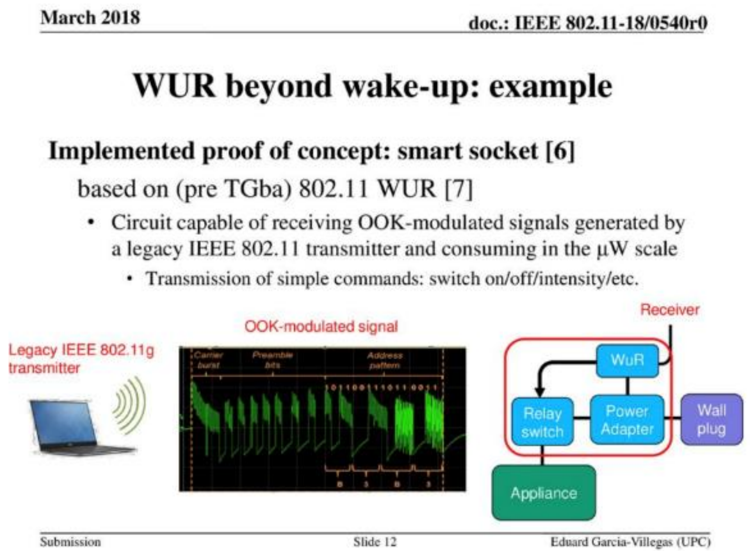
Wakeup radios are another form of "RF-lite"

- How do you make a radio really low power?
  - Turn it off
- Problem: how do you know when to turn the radio on?
- Idea: can we design a simpler radio where the only purpose is determining whether a signal exists or not?

Concept: Can we design something (much?) lower power that can't do general purpose data, but can signal wakeup?

- Energy detectors
  - Simple, but prone to false wakeups

- Extremely simple signaling?
  - Very often some form of on-off-keying (OOK)
  - Seeing new life
    - In mainstream networks, e.g. 802.11ba
    - In sensor network research, e.g. Zippy
    - Tuned energy harvesting frontends
    - Manipulated standards for lower-BW signals



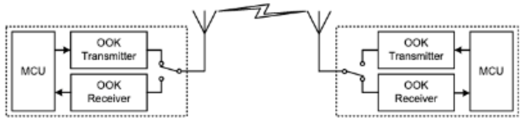
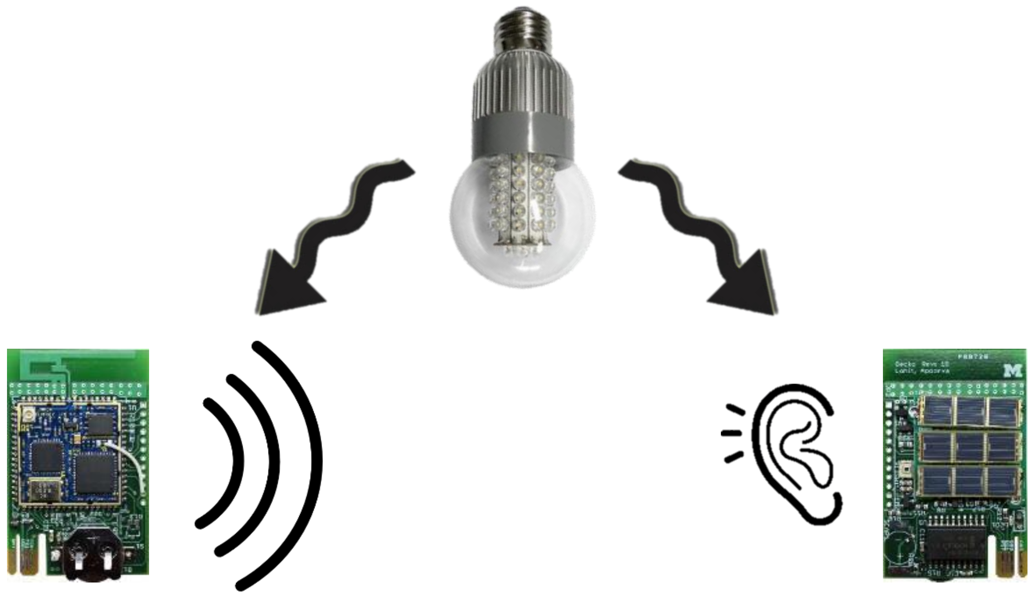


Figure 1: Proposed mote architecture with a micro-controller (MCU), OOK transmitter, and always-on ultra-low power OOK receiver.

Figure 2: Example OOK signal at the input to the receiver and its corresponding demodulated output.

(Re)-emerging new ideas in wakeup design

- Decoupling synchronization from communication
- External synchronization sources?
  - Ambient 60 Hz wave
  - Sudden change in room lighting, or a noise



- Synchronization and time-keeping burden is shifted to infrastructure

Outline

- Backscatter
- Backscatter Uses
  - RFID
  - NFC
  - Sensors (Backscatter LoRa)
  - Localization
- Wakeup Radios

Class Summary

- Network Fundamentals
- Bluetooth Low Energy
  - Advertisements, Connections
- 802.15.4
  - Thread, Zigbee, Mesh Routing
- WiFi
- Cellular
- LPWANs
  - LoRaWAN, Sigfox, Research and Challenges
- Other
  - Localization, Satellite Communication, Backscatter