

# Lecture 17

# Backscatter & RFID

CS397/497 – Wireless Protocols for IoT  
Branden Gena – Winter 2023

Some slides borrowed from Ambuj Varshney Uppsala / UC Berkeley

Materials in collaboration  
with Pat Pannuto (UCSD)

# Administrivia

- Hw: Cellular
  - Due tonight
- Lab: LoRa
  - Next week Friday
- Final Design Project
  - Should be released tonight, maybe tomorrow
  - Formal design review of an application
    - Consider energy, costs, etc.
  - Writeup due Wednesday of exam week

# Today's Goals

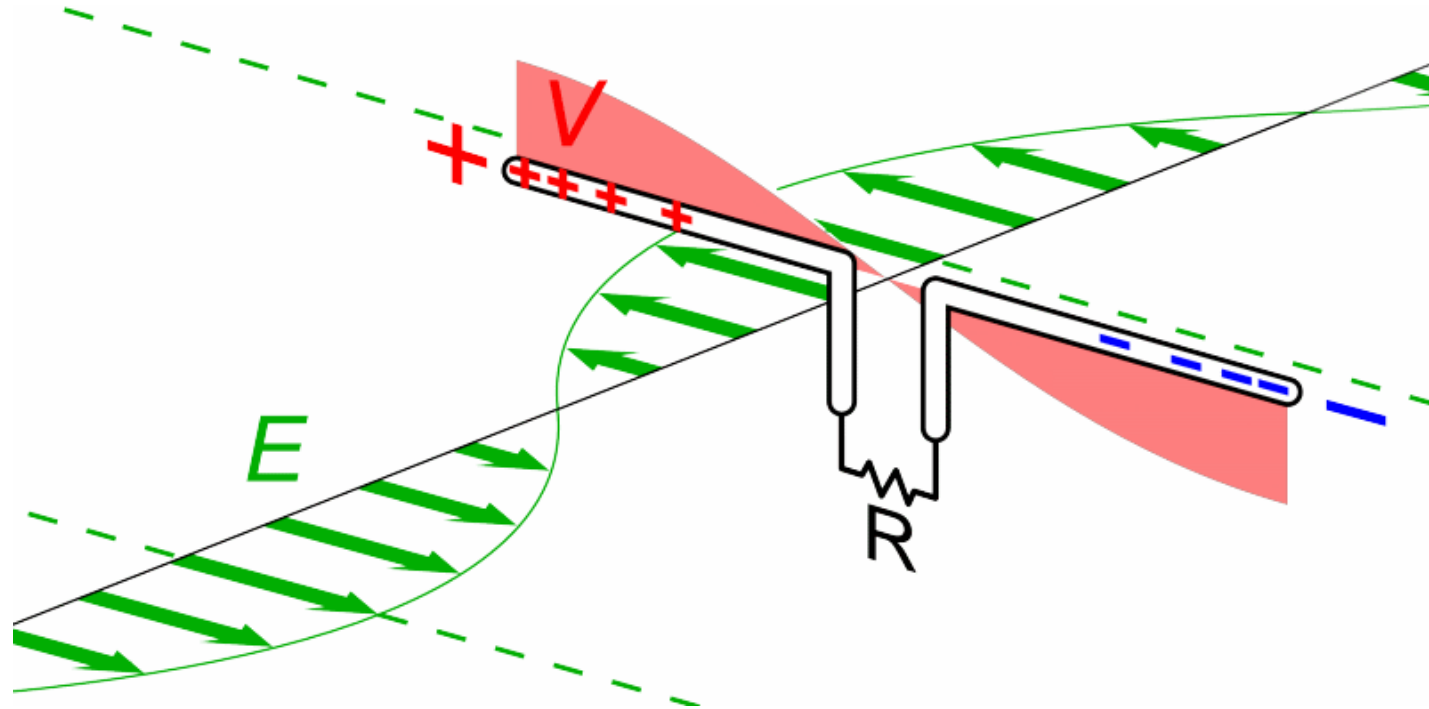
- Describe backscatter communications
- Understand one use of backscatter: RFID
- Explore how backscatter techniques can be used for applications
  - Sensor networks
  - Localization

# Outline

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

# What does an antenna *do*?

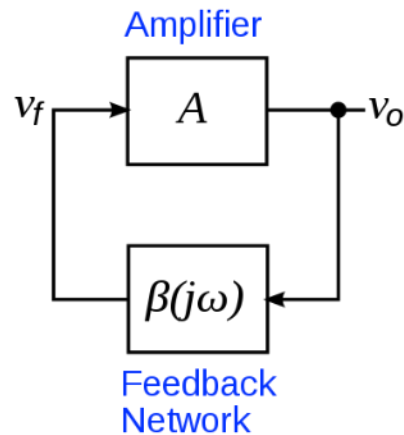
- Loosely: Converts between electric and magnetic waves



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

# What generates electric waves?

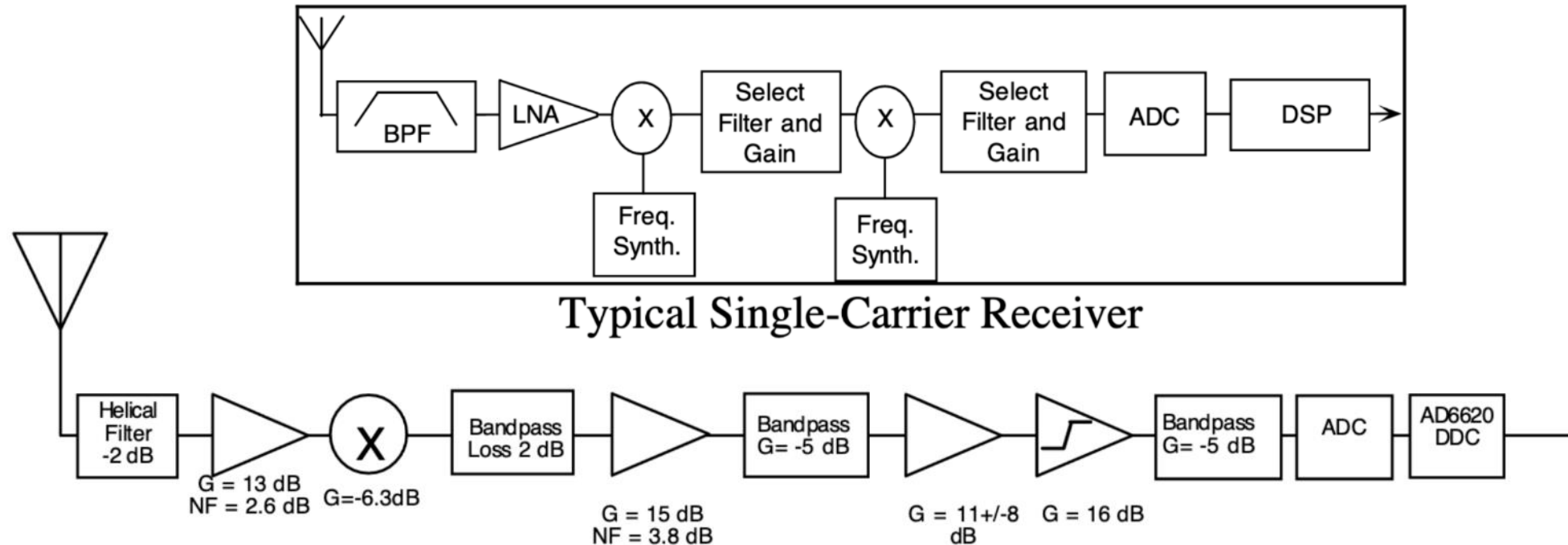
- Lots of stuff nowadays...
- Most commonly a frequency-selective resonator into an amplifier
  - i.e.



- Also 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:



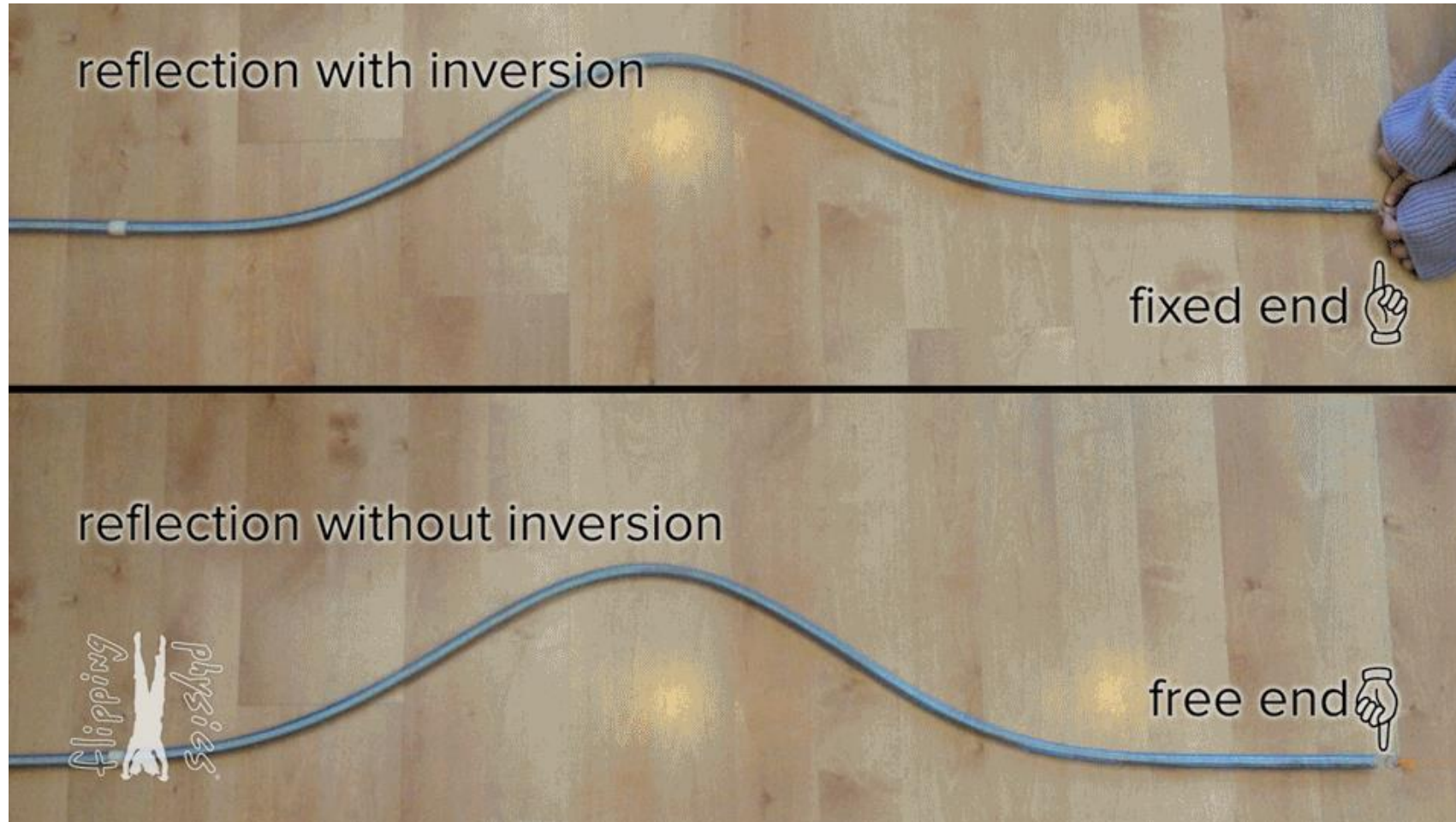
Graphics from Analog Devices whitepaper: <https://www.analog.com/media/en/technical-documentation/tech-articles/480501640radio101.pdf> — significantly more detail here

# 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
  - 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

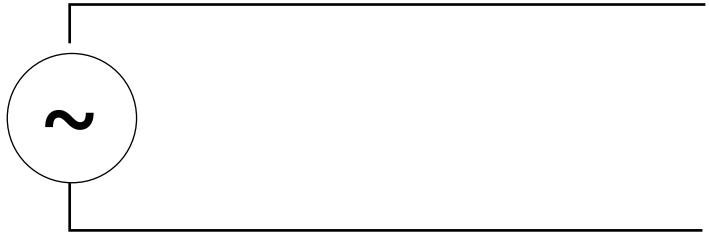


# What happens if nothing 'receives' the wave?

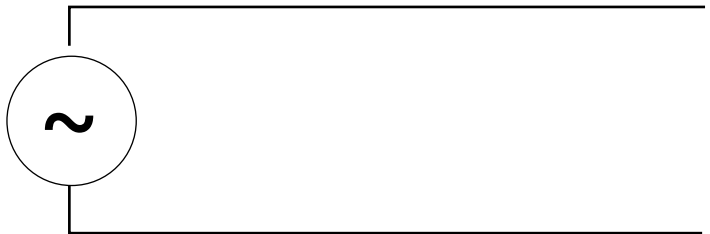


From: <https://www.flippingphysics.com/standing-waves.html>

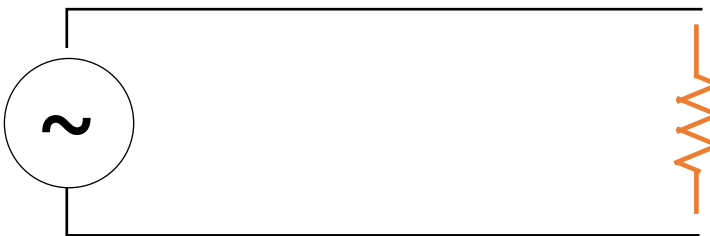
# "Fixed end" and "Free end" in electronic transmission



Short Circuit = "Free End"  
- Reflects wave



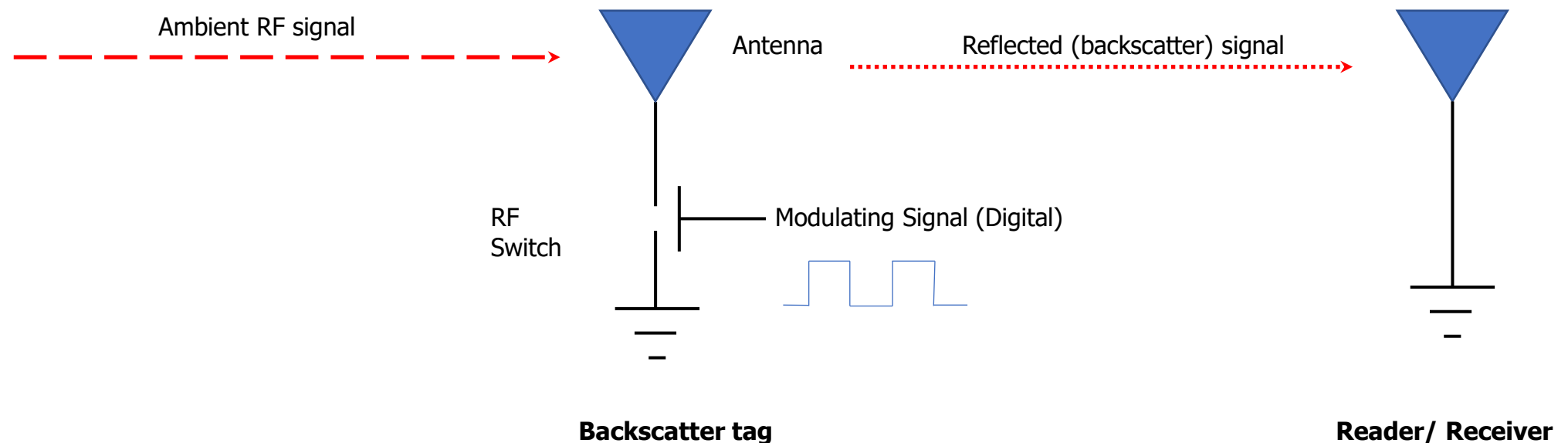
Open Circuit = "Fixed End"  
- Inverts wave



Matched Load  
- Absorbs wave (no reflection)

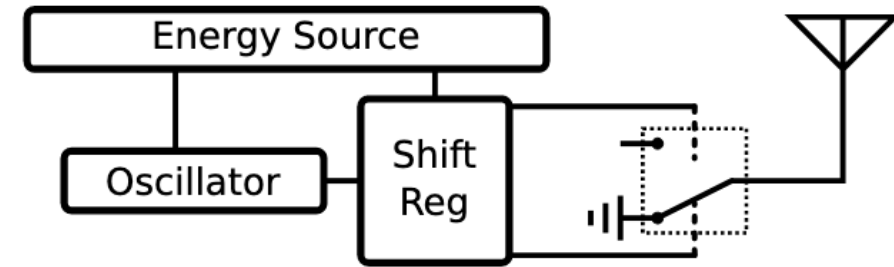
# Backscatter theory of operation

- 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)

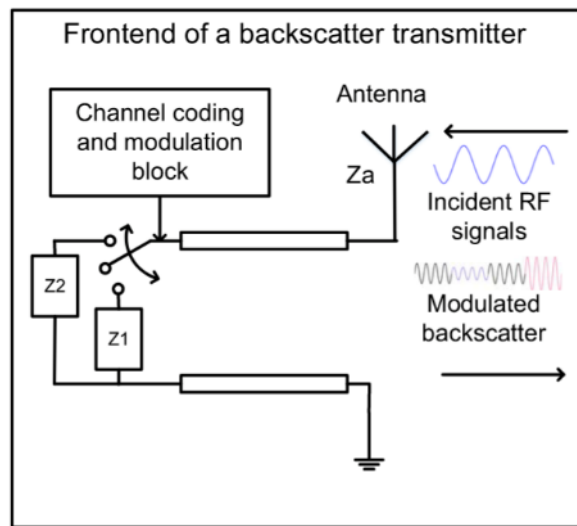


# Backscatter radio designs

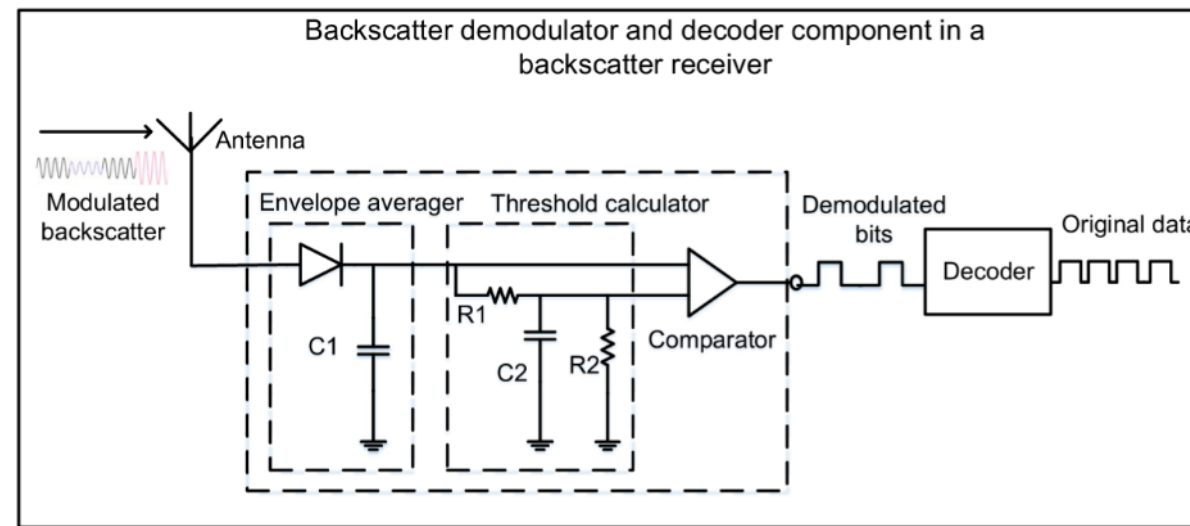
- Simple versions just 'reflect or don't reflect'



- Modern designs can do more advanced modulation as well



(a)



(b)

# Break + Spycraft

- How would you use backscatter plus a microphone to secretly record someone?

# Break + Spycraft

- How would you use backscatter plus a microphone to secretly record someone?
  - Use microphone to change if antenna is grounded or not
  - Transmit power at the backscatter tag and collect microphone data from the response

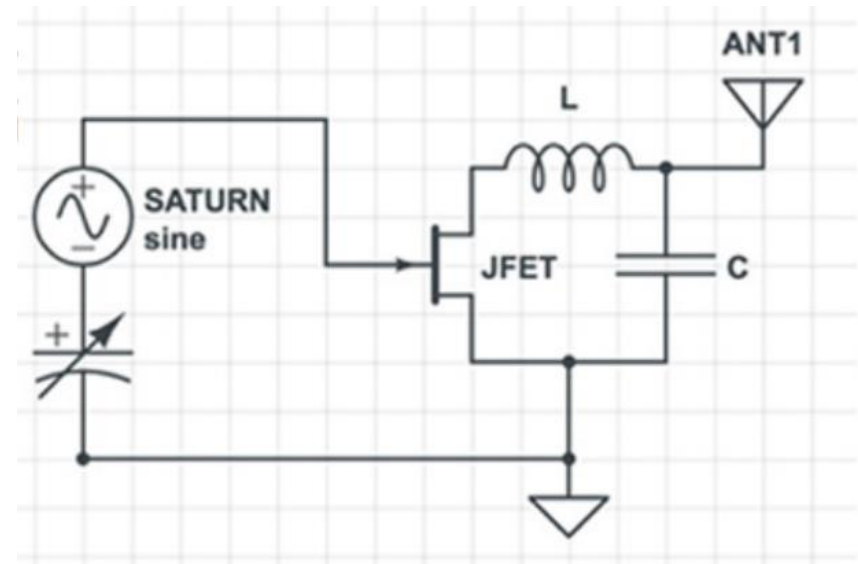
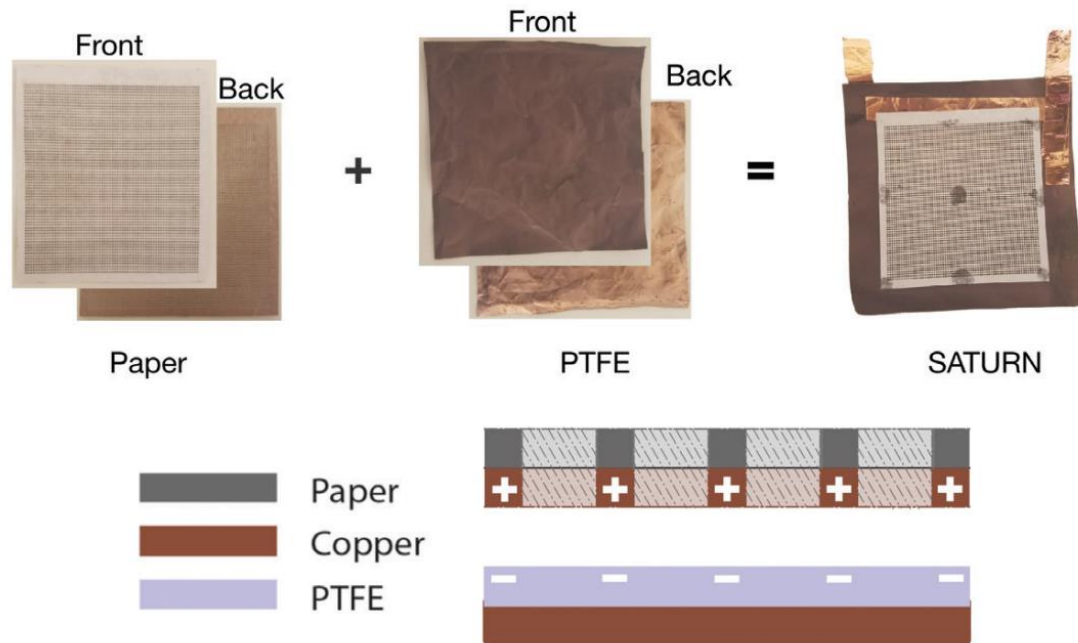
# Backscatter is an *old* idea — history in spycraft!

- 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



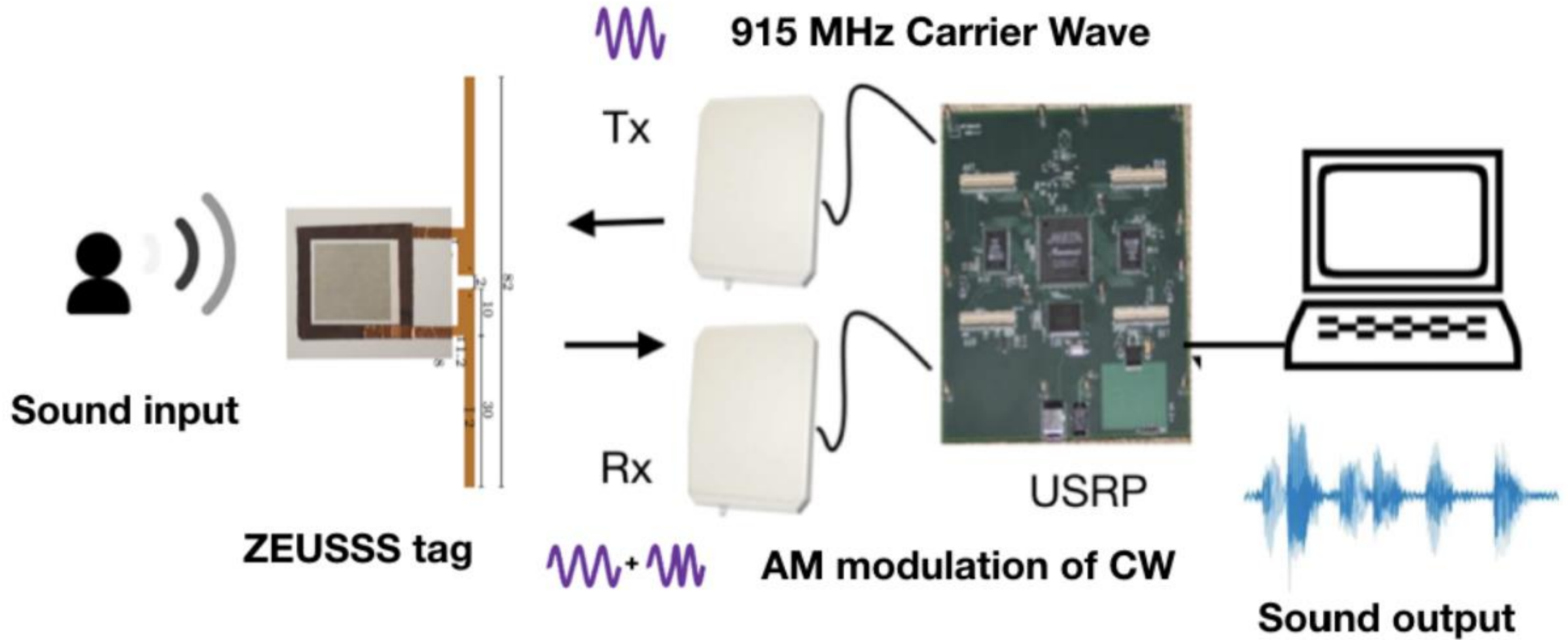
# Simple sensors can trigger backscatter

- 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 (PhD student at Georgia Tech)



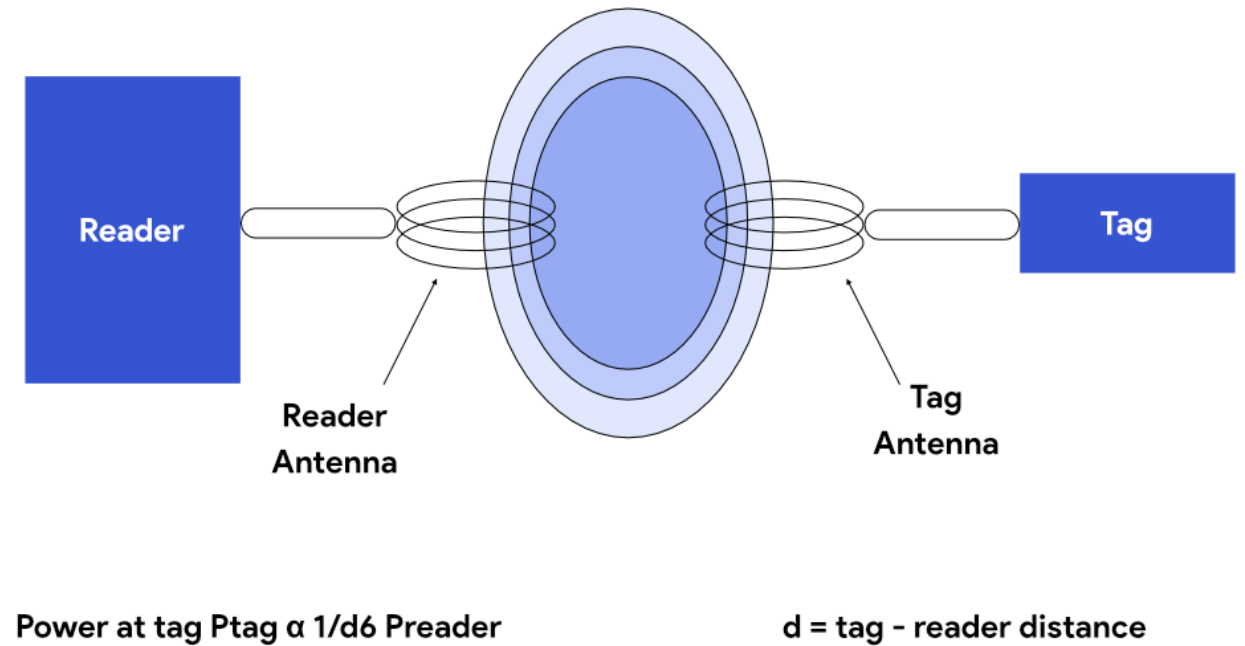


# Complete transmission path for SATURN audio



# Alternative: 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



# Outline

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

# RFID is *everywhere* nowadays

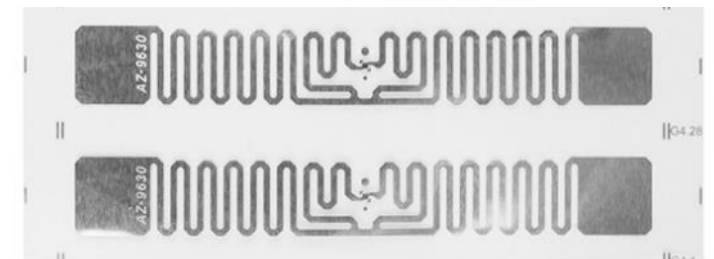
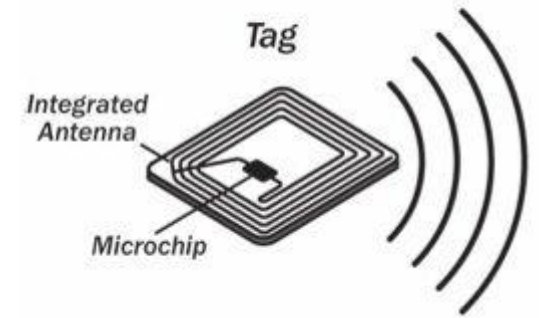
- Fundamental design principle is *asymmetry*
  - Extremely simple, cheap tags
  - Complex readers



**New Sticker Toll Transponders**

# 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

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

- Low Frequency ( $\sim 300$  kHz) — mostly legacy
  - $\sim 10$ cm read range (inductive coupling)
- High Frequency (3 $\sim$ 30 MHz; often 13.56 MHz)
  - Passive: 4 $\sim$ 7 m max (usually inductive coupling, I think)
  - Semi-Passive: 10 $\sim$ 30 m max
  - Active: 30+ m
- Ultra-High Frequency (300 MHz  $\sim$  3 GHz)
  - Passive: Up to 12 m (backscatter)
  - Active: Up to 100 m

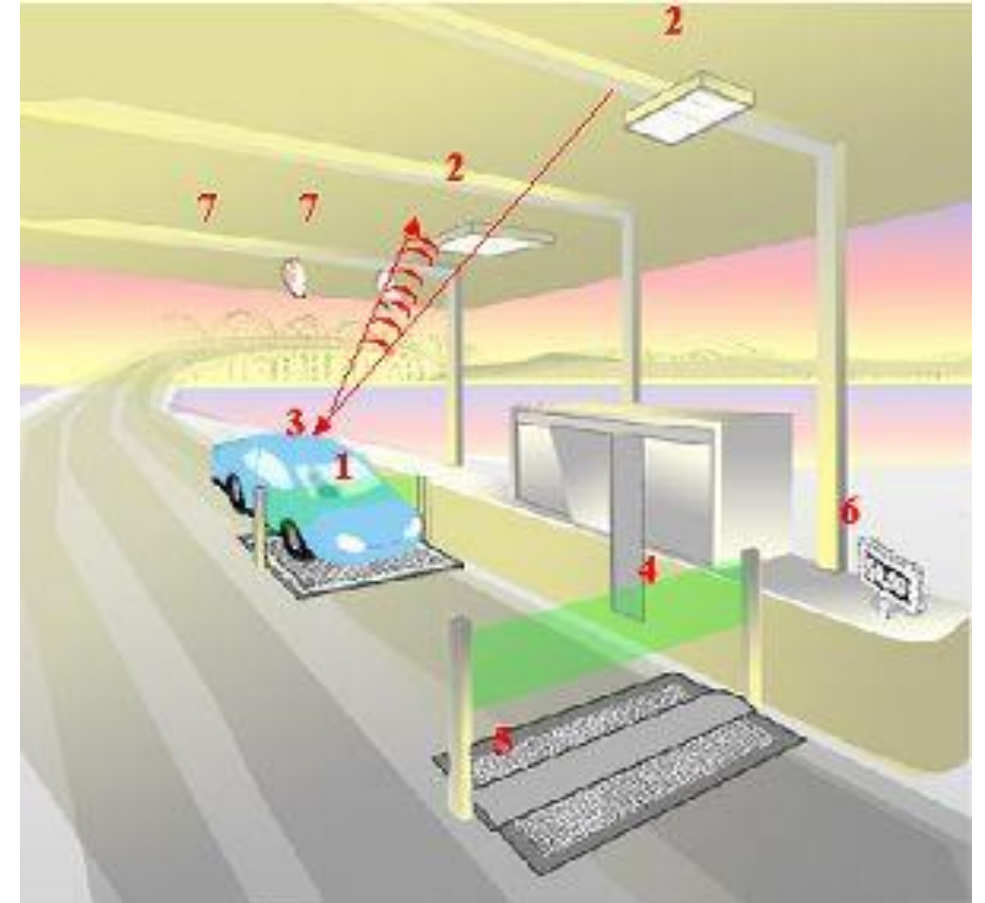
# RFID challenges

- 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 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

<b>Header</b>	<b>EPC Manager</b>	<b>Object Class</b>	<b>Serial Number</b>
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

# Near Field Communication (NFC)

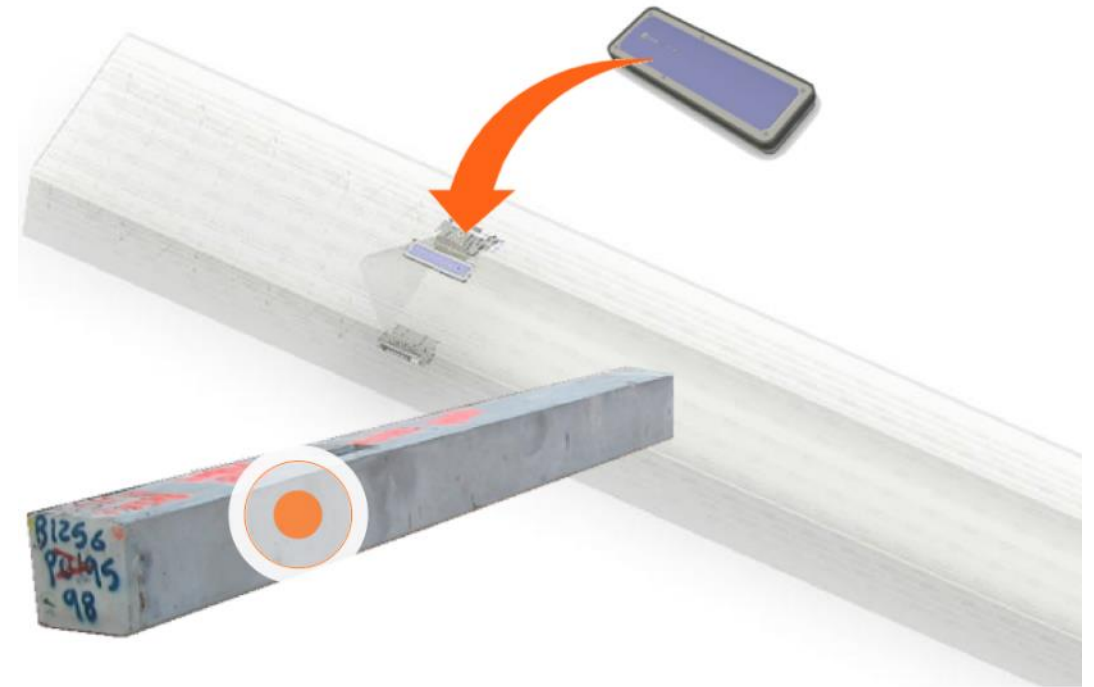
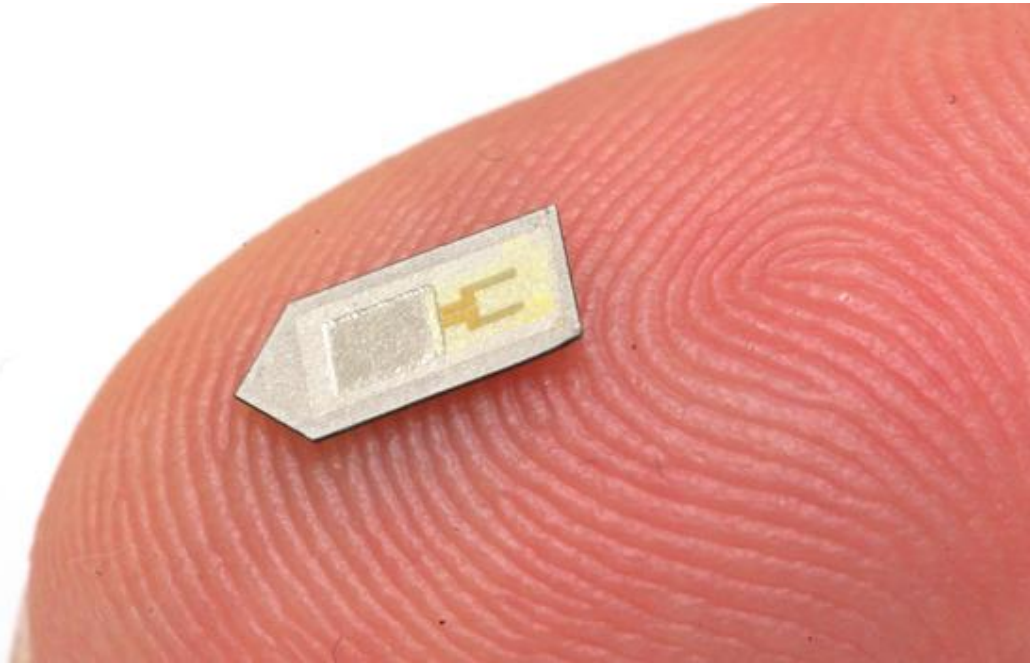
- Inductive Coupling concept (13.56 MHz)
  - But attached to a powered and capable device (smartphone)
  - 10-20 cm range max (usually <10)
- Can act as a tag or as a reader
  - Allows smartphone to power a tag if needed
  - Alternatively, smartphone could act like a card and respond to a reader
  - Two smartphones can communicate without power transfer
- Data rate 100-400 kbps!
  - nRF52840 capable of 100 kbps communication with attached antenna

# Outline

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

# “Embedded” sensors

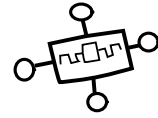
- How do you change batteries in a device that’s inside a wall or inside someone’s body?



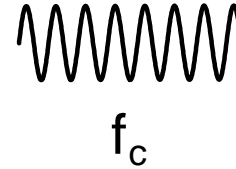


# Backscatter for sensor networks

Conventional  
Radio



Conventional  
Transceiver



$f_c$

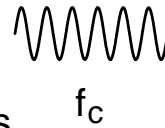


Receiver

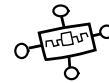
Backscatter  
Transmissions



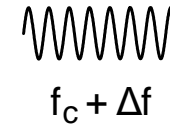
Ambient Wireless  
Signal Source



$f_c$



Backscatter Tag



$f_c + \Delta f$

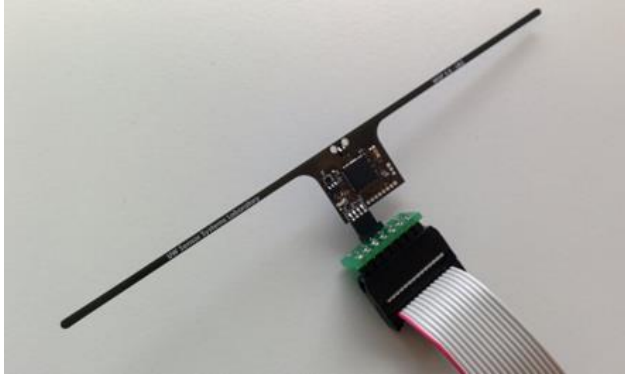


Receiver

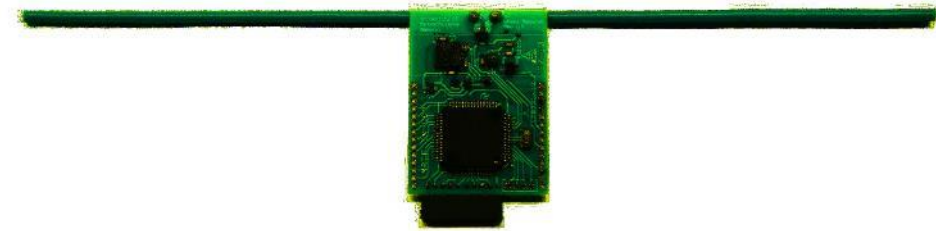
- Backscatter allows transmissions at up to 10000x lower power than conventional radios
  - Makes it very attractive for low-energy sensing devices

# RFID sensors

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



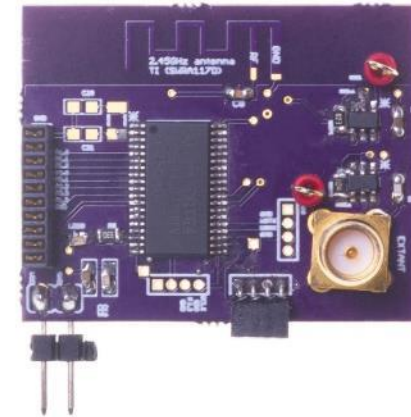
WISP 5.0  
University of Washington



Moo 1.0  
University of  
Massachusetts

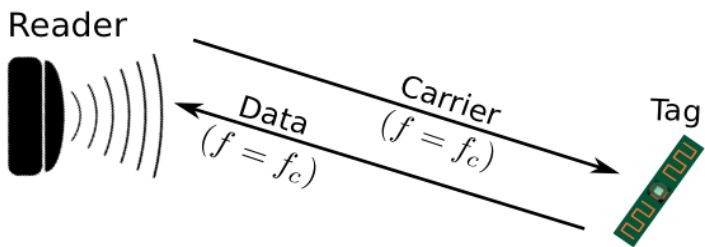
# Backscatter + LPWAN = usable?

- 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  $\mu\text{W}$ 
  - (Next few slides stolen from Ambuj's talks)

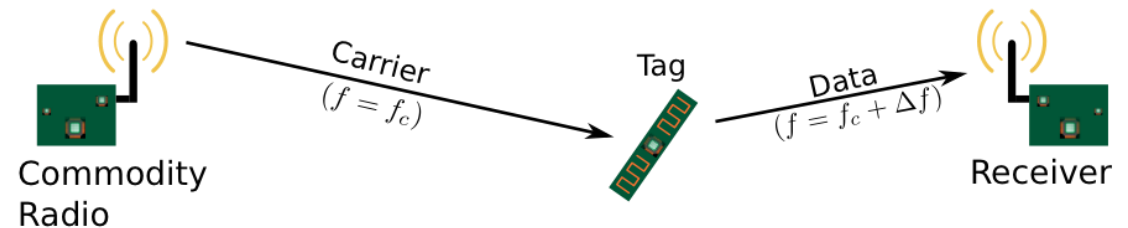


# Design element #1: LoRea decouples the carrier signal generation and reception

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



Monostatic configuration



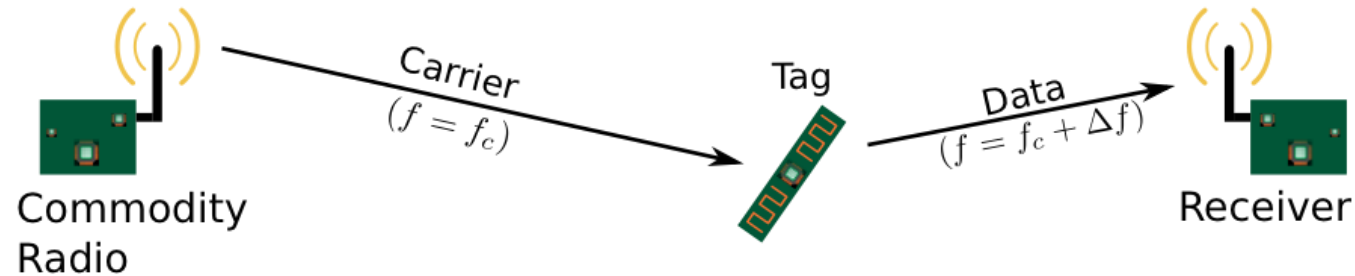
Bi-static configuration

- 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**

# 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

# LoRea outperforms state-of-the-art systems

System name	Communication range
<b>LoRea – 868 MHz (SENSYS 2017)</b>	<b>3400 m</b>
<b>LoRea – 2.4 GHz (SENSYS 2017)</b>	<b>225 m</b>
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

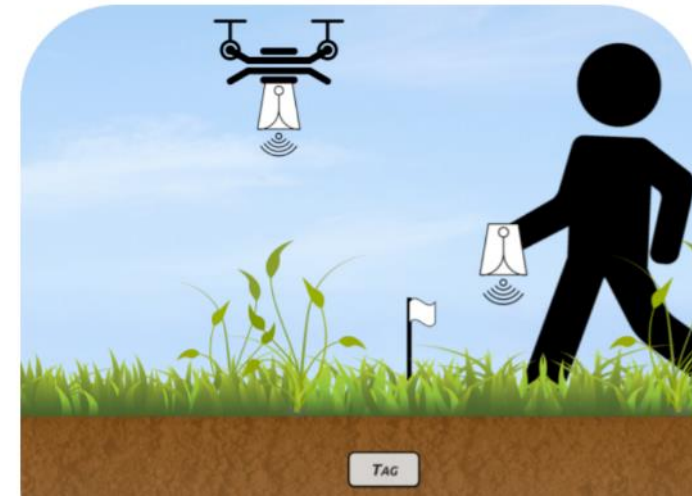
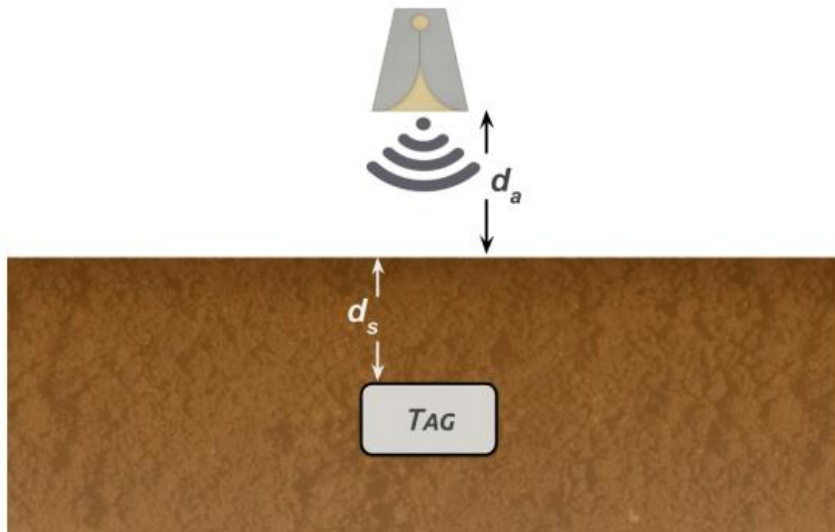
# Future research directions for backscatter sensor communication

- 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



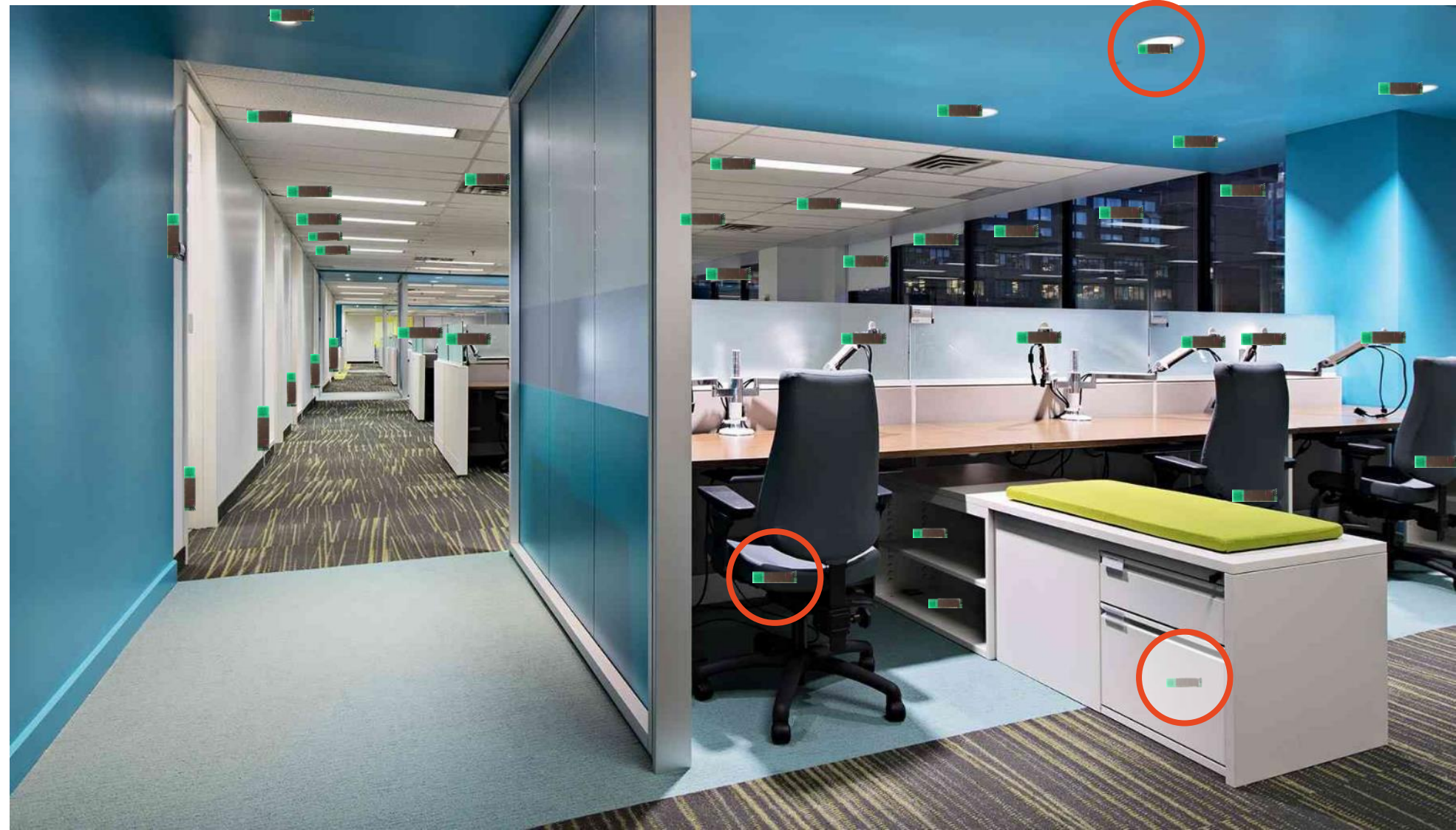
# Break + Open Question

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

# Outline

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

# Slocalization: Ultra wideband backscatter localization

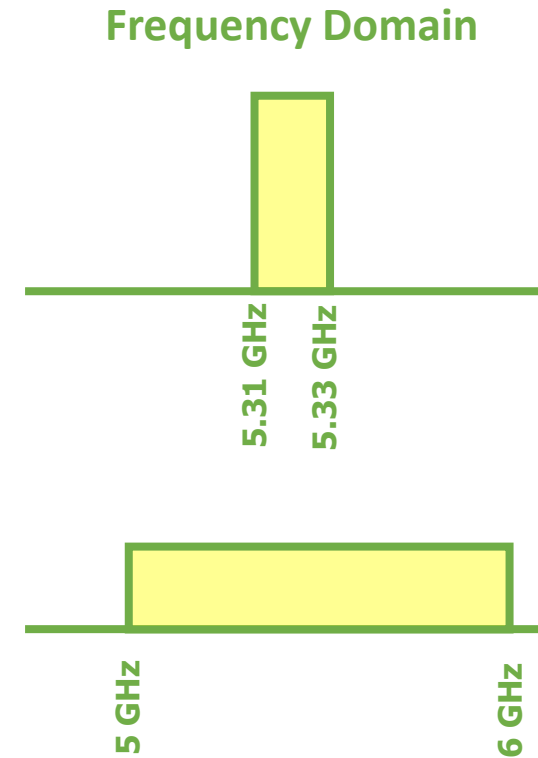
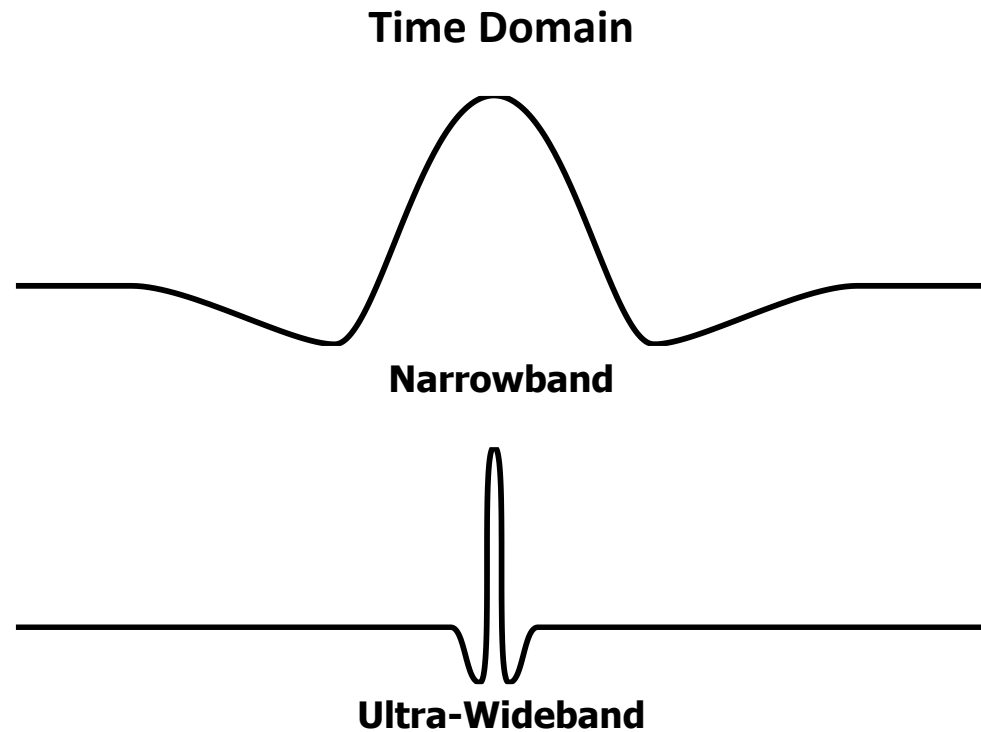


# Why RF, why ultra wideband, why backscatter for ubiquitous localization?

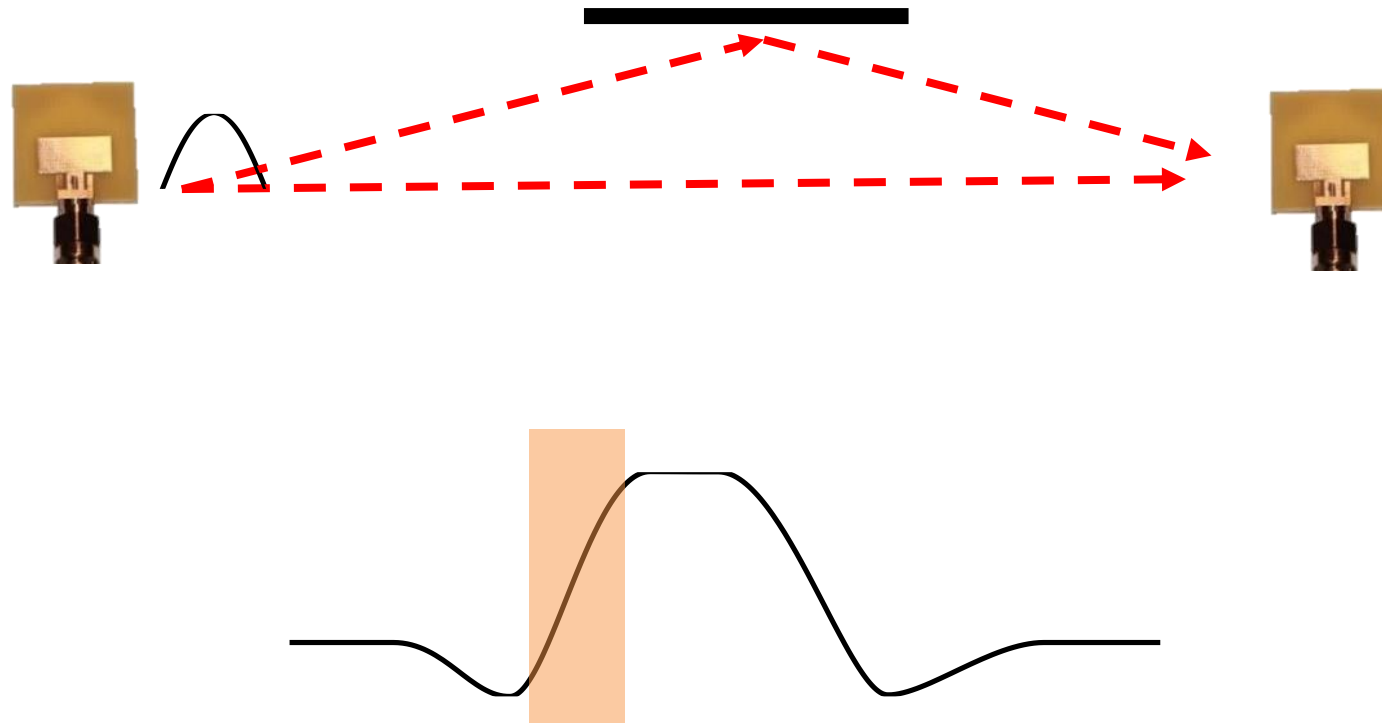


Mautz, Rainer. "Indoor positioning technologies." (2012).

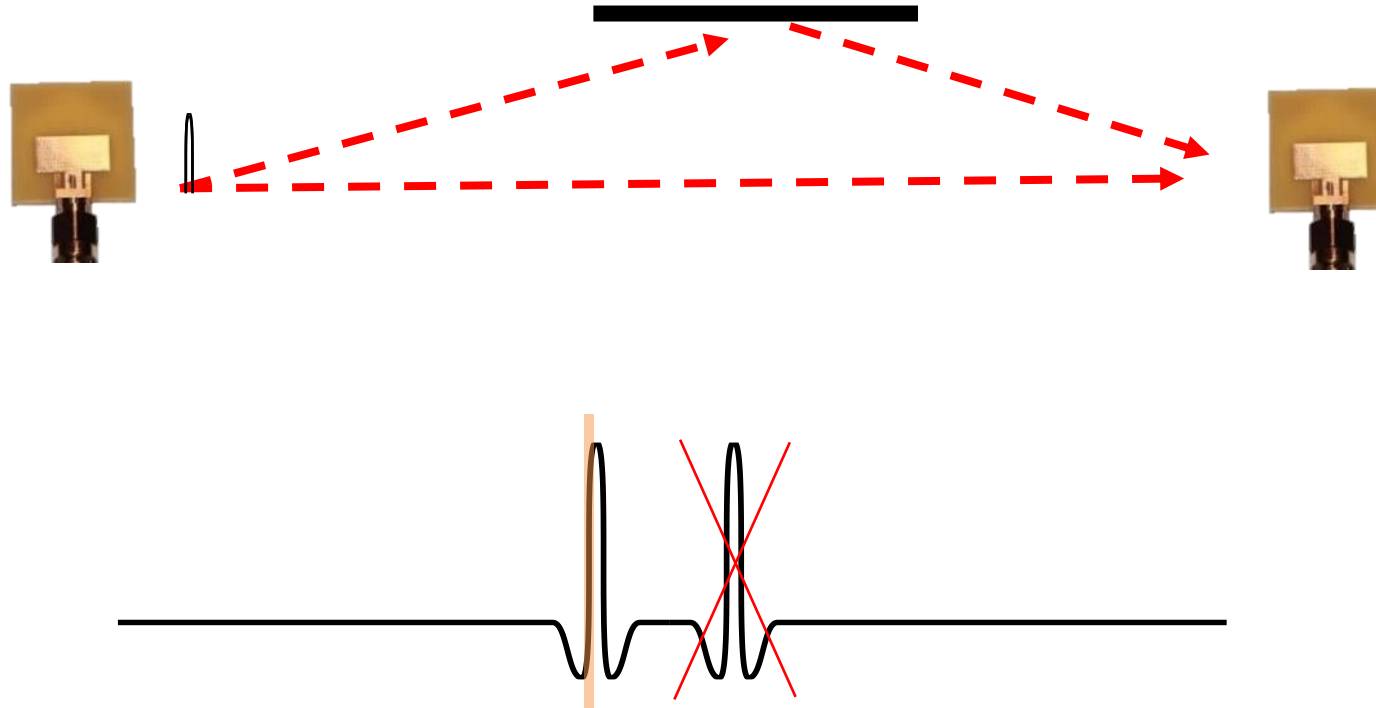
# Why RF, why ultra wideband, why backscatter for ubiquitous localization?



# Reflections make time-of-flight estimation difficult and inaccurate

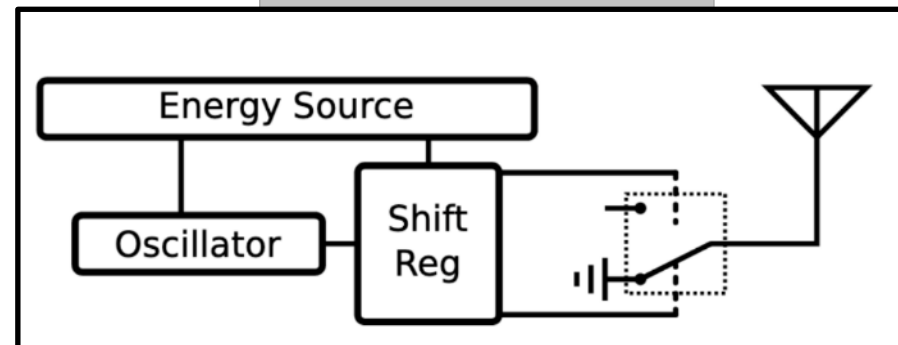
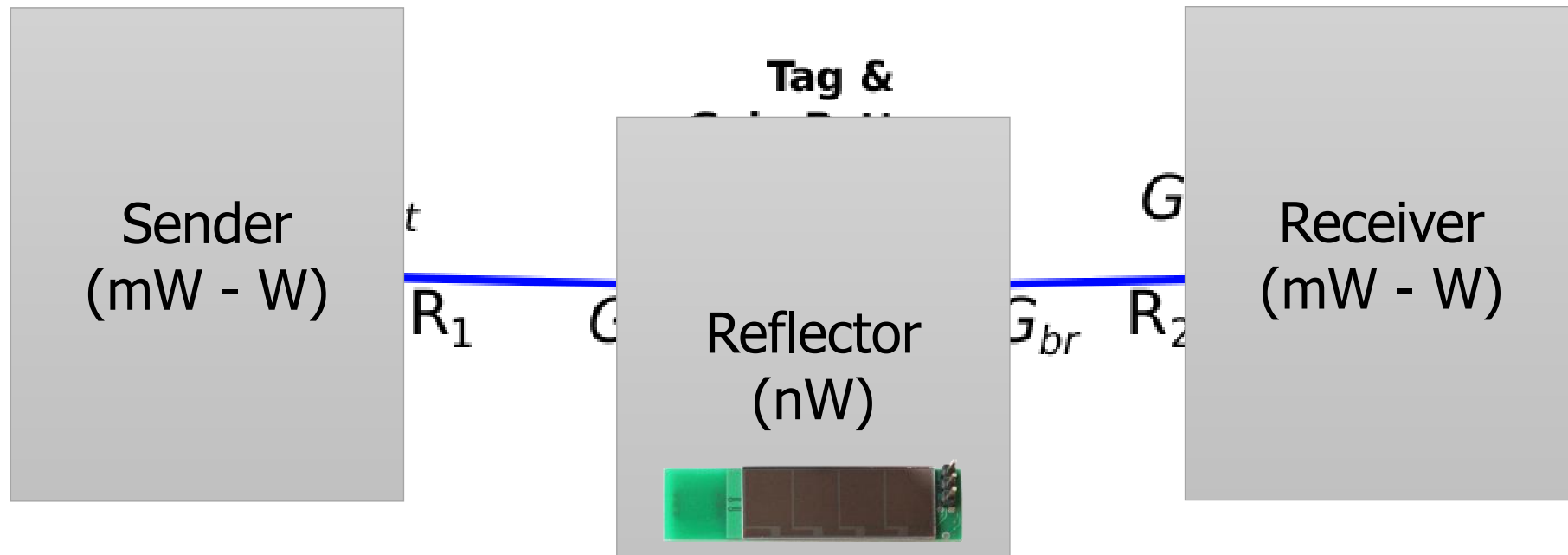


Ultra wideband can better disambiguate multipath and identify signal arrival time





# 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



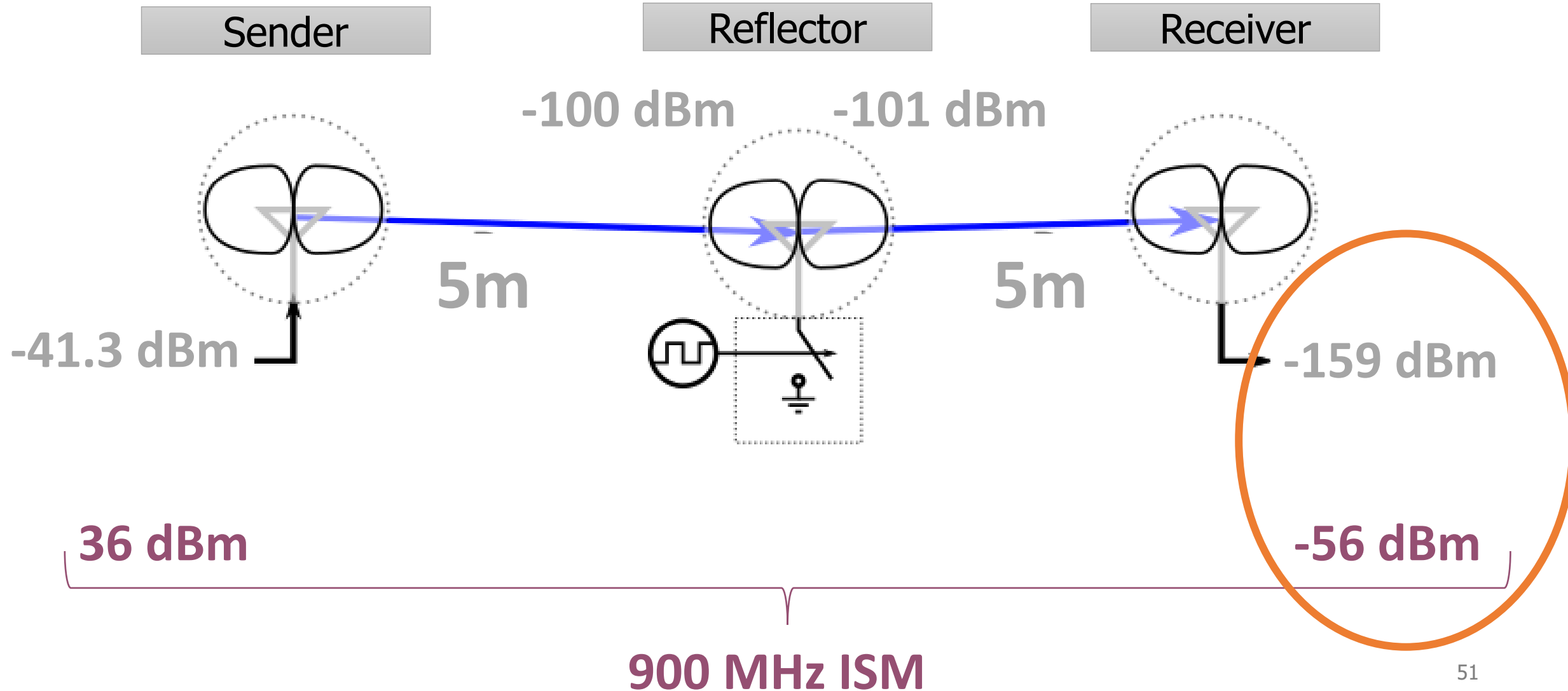
- Covers areas 30m+
  - “through walls”
- Decimeter accurate
- $<1 \mu\text{W}$  tag
  - (COTS, can do order of magnitude or more better with VLSI)
- (Nearly) unlimited number of concurrent tags
- **1-15+ minutes per location fix**
  - **A latency/energy tradeoff for localization**

Slocalization: Sub- $\mu\text{W}$  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.**

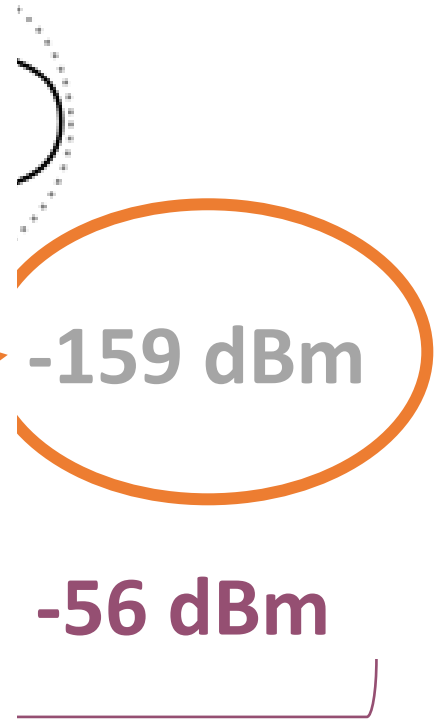
UWB Backscatter is passive reflection of a lot less energy than traditional communications



UWB Backscatter is passive reflection of a lot less energy

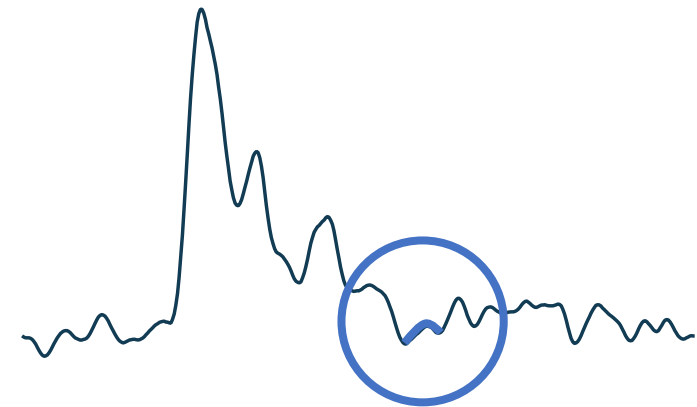
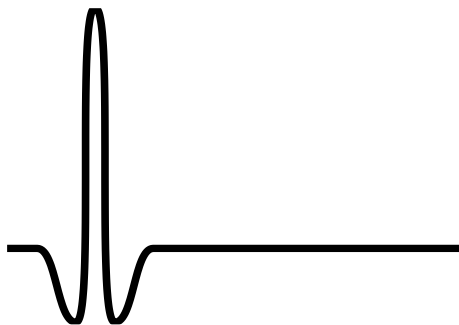
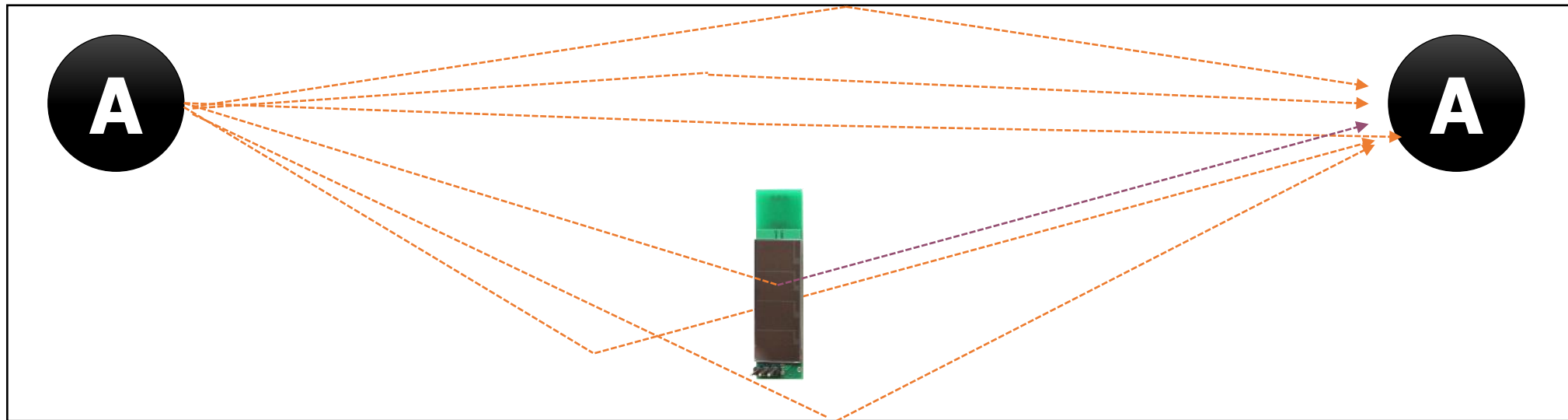
Packet Error Rate	Data Rate	Typical Receiver Sensitivity	Units
1%	110 kbps	-106	dBm/500 MHz
10%	110 kbps	-107	dBm/500 MHz
1%	850 kbps	-101	dBm/500 MHz
	6.8 Mbps	-93 (*-97)	dBm/500 MHz
10%	110 kbps	-106	dBm/500 MHz
	850 kbps	-102	dBm/500 MHz
	6.8 Mbps	-94 (*-98)	dBm/500 MHz

Typical receiver sensitivity ranges from -94 to -106



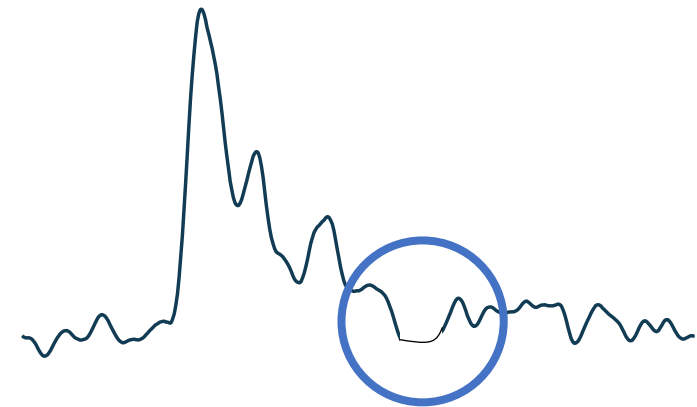
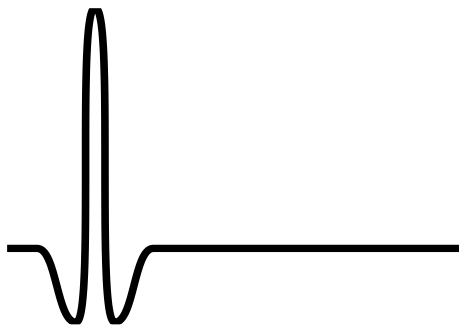
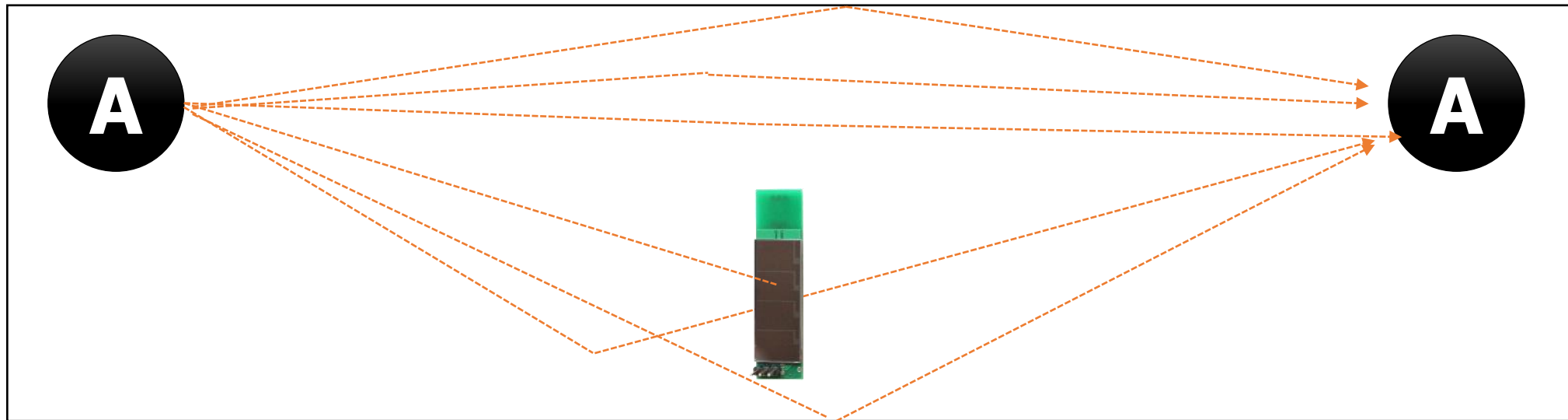
# How do we recover a signal that is way below the noise floor?

- Exploit tag stationarity and environmental stability



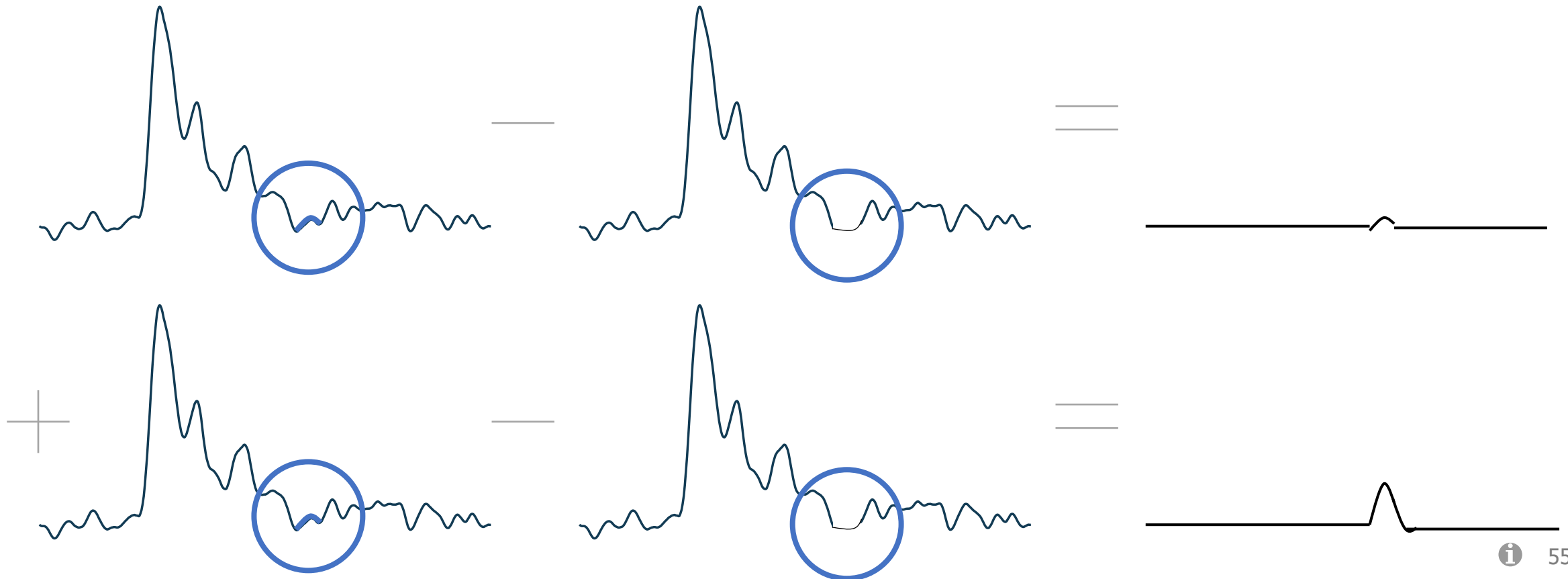
# How do we recover a signal that is way below the noise floor?

- Exploit tag stationarity and environmental stability

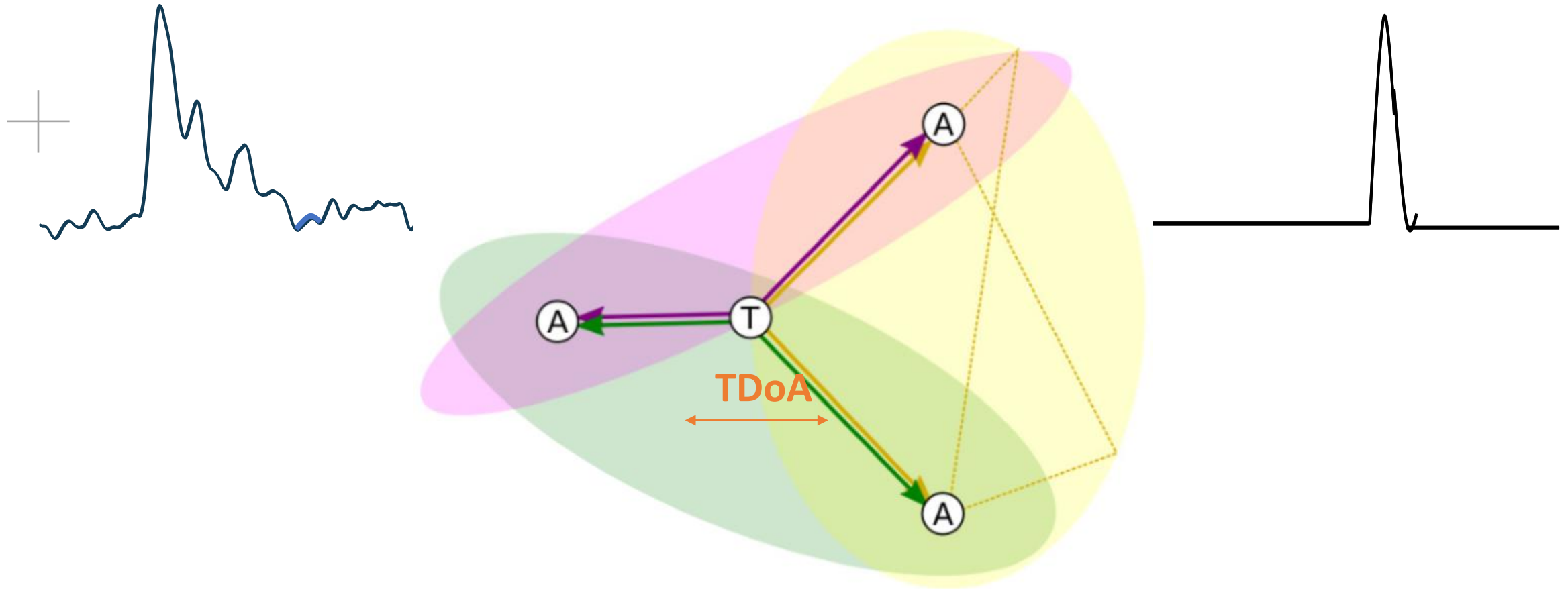


Ideally, the only change in the channel impulse response is the tag reflection

- Subtracting the environment finds the tag



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

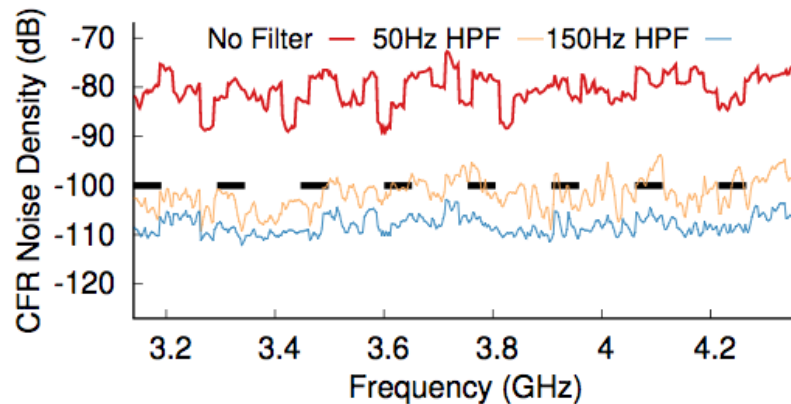


- First peak is anchor—anchor path, then anchor—tag—anchor

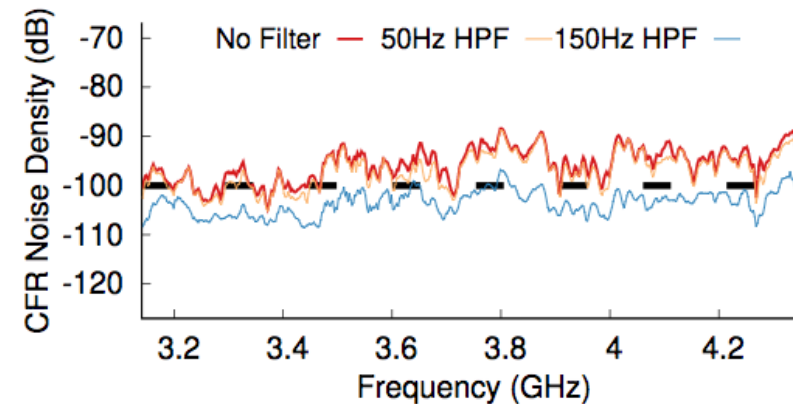


# Extracting the tag signal in the real world has a few additional challenges

- 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

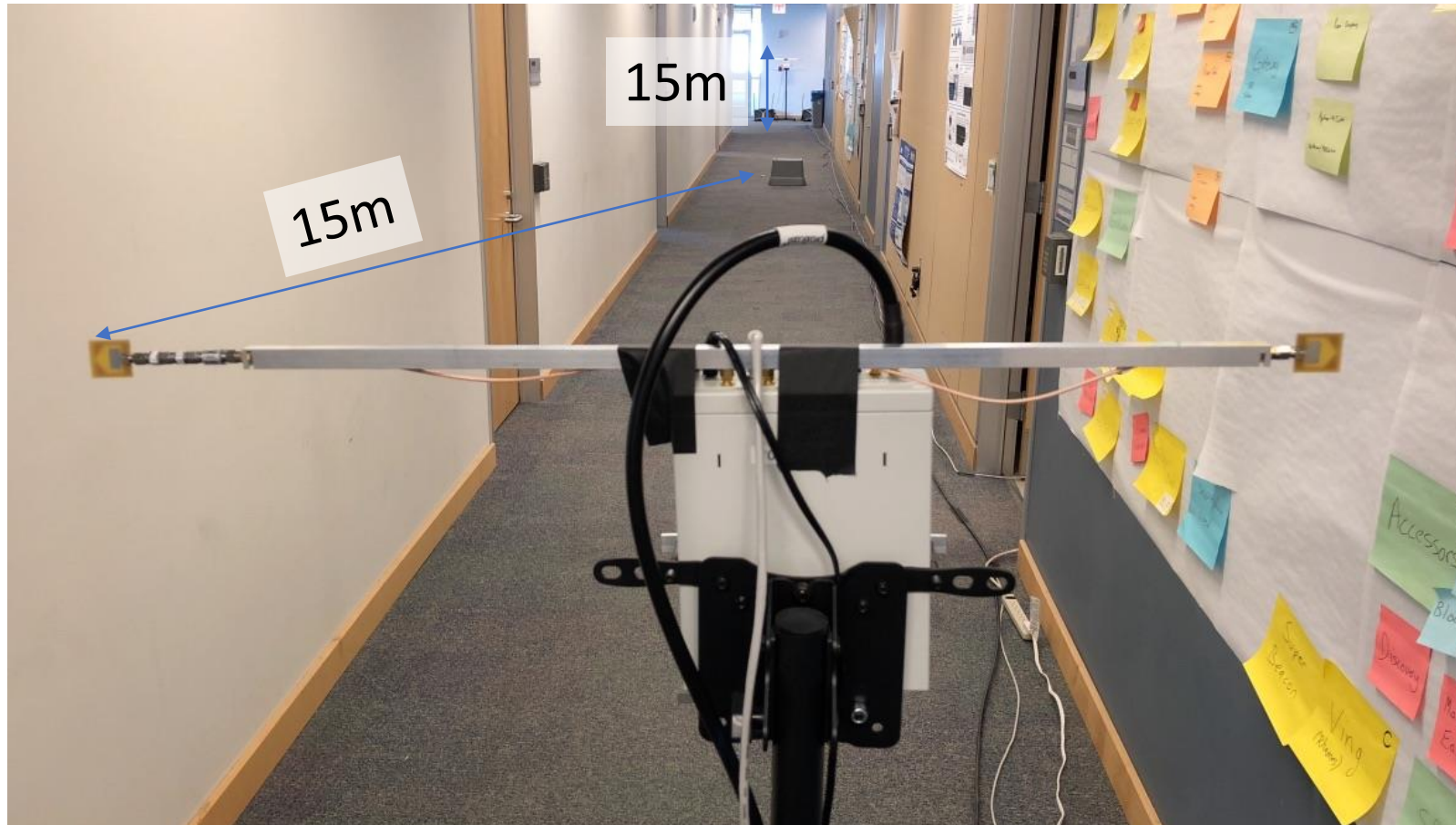


(c) CFR Noise Fluorescents

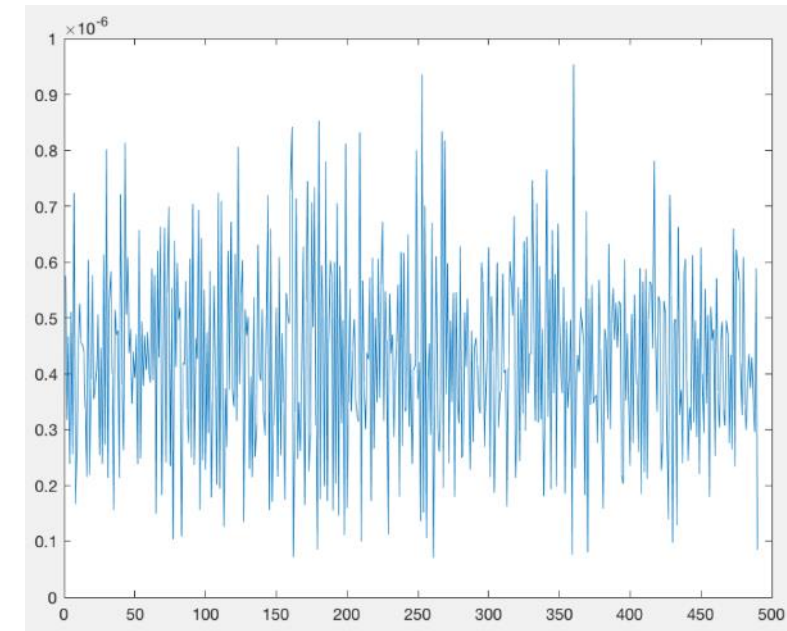
- Finding tag phase offset currently requires brute force search

# Does it really work?

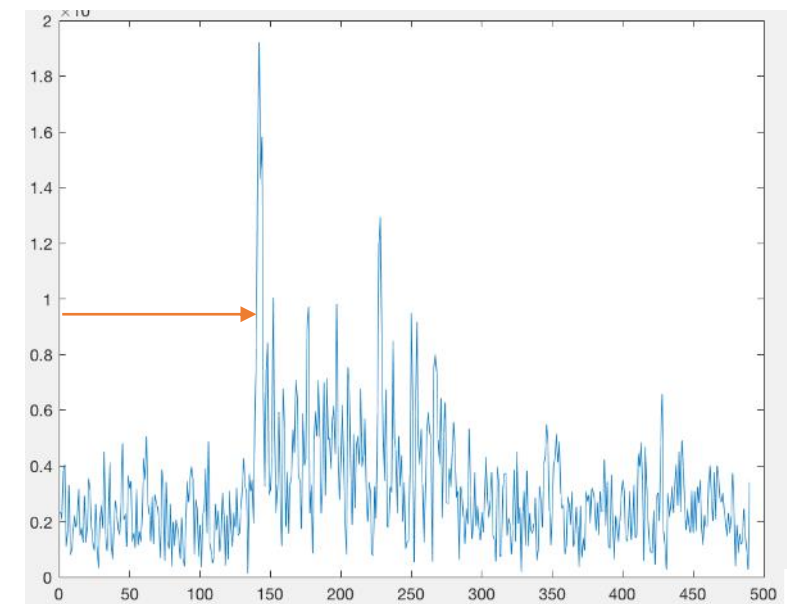
- 15 minutes can cover 30 meters
- 30 cm average error (3D Euclidean distance)



After a few seconds



After a few minutes



# Outline

- Backscatter
- Backscatter Uses
  - RFID
  - 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](#)

March 2018

doc.: IEEE 802.11-18/0540r0

## WUR beyond wake-up: example

### Implemented proof of concept: smart socket [6]

based on (pre TGba) 802.11 WUR [7]

- Circuit capable of receiving OOK-modulated signals generated by a legacy IEEE 802.11 transmitter and consuming in the  $\mu\text{W}$  scale
  - Transmission of simple commands: switch on/off/intensity/etc.

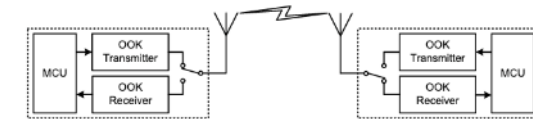
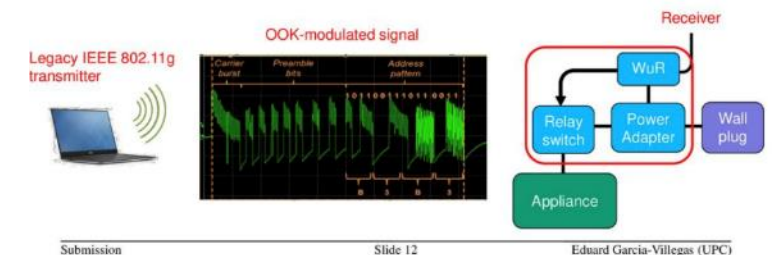


Figure 1: Proposed mote architecture with a micro-controller (MCU), OOK transmitter, and always-on ultra-low power OOK receiver.

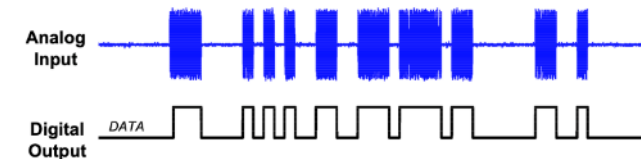
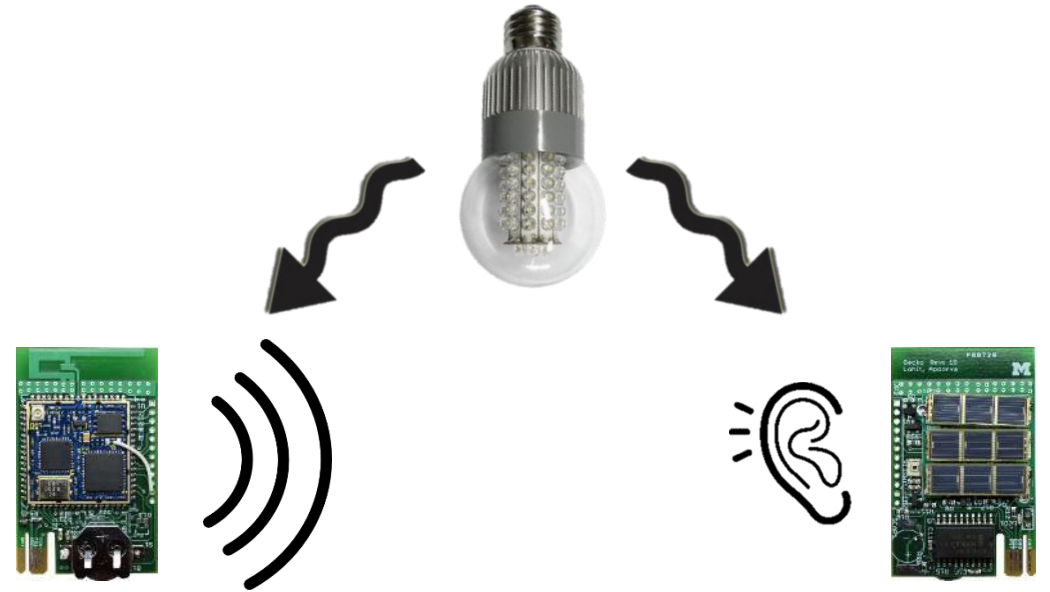


Figure 2: Example OOK signal at the input to the receiver and its corresponding demodulated output.

# (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
  - 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, Backscatter

