6.S062: Mobile and Sensor Computing

Lecture 6: Battery-Free Networking and Sensing

Some material adapted from Haitham Hassanieh (UIUC)

RFID (Radio Frequency IDentification)

Access Control

Inventory control

Security Sensitive Applications

Tracking & Localization

Long-Range Payment Systems

RFID (Radio Frequency IDentification)

Access Control

Inventory control

Largest and fastest growing market of networked devices by unit sale:
5 billion sold in 2016 alone

Long-Range Payment Systems

Basic Principle of Operation

RFID: cheap battery-free stickers

Reply to wireless reader
with a unique identifier

History of RFIDs

- WWII: Aircraft IFF Transponder
  - Identify Friend or Foe, Transmitter-Responder

- 1945: "The Thing" or "The Great Seal Bug"
  - "Gift" given by the Soviets to American ambassador

- 1980s: development of E-Toll transponders

- 2004: Auto-ID lab at MIT led to the birth of modern battery-free RFIDs
  - Goal: supply chain chain optimization
  - Paper: "Towards the 5 cent tag"

Types of RFIDs

Frequency Range

UHF (~900MHz)

HF (13.56MHz)

LF (120-150kHz)

long range (few m)

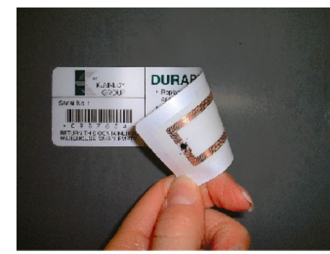
short range (few cm)

Range of Operation

"need to tap"

Power consumption

Where do these fall?



Types of RFIDs

Frequency Range

UHF (~900MHz)

HF (13.56MHz)

LF (120-150kHz)

the vast majority of RFIDs

Cost

few cents

10s to 100s of $

Power consumption

Passive (battery-free)

Semi-Passive or Semi-Active

Active (with battery)

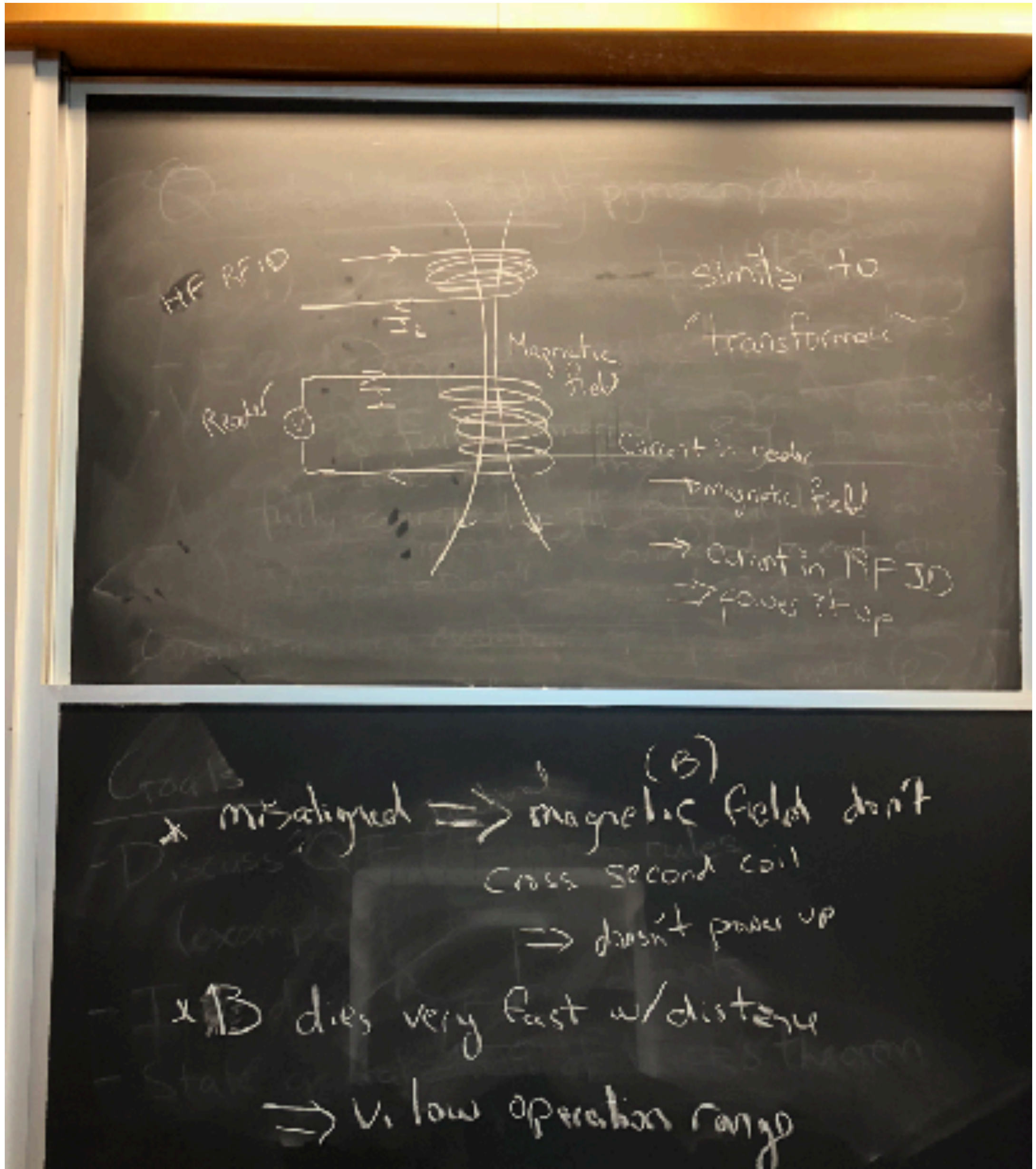
Other less common versions: 2.4GHz, UWB (3-10GHz), etc.

How does an RFID power up?

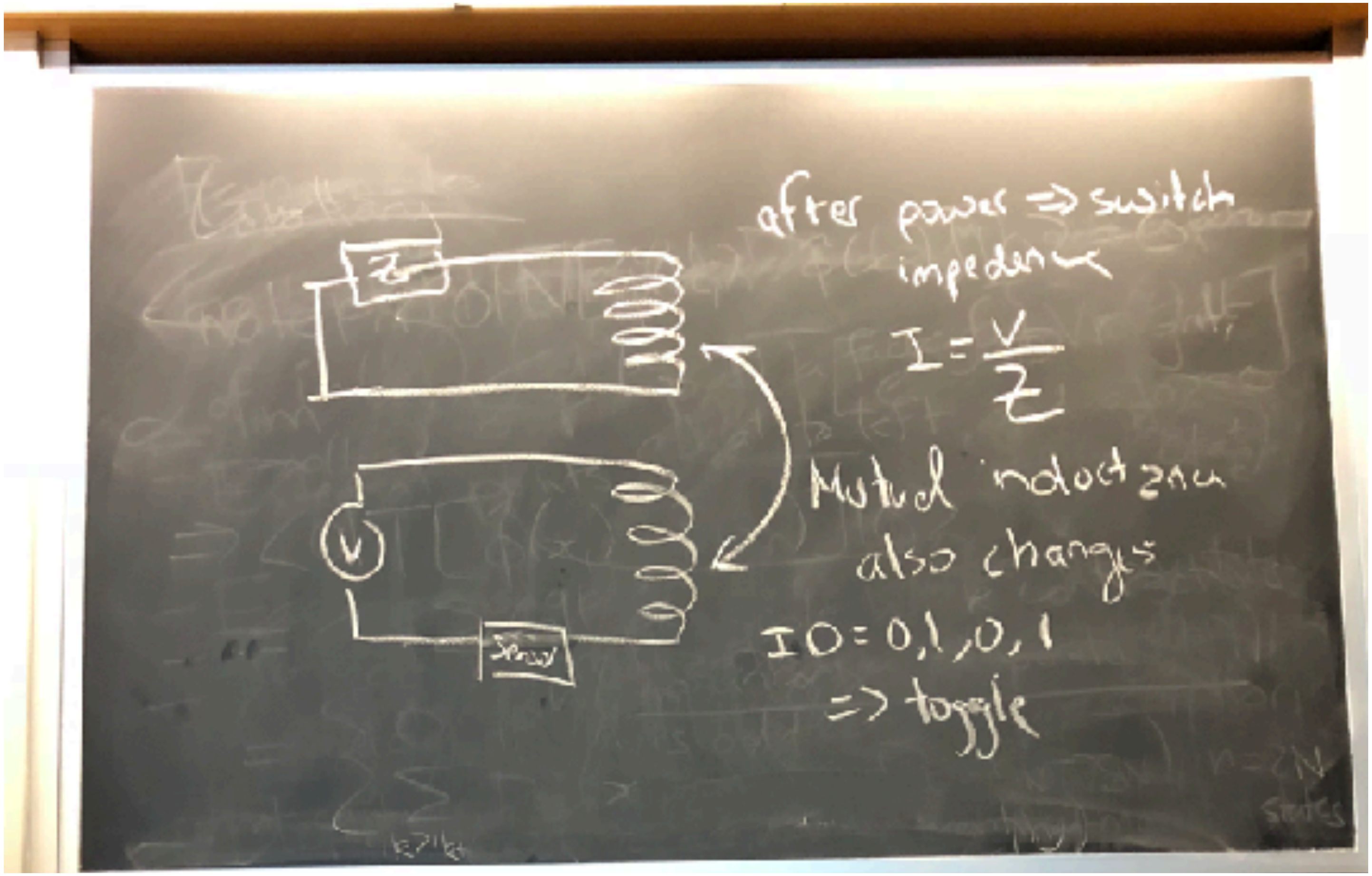
Harvests Energy from Reader's Signal

Inductive Coupling		Backscatter
LF (120-150kHz)	HF (13.56MHz)	UHF (~900MHz)
Magnetic (Near Field)		Electromagnetic (Far Field)
Coil		Antenna

Inductive Coupling



Inductive Coupling

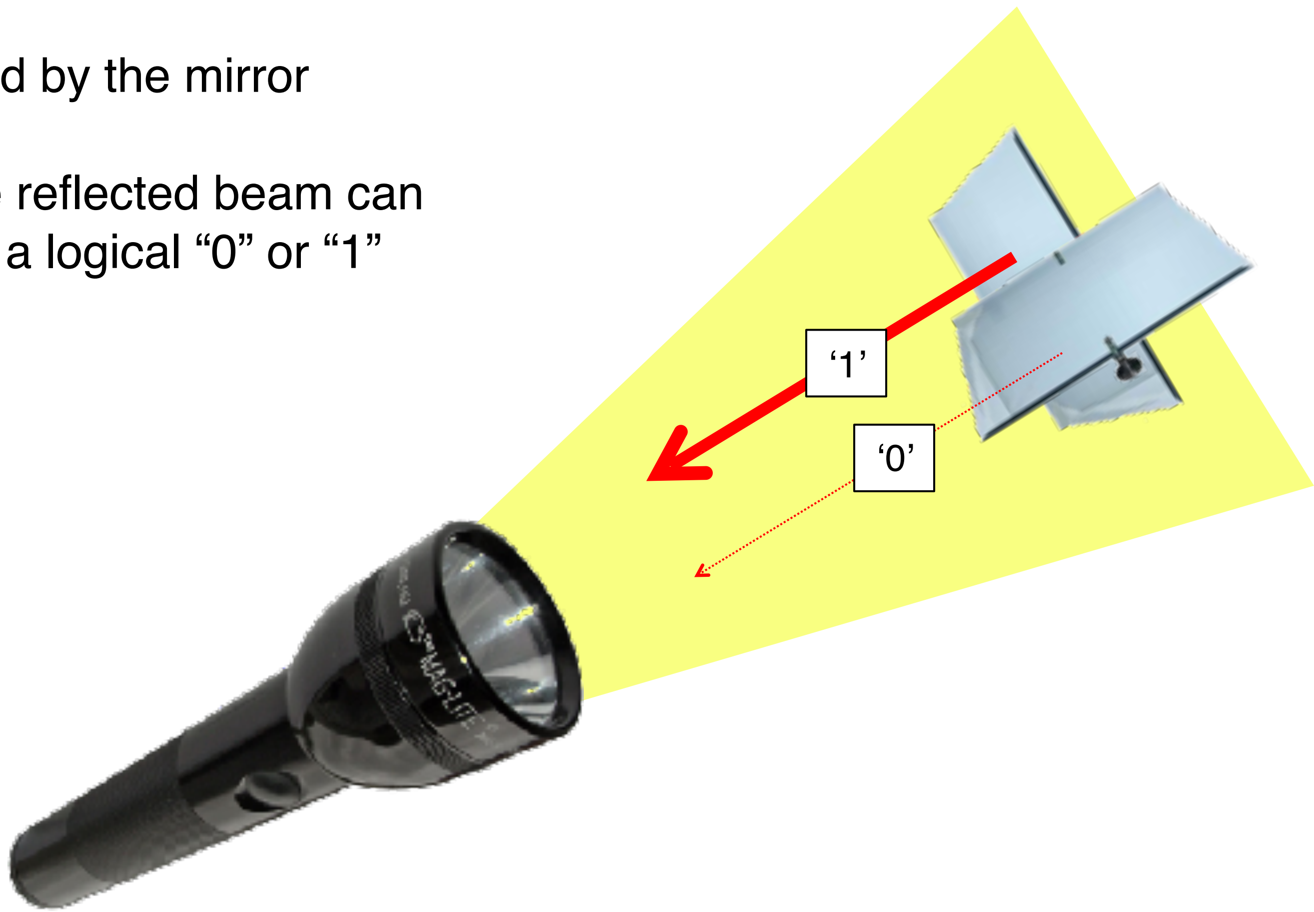


Rest of This Lecture

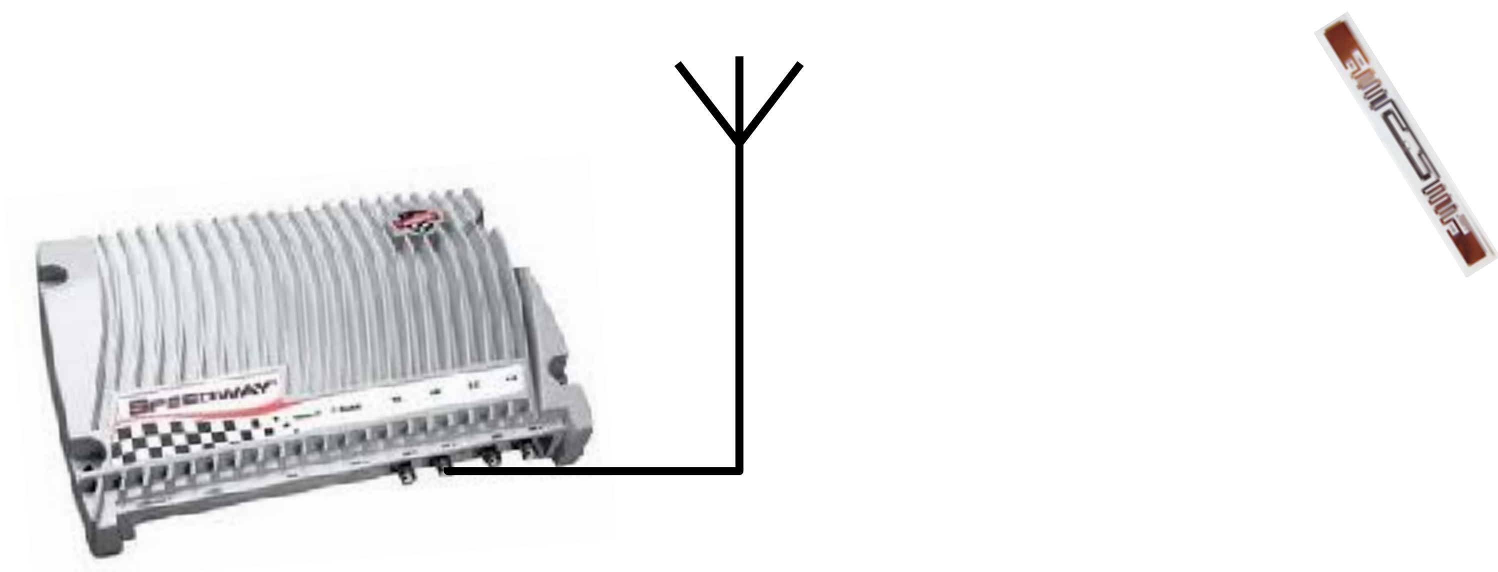
- Understanding RFID communication
- RFID Localization

Backscatter Communication

- A flashlight emits a beam of light
- The light is reflected by the mirror
- The intensity of the reflected beam can be associated with a logical "0" or "1"



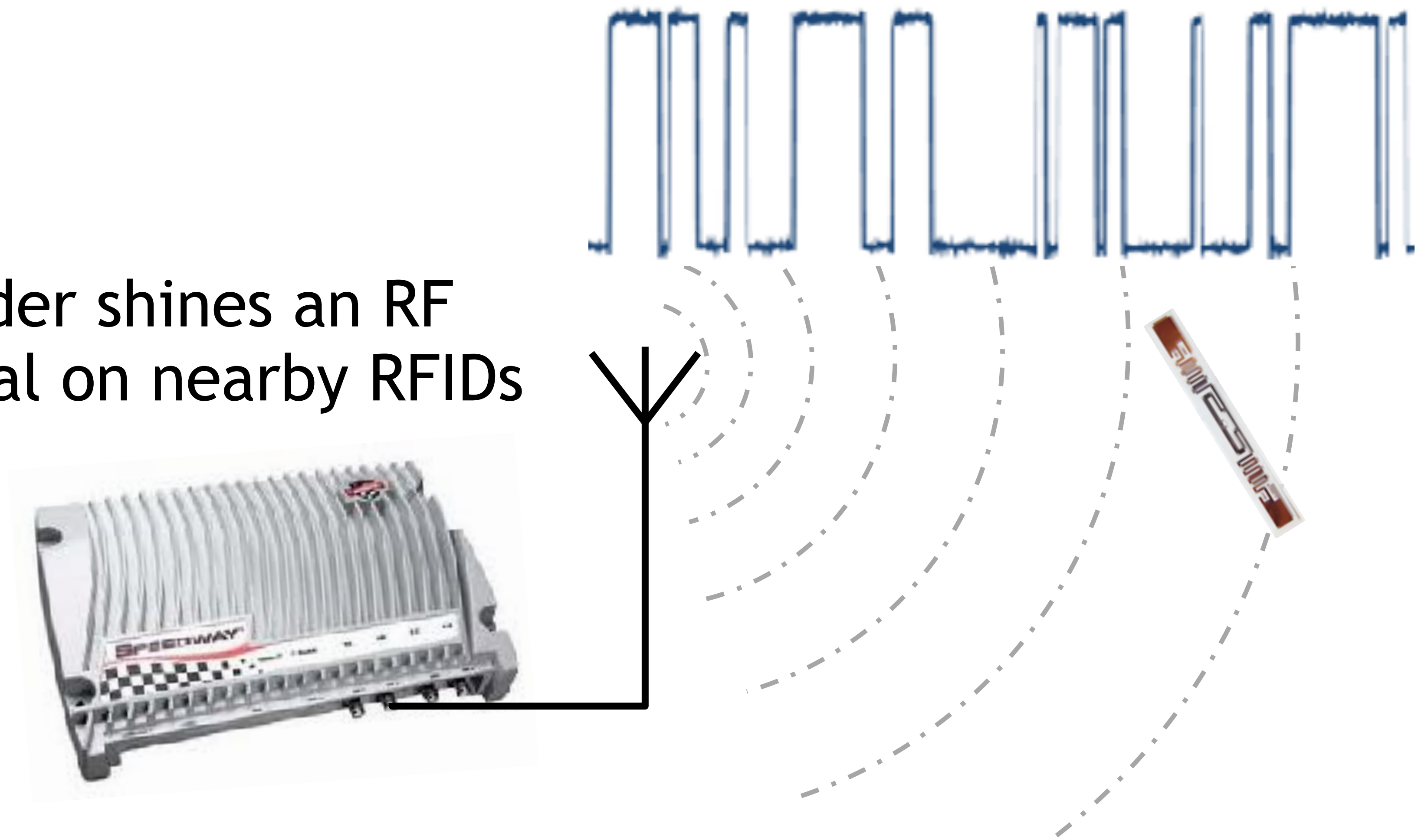
Backscatter Communication



Backscatter Communication

Tag reflects the reader's signal using ON-OFF keying

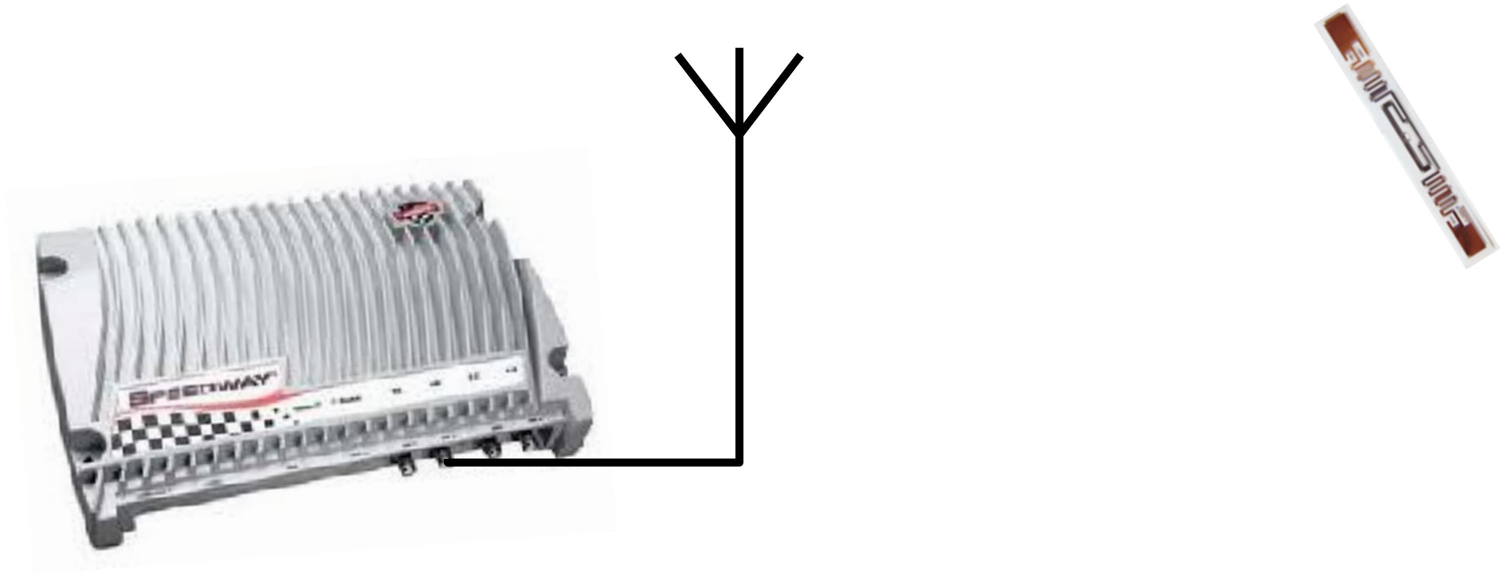
Reader shines an RF signal on nearby RFIDs



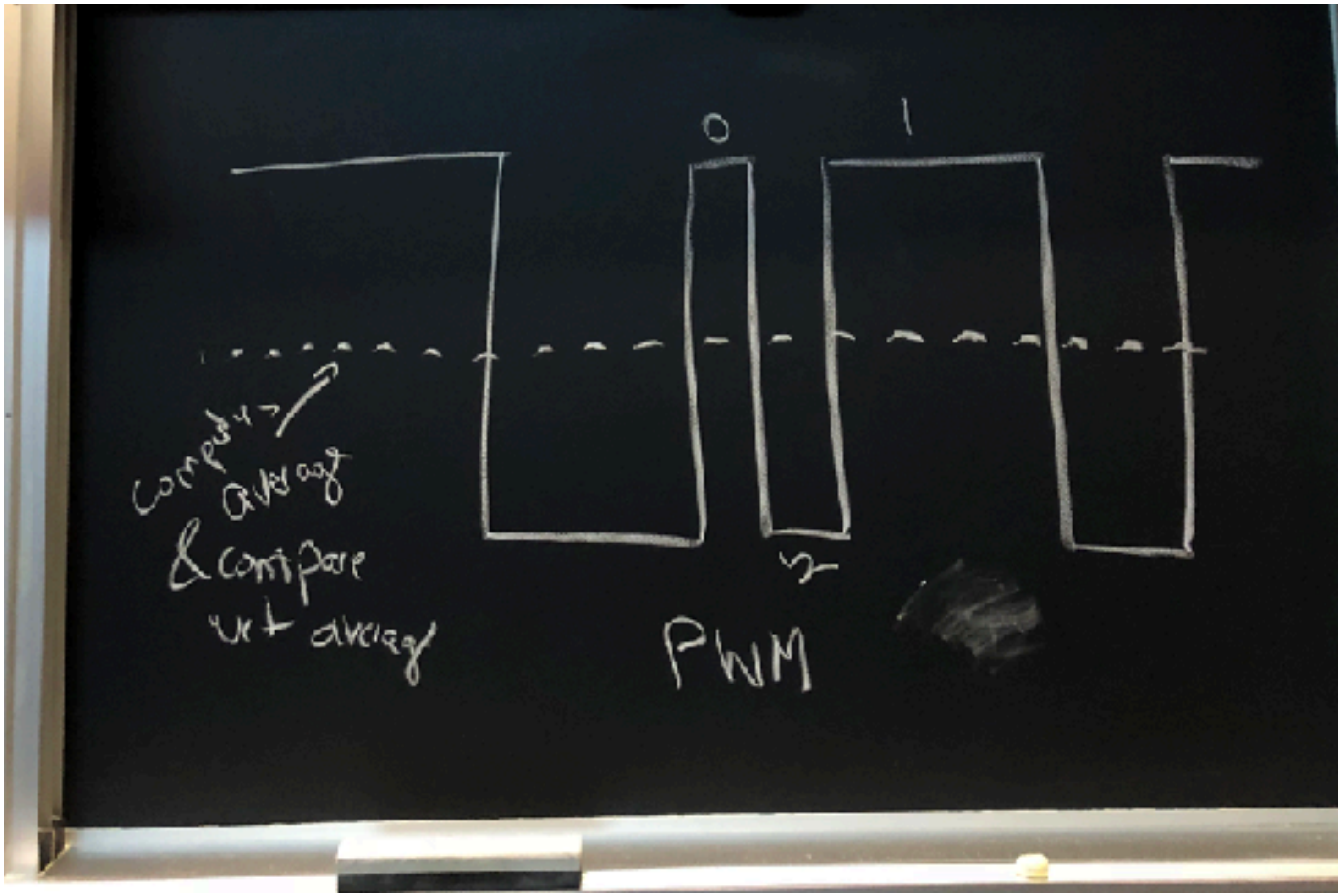
Backscatter Communication

RFIDs are synced by the reader's signal:

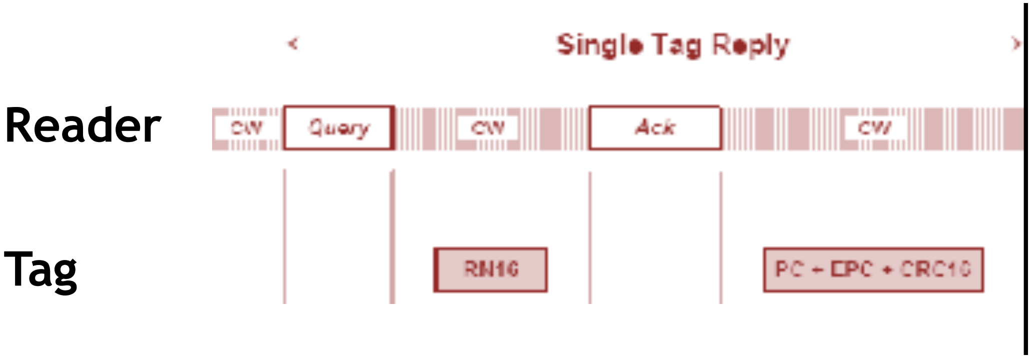
- Time synchronization
- Frequency synchronization



Backscatter Communication



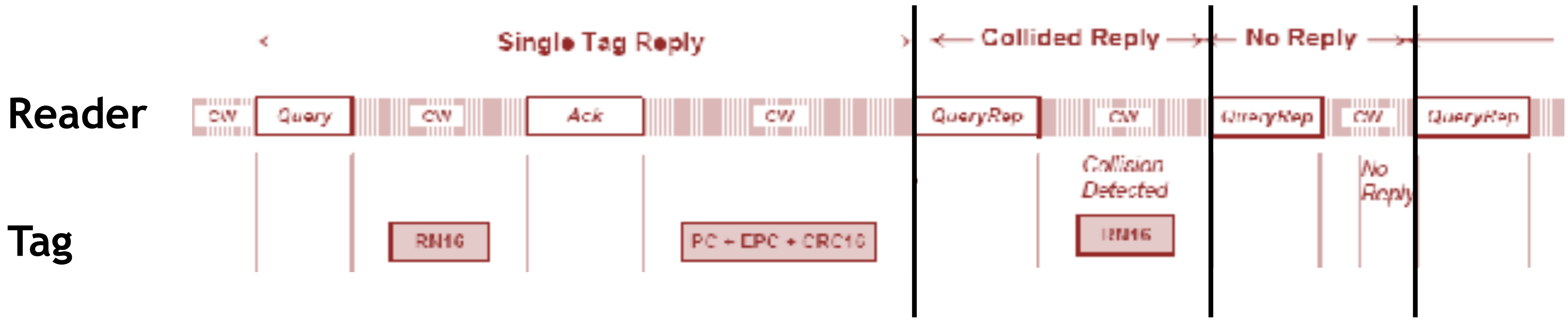
EPC Gen2 Standard - MAC



Slotted Aloha:

– Reader allocates Q time slots and transmits a query at the beginning of each time slot
– Each tag picks a random slot and transmits a 16-bit random number
– In each slot:
  • RN16 decoded → Reader ACKs → Tags transmits 96-bit ID
  • Collision → Reader moves on to next slot
  • No reply → Reader moves on to next slot

EPC Gen2 – MAC



Inefficient:

- If reader allocates large number of slots → Too many empty slots
- If reader allocates small number of slots → Too many collisions

EPC Gen2 – MAC: Minimizing Collisions

- N RFID Tags & K Time slots
- Each tag picks a slot uniformly at random to transmit in
- *Let's assume the reader knows the number of tags N; how should it set K?*

- Probability that a tag transmits in a given slot:

$$p = \frac{1}{K}$$

- Probability that any tag transmits in a given slot without collision:

$$E = Np(1-p)^{N-1}$$

- To maximize E, set:

$$\frac{dE}{dp} = 0$$

- p=1/N => K=N

EPC Gen2 – MAC: Minimizing Collisions

- N RFID Tags & K Time slots
- Each tag picks a slot uniformly at random to transmit in
- *Let's assume the reader knows the number of tags N; how should it set K?*

- Probability that a tag transmits in a given slot:

$$p = \frac{1}{K}$$

- Probability that any tag transmits in a given slot without collision:

$$E = Np(1-p)^{N-1}$$

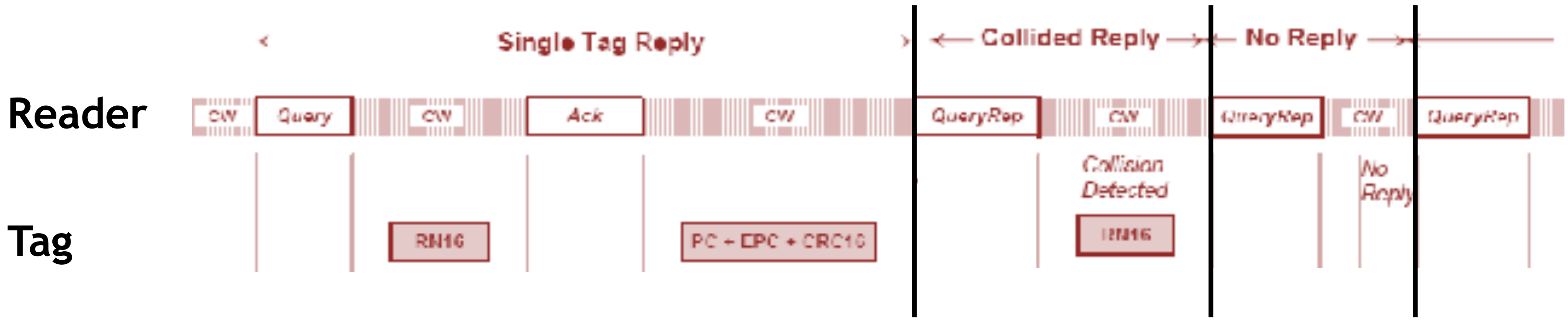
- To maximize E, set K = N

- Efficiency (probability that "any" tag occupies a time slot):

$$\text{Efficiency} = E = \left(1 - \frac{1}{N}\right)^{N-1}$$

$$\text{Efficiency} \leq lim_{N \to \infty} E = \frac{1}{e} = 0.37$$

EPC Gen2 - MAC



Inefficient:

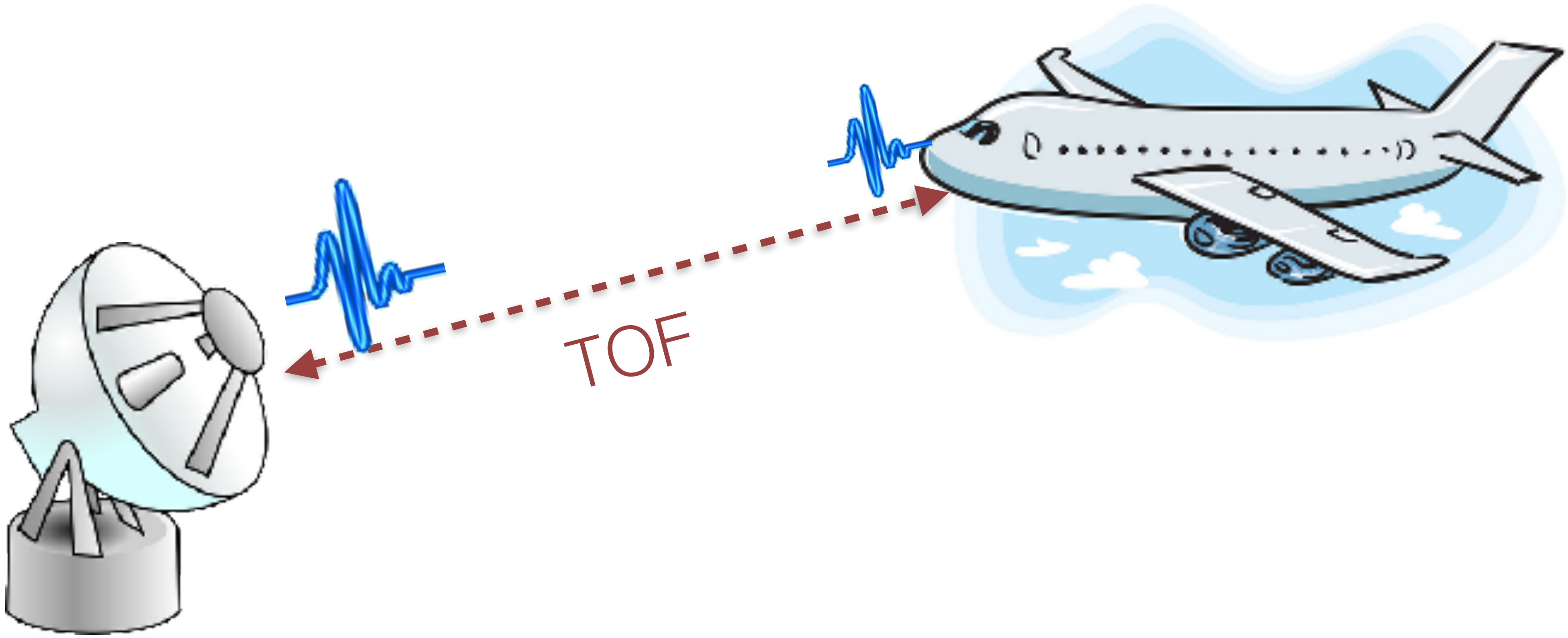
- If reader allocates large number of slots → Too many empty slots
- If reader allocates small number of slots → Too many collisions
- If reader knows number of tags = N → Allocate K=N slots → 37% efficiency
- Downlink overhead

Significant work on “spanning trees”, efficient scanning, decoding with collisions, etc.

Rest of This Lecture

- Understanding RFID communication
- **RFID Localization**

How Can We Bring WiTrack's Capabilities to Battery-Free RFIDs?

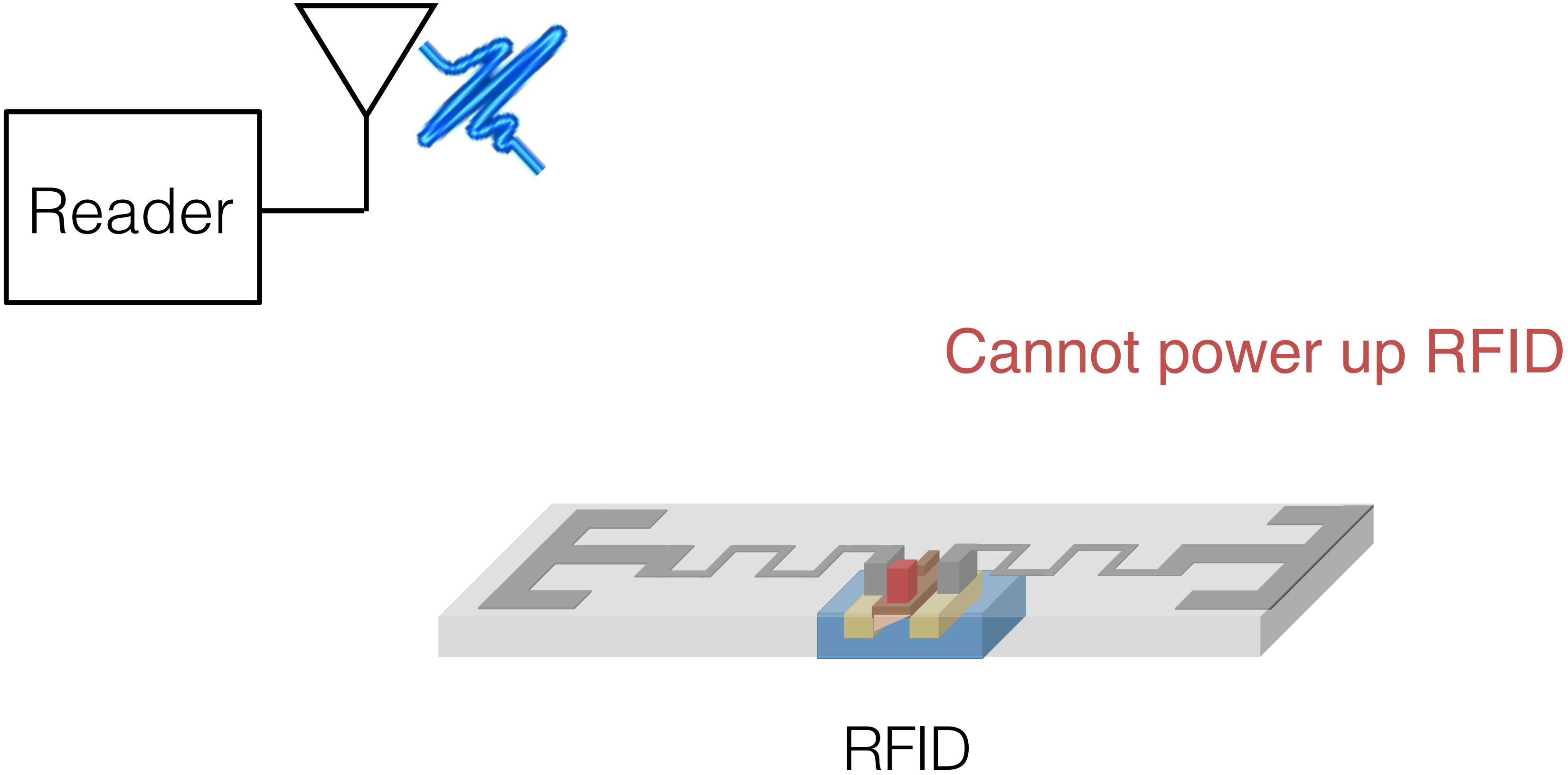


WiTrack/Radar:

Localize by measuring the Time-of-flight

Distance = Time-of-flight x speed of light

How about we just transmit a very short pulse?



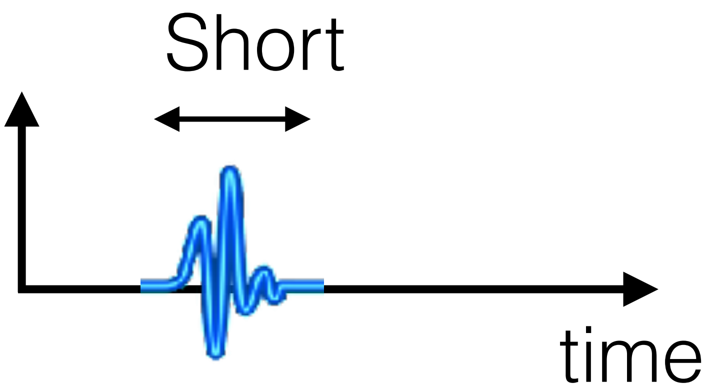
Problem: RFIDs cannot power up from a very short pulse

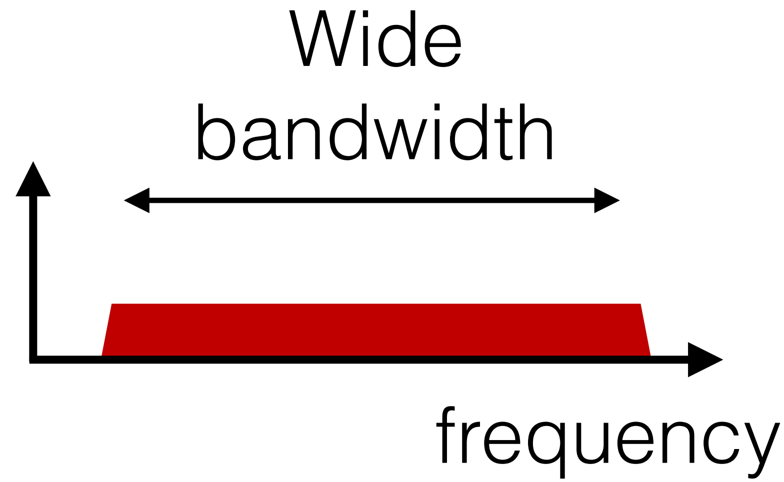
RFind

- RFind brings radar capabilities to billions of deployed battery-free RFIDs
- It can accurately estimate the time-of-flight in real indoor environments with dense multipath
- Implemented and evaluated a prototype of RFind in real-world environments

Where Radar Resolution Comes From

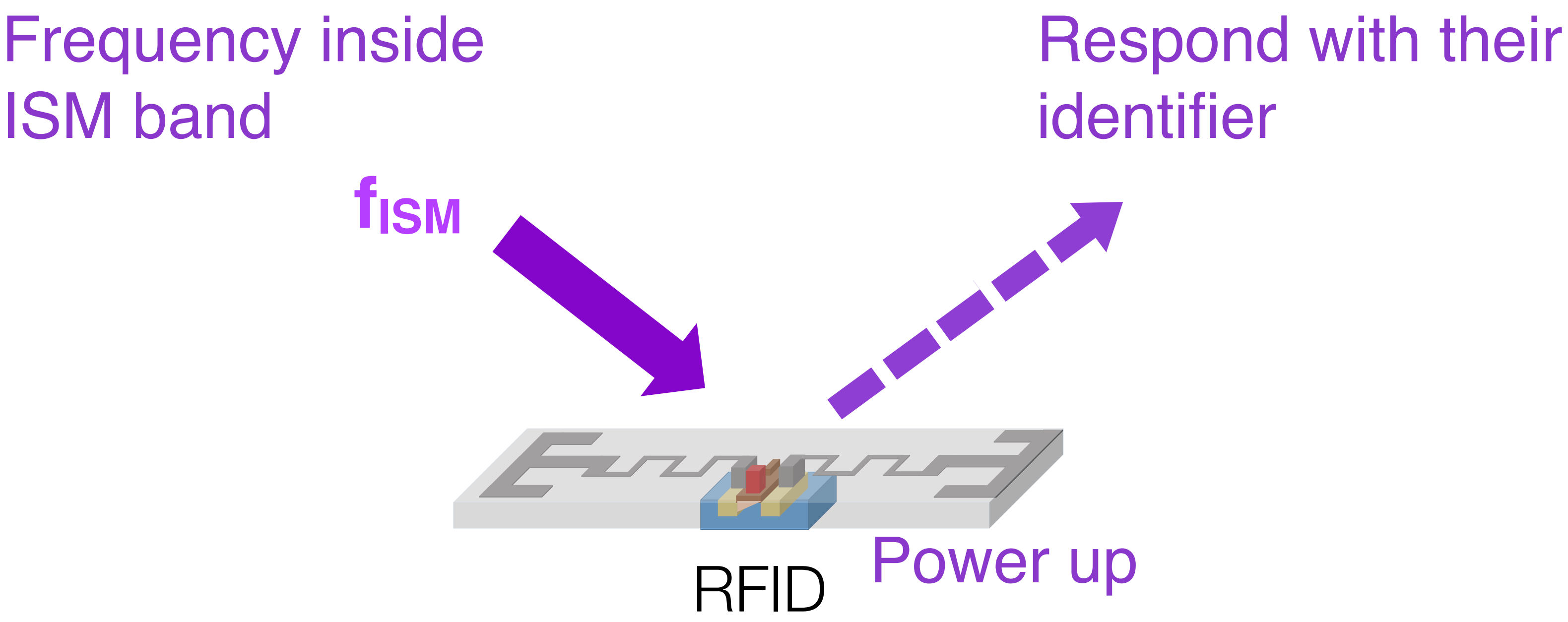
Short pulse allows measuring time at very fine granularity



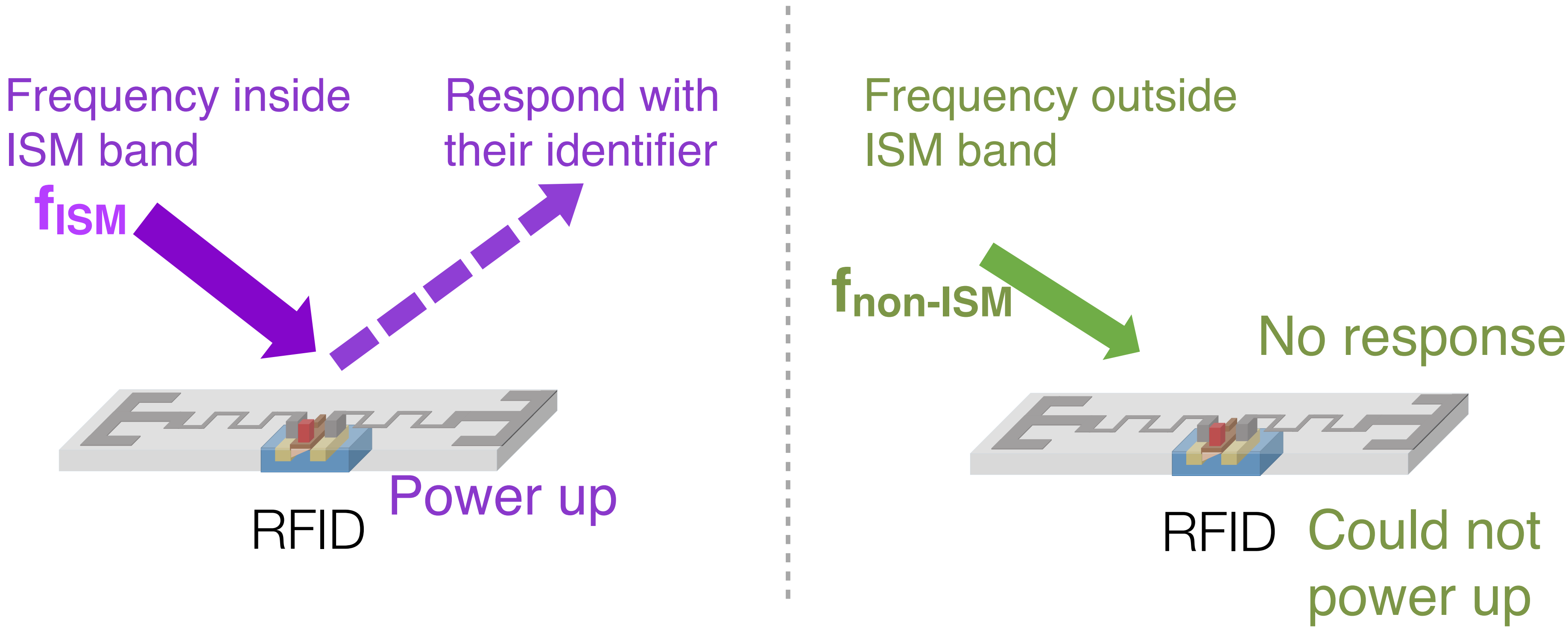


Can we achieve wide bandwidth on battery-free off-the-shelf RFIDs?

Problem: Battery-free RFIDs are designed to respond to a very narrowband signal

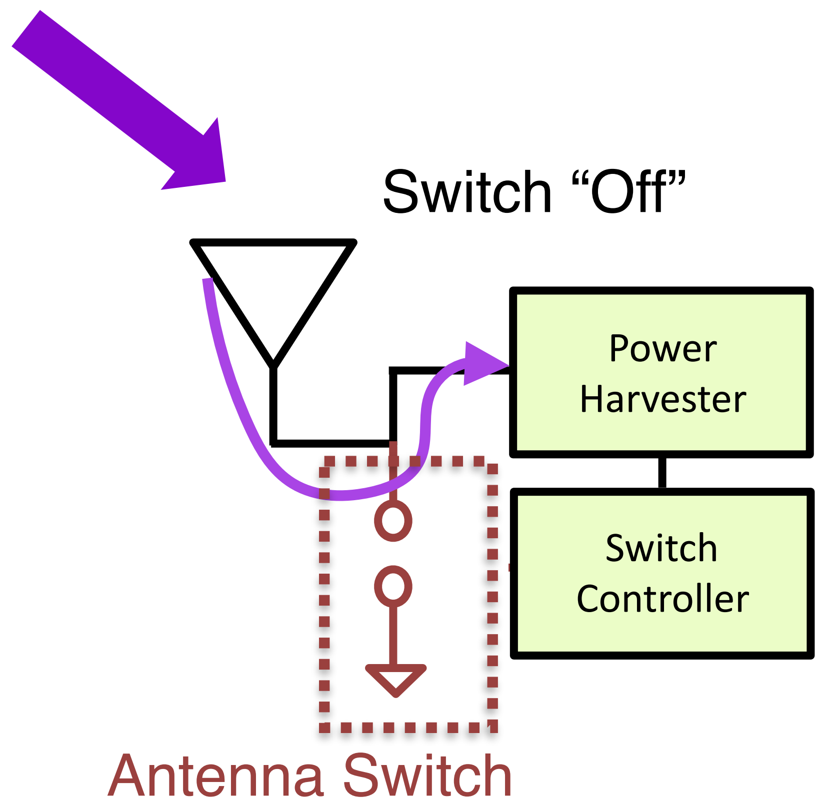


Problem: Battery-free RFIDs are designed to respond to a very narrowband signal



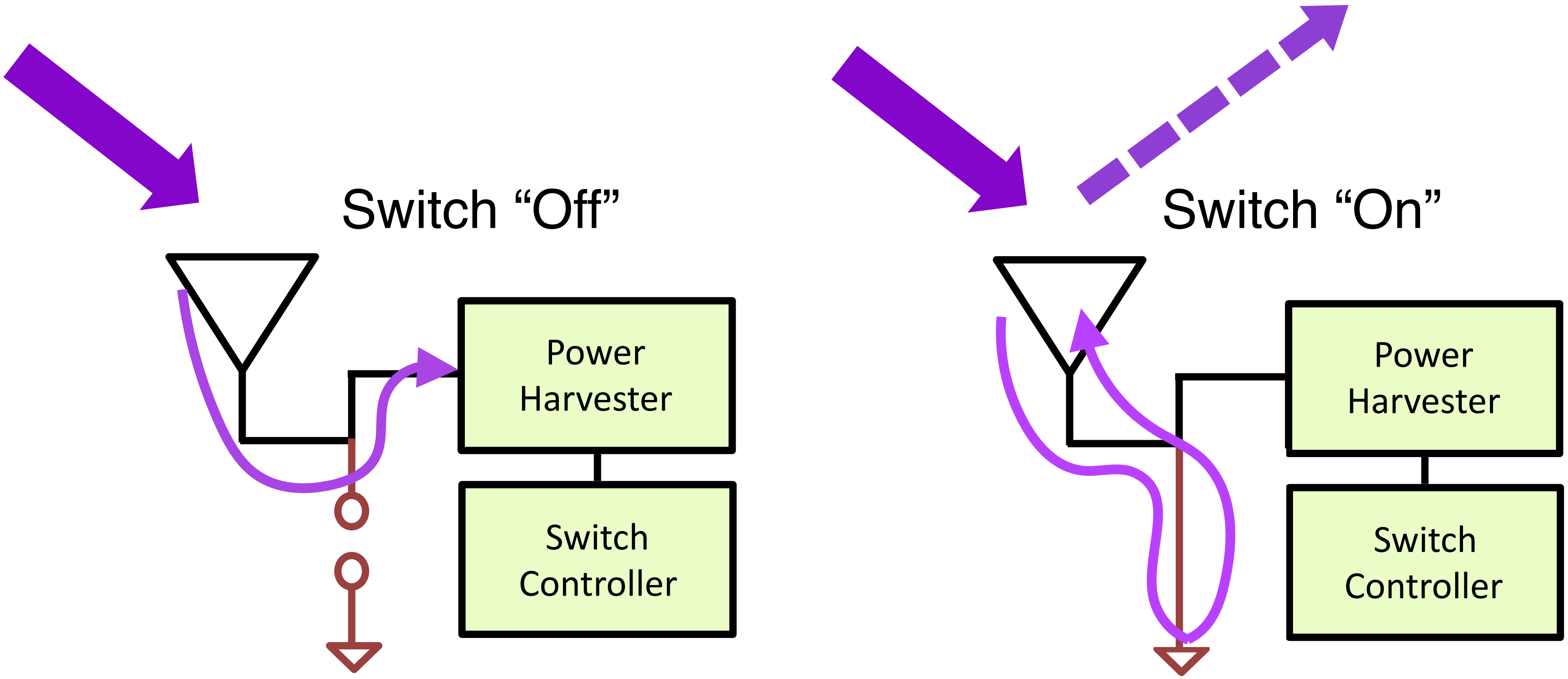
Battery-Free RFIDs are optimized to harness power from signals within the UHF ISM band (very narrow for time-of-flight estimation)

Key Realization:
RFID Modulation is Frequency Agnostic

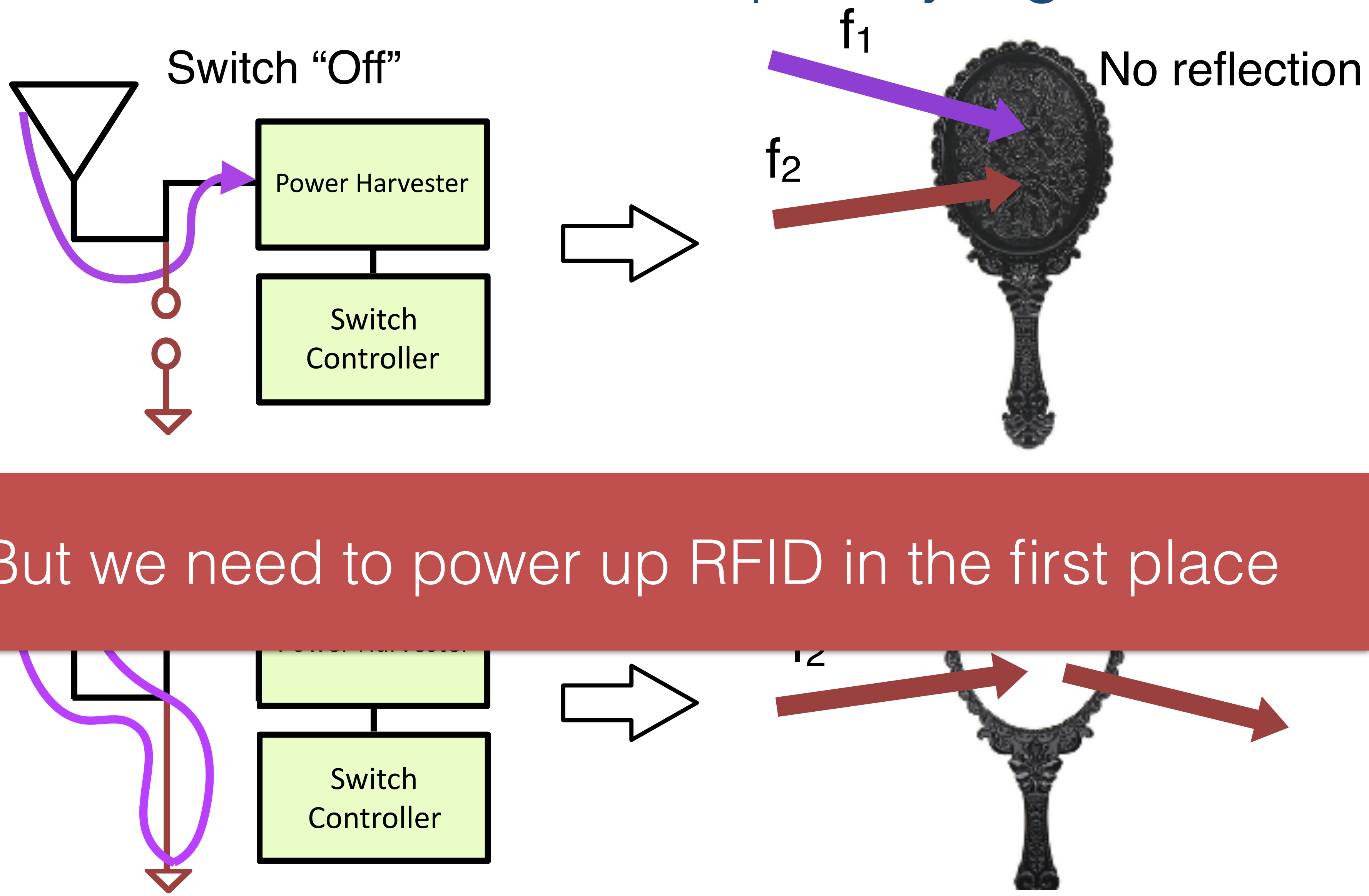


Simplified RFID schematic

Key Realization:
RFID Modulation is Frequency Agnostic



Key Realization:
RFID Modulation is Frequency Agnostic



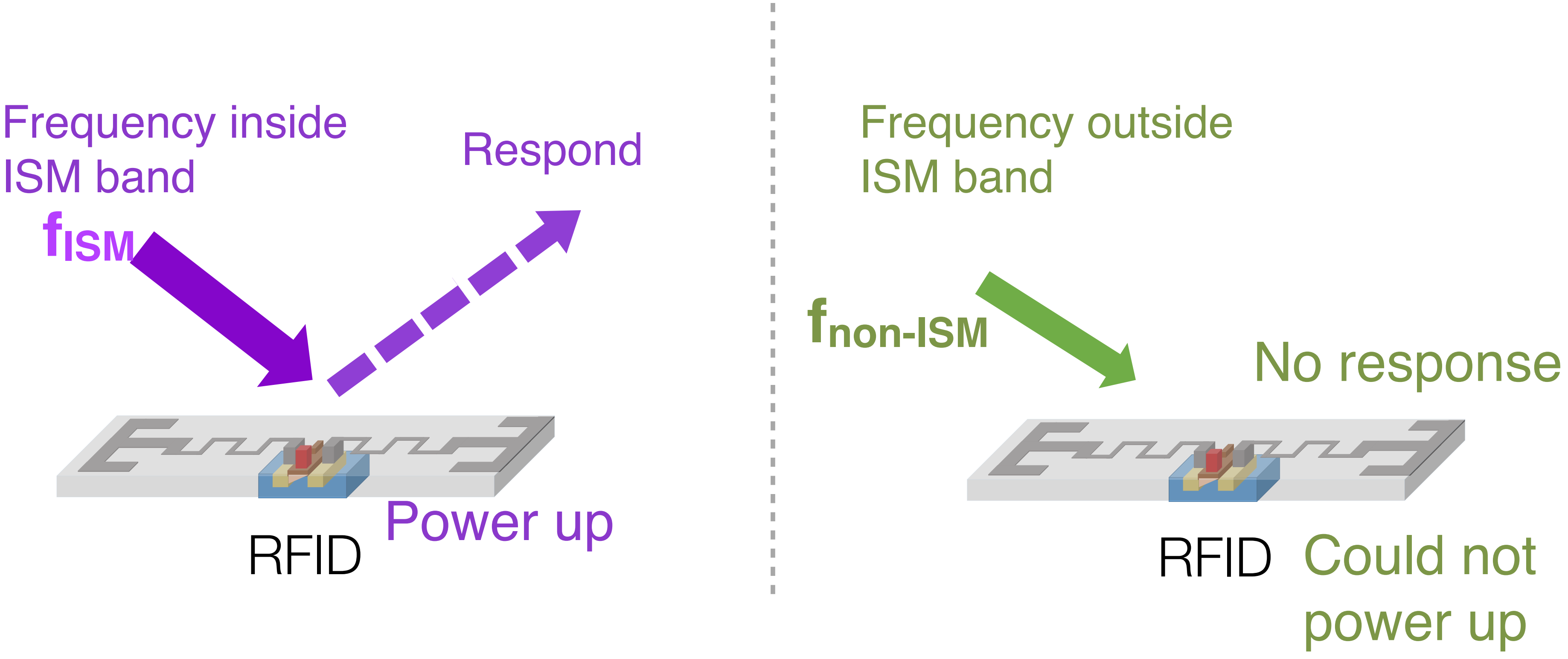
But we need to power up RFID in the first place

<u>Dual-Frequency Excitation</u>

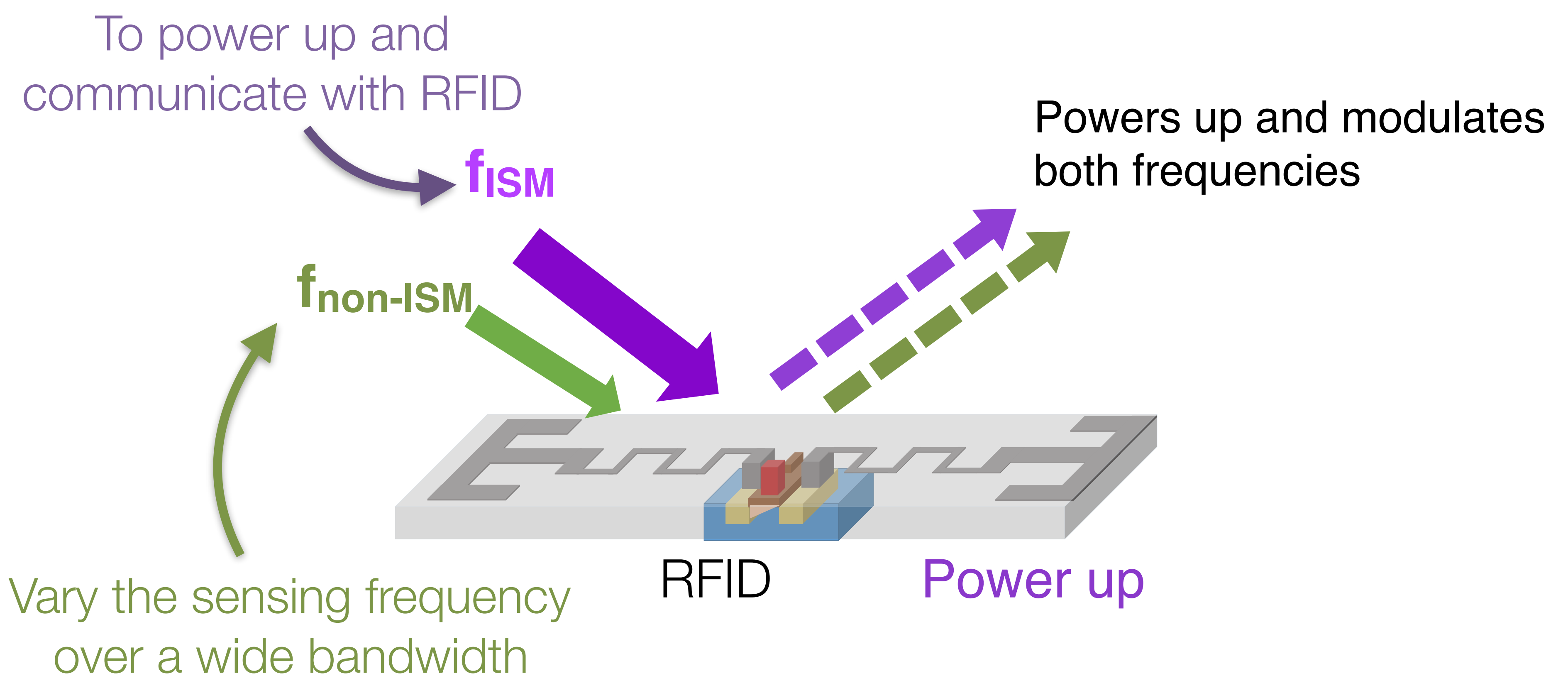
a technique that decouples powering up from sensing in RFID localization

Dual-Frequency Excitation

Battery-Free RFIDs are optimized to harness power from signals within the UHF ISM band (very narrow for localization)

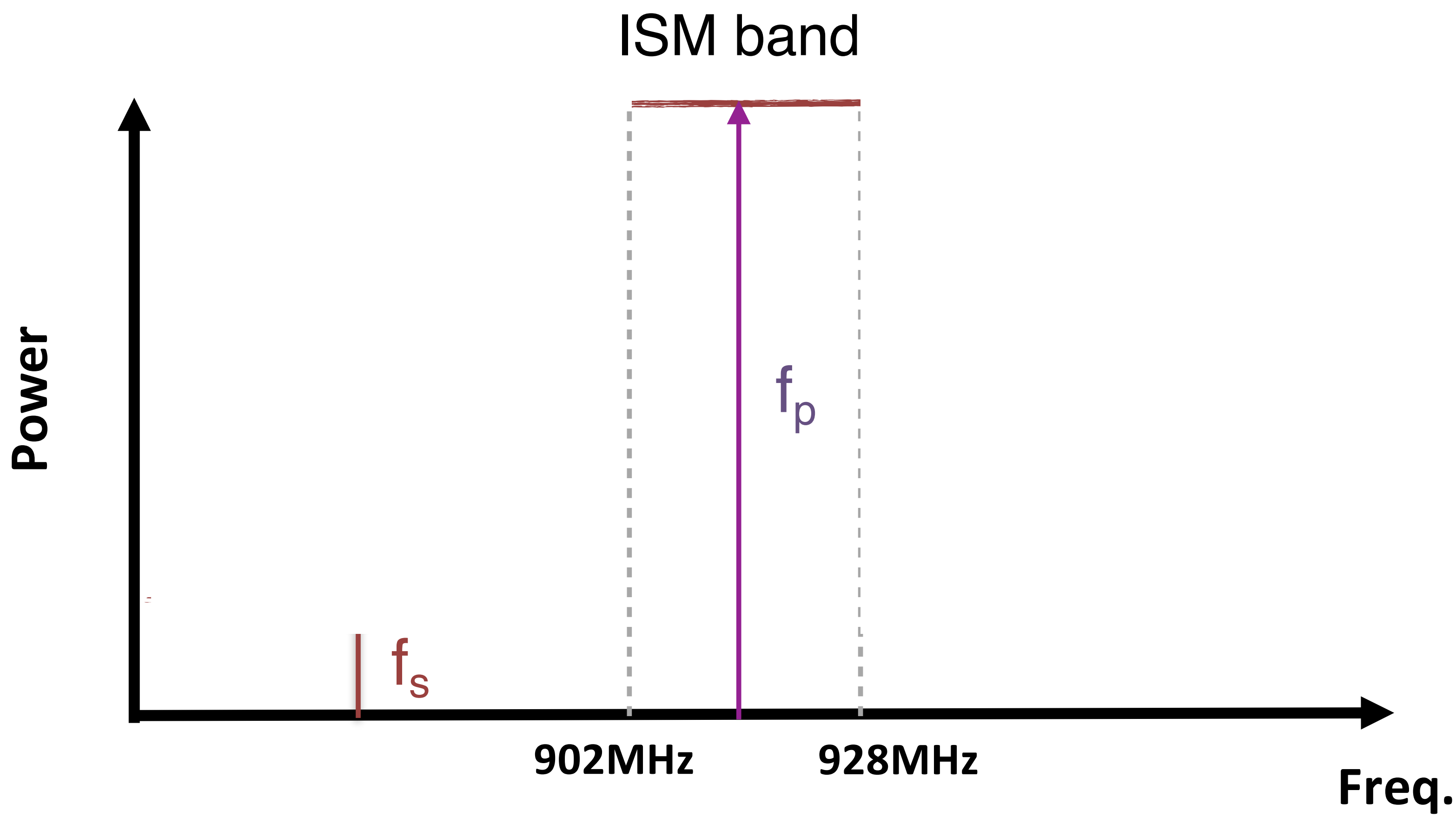


Dual-Frequency Excitation

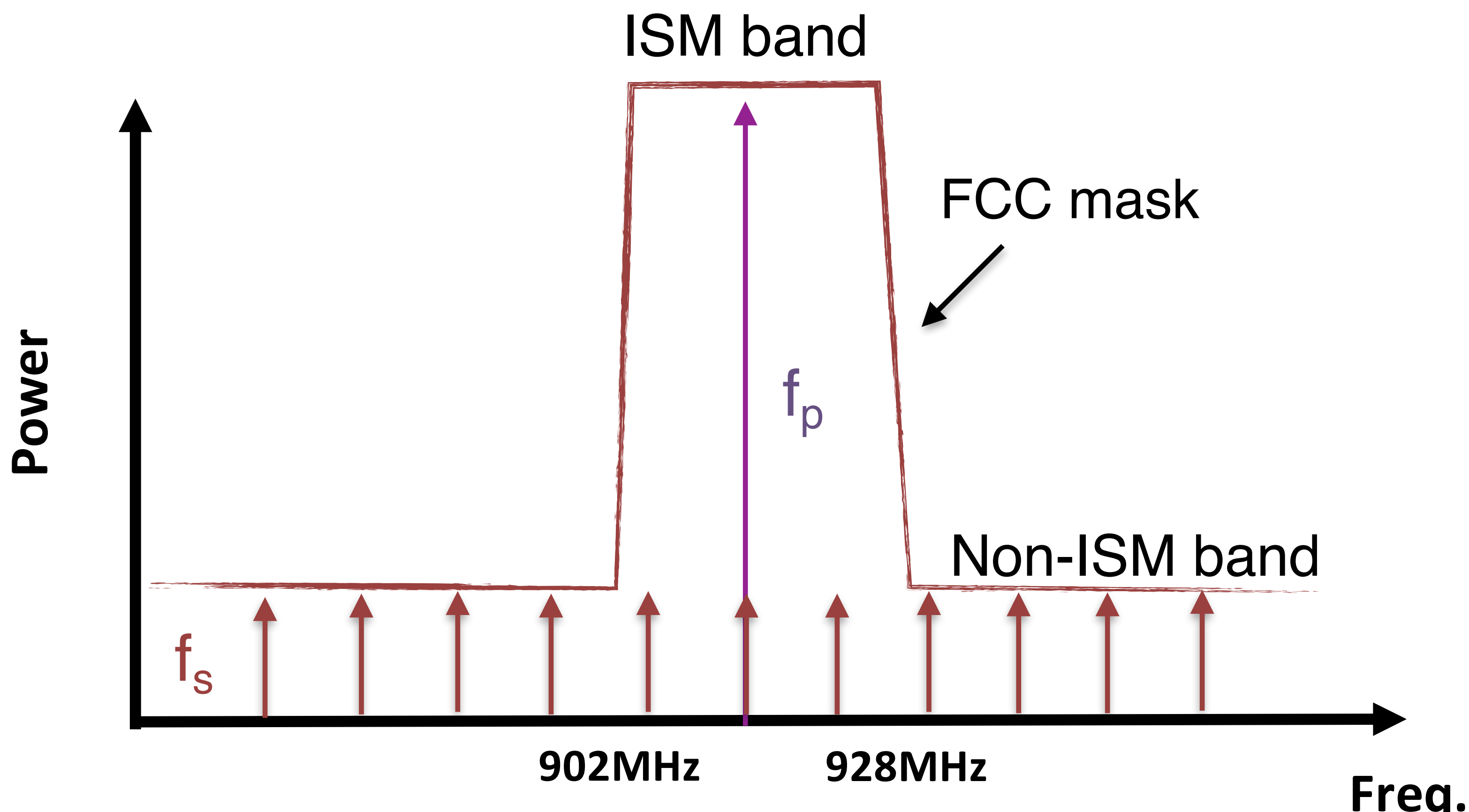


Wide Bandwidth → Time-of-flight → Accurate Localization

How can we perform wideband sensing despite FCC regulations?



How can we perform wideband sensing despite FCC regulations?

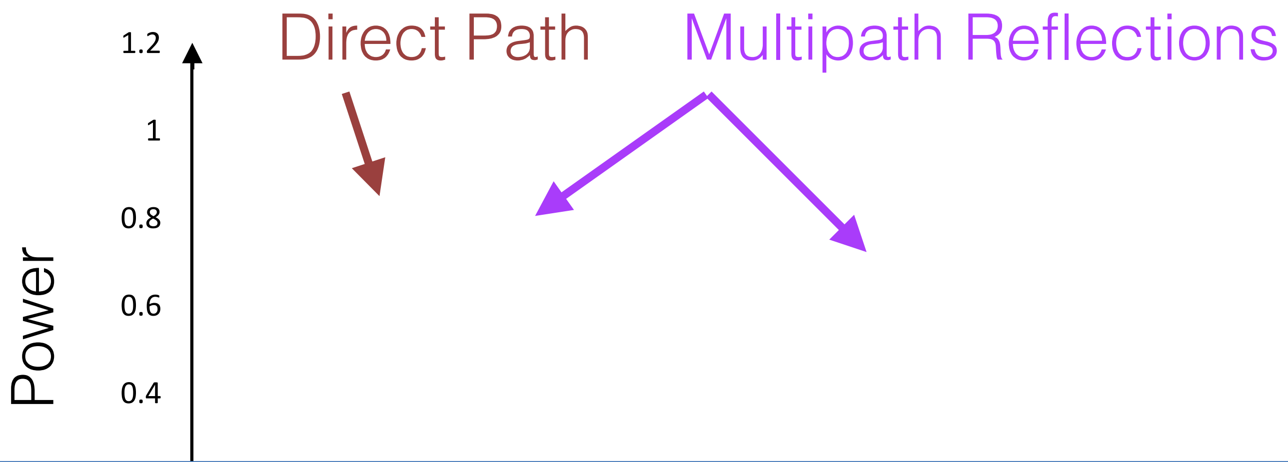


Sensing frequency can be transmitted at ultra-low power and swept over time

From Wide Bandwidth to Accurate Time-of-Flight Estimation

Estimating the Time-of-Flight

- Wide bandwidth can be used to estimate the channel taps in the time domain
  - Perform Inverse Fourier Transform

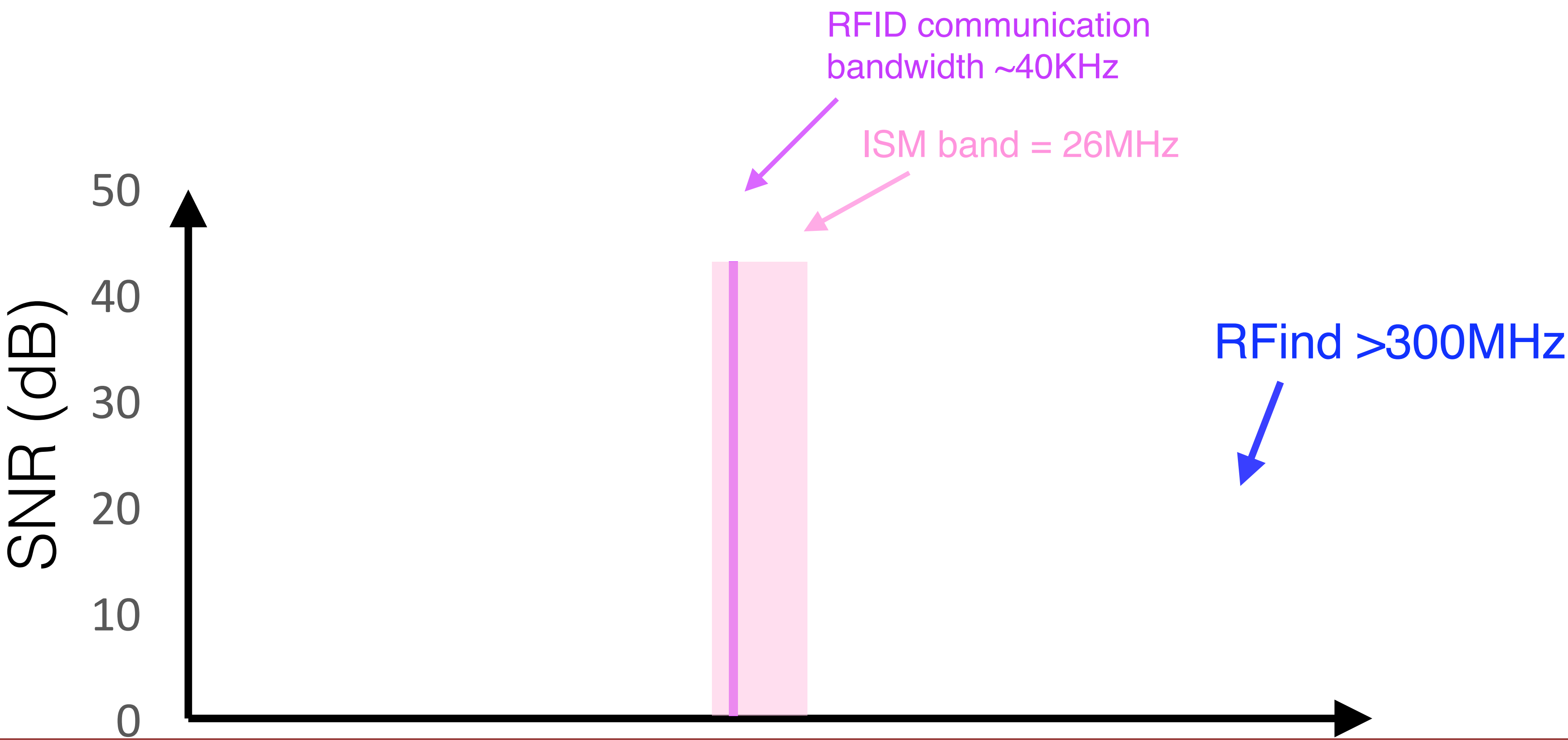


Leverages a super-resolution algorithm using multipath-suppressed phases to achieve high localization accuracy

Implementation & Evaluation

- Reader is implemented on USRP software radios
  - Two for Tx: one high power inside ISM band and another low-power outside ISM
  - Three coherent Rx for 3D localization
- Compliant to EPC Gen2 RFID protocol & FCC regulations
- Evaluation:
  - Tested various off-the-shelf battery-free RFIDs
  - Real indoor environments with multiparty
- Ground truth: Bosch laser measure

How much bandwidth can RFind emulate?



Achieve high SNR over wideband despite ultra-low power of sensing frequency (FCC)

Accuracy vs. Bandwidth

ISM Band Only

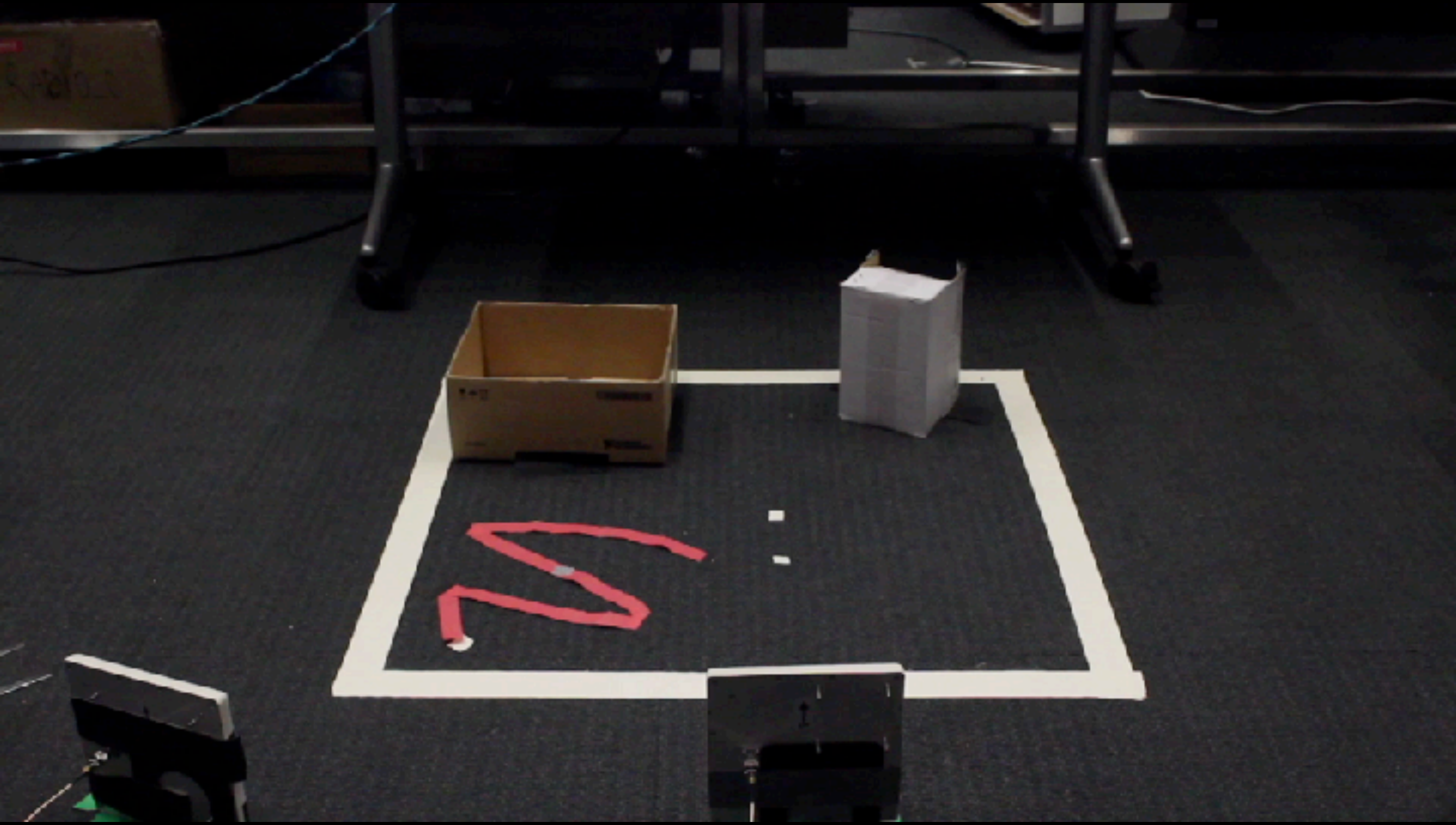
RFind

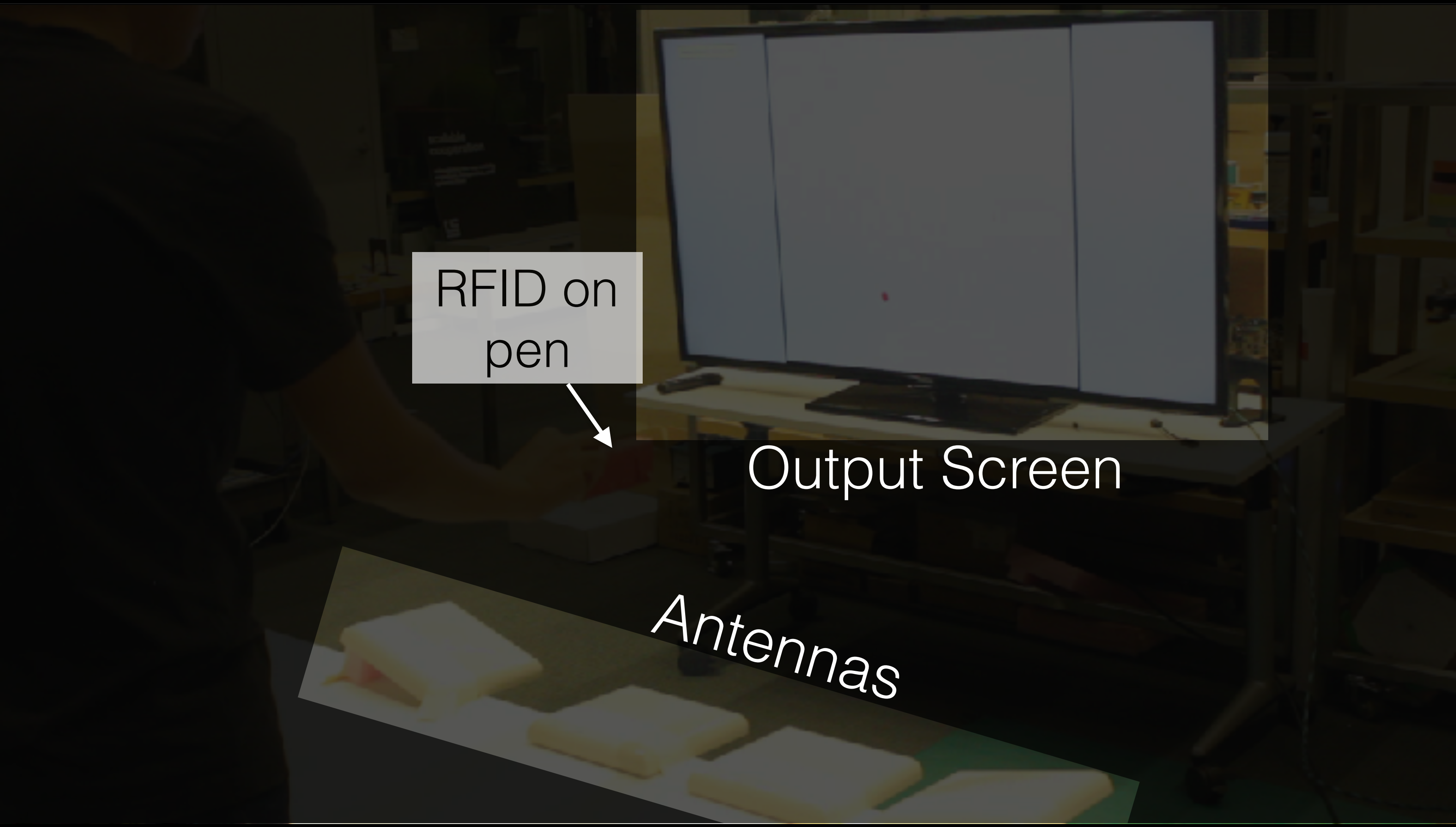
3D Localization Accuracy

90-th percentile error < 3cm

Median error < 1cm

Sub-centimeter accuracy on off-the-shelf battery-free RFIDs despite their very narrow bandwidth




RFID on pen
Output Screen
Antennas

Summary of Lecture

- Battery-free networking and sensing (RFIDs)
- History of RFIDs
- Operation and classes of RFIDs
- Backscatter communication, MAC protocol, efficiency
- Localization using frequency-agnostic backscatter
- Emerging applications: quality control, virtual reality, and robotic automation
- Next frontier?