http://www.mit.edu/~fadel/courses/MAS.s60/index.html

MAS.S60

How to Wirelessly Sense Almost Anything

Lecture 5:
Energy Harvesting & Backscatter Communications

Lecturers

Fadel Adib (fadel@mit.edu)

Aline Eid (alineeid@mit.edu)

TA

Tara Boroushaki (tarab@mit.edu)

This Week in EH and Backscatter

Bridgestone steps up investment in RFID truck tires

13 Oct 2022

Share:

Japanese tire maker aims to expand offering at global sites by 2024

Tokyo – Bridgestone aims to invest "intensively" in the production of RFID-tagged truck & bus tires over the next two years, towards incorpor TBR products.

Wiegand Energy Harvester Opens New Windows to the Internet of Things

Windows to the Internet of Things

TechCrunch+

Market Analysis

Wireless power company Emrod beams 550 W across an Airbus warehouse

The European Space Agency and Airbus teamed up with New Zealand-based startup Emrod to demonstrat...

How to Wirelessly Sense Almost Anything

sensing the physical world & transmitting data wirelessly

sensing via the wireless signals themselves

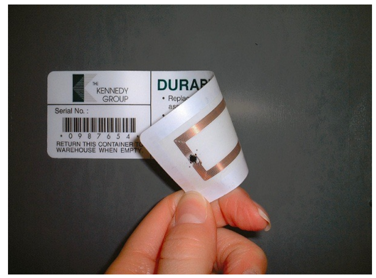
This lecture is a combination of both

Objectives of Today's Lecture

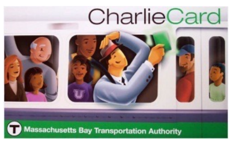
Learn the fundamentals, operation, and applications of
Batteryless IoT Devices

1. How can we make a batteryless IoT device?
2. What is backscatter communication?
3. How does energy harvesting work?
4. How do RFIDs work?
5. How do you unlock new capabilities with RFIDs?

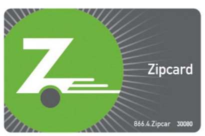
RFID (Radio Frequency IDentification)



Access Control



Security Sensitive Applications

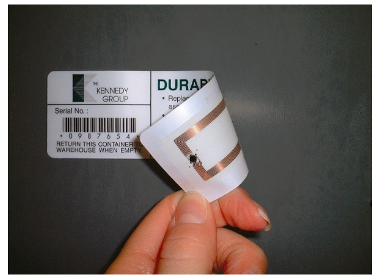


Long-Range Payment Systems

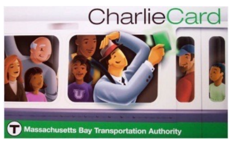
Inventory control

Tracking & Localization

RFID (Radio Frequency IDentification)



Access Control



Inventory control

> 100 Billion in the world

Long-Range Payment Systems

Tracking & Localization

Basic Principle of Operation

RFID: cheap battery-free stickers

Reply to wireless reader
with a unique identifier

Types of RFIDs

Frequency Range

UHF (~900MHz)

HF (13.56MHz)

LF (120-150kHz)

long range (few m)

short range (few cm)

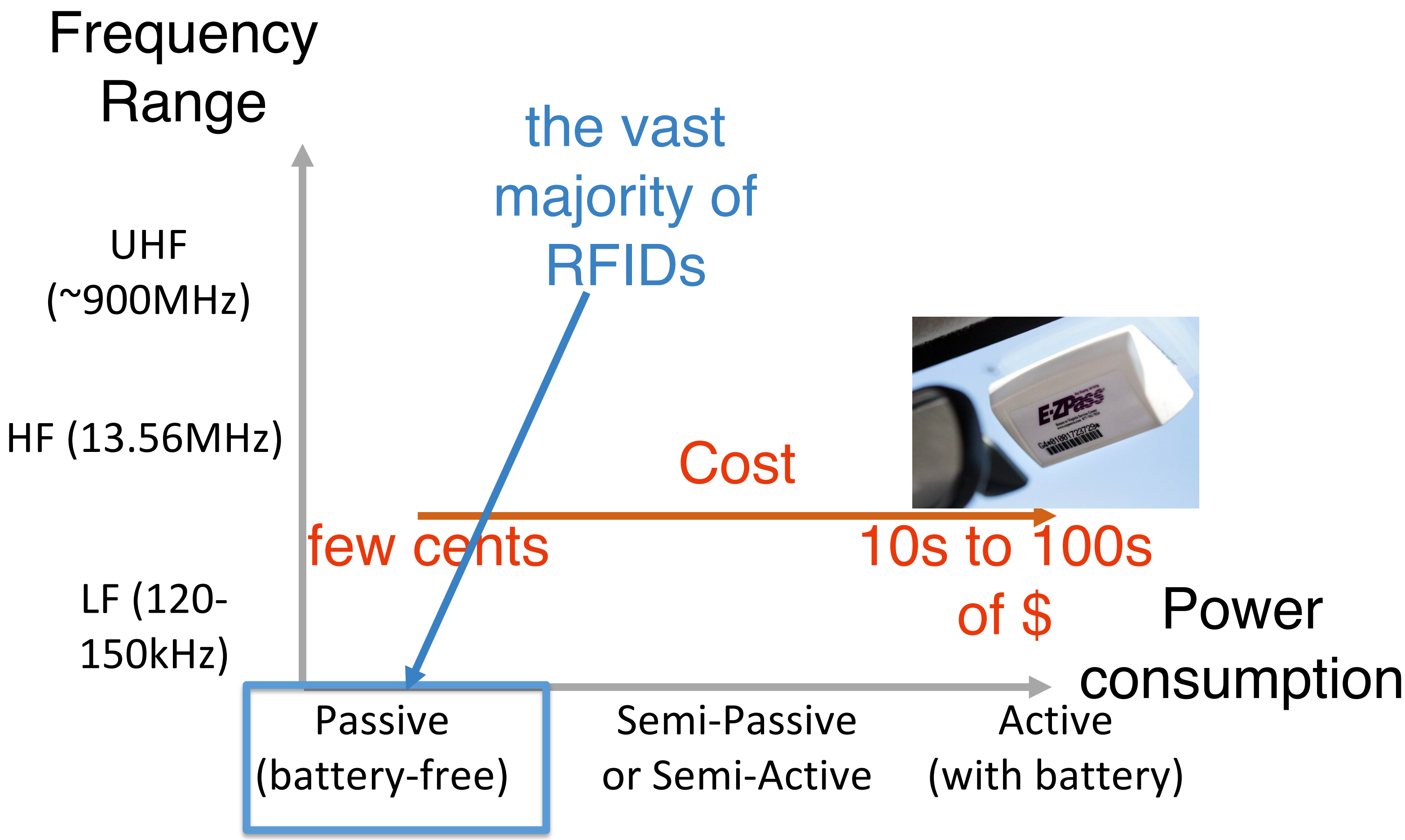
Range of Operation

"need to tap"

Power consumption

Where do these fall?

Types of RFIDs



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

Types of RFIDs

	Passive	**Semi Passive**	**Active**
Power Source	RF (Reader Signal)	Battery/Energy Harvesting	Battery/Energy Harvesting
Communication Scheme	Backscatter	Backscatter	Conventional
Power Consumption	~10 μW	~10 μW	10-100 mW
Communication Range	< 20 m	< 40 m	> 50 m
Cost	~5 c	~2$	>2$

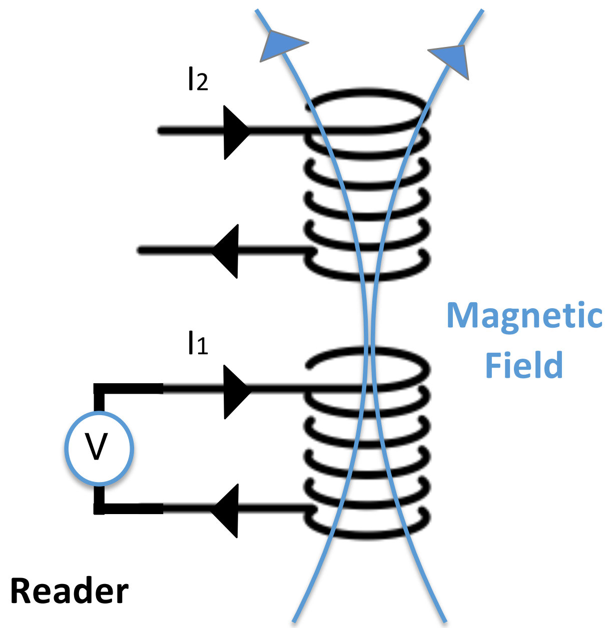
How does an RFID power up?

Harvests Energy from Reader's Signal

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

Inductive Coupling

How to power in HF/LF?



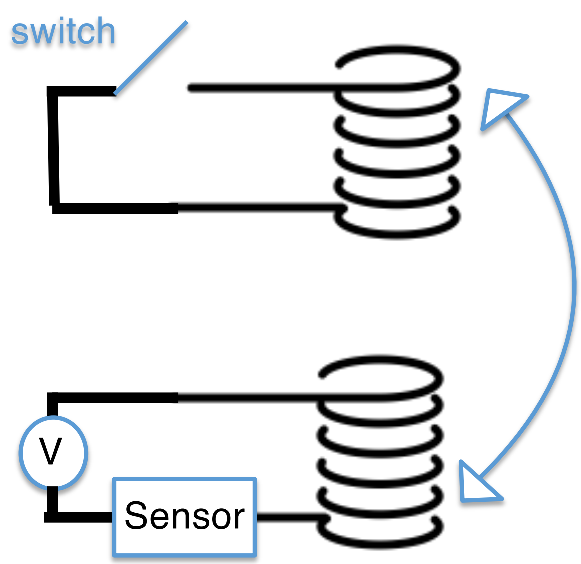
1. Current in reader coil → a magnetic field
2. Magnetic field passes through RFID's coil → current in the RFID
3. RFID harvests energy & powers up

- *What happens if coils misaligned?*
  Magnetic field lines not aligned with RFID's coil → RFID doesn't power up
- Also, magnetic field decays quickly with distance → low operation range

What other technologies operate like this?

Inductive Coupling

- Magnetic field also induced in the reverse direction (mutual inductance)
- By turning a switch (transistor) on/off, the tag can communicate bits that are sensed due to the mutual coupling

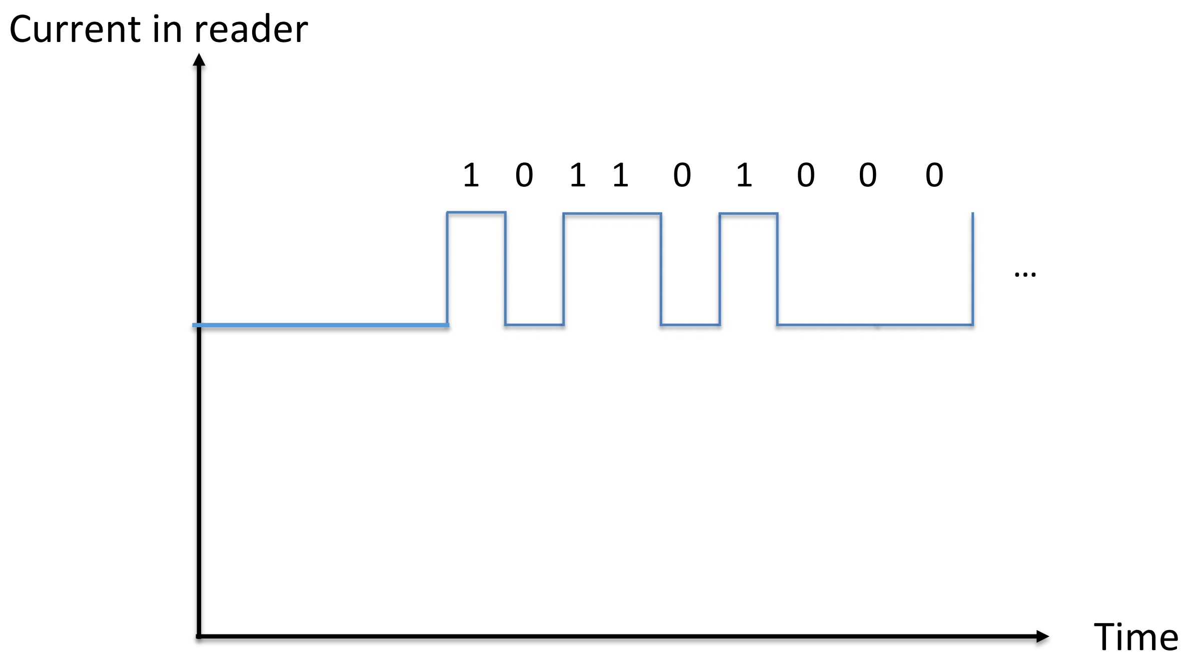


After powering up

1. RFID switch turns on/off (to communicate data in binary)
2. this impacts current in the reader (due to mutual inductance)
3. by sensing current change b/w two states, the reader can decide the transmitted bits

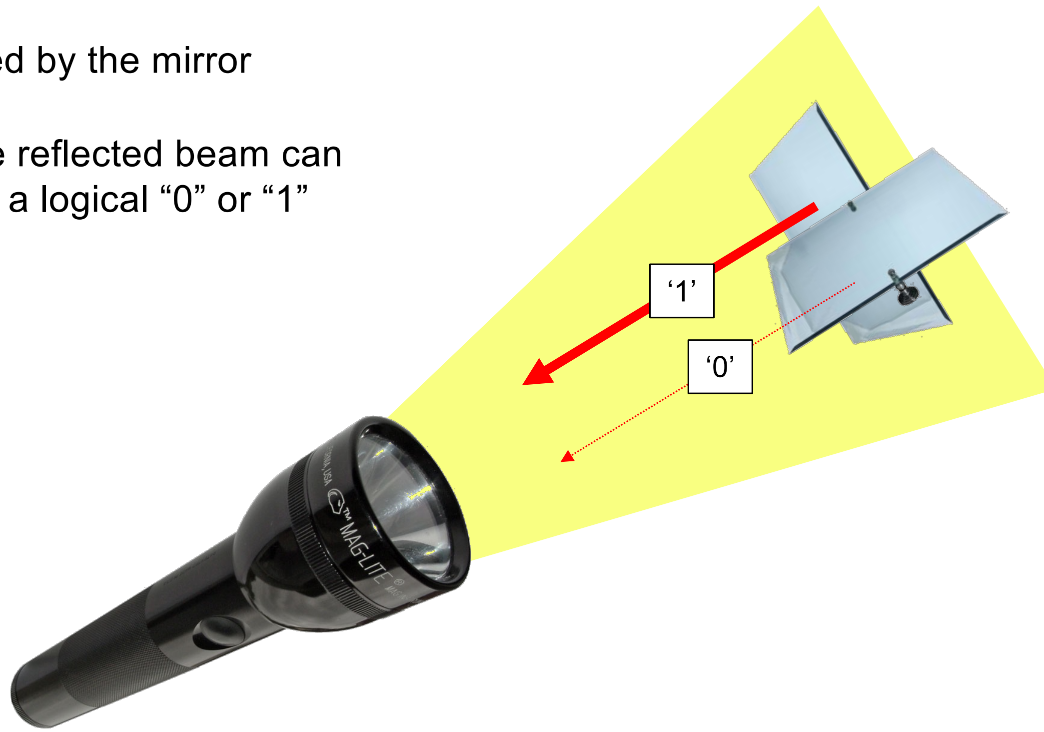
How does the receiver decode?

- Senses changes in the current

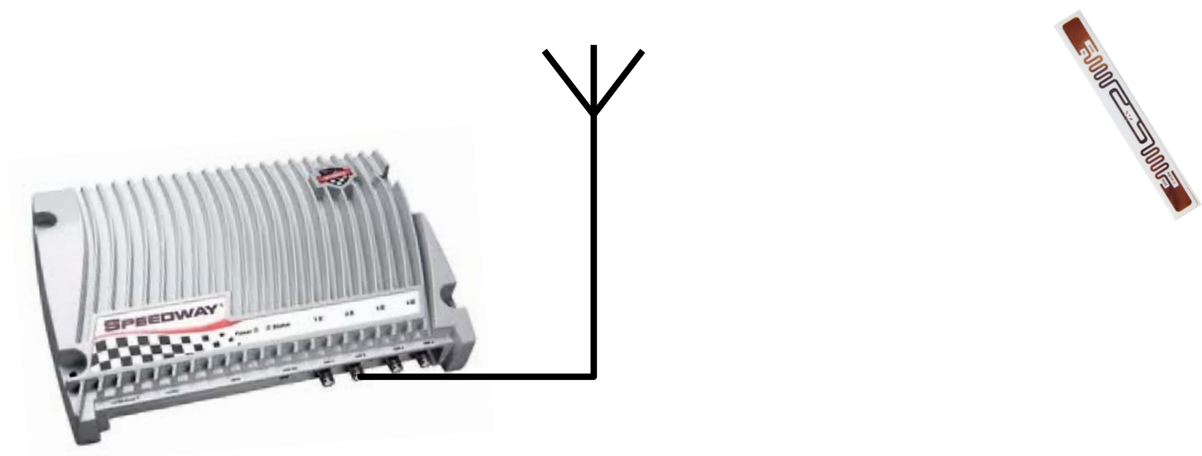


UHF Backscatter Communication

- 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”



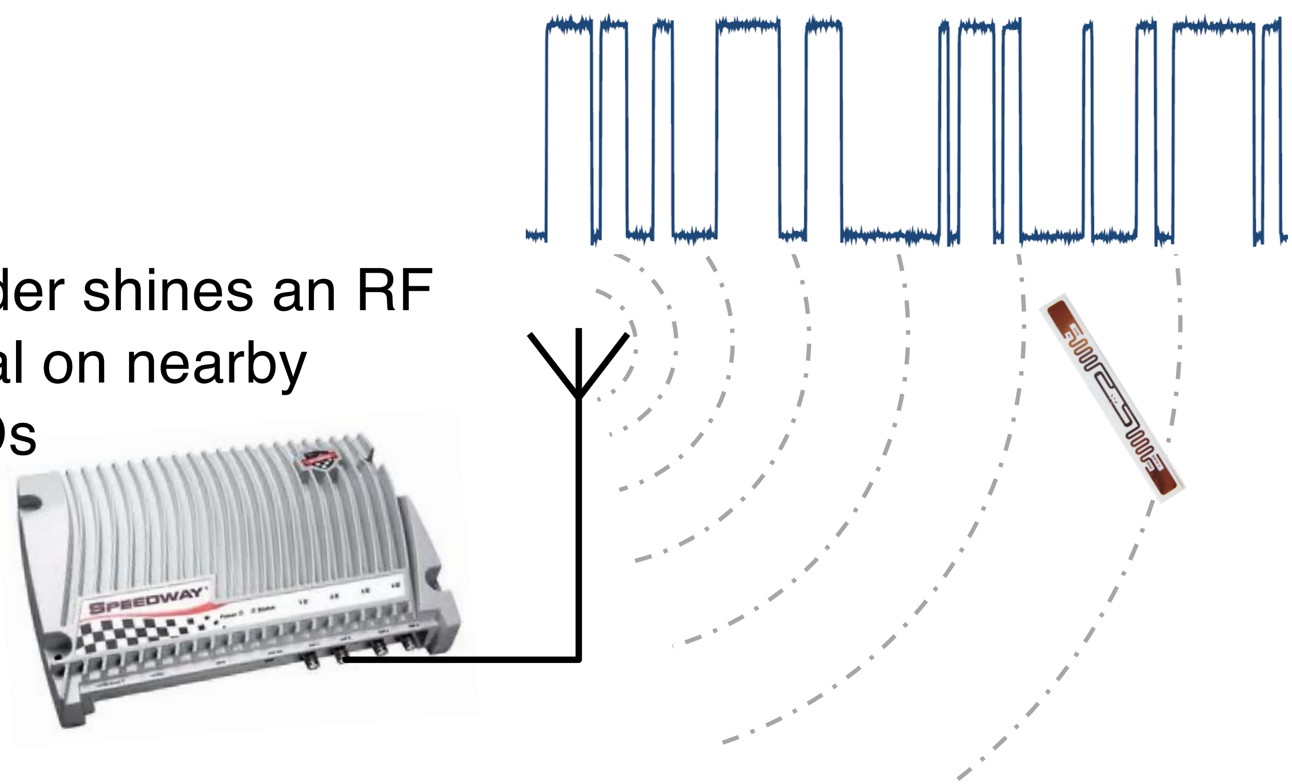
Backscatter Communication



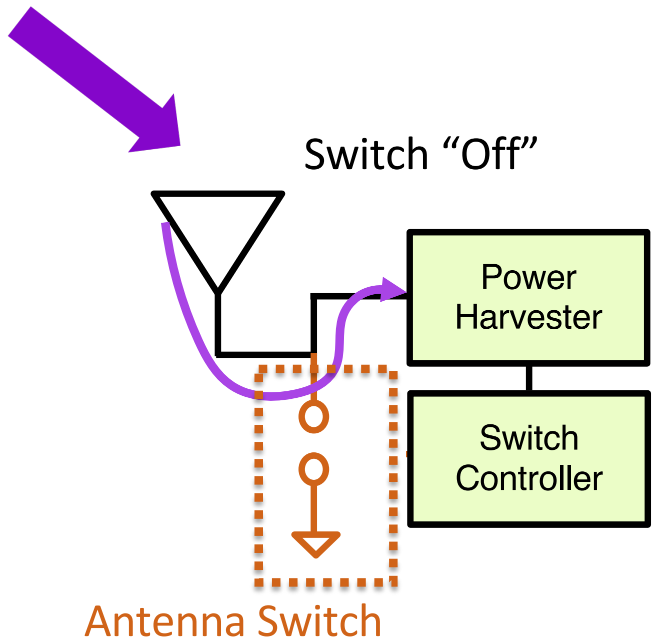
Backscatter Communication

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

Reader shines an RF
signal on nearby
RFIDs

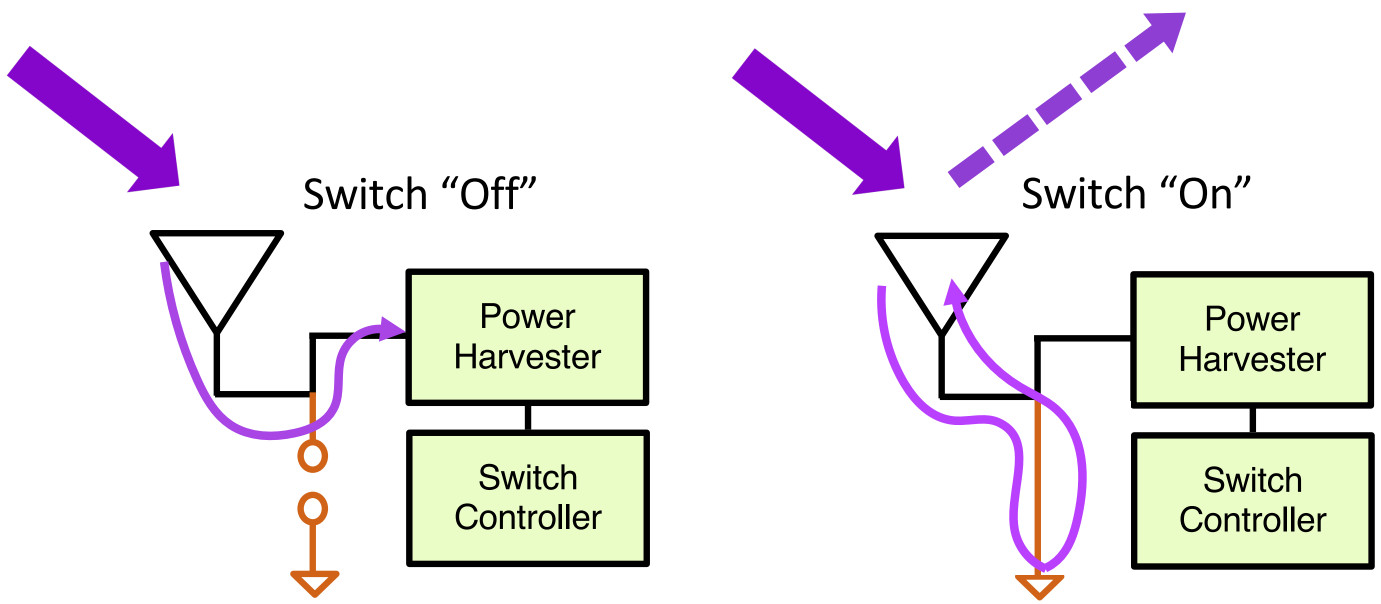


Uplink Communication

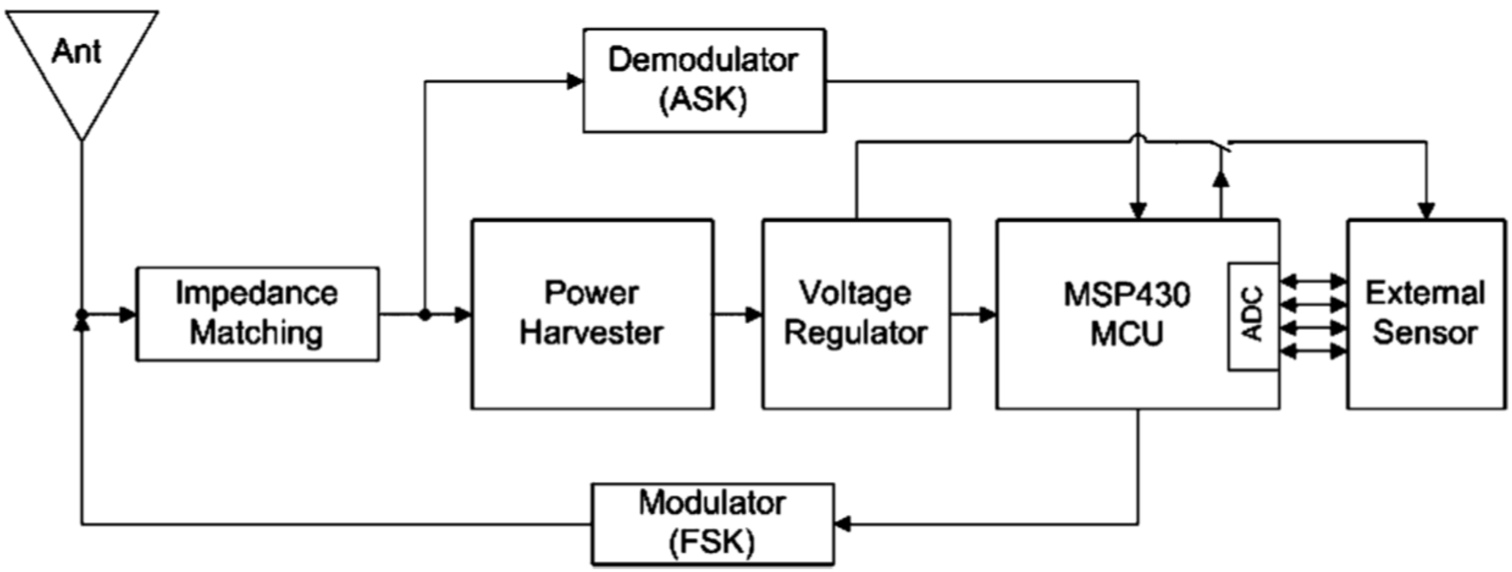


Simplified RFID schematic

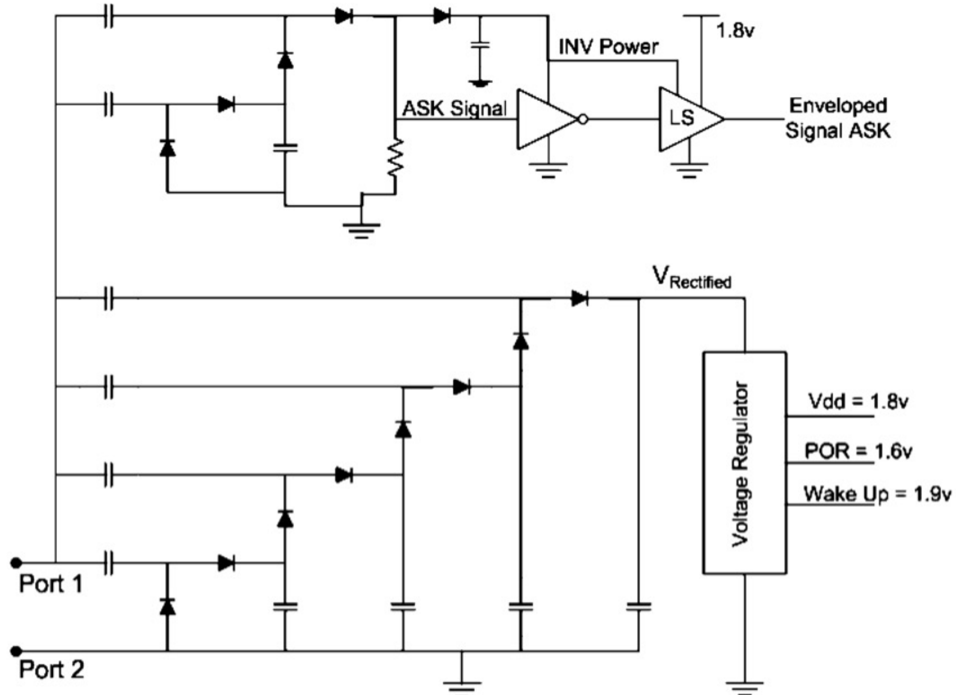
Uplink Communication



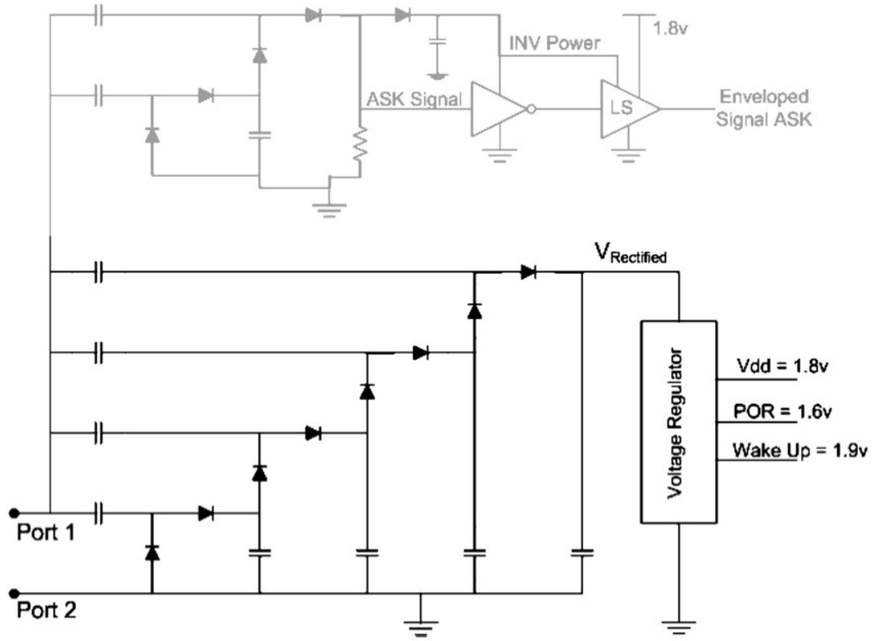
Backscatter Schematic



Demodulation/Harvesting

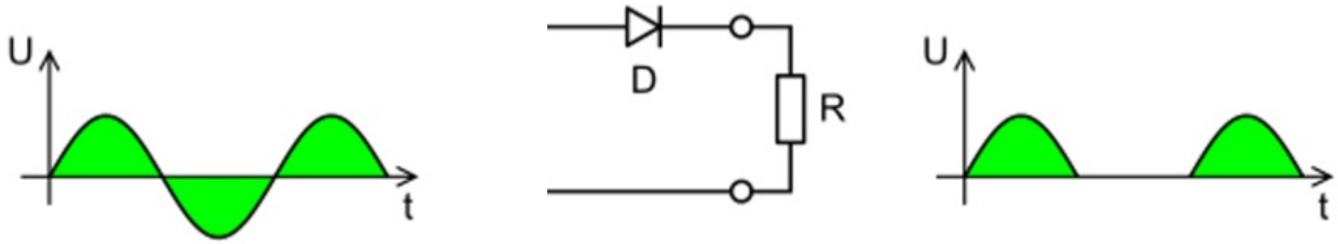


Power Harvester

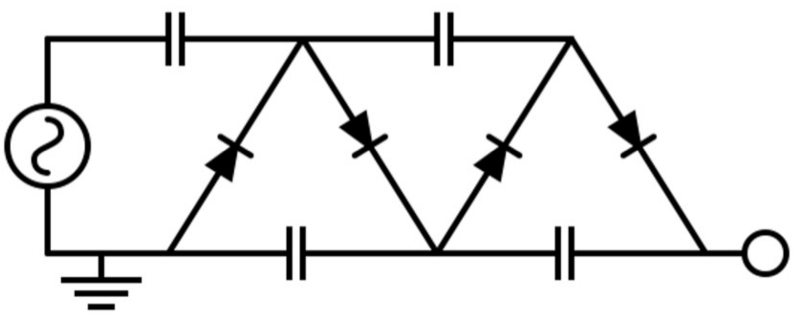


Voltage Rectification

A rectifier is an electrical device that converts alternating current (AC), which periodically reverses direction, to direct current (DC), which flows in only one direction.



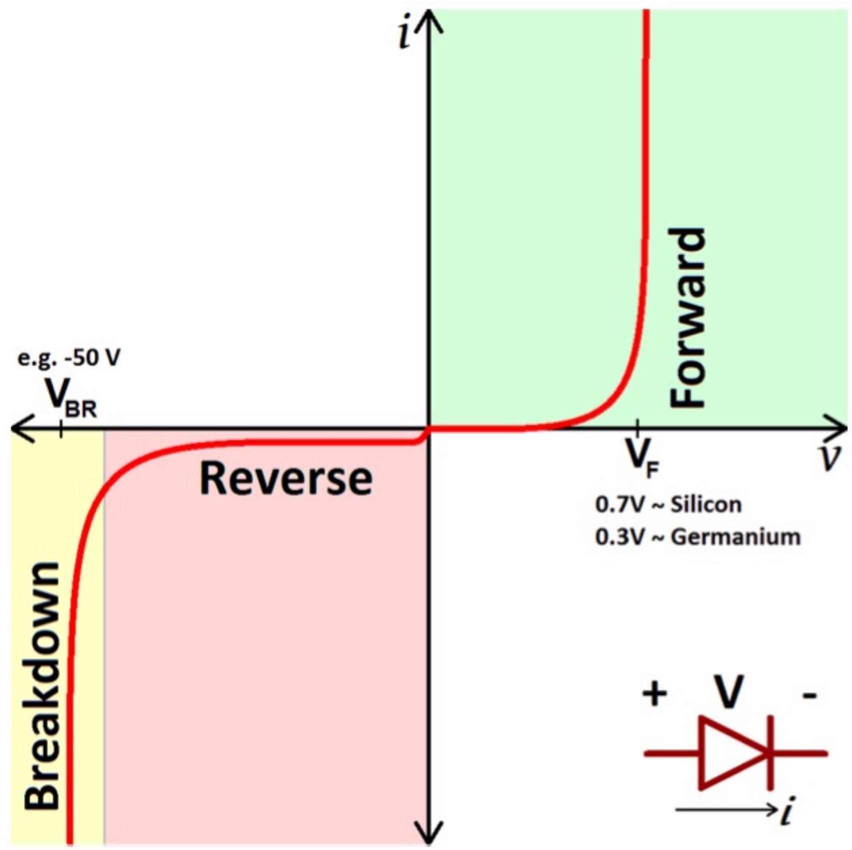
Half-wave rectifier



Voltage-multiplying rectifiers

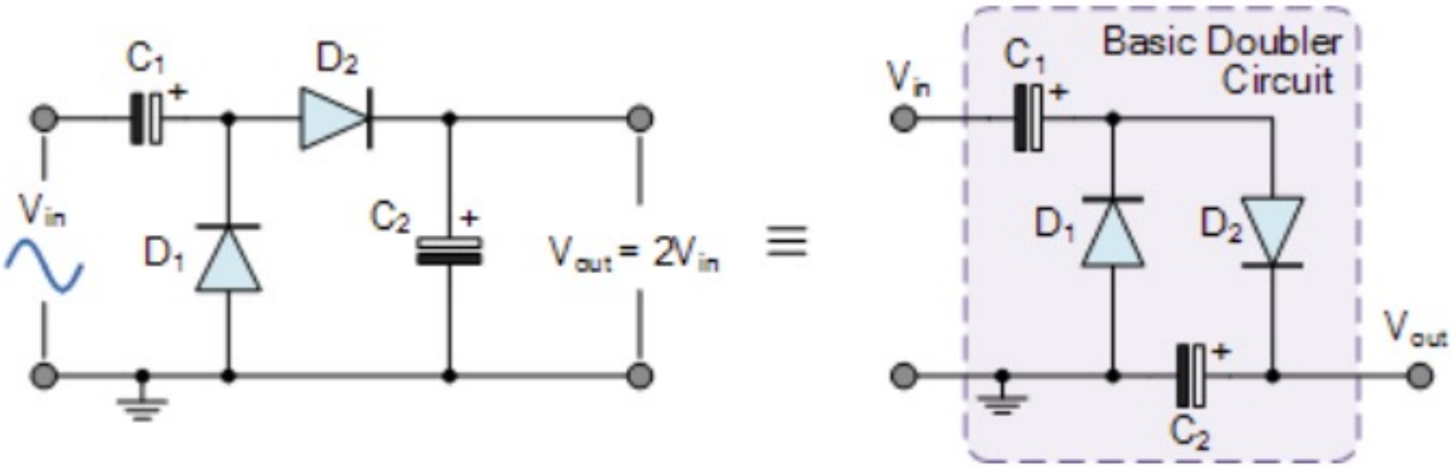
Voltage Rectification

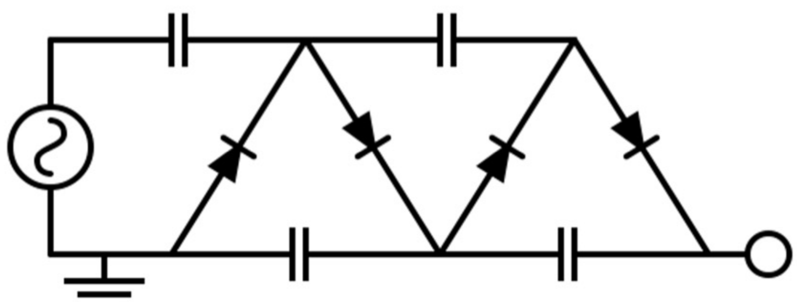
Schottky Diode I-V Curve



Diode

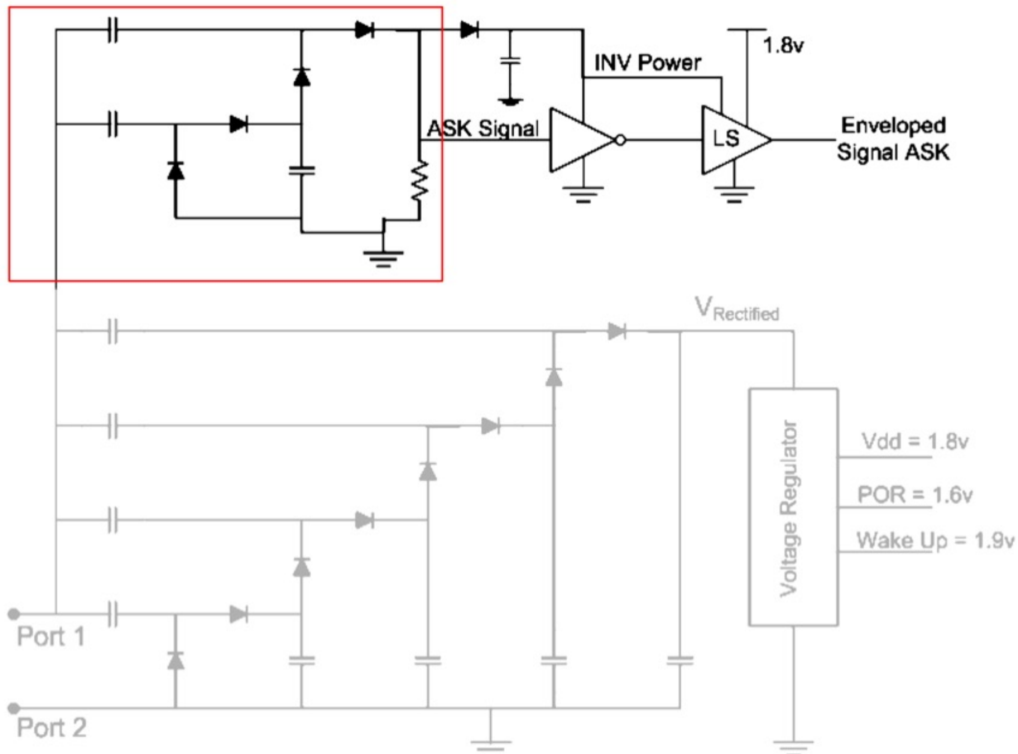
Voltage Rectification-Voltage Doubler



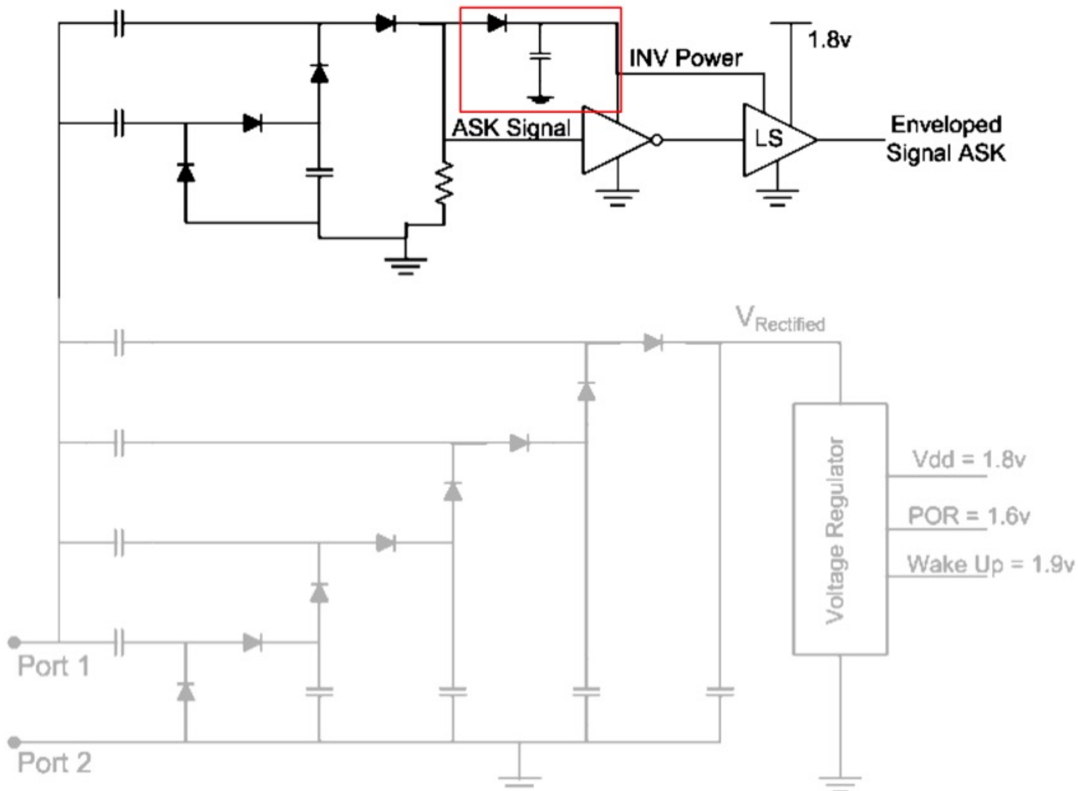


Voltage Quadrupler

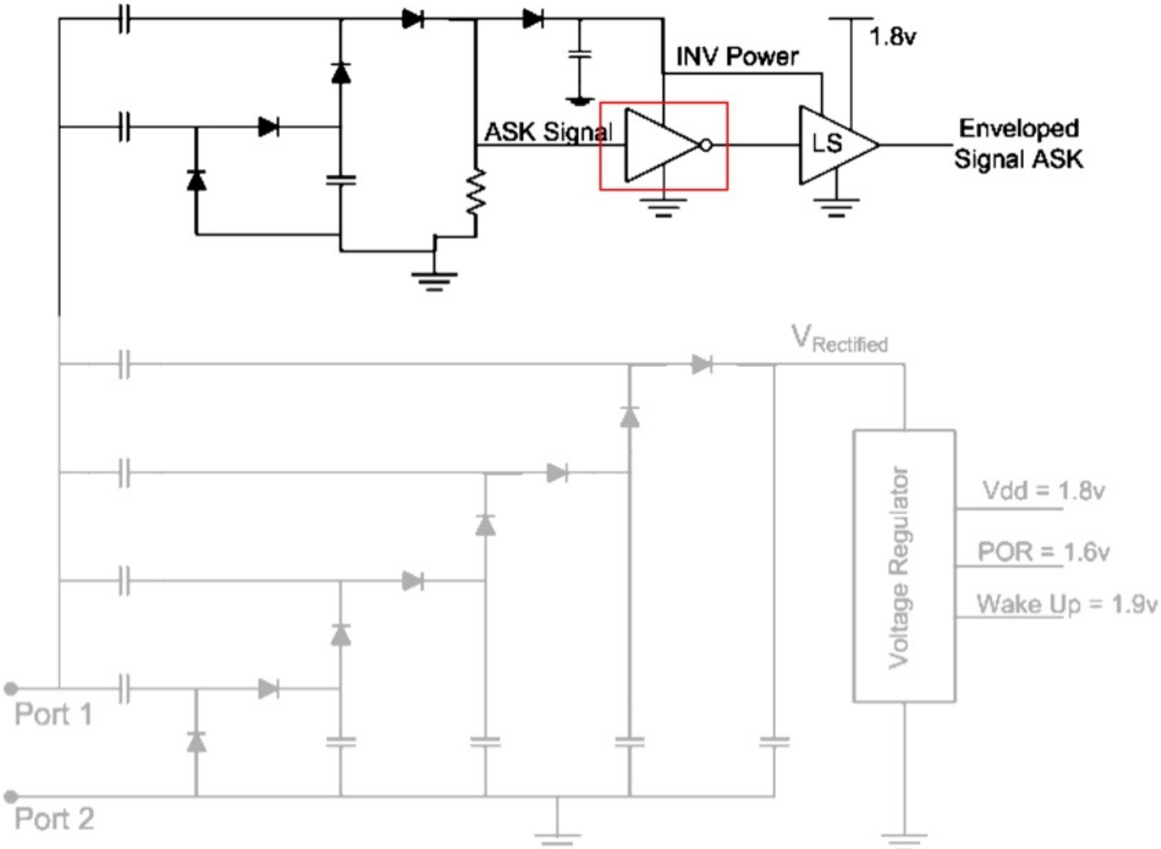
Demodulation

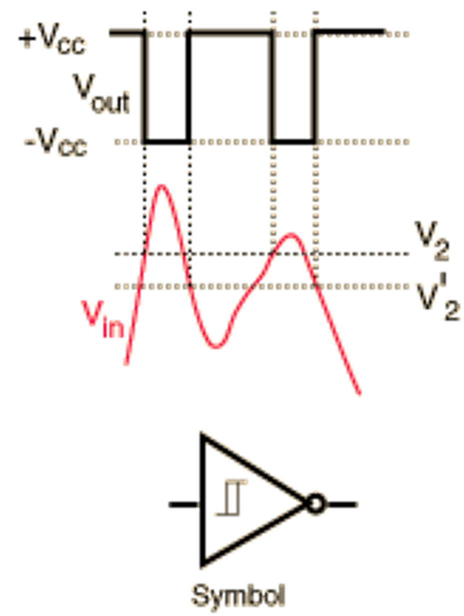


Demodulation

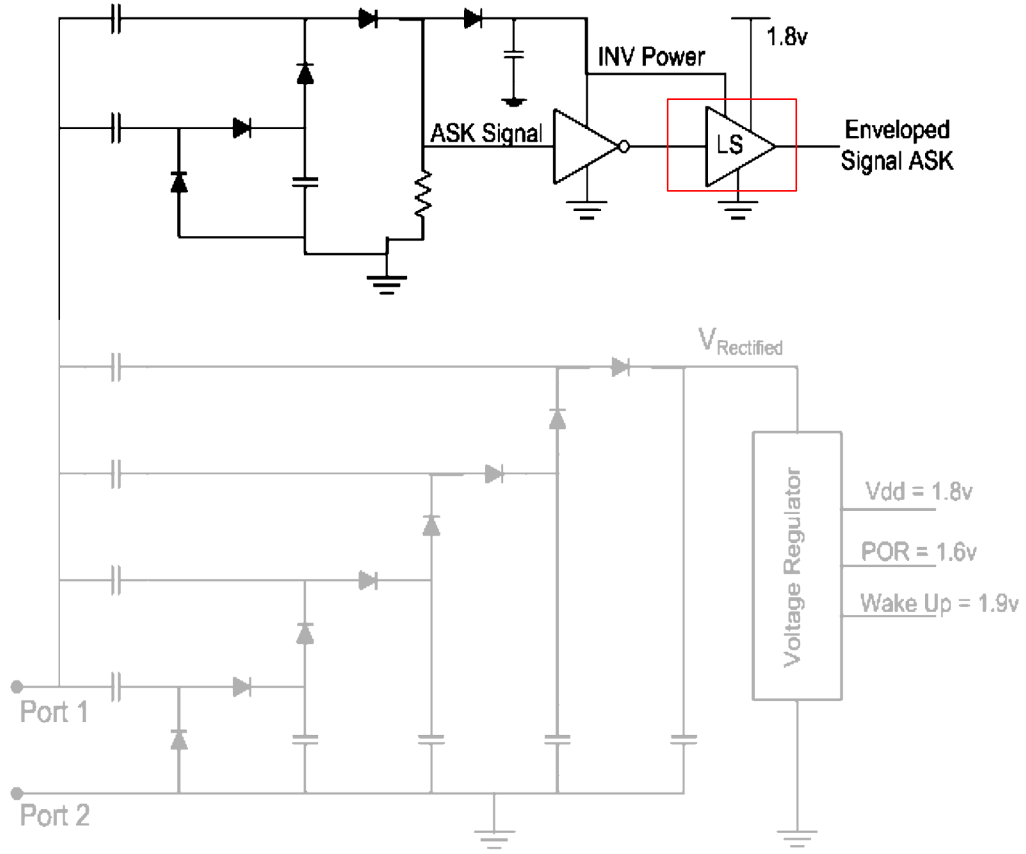


Demodulation





Demodulation

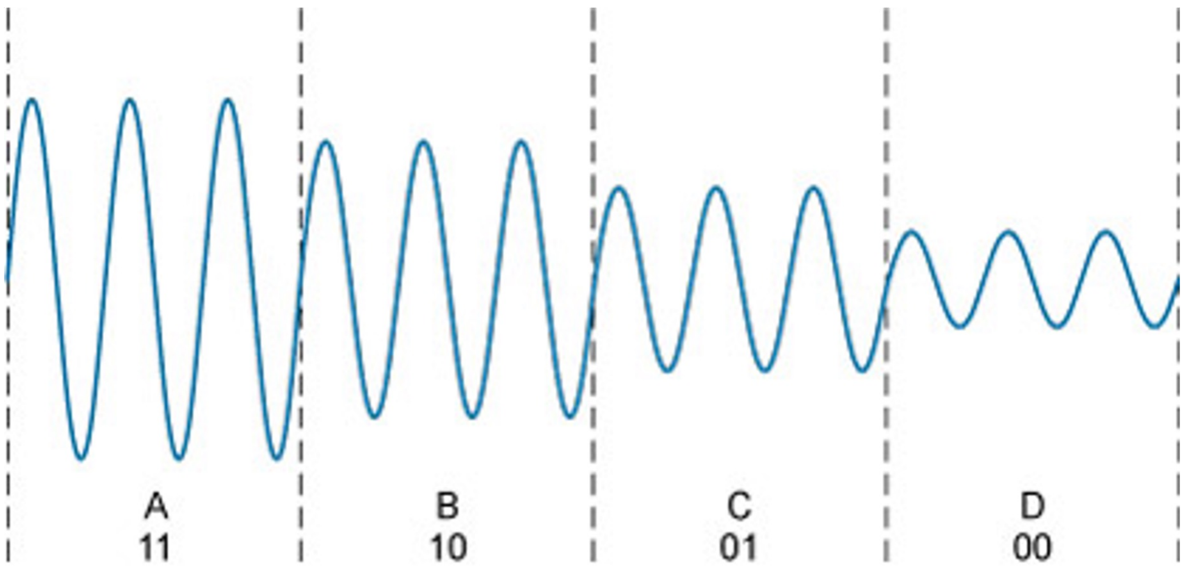


ASK: Amplitude-Shift Keying

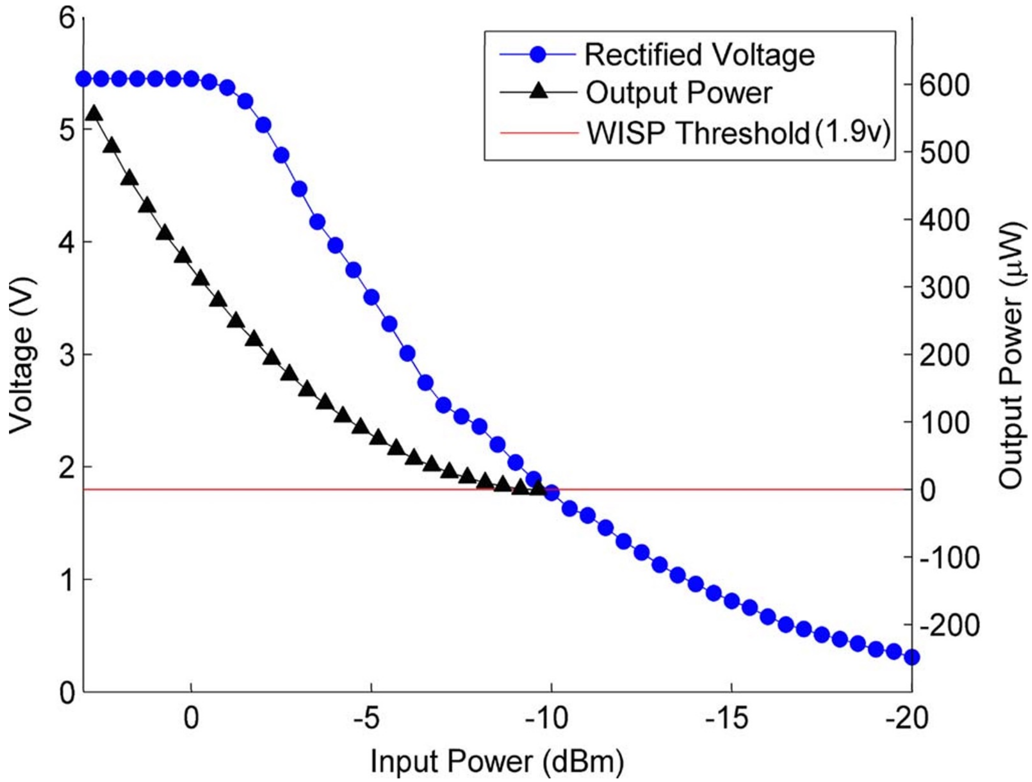
ASK Modulated Input Wave

Demodulated Output Binary Sequence

ASK: Amplitude-Shift Keying

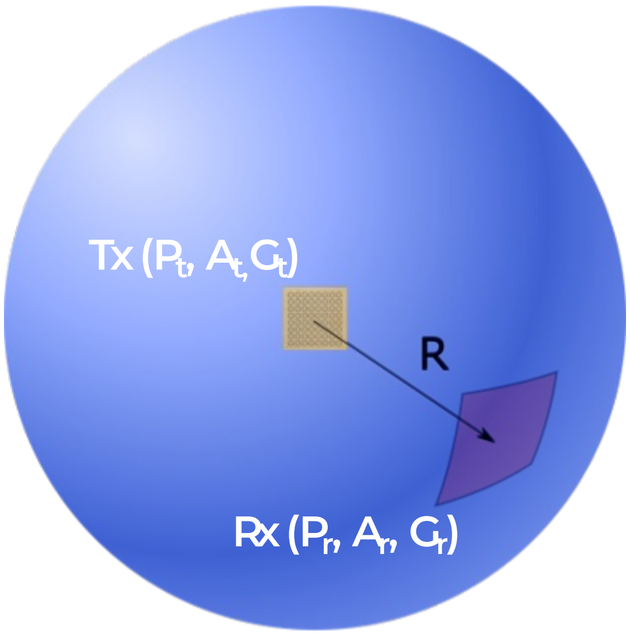


Power Budget



Operating threshold of -9.5dBm

Friis Equation



Receiver Aperture

$$P_r = P_t G_t \frac{A_r}{4\pi R^2}$$

Tx Antenna Gain

$$A_r = \frac{G_r \lambda^2}{4\pi}$$

Inverse Path Loss

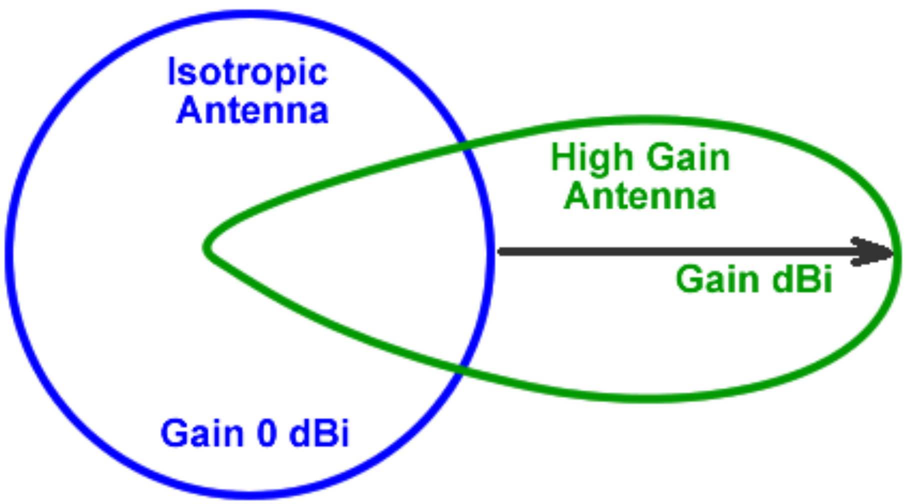
$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2$$

Power Budget

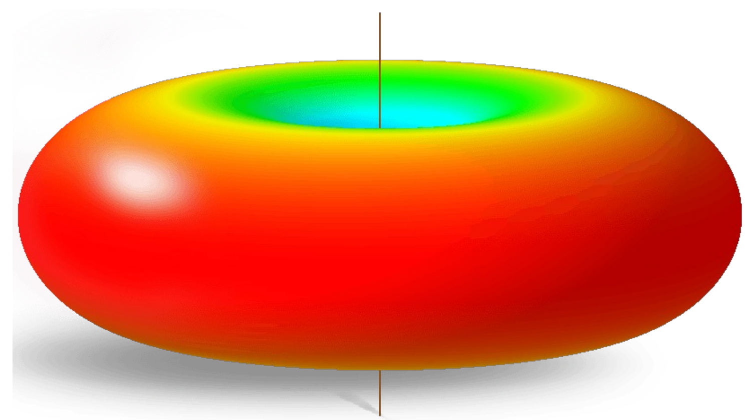
$$P_r = P_t - 20log\left(\frac{4\pi R}{\lambda}\right) + G_t + G_r - L_P$$

Gain

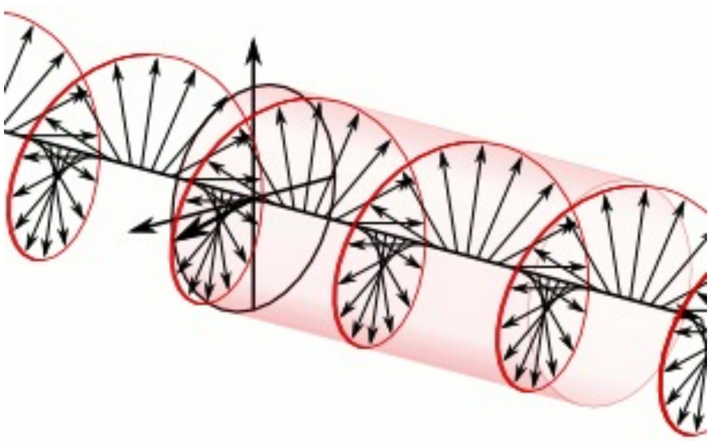
Measure of how well you can focalize your power



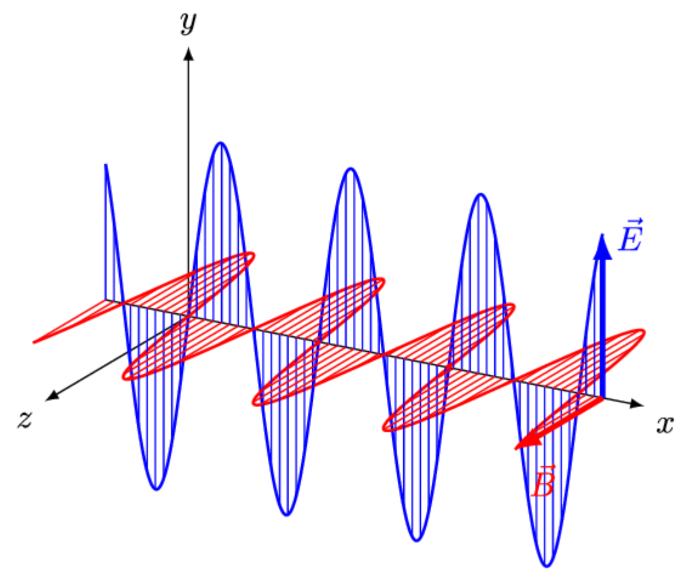
Dipole Antenna on tags: 2dBi



Antenna Polarization



Circular Polarization



Vertical Polarization

Power Budget

$$P_r = P_t - 20log\left(\frac{4\pi R}{\lambda}\right) + G_t + G_r - L_P$$

- P_T = 1 W = 30 dBm
- G_T = 6 dBi (regulatory limit)
- G_R = 2 dBi (dipole antenna)
- λ = 0.33m (915 MHz)
- L_P = 3 dB

→ Maximum Operational Range of 4.3m

Link Budget – 2 way

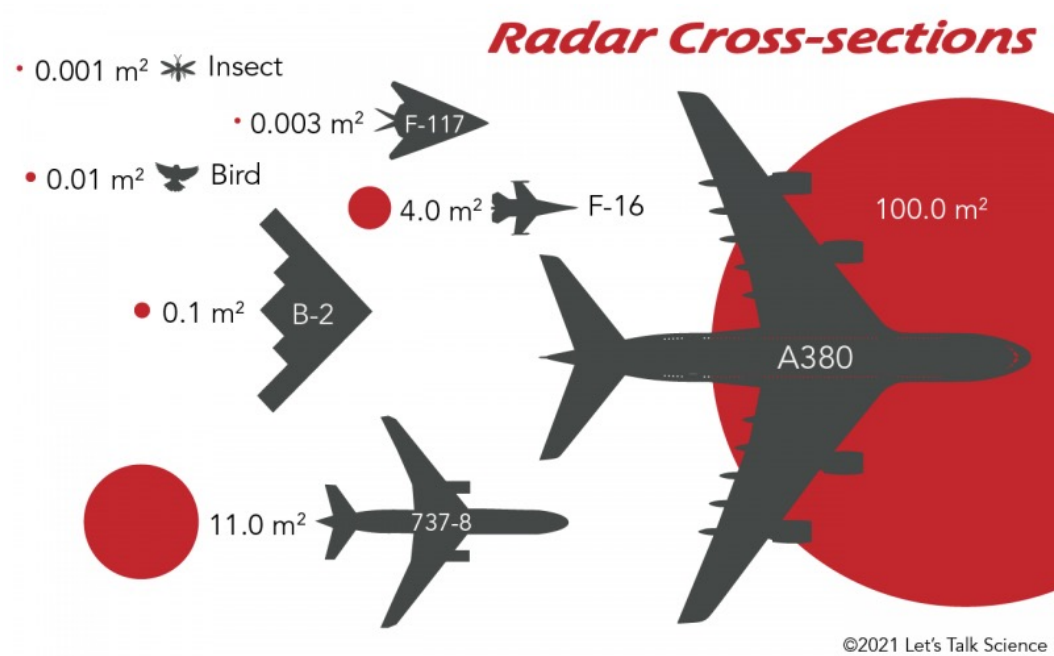
1-way: $P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2$ $G_r = \frac{A_r 4\pi}{\lambda^2}$ $\sigma = \frac{4\pi A_r^2}{\lambda^2}$

2-way: $P_r = P_t G_t^2 G_r^2 \left(\frac{\lambda}{4\pi R}\right)^4$ $P_r = P_t G_t^2 A_r^2 \frac{1}{(4\pi)^2 R^4}$ $P_r = P_t G_t^2 \frac{\sigma\lambda^2}{(4\pi)^3 R^4}$

→The larger the tag is, the higher the power received on the reader

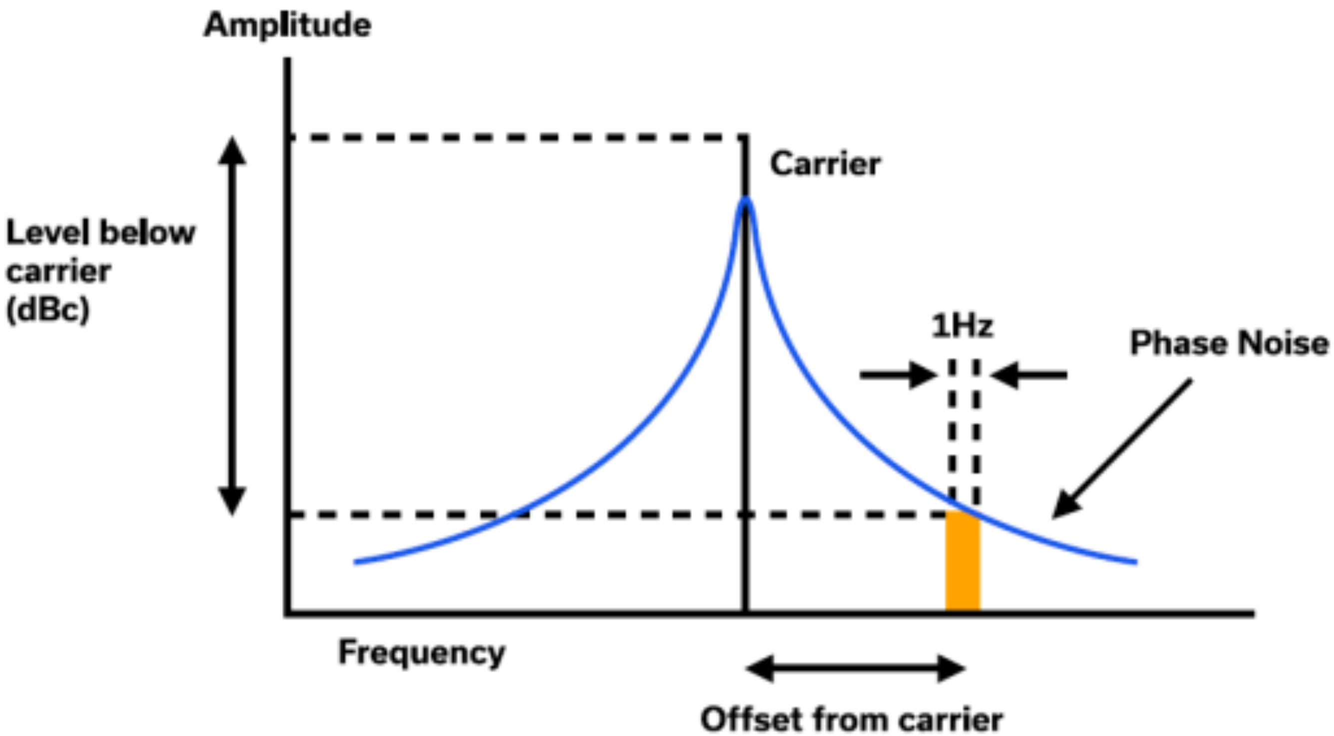
→Similar to radar: RCS

Speaking of RCS: The measure of Stealth



RFID Tag has RCS of 0.0025 m^2

Reader Sensitivity-Phase Noise



Maximum Communication Range

$$S = P_t - IL \ - PN + 10\log(BW)$$

$$P_r > S$$

$$P_t + 2G_t + 2G_r - 40log\left(\frac{4\pi R}{\lambda}\right) > P_t - IL \ - PN + 10\log(BW)$$

$$2G_t + 2G_r - 40log\left(\frac{4\pi R}{\lambda}\right) + \mathrm{IL} + \mathrm{PN} \ - 10\log(\mathrm{BW}) > 0$$

→ Maximum Communication Range of 24m

Power Budget

$$\frac{P_{\text{out}}}{P_{\text{active}}} = \frac{T_{\text{on}}}{T_{\text{on}} + T_{\text{sleep}}} = \text{Duty cycle}$$

1.8 V * 600 µA = 1.08 mW

Output power available at 0 dBm input is 310 µW (from previous figure).

310 µW / 1.12 mW → 27%

Energy Consumption

$$\frac{P_{\text{out}}}{P_{\text{active}}} = \frac{T_{\text{on}}}{T_{\text{on}} + T_{\text{sleep}}} = \text{Duty cycle}$$

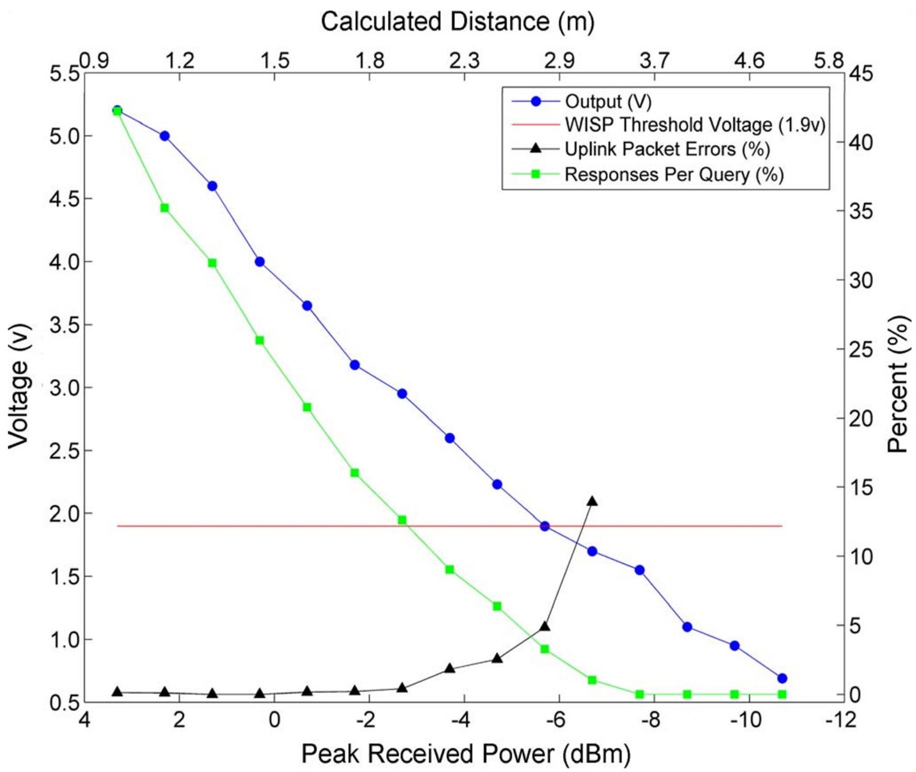
1.8 V * 600 μA = 1.08 mW

Query time is 2ms: 2 ms * 1.08 mW = 2.16 μJ.

Energy in capacitor is $C\,V^2/2$. For C = 10 μF, baseline energy is 10 μF * $(1.8\text{ V})^2 / 2$ = 16.2 μJ

$C\,V^2 / 2$ = 16.2 μJ + 2.16 μJ ⇒ V = 1.916, in order to complete the query.

Evaluation

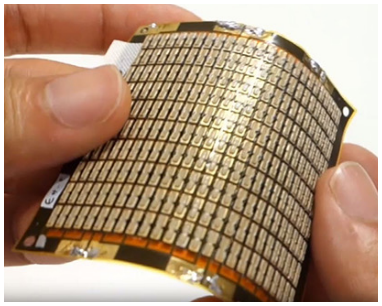


Observation:
WISP turns on around -5.9dBm

Alternative Power Sources

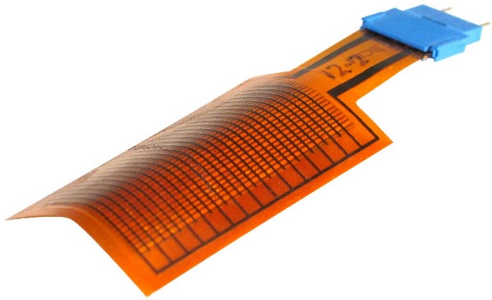
Solar Energy:

- Unpredictable source
- Intermittent supply



Thermal Energy:

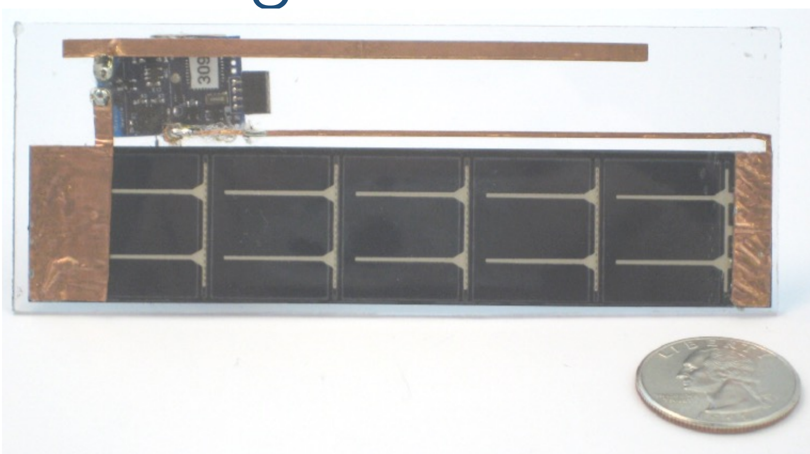
- Low efficiency
- Limited applicability

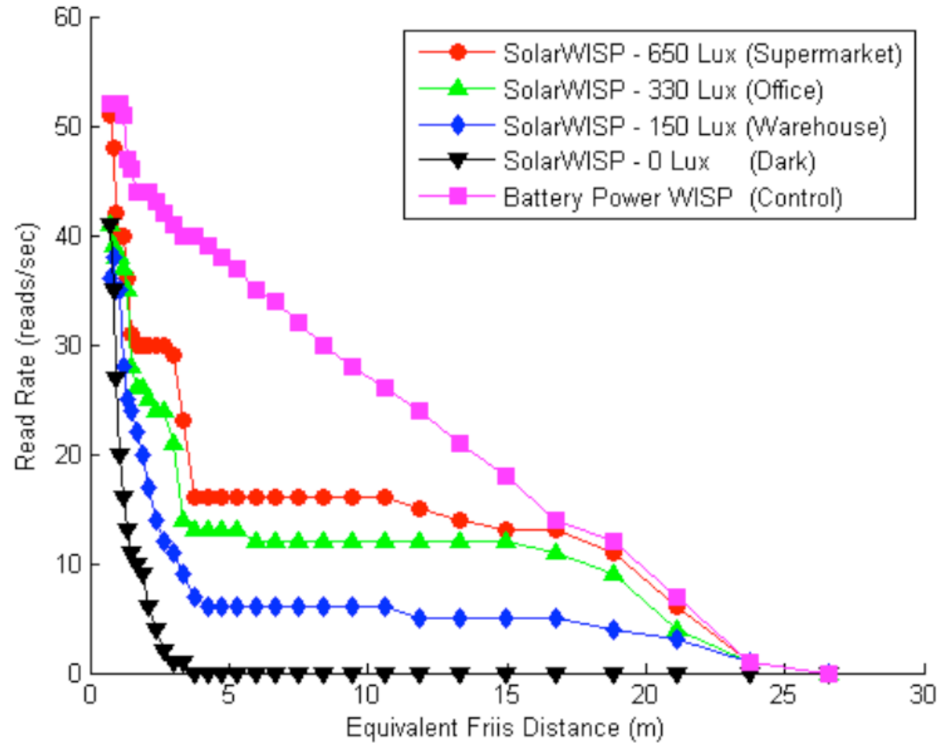


Mechanical/Vibrational Energy:

- Material degradation with time
- Limited applicability

Enhanced WISP Range with Solar Powered Tag



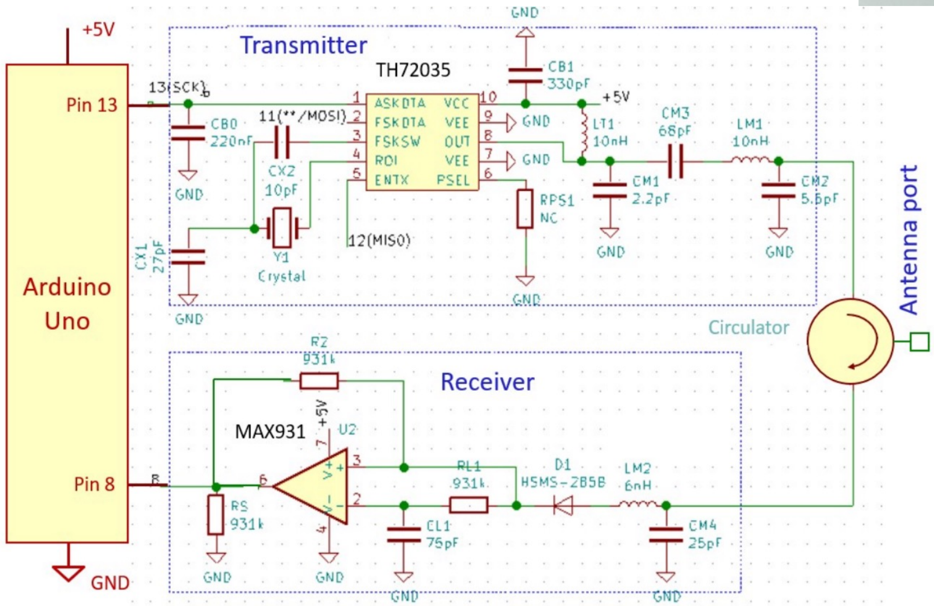


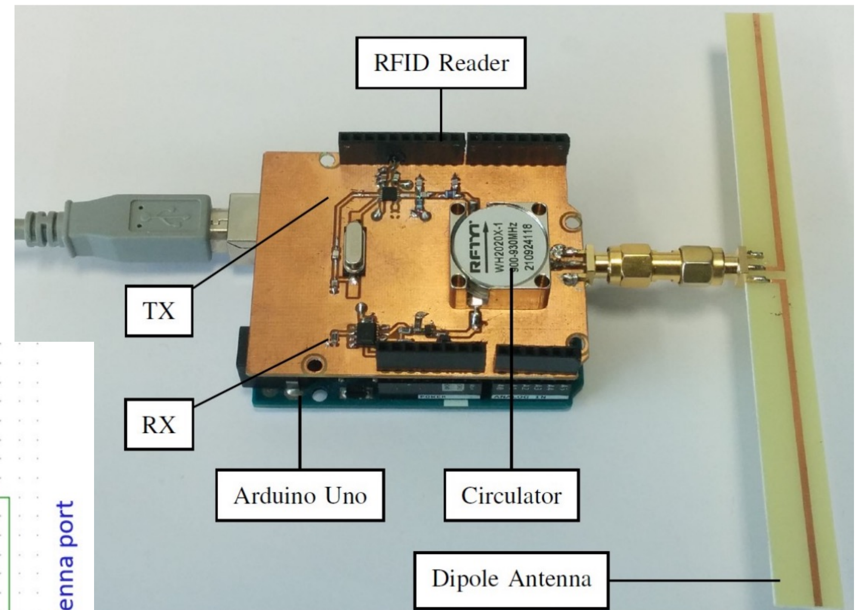
Simple Low-Cost UHF RFID Reader

Reader capable of:

- generating any commands defined by the EPC Gen2 RFID protocol
- processing tag response in real time.

A project idea?





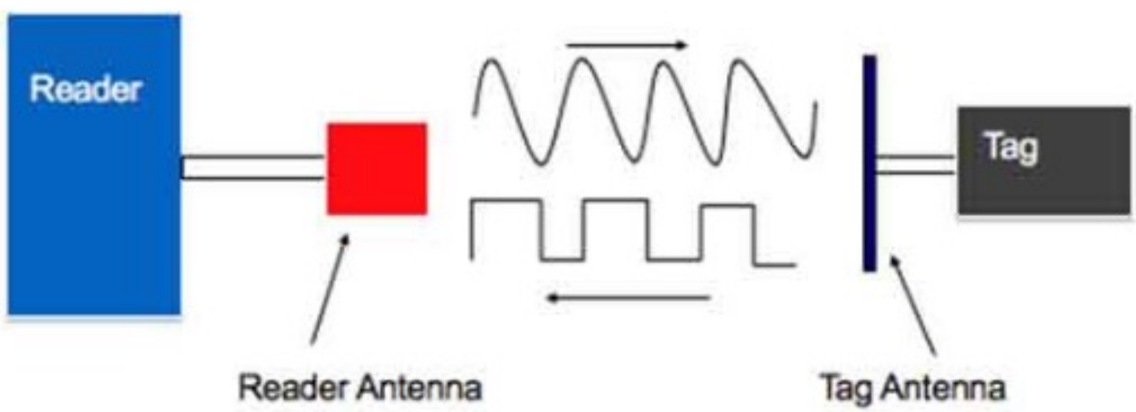
Unlocking New Capabilities with Deployed RFID Tags

Example: RFind

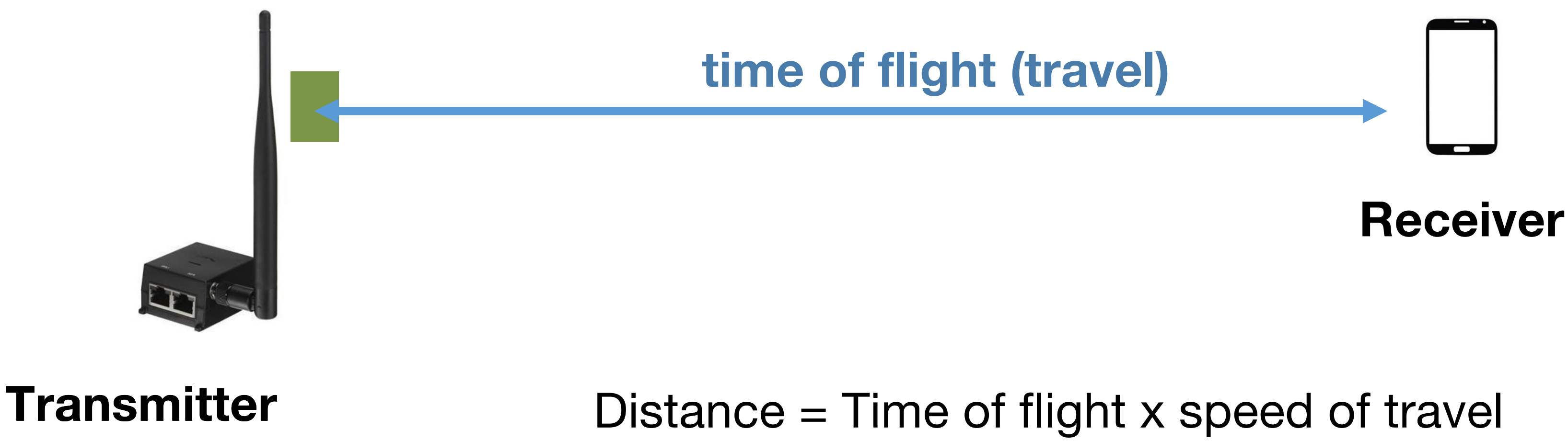
Motivation

- Can we use these battery-less stickers called RFIDs to get sub-centimeter localization in 3D space?

- RFIDs communicate with a wireless reader by switching their impedance when the reader excites them with a specific carrier frequency. RFind uses this property to compute the time of flight (TOF) for localization



Measuring the Time-of-Flight (ToF)



Distance = Time of flight x speed of travel

Can use trilateration (intersection circles/spheres)

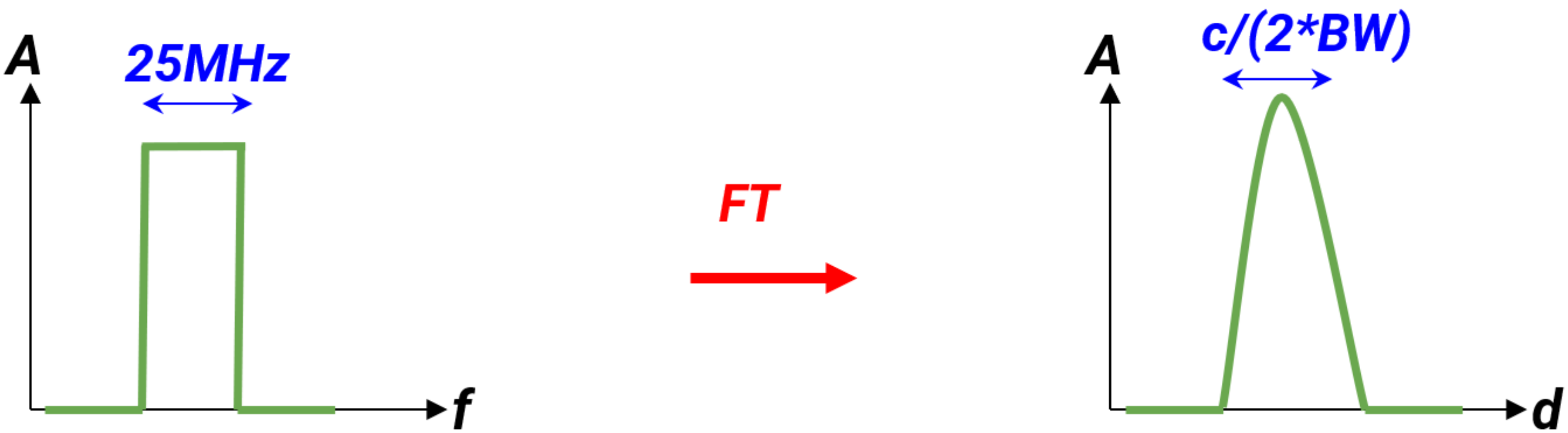
How do we know when the signal was transmitted?

Why and where do we need high accuracy localization?



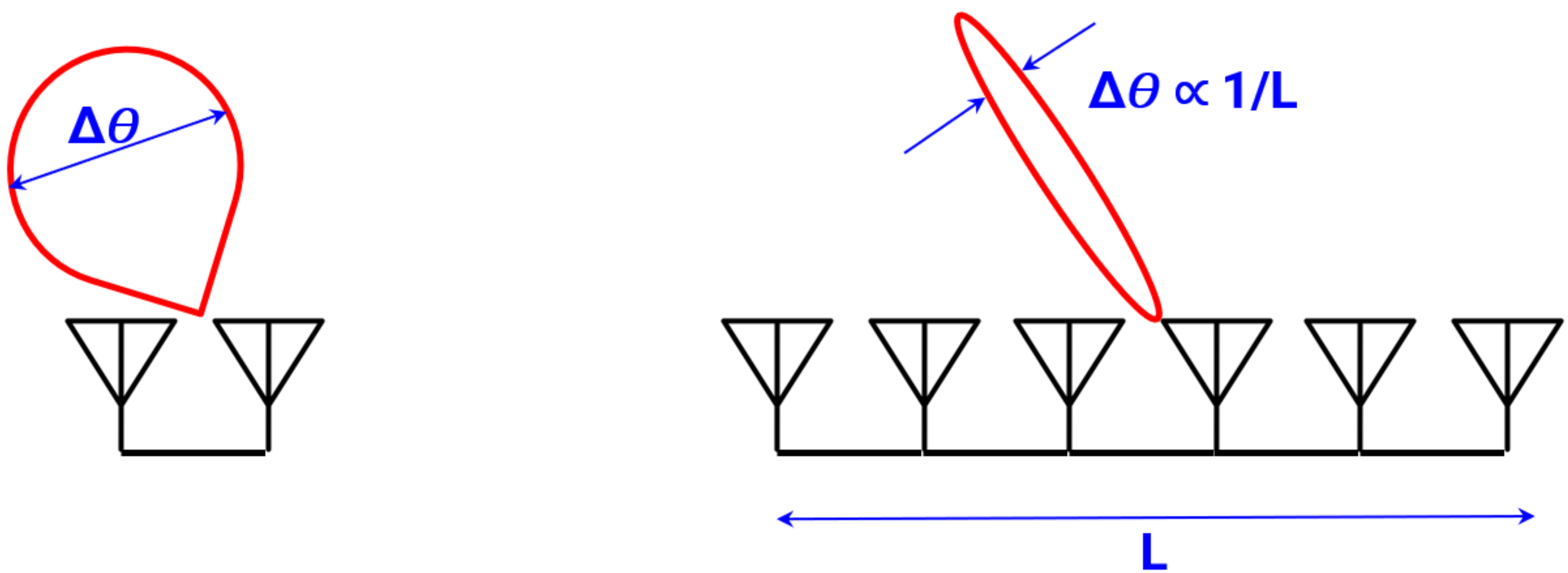

How can we achieve high accuracy localization?

- Large Bandwidths



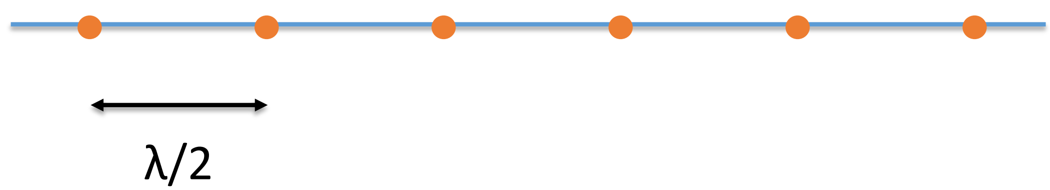
How can we achieve high accuracy localization?

- Large Antenna Arrays



How can we achieve high accuracy localization?

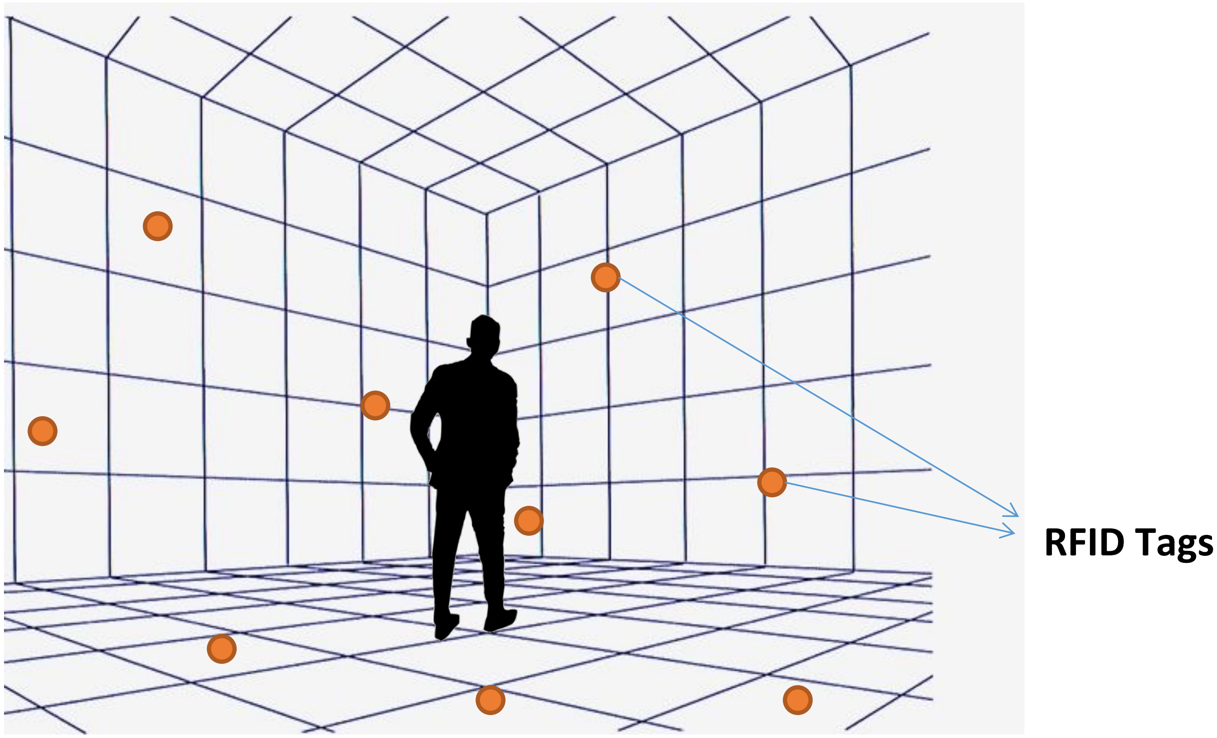
- Using Phase



λ = 30cm (at 900MHz) → ambiguous at 15cm

Previous Work

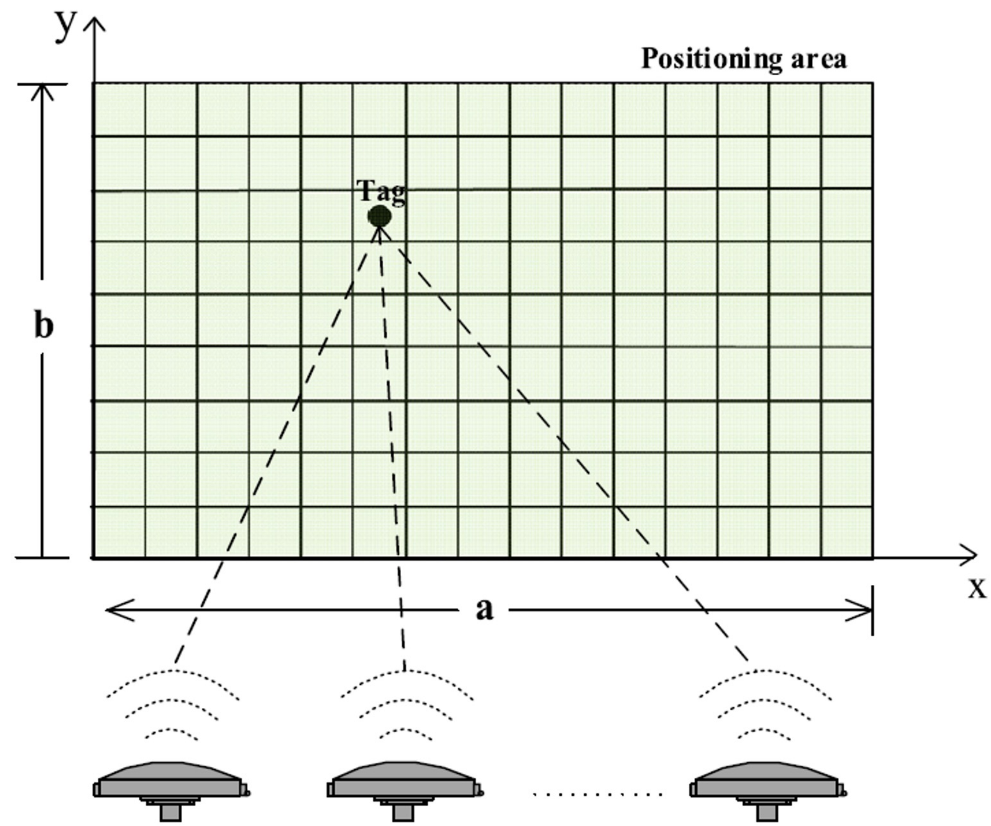
- Using reference tags in the environment



Previous Work

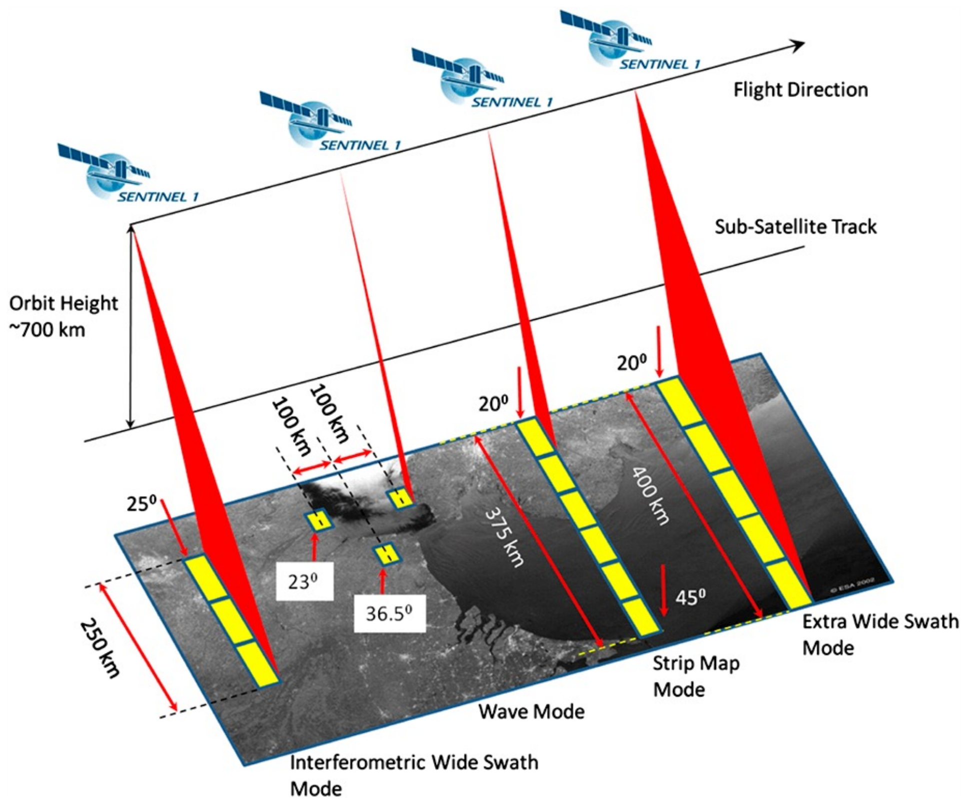
Synthetic Aperture Radar (SAR):

- moving either the RFID or the reader in a predefined trajectory over several wavelengths.



SAR: Main Applications

Satellite Imaging



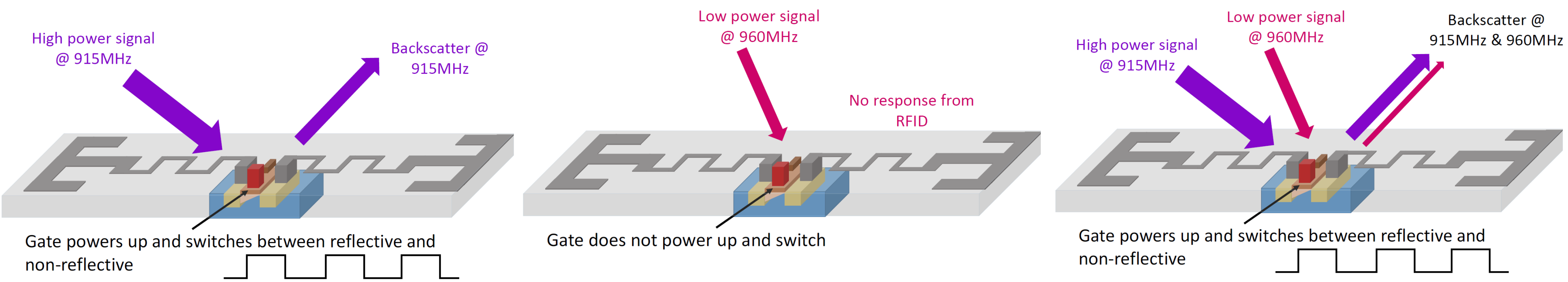
Airport Scanners

Previous Work

- Designing new expensive hardware for RFIDs to get large bandwidth:
  - non-compliant with FCC regulations
  - Renders all current RFIDs useless

Rfind Solution

- Frequency Agnostic Modulation

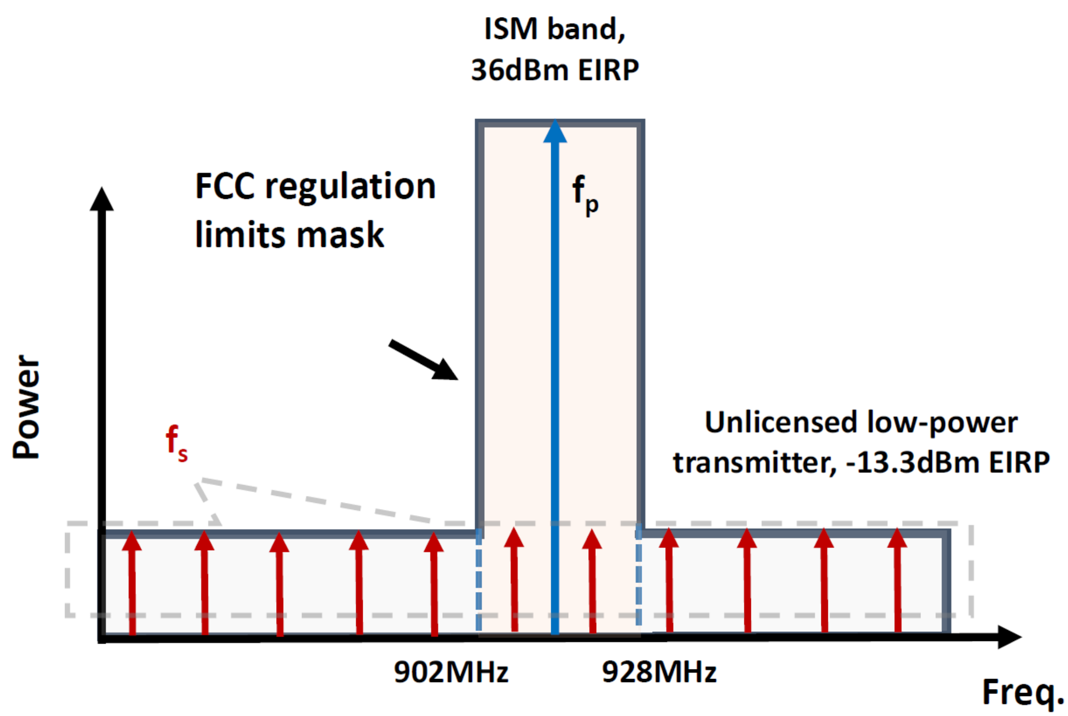


Challenges

- Using a large bandwidth would require expensive hardware such as high-speed ADCs
- The ISM band for RFID (28MHz) is not sufficient to get sub-centimeter localization accuracy and if RFind transmits in the band outside the ISM band then it must limit itself to an extremely low power to remain compliant with FCC regulations
- High accuracy localization cannot be done due to multipath from various objects surrounding the item of interest.

RFind Localization Strategy

- Decoupling Sensing & Power Delivery

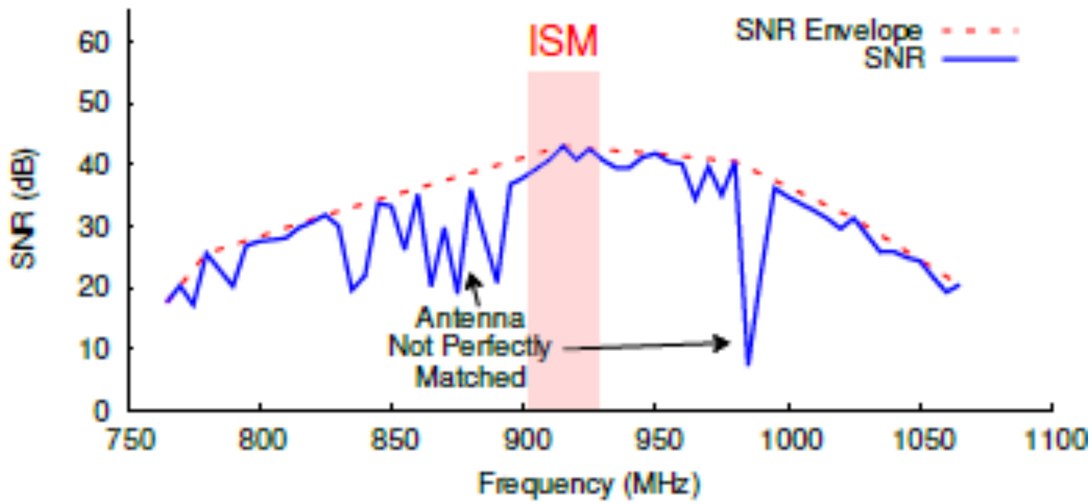


What happens if just use ISM?

Why not transmit at high power outside ISM?

RFind Localization Strategy

- Decoupling Sensing & Power Delivery



RFind Localization Strategy

- Localization using large virtual bandwidth

Channel Estimation (in frequency domain):

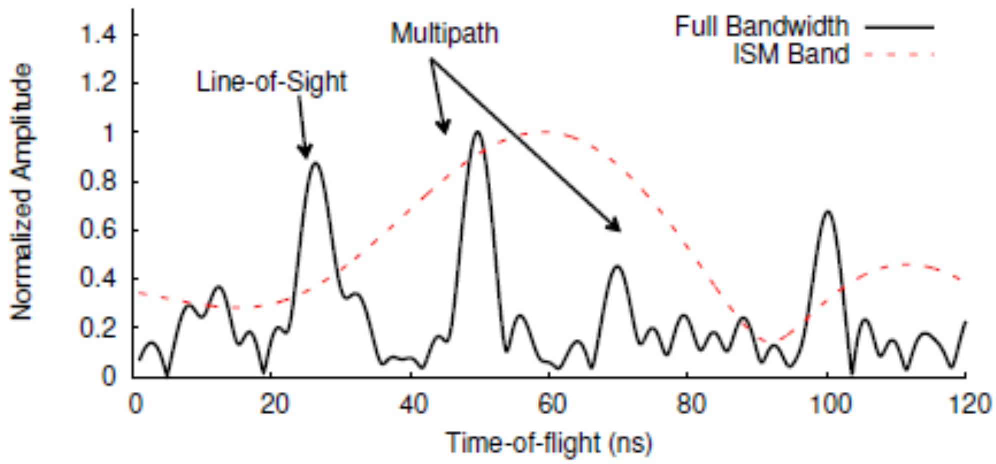
$$h_k = \sum_t y_t p_t^*$$

Identifying tl

$$S(\tau) = \sum_{k=1}^{K} h_k e^{j2\pi(k-1)\Delta f \tau}$$

RFind Localization Strategy

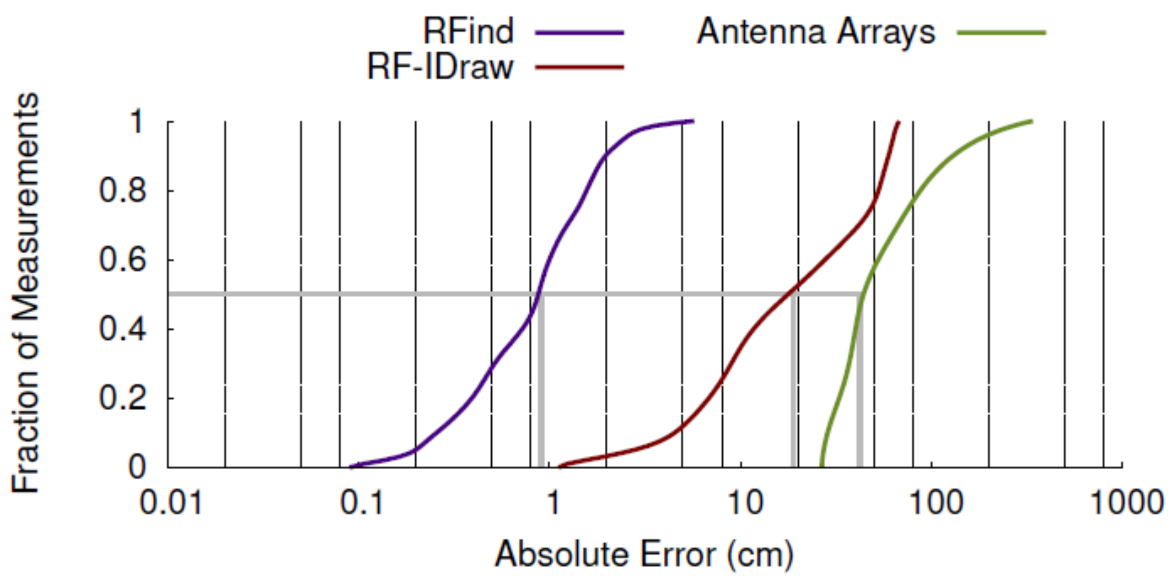
- Localization using large virtual bandwidth



$$\sum_{i=1}^{L} a_i sinc\left(B(t - \tau_i)\right)$$ → Main lobe width = 1/B

Experimental Results

2D Localization



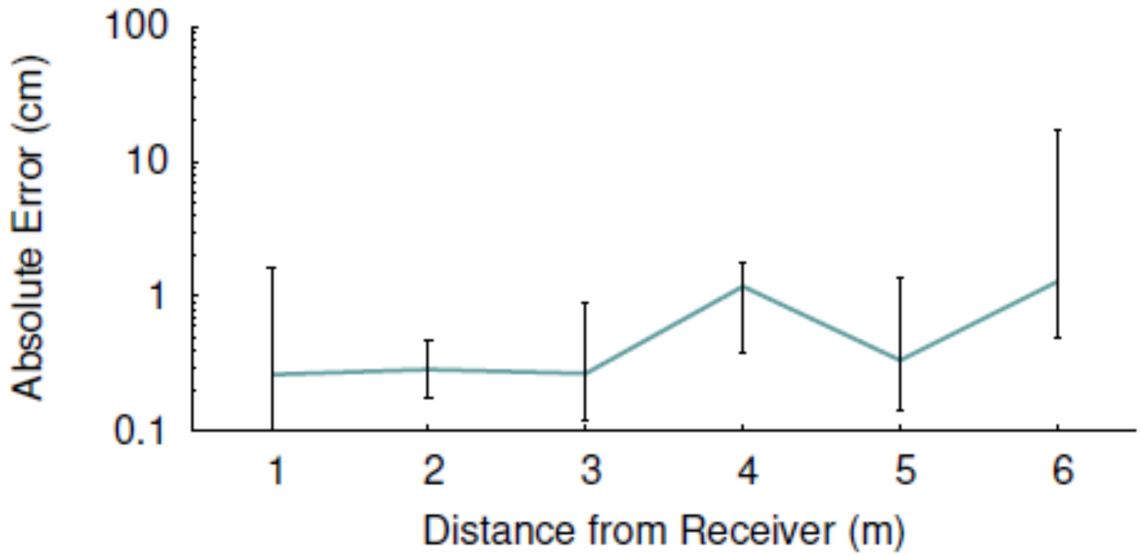
RFind : 90th Percentile Error = **1.92cm** and Median Accuracy = **0.91cm**

RFIDraw: 90th Percentile Error = **61.6cm** and Median Accuracy = **19cm**

AoA: 90th Percentile Error = **129cm** and Median Accuracy = **42.4cm**

Accuracy vs. Distance

1D Localization



Where is RFID technology today?

1. **Research-wise:**
   - Localization: sub-cm accuracies
   - Sensing: health monitoring, environmental sensing (chemical/gas), agricultural (moisture/temperature), etc.
   - Frequency Spectrum: UHF, WiFi/Bluetooth, UWB, mm-waves
   - Applications: Robotics, AR, health, digital twinning

2. **Real-world Uses:**
   - Multiple startups in the space: Cartesian, Atheraxon, Williot, Farsens
   - Used in retail, warehousing, access control, sensing, long-range payment systems

3. **Standards:**
   - EPC Gen 2
   - RAIN Alliance

Objectives of Today's Lecture

Learn the fundamentals, operation, and applications of

Batteryless IoT Devices

1. How can we make a batteryless IoT device?
2. What is backscatter communication?
3. How does energy harvesting work?
4. How do RFIDs work?
5. How do you unlock new capabilities with RFIDs?

Next Class: Hacking Sensors

1) Required
- WALNUT
- Inaudible Commands

2) Optional
- Security for IMDs
- Audio Injection Attacks
- Long Range Attack and Defense

3) Project Proposal
- Due date: October 20