IEEE RFID 2026: Tutorial Sessions

- The RF in RFID → How radios communicate
- Energy Harvesting → How passive chips get power
- Circuits → What's in the chips and why
- Cryptography → How chips talk securely (or not!)
- Middleware and Applications → How to get data for the real world
- Applied RFID: Tires → Example of real business application
- Applied RFID: PLCs → Examples of real data capture

The RF in RFID

IEEE RFID 2026 Tutorial #1

Presented by Daniel Dobkin

Purposes of this Tutorial

- Introduce concepts needed for understanding radio links
  - Types of radio frequency identification and sensing
  - Signals, propagation, links, protocols
  - Location and realistic propagation
- Provide background needed for other tutorials/conference papers

Outline

- Radios for identification; passive and active devices
- Radio basics: signals, antennas, propagation, reception
- Communications protocols (introduction)
- Locating objects with radio signals
- Propagation in realistic environments

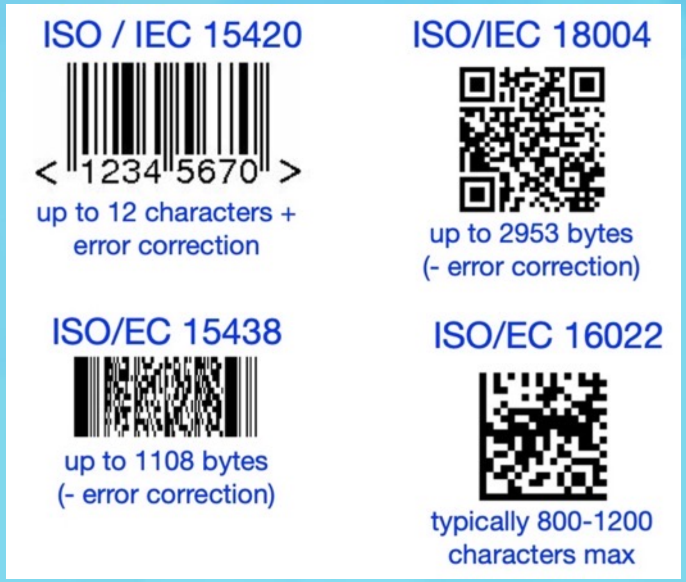
Real World Play Time

(IF we get this set up):

- Attendees hold up tagged badges, read them, who is read?
- Put badges behind person or under arm or … ; what is read?
- Move away; what is read?
- Lessons: passive range, location, ambient effects
  - Comparison to active beacons in Jeffrey Dungen's Tutorial #4!

Identification: I See You

- Initial automated identification extrapolated from human sight:
  - Bar codes and later QR codes
- Advantages:
  - Easily integrated with human-readable labeling, small added cost
  - QR codes can support unique item identification
  - Bar and QR codes can be read with a phone camera (today)
- Disadvantages:
  - Labels can be easily damaged or obscured
  - If you can't see it you can't read it
    - Human or specialized orientation setup needed
    - High volume environments can be challenging



Radios for Identification

- Radio wavelength >> optical:
  - Propagation is not line-of-sight
  - Shadowing is relatively weak
  - Many common optically-opaque objects are transparent
- Result:
  - Radios can see more of the surroundings than cameras or eyes
  - Big advantage in inventory capture, item location/management
    - BUT: water and metal are still opaque
    - Location can be difficult! Hall of mirrors = easy to see, not easy to find

Phenomena	Frequency	Wavelength/ size
Green light	600 THz	0.5 μm
US ISM	915 MHz	33 cm
People / stuff	0.001-10 Hz	30 cm – 2 m

Image: Mike Pennington

Active and Passive RFID

- Active RFID: beacon transmits a radio signal
  - Typically long range - hundreds of meters to kilometers possible
    - We'll cover this in propagation discussion
  - BUT: requires power source, expensive to purchase and maintain
- Passive RFID: tag reflects an existing radio signal
  - Range is limited by regulation and physics – centimeters to 10's of meters
  - Power provided by radio signal from reader device, no battery, simple TX
    - CHEAP!
    - CHEAP!
    - CHEAP!
    - Can last a very long time, no battery to replace
    - And did we mention – CHEAP!

Chips and Chiplessness

- Backscatter behavior can be influenced by antenna shape, load behavior, ambient
  - Chipless tags
  - Chipless sensors
- Cheap and simple BUT:
  - Encoding often analog, can be challenging, limited ID span
  - Range may be limited
    - Which can be a feature!
- Discussion mostly deferred to plenary talk on Thursday…

Radio Communications

- Electromagnetic Waves
- Inductive and Radiative Coupling
- Common RFID Bands
- Antenna Gain and Patterns
- The Friis Equation
- Link Budgets
- Antenna Arrays

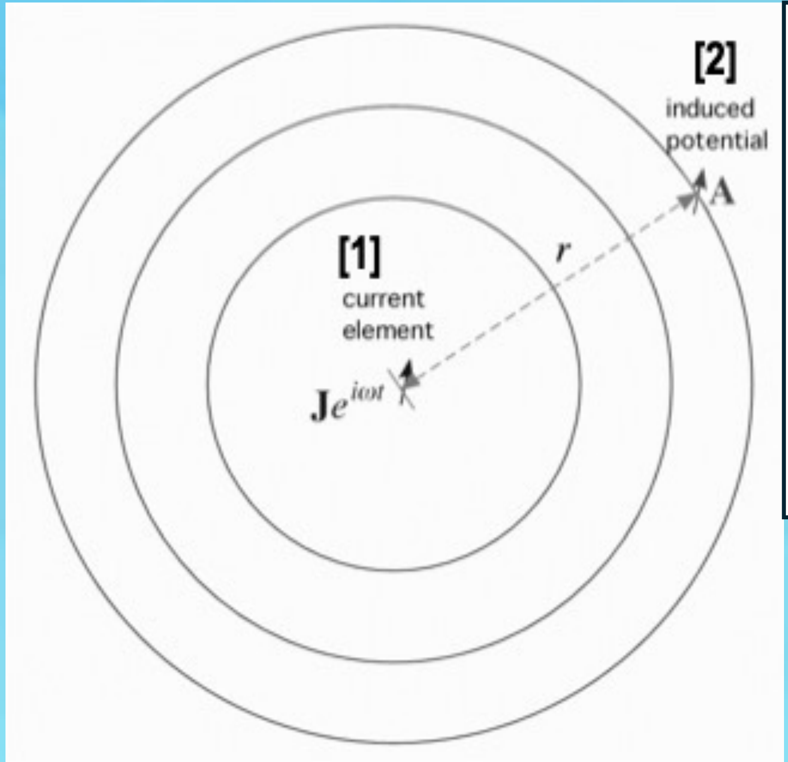
Electromagnetic Waves

- A current at [1] creates a vector potential at [2] with time delay (r/c), amplitude 1/r
- Charge induces a scalar potential ϕ
- Electric field at location 2 is:

$$\vec{\mathbf{E}} = -\frac{d\vec{\mathbf{A}}}{dt} - \nabla\phi$$

- If you put a (small) wire at [2] the induced voltage is

$$\vec{\mathbf{E}} \cdot d\vec{l}$$



$$\mathbf{A} = \mu_0 \mathbf{J} \frac{e^{-ikr} e^{i\omega t}}{4\pi r}$$

$$k = \frac{\omega}{c}$$

$$\omega = 2\pi f$$

$$\mu_0 = 4\pi \times 10^{-7} \text{Henry/meter}$$

$$\frac{d\mathbf{A}}{dt} = i\omega\mathbf{A}$$

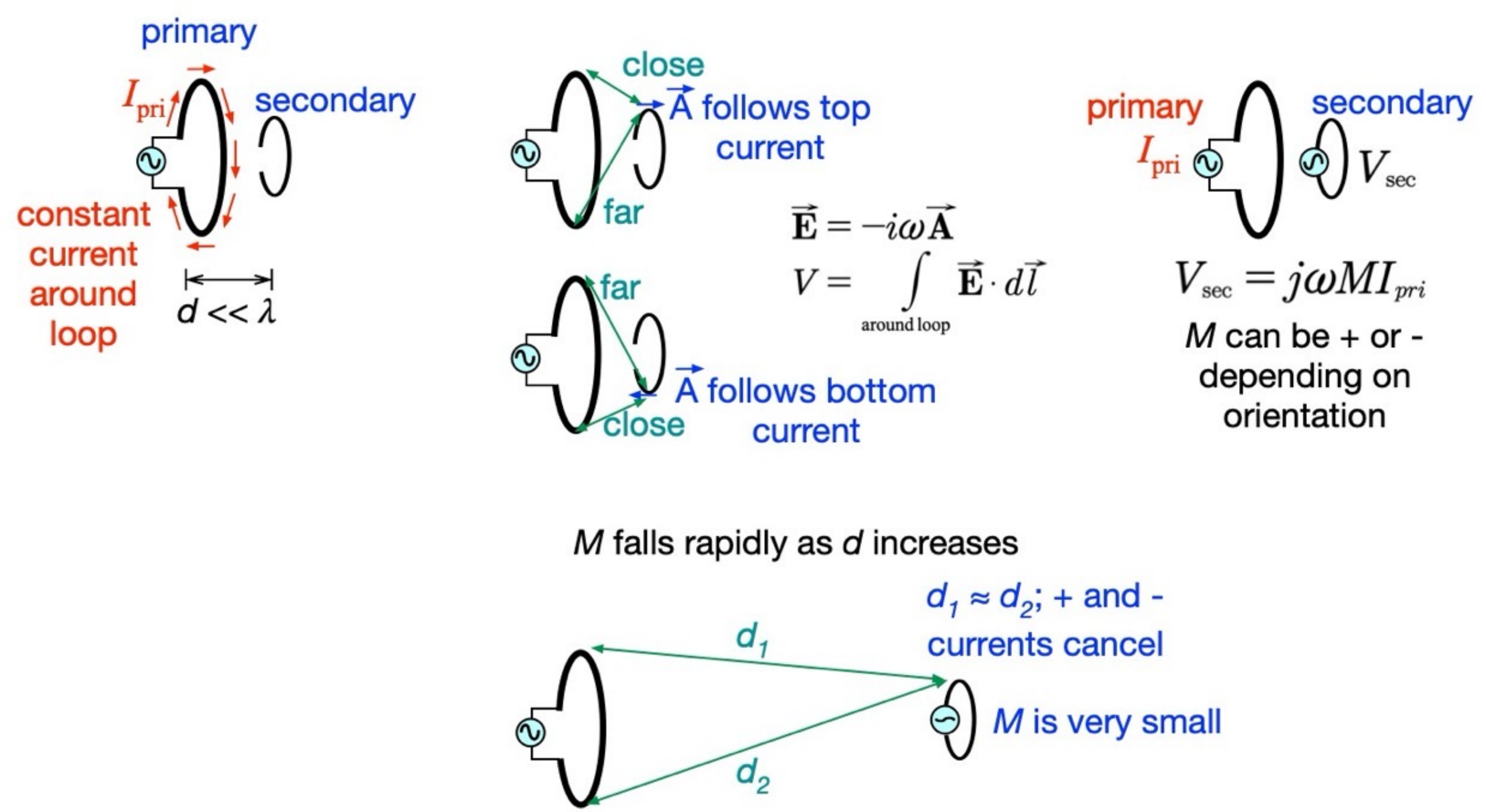
$$\phi = \mu_0 c^2 Q \frac{e^{-ikr} e^{i\omega t}}{4\pi r}$$

Near and Far: Induction and Radiation

- Wire size, distance << wavelength λ:
  - Phase doesn't matter but distance to wire does
  - Induced signals change with position of receiver in complex fashion
  - NEAR FIELD or INDUCTIVE coupling
- Wire size << λ to > λ, distance large compared to λ, wire size:
  - Shape of wire influences the radiated potential in each DIRECTION (directivity), but received signal then just falls as (1/r)
  - FAR FIELD or RADIATIVE coupling

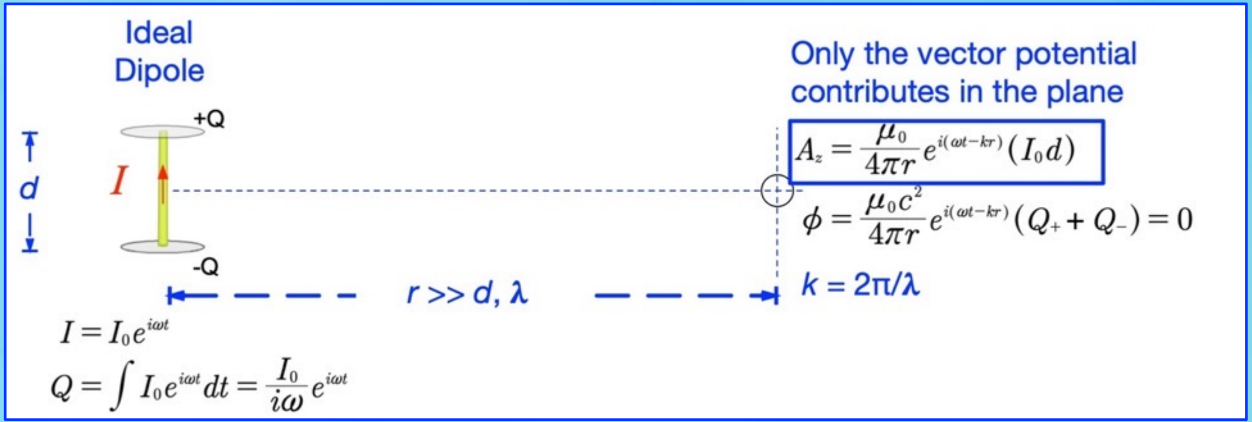
Inductive Coupling

- Wire size, distance << wavelength λ:
  - Phase doesn't matter but distance to wire does
  - Induced voltage follows nearest currents: mutual inductance M
  - Coupling M falls rapidly for distance large compared to loop sizes



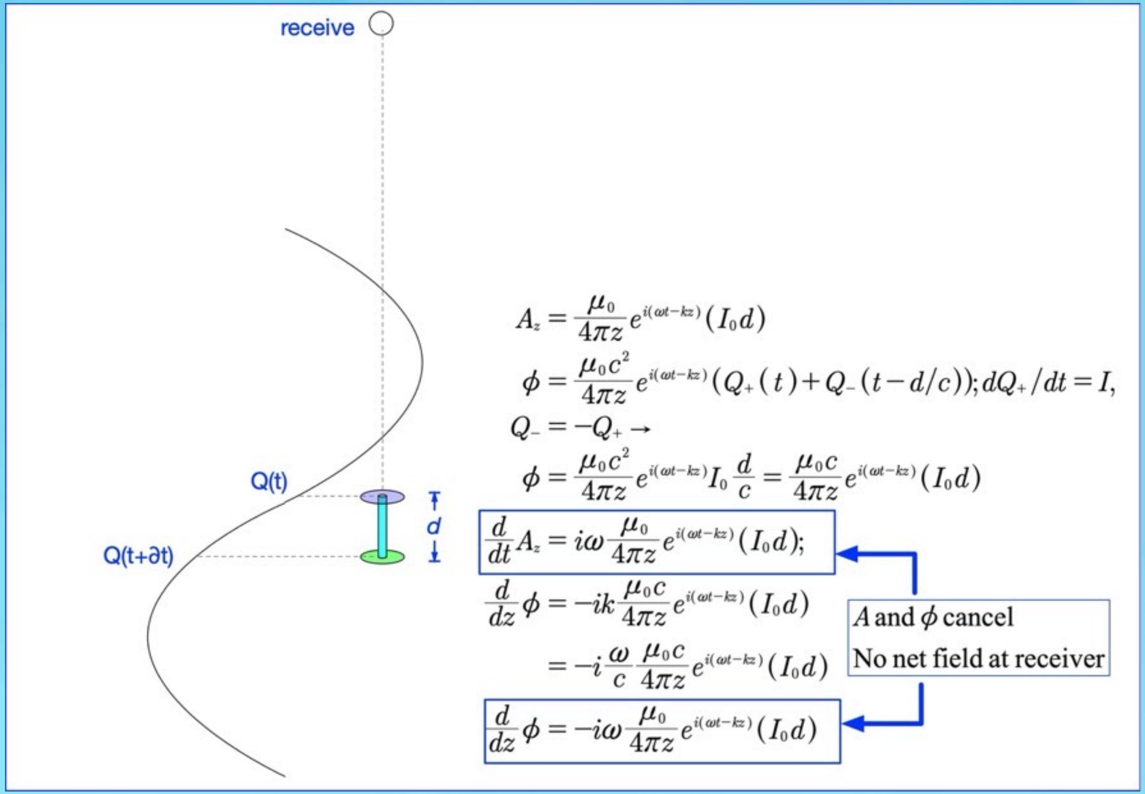
Radiative Coupling: Short Dipole

- Only A contributes in the plane



- Dipoles transmit in the plane, not on the axis!
  - Still true for *d* comparable to wavelength but harder to compute
  - Full pattern is sinusoidal

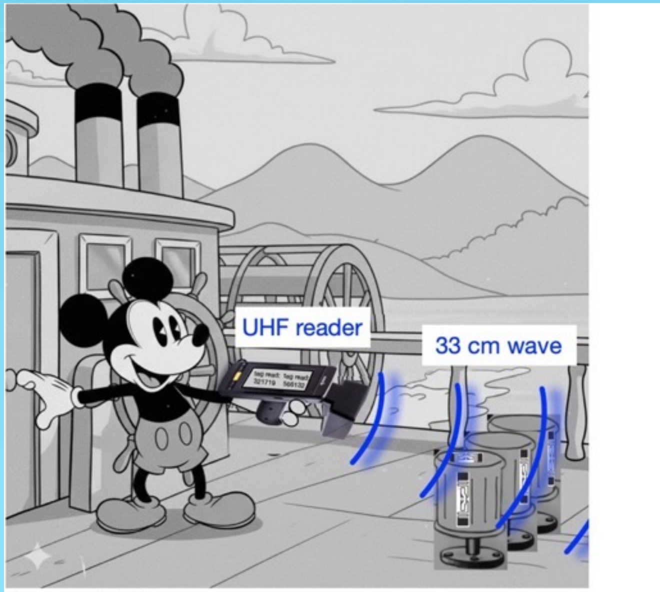
- No transmission along dipole axis



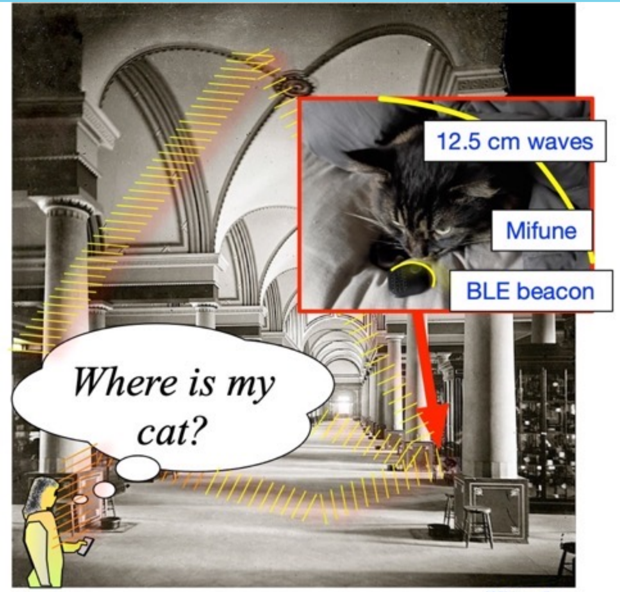
Common RFID Bands

- HF: ISM 13.553-13.567 MHz , λ ≈ 22 meters: INDUCTIVE
- UHF: ISM 902-928 MHz, λ ≈ 0.33 m: RADIATIVE
- BLE: ISM 2400-2483 MHz, λ ≈ 0.12 meters: RADIATIVE

image: Basile Moran



Based on Steamboat Willie



Wikimedia

ISM: "Industrial, Scientific and Medical"

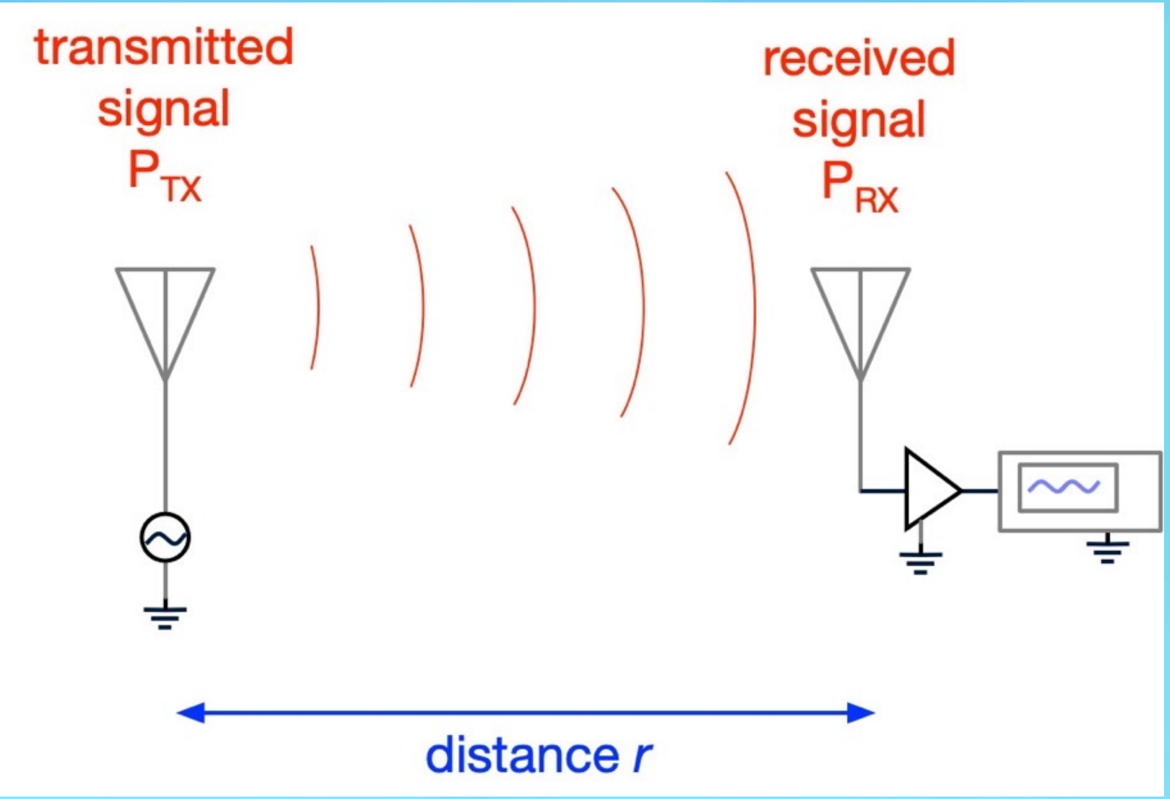
HF: "High Frequency"

UHF: "Ultra-High Frequency"

BLE: "Bluetooth Low Energy"

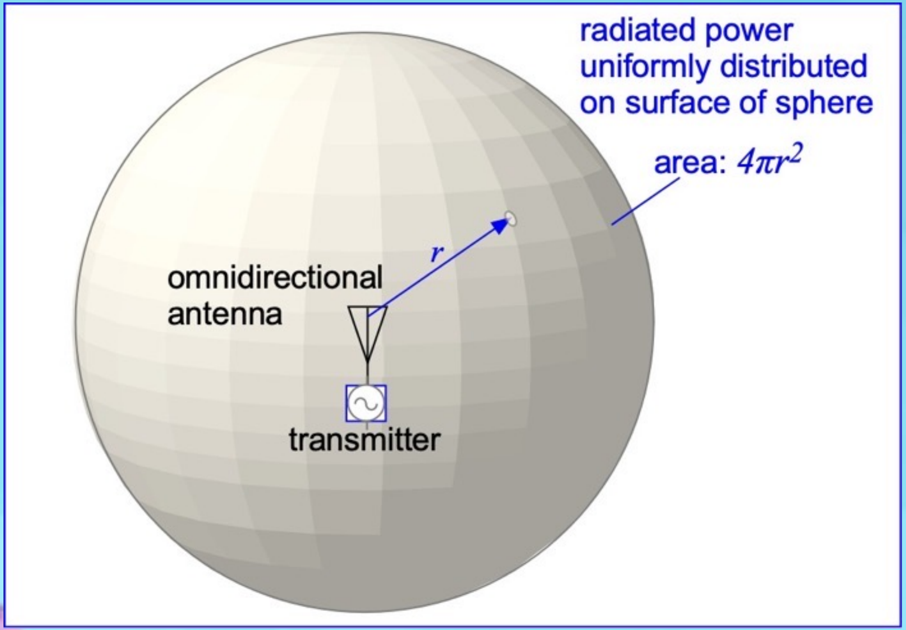
Radiative Transmission/Reception

- (Vector+scalar) potential from current in transmit antenna creates electric field → voltage in receiving antenna
- Received signal depends on:
  - Transmitted signal
  - Antennas
  - Orientation
  - Distance
  - and stuff in the way or nearby (later)

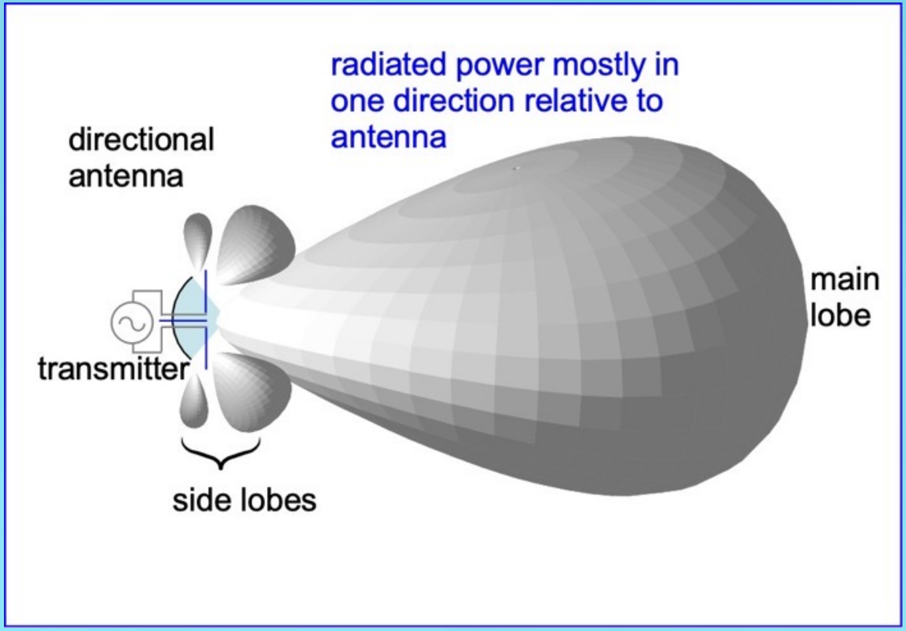


Antenna [Directive] Gain

- Simple "ideal" antenna would transmit energy in every direction equally
  - Power/m^2 = power/$4\pi r^2$

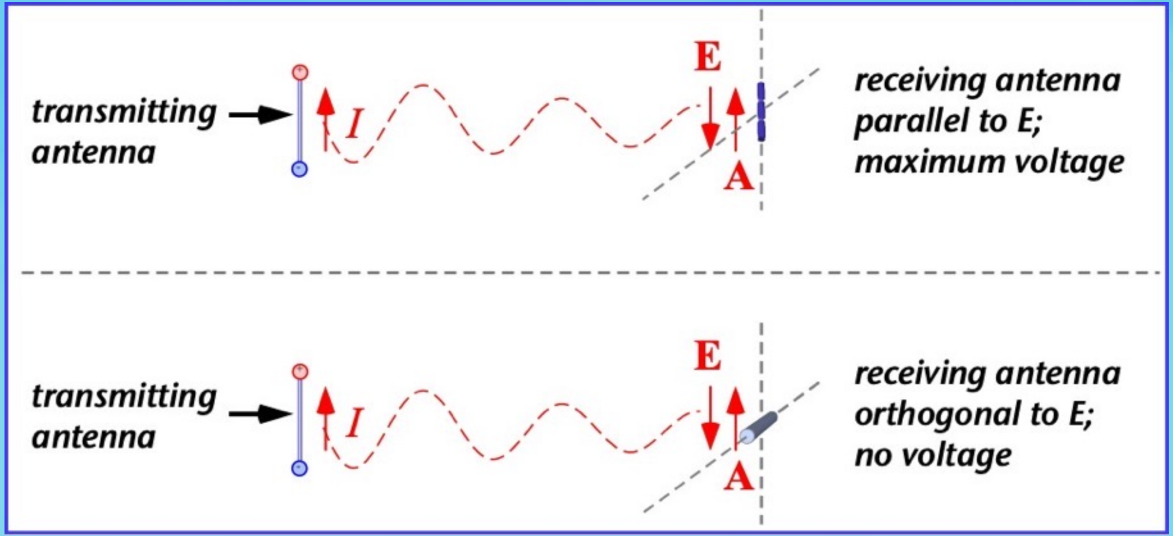


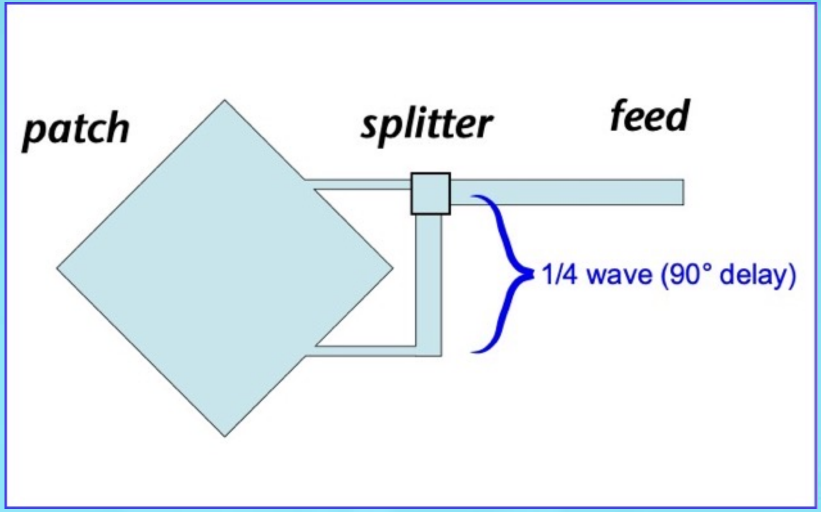
- Real antennas send most of the signal in a specific direction: "Directive gain"
  - NOT actual increase in total power! Just redistribution



Antenna Polarization

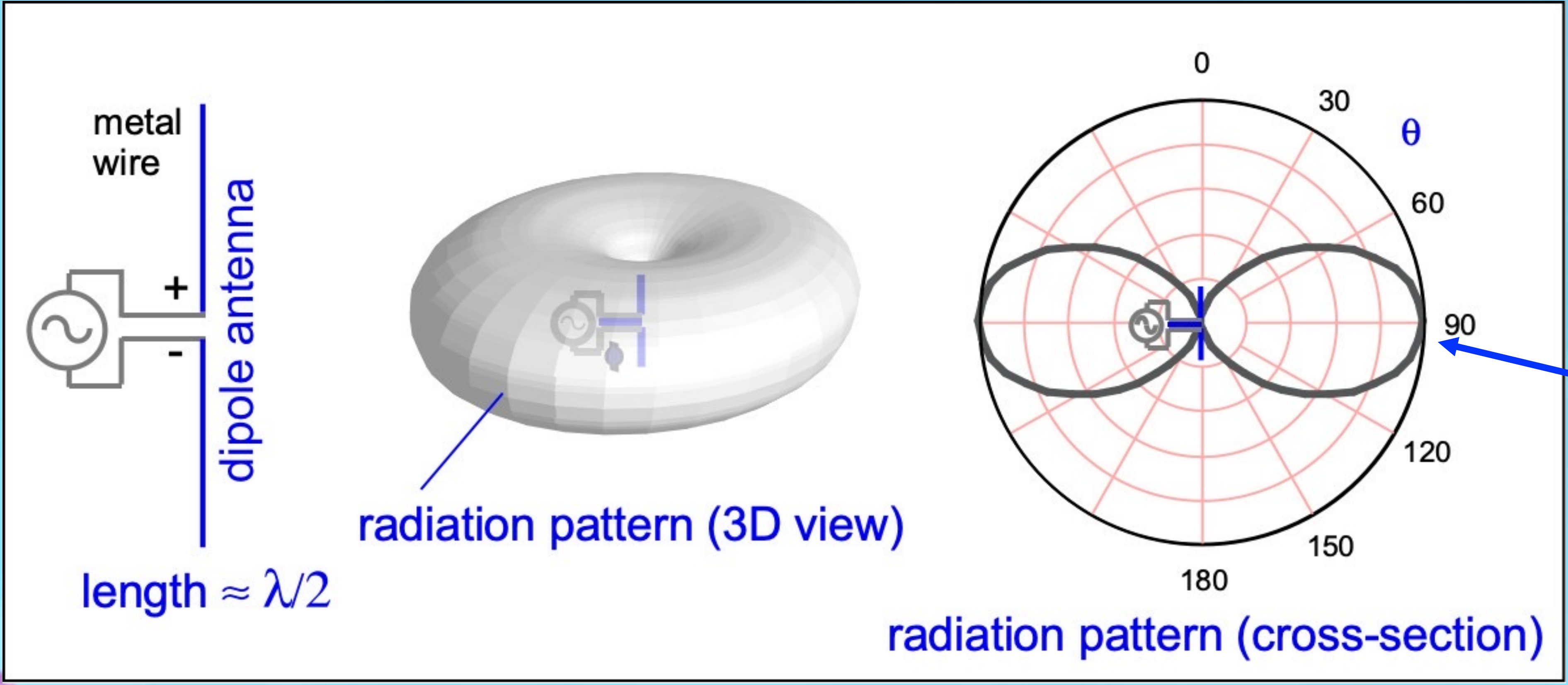
- Vector potential and thus electric field are in the direction of current flow
  - For the short dipole we looked at before, radiated field is vertical
- Direction of field is the *polarization* of the antenna
- We can make circular polarization by using perpendicular currents excited 90° out of phase





Antenna Pattern Example: Dipole

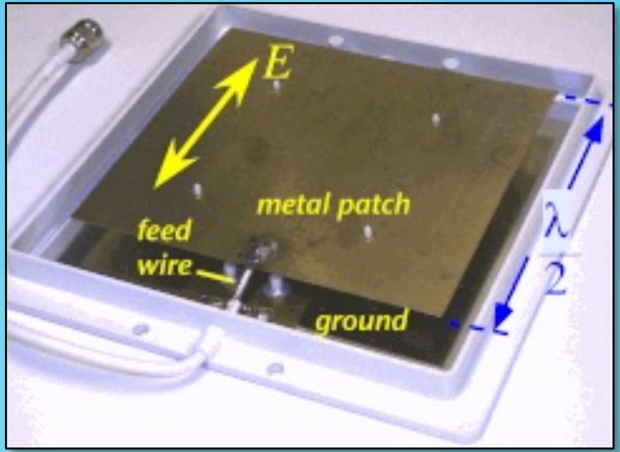
- Dipole antenna energy mostly perpendicular to dipole, zero along axis, uniform in $\theta = 90°$ plane



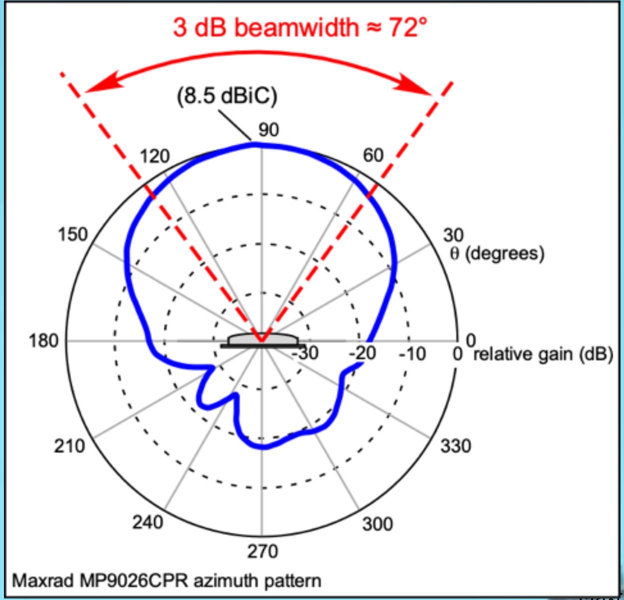
Maximum directive gain about 2.3 dBi; ≈1.8 dBi for a small RFID tag antenna

Antenna Pattern Example: Patch

- Patch antenna = rectangular metal above metal ground plane
  - Feed wire configured for optimal match



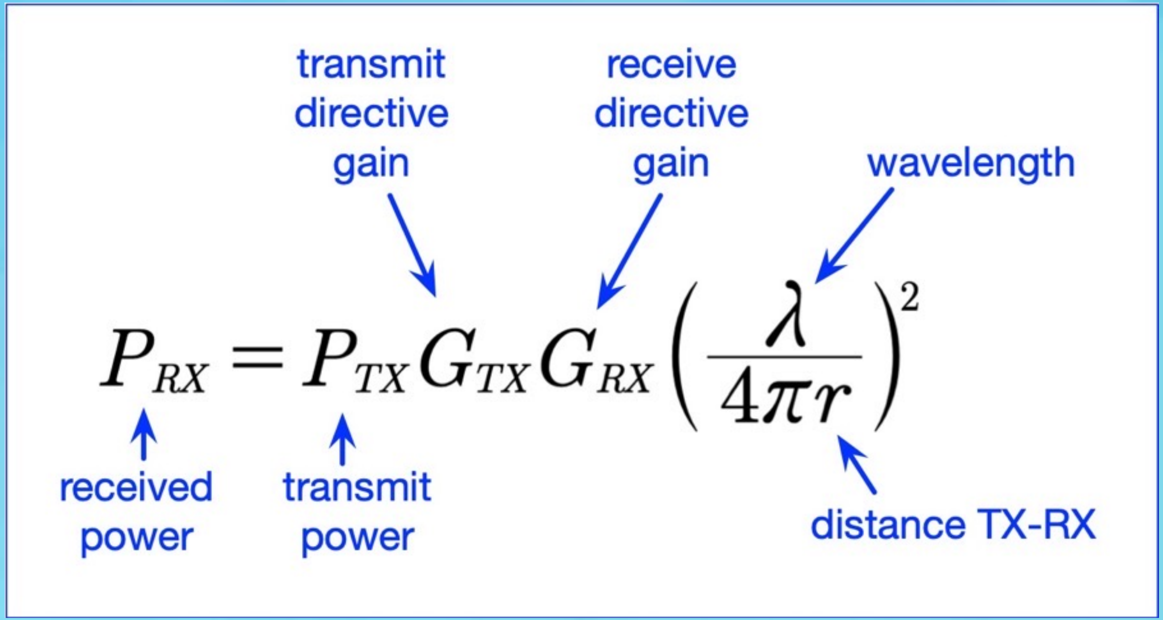
- Commercial patch antenna example
  - Circular polarization
  - Beamwidth about 72°, maximum gain about 8.5 dBiC (deciBels from isotropic, circular)
  - Reduced but non-zero radiation BEHIND the antenna
    - Recall -20 dB is a factor of 1/10 in voltage
    - Voltages are what adds when signals are received by another antenna, so this is not always negligible!



Maxrad MP9026CPR azimuth pattern

The Friis Equation

- Signal IN EMPTY SPACE depends on transmit power, transmit antenna directivity (gain), distance, received antenna directivity
  - Wavelength dependence is from definition of antenna gain vs. aperture, NOT propagation
- The Friis equation applies to simple open spaces; real environments can be MUCH MORE COMPLEX
  - We will discuss this in the Real Environments section a bit later…

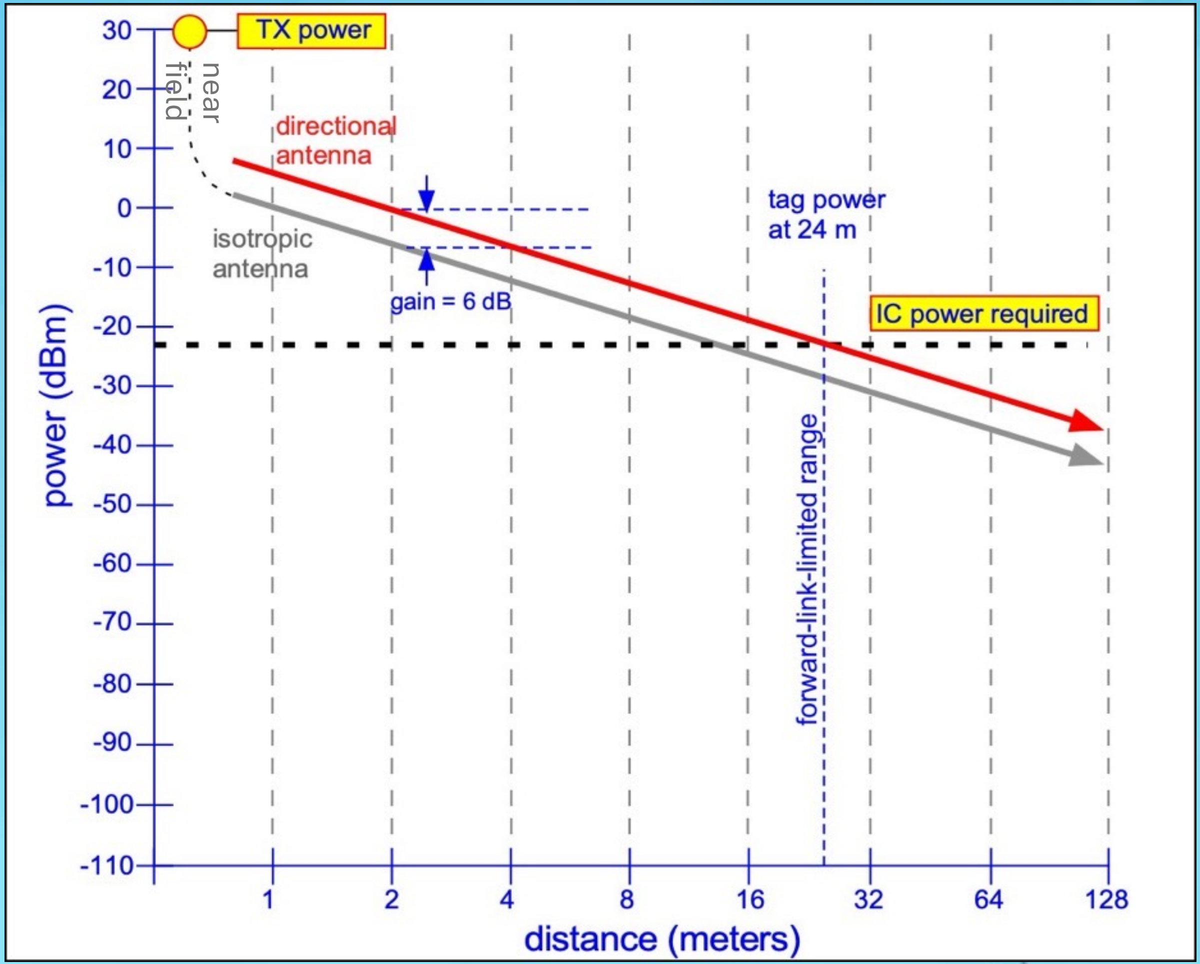


$$P_{RX} = P_{TX} G_{TX} G_{RX} \left(\frac{\lambda}{4\pi r} \right)^2$$

NOTE: Valid for distances larger than antenna size, wavelength. Polarization is not included above but can be important!

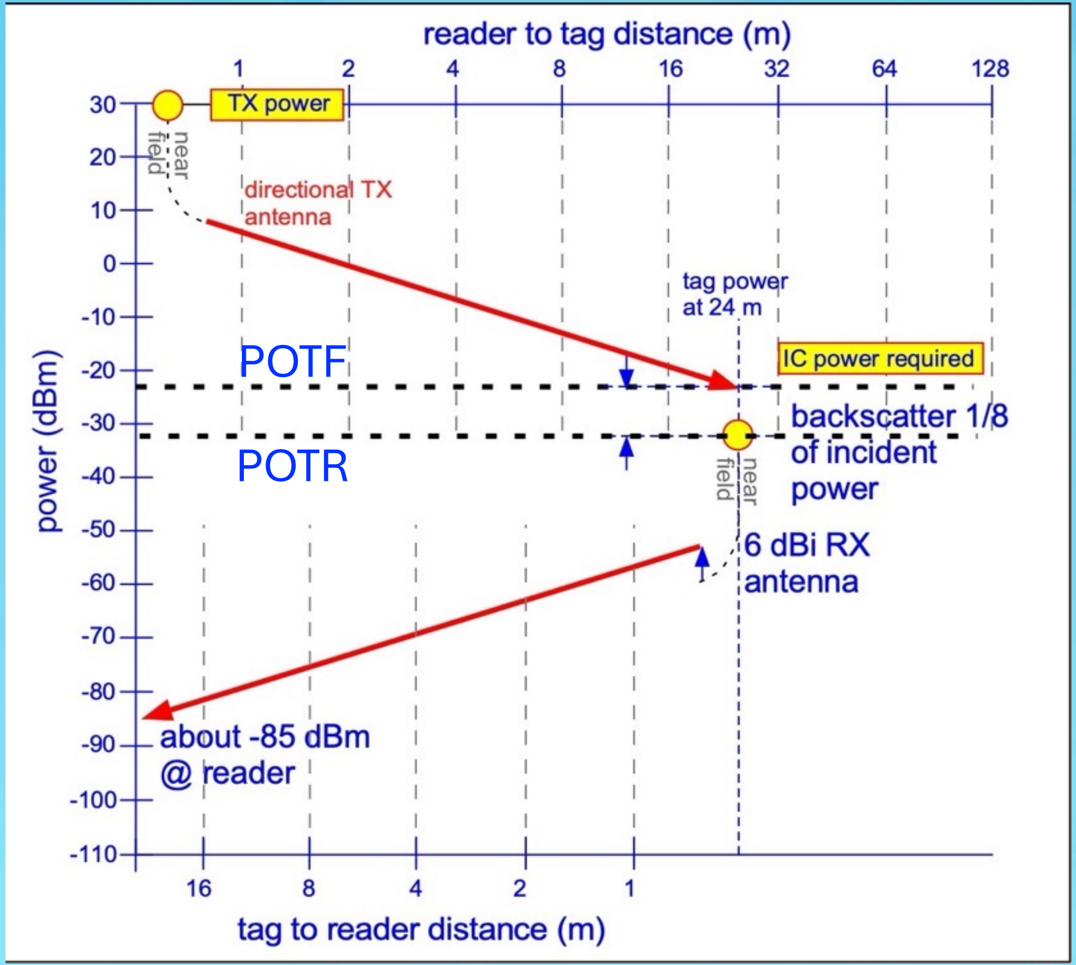
Forward Link Budget

- The radio link needs to transmit enough power for the receiver to hear and demodulate the signal; in logarithmic terms:
  - Transmit power + directive gain – propagation loss = received power
  - Received – (minimum received) = link budget
- Example for passive tag receiver:
  - 1 W transmit power with 6 dBi antenna (assuming tag antenna gain ≈ 1) provides -23 dBm to tag 24 meters away: *forward-link-limited range*



Reverse Link Budget: Backscatter

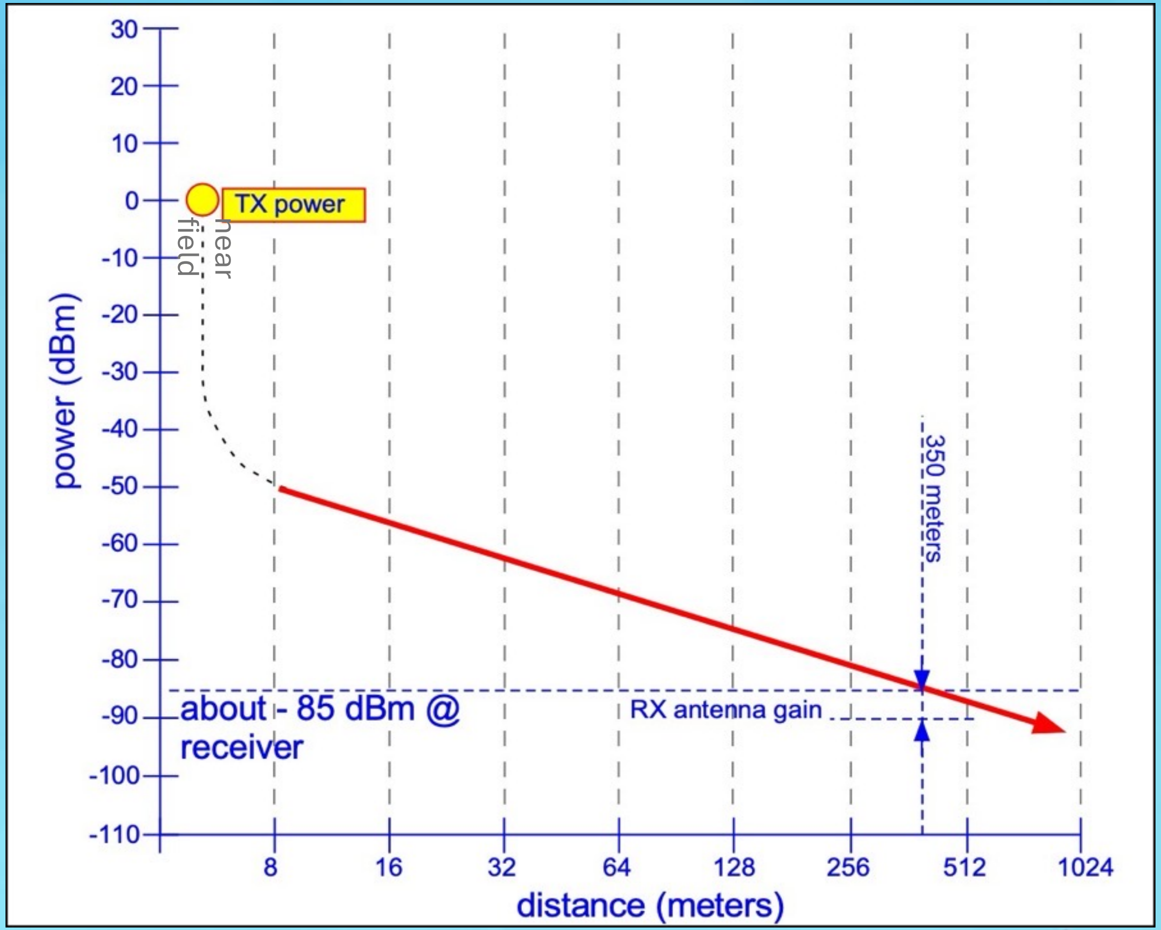
- A passive RFID tag doesn't have its own transmitter, just backscatters incident RF
- Result: reverse-link starts with power reduced by $1/r^2$ and then propagates back ($1/r^2$) so:
- Power at reader goes as ***$1/r^4$***!
  - If we move the tag 2x (3 dB) farther, received signal falls by 16x (12 dB)



We again assume tag antenna gain is close to 1; POTF and POTR are power-on tag forward and reverse (Voyantic)

Beacon Link Budget

- BLE beacon has its own transmitter but needs to run on a battery or harvested energy
  - Transmit power can be one mW or less
- TX antenna gain may be small
- BUT we still can get lots of range in open space
  - 14x farther for the same received signal vs. passive tag!

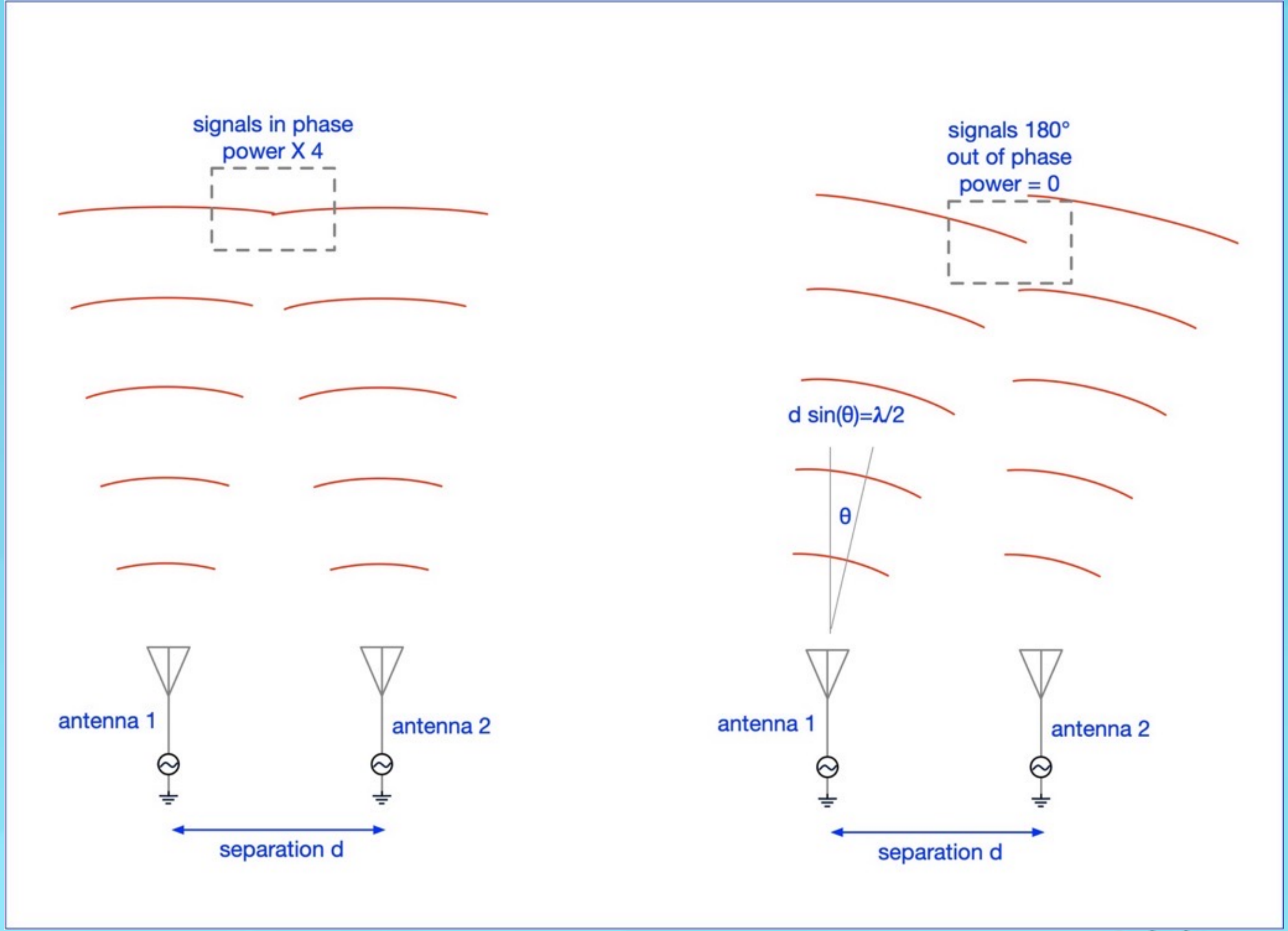


Passive Links: Practical Considerations

- Tags are often much smaller than a half-wavelength
  - A small tag might be 1.5 cm vs. $\lambda/2 \approx 15$ cm @ 915 MHz
  - Theoretical efficiency is not affected but PRACTICAL efficiency IS, because impedance decreases with size; 2 ohms is hard to match!
  - More details in Energy Harvesting (next session)
- Orientation of tag antenna is often not controllable
  - Low (directive) gain is good!
  - BUT there are directions where a null exists
  - AND reflections from environment will create multiple incident waves
  - AND stuff near the tag antenna affects gain and impedance
- Reader antenna directivity can be used to find the tag
  - See Location discussion

Antenna Arrays and Beamforming

- Two antennas create potentials that can add or subtract
  - Power goes as SQUARE
  - Directive gain of the array increases with more antennas
- We can change the relative phase of elements to DIRECT the beam
- Very powerful tool but often complex and expensive



Examples: Impinj xArray, Zebra ATR7000;

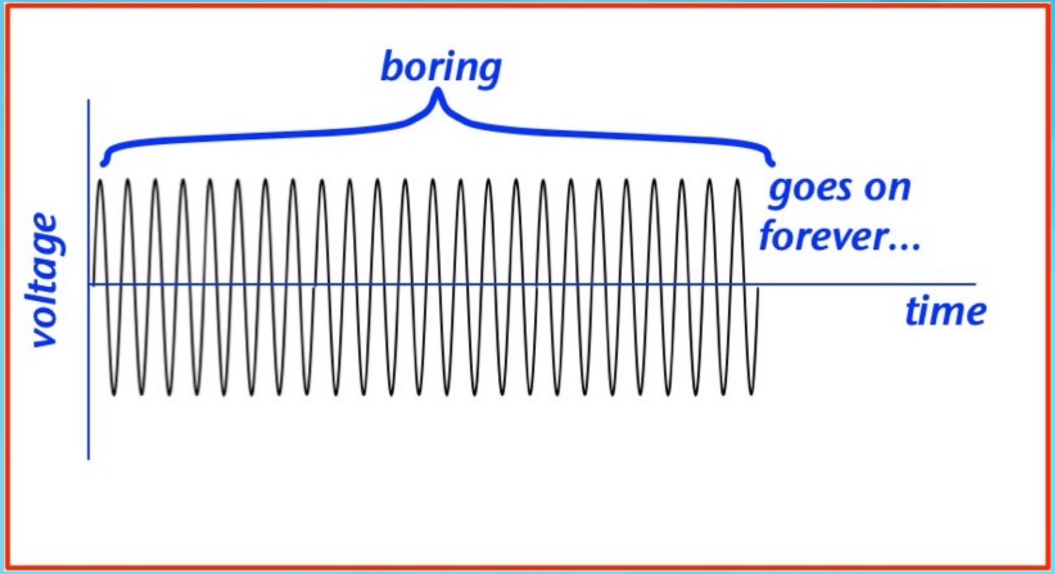
Wang et. al. NSDI 2019

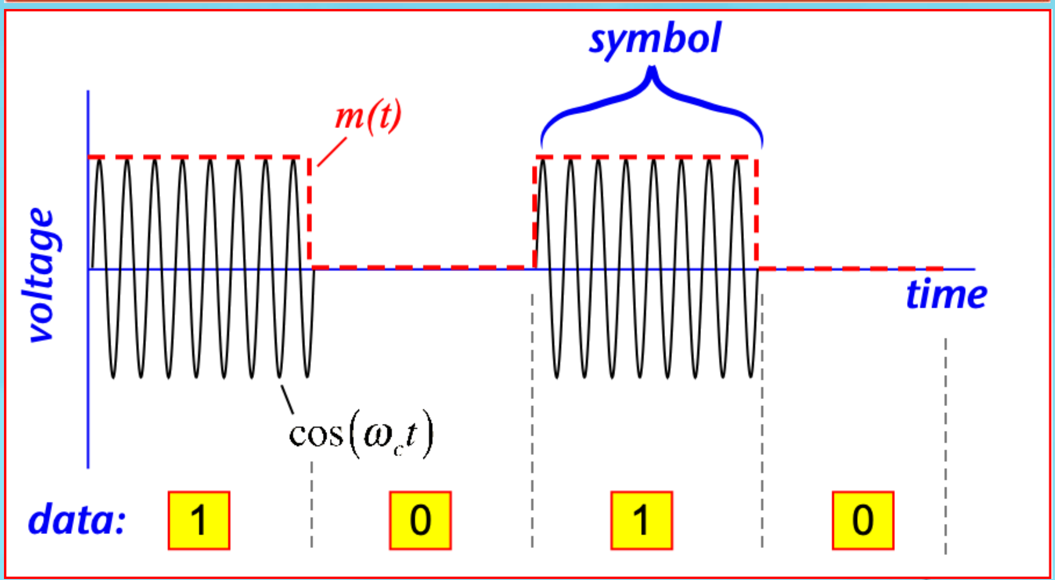
Modulation

- A CW (continuous wave) signal conveys no information
  - One note…

- We need to modulate to convey information
  - One note with a message!

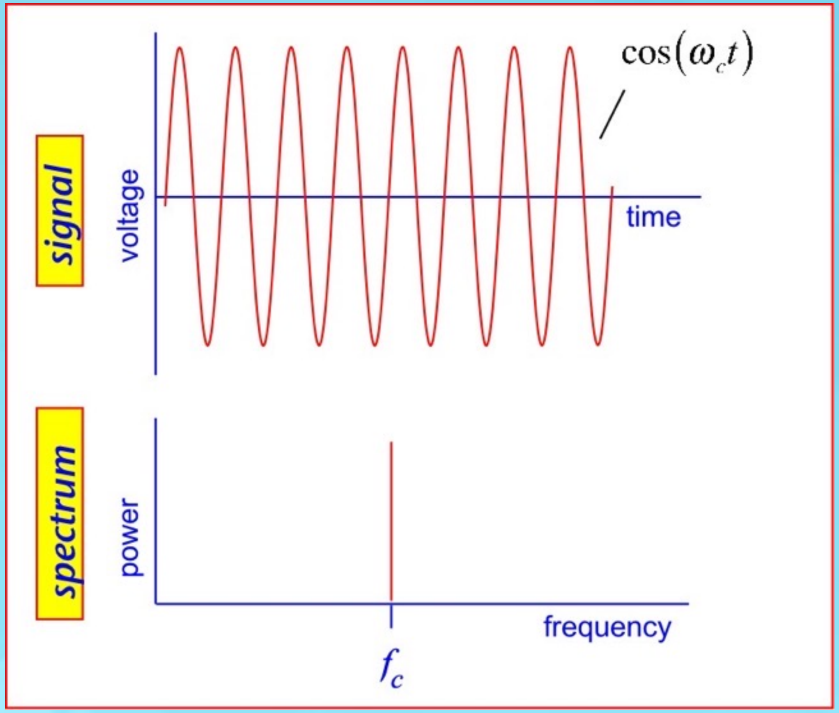
Getz Plays Jobim: One-Note Samba



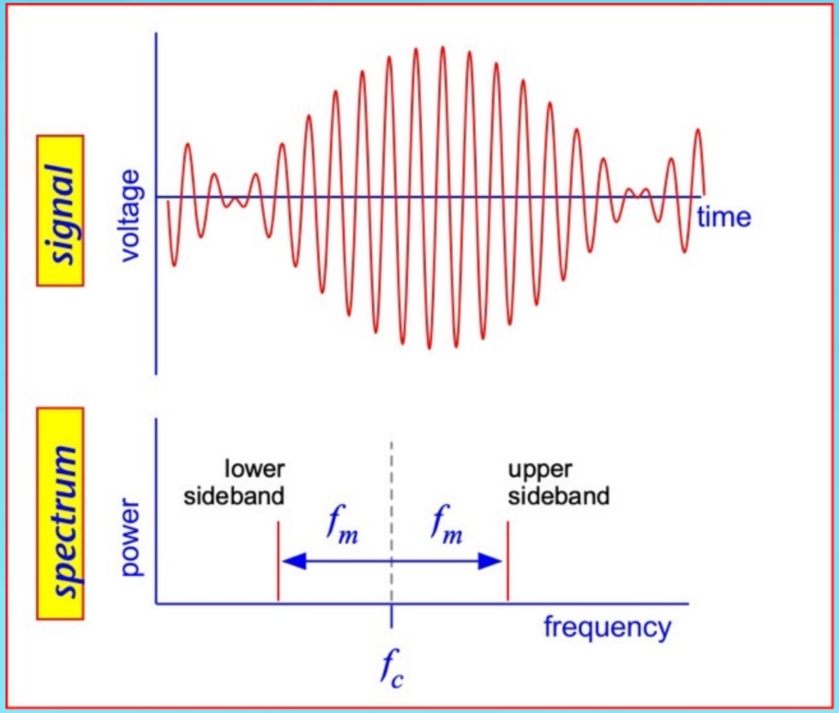


Time and Frequency

- The spectrum of an unmodulated wave is just a spike (fundamental)

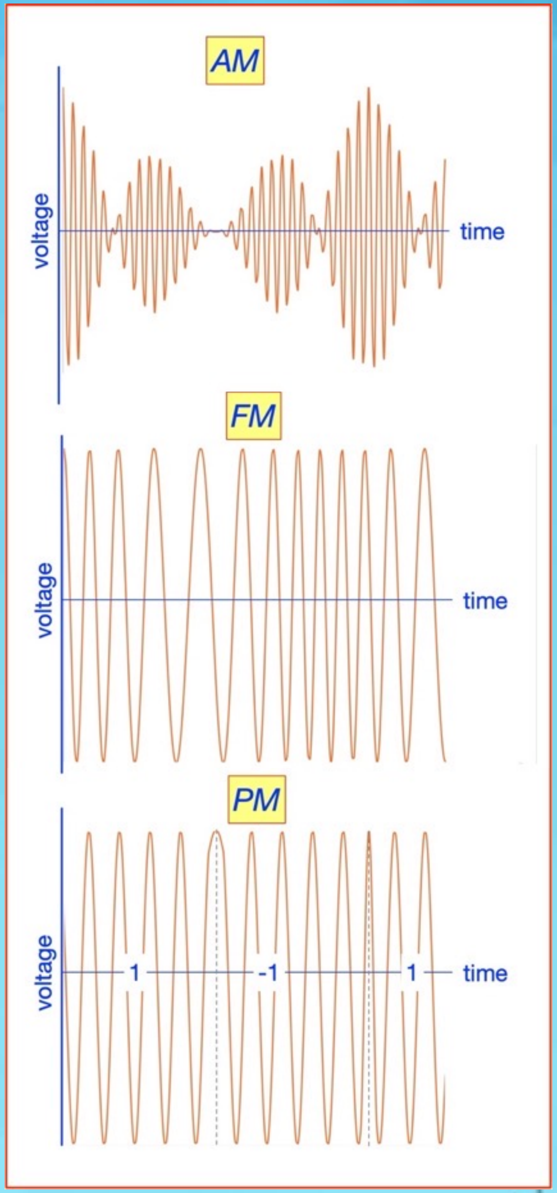


- A modulated cosine has additional frequency components



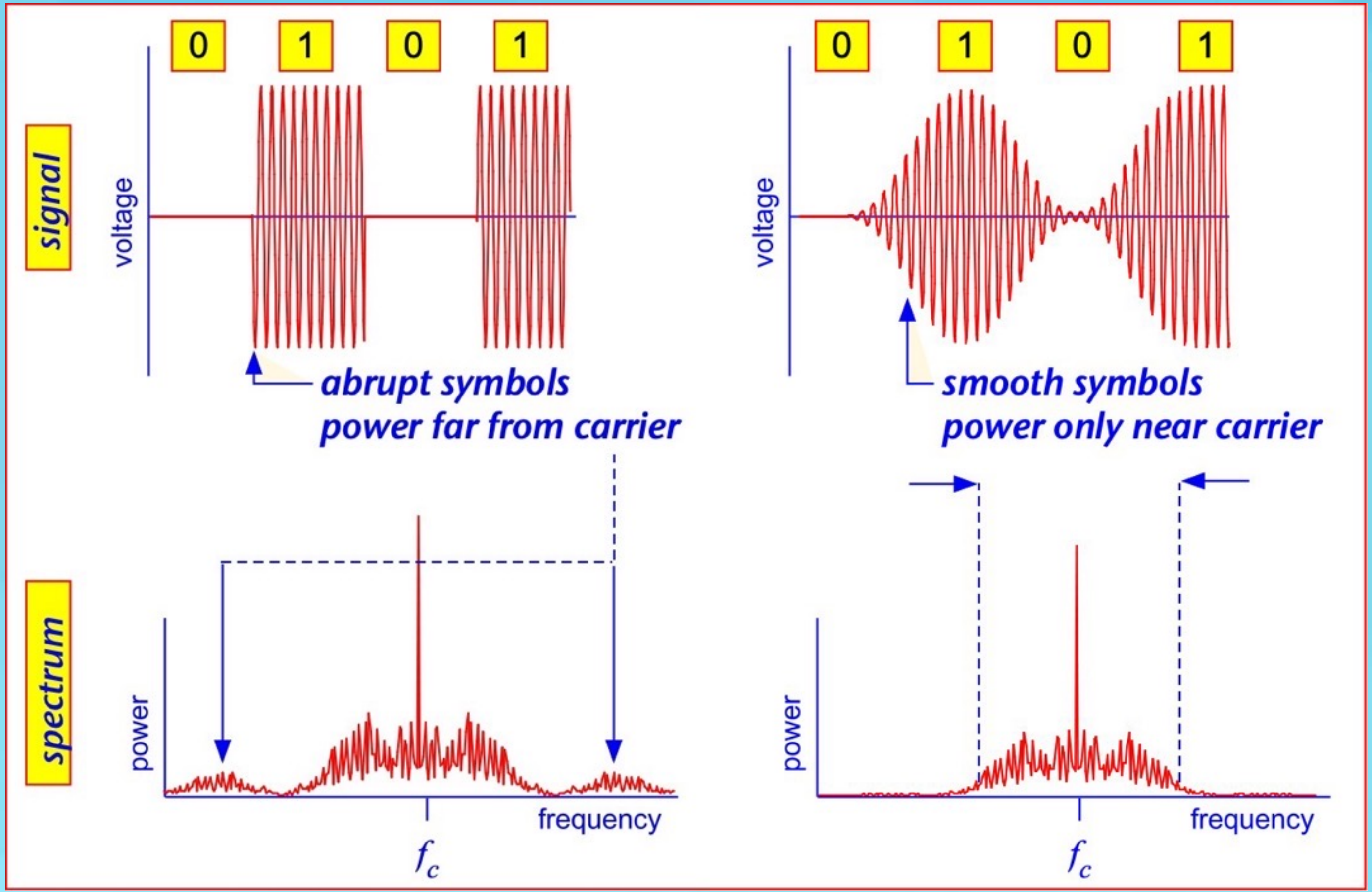
Ways to Modulate

- Amplitude Modulation (AM)
  - Change the amplitude of a single frequency
    - But still creates new frequencies
  - Digital version: amplitude-shift keying (ASK)
- Frequency Modulation (FM)
  - Change fundamental frequency
  - Digital version: frequency-shift keying (FSK)
- Phase Modulation (PM)
  - Not used in (ancient) commercial radio!
  - But very useful in digital: phase-shift keying (PSK)



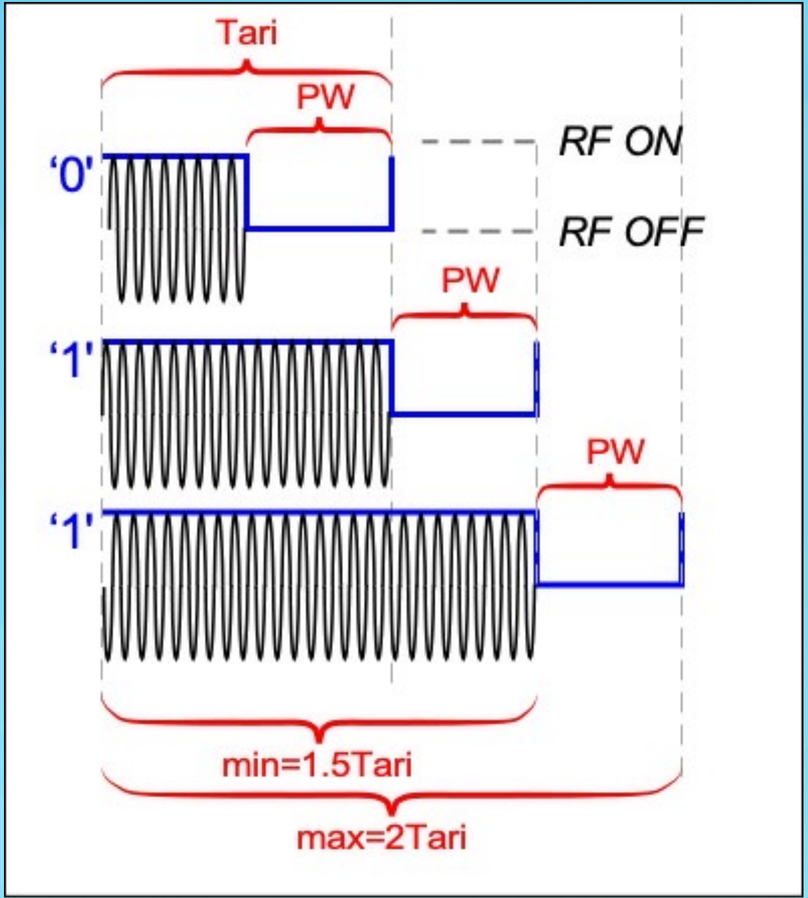
Abrupt and Smooth Modulation

- Modulation approach also affects frequency spectrum
- Abrupt modulation gives spurious frequencies far from carrier
  - But easy to decode
- Smooth modulation gives narrow spectrum
  - But decoder needs to look at the right time



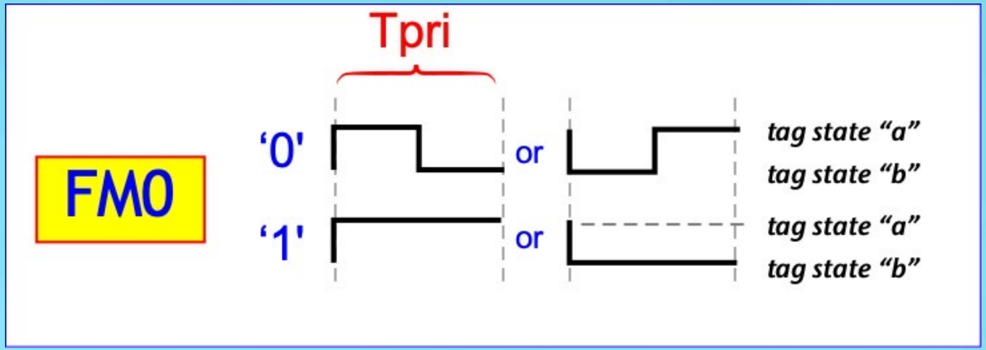
Modulation for Passive UHF RFID: Reader

- Pulse-interval-encoding (PIE):
  - Amplitude-modulation BUT both 0 and 1 symbols contain RF-on times!
    - Tag needs RF power to stay on; duty cycle 50% for ‘0’ symbol, larger for ‘1’ symbol
    - Ensures that tag received power remains close to continuous-wave value even for long sequence of ‘0’ symbols
    - Typical value of Tari ≈ 25 microseconds
      - Minimum value 6.25 microseconds



Modulation for Passive UHF RFID: Tag

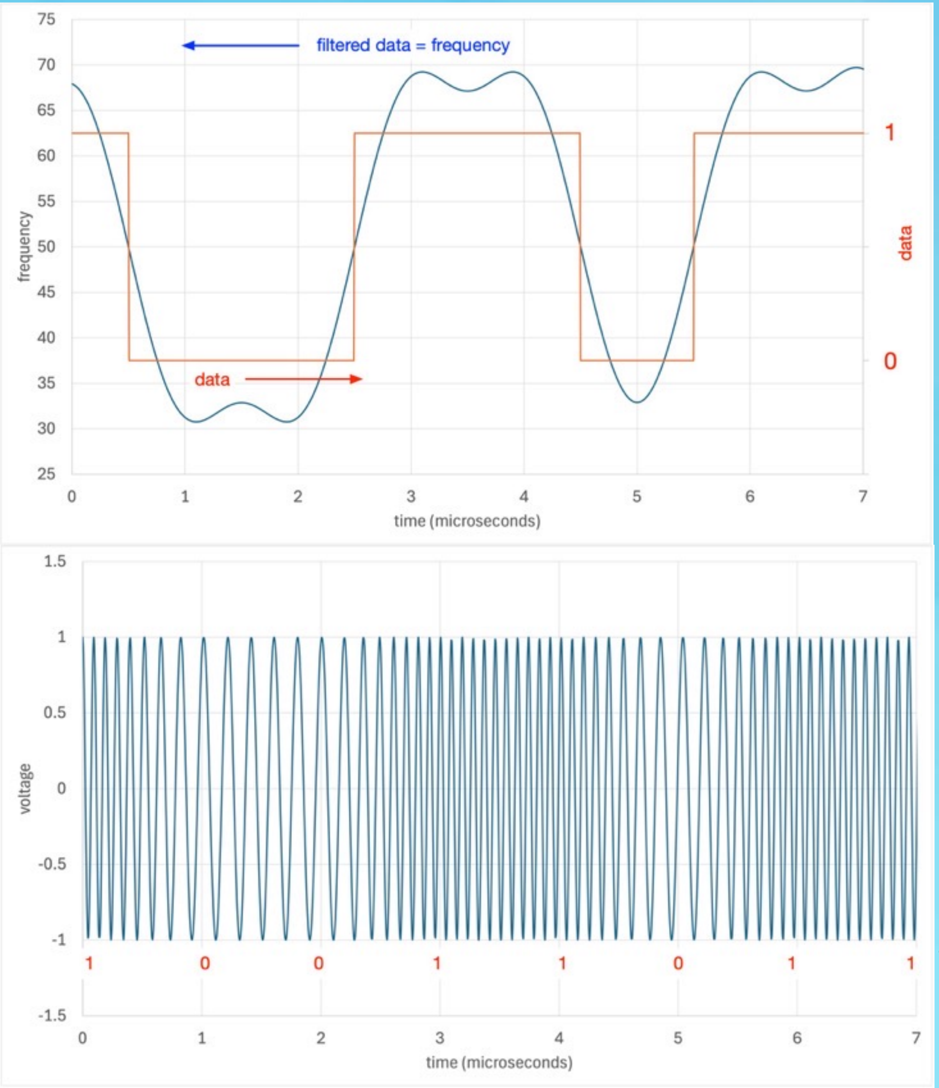
- Tag doesn't have a transmitter!
  - We can only modify the way we SCATTER the signal from the reader
  - AND we have NO CONTROL over the environment the antenna is in, or the phase or amplitude of the incoming signal
  - So we can only CHANGE the scattered signal with no idea of what change we made
- Tag signals just involve these changes:
  - A symbol with change in the middle and edge is '0'
  - A symbol with change only at the edge is a '1'



- Option to use more transitions for a single symbol (MMS): more time but better SNR

Modulation for Bluetooth Low Energy

- Active radio, 1 MHz or 2 MHz channels
- Basic modulation is Gaussian Frequency Shift Keying
  - Filter the data with a Gaussian, then modulate frequency; trade intersymbol interference for narrower spectrum
    - Everything exaggerated at right so you can see what's going on
  - Amplitude constant
  - Basic: 1 bit/symbol, 1 Mbps



GREATLY exaggerated for clarity, NOT BLE-compliant!

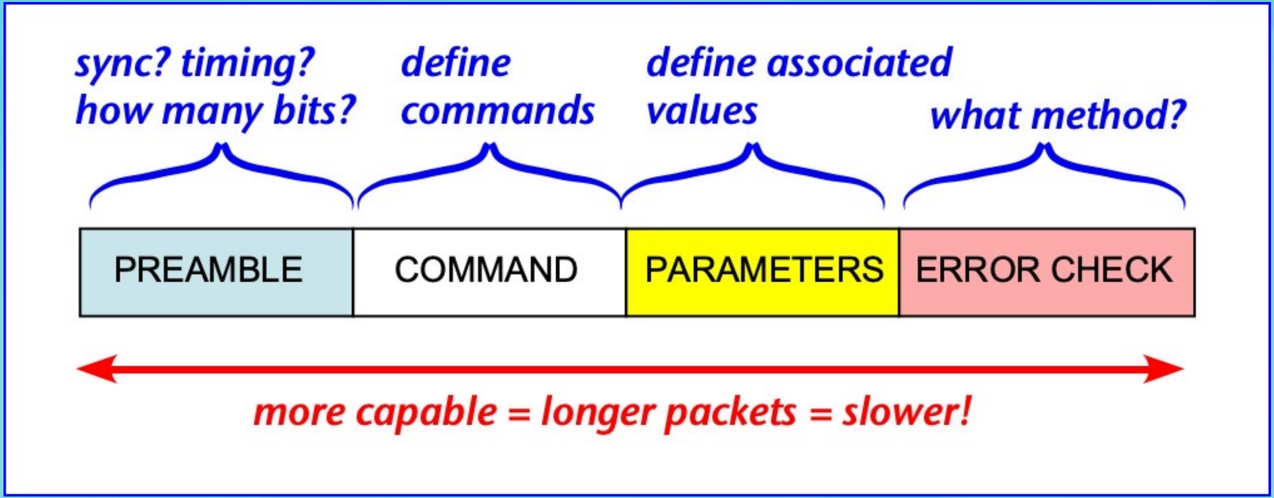
Based on: Implementation of Digital Signal Processing: Some Background on GFSK Modulation, S. Gerez, U. Twente, March 2016

Communications Protocols

- Packet structure
  - Example: Passive RFID
  - Example: Active Beacon
- Medium access

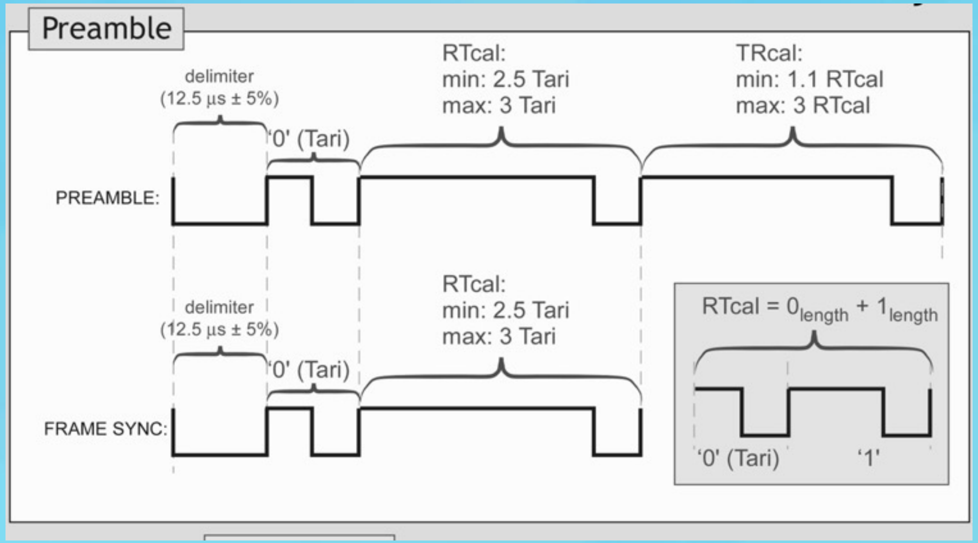
Packets

- Once signal is modulated, information is usually sent in discrete packets
  - Preamble, address/command, data, error checking
- Huge variety of standards; some of the most common are
  - ISO 15693/14483 for inductive
  - EPC Class 1 Gen 2 v2/3 for passive RFID (ISO 18000-63)
  - Bluetooth Low Energy for beacons
  - 802.15.4z Ultrawideband



ISO 18000-63 (EPC C1G2) Reader Packet

- C1G2 uses different packet structures for different commands
- Preamble contains PIE/FM0-MMS timing information for rest of packet
- Most common packet: Query
  - 8 parameters + (short) error check



Query

	Command	DR	M	TRext	Sel	Session	Target	Q	CRC5
# bits	4	1	2	1	2	2	1	4	5
	1000	0: DR=8 1: DR=64/3	00: M=1 01: M=2 10: M=4 11: M=8	0: no pilot 1: pilot tone	00: all 01: all 10: ~SL 11: SL	00: S0 01: S1 10: S2 11: S3	0: A 1: B	0-15	

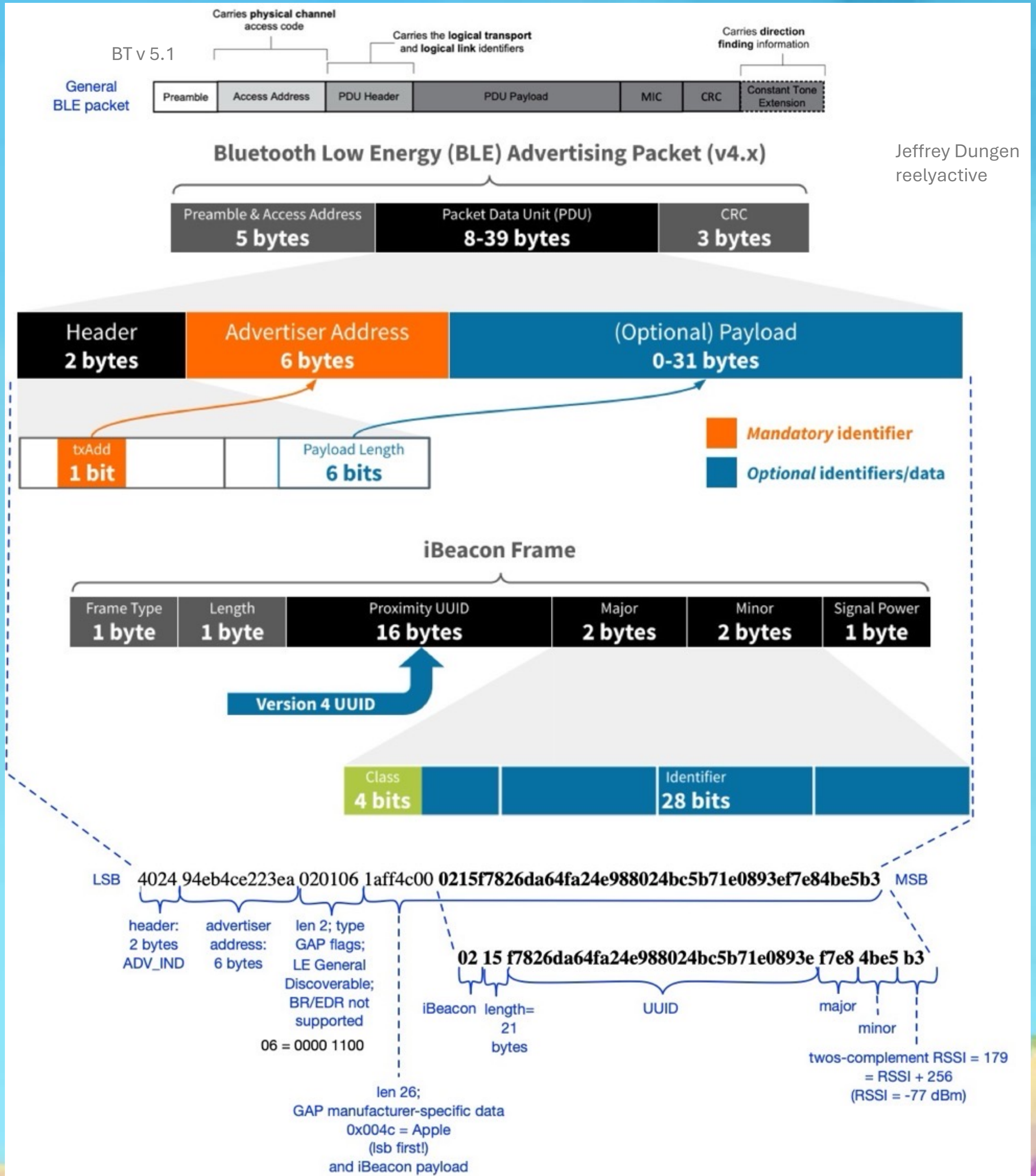
tag reply: preamble+RN16

Define tag reply (DR, M, TRext) — Tags that participate (Sel, Session, Target) — Who talks when (Q)

Gen2 V3 has some additional provisions for avoiding marginally-powered tag responses

Bluetooth Low Energy (BLE) Packet

- Basic BLE using simple GFSK modulation, 1 Msps
  - Up to 2,120 bits/packet
- Example packet: iBeacon (Apple)
  - Preamble/access removed for clarity
  - Type: BLE only (standard Bluetooth not supported)
  - iBeacon ID
  - RSSI = received signal strength at 1 meter, for estimating distance

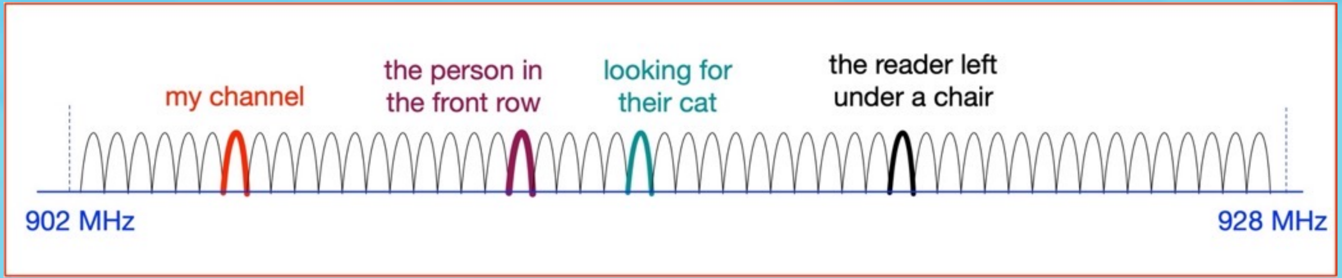


Jeffrey Dungen reelyactive

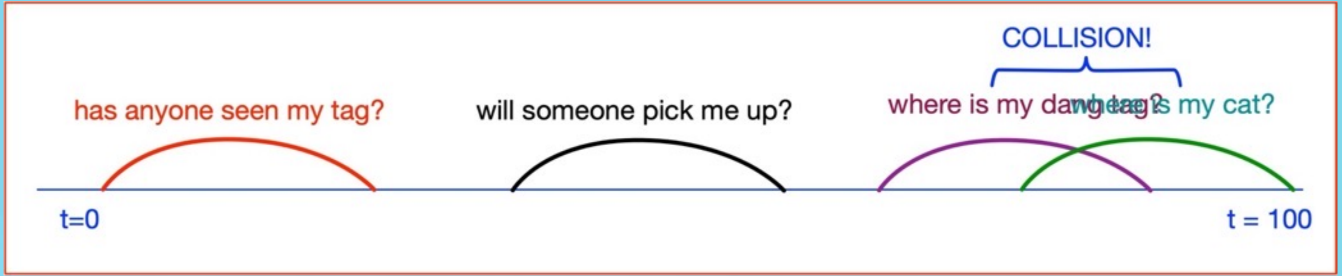
Medium Access

- In a simple world there's only one reader and one tag
  - In the real world everybody competes for the same frequency at the same time
- Various ways to take turns:
  - Frequency Division Multiple Access: sing a different note
  - Time Division Multiple Access: wait for a solo
  - Code Division Multiple Access: counterpoint

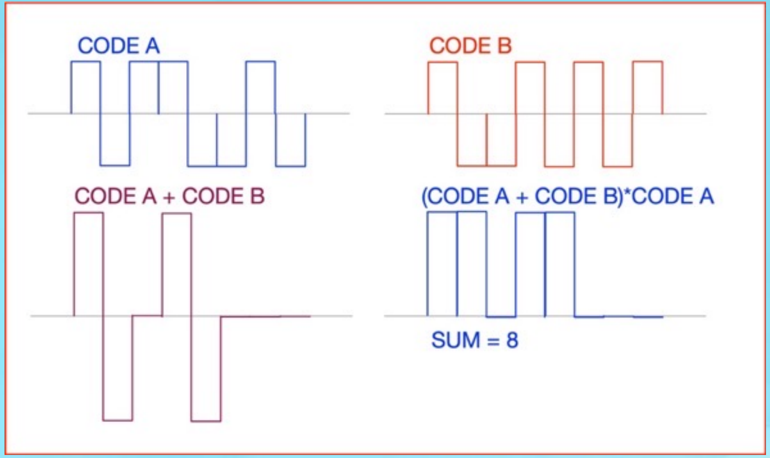
FDMA



TDMA

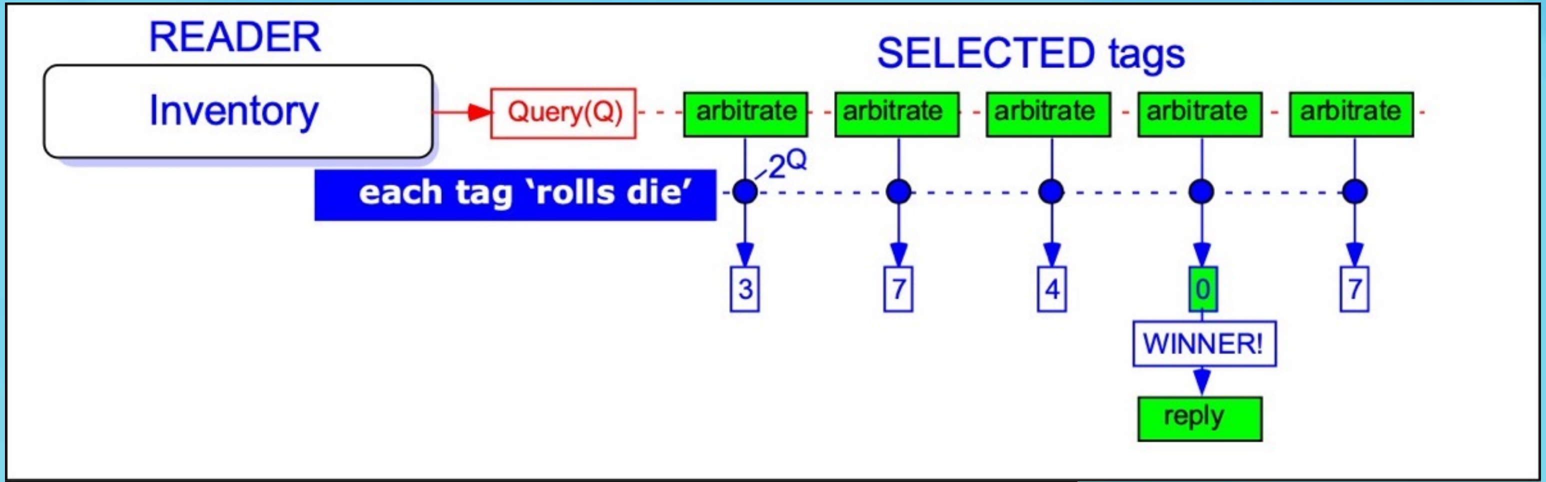


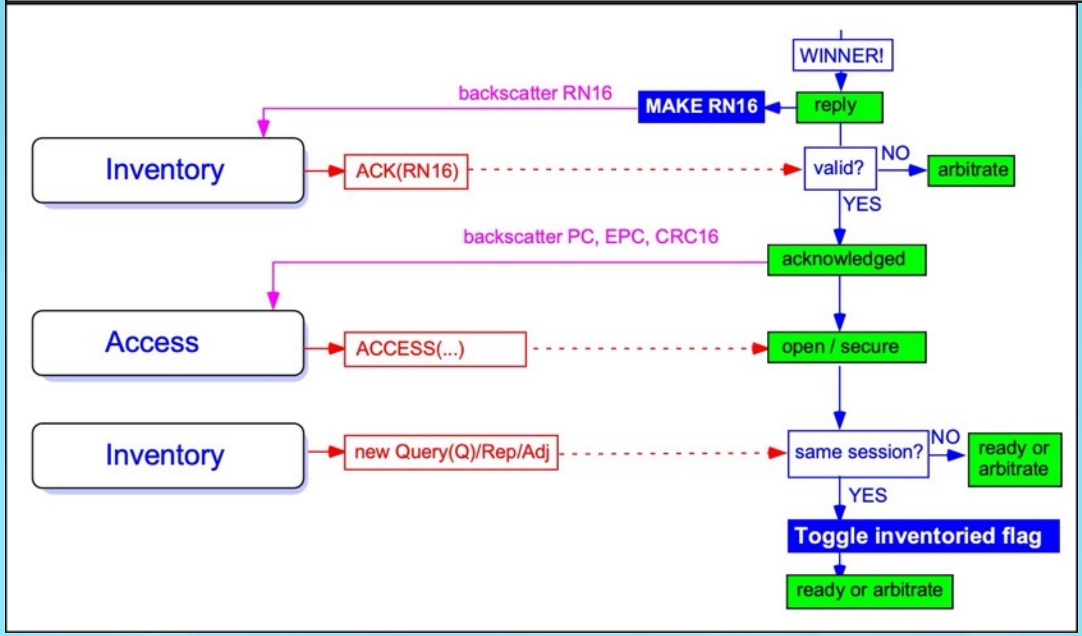
CDMA



Passive UHF RFID: Mix of FDMA/TDMA

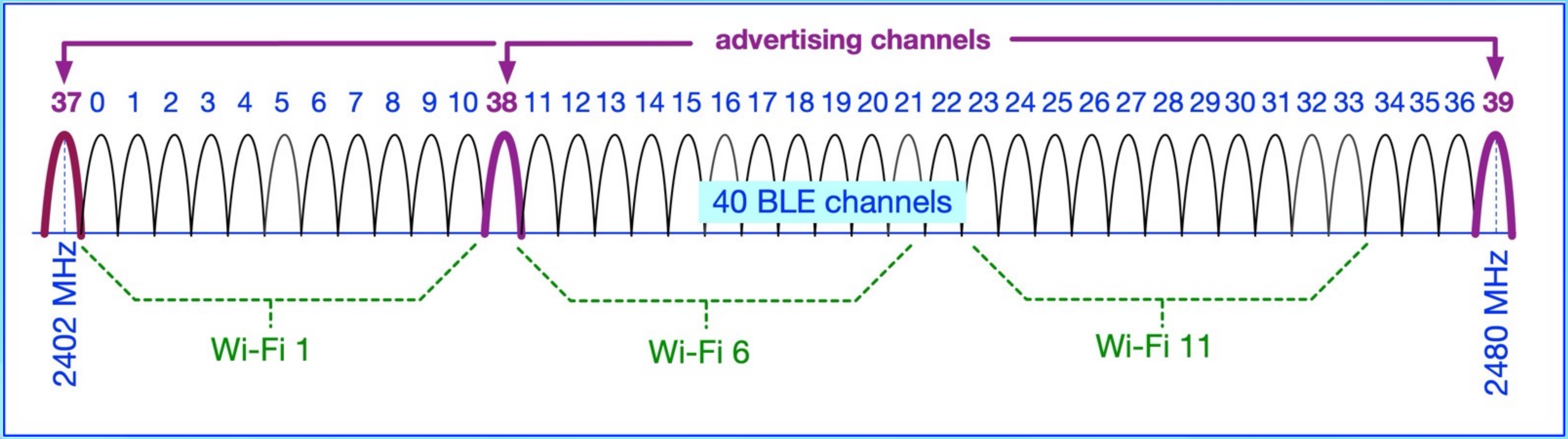
- FDMA, US ISM: Reader chooses a new 500 kHz band at random every 0.4 s
- TDMA, Slotted Aloha: Reader sends a Query command, tags choose random #, count down until 0, then reply
  - IF tag reply is acknowledged, that tag owns the frequency band until discussion with the reader is complete





BLE: Mix of FDMA and Whenever

- Beacons that just post information talk whenever they want to
- They can also advertise to form a connection
- Both cases use advertising channels 37, 38, 39, which do not overlap the main 2.4 GHz Wi-Fi bands
  - Back-and-forth uses random sequence over all channels

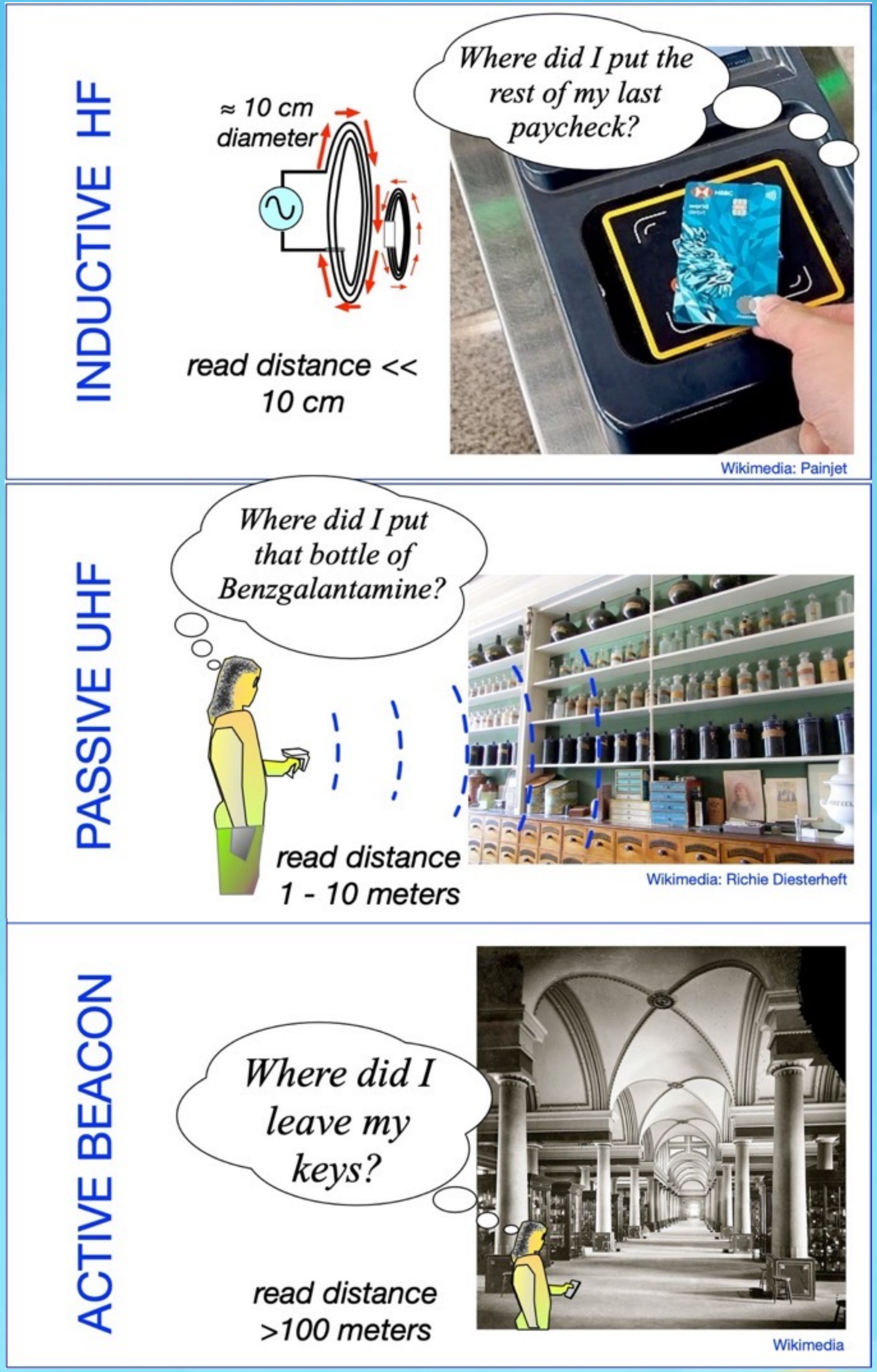


Finding Stuff

- Overview of Radio Location
- Received Signal Strength
- Time of flight
- Angle of arrival
- Phase
- Practical Location

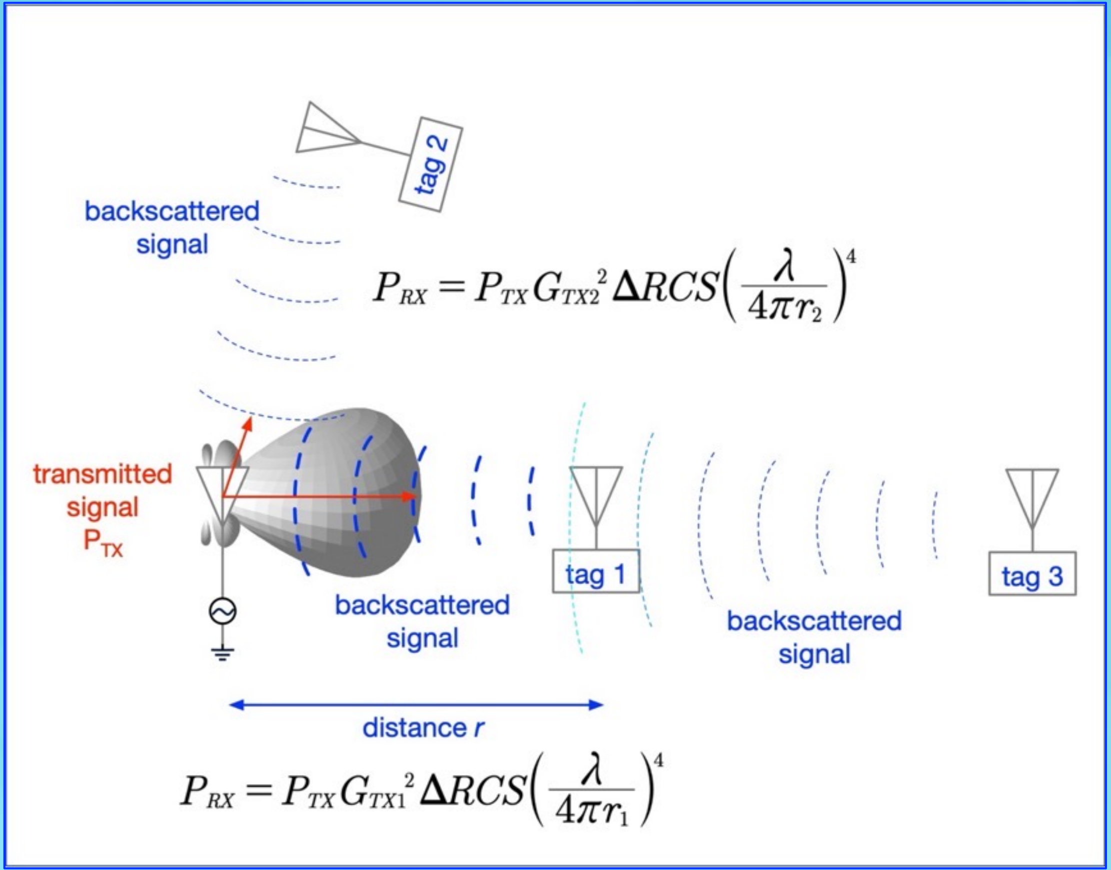
Radio Location

- Identifying an object may not be helpful if we don't know where the object is!
- Tradeoff with range:
  - Inductive tag range 1 to a few cm: if I read it, it's there!
  - Passive tags up to 10's of meters: where is it in the room (or next door)?
  - Active beacons, 10's to 100's of meters: where is it in the neighborhood?



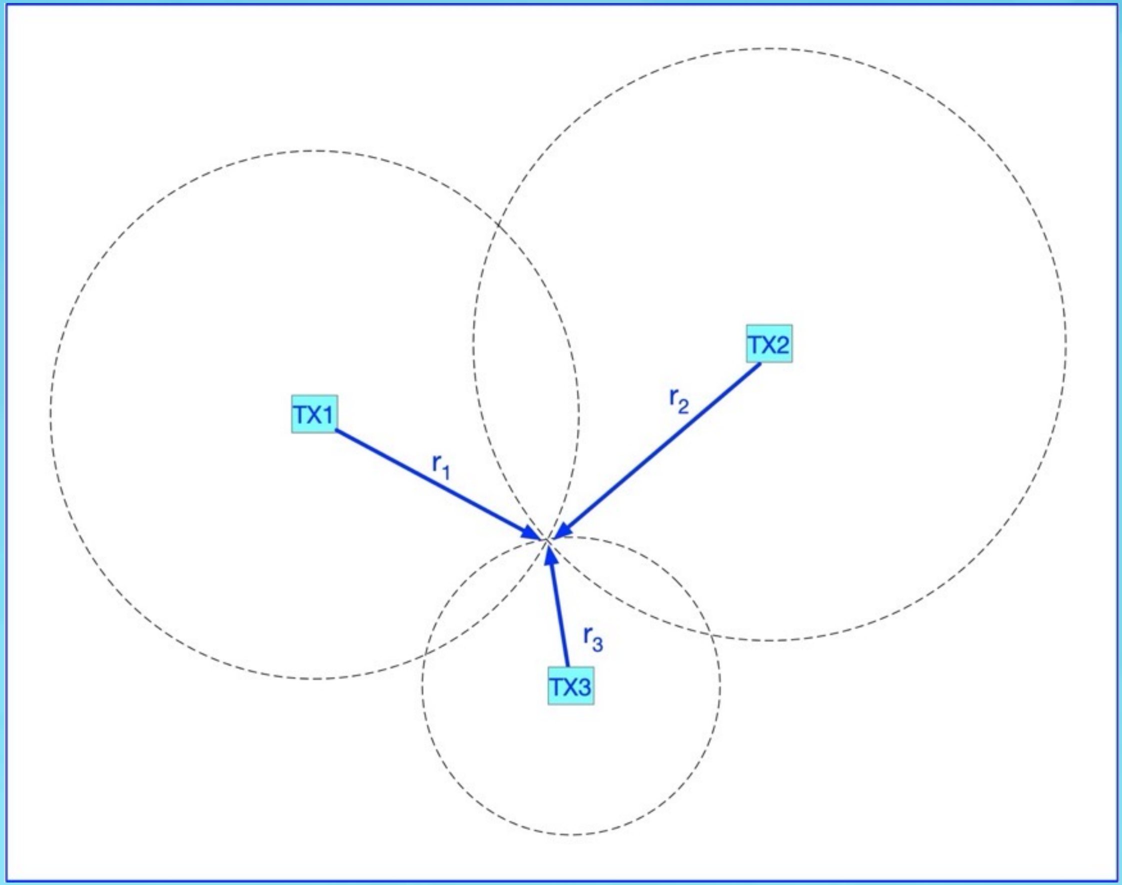
Received Signal Strength (RSSI)

- Beacon: Received power ≈ (antenna gain)*(1/distance)^2
- Passive tag: Backscatter power ≈ (antenna gain)^2 * (1/distance)^4
- Both distance and angle of incidence affect RSSI
  - Use multiple antenna locations OR orientations to distinguish between distance and angle



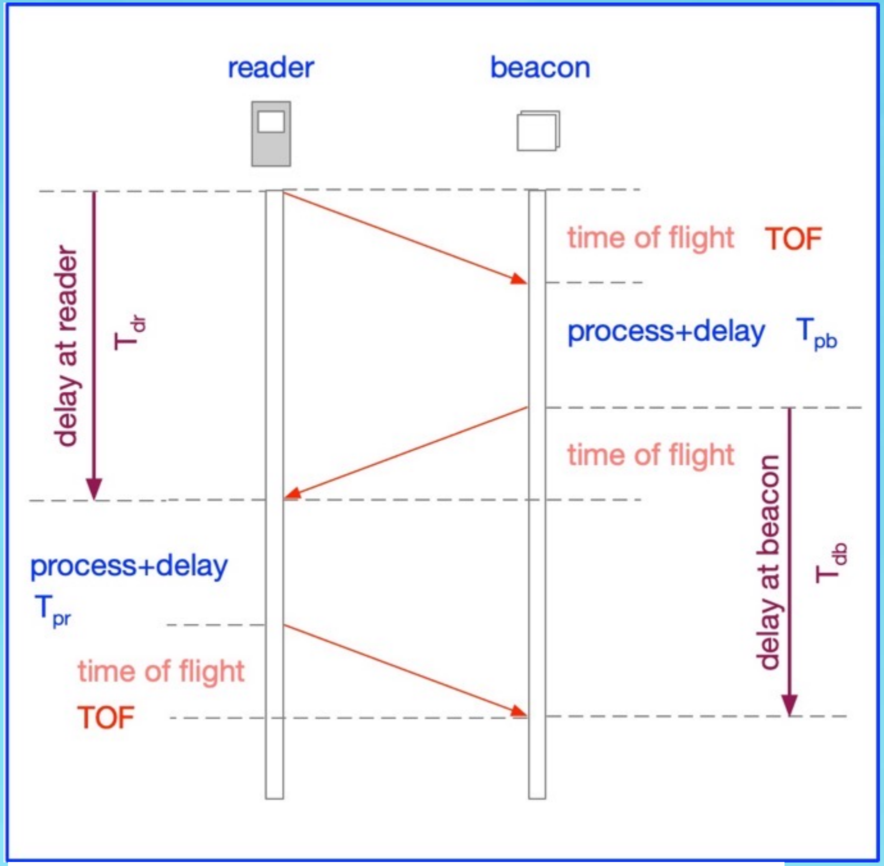
Time of Flight

- RF signals move at the speed of light
  - Distance = (propagation time) • c
- Distance to three non-collinear points = location
  - At least in a plane!
- BUT: Absolute position requires knowledge of absolute time of transmission and reception
  - Often not available



Two-Way Time of Flight

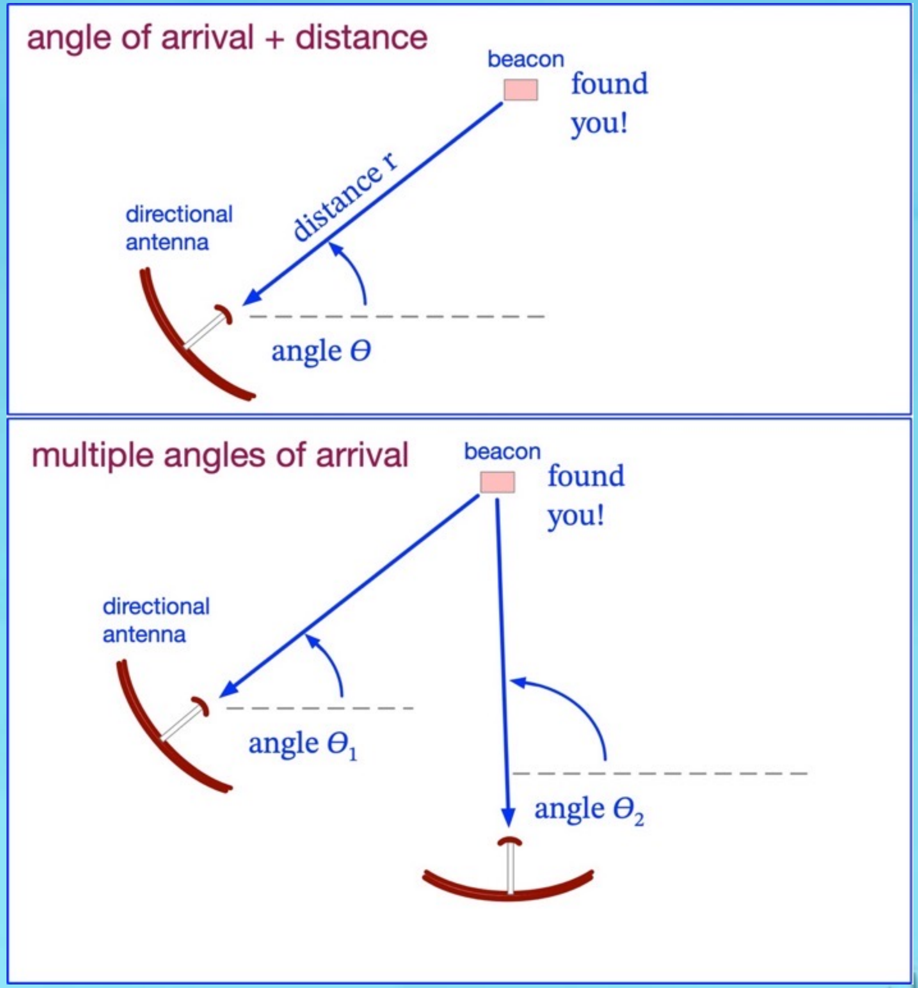
- Bidirectional transmissions can be used to estimate total delay
  - BUT the time for processing received signals and retransmitting is often bigger than propagation times!
    - Example: 5 meters = 15 ns time of flight, whereas typical process delays are many microseconds
  - So use nominal delay, report delay value in packet, send both ways
    - error is then the clock error * DIFFERENCE in delay times, can be < 1 ns
  - Roughly what is used in 802.15.4 with ultrawideband pulsed signals; also supported in BLE, but lower precision



$$TOF = \frac{1}{4}(T_{dr} + T_{db} - T_{pr} - T_{pb})$$

Angle of Arrival

- If we have a directional receive antenna (or array), we can determine signal angle of arrival
  - Rotate a single directional antenna and look for maximum amplitude OR
  - Use phase-vs-position for an array
- If we know the range from time-of-flight, OR we have multiple antennas not collinear with the signal, we can find the location
- BUT easily fooled by multipath!



Phase-Based Location

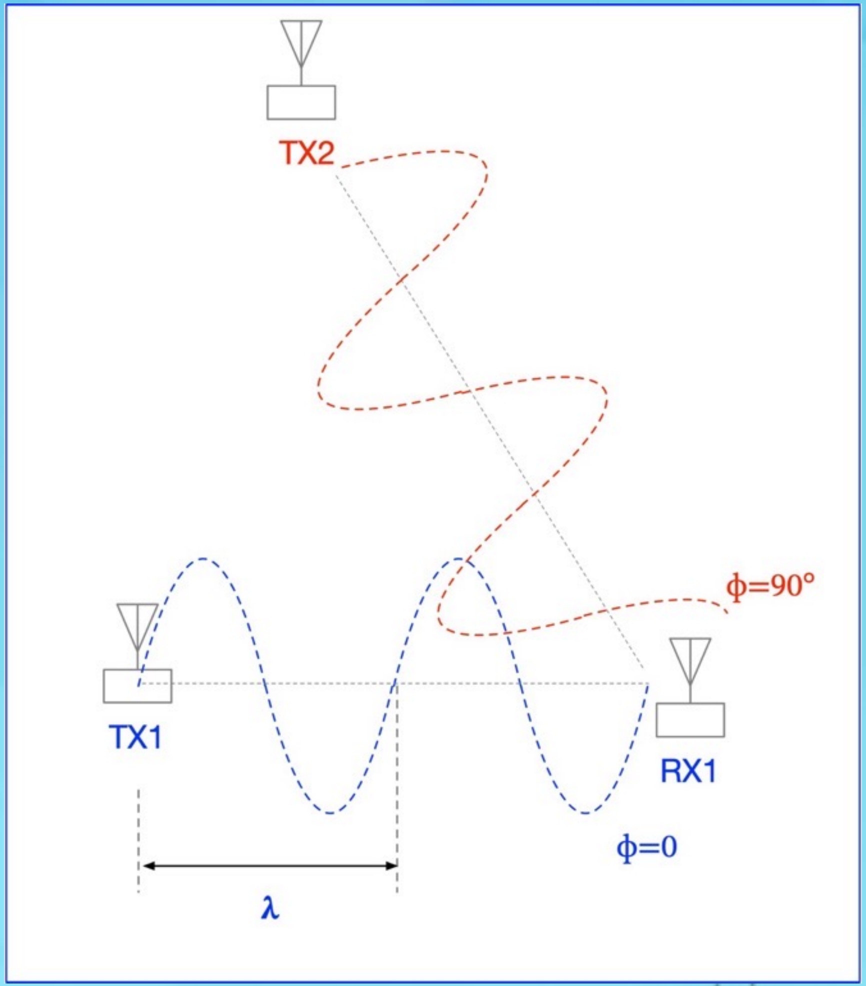
- A single frequency wave has a specific phase at any place and time
- If I can measure the phase of a received signal, I know exactly where I am in the wave
  - BUT I do NOT know which wave I'm in!
- CHANGE in phase vs. frequency gives range

$$\phi = kd = \frac{2\pi f d}{c} \rightarrow \frac{\Delta\phi}{\Delta f} = 2\pi \frac{d}{c}$$

$$d = 3\,m \rightarrow \frac{d}{c} = \frac{3}{3 \times 10^8} = 10\,ns$$

$$\Delta f = 20\,MHz \rightarrow \Delta\phi = 1.25\,rad = 72^o$$

Used in BLE channel sounding, but requires careful phase calibration

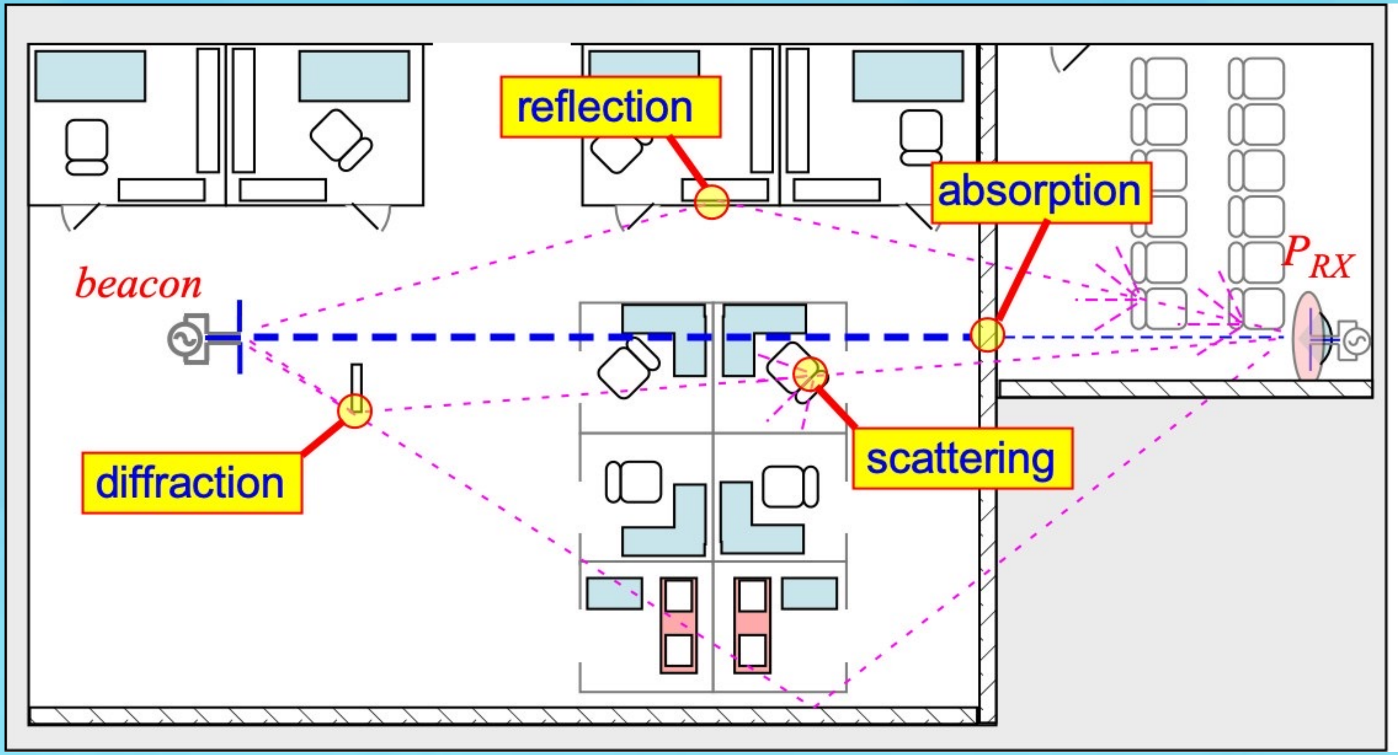


Practical Location (EPC Gen2)

- The simplest way to find objects with UHF RFID depends on SIMPLE handheld readers, basic RSSI data, and HUMAN skills:
  - Handheld reader with short range and some antenna gain
  - Wander through candidate area until you detect the tag you want
  - Randomly vary position and orientation, watch for INCREASE in signal strength
  - Human and reader MOVE in the direction of maximum signal strength
  - ITERATE until visual identification is possible
- VERY fast and efficient in retail environments
  - Robust to propagation issues because you iterate to close range
  - Generalizable to automated procedures
    - e.g. Motroni et. al., IEEE JRFID #8 p. 559, 2024, using phase history

Real Environments

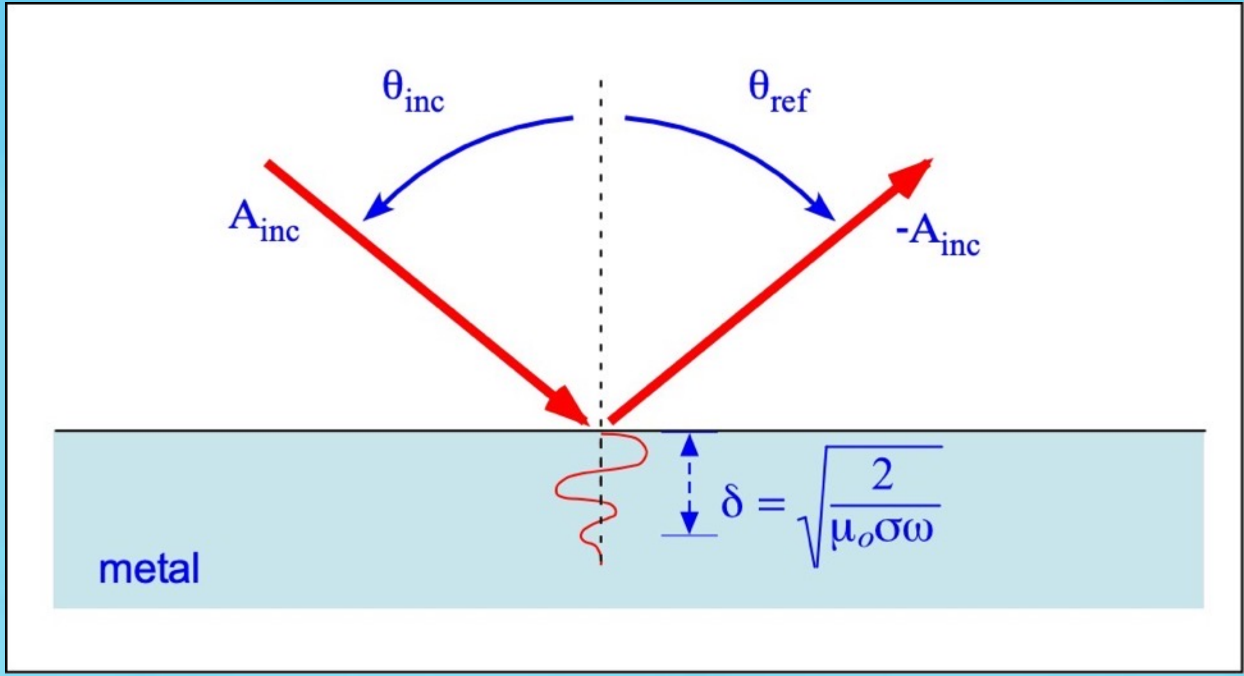
- Many challenges for communication /localization in realistic environments
  - Reflection
  - Absorption
  - Diffraction
  - Multipath
  - Constructive/destructive interference, fading



Backscatter tag goes both ways!
Everything is squared!

Reflection from Metal Surfaces

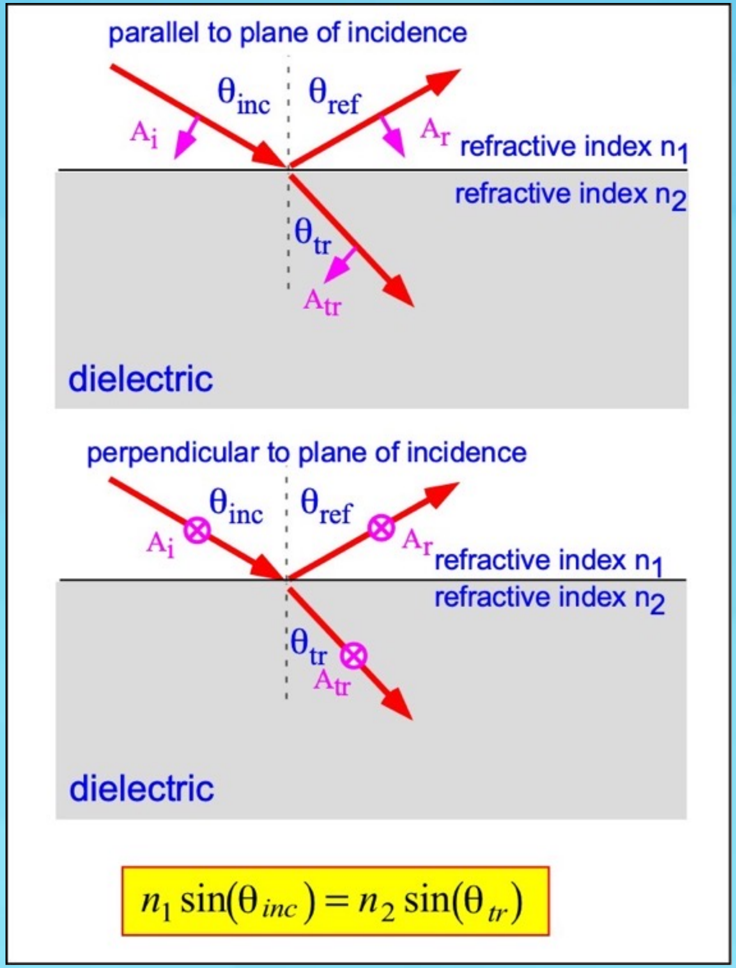
- Incident potentials induce motion of electrons in metals, creating a second wave: REFLECTION
- Smooth metal surface:
  - Angle of incidence = angle of reflection
  - Essentially zero transmission through the metal (but see Diffraction!)



Typical values of δ 1-10 microns at GHz frequencies…

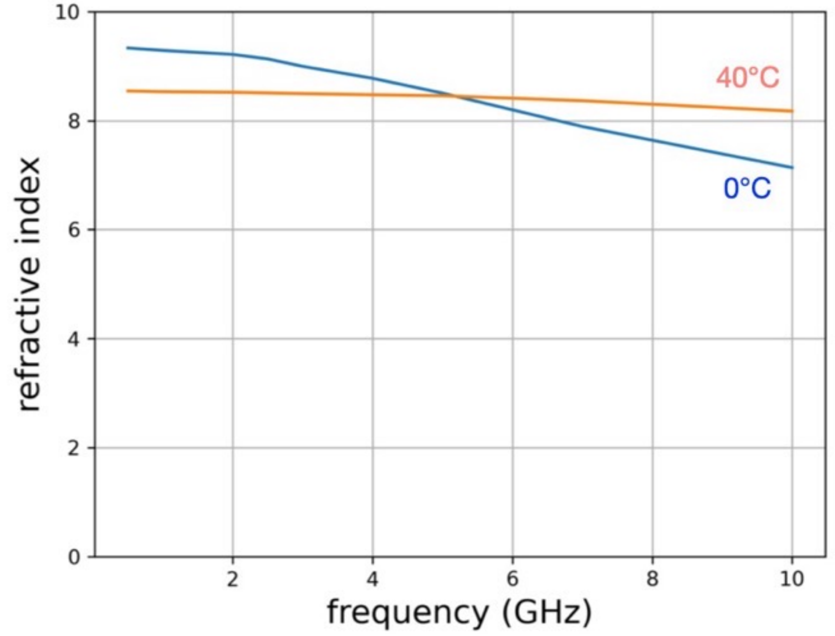
Dielectric Surface

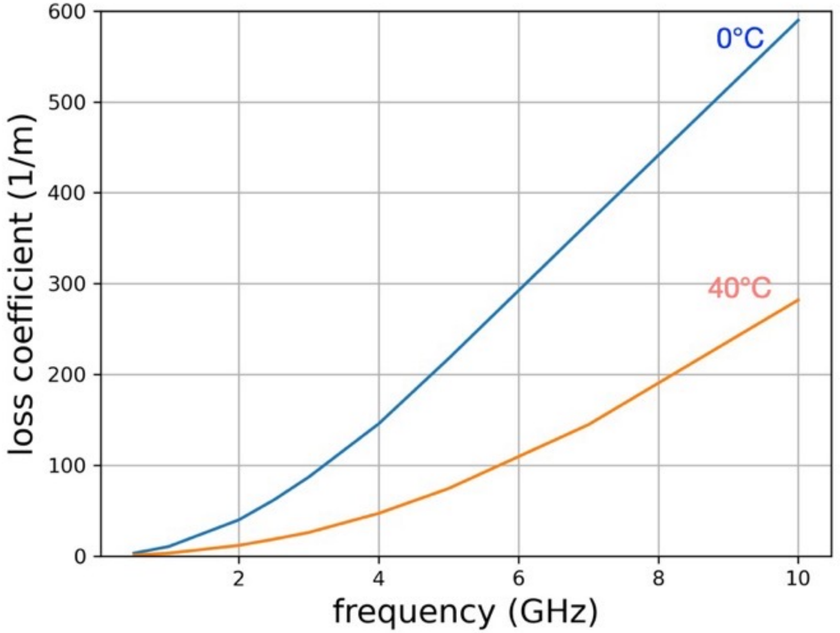
- Part of signal is reflected, part transmitted through dielectric
  - Often also absorption
- Transmitted signal is usually oriented differently from incident signal, but returns to original direction on exit IF surfaces are parallel
- Angle of reflection is independent of polarization, but magnitude is NOT!
  - Ex: 0 reflection from the floor for vertical polarization, ≈ 60° incidence (Brewster's angle)



Water

- Water is an unusual dielectric
  - Very high dielectric constant at RF frequencies:
    - n = 8 to 9 for f < 5 GHz
  - Absorption ≈ 7/m @ 0.9 GHz, 40/m @ 2.4 GHz at room temperature
    - 10 dB attenuation in 15 cm @ 0.9, 2.5 cm @ 2.4 GHz
- Humans are mostly water, strong reflectors and absorbers
- Food items are also often all wet

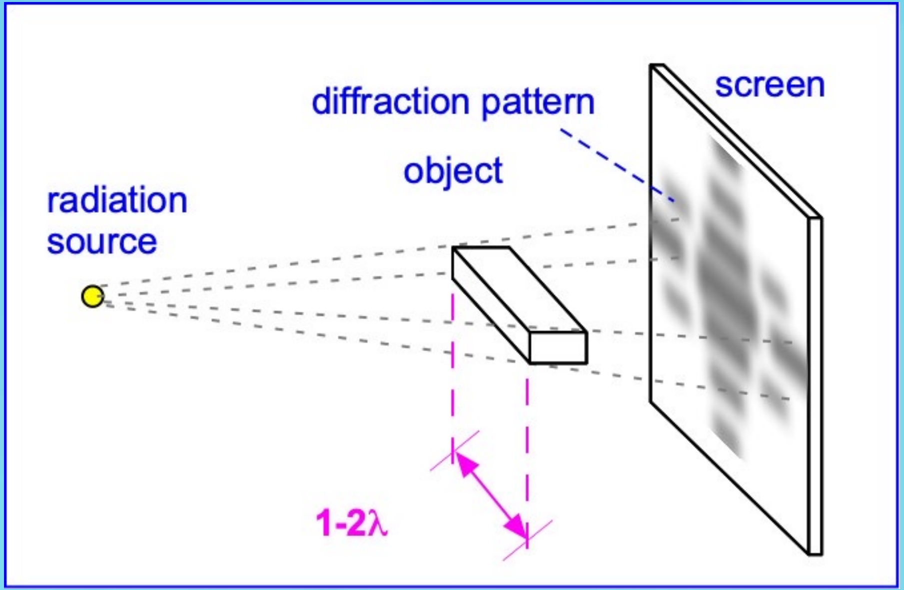




based on Turner et. al., J. Atmospheric and Oceanic Tech v 33 p. 33 (2016)

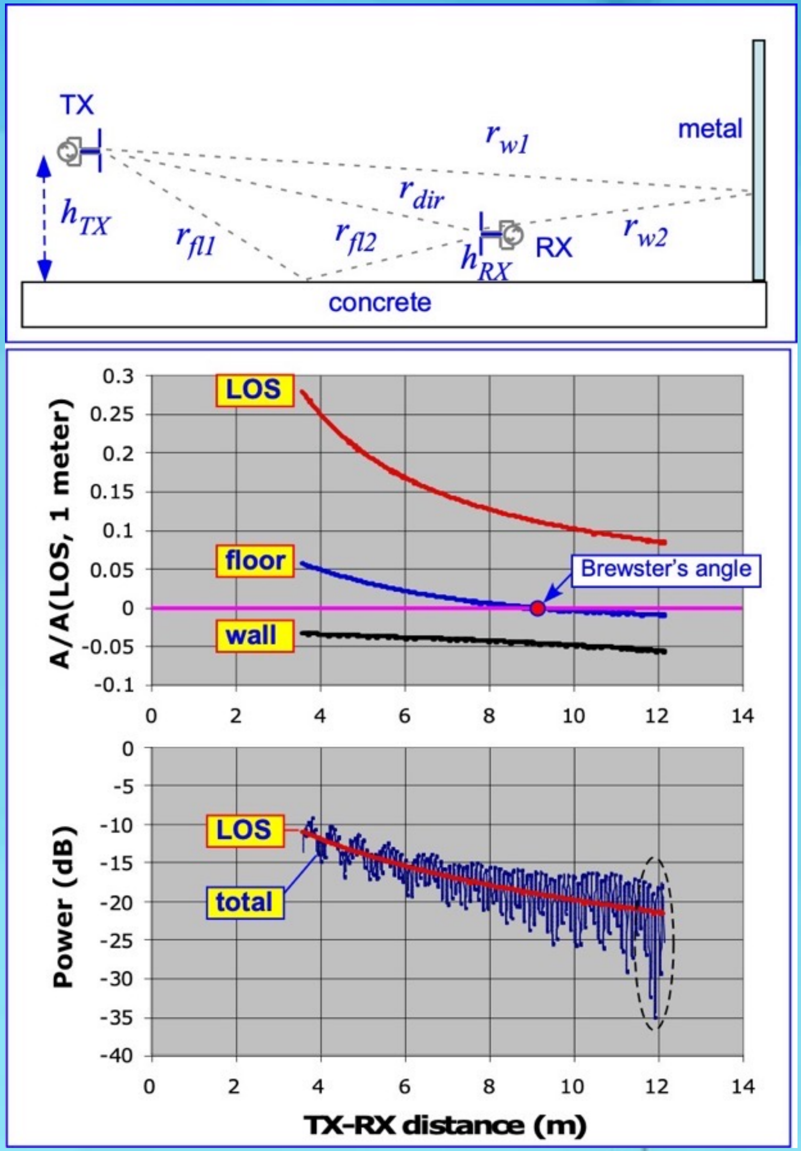
Diffraction

- The current that sends fields to 0 inside the metal does NOT necessarily have the same effect far away: DIFFRACTION
  - Typically important for object size of ≈ 0.1 wavelength to a few wavelengths
  - That's 3 cm to 3 meters for 1 GHz = TYPICAL SIZE OF OBJECTS IN HUMAN WORLD
- Result is that waves "bend around" human-sized obstacles
  - obstacles act as (re-)transmit antennas
  - response can be very complex



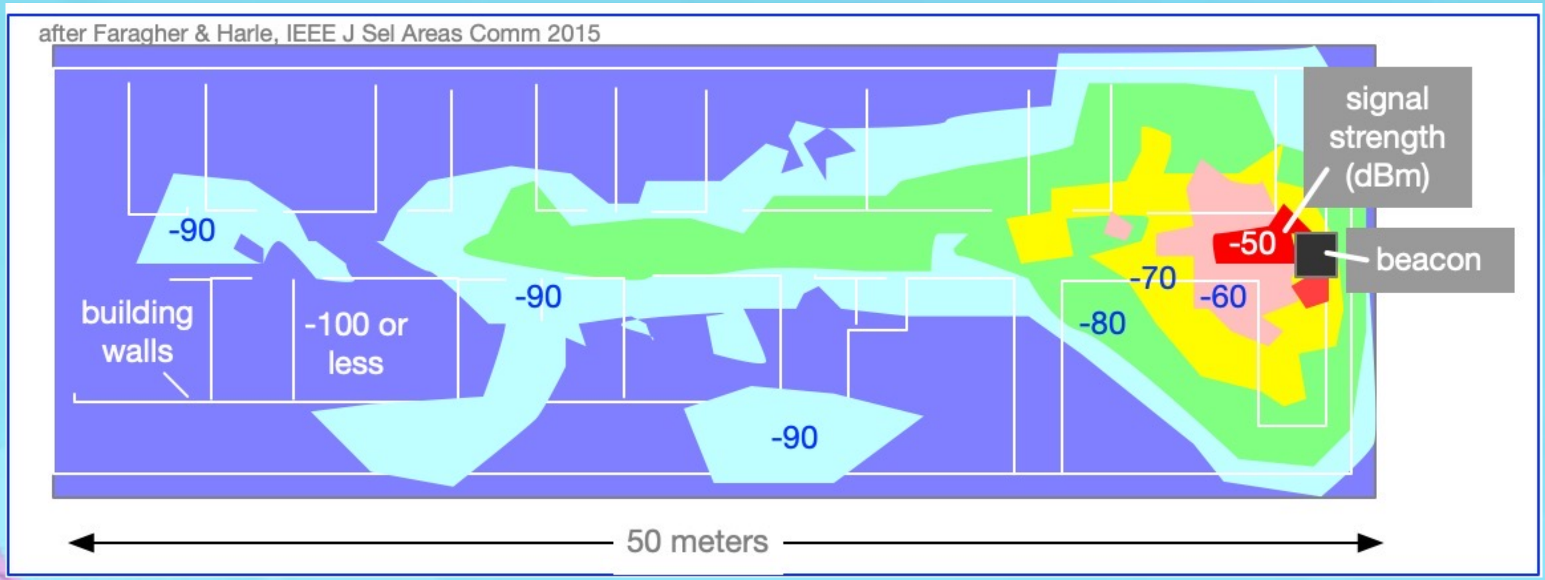
Multipath

- Real environments usually have LOTS of stuff
  - Direct, reflected, diffracted, transmitted beams may add or subtract depending on relative phase, polarization
- Result: MULTIPATH FADING
  - VERY complex spatial/time dependence of amplitude and phase for each path
  - Add them all up (with receive antenna gain) to get – a mess!
    - SIMPLE example at right: 2.45 GHz direct, floor reflection, wall reflection already give >10 dB fading at 10 meters
    - Real world is often much more complex



Empirical Approach: Fingerprinting

- Collect RSSI data for multiple reader locations and multiple tag or beacon locations
- AI or numerical fit to match received signals to environment and locate tag or beacon



Example for BLE beacon in building interior

PROBLEMS:

- Time dependence as people and things move
- Computational complexity with multiple beacons

Finding Things Found Out

- Accurate location is possible:
  - In open spaces, especially with UWB signals
  - In complex spaces if multiple simultaneous paths AND characterization data (fingerprints) are available
  - With human (or AI) control of antenna position/orientation and ability to get to short range

Conclusions

- Radio waves have many advantages over light for finding and identifying objects in SOME circumstances
- Different frequencies and wavelengths have different time and space scales and behavior in practical environments, thus different applications
- Transmission and reflection can both be used to send signals
- Equipment choice is a complicated tradeoff of size, cost, speed, application requirements, regulations, standards
- Once you get something that works you might leave it alone!
  - Or not… that's what the conference is for!

Thanks to… (at least)

- The D4N team
- Brendon Parsons
- Christopher Saetia
- Sam Singh
- Rich Marshall
- Juho Partanen
- RFID Inc.: Lucas Heurich, James Heurich
- ASYGN: Sofia Benouakta
- Pavel Nikitin

…and to everyone in the audience who stayed awake through the talk!

ANY QUESTIONS…

…YOU DIDN’T WANT TO ASK

Because you don’t want to know

Additional Information

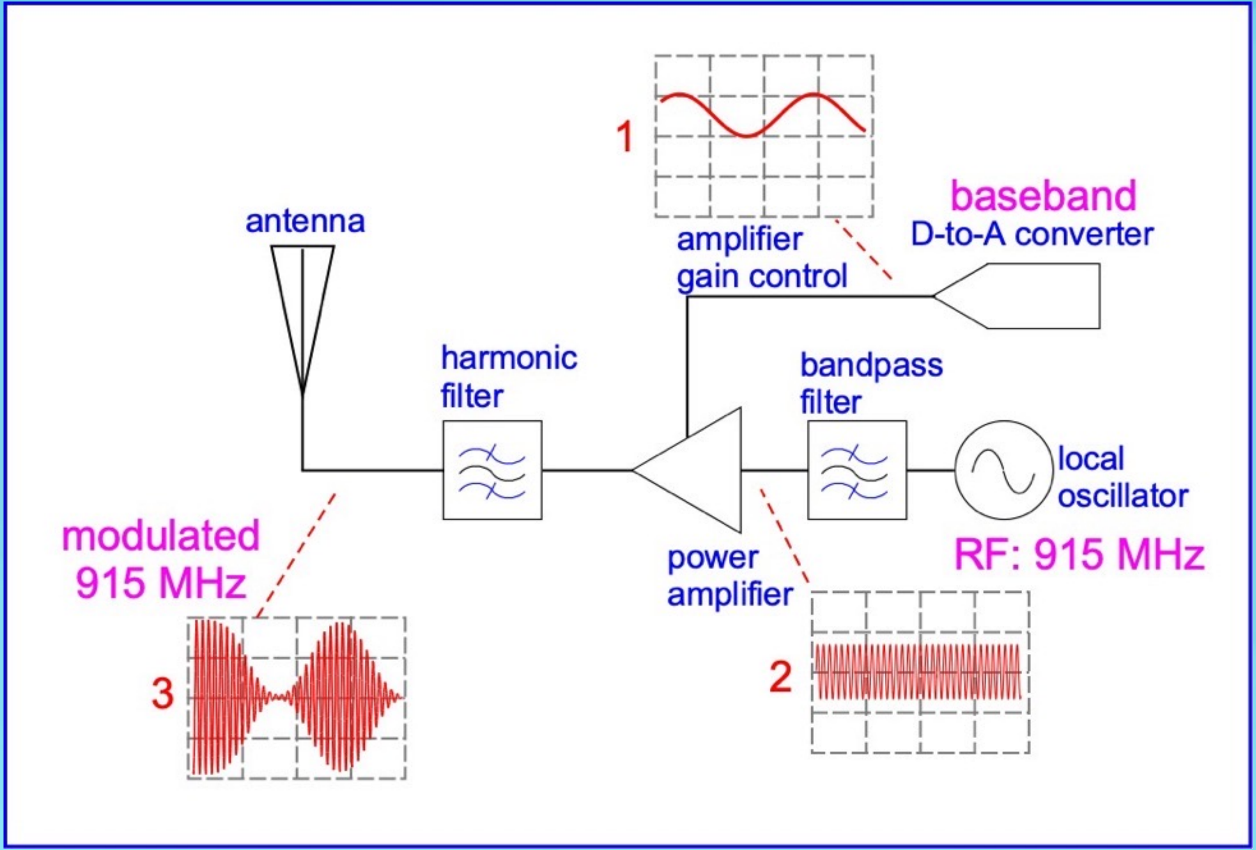
- Radio architectures
- BLE packet data ordering
- Transmission lines and the Smith chart
- RFID/BLE bands and regulatory issues
- Statistical models of received power in real environments
- RF formula summaries (Greg Durgin)
- Ultrawideband modulation and coding
- Phase-based ranging details
- Tag modulation
- Sensor tags
- Dielectric reflection: Brewster's angle
- Complex exponentials, gradients

Radios

- Reader Architecture
  - Transmitter
  - Receiver
  - Combined TX/RX
- Tag/Beacon Architecture
  - Chipless
  - Passive
  - Active

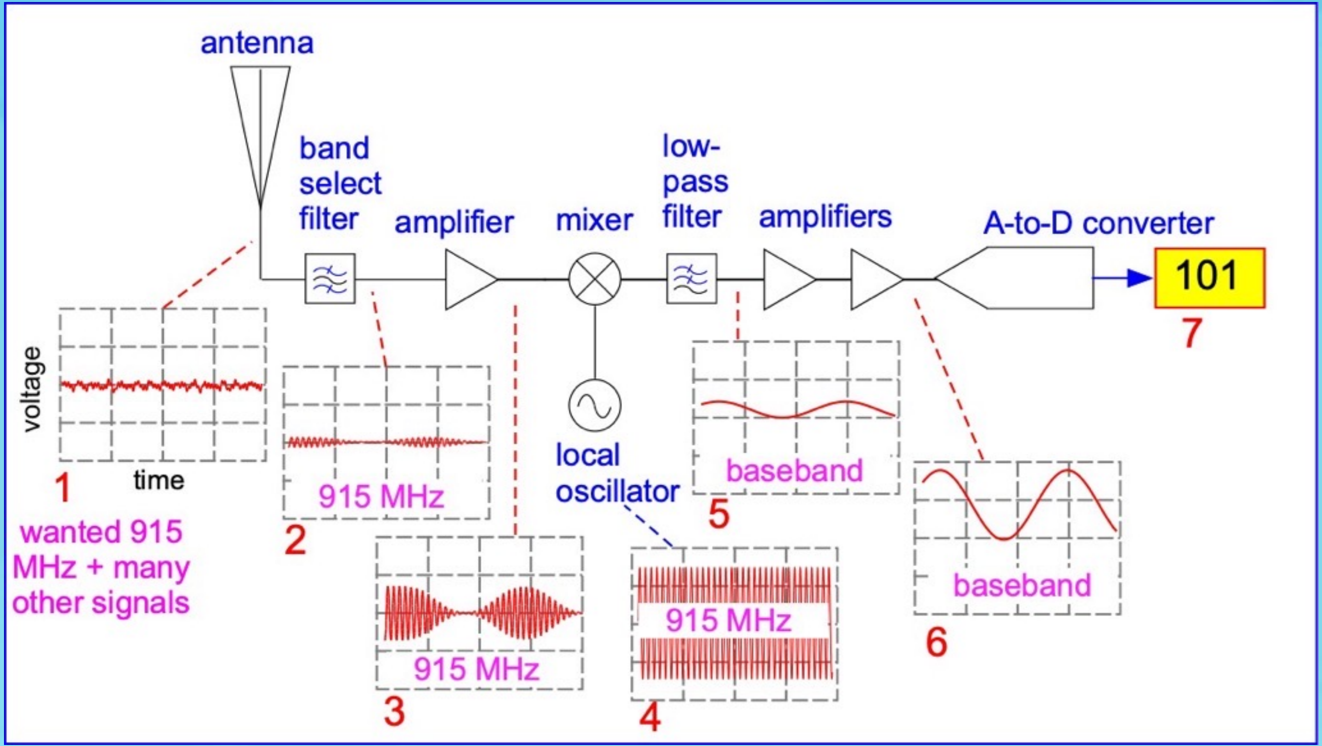
Example Transmitter Architecture

- Direct-conversion with modulation:
  - Local oscillator creates constant sinusoidal signal; frequency varies e.g. over allowed channels in 902-928 MHz ISM band
  - Amplify with varying gain determined by baseband signal
  - Resulting modulated signal is filtered to remove any harmonics, then sent to antenna
  - Note that in many cases, two signals 90 degrees out of phase may be used to support phase-modulation as well as amplitude-modulation



Example Receiver Architecture

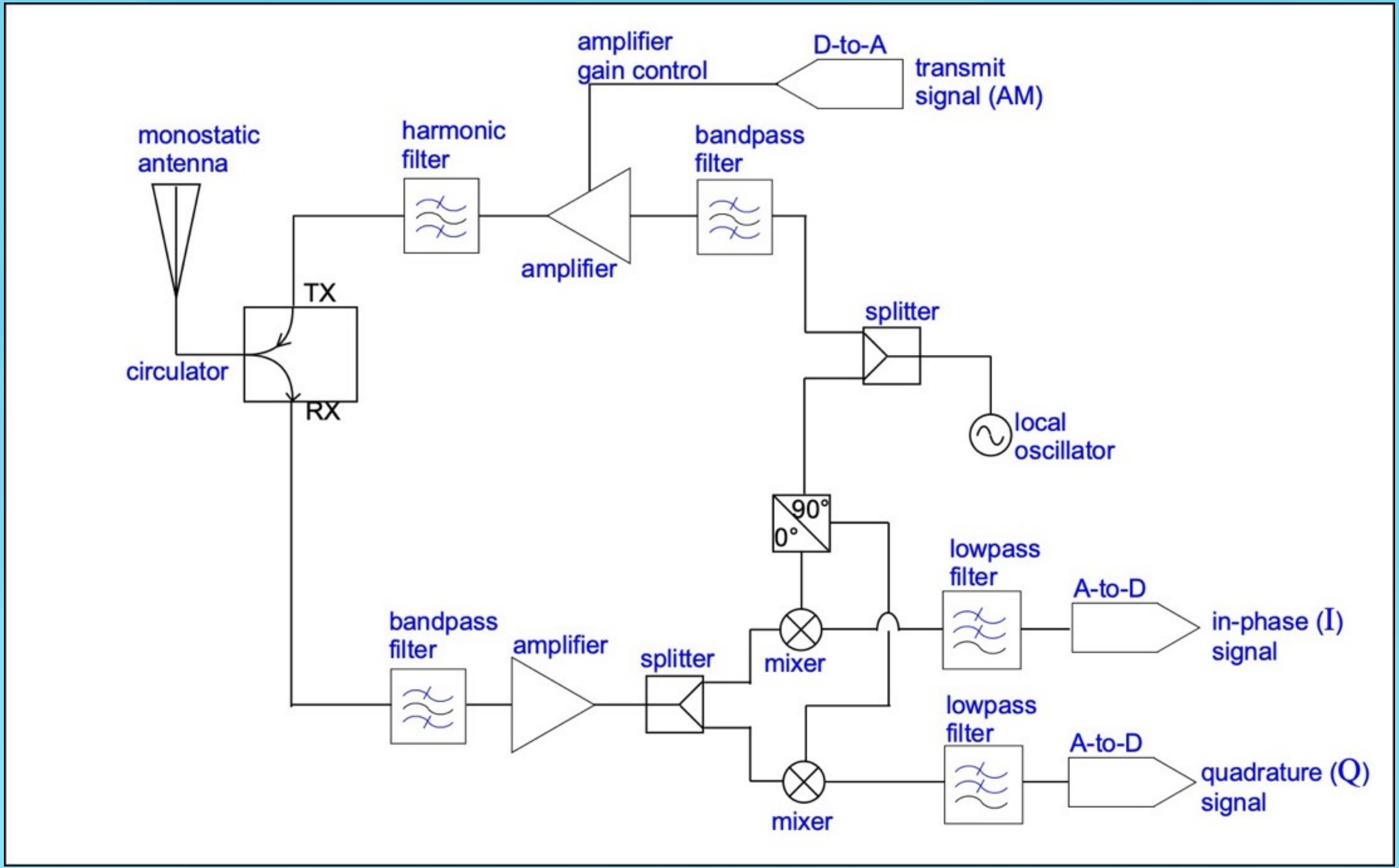
- Direct Conversion receiver:
  - Optional filtering of band (e.g. US ISM 902-928 MHz)
  - Optional amplification of RF signal
  - Local oscillator signal mixed with received signal using nonlinear device:
    - Result: f(LO) + f(RF), f(LO) – f(RF)
  - Filter to select only the difference (f(LO)), amplify, convert to digital



For backscatter radio, the same local oscillator supports transmit and receive. Two separate paths using 90° phase-shifted oscillator signals (I and Q) may be used to detect phase of the received signal

Reader TX/RX Architecture

- Example of monostatic (one-antenna) reader
  - Single local oscillator for TX and RX, both direct conversion
  - Amplitude modulation for TX; in-phase/quadrature (I/Q) demodulation
  - Circulator connects both transmit and receive to one antenna, minimizes TX-RX coupling (we hope!)



after reader diagram from Pavel Nikitin

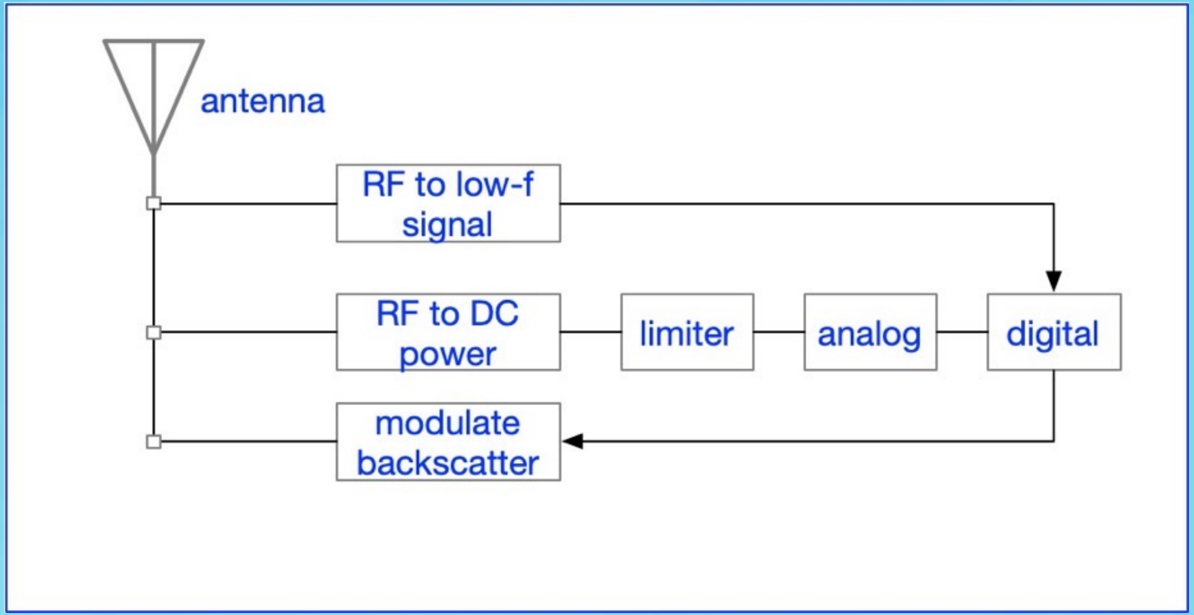
Commercial readers may include additional amplifier stages, other features

Tag Architecture

- Chipless tag needs to:
  - Vary RF response to send an informative signal to the transmitter
- Chip tag needs to:
  - Wake up when transmitted signal is present
  - Detect header and reader message(s)
  - Vary antenna behavior to backscatter response
- Active beacon needs to:
  - Send a fixed signal at a fixed time interval
    - Option to listen for trigger or turnon
    - Option to respond to sensor inputs
    - Option for full duplex communication with reader

Passive Tag Architecture

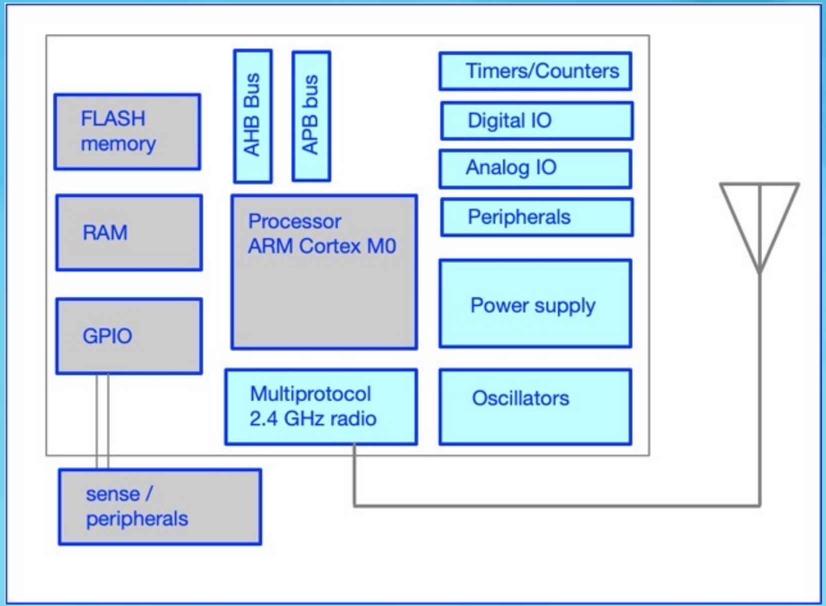
- Tag first needs to convert incident RF to DC to operate analog and digital circuitry
  - Stacked rectification to boost voltage
- Additional data blocks:
  - Envelope detector for data from reader
  - Modulate backscattered signal by changing load presented to the antenna to reply
- Details in Tutorials #2 and #3

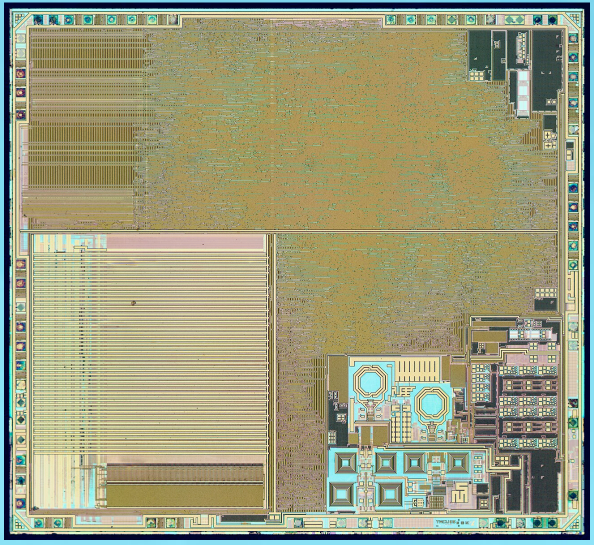


After Design and Implementation of A Sub-1V Analog Front-end for Passive UHF RFID Tag, J. Huang, J., Shen, X. Wang [Shenzhen Medica / Peking U] 2nd Int'l Conf Inf Tech Computer App (ITCA) 2020 p. 660

Active Tag Architecture

- Battery for power, memory for data
- Turnon: timer or optional sensor/listener
- Memory access, beacon transmission
- Optional interfaces to surroundings / sensor data
- Details in tutorial #4



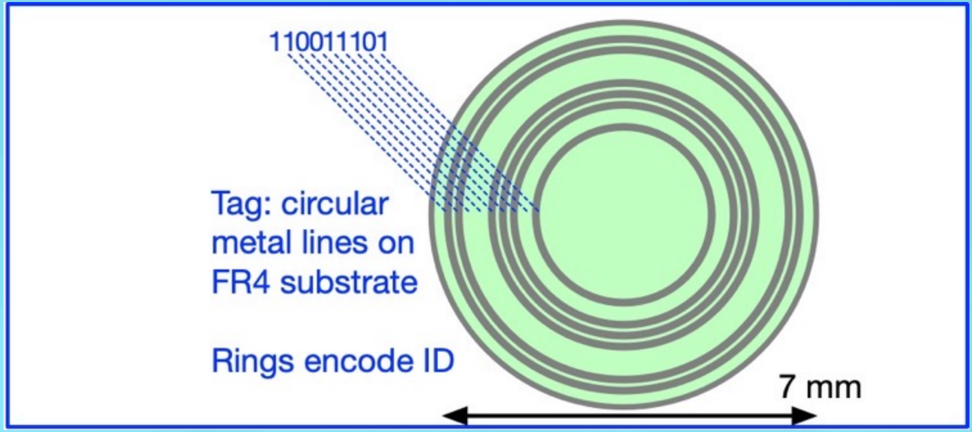


Nordic Semi nrf51822

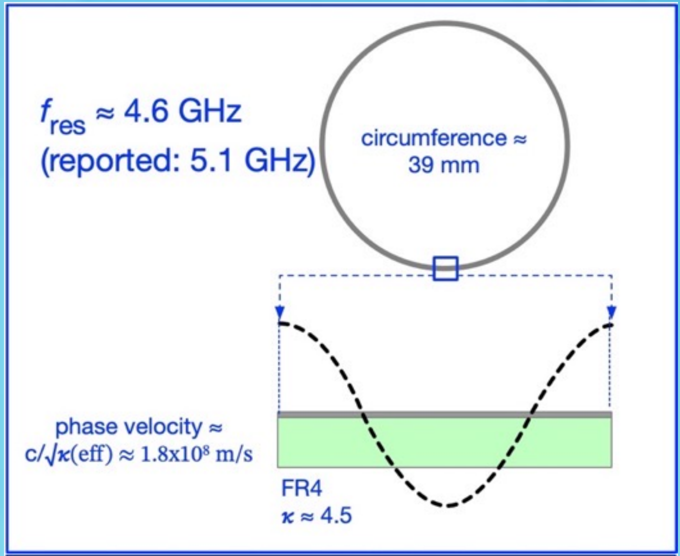
http://zeptobars.com/en/read/nRF51822-Bluetooth-LE-SoC-Cortex-M0

Chipless Tag Example

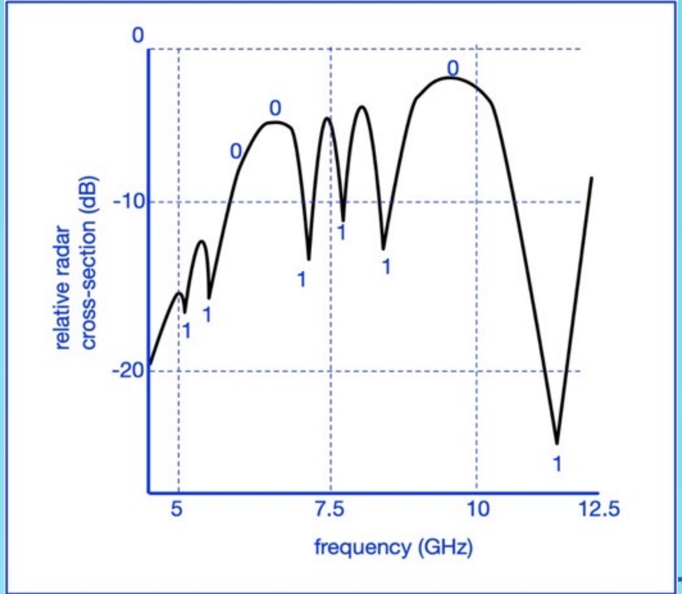
- Circular FR4 substrate with metallic rings as resonators
  - Based on Habib et. al. IEEE EIT 2016



- Roughly: just wave propagating around a circular microstrip line



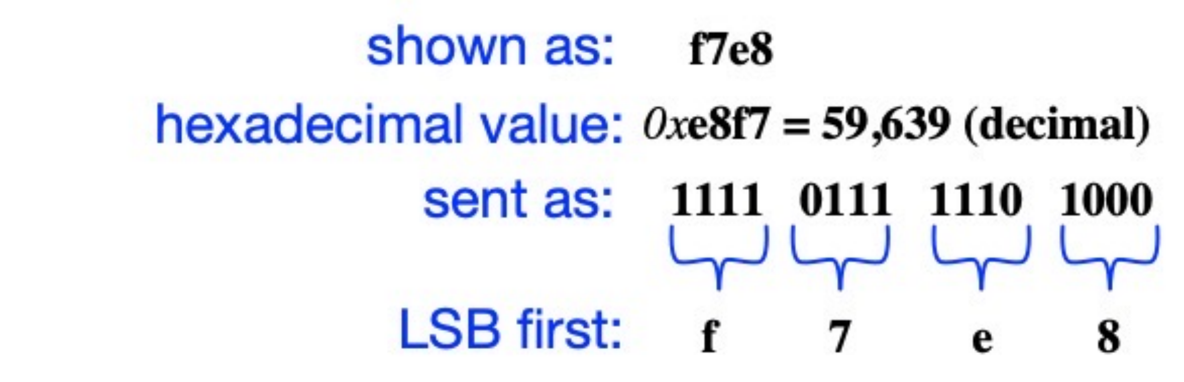
- RESULT: broadband reflection vs. frequency = tag ID
- No chip needed
  - BUT 9 bits = 512 tags! Not much ID space...



Response estimate based on Habib figure 5

Bluetooth Low Energy (BLE) Packet: Data Ordering

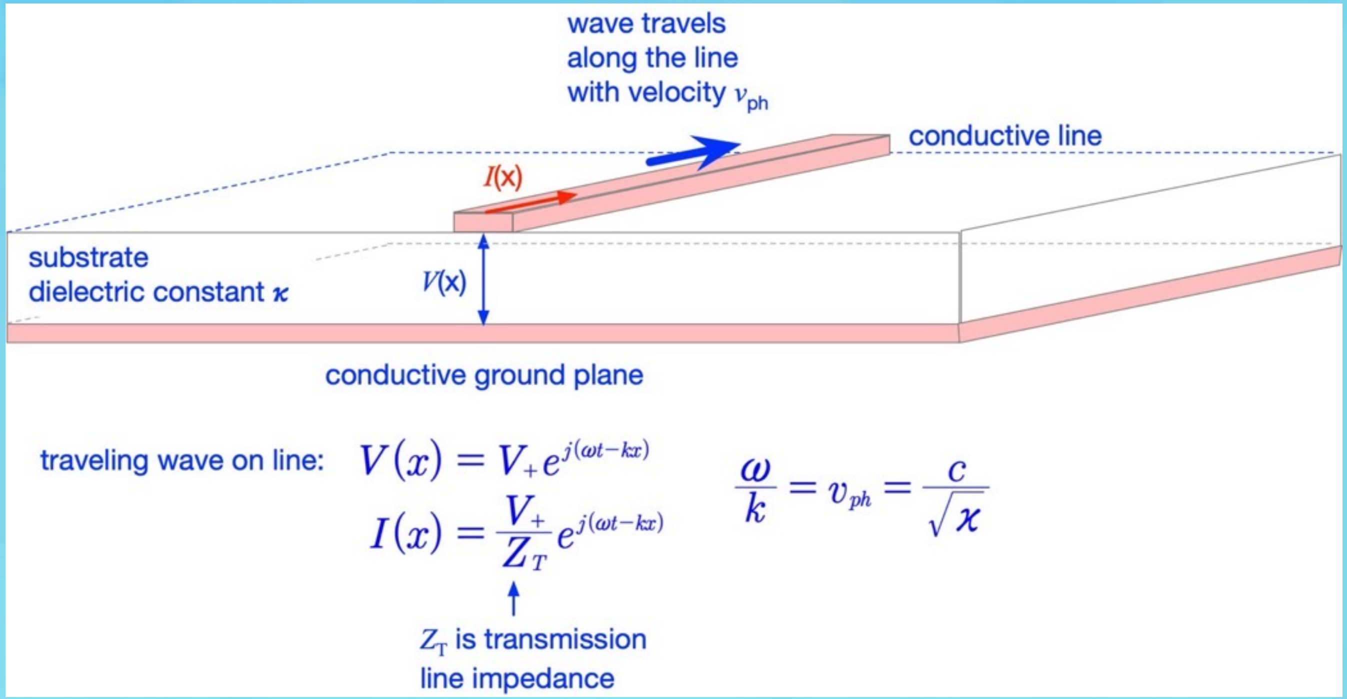
- Data is SENT Least-Significant-Byte (LSB) first (“Little-Endian”), but sometimes written in conventional hexadecimal byte format
  - Example: iBeacon packet MAJOR identifier from previous slide
  - This is the opposite of how we usually write numbers and can be confusing!
- Note manufacturer-specific packet sections may use other conventions, e.g. MSB!
  - Tutorial #4 will provide more details



Transmission Lines

Valid when wavelength >> substrate thickness and line width

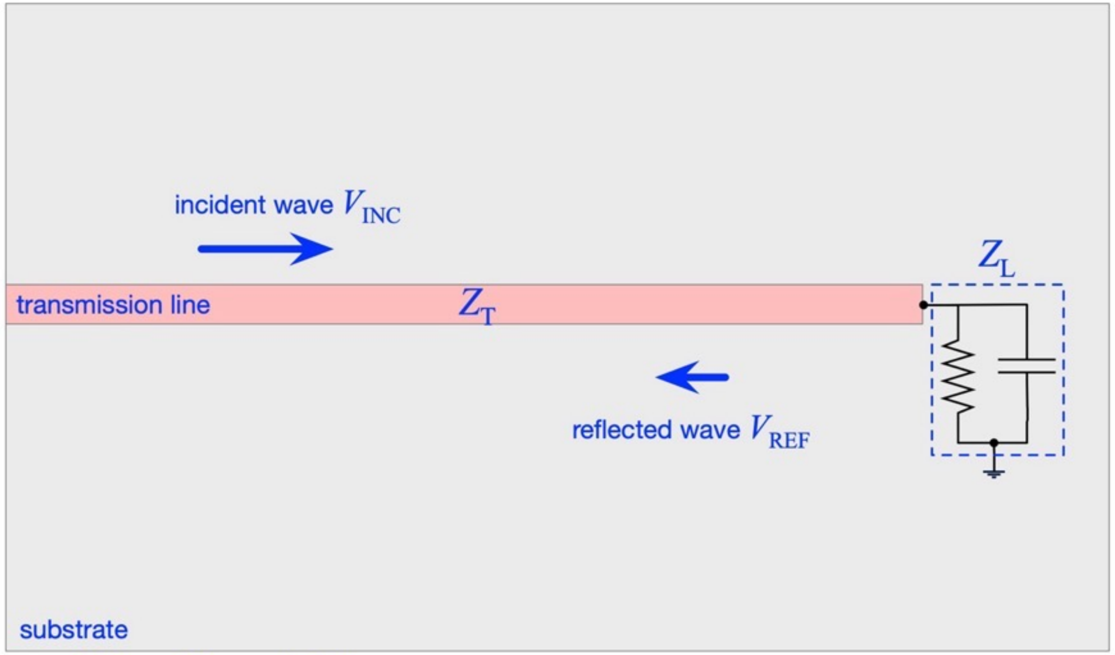
- Radio waves can propagate along appropriate metal structures
  - Most common is a conductive line over a conductive ground plane, but many other waveguide structures possible
- If loss is small, the wave is simply moving along the transmission line
  - Although velocity is less than that of light in vacuum!



Note that this works because the current in the line and the ground plane cancel when viewed from far away: no radiation!

Reflections on Reflection

- To use the signal you connect the transmission line to a load
  - The load has a finite impedance, often frequency-dependent
- If the load impedance is not equal to the transmission line impedance, some of the signal is reflected



$$V = V_{INC} + V_{REF}$$

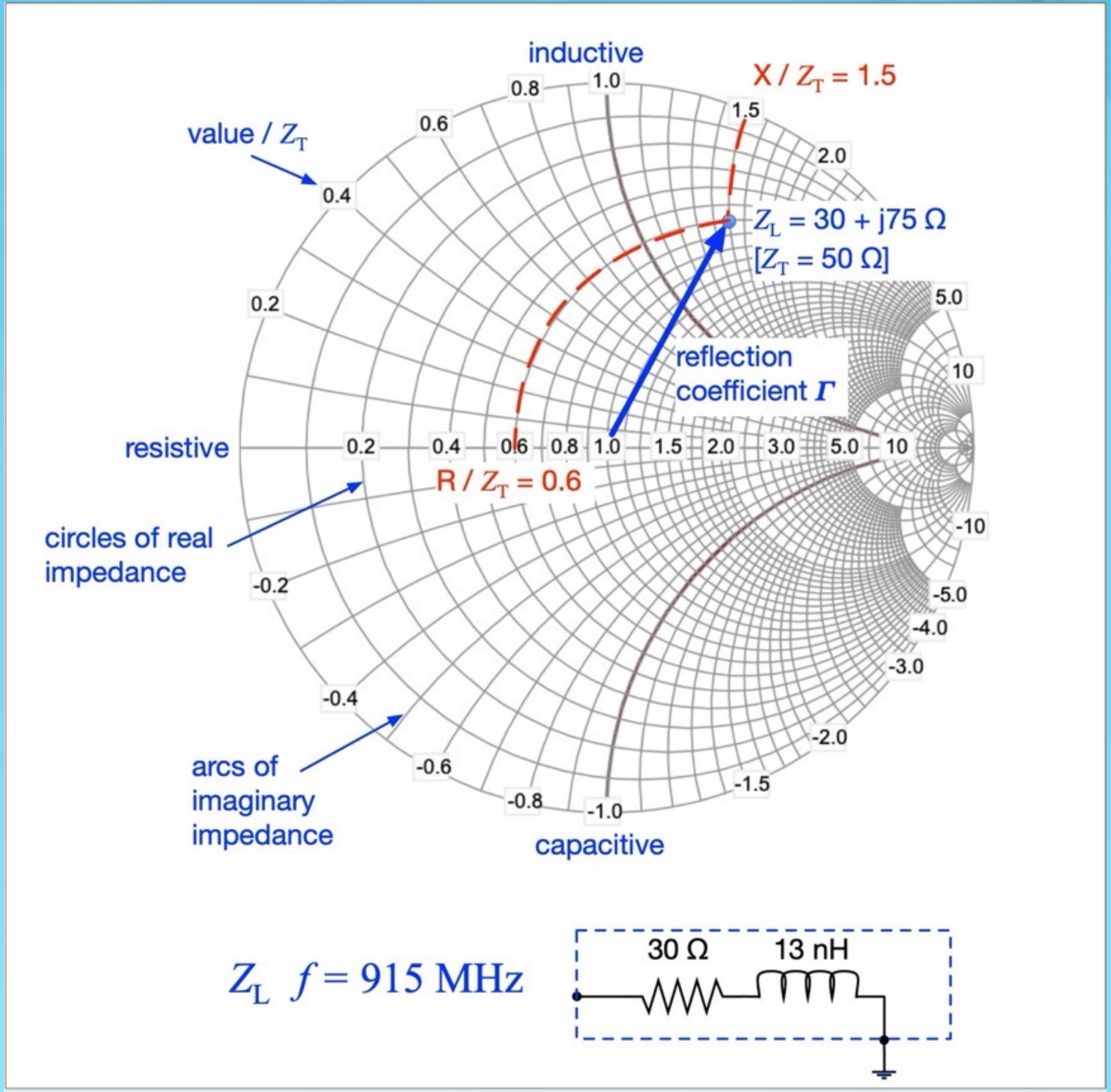
$$I = I_{INC} - I_{REF}$$

$$V_{REF} = \Gamma V_{INC}$$

reflection coefficient $\Gamma = \frac{Z_L - Z_T}{Z_L + Z_T}$

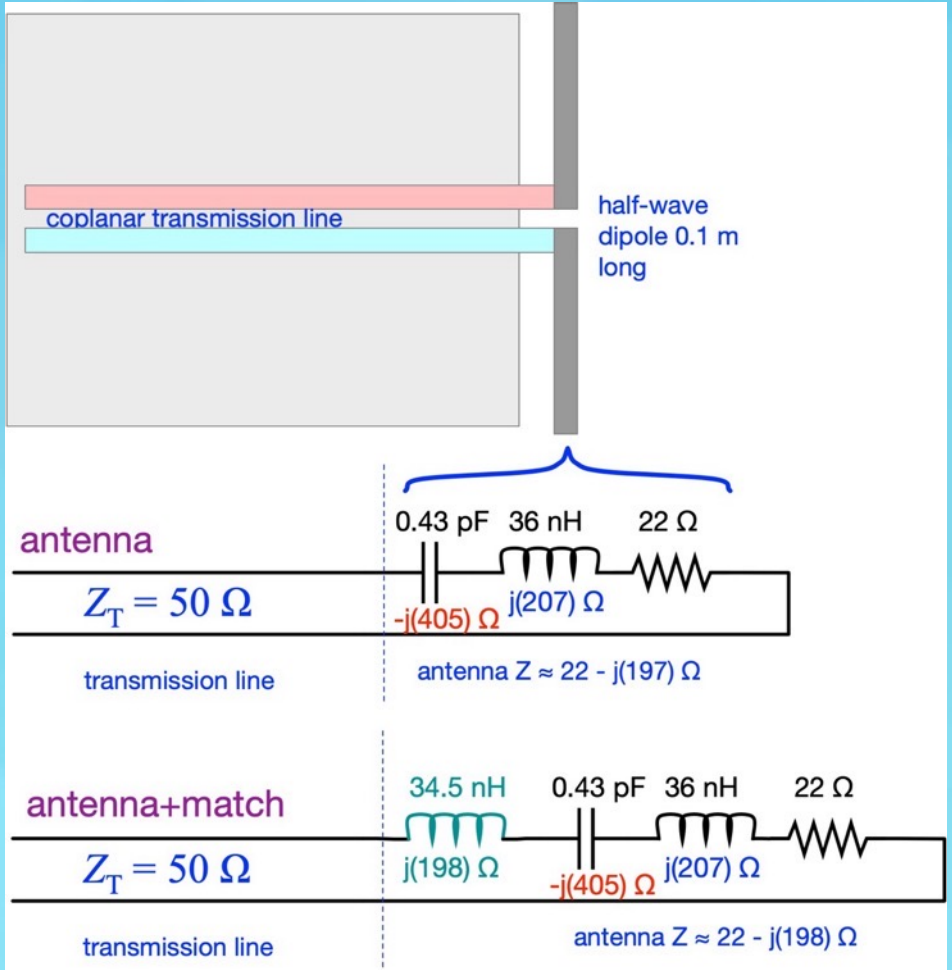
The Smith Chart

- The reflection coefficient is a point in the complex plane
  - Passive elements require $|\Gamma| \leq 1$
- If we overlay the corresponding load impedance for each complex reflection, we get the Smith Chart
  - Translation between complex reflection and impedance



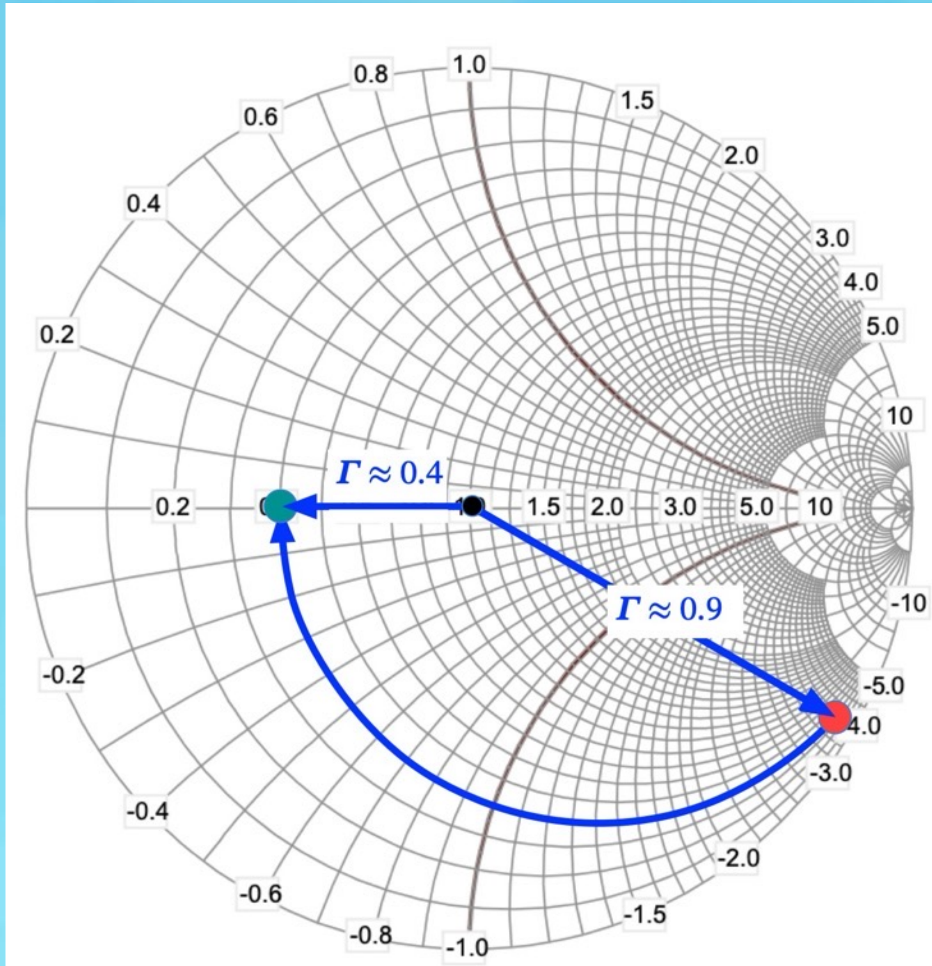
Antenna Matching Example

- Transmission line (Z=50 Ω) connected to dipole antenna
  - Length about λ/3
  - Not matched; part of the signal will be reflected
- Add series inductor to remove reactive component of antenna impedance
- We can do the math, OR we can use the Smith chart to SEE what's happening...



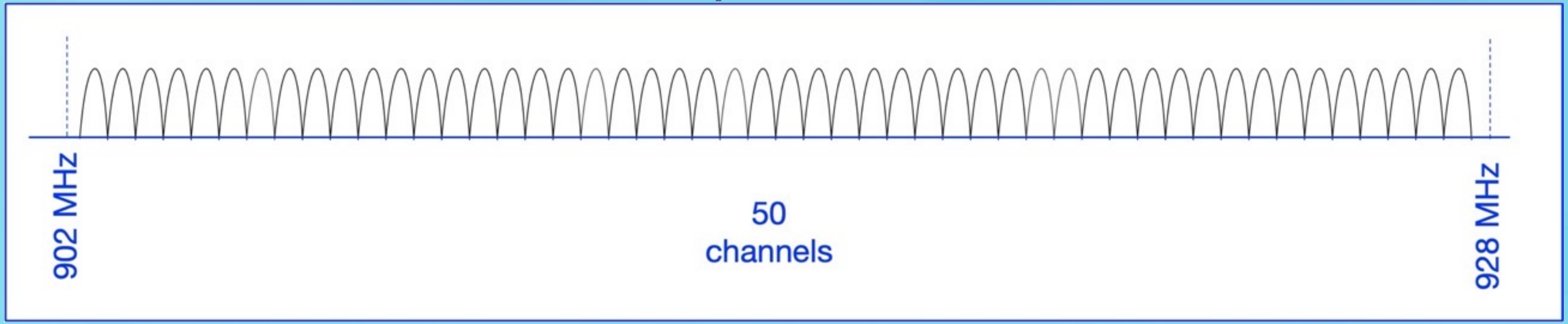
Antenna Matching Example: Smith Chart View

- Antenna has reflection coefficient of about 0.9 (red dot)
  - Very little power will be transmitted by the unmatched antenna
- Series inductor causes us to rotate on a circle of constant real impedance
  - Minimum when we reach real axis (green dot)
- With addition of the matching circuit, reflection coefficient reduced to 0.4
  - Most of the power from the transmission line gets to the antenna
    - We can do better with additional shunt elements (future discussion)

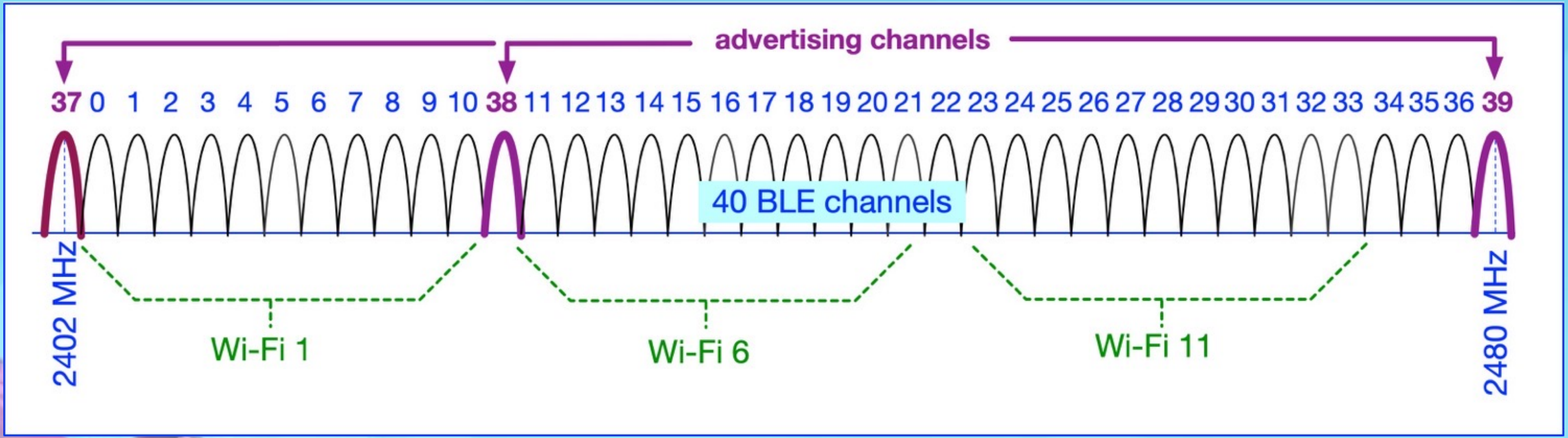


Common RFID Band Channels

- UHF: ISM 902-928 MHz, 500 kHz channels



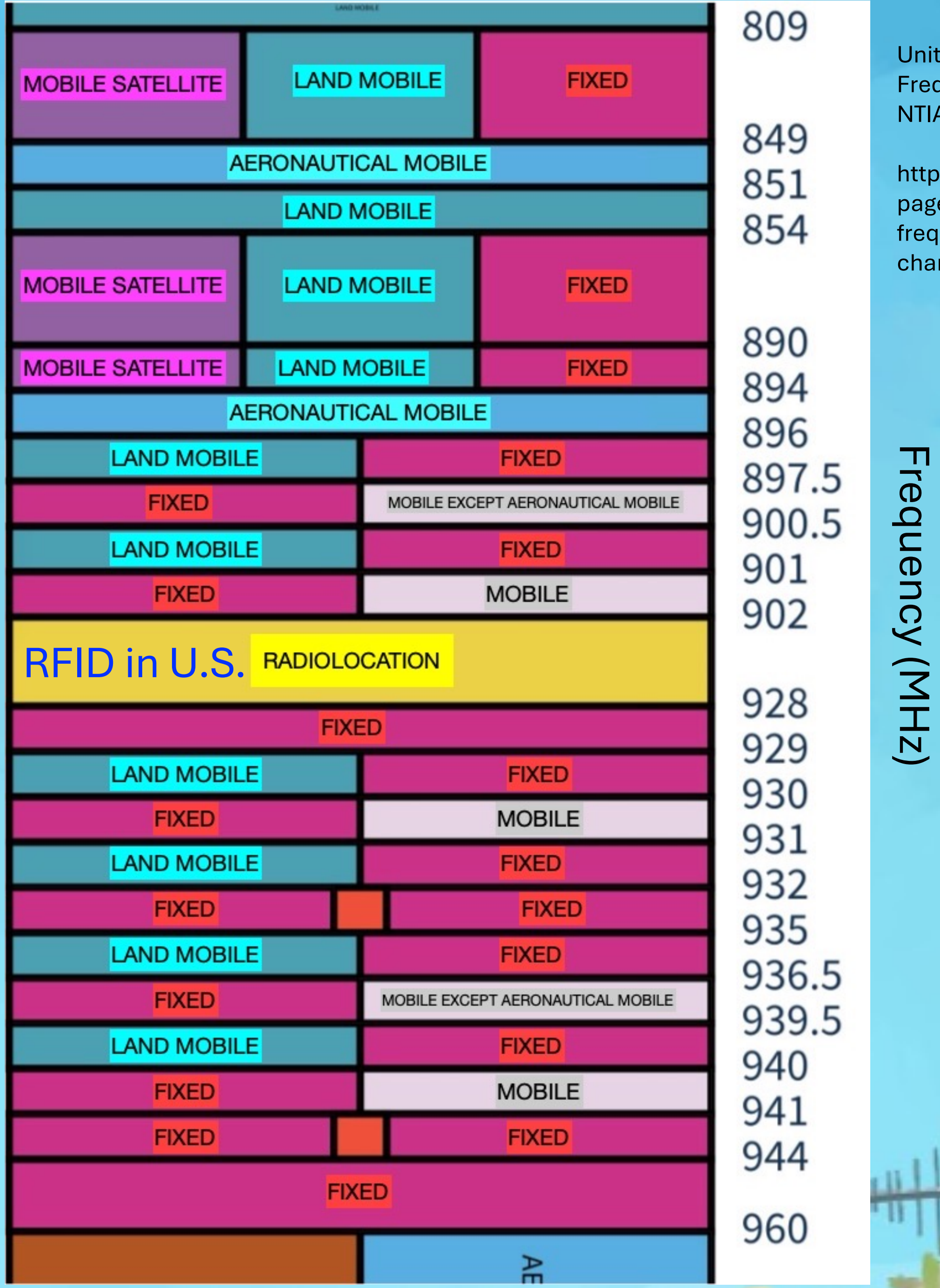
- BLE: ISM 2400-2483 MHz, 2 MHz channels



Regulatory Issues

- Governments have regulated frequency usage and allowed power since early 20th century
  - US FCC, EU, Japan, China, Americas, etc. SIMILAR BUT NOT THE SAME
  - Most RFID applications use specific shared frequency bands :
    - Anyone can use BUT
    - Rules on maximum power, antenna gain, channel size, usage times

For current global RFID information see:
“Overview of UHF frequency allocations for RAIN RFID”
Available from
https://therainalliance.org/radio-regulations-advisory-council/

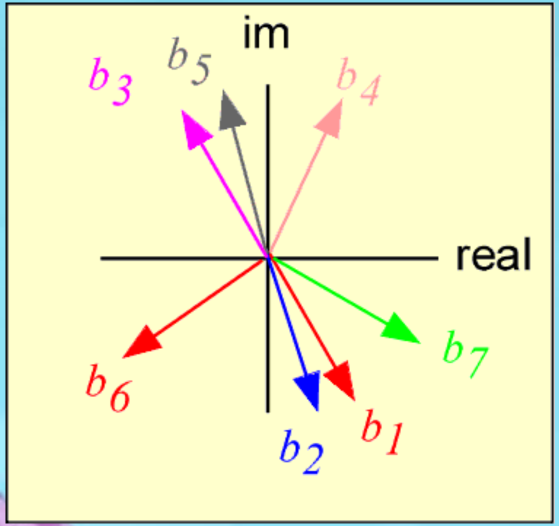


United States Frequency Allocations NTIA September 2025

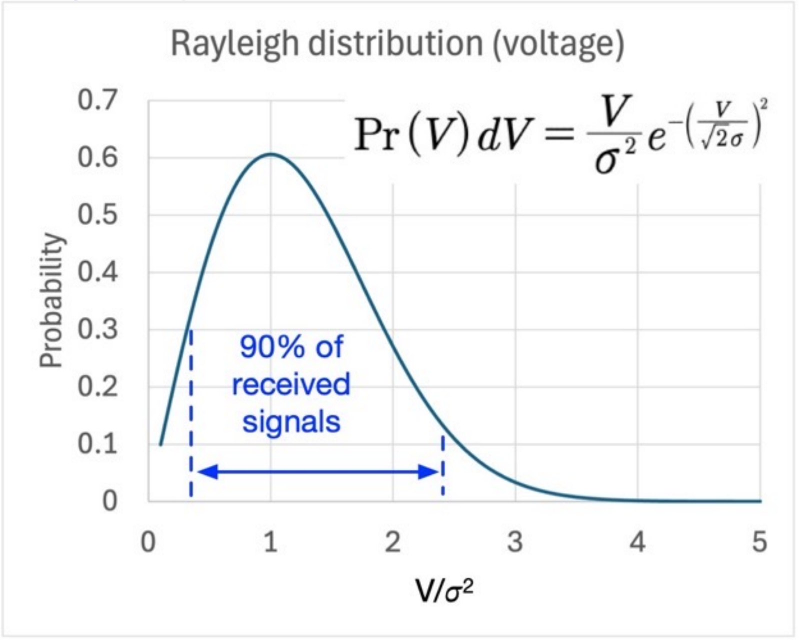
https://www.ntia.gov/page/united-states-frequency-allocation-chart

Statistical Models of Received Power

- How can we model what we will get in a complicated environment?
- Traditional approach: admit ignorance
- Example: assume large number of paths, each provides the same received voltage but at random phase



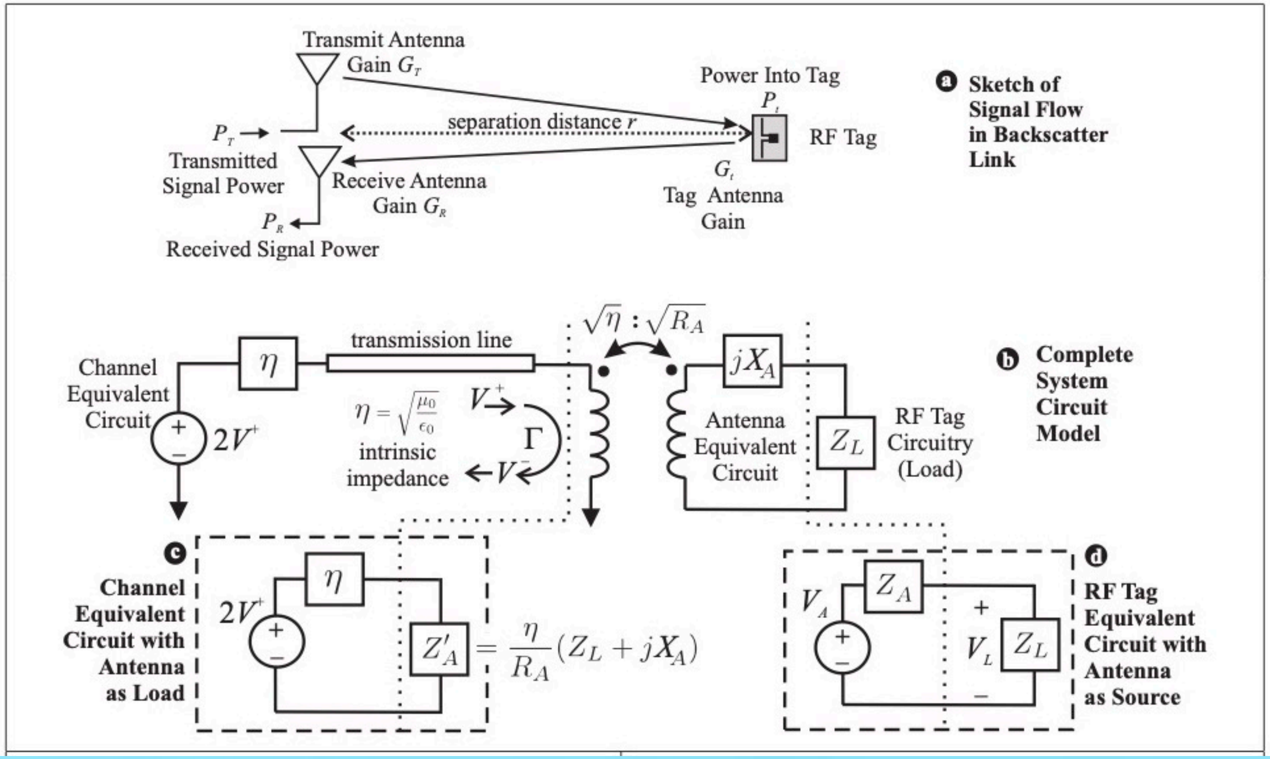
- For more than ≈ 6 beams, the received voltage follows a Rayleigh distribution:



Hard to use raw RSSI for location with 18 dB fading range!

Summary Tables (Greg Durgin)

TABLE I: Equivalent circuit with physical quantities for antennas in forward and backscatter links.



Voltage Formulas

$$V^+ = \frac{\lambda\sqrt{2\eta G_T G_t P_T}}{4\pi r}\exp\left(j\left[\phi^+ - \frac{2\pi r}{\lambda}\right]\right)$$

$$V^- = \Gamma V^+ = \frac{Z'_A - \eta}{Z'_A + \eta}V^+ = \frac{Z_L - R_A + jX_A}{Z_L + Z_A}V^+$$

$$V_A = 2V^+\sqrt{\frac{R_A}{\eta}}$$

$$V_L = \frac{V_A Z_L}{Z_A + Z_L}$$

RF Power Formulas

$$P_t = \frac{P_T G_T G_t \lambda^2}{(4\pi r)^2}(1 - |\Gamma|^2)$$

$$P_R = \frac{G_R G_t \lambda^2 |V^-|^2}{32\eta\pi^2 r^2} = \frac{P_T G_R G_T \lambda^2}{64\pi^3 r^4}\sigma_{\mathrm{RCS}}$$

$$\sigma_{\mathrm{RCS}} = \frac{G_t^2\lambda^2|\Gamma|^2}{4\pi}$$

$$\Delta\sigma_{\mathrm{RCS}} = \frac{G_t^2\lambda^2}{4\pi}\left|\frac{2R_A(Z_{L1} - Z_{L2})}{(Z_{L1} + Z_A)(Z_{L2} + Z_A)}\right|^2$$

$$\Delta\sigma_{\mathrm{sRCS}} = \frac{1}{4}\Delta\sigma_{\mathrm{RCS}}$$

Electromagnetic Field Formulas

$$\vec{E} = \frac{V^+}{\lambda}\sqrt{\frac{4\pi}{G_t}}\hat{e}$$

$$\vec{H} = \frac{V^+}{\lambda\eta}\sqrt{\frac{4\pi}{G_t}}\hat{h}$$

$$\vec{S}_t = \frac{|V^+|^2}{2\eta}\hat{k}$$

$$\vec{S}_R = -\frac{G_t|V^-|^2}{8\eta\pi^2 r^2}\hat{k}$$

Physical Model Inputs

λ	wavelength of radiation (m)
r	transceiver-tag separation distance (m)
η	impedance of free space (377 Ω)
Z_A	port-side complex RF tag antenna impedance (Ω)
Z'_A	channel-side complex RF tag antenna impedance (Ω)
Z_L	complex RF tag load impedance (Ω)

Voltages

V^+	forward-propagating (impinging) wave (V)
V^-	backward-propagating (reflecting) wave (V)
V_A	equivalent RF tag antenna voltage (V)
V_L	tag antenna terminal voltage (V)
Γ	voltage reflection coefficient
ϕ^+	excess phase offset

Powers and Gains

P_T	transmitted power (Watts)
P_t	power absorbed by RF tag (Watts)
P_R	ideal received power (Watts)
G_T	transmit antenna gain
G_t	RF tag antenna gain
G_R	receive antenna gain
σ_{RCS}	RF tag antenna mode radar cross section (m²)
$\Delta\sigma_{\mathrm{RCS}}$	RF tag differential RCS, classical (m²)
$\Delta\sigma_{\mathrm{sRCS}}$	signal power RF tag differential RCS (m²)

Electromagnetic Fields

$\vec{E}$	incident electric field (V/m)
$\vec{H}$	incident magnetic field (A/m)
$\vec{S}_t$	tag-incident average Poynting vector (Watts/m²)
$\vec{S}_R$	RX-incident average Poynting vector (Watts/m²)
$\hat{e}$	electric field polarization
$\hat{h}$	magnetic field polarization
$\hat{k}$	direction of propagation ($\hat{e} \times \hat{h}^* = \hat{k}$)

Bandwidth and Ultrawideband

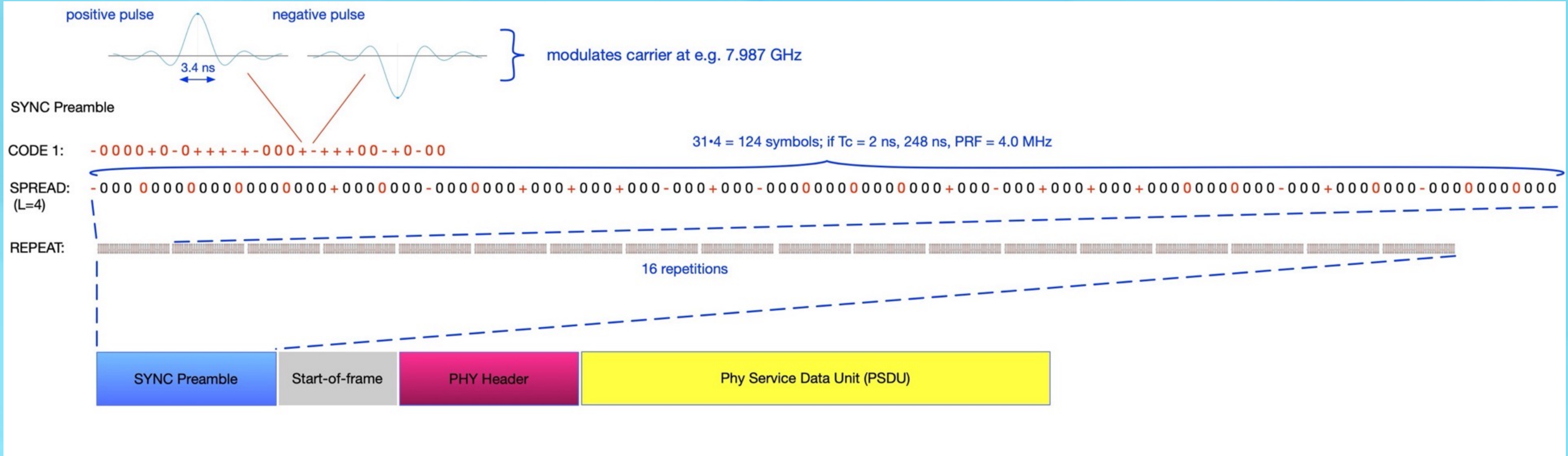
- Bandwidth of typical unregulated signals (e.g. ISM, UNII) are ≈ 1 MHz ⇒ timing accuracy ≈ ±1 μs ≈ ±300 meters
  - Ok for ships on the open sea, not helpful in a room
- For accurate timing: ultrawideband (UWB)!
  - Up to >1 GHz bandwidth = 1 ns = 30 cm
    - cm accuracy achievable in some cases
  - BUT low power required to avoid interference with other users: limited to –42 dBm/MHz
    - That's -15 dBm (30 microW) in 500 MHz
  - So complex coding is used to provide coding gain and recover the wanted signal in the presence of wideband and narrowband interference

802.15.4: Everything for Everybody…

- Physical layer supports:
  - Direct-sequence spread spectrum (DSSS), two varieties
  - Simultaneous binary shift/ASK => simultaneous DSSS
  - Ultrawideband (UWB), Chirped Spread Spectrum (CSS)
  - 780/950 MHz with other keyed modulations
  - Channel hopping
  - Packet extensions for location
- MAC:
  - Frames up to 127 bytes
  - Ethernet support through fragmentation
- Used by various upper layers:
  - Zigbee, WirelessHART, MiWi, 6LoWPAN, Thread, SNAP…

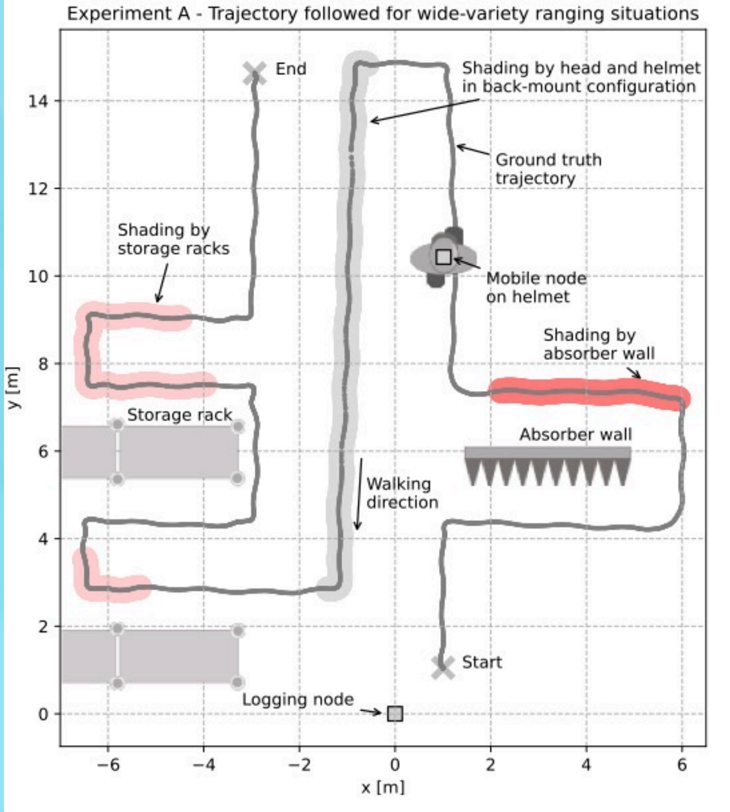
Example: 802.15.4z Coding (partial)

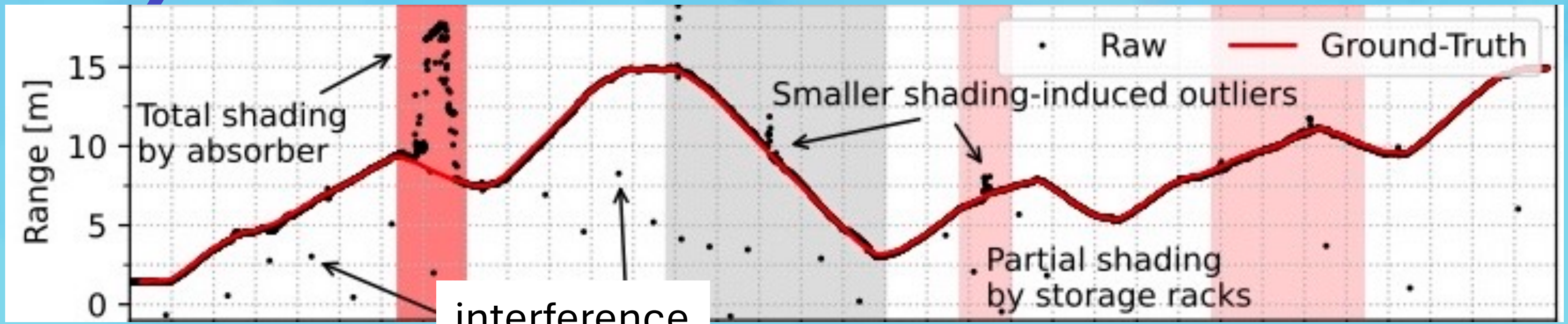
- SYNC Preamble using nsec-scale pulses...

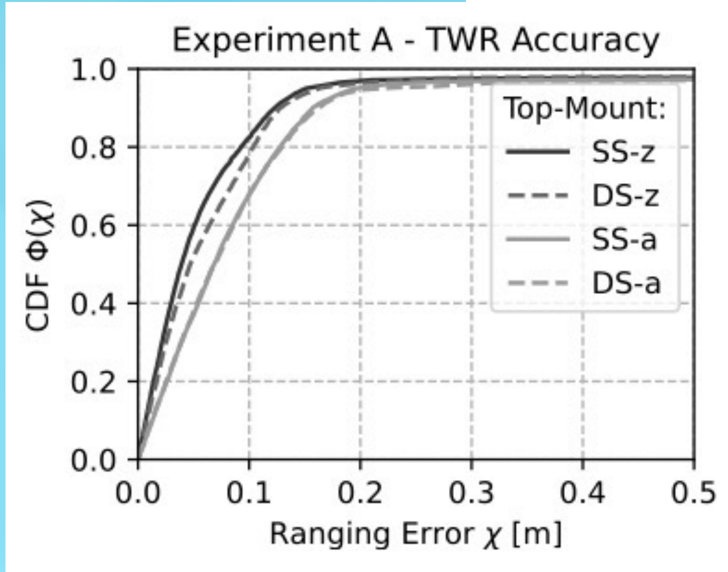


Rohde and Schwarz White Paper: High rat epulse ultrawideband physical layer testing and certification captured December 2025

802.15.4z Location Performance (Tiemann et. al. 2022)





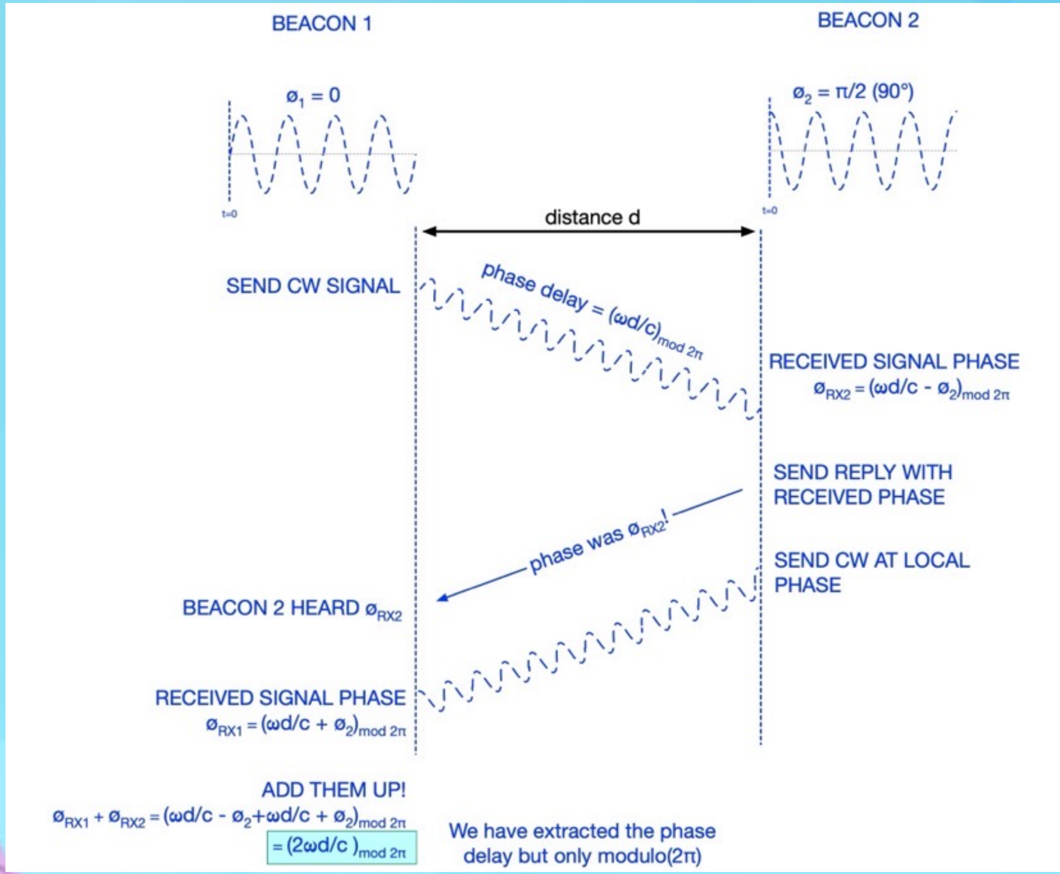


- With minimum interference, unoccluded results often accurate to 10-20 cm
- BUT occlusion or interference can give rise to multi-meter error!

- Experimental Evaluation of IEEE 802.15.4z UWB Ranging Performance under Interference, J. Tiemann, J. Friedrich and C. Wietfield, Sensors v 22 p. 1643 (2022)

Phase-Based Ranging: Details

- Step 1: determine phase delay at a single frequency



- Step 2: Repeat the process to obtain the dependence of phase on frequency

$$\phi(f_1) = \left(\frac{2\omega_1 d}{c}\right)_{\mathrm{mod}\,2\pi} \quad \phi(f_1+\delta f) = \left(\frac{2[\omega_1+\delta\omega]d}{c}\right)_{\mathrm{mod}\,2\pi}$$

$$\phi(f_1+\delta f) - \phi(f_1) = \left(\frac{2(\delta\omega)d}{c}\right)_{\mathrm{mod}\,2\pi} \rightarrow d = \frac{c(\delta\phi)_{\mathrm{mod}\,2\pi}}{4\pi(\delta f)}$$

- Channel spacing 2 MHz for BLE:

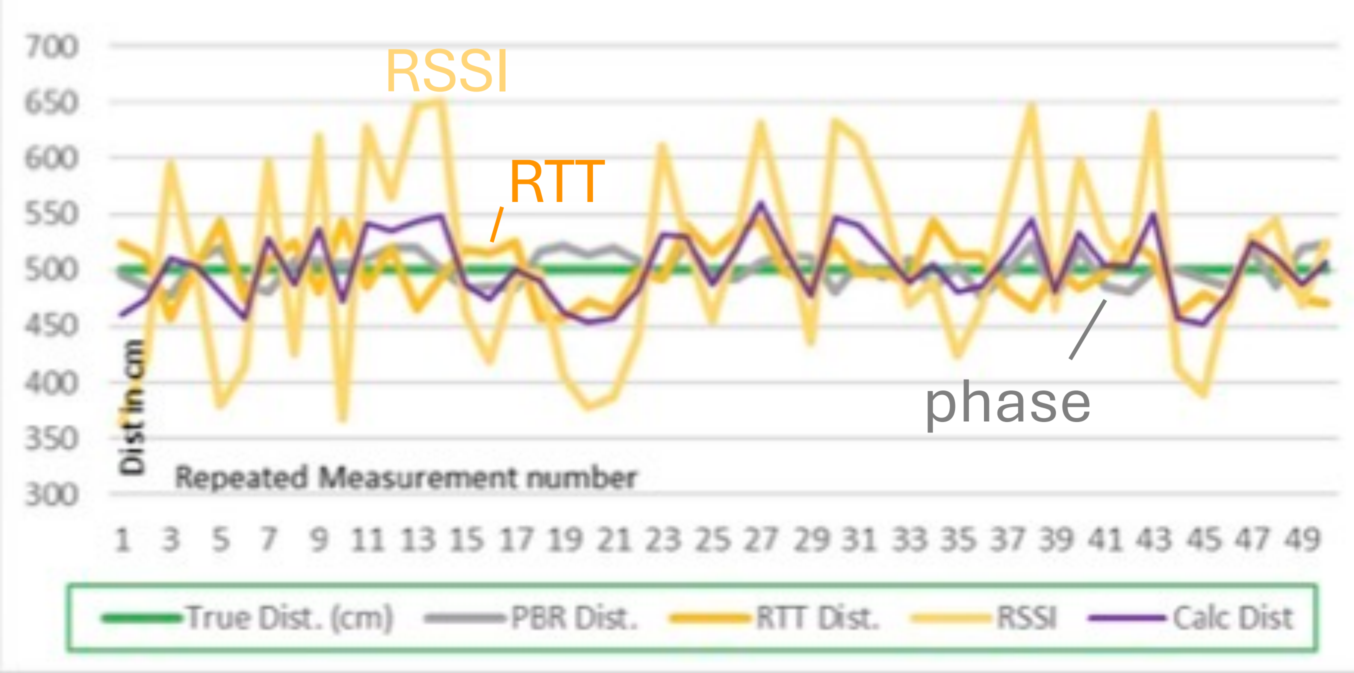
$$\frac{2\pi c}{4\pi(\delta f)} = \frac{c}{2(\delta f)} = \frac{3\times 10^8}{4\times 10^6} = 75 \text{ meters}$$

- Multichannel phase-based ranging ambiguity size >> single channel
  - 75 meters ≈ 250 ns; actual distance easily classified by delay-based ranging
  - BLE supports multiple frequencies, corrections for frequency drift between beacons

BLE 6.0 Location Performance: Conventional

- Best results obtained by COMBINING methods:
  - RSSI, phase-based ranging, two-way time-of-flight, 5 meter outdoor distance
    - RSSI max error 31%
    - Round-trim-time error 10%
    - Phase-based ranging error 7%
  - Measurements combined with encryption provisions to detect "man-in-middle" attacks

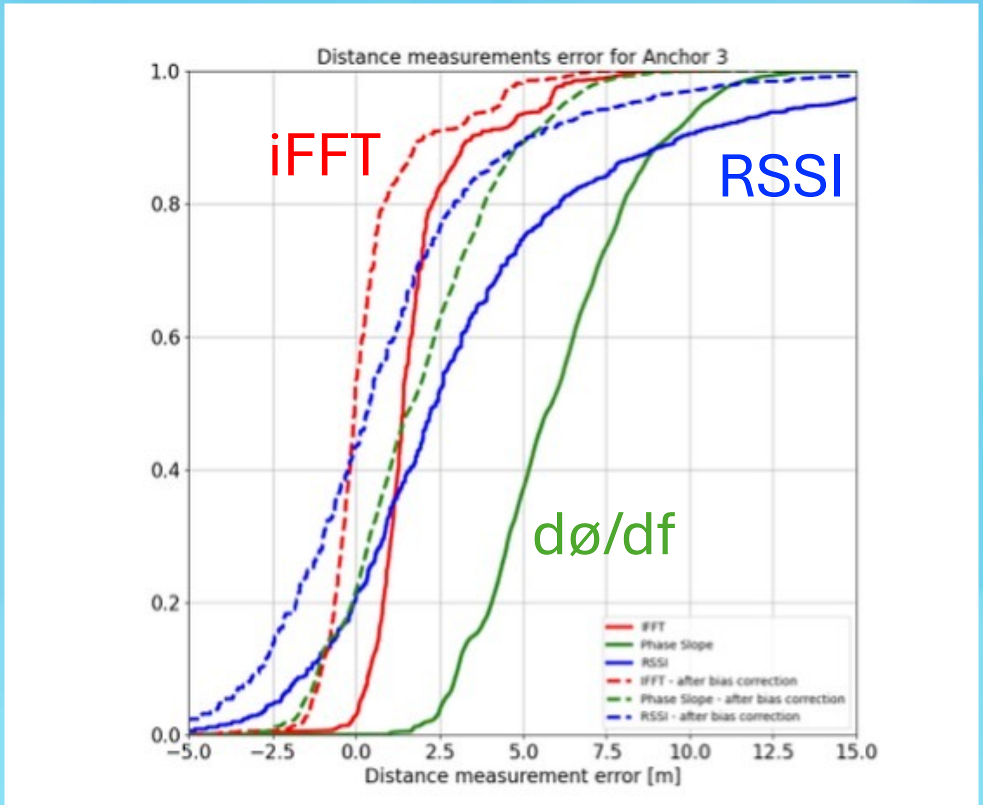
Actual line-of-sight distance 5 m = 500 cm



"BLE Channel Sounding: Novel Method for Enhanced Ranging Accuracy in Vehicle Access", Suresh D., P. Joshi, P. Parandkar, A. Gambhir and K. Sudharshan, IEEE Access v 13 p. 67531 (2025)

BLE 6.0 Location Performance: Algorithmic Approach

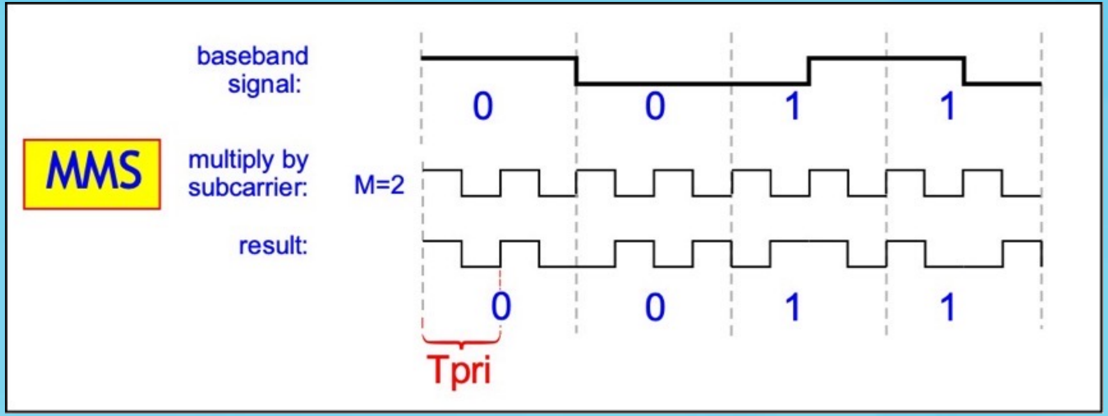
- Over distances to 15 meters in fairly complex indoor environment, inverse Fourier Transform gives most consistent results
  - You’re extracting the equivalent time-of-flight paths, can remove all but the shortest one



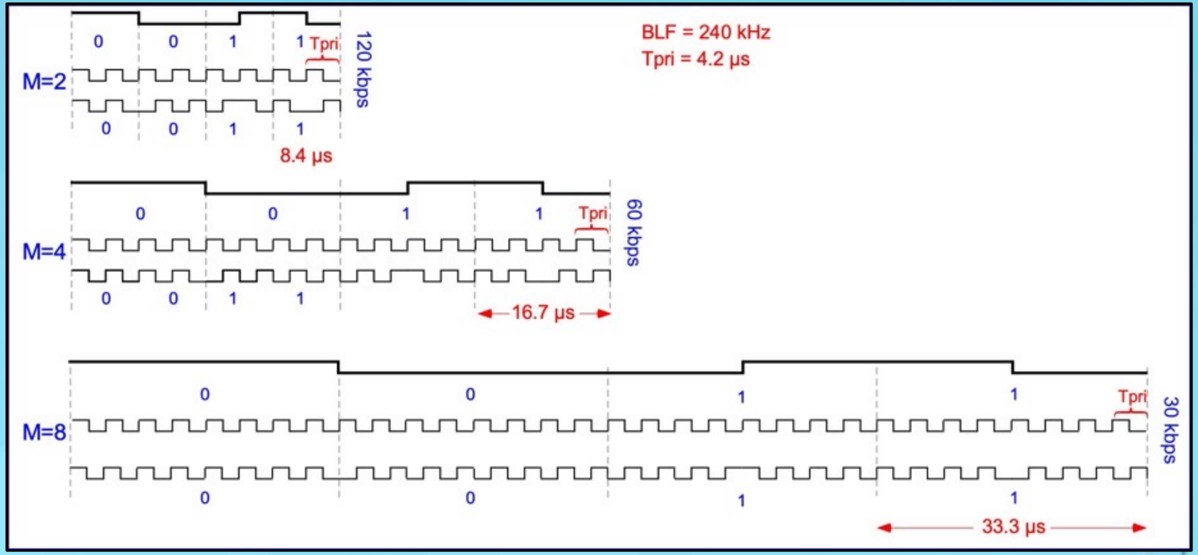
“Experimental Evaluation of Multicarrier Phase Difference Localization in Bluetooth Low Energy”, M. Nikodem, G. Trajnowicz, G. de Blasio and F. Quesada-Arencibia, IEEE Sensors Journal v 25 p. 1548 (2025)

Tag Modulation: MMS

- More tag transitions per symbol provides better signal:noise: MMS

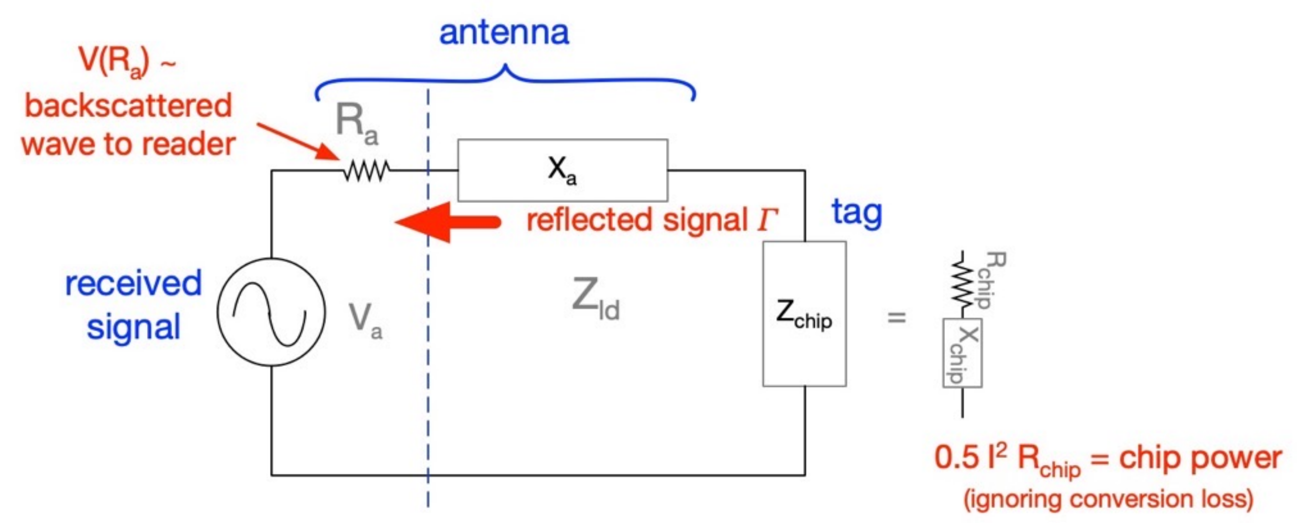


- Increase M to get better noise performance, BUT tradeoff: slower data transmission

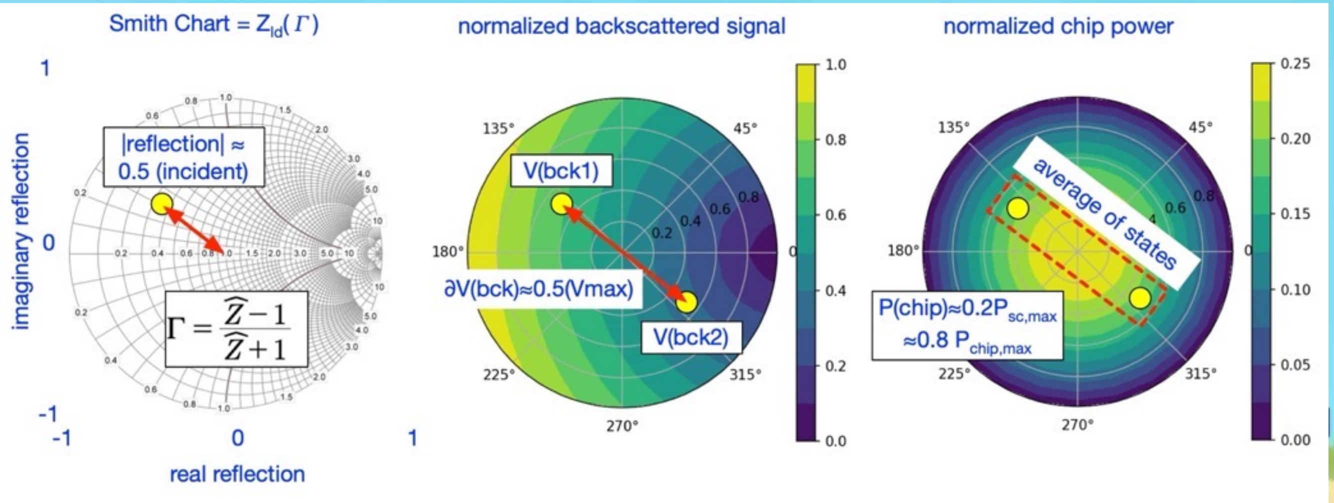


Tag Modulation: Change Antenna Load

- To modulate backscattered signal we change the load presented to the tag antenna
  - BUT: this also changes the received power that runs the tag IC!



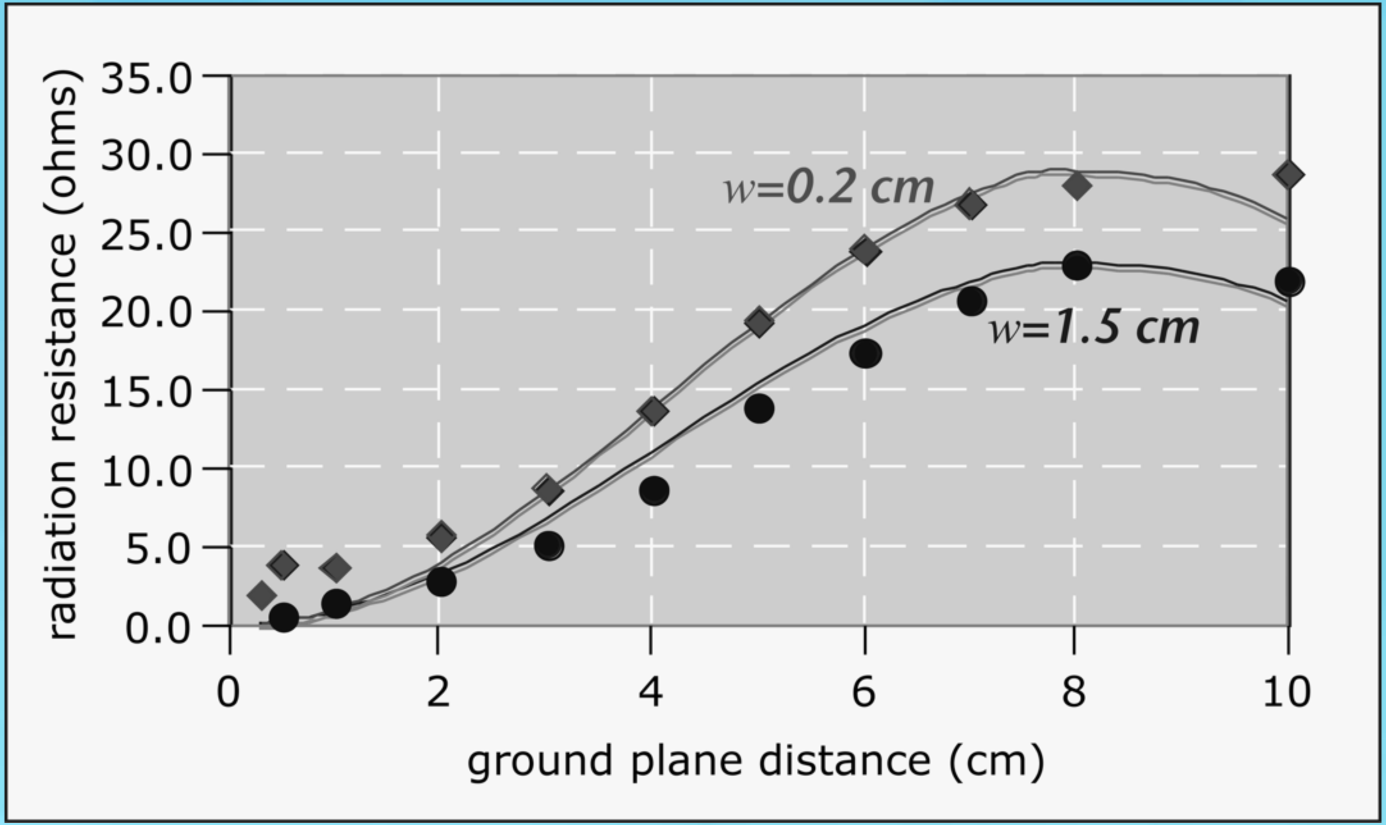
- Need to balance modulation depth and received power



tag-backscatter-illustrations.graffle: Smith-chart-as-RXandTX

Tag Environment: Near Metal Surface

- Tag impedance changes dramatically as a tag nears a metal surface (ground plane here)
- Result is shorter read range if the tag is designed for operation in open air
- Similar results near water, less dramatic effects from other dielectrics

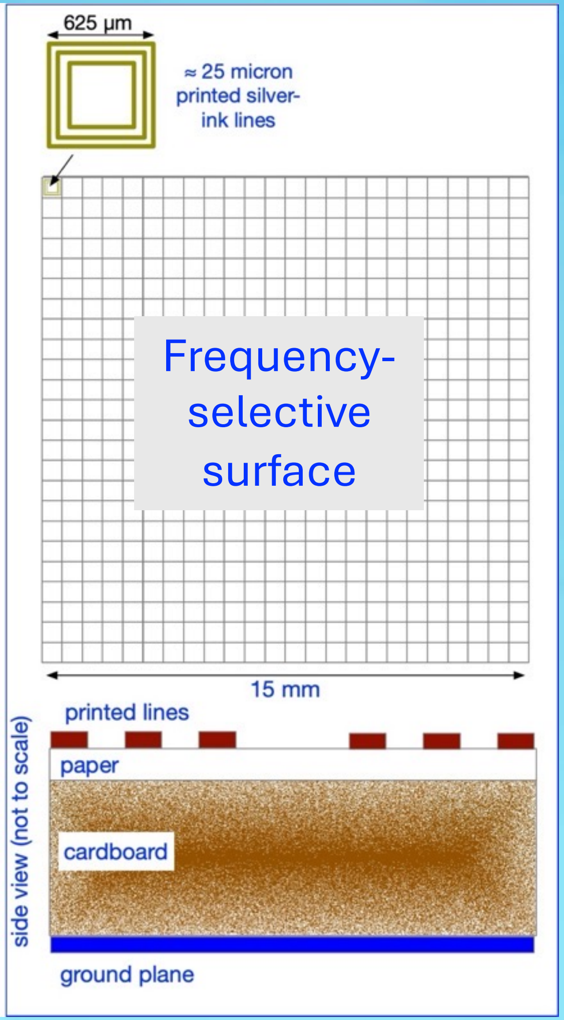


Just Don't Be Insensitive

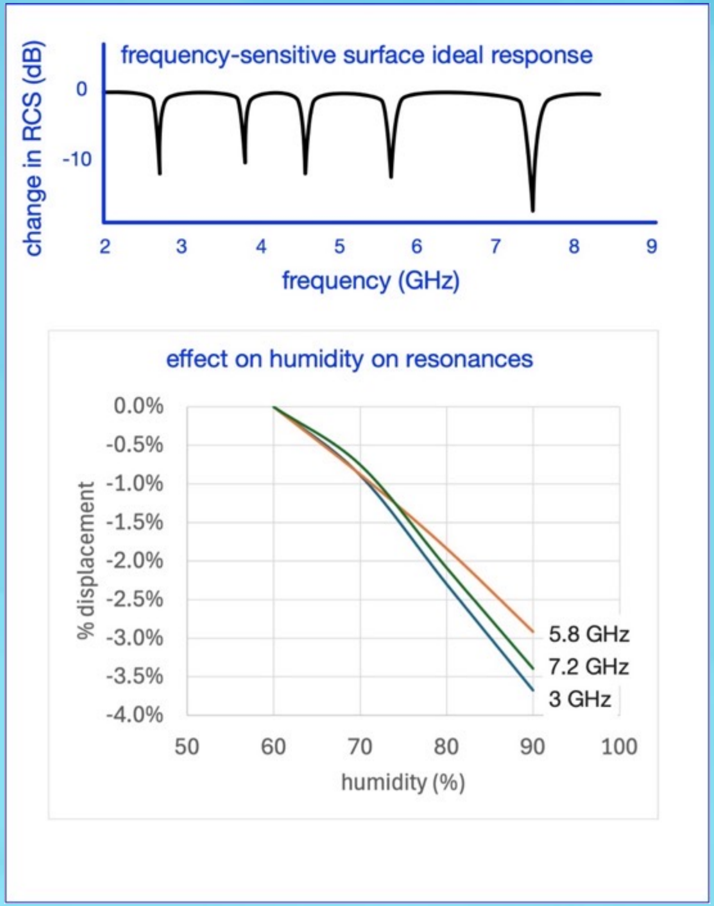
- Once you identify the object, why not identify the world the object is in?
  - Temperature: a hot topic
  - Humidity: all wet
  - Atmospheric pressure: a pressing concern
  - Spoilage: stinky
- Once you sense you need to send
  - Data must be included in transmissions from sensor/tag/beacon

Chipless Sensing Example: Humidity

- Low-cost humidity sense using silver nanoparticle ink on paper, overlay on cardboard+ground plane: “frequency selective surface”
  - After Borgese et. al. IEEE Sensors 2017



- Resulting resonances sensitive to ambient moisture
  - But RCS measured from 25 cm away!
  - And humidity response time ≈ 10 minutes



Example IC-based Sensors

- Commercial products
  - HF, UHF, BLE communications
  - Passive, BAP, active
  - Temperature, humidity, strain, light
  - BUT NOT $0.05/tag!

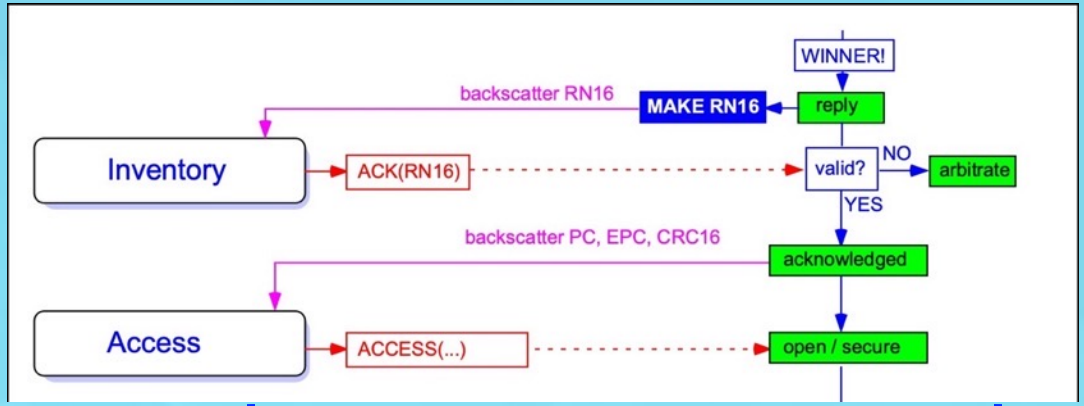
Vendor	Tag	Description	Sense Range
ASYGN	AS3213.T	Sensor chip, temperature	-40 to 120°C
	AS3213.S	Strain	3.5 ppm
	AS3213.RH	Relative humidity	0-100%
	AS3213.L	Illumination*	200-12000 Lux
Axzon	AZN5200	Temperature, BAP/P UHF RFID	-30 to 65°C
CSL	CS8300	Temperature, BAP UHF RFID	-24 to 64°C
EM Micro	EM4325	Temperature, BAP/P UHF RFID	-40 to 60°C
GAO RFID	127003	Active TX, 2.45 GHz	-20 to 60°C
	127044	Active TX, BLE	10 to 25°C*
	115400	Temperature/moisture, BAP/P	-40 to 86°C+moisture
Osrfid	FM13DT160	BAP/P, UHF/HF	-30 to 50°C
RFID Inc.	2509-TMP	Ceramic, on-metal, passive UHF	-40 to 85°C
	7334-TMP	Ceramic, on-metal, passive UHF	-40 to 85°C
	9824-TMP	Adhesive, passive UHF	-40 to 85°C
RFMicron	Magnus S3	Temperature + RSSI/match	-40 to 85°C
Smartrac	Dogbone	Passive UHF adhesive tag	“dry” and “wet”

* Not the animation studio!

Temperature Chip Example

- NMV2D, Wernher von Braun Research Center
  - Standard EPC G2V2 chip +
  - Temperature sense: read values from user memory using EPC G2 commands
    - Zero values to get memory read rolling
    - Calibration parameters for quadratic T-vs-V fit
    - Temperature parameter
  - Chip must remain continuously powered for all this!

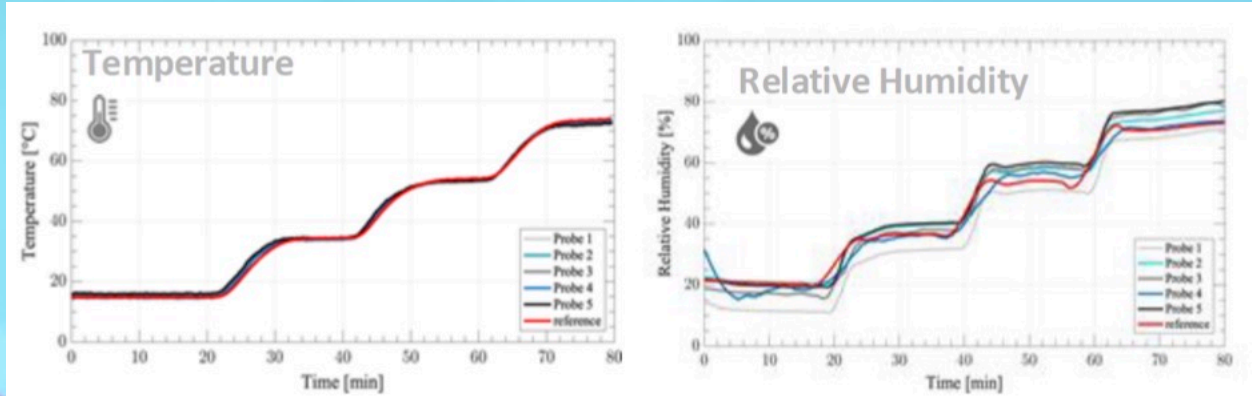
- Inventory + reply + 8*(write 0) + 3*(read fit parameters) + 10* (read temperature parameter value)

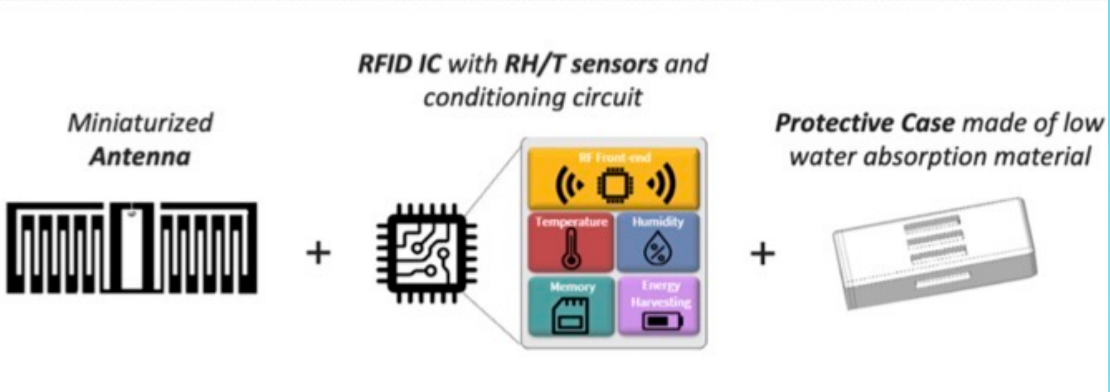


21 extra commands!

Temperature/Humidity Example

- ASYGN AS3213RH, RADIO6ENSE tag
- In-container monitoring for T and RH
  - Data from AIM Case Study “Smart Pharmaceutical Packaging: A Passive Temperature and Humidity Sensing Solution”
    - Read range NOT given, probably short





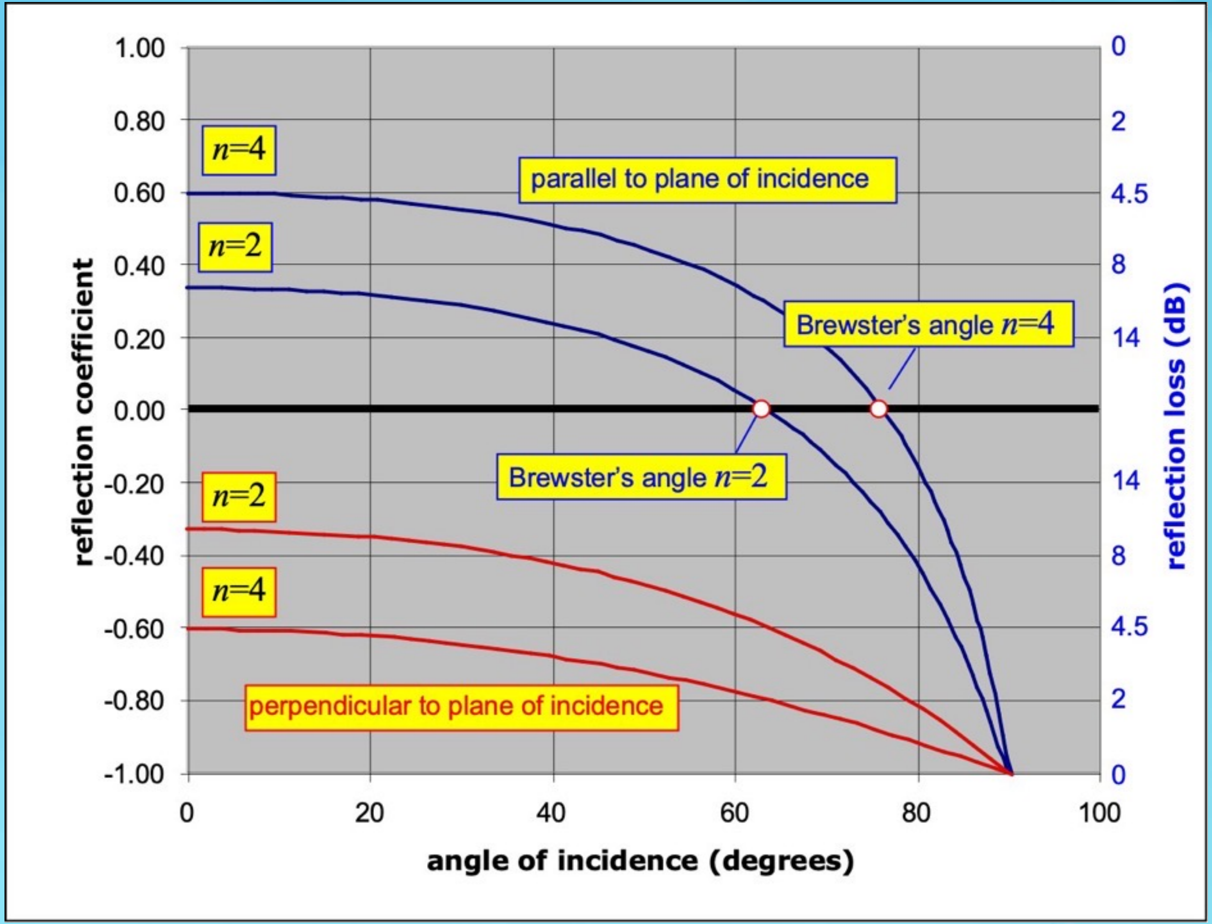
Courtesy of: Sofia Benouakta

Companies in the sensor space

- From https://www.cognitivemarketresearch.com/battery-free-rfid-sensor-market-report captured 11/25/25:
  - Alien Technology LL, CRF MicronInc., IdentivInc., Axzon Inc., Avery Dennison Corporation, Smartrac Technology GmbH, Zebra Technologies Corporation, Checkpoint Systems Inc., Thin Film Electronics ASA, Vishay Intertechnology Inc.
  - Claims >$500M global, about $120M US market for sensors… ?? Others report drastically different numbers, but of course part of that is the definition of the market…

Reflection from Dielectric (cont.)

- Magnitude of reflection is VERY dependent on polarization
  - **A** parallel to plane of incidence: zero reflection at *Brewster's angle*
  - **A** perpendicular to plane of incidence: reflection magnitude increases monotonically with angle
- Refractive index 2-3 for typical building materials
  - Absorption of concrete can be very dependent on water content and age of structure



Notation

- Complex exponentials:

$$e^{ix} = \cos(x) + i \cdot \sin(x)$$

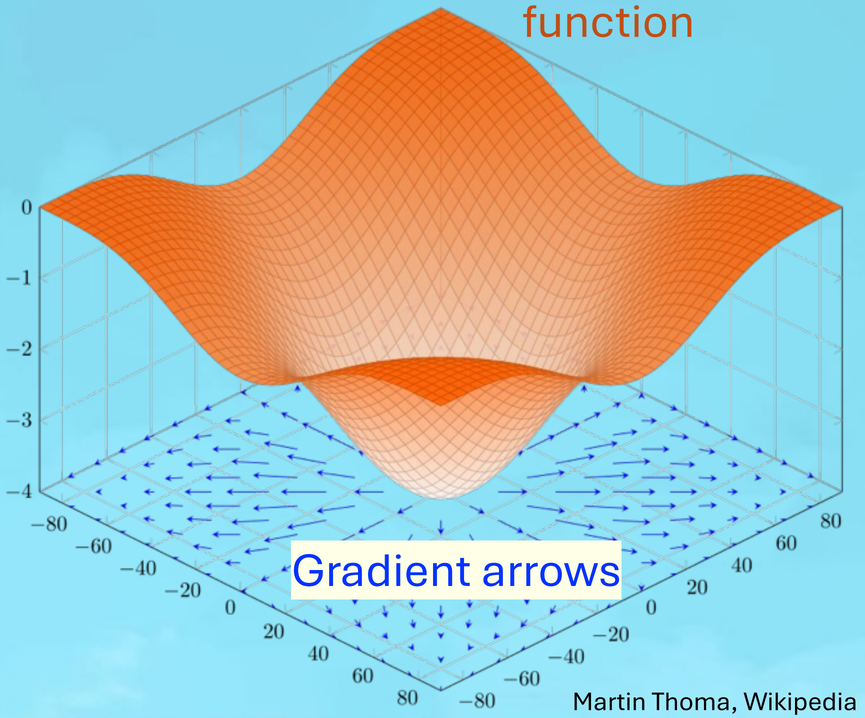
$$e^{i\omega t - ikx} = e^{i\omega t} e^{-ikx} = \text{traveling wave moving to right @ } \Delta kx = \Delta wt \rightarrow \frac{x}{t} = v = \frac{\omega}{k}$$

$$\text{in vacuum: } \omega = ck \rightarrow v = c \text{ (velocity of light)}$$

- Gradients, 3D:

$$\phi = f(x,y,z) \quad (scalar)$$

$$\nabla \phi = \left[\frac{df}{dx}, \frac{df}{dy}, \frac{df}{dz} \right] (vector)$$



Martin Thoma, Wikipedia