WiFi localization

Milan Pandurov

Outline

- Indoor localization
- WiFi localization
- WiFi basics
- Localization approaches
- Prevention of localization

Indoor positioning systems (IPS)

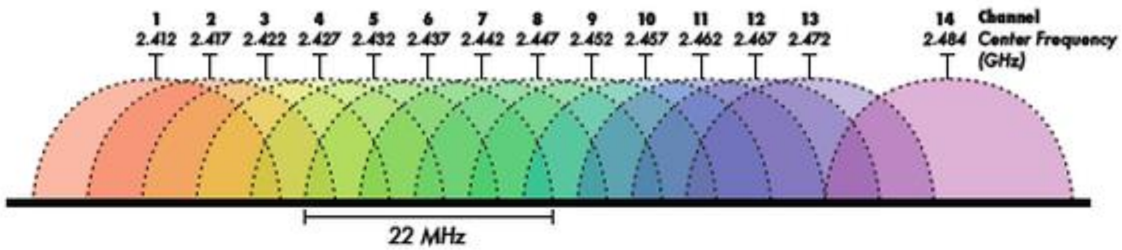
- Non radio technologies
  - Magnetic
  - Dead reckoning
  - Known visual features (markers)
- Radio technologies
  - Bluetooth
  - **Wi-Fi based positioning**

WiFi localization

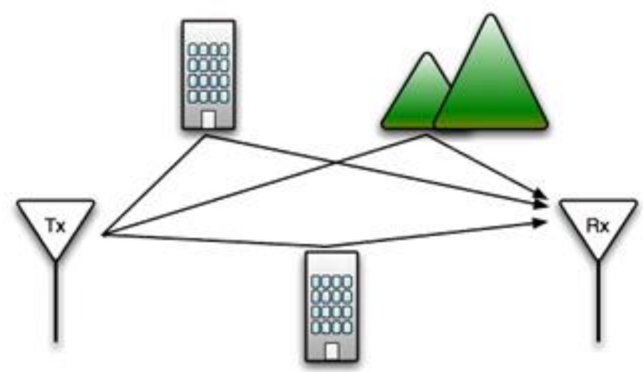
- Different techniques
  - RSSI based
  - Fingerprinting based
  - **Angle of arrival based**
  - **Time of flight based**

Basic Wi-Fi concepts

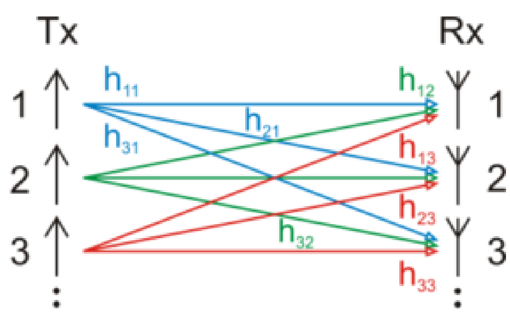
- WiFi channels



- MAC
- Channel estimation
- Multipath propagation



- MIMO



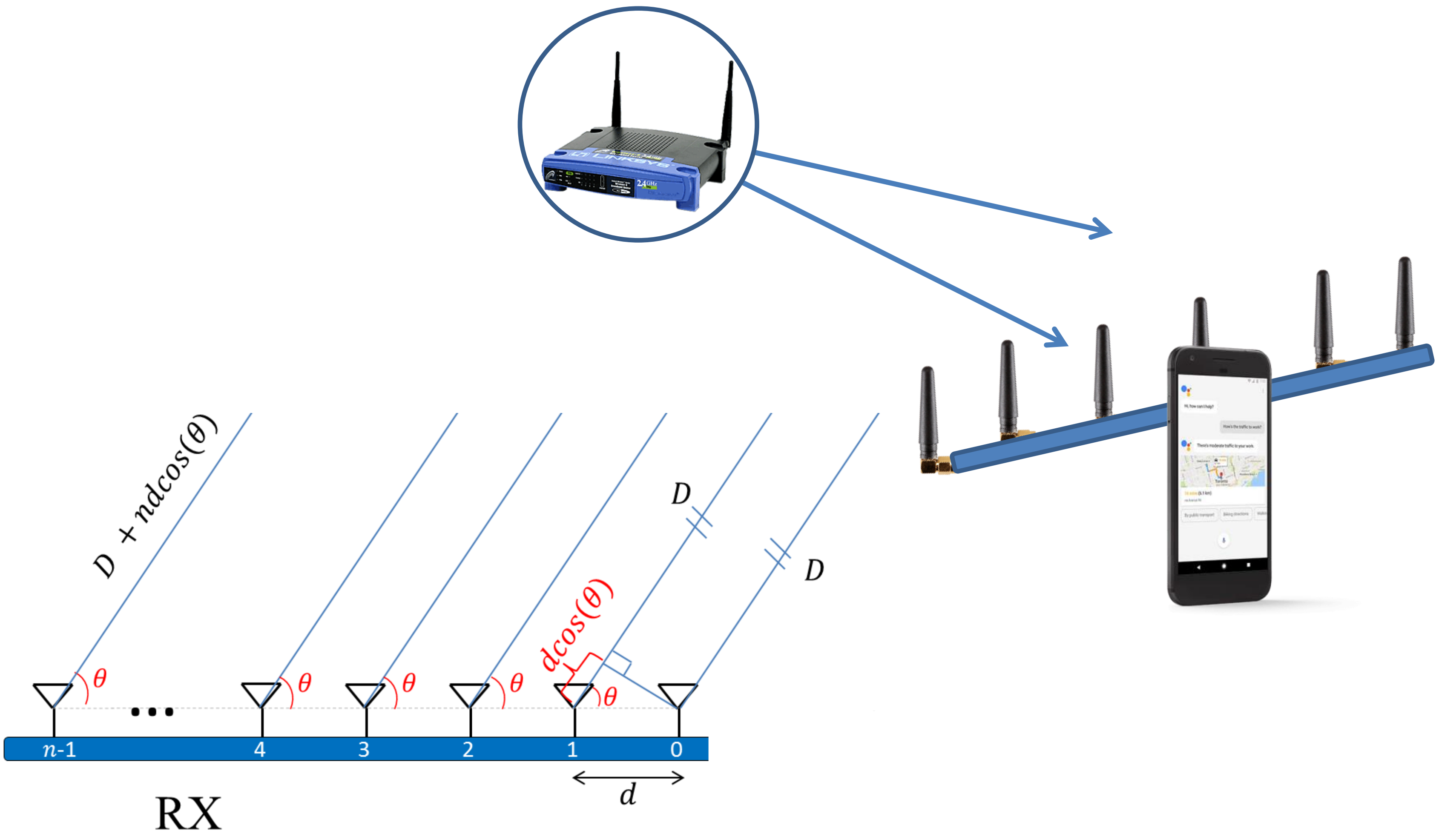
Angle of arrival based localization (*AoA*)

- One approach to localize users

"Accurate Indoor Localization With Zero Start-up Cost"
Swarun Kumar, Stephanie Gil, Dina Katabi, Daniela Rus

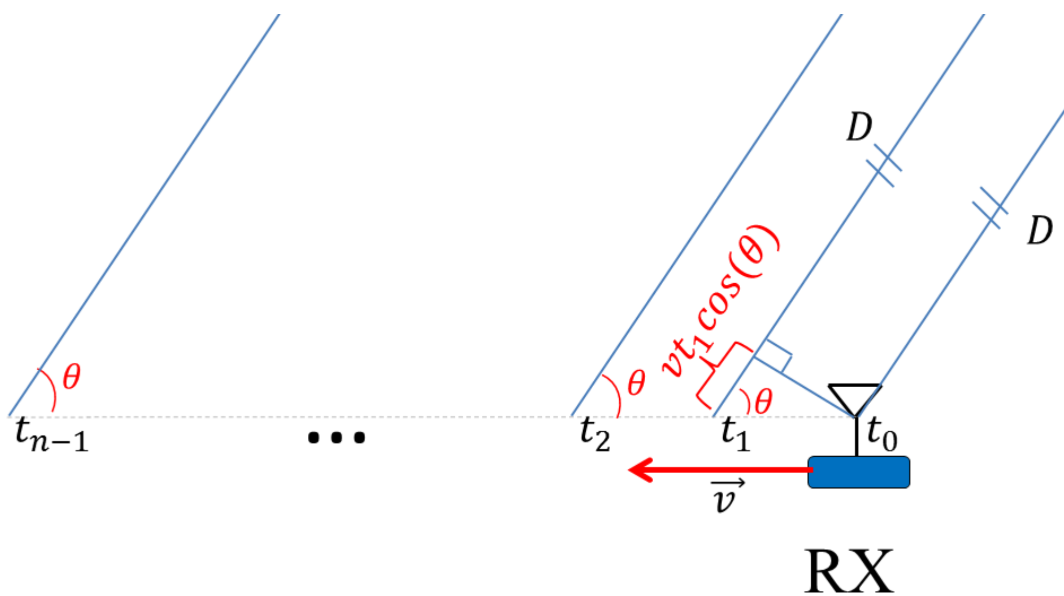
- Developed system: ***Ubicarse***

Angle of arrival – how does it work



Synthetic aperture

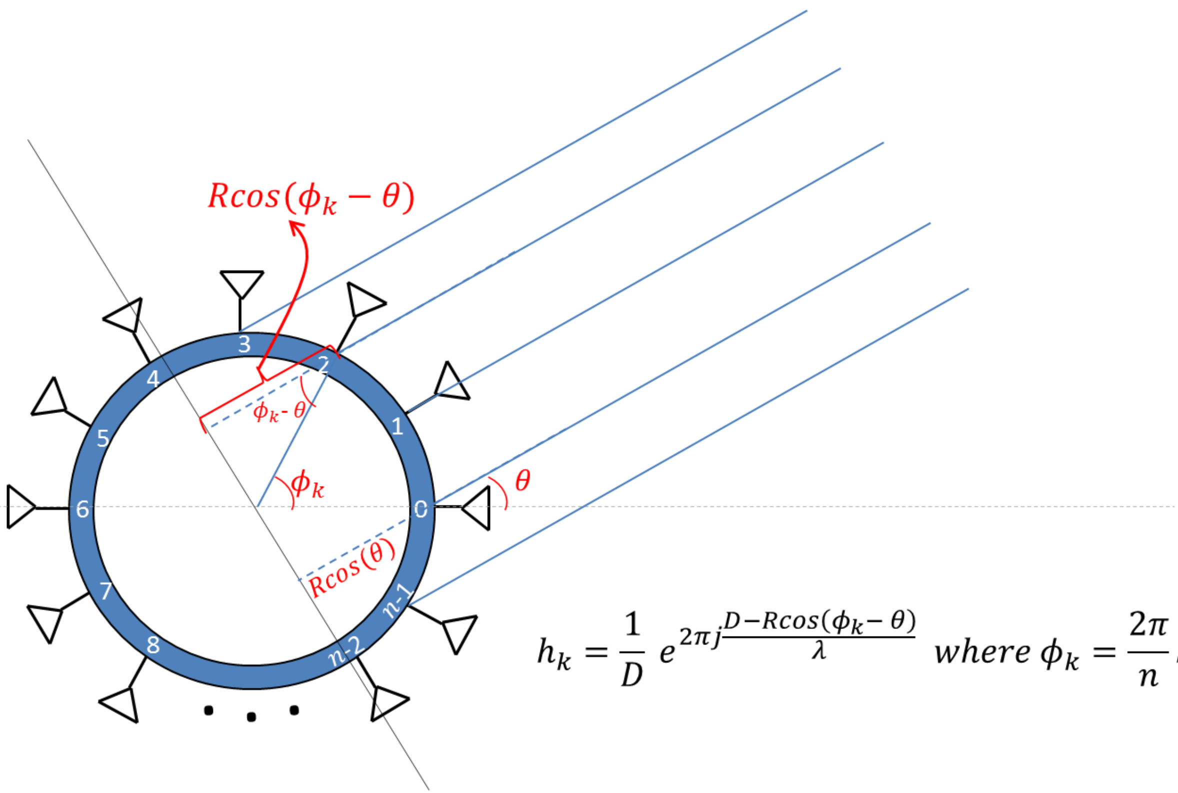
- Emulate antenna array
- Technique used in ***synthetic aperture radar (SAR)***

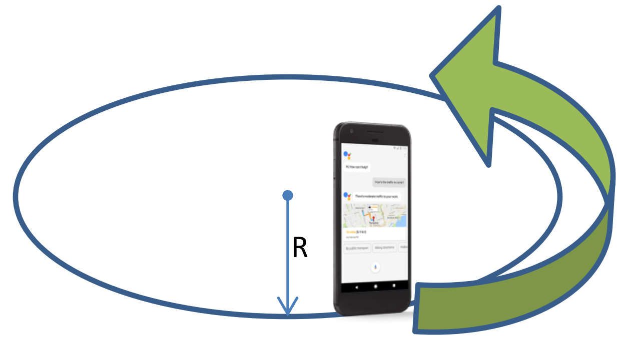


$$h_t = \frac{1}{D} e^{2\pi j \frac{D + vt\cos(\theta)}{\lambda}}$$

Circular SAR (1/2)

- Start with idea of emulation of circular antenna array





$$h_k = \frac{1}{D}\, e^{2\pi j \frac{D - Rcos(\phi_k - \theta)}{\lambda}} \quad where\ \phi_k = \frac{2\pi}{n} k$$

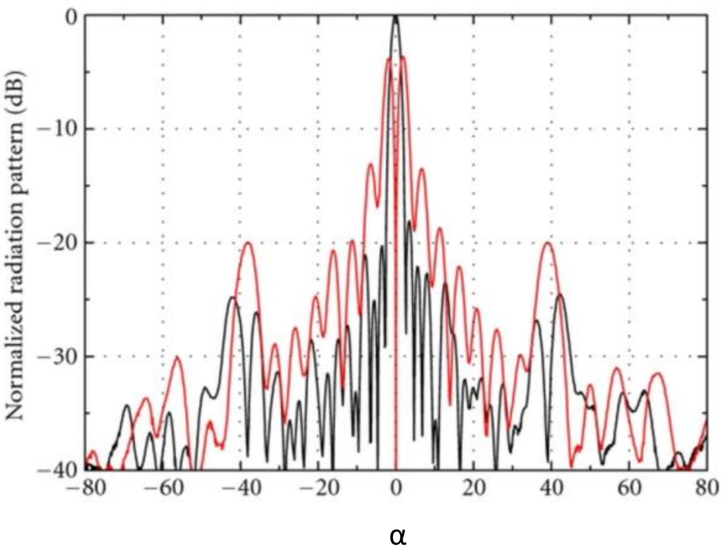
Circular SAR (2/2)

- Channel model for k^th^ snapshot of antenna:

$$h_k = \frac{1}{D} e^{\frac{-j2\pi}{\lambda}(D + rcos(\Theta - \phi_k))}$$

- Relative power along direction α

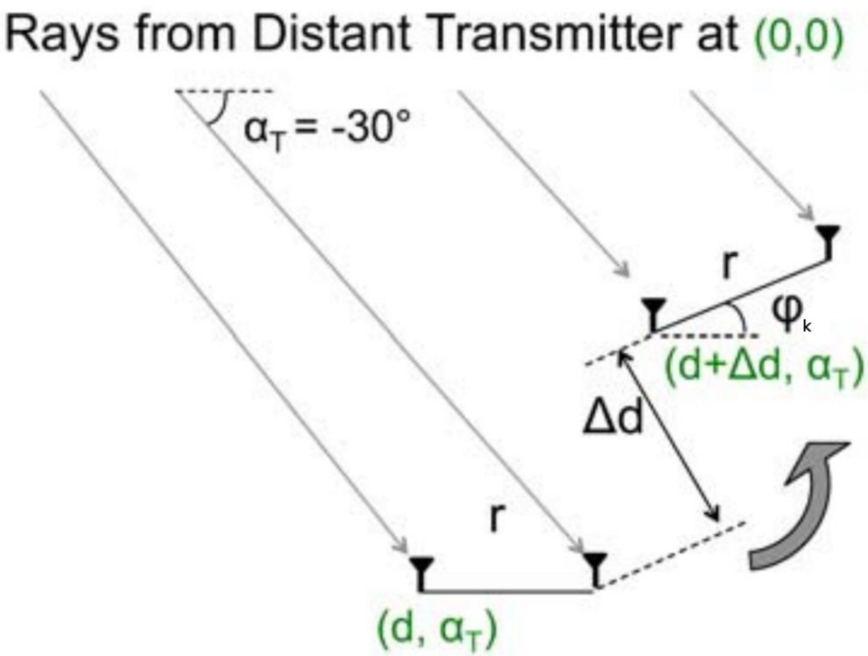
$$P(\alpha) = |\frac{1}{n}\sum_{k=1}^{n} h_k e^{\frac{j2\pi}{\lambda} rcos(\alpha - \phi_k)}|^2$$



Ubicarse - solution

- Translation resilient SAR
- Create accurate indoor positioning system
  - MIMO capabilities of modern devices
  - Information of device’s orientation

Translation-resilient SAR



Measurements at antennas

$$h_{1,k} \approx \frac{1}{D} e^{\frac{-j2\pi}{\lambda}\left(D + \frac{\Delta y_k}{sin(\alpha_T)}\right)}$$

$$h_{2,k} \approx \frac{1}{D} e^{\frac{-j2\pi}{\lambda}\left(D + \frac{\Delta y_k}{sin(\alpha_T)} + rcos(\alpha_T - \phi_k)\right)}$$

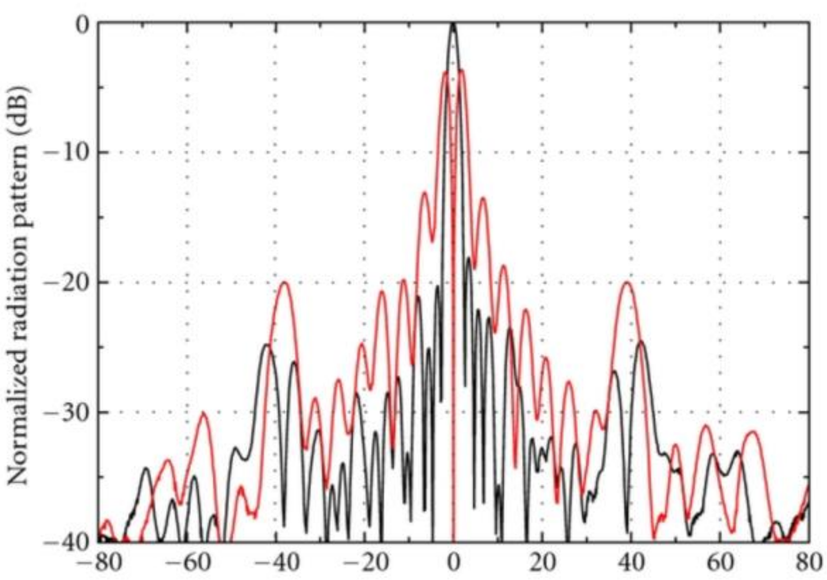
Relative channel

$$\hat{h_k} = \frac{1}{D^2} e^{\frac{-j2\pi}{\lambda} rcos(\alpha_T - \phi_k)}$$

Translation-resilient SAR

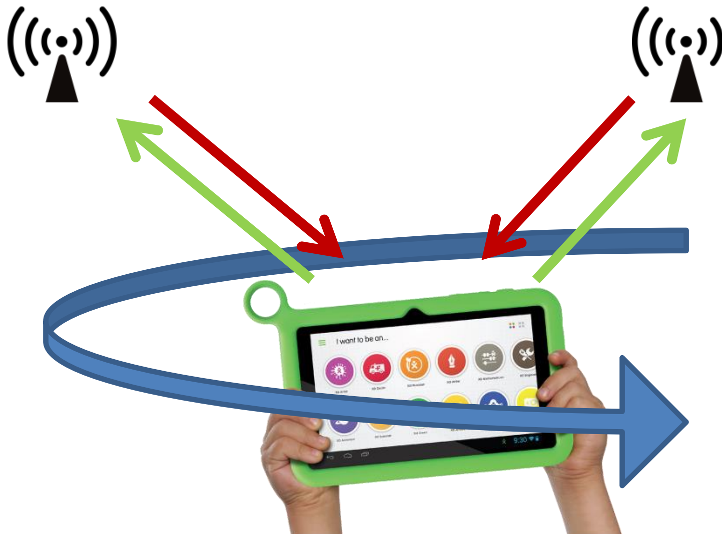
- Use same SAR formula for relative channel power:

$$P(\alpha) = |\frac{1}{n}\sum_{k=1}^{n} \hat{h_k} e^{\frac{j2\pi}{\lambda} r cos(\alpha - \phi_k)}|^2$$

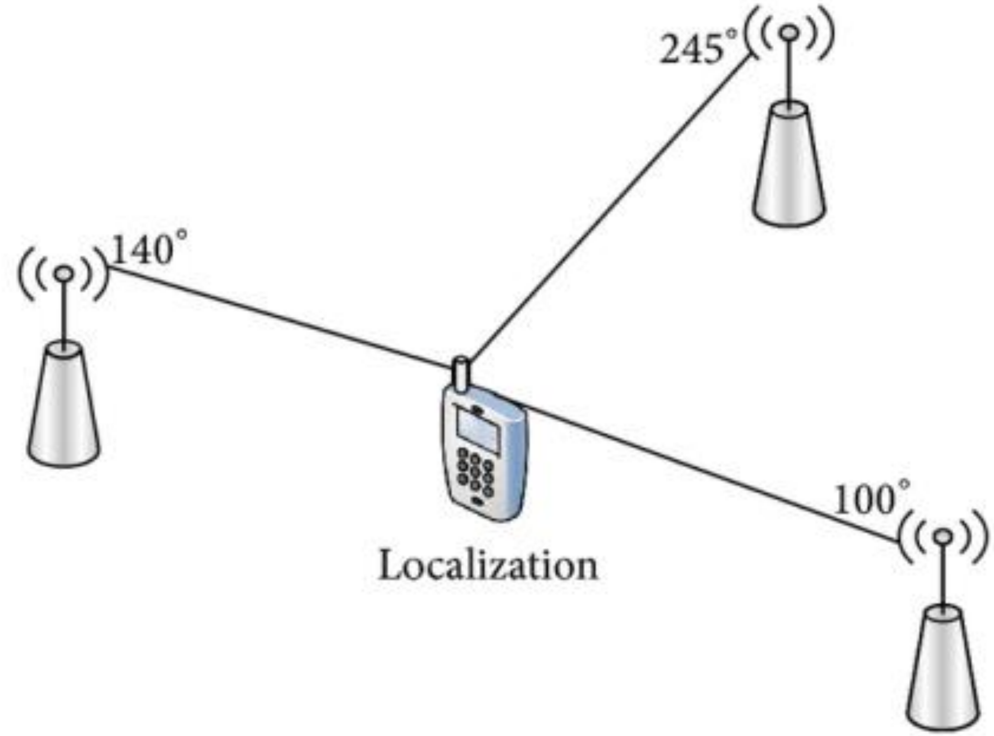


Accurate device localization

- Localization proces:
  1. App asks user to twist device
  2. Issues beacon requests to neighbor access points to estimate channels from them
  3. Perform SAR to generate multipath power profiles
  4. …
  5. Show precise location



Calculate location

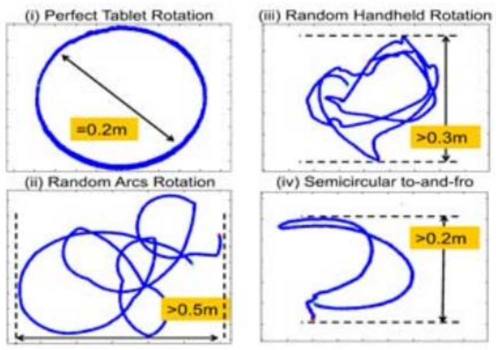


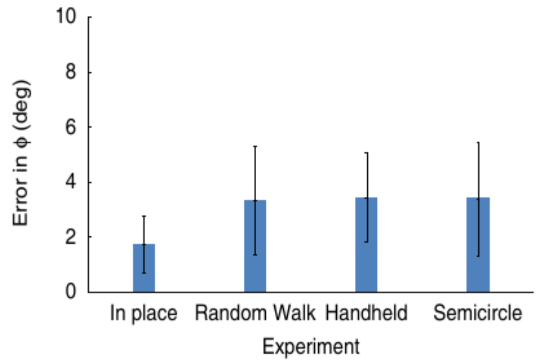
Object geotagging

- Localize devices with no radio devices attached
- Using camera & stereo vision algorithms

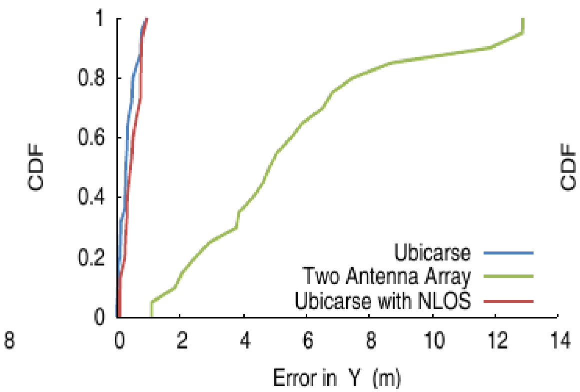
How does Ubicarse perform

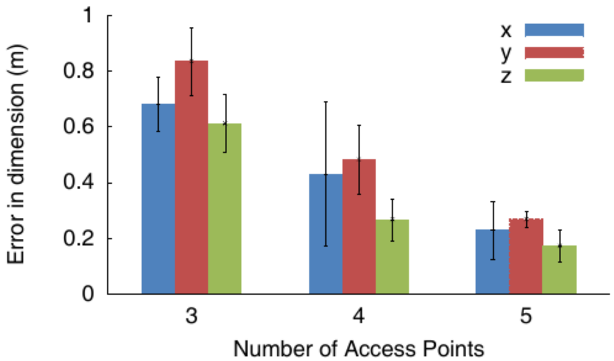
- Translation resilience





- Device localization





Different approach

- What if we don't want to:
  - Have absolute position, but just absolute distance
  - Have many access points
  - Have to rotate device
- Different use cases:
  - Smart home occupancy
  - Geo-fencing

Time of flight

- Time it takes for signal to propagate from transmitter to receiver
- Absolute time of flight
- High precision required

Calculate absolute ToF

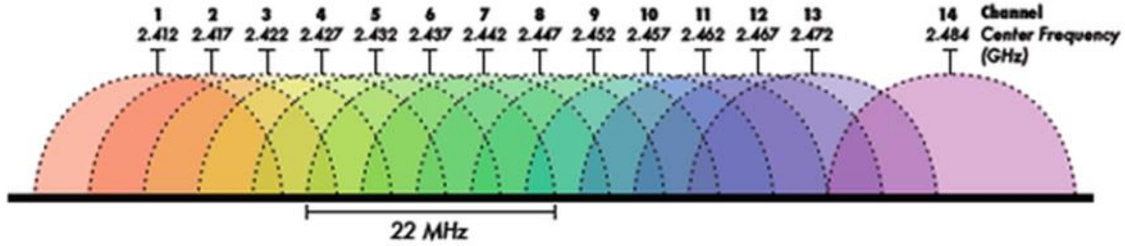
- Emulating ultra wideband radio with WiFi

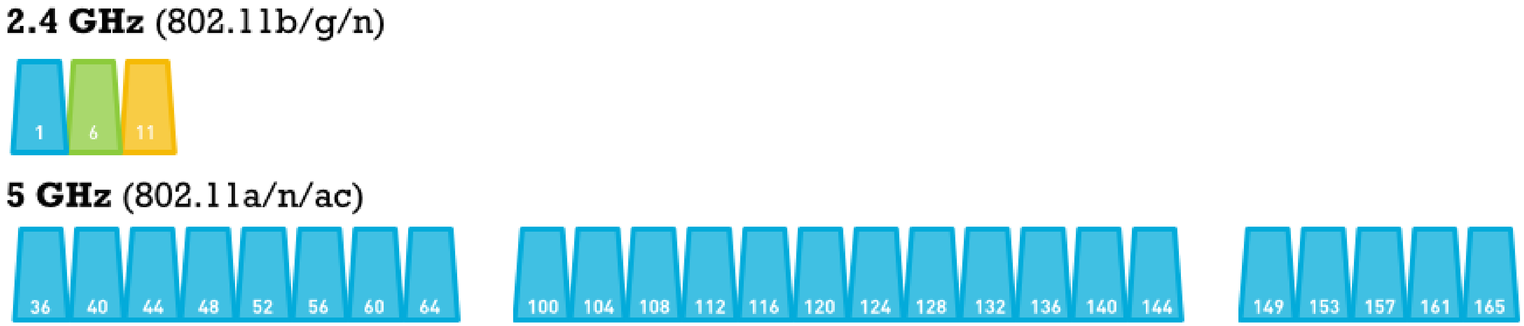
"Decimeter-Level Localization with a Single WiFi Access Point"
Deepak Vasisht, Swarun Kumar, Dina Katabi

- Developed system: **Chronos**

WiFi channel

- Can WiFi channels be combined to emulate ultra wideband radio?





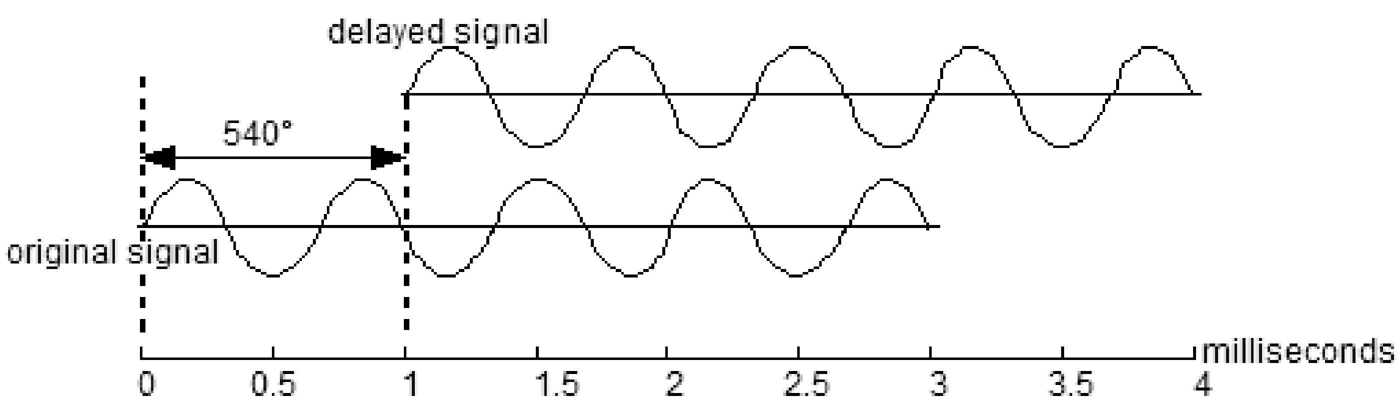
Chronos

- Indoor positioning system
- Calculates absolute distance by measuring ToF
- Sends data over different WiFi channels to emulate wide band radio
  - Different frequencies have different properties

Measuring time of flight

- For a single channel

1. $h = ae^{-j2\pi f\tau}$
2. $\angle h = -2\pi f\tau \ mod\ 2\pi$
3. $\tau = -\frac{\angle h}{2\pi f} \ mod \frac{1}{f}$



Measuring time of flight

- Modulo measurements @2.4GHz
  - ToF = modulo 1/f (0.4ns) – {0.1ns, 0.5ns, 0.9ns,...}
  - Distance = modulo 12cm – {3cm, 15cm, 27cm,...}
- For a range of channels we get system of equations

$$\forall i \in \{1, 2, ..., n\} \quad \tau = -\frac{\angle h_i}{2\pi f_i} \; mod \frac{1}{f_i}$$

Measuring time of flight

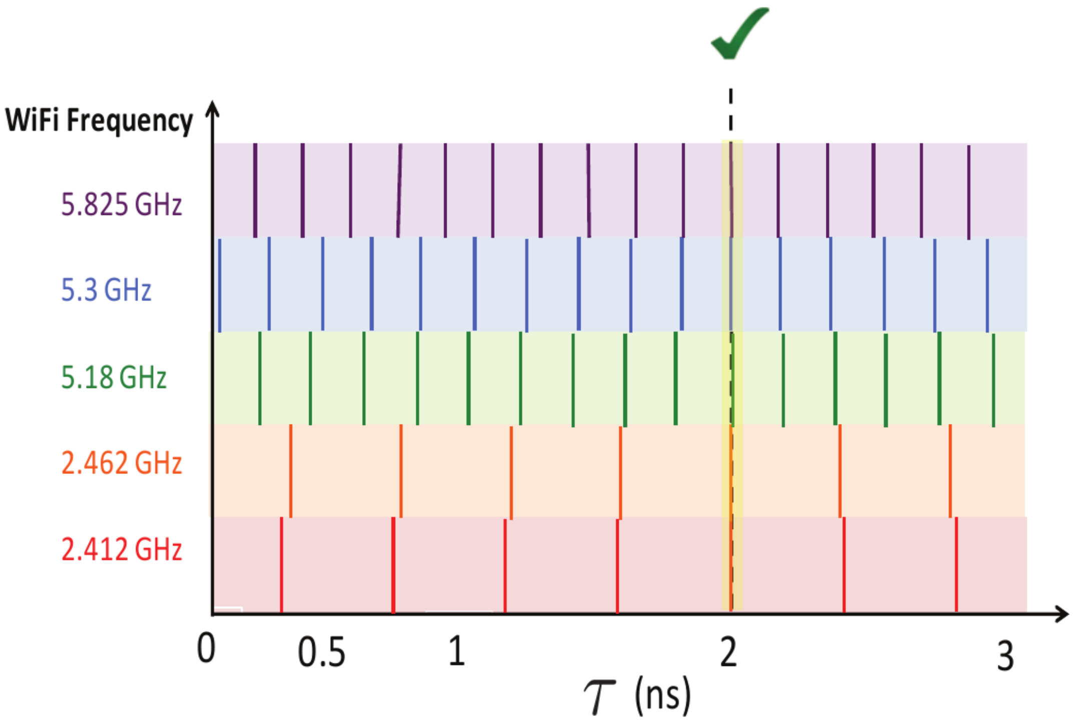
- **Chinese remainder theorem**

$$x \equiv 2 \ (mod\ 3)$$
$$x \equiv 2 \ (mod\ 4)$$
$$x \equiv 1 \ (mod\ 5)$$

- Problem to solve

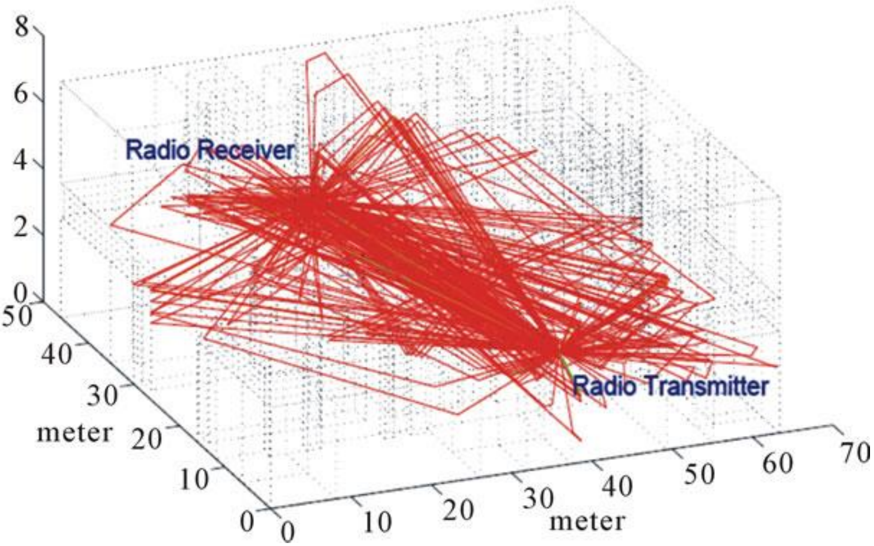
$$\tau = -\frac{\angle h_i}{2\pi f_i} \ mod \frac{1}{f_i}$$

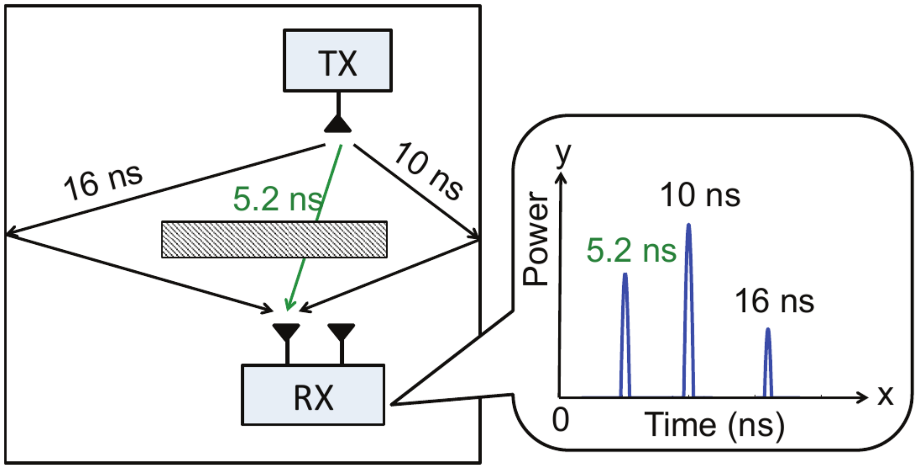
$$\forall i \in \{1, 2, ..., n\}$$



Multipath

- Generate multipath profile
- Choose shortest path – first peak





(a) Testbed

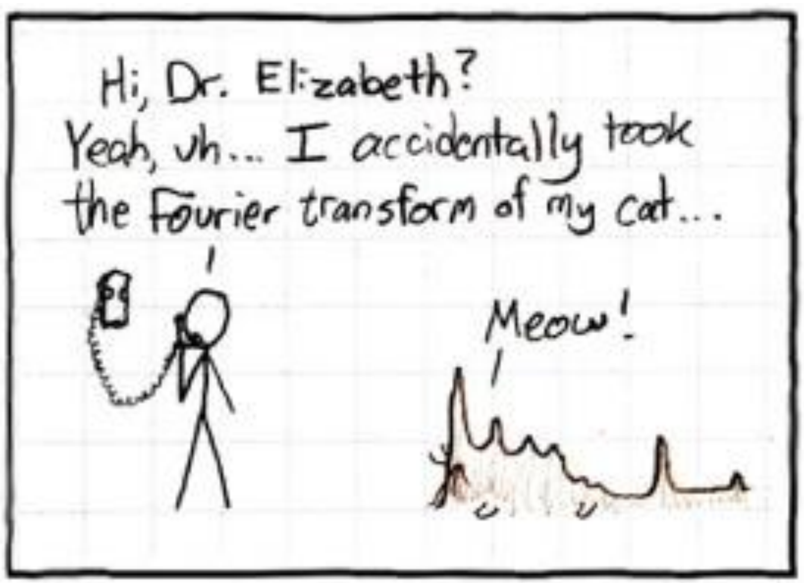
(b) Multipath Profile

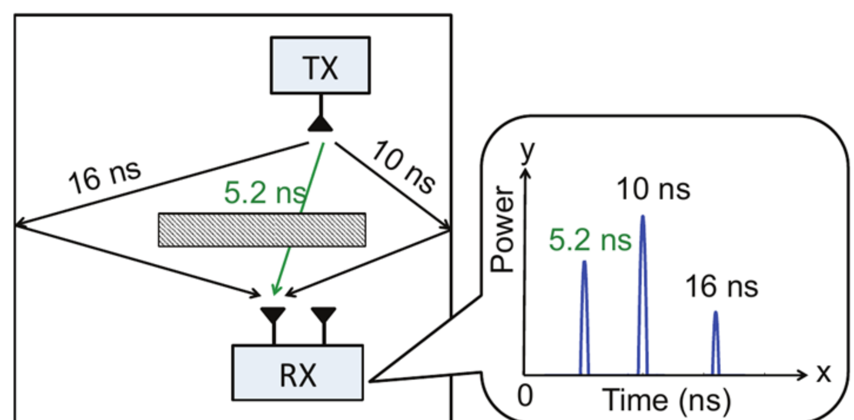
Computing multipath profiles

- Signals reach receiver over *p* different paths

$$\hat{h}_i = \sum_{k=1}^{p} a_k e^{-j2\pi f_i \tau_k}$$

- Discrete Fourier transform?





(a) Testbed (b) Multipath Profile

Phase offset

- Two phase offsets are created:
  - PLL Phase offset
  - Carrier frequency offset
- Recorder state information on transmitter

$$CSI_i^{tx}(t) = \hat{h}_i e^{j(f_i^{tx} - f_i^{rx})t \; + \; j(\Phi_i^{tx} - \Phi_i^{rx})}$$

- Recorder state information on receiver

$$CSI_i^{rx}(t) = \hat{h}_i e^{j(f_i^{rx} - f_i^{tx})t \; + \; j(\Phi_i^{rx} - \Phi_i^{tx})}$$

Fixing phase offset

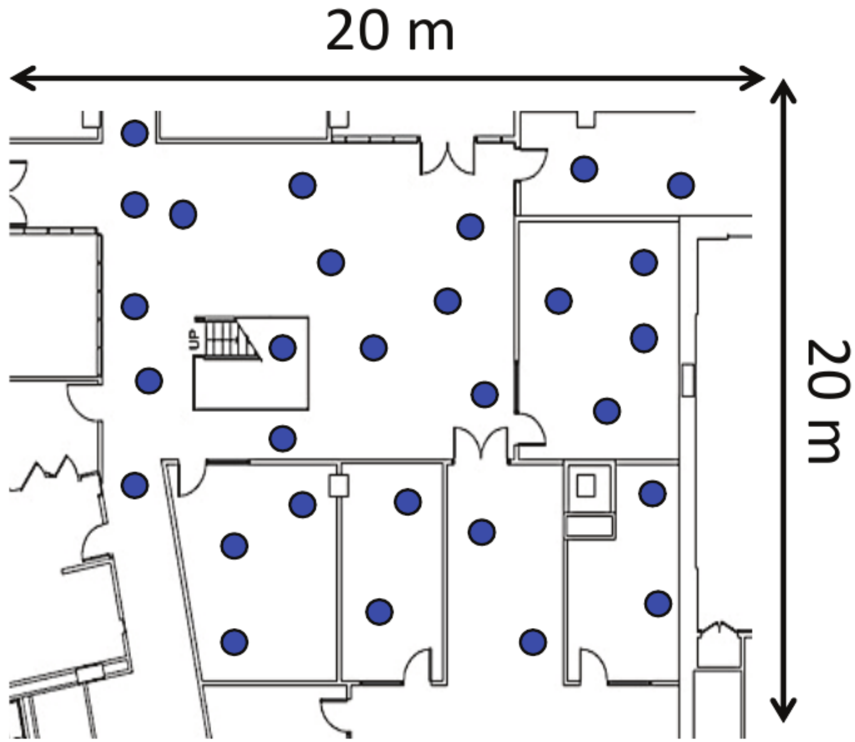
- Multiplying CSI at receiver and sender to recover wireless channel:

$$\hat{h}_i^2 = CSI_i^{rx}(t)\ CSI_i^{tx}(t)$$

- Use that channel to calculate propagation time

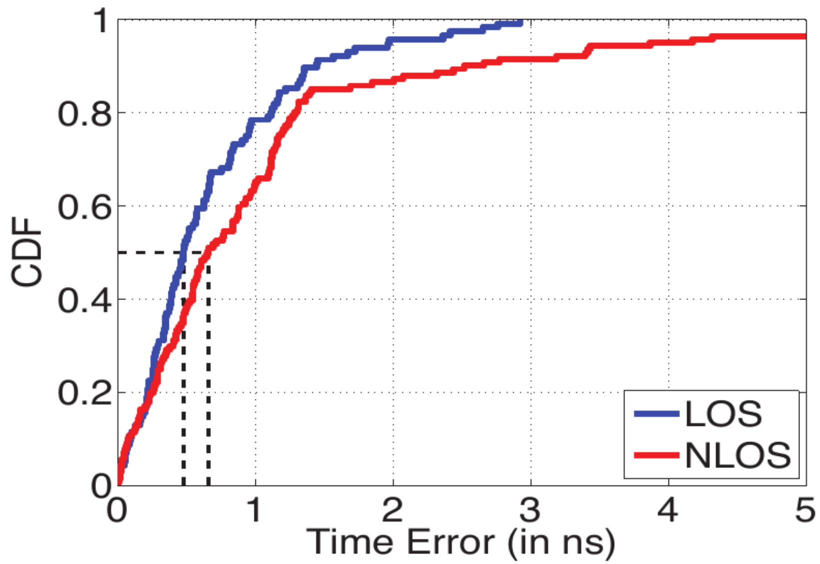
How does Chronos perform

- Test environment for measurement correctness

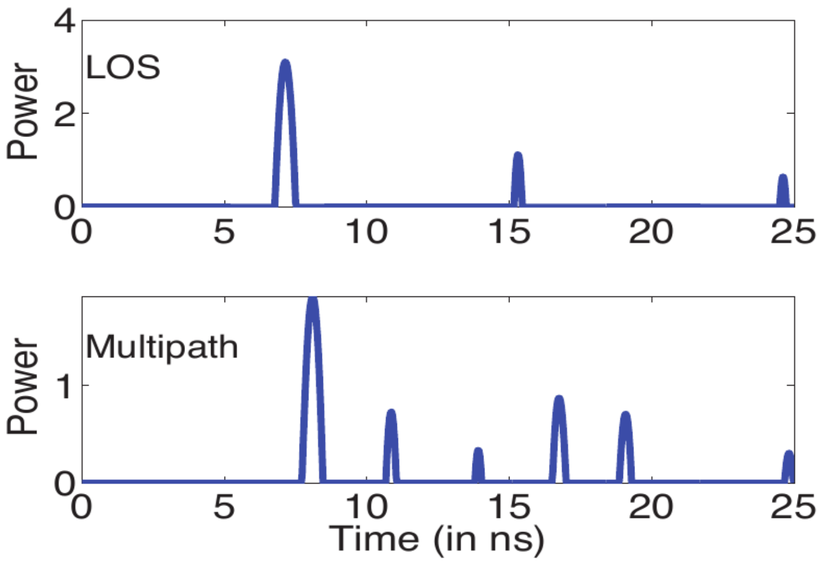


Measurement correctness

Time of flight results

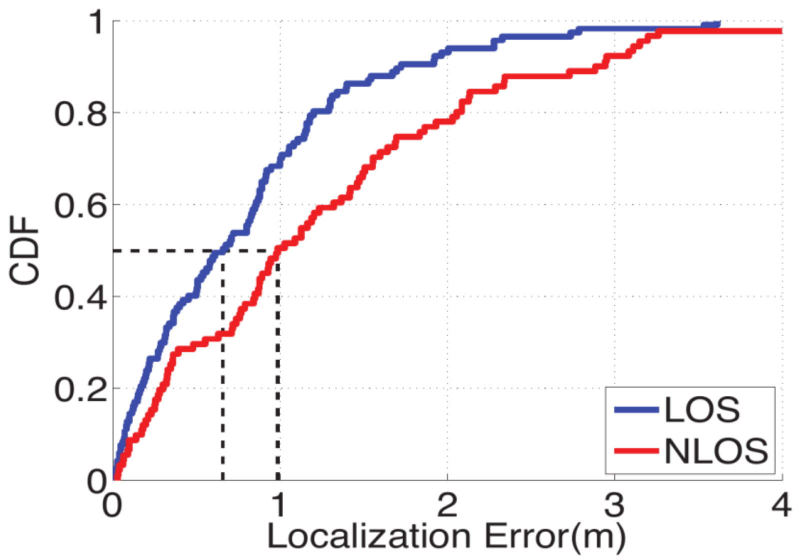


Multipath profile results

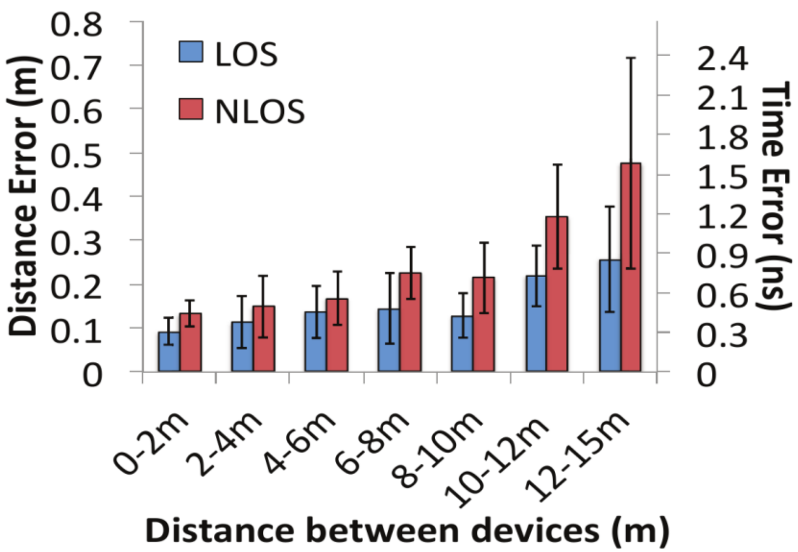


Location accuracy

Location accuracy



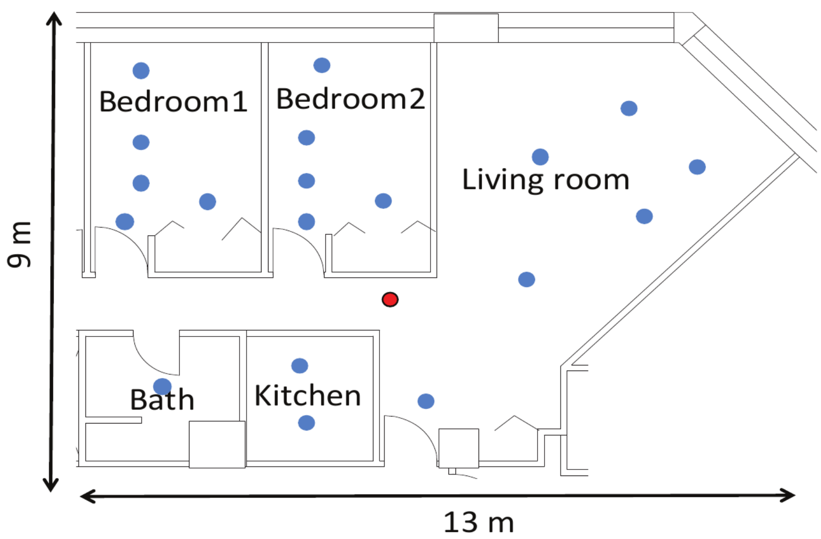
Ranging accuracy



Real use case performance

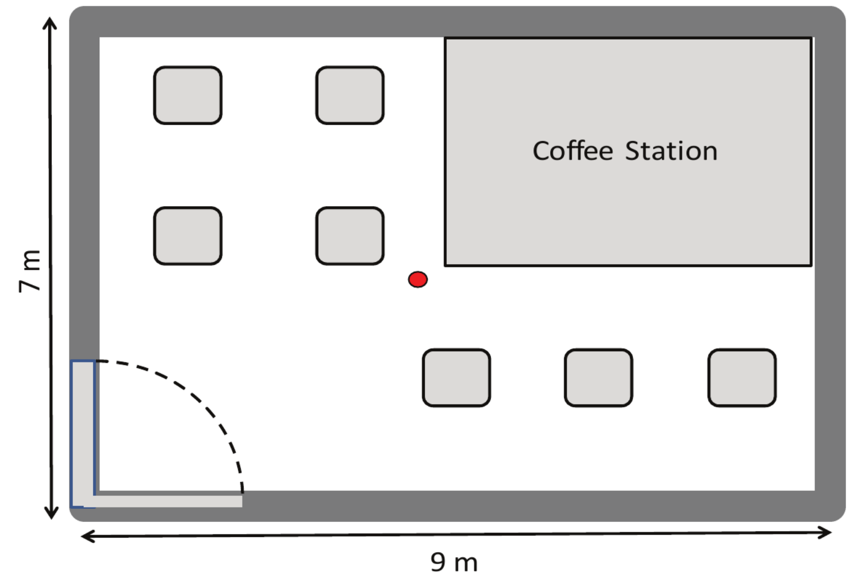
Room occupancy

94% correct



WiFi Geo-fencing

97% correct



Privacy concerns

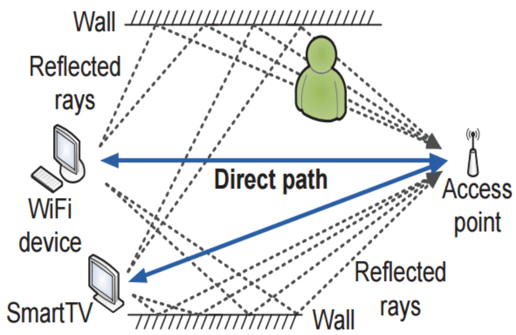
- Can we use WiFi signal as covert channel?
- WiFi signals travel through walls
- Curious neighbor, or burglar?

What can one hear?

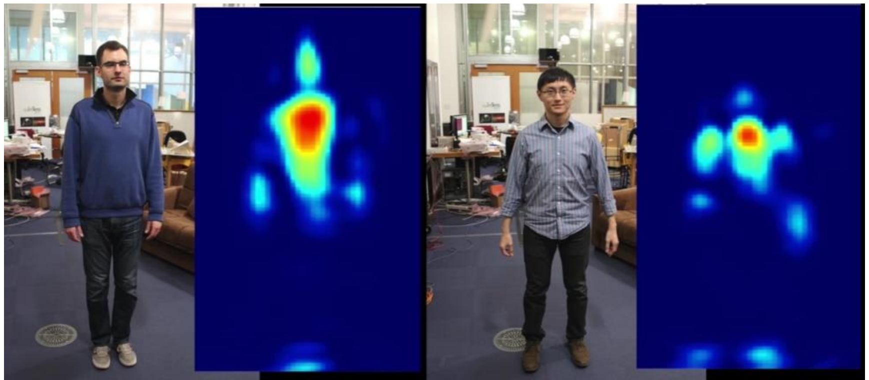
- WiHear [link]

(a) æ (b) u (c) s

- E-eyes [link]



- See through walls with WiFi [link]



Solution?

Less radical solution?

Usable solution?

- Privacy leakage lays in physical not in logical (data) layer
- Just distort physical layer (obfuscate)

"PhyCloak: Obfuscating Sensing from Communication Signals"

Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan, Anish Arora

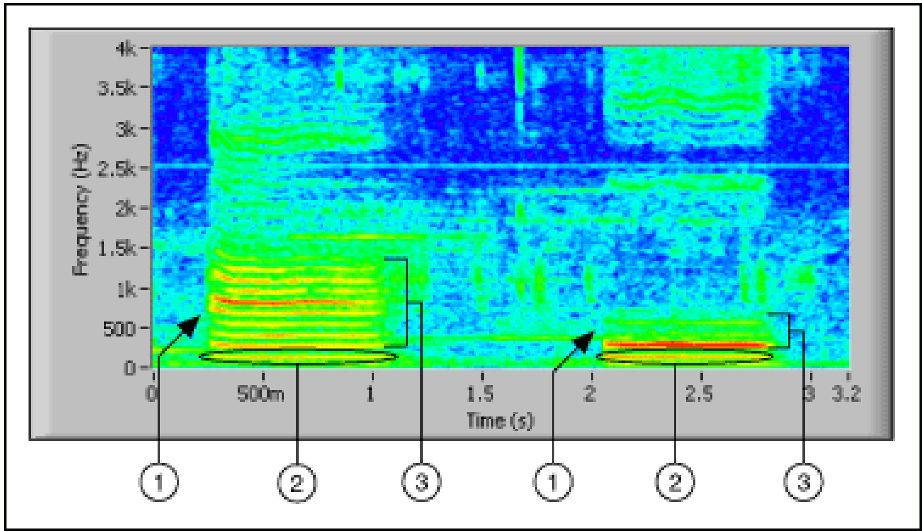
- Developed solution: ***PhyCloak***

What is sensitive data?

- Reflected signal from obstacles

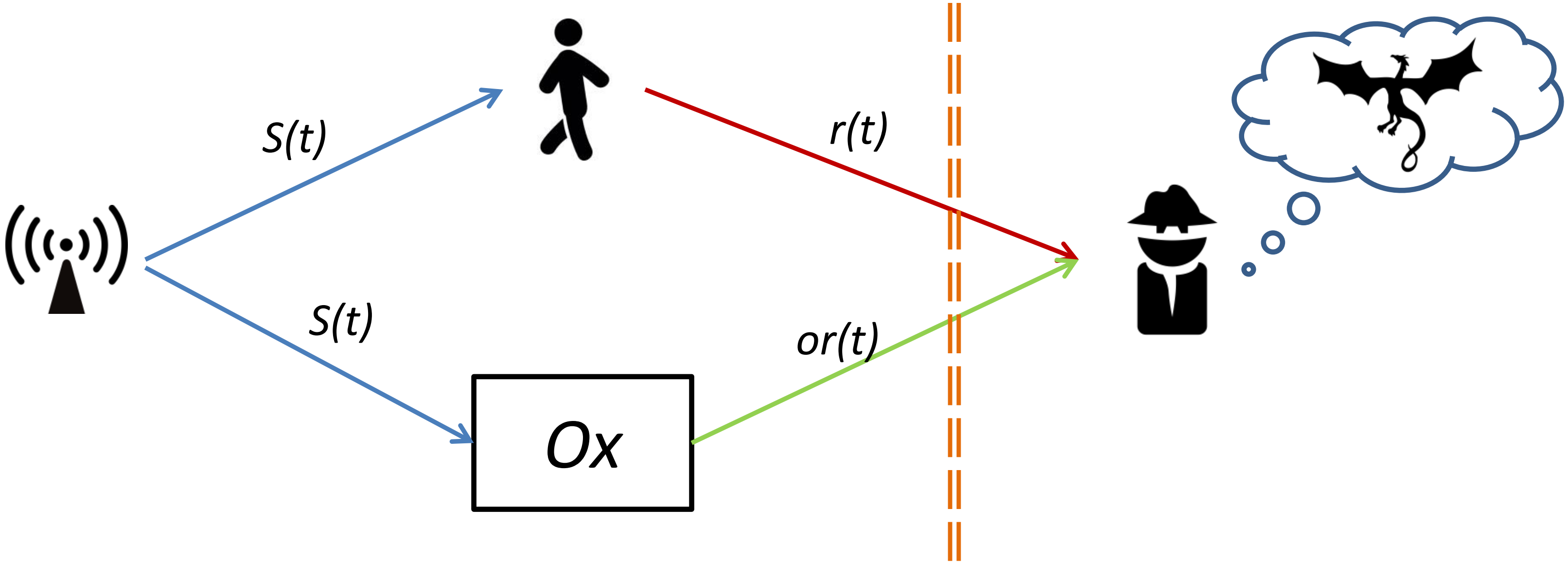
$$r(t) = a\ s(t)\ e^{j2\pi(f_c+\Delta f)(t+\Delta t)}$$

- 3 degrees of freedom (3DoF)
  - Amplitude gain
  - Delay
  - Doppler shift

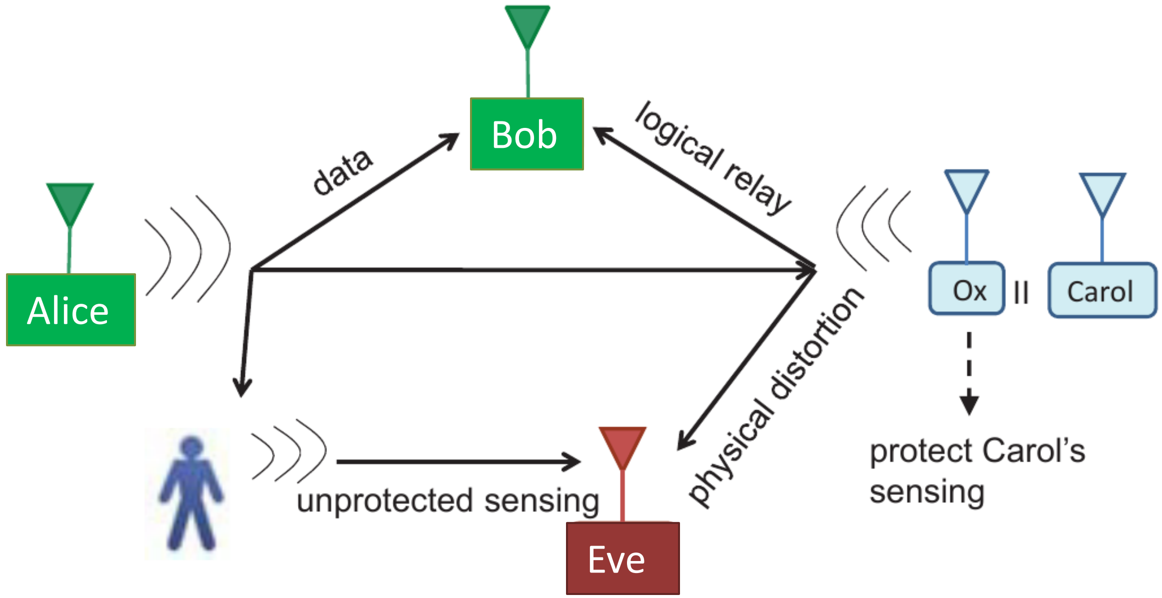


How to hide sensitive data

- Obfuscator needs to change 3DoF of reflected signal
- Build obfuscator to create another multipath signal
- Create signal in a way to cancel sensitive data out



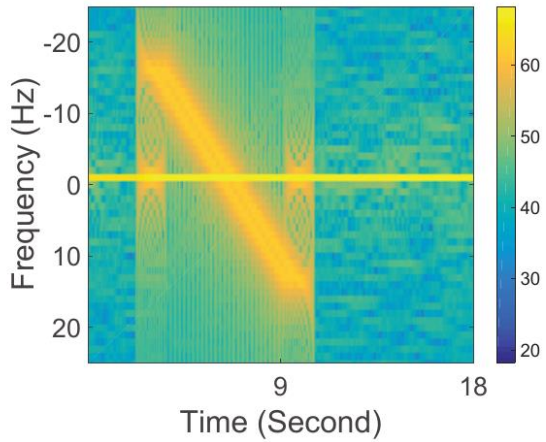
System goals

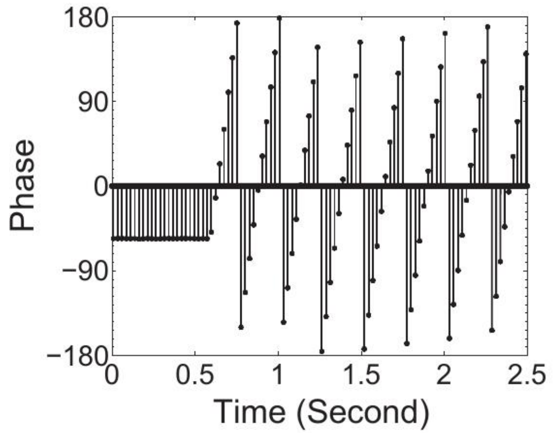


- Obfuscate Eve's sensing
- Preserve Carol's sensing
- Don't degrade throughput in link Alice – Bob
- **Online self-channel estimation**

Obfuscating 3DoF

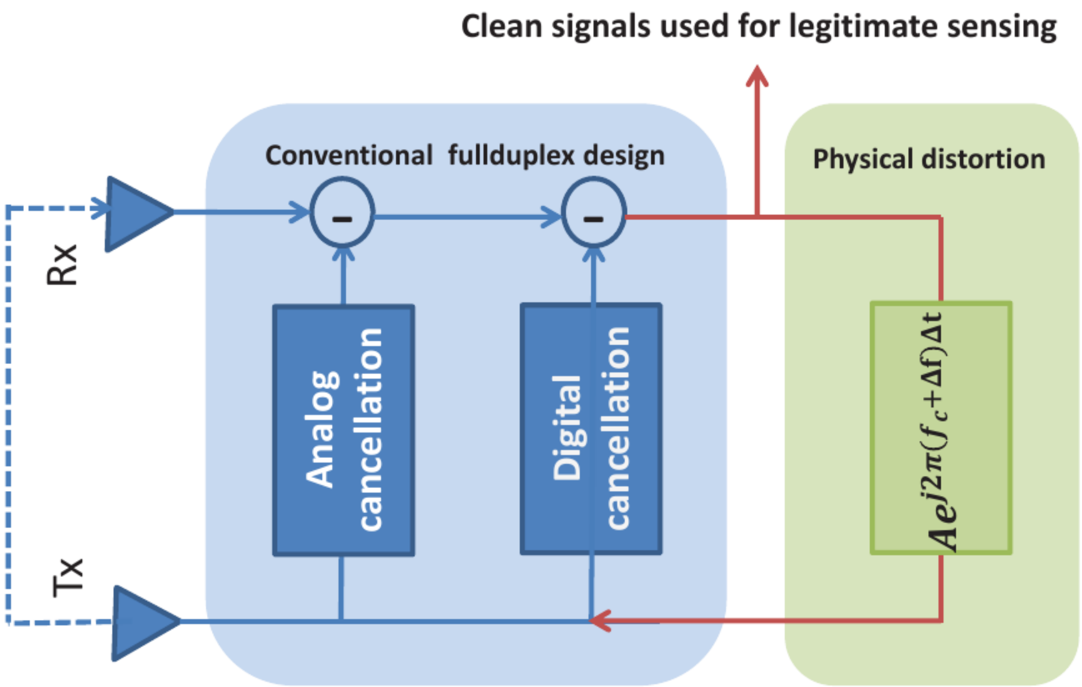
- Amplitude gain
  - Amplify received samples with different levels
- Doppler shift
  - Rotate nth sample by $2\pi n\Delta f\overline{\Delta t}$
- Delay
  - Delay to be forwarded signals
  - Done by rotating samples by fixed phase





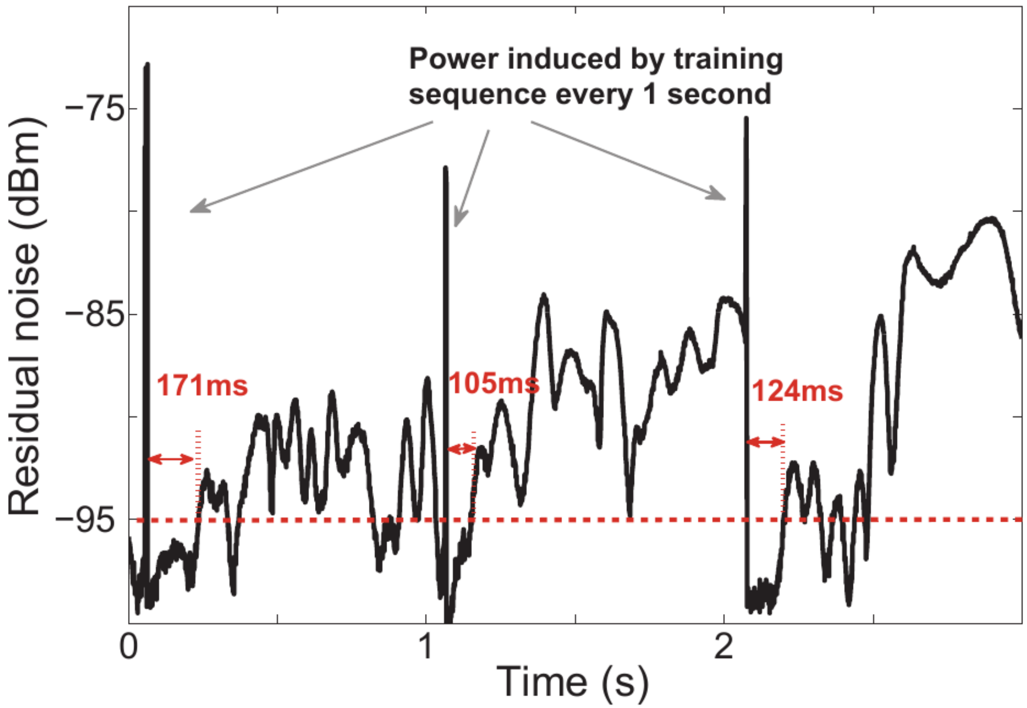
PhyCloak design

- High level block diagram



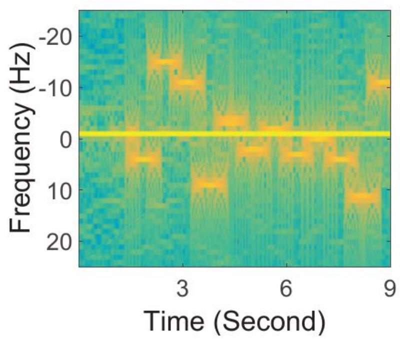
Self channel estimation - problem

- Human movement near Ox causes strong residual noise

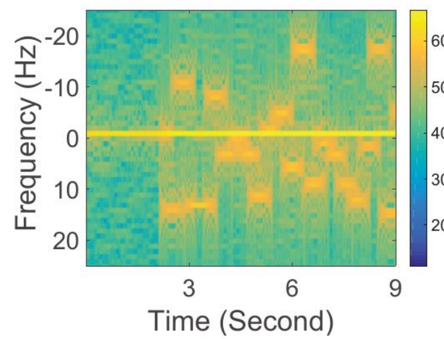


Hiding Doppler shift

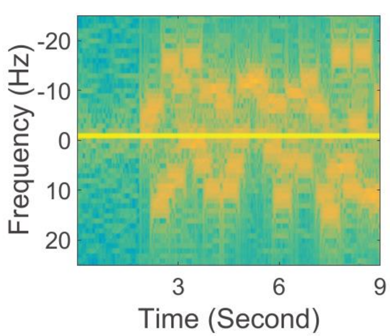
- By carefully choosing time to change phase Doppler shift can be hidden



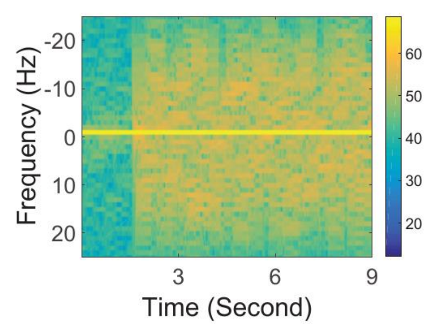
(a) 1s



(b) 0.5s



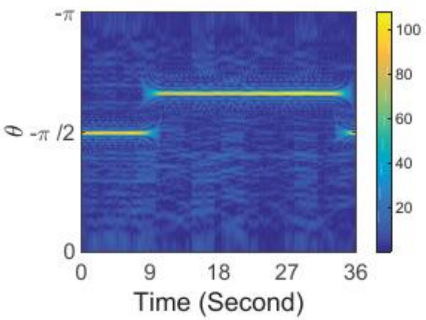
(c) 0.125s



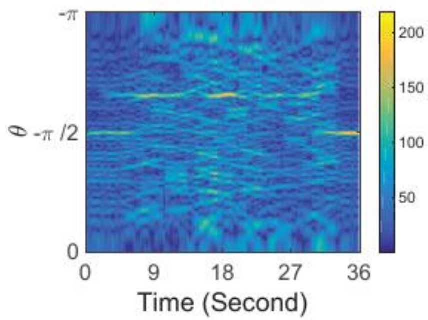
(d) 0.05s

Results of obfuscation

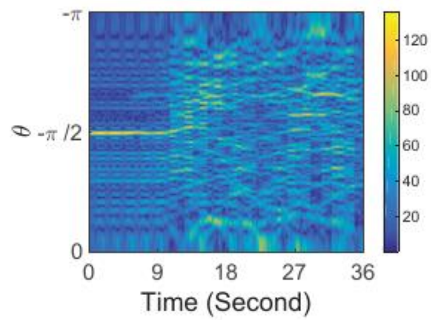
- Signal to Obfuscation Ratio (dB)
- Hiding human motion



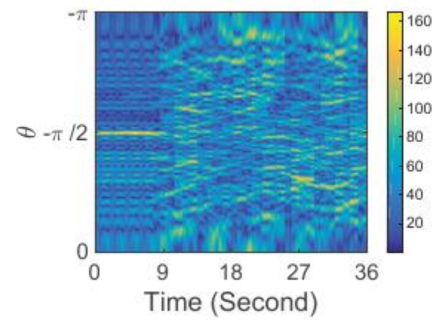
(a) Motion towards a Wi-Vi style sensor with constant angle



(b) 0dB



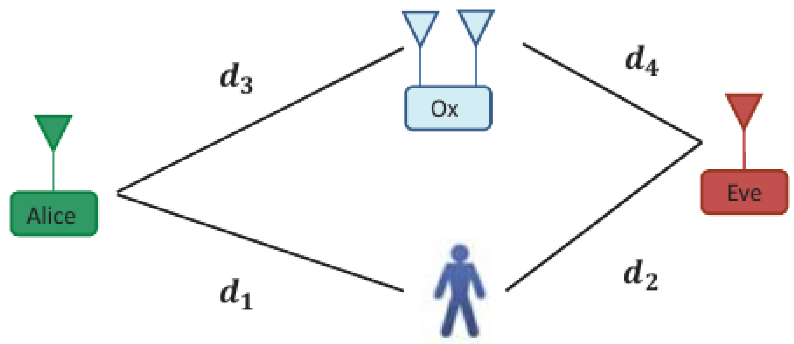
(c) -3dB



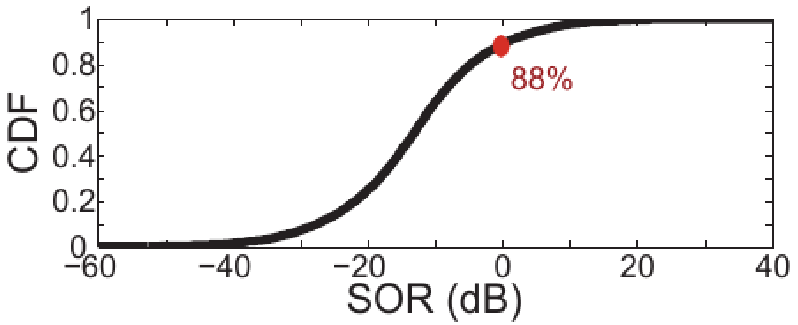
(d) -6dB

Results of obfuscation

- Test scenarios:



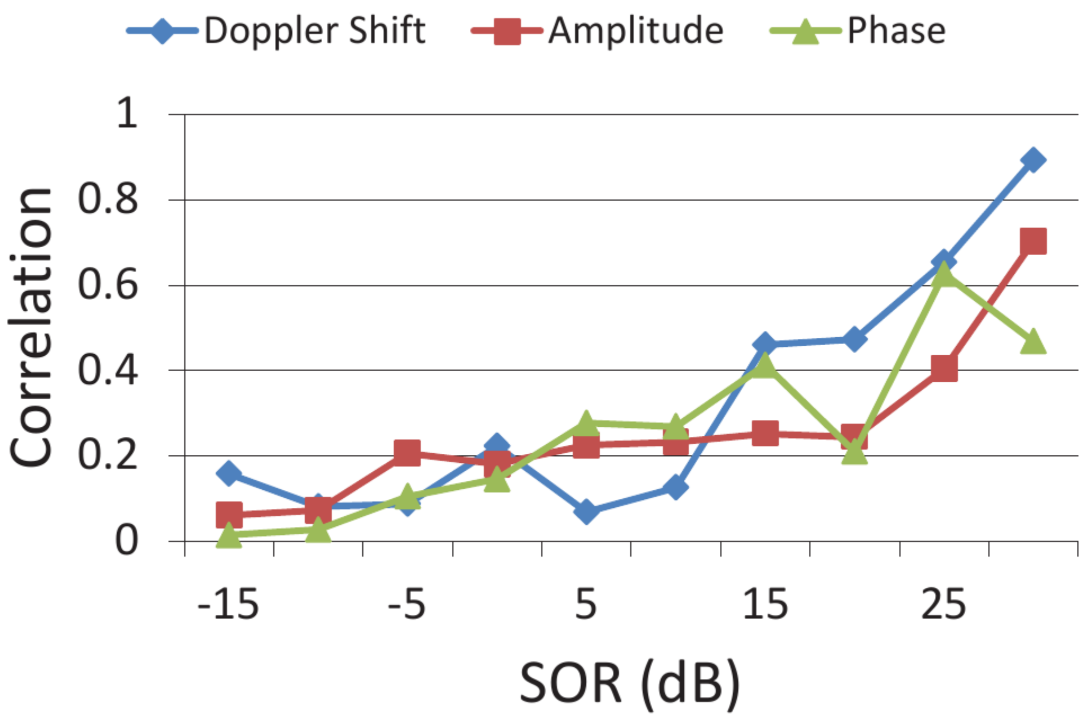
(a) Placement of all the involved parties



(b) SOR distribution

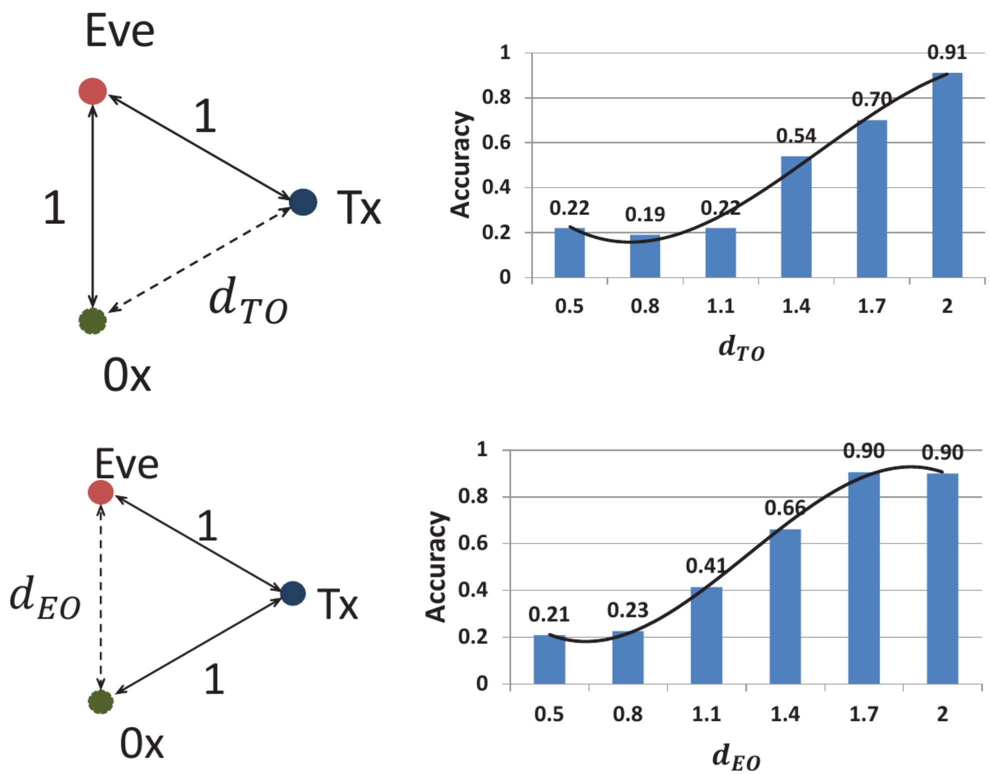
Obfuscation performance

- 3 Dof correlation vs SOR



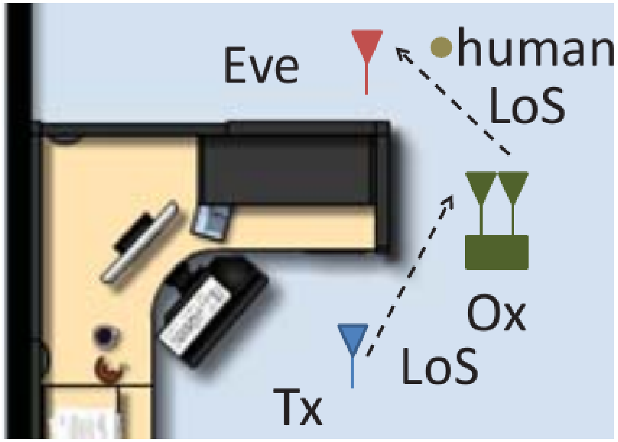
Obfuscation performance

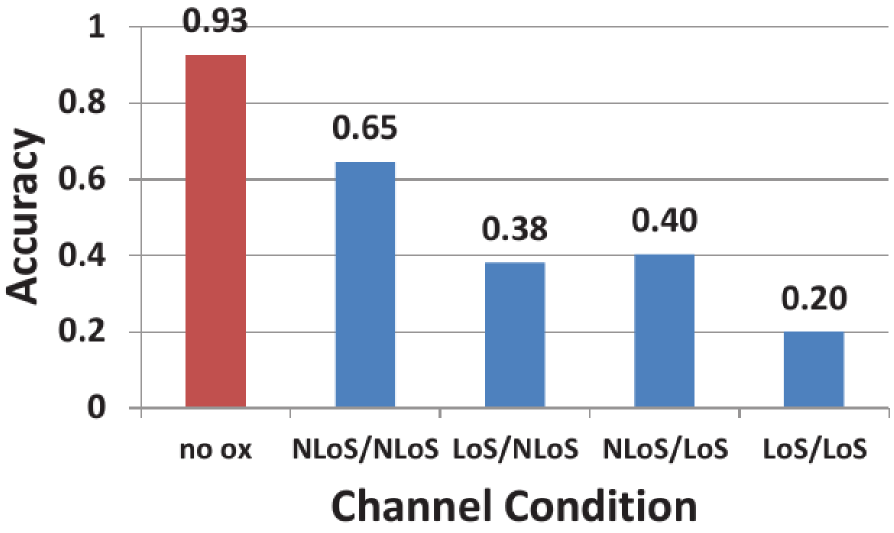
- WiSee gesture detection accuracy
  - Recognizes gestures: drag, push, dodge…



Obfuscation performance

- WiSee NLOS/LOS performance





Wi-Fi localization

QUESTIONS?