Today

- What does the network know?
- Communication Privacy
- Location Privacy
- Sensing Privacy / RF-Protect

What does the Network Know?

Location

- 3rd floor AP on Siebel
- ArrayTrack → what room are your device in Bldg

Historical Location

- Collaborate

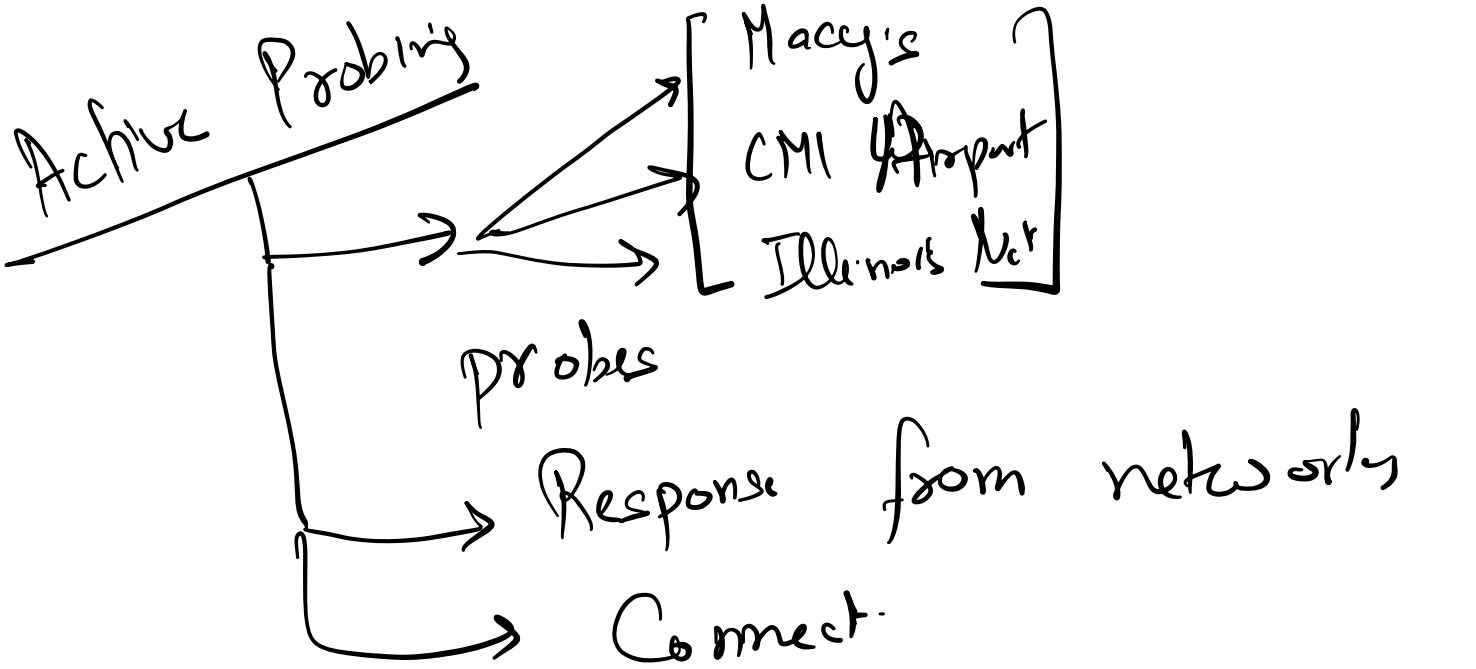
MAC address

Macy's → Bath & Body Works

Probing

Passive Connection

- wait for AP to broadcast
- check if you have credentials for that AP
- exchange info & connect.



Type of device ↑ device

Passive sensing → when people are
→ breathing
→ emotional state.

Would through walls.

Communication Privacy Efforts

MAC randomization.

↳ XX:XX:XX:XX:XX:XX

Macy's

Nordstrom

Active probing.

↳ Macy's

Illenois Net

CMI Airport

Einstein Bros.

Macy's

Probing

Randomly

MAC

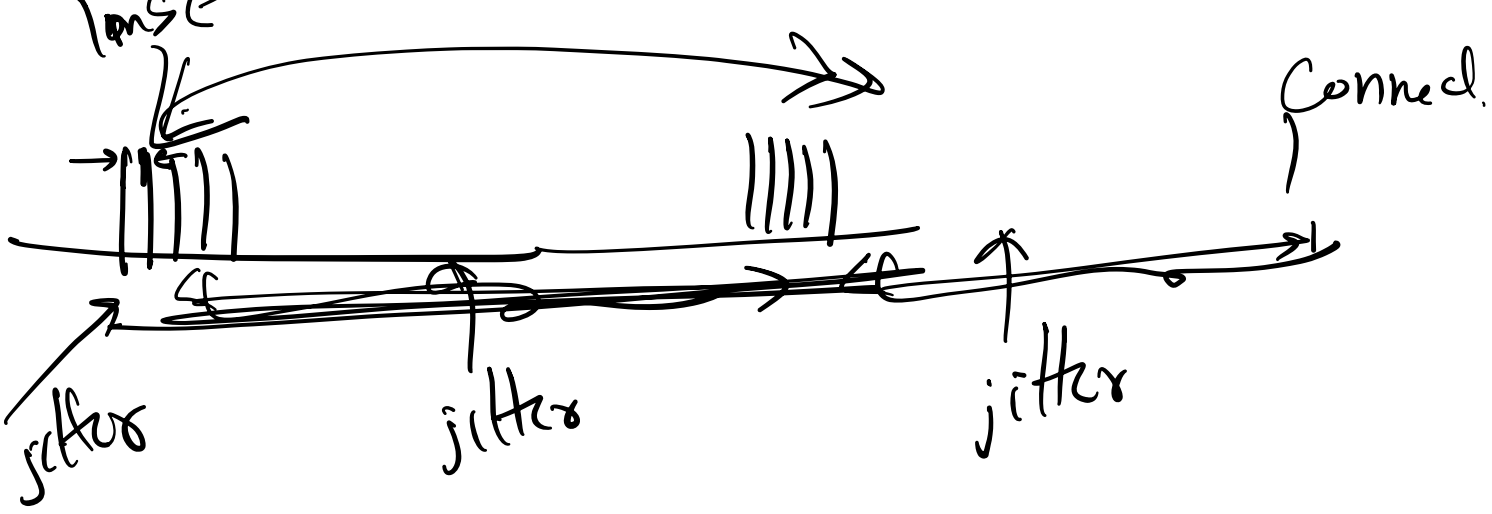
Macy's

Connect

Real MAC

Timing-based Attacks

~~allms~~



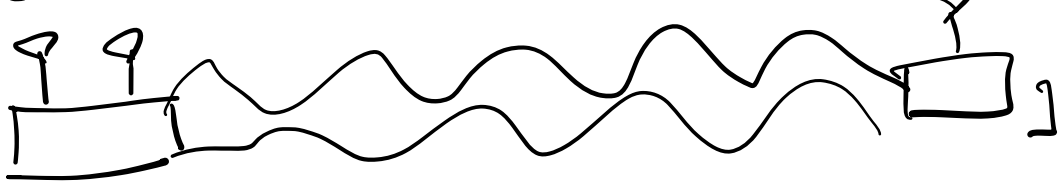
(Timing-jitter based defenses) kind of new.

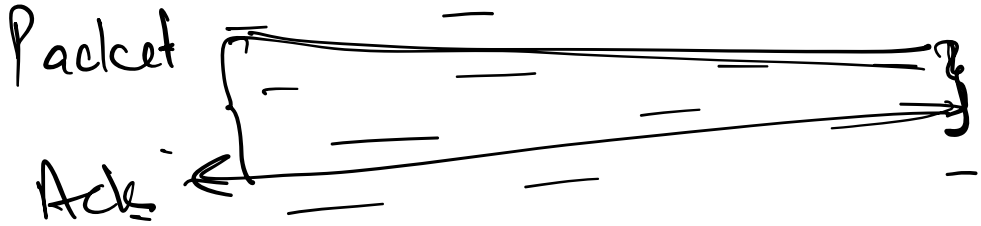
Location Privacy

- Building-level location
- Room-level location

Angle

Distance



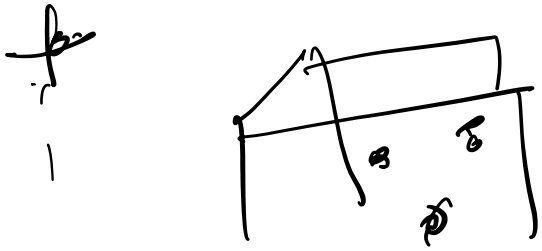


30m
100ns
9 μs
time
10μs
11 μs

randomize this time by a bit

reduce ToF based location

Chronos



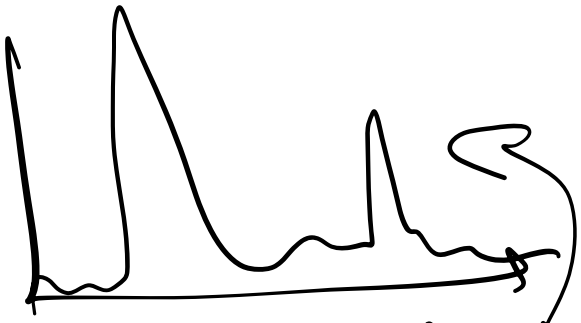
accuracy

Random noise ⟵

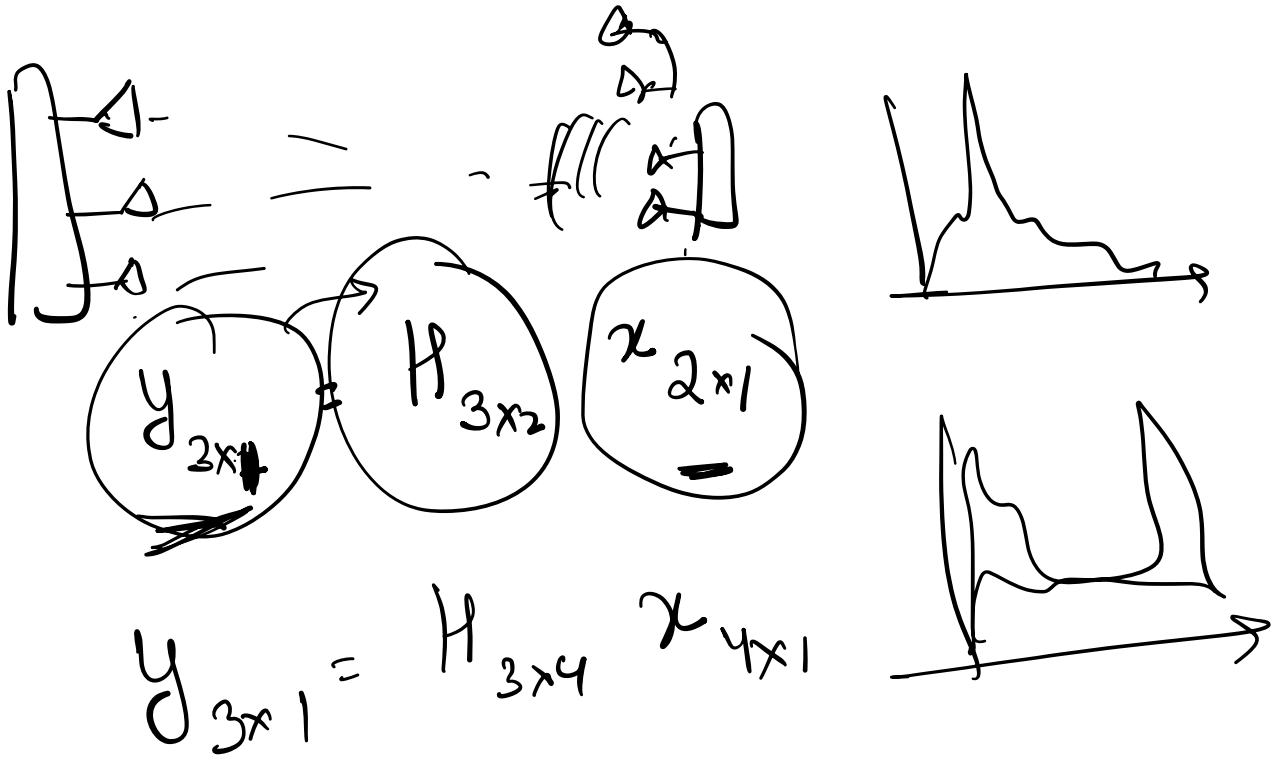
↳ the adversary can average.

Angle-based localization

Beamforming



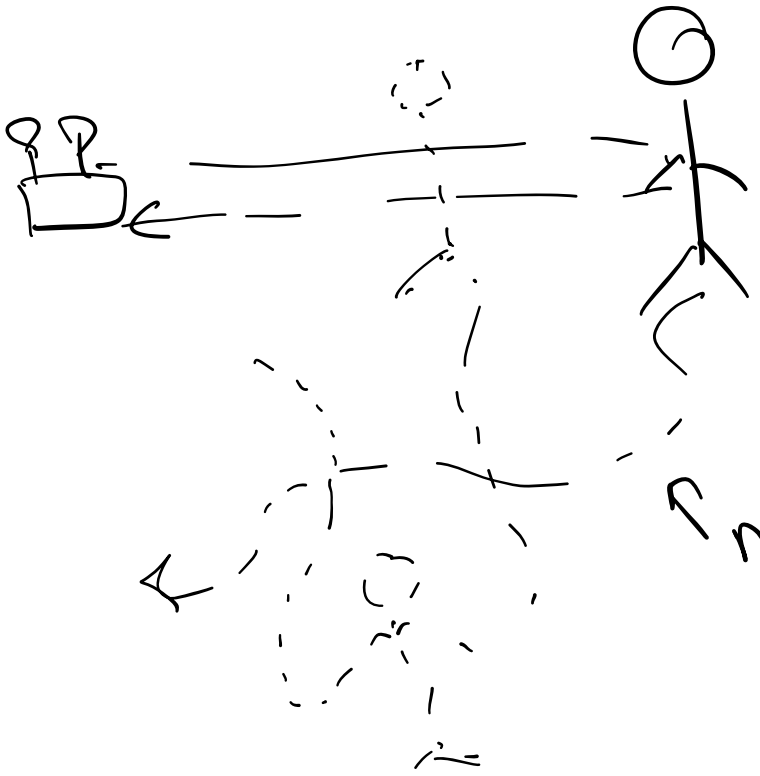
$$\underset{3\times 1}{\vec{y}} = \underset{3\times 1}{\vec{H}} \; \underset{1\times 1}{x} \rightarrow \begin{bmatrix} h_1 \\ h_2 \\ h_3 \end{bmatrix} \quad h_2/h_1 \;\; h_3/h_2$$



$$y_{3\times 1} = H_{3\times 4}\, x_{4\times 1}$$

Sensing Privacy

WiTrack



"Soli"

↑ make this person disappear is very hard.

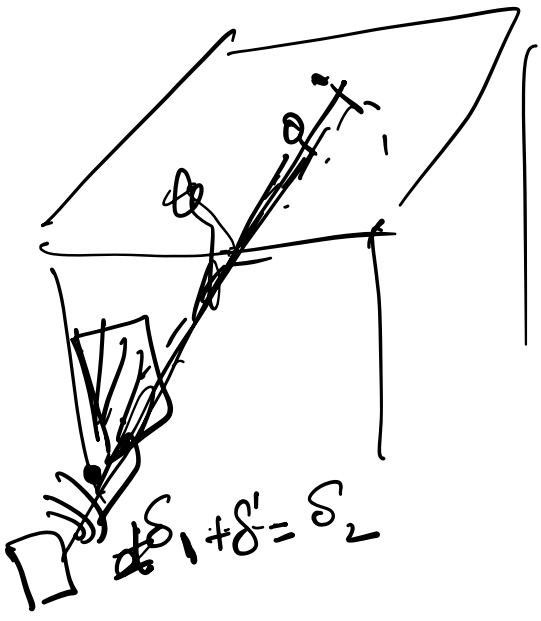
→ Spoof distances

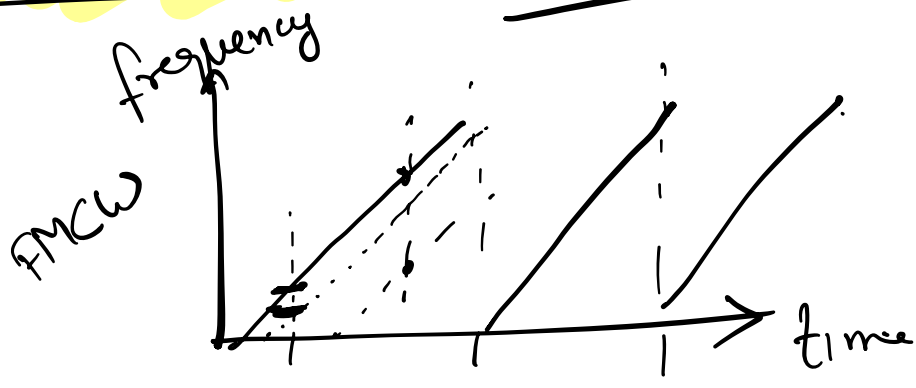
→ Angles

→ Realistic.

Distance Spoofing

WiTrack-like.





frequency shift $\propto$ delay

↑

induce different freq. shifts.

kHz-level

Reflector just adds a delay

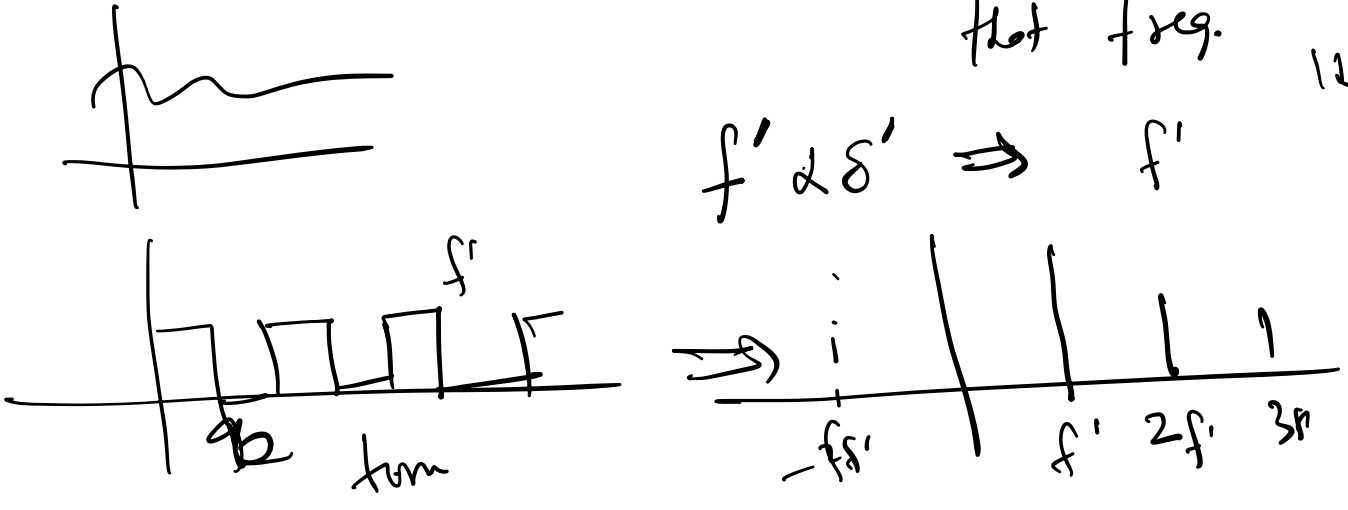
1GHz

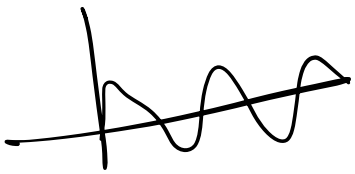
ns

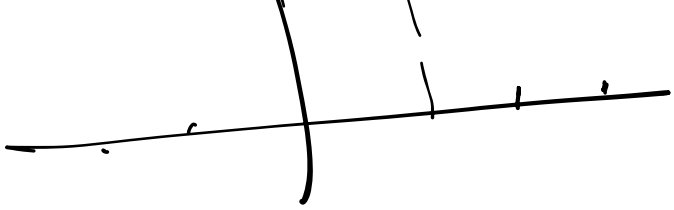
turn the reflector on-off at that freq.

1kHz

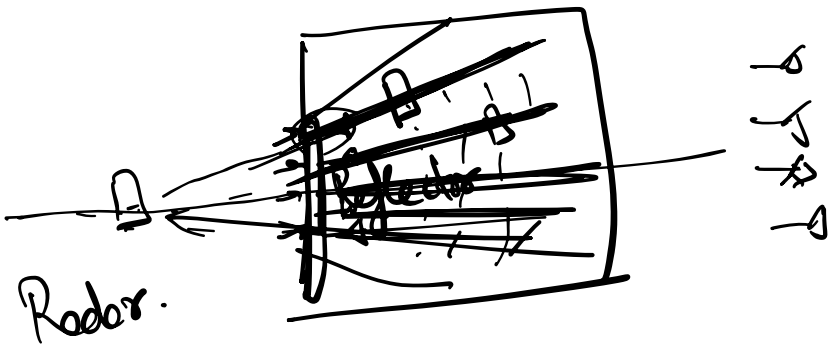
$f' \propto \delta' \Rightarrow f'$







Angle Spoofing

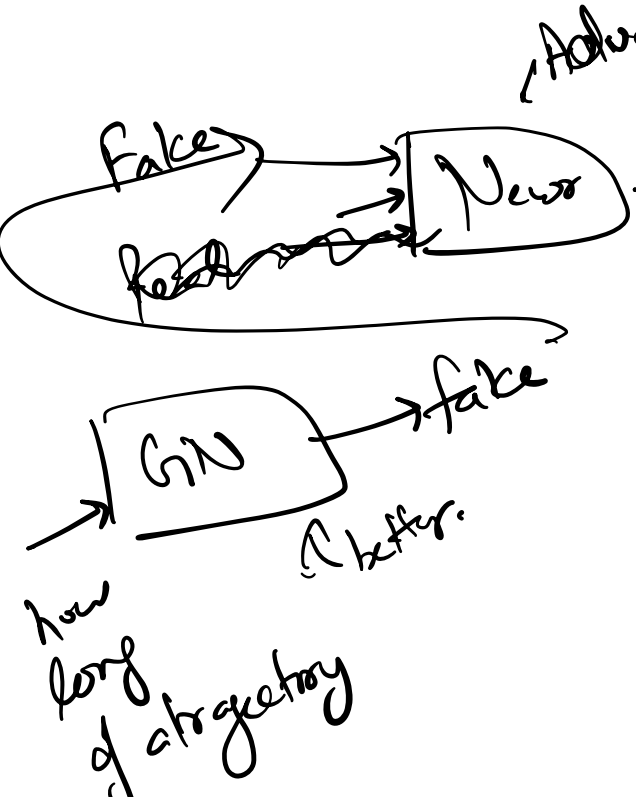


Switch between antennas

Switch across frequen

Distance & Angle ⟹ how do I make it realistic?

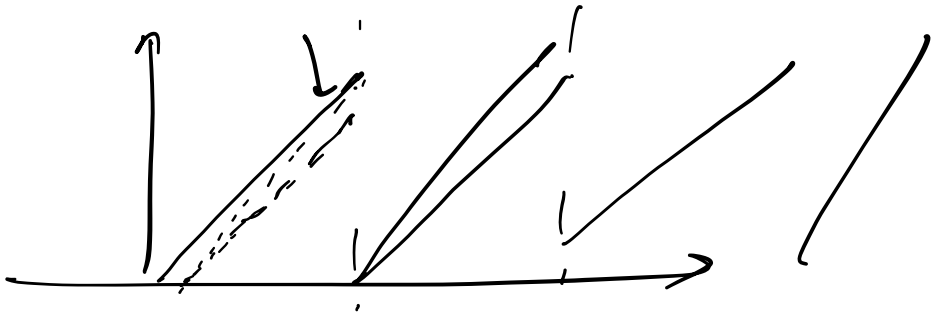
↳ GAN → Generative Adversarial Network.



Conditional GAN

Limitations

- People through walls
  - generate trajectories that do not intersect the wall.
  - input the floor plan into the GAN.
- 2D floor
- FMCW
  - Wi-Fi



RF-Protect Demo