RF is the new LIGHT | Sensing, Localization, and Privacy

Neal Patwari

Sensing and Processing Across Networks
Washington University in St. Louis
span.engineering.wustl.edu

Outline

Outline

RF is the new Light

- Don't turn out the lights
- Analogy: Mental model
- Larger wavelength, penetrate nonconductors
- Generate new ideas

Light Analogy: Astronomy

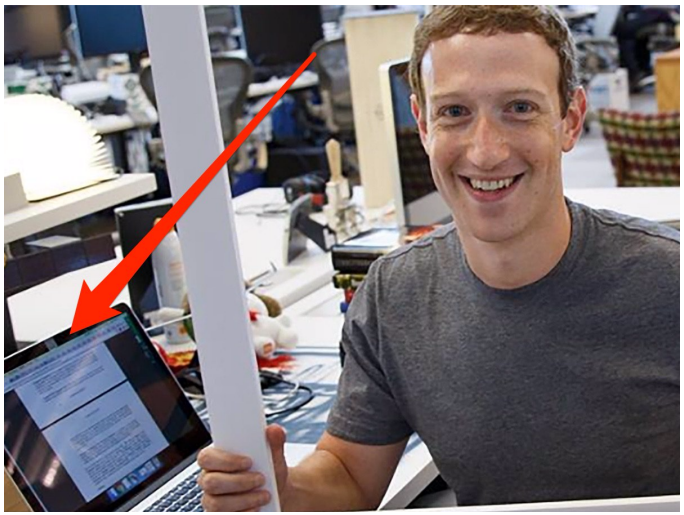
Giovanni Corrado Leone,
https://www.backpacker.com/survival/how-to-navigate-by-the-stars

- Home of Galileo
- Stars, planets: light sources
- Orientation
- Tracking of planets
- Measurement of angle-of-arrival

Topics of Talk

- Localization
  1. Device-free localization
  2. Source localization
3. Sensing
- Privacy
  4. Radio window attack
  5. Remote transceiver attack

RF Attacks on Privacy



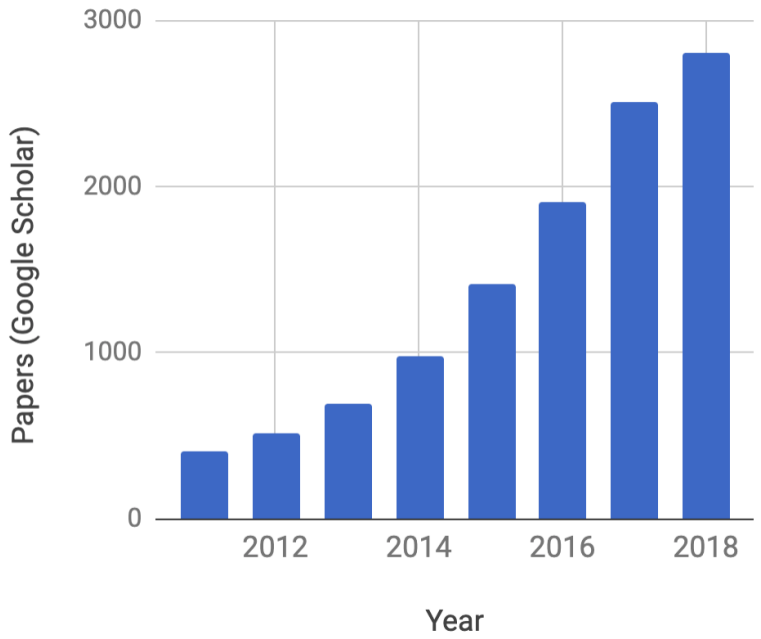
Gizmodo

- Using RF to monitor activities, locations, health
- Privacy issues arise
- No cover for RF
- Every IoT / smart device has it

RF Sensors Measure the Channel

Each new low-cost measurement capability widens the RF sensing application space

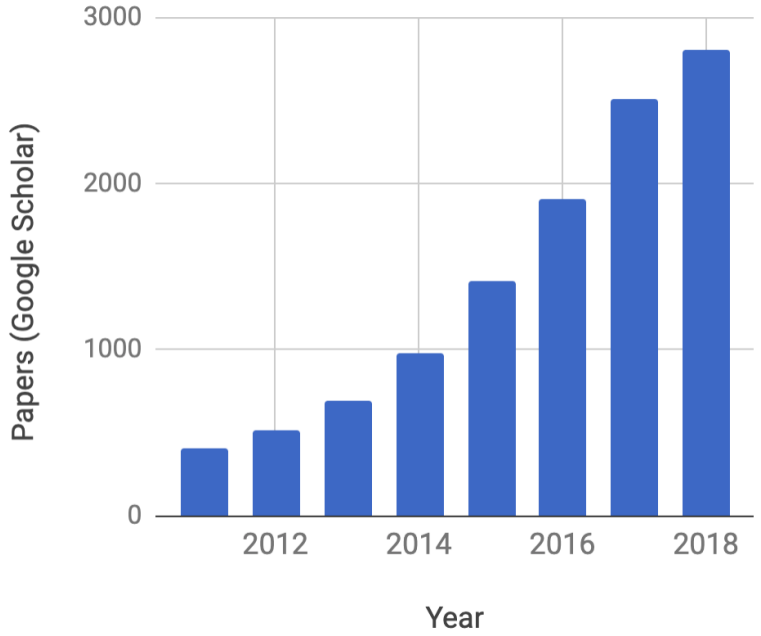
- Received signal strength (RSS)
- Ultra-wideband impulse response (UWB-IR)
- Channel state information (CSI)



Advantage of CSI, UWB-IR

RSS “course-grained”, CSI “fine-grained”: not exactly...

- CSI: high dimensionality is space, frequency diversity
- Both: affected by multipath fading
- Both: Quantized (CSI: 16-20 bits, RSS: 8 bits)
- When RSS has 16 bits: can have identical performance



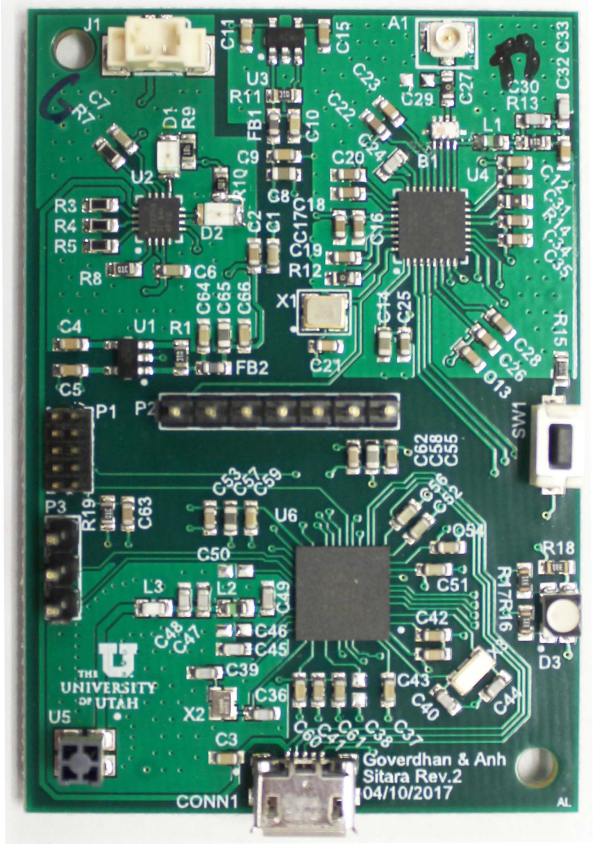
[2] Anh Luong et al., “RSSI step size: 1 dB is not enough!,” ACM HotWireless 2016.

[3] Jie Wang et al., “Device-free wireless sensing: Challenges, opportunities, and applications.” *IEEE Network* 32(2), 2018.

Narrowband RF Sensor

Sitara: Low-cost ($25) narrowband software-defind RF sensor

- <1 GHz transceiver (TI CC1200)
- μC: Cortex M4, 62 MHz (nRF52840)
- Backhaul: BLE 5
- Clock: Fine-grained control (VCTCXO)
- Open hw & sw: `https://github.com/SPAN-WashU/Sitara`



Sitara Applications

- RSS very accurately (0.01 dB error)
- Frequency offset
- Frequency synchronization
- Crowdsourcing device
- Base for UWB (via DW1000 cape)

Topics of Talk

- Localization
  1. Device-free localization
  2. Source localization
3. Sensing
- Privacy
  4. Radio window attack
  5. Remote transceiver attack

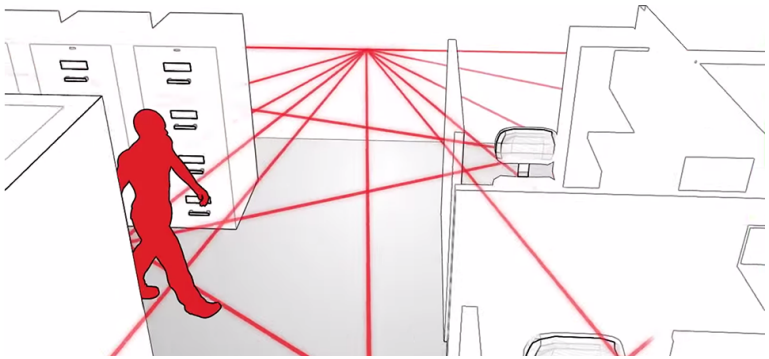
Outline

RF is the new Light: Changes

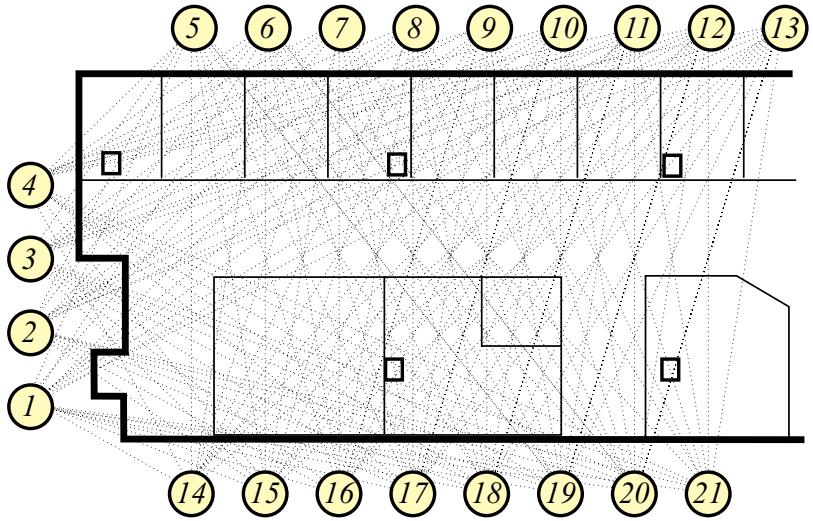
Track based on changes in measured scattered light (RF)

Light

RF



Device-free Localization: Problem Statement



- Radio channel measurements change most due to people in environment near link
- One person / object affects multiple links
- Mesh network of N nodes $\rightarrow \mathcal{O}\left(N^2\right)$ RSS measurements
- Find: Count, locations of people

Radio Tomographic Imaging

We first explored radio tomographic imaging (RTI) for DFL[1]:

- Measure y_l on link l: attenuation vs. empty area, variance, histogram difference
- Presume it is linear combination of presence x_p in pixels p close to link line

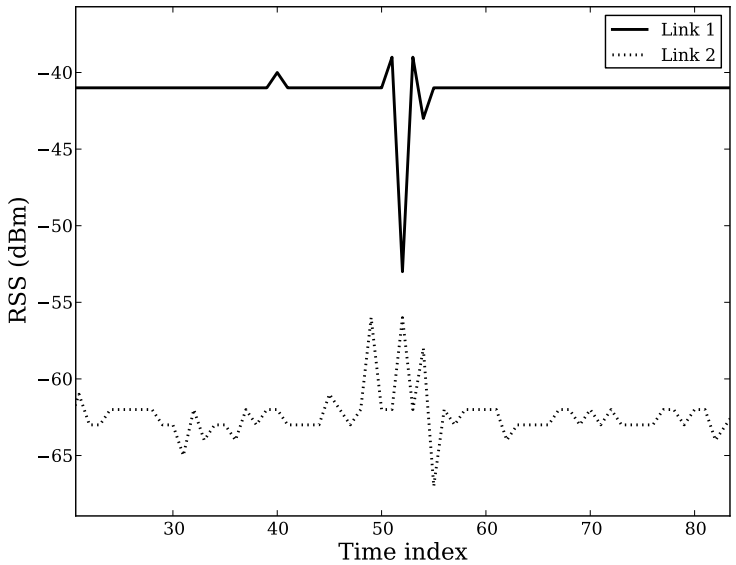
$$\mathbf{y} = W\mathbf{x} + \mathbf{n}$$

- $W = [[w_{l,p}]]_{l,p}$ = weight of pixel p in link l
- Pick regularization method
- Solve inverse problem $\hat{\mathbf{x}} = \Pi\mathbf{y}$

Pros: Fast, real-time algorithm; scales with # people

[1] N. Patwari and P. Agrawal, "Effects of Correlated Shadowing: Connectivity, Localization, and RF Tomography", IPSN 2008.

Challenges of Radio Tomographic Imaging



Two identical links. A person walks, crossing at time 52. Link 1 has high attenuation for one sample, link 2 has high variance and an increase in average RSS over several samples.

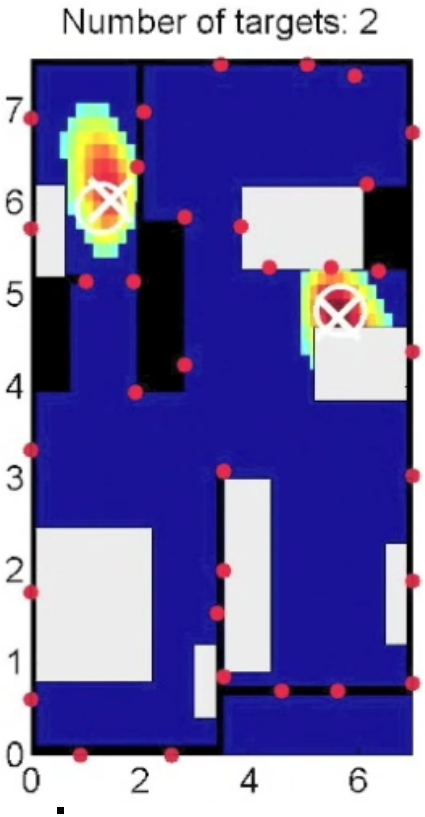
- Area where person impacts link varies
- The $\pm\Delta$ of RSS impact varies

1. Measure multiple frequency ch. / link[2]
2. Estimate params. of model for each link[3]

[2] O. Kaltiokallio, M. Bocca, and N. Patwari, "Follow @grandma: long-term device-free localization for residential monitoring", *SenseApp 2012*.

[3] O. Kaltiokallio, R. Jäntti, N. Patwari, "An adaptive radio tomographic imaging system", *IEEE TVT*, 2017.

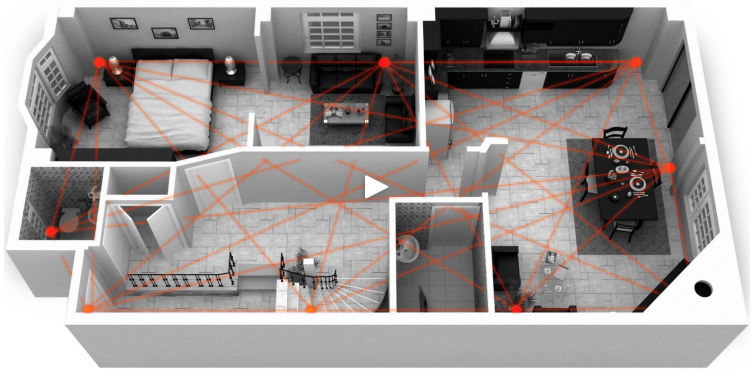
RSS-DFL: Survey of Current Capabilities

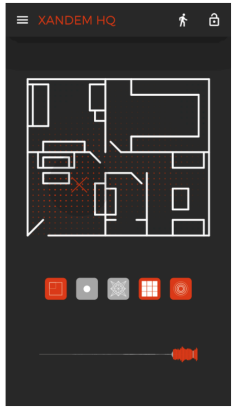


- Error: 7cm - 2m (5-35 nodes in 15-150 m^2)
- Multiple people, building structure, motion vs. change, 2D & 3D, in & outdoors[4]
- Algs: RTI, ML, statistical inversion

[4] N. Patwari, "One decade of sensorless sensing: Wireless networks as human context sensors", IEEE Signal Processing and Wireless Communications (SPAWC) 2015, Plenary Talk Slides

Device-free Localization Products





- Xandem, `xandem.com` (I am affiliated)
- Aura Home
- Origin Wireless
- RSS-based security system / home automation sensor
- Next: embedded in switches, outlets

DFL: Open Topics

- CSI+ML dominates DFL research
- Training gets stale quickly: 2× Error every 6 changes[5]
- Need updates, perhaps from located sources
- Adaptive statistical models for CSI

[5] B. Mager, et al. "Fingerprint-based device-free localization performance in changing environments," IEEE JSAC 33(11), 2015.

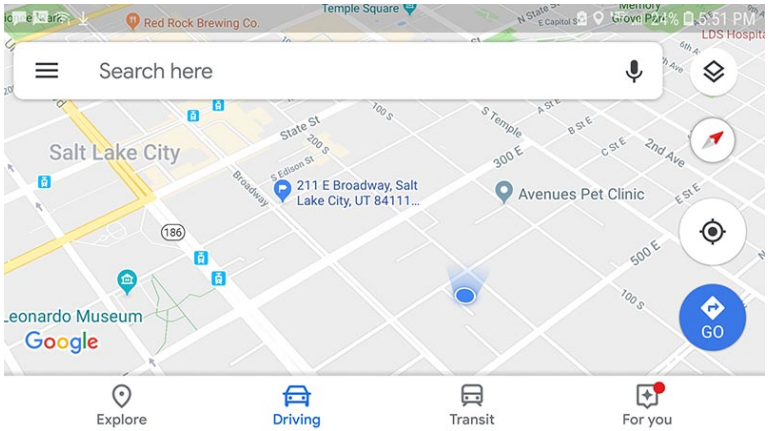
RF is the new Light: Source Localization

Locate sources of light (RF)

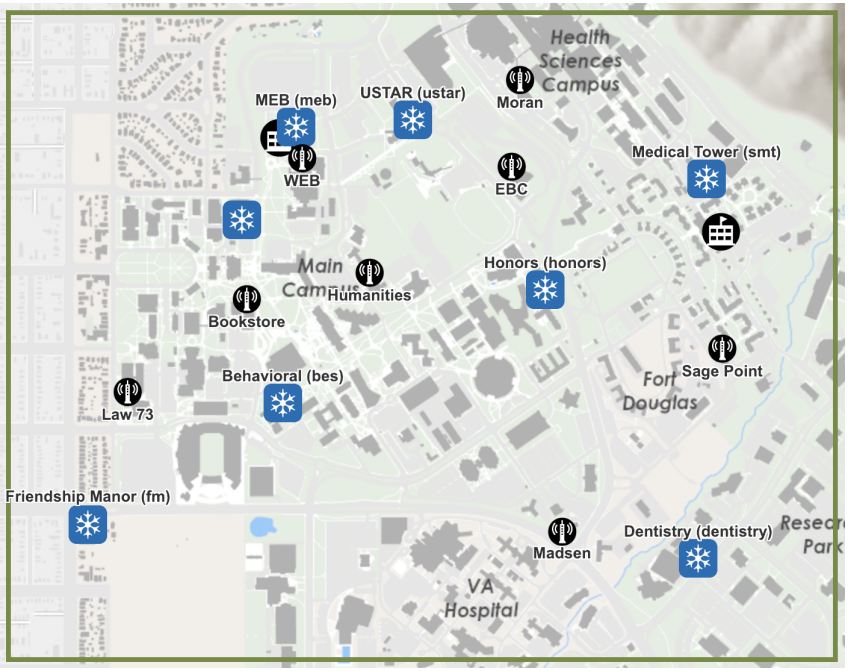
Light

Otto Phokus, flickr.com/photos/jbmac/4737231422

RF



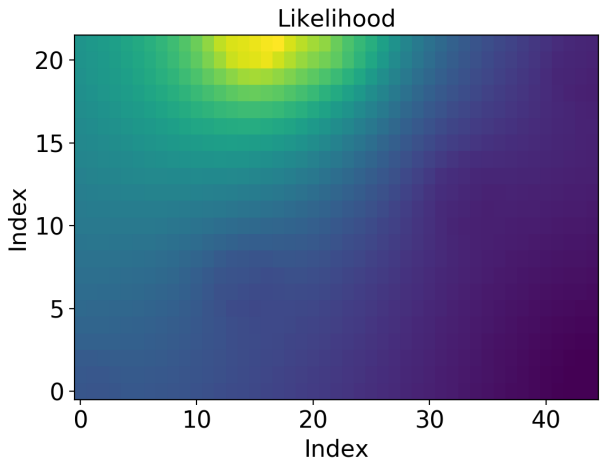
Powder: Open Outdoor SDR Platform

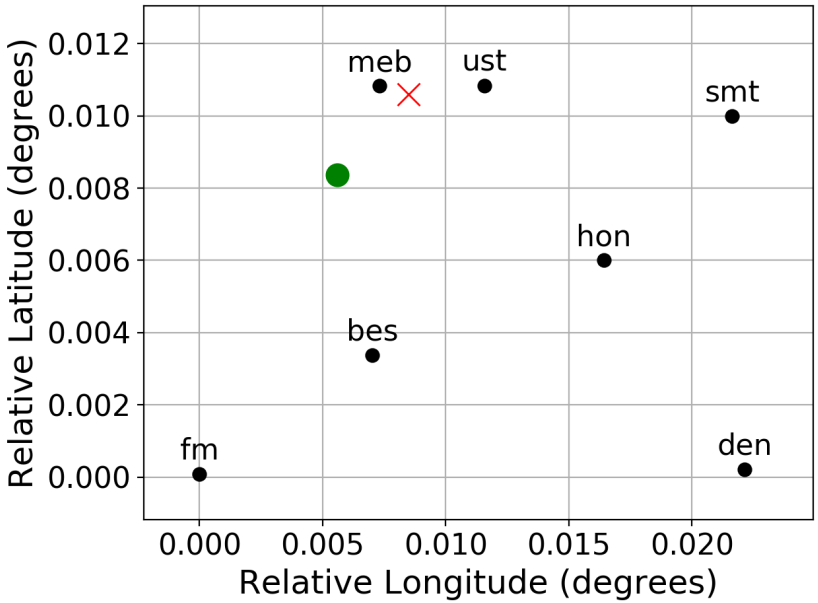


https://powderwireless.net

- In Salt Lake City Utah
- Currently on 8 rooftops, 8 endpoints
- NI X310 and B210s, compute nodes
- Plan to deploy over 14 km^2
- Deploy arbitrary s/w: srsLTE, OAI, GNU Radio

Powder: Localization Research



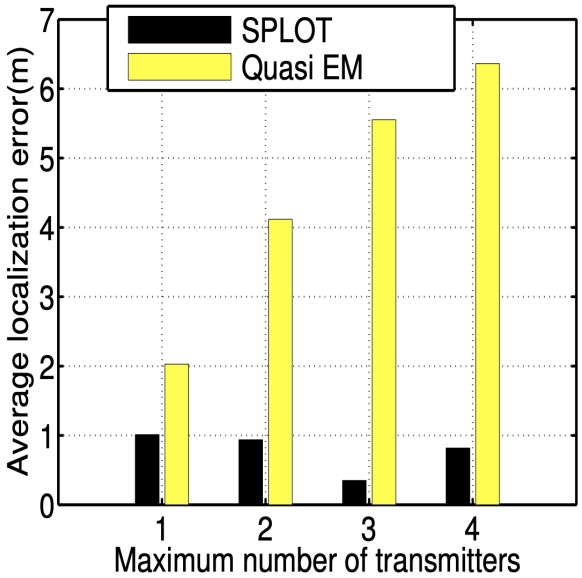


- MWW2019 tutorial, incl. RSS localization
- `gitlab.flux.utah.edu/powderrenewpublic`
- Future: Time synch via SyncE & GPS
- Massive MIMO from Skylark Wireless

Motivation: Source Localization

- Consider dynamic spectrum access for consumers
- Requires collaborative sensing & localization
- Privacy, bandwidth concerns would likely preclude saving, transfer of raw signal samples from consumer devices to cloud
- Thus RSS, Doppler, AOA remain

Simultaneous Source Localization

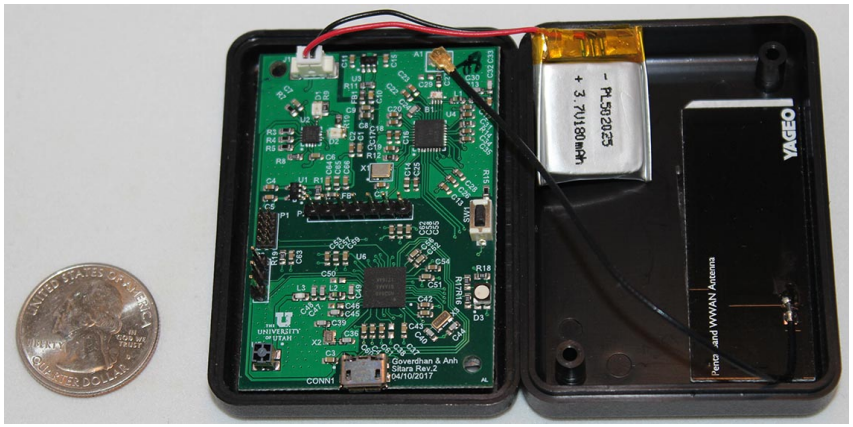


- RSS meast's may include multiple TXs
- Problem: Estimate number, location of TXs
- Our solution: SPLOT[6]
- Outperforms SotA quasi-EM method

[6] M. Khaledi, et al. "Simultaneous power-based localization of transmitters for crowdsourced spectrum monitoring" MobiCom 2017.

PocketSDR: Large Participant Studies

Goal: Enable large (100s) participant research Motivation: Study collaborative sensing at high density w/ actual mobility



- RF spectrum $\overset{CC1200}{\leftrightarrow}$ Sitara $\overset{BLE}{\leftrightarrow}$ Phone $\overset{4G}{\leftrightarrow}$ Server
- Can exchange 52 kSps over BLE 5
- Participant recharges over μUSB
- Otherwise, pocket and forget it

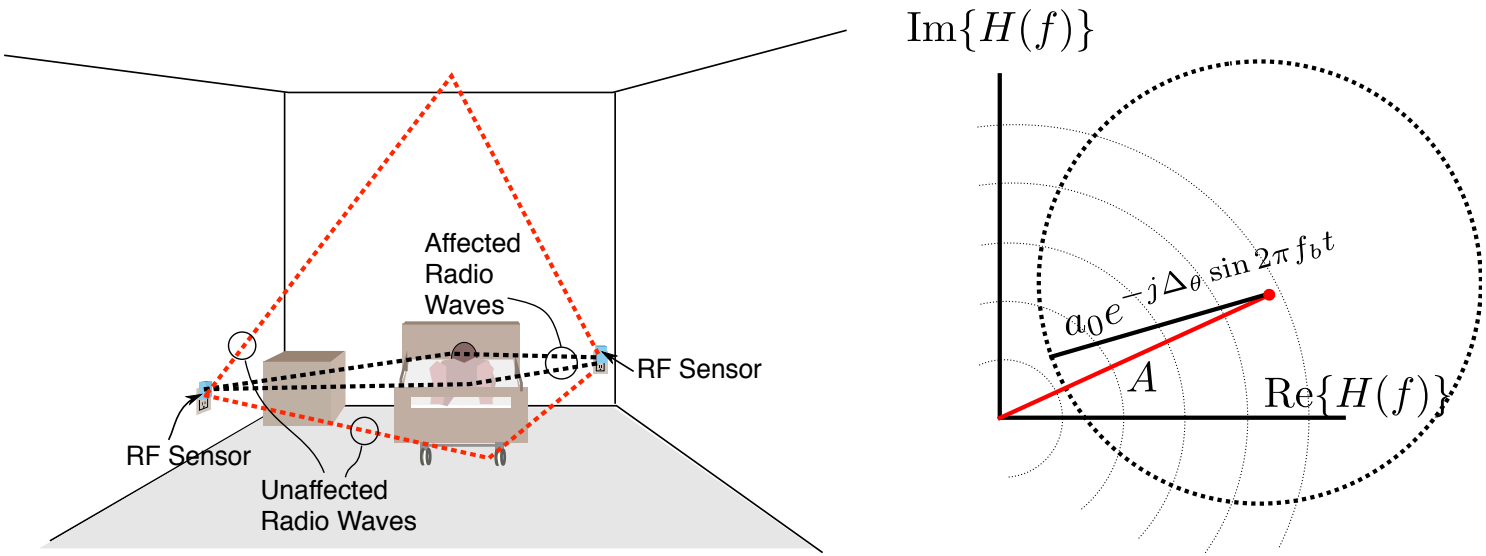
[6] P. Smith, et al. "Sitara: spectrum measurement goes mobile through crowd-sourcing" IEEE MASS 2019.

Outline

Light: Breathing Localization

- We are familiar with how to use light to monitor breathing
- Medical “gold standard”

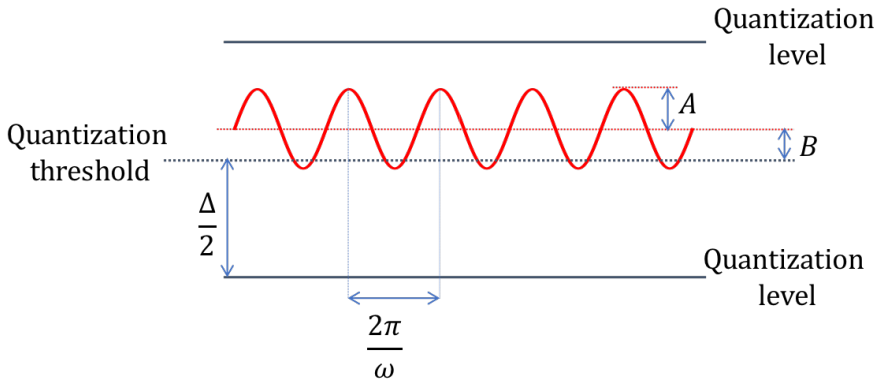
RF-based Breathing Rate Estimation

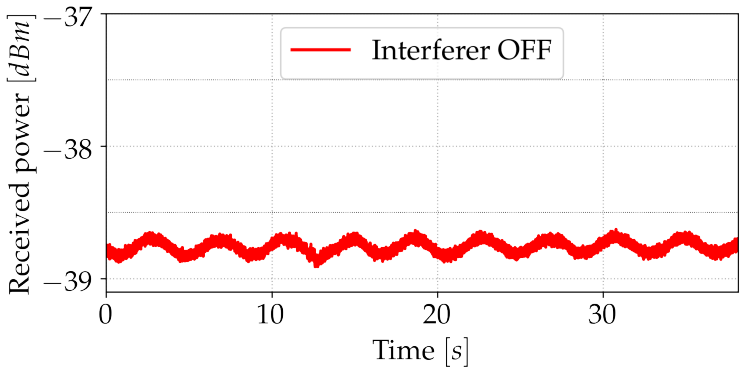


RX sees a phasor sum of affected (black) and not affected (red) paths. A phase change to affected paths changes the RSS (squared magnitude of the sum).

- Related: radar reflectometry for vitals monitoring
- Observation: Breathing *also* changes RSS on some links

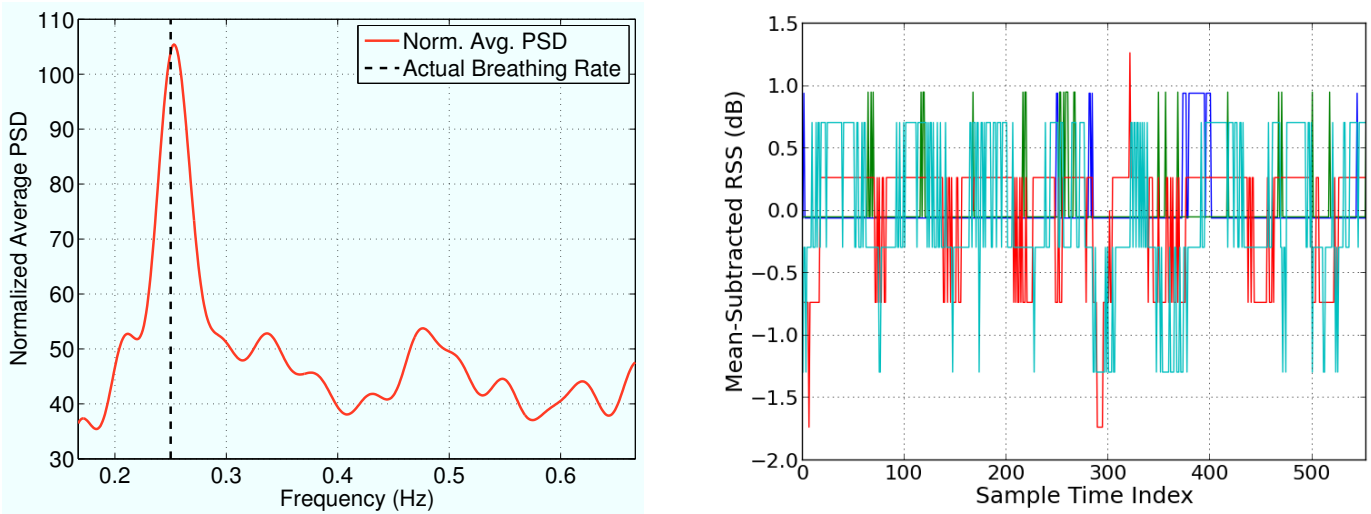
RF-based Breathing Monitoring: Problem





- Typical RSS peak-to-peak change of 0.1-0.2 dB
- Quantization step size: 1 dB
- Many links will not observe breathing-induced changes
- Several solutions

Solution 1: Measure Lots of Links

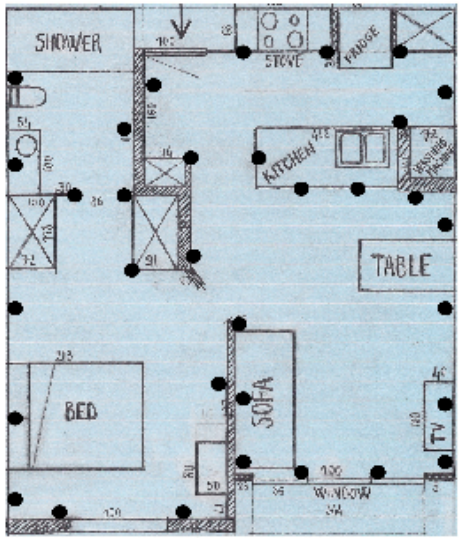


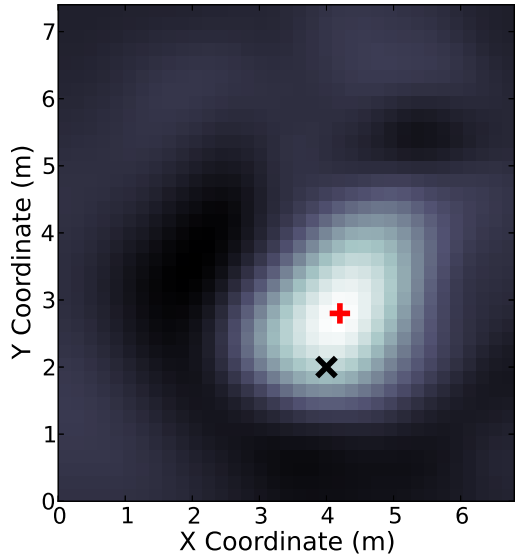
Patient breathing at 0.25 Hz: (Left) Avg. PSD over all links. (Right) RSS vs. time (30 sec duration) for five best links.

- RSS changes in some
- This setup: 20 sensors around patient bed [7]
- Estimator: Peak of avg. PSD (MLE) has 0.4 bpm error

[7] N. Patwari, et al. "Monitoring Breathing via Signal Strength in Wireless Networks", *IEEE Trans. Mobile Computing*, 2014.

Breathing Localization





- Amplitude at breathing rate $\propto$ link - person proximity
- Breathing Tomography: Locate breathing w/ 2 m avg. error[8]

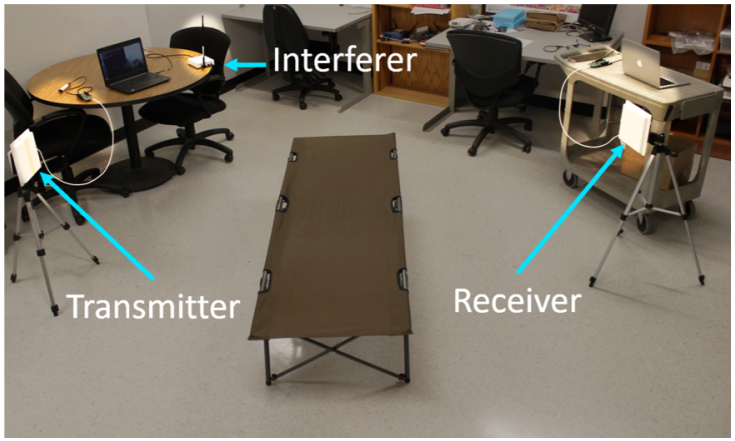
[8] N. Patwari, et al. "Breathfinding: A Wireless Network that Monitors and Locates Breathing in a Home", *IEEE J. Sel. Topics in Signal Processing*, 2013.

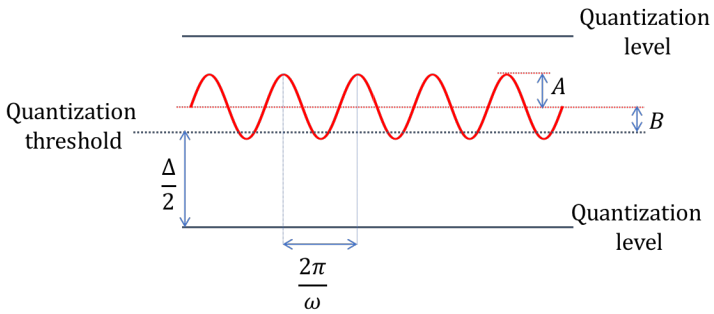
Other Solutions

- Use frequency or spatial diversity
- Use other devices without the (same) quantization problem: CSI, UWB-IR, Sitara. (We compared on 20 patients[9])
- Add *helpful interference* to RSS

[9] P. Hillyard et al., "Comparing respiratory monitoring performance using commercial wireless devices," *ACM Mobicom 2018*.

Breathing Monitoring: Add Noise

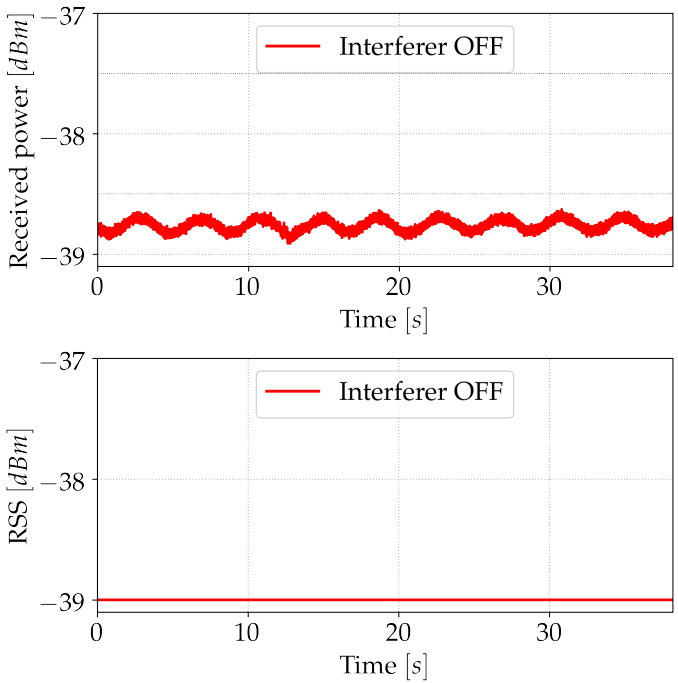


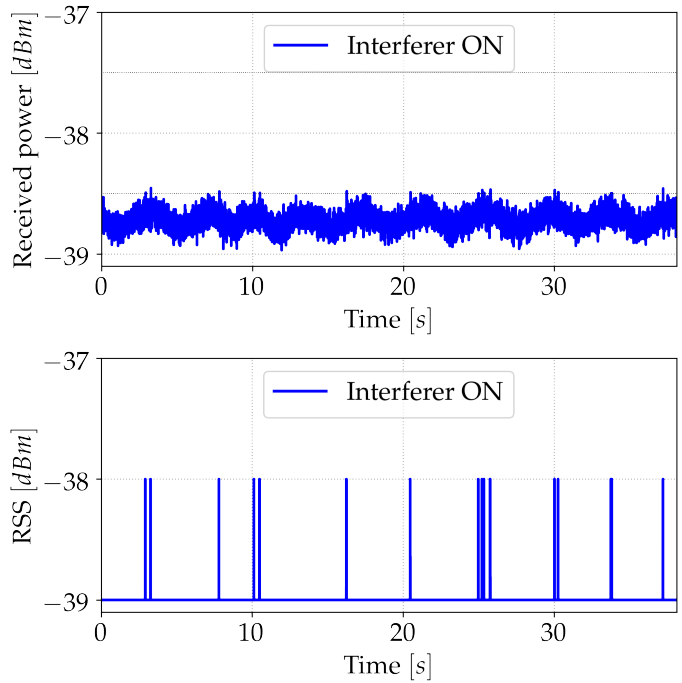


- Solution 3: transmit interference from 3rd device[10]
- Setup: TX 64 square QAM signal, known power
- Increases probability RSS takes two quantized values

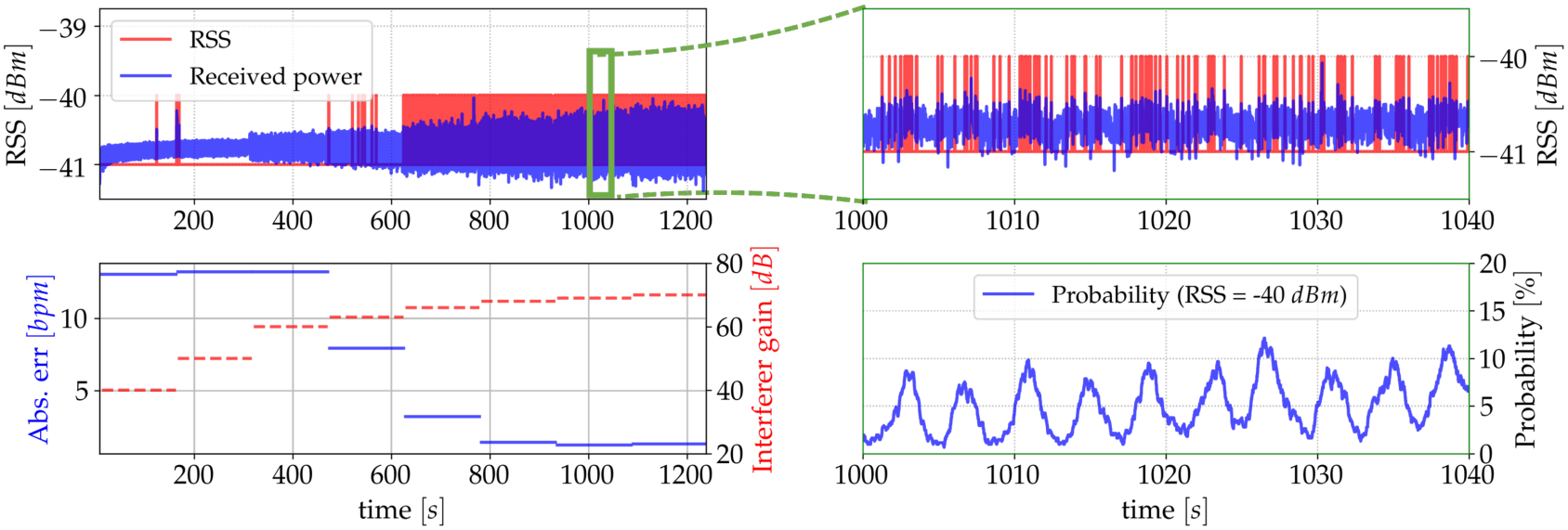
[10] A. S. Abrar, N. Patwari, A. Baset, S. K. Kasera, "Bounding the Ability to Monitor Breathing via Received Signal Strength", in preparation.

Add Noise = Add Robustness



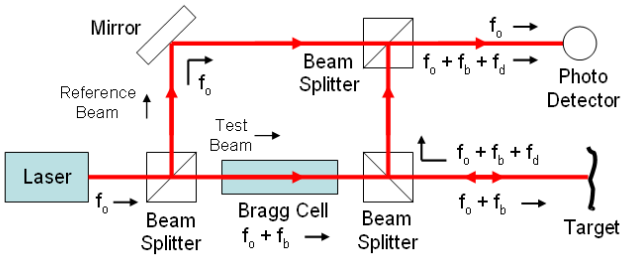


Exp Results: Error vs. Interference Power



Interferer power is increased each 180 sec (- - - -). At high power, abs. err. is reduced, and has a minimum. (RIght) Zoomed in quantized RSS (red) shows increased probability of being = −40 dBm once per period.

Audio Vibration Monitoring



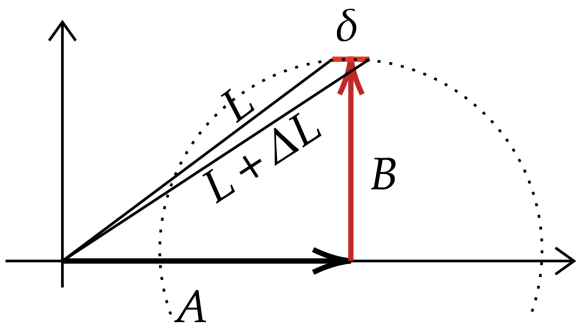
- Wikipedia: *Laser Doppler Vibrometer*
- Used by spies to eavesdrop sound vibrations on windows
- RF would go through walls

Audio Vibration Monitoring

- WiFi CSI can measure audio[11]
- CSI not needed; narrowband RSS contains audio vibrations

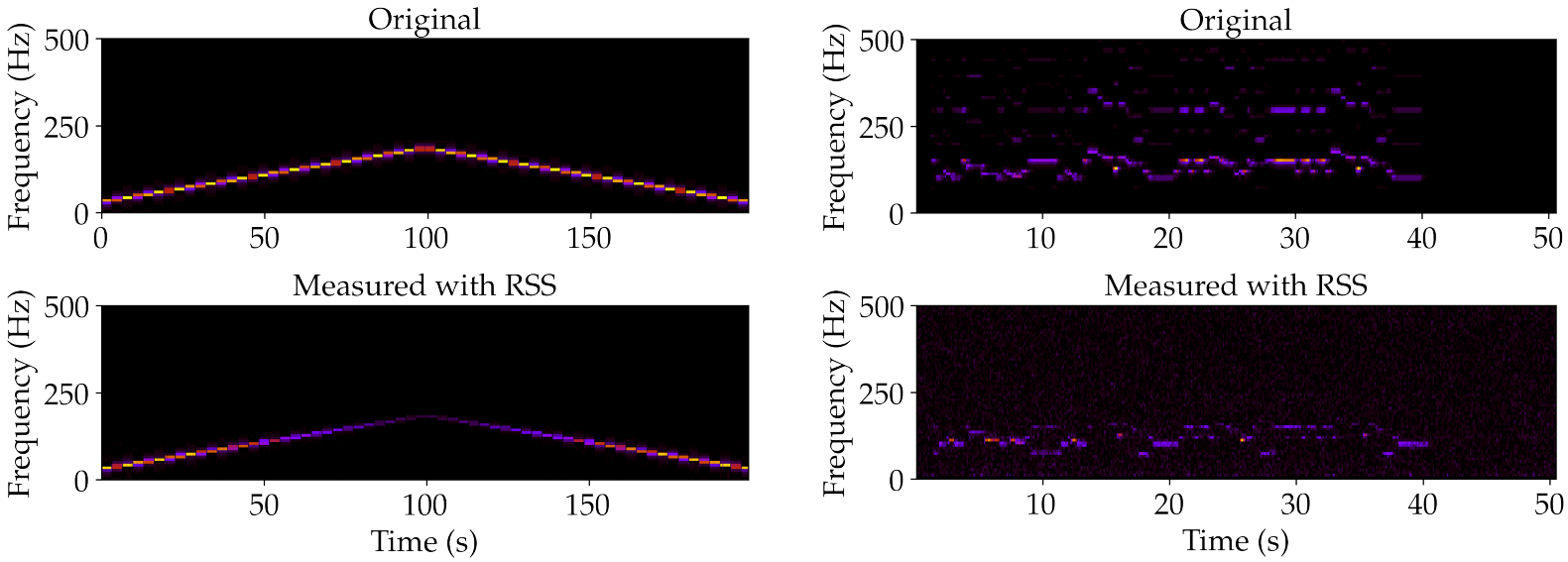
[11] "Teng Wei, et al. "Acoustic eavesdropping through wireless vibrometry." MobiCom 2015.

Audio Vibration Monitoring



- A is static (unaffected) signal
- B is signal affected by vibration
- Vibration ampl. $\Delta z \rightarrow$ phase change $\delta \rightarrow$ Power change
- In dB, change $\approx \frac{20\pi}{\ln 10} \frac{\Delta z}{\lambda}$
- $\Delta z = 0.2$ mm and 900 MHz results in 0.017 dB power change
- But, Δz decreases as audio freq increases

Audio Vibration Monitoring Results



- Google Home plays mp4 tracks
- Left: sweep; Right: Harry Potter theme
- 1 Sitara TX on table, 1 RX elsewhere
- Audio below $\approx$ 200 Hz is well observed

Outline

Security of IoT Devices

- Mirai exploited 600k IoT devices (webcams, routers) [12]
- IoT device hacking: prevalent, growing problem

[12] "Inside the infamous Mirai IoT Botnet: A Retrospective Analysis", Cloudfare, 14 Dec 2017.

Breathing Monitoring: Privacy Issue

"Amazon's Echo Spot is a sneaky way to get a camera into your bedroom", The Verge, 28 Sep 2017.

- Hesitation to place a video camera, mic in private spaces
- People know what a hacker might access from video
- Most don't know a hacker could access from a transceiver: your vital signs, activity, even audio
- Our focus: attack to estimate frequency and amplitude of a sinusoid

Attack on Breathing Privacy

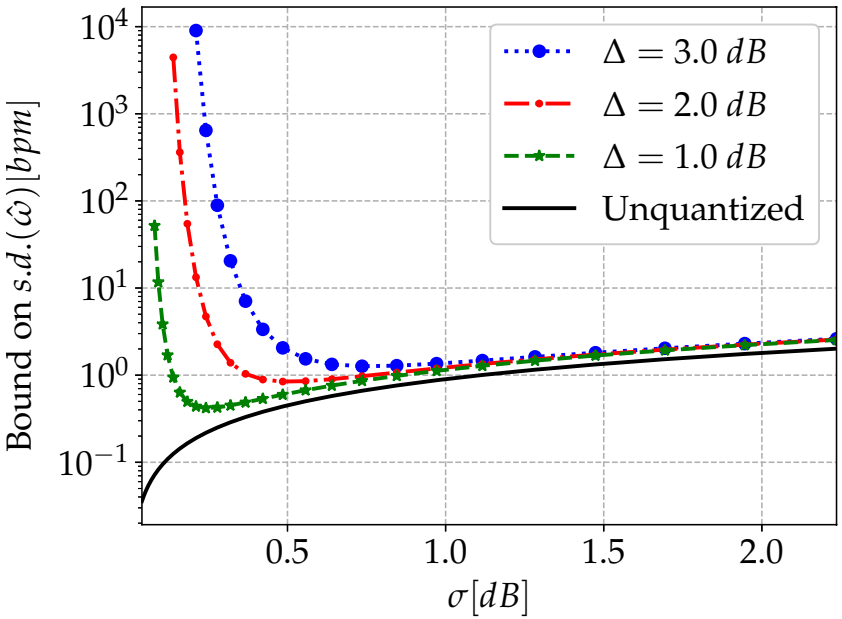
Assume a hacker can run s/w on transceivers in your home, to TX and access RSS $y[k]$:

$$y[k] = Q\left\{A\cos(\omega k/f_s + \phi) + B + \nu[k]\right\},$$

quantizer $Q\{\}$, amplitude A, phase ϕ, time k, and offset B, in noise $\nu[k]$, at max sample rate f_s possible from transceiver. No assumed computation, alg limits.

What is this attacker's ability to est. breathing rate?

Attack on Breathing Privacy: Our Approach

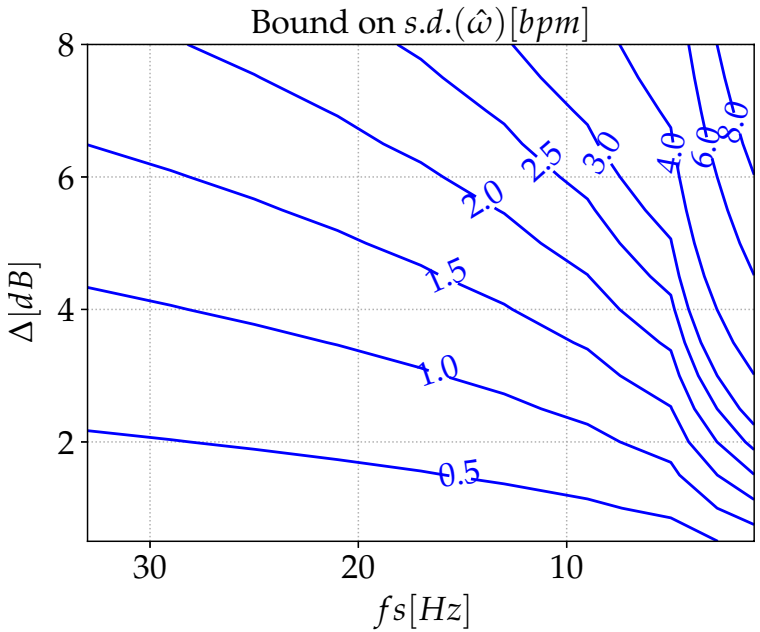


- Cramér-Rao lower bound (CRLB) on variance of unbiased est. of rate ω
- Assume noise is iid $\mathcal{N}\left(0, \sigma^2\right)$
- Offset from quantization threshold B is uniform

- Bound: fcn. of Δ (step size), f_s, σ[13]
- Assume best case for attacker: optimal interference power

[13] A. S. Abrar, N. Patwari, A. Baset, S. K. Kasera, "Bounding the Ability to Monitor Breathing via Received Signal Strength", (in preparation).

Implications of Our Approach



- CRLB: std. dev. $(\hat{\omega})$ only guaranteed high when RSS step size is high (6 dB) & RSS update frequency is low (2 Hz)
- Bad news for transceivers for mobile (fading) channels (e.g., power control)
- Future work: Adaptive RSS schemes in h/w that reduce rate, accuracy in static channels

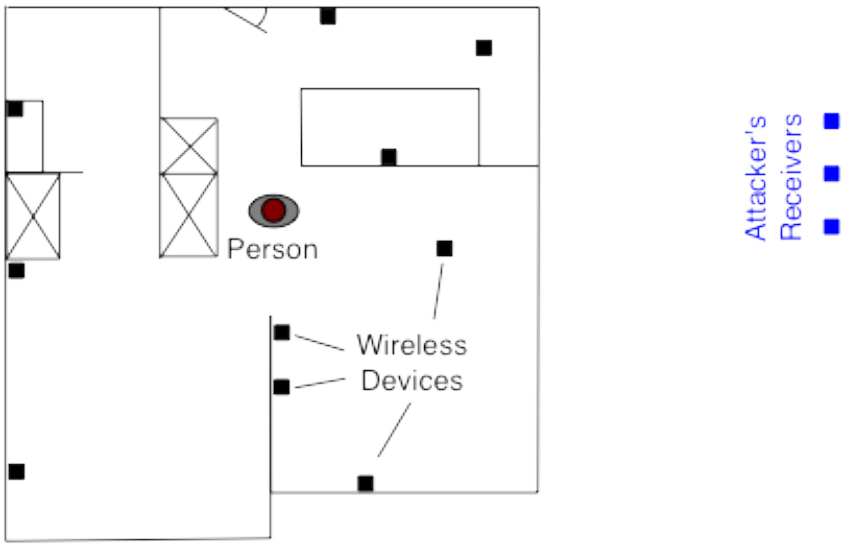
Radio Window Attack: Introduction

Philip Johnson Glass House, `https://youtu.be/eOzimeZDFKo`

- If you live in a glass house...
- You understand what light bulbs do to your privacy
- Non-metal walls are “glass” to radio waves
- Wireless device = RF “bulbs”

Radio Window Attack Model

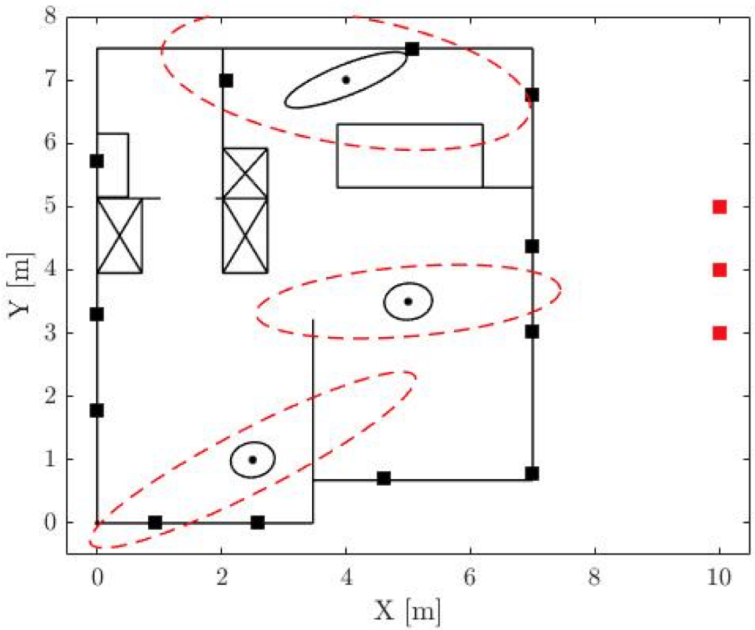
Wireless devices where people's locations, activities should not be revealed (embassy, base, corporate office). Attacker:



Example layout of wireless devices ■ in a home and attacker's receivers ■

- can't enter area
- can place receivers outside
- doesn't transmit (avoid detection)
- can't decode/decrypt data
- can measure channel when devices TX
- may or may not know device locations

Radio Window Attack Analysis

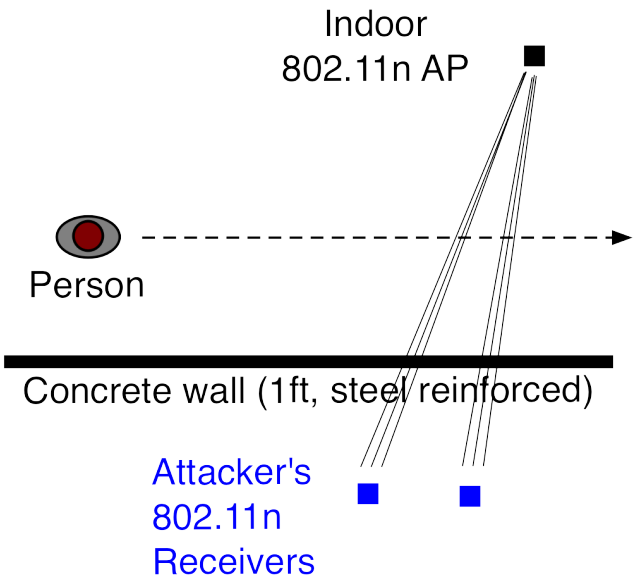


Example: Lower bound on 3σ covariance ellipse (- - - -) for localization of person at three actual locations ● with attacker's receivers ■.

- How well can the attacker know a person's location?
- Measurements are made at different times
- Attacker would *track* person using motion model
- Approach: Find lower bound on RMSE (van Trees bound)[14]

[14] O. Kaltiokallio, A. S. Abrar, N. Patwari, "RMSE bounds for RSS-based device-free localization", (in preparation).

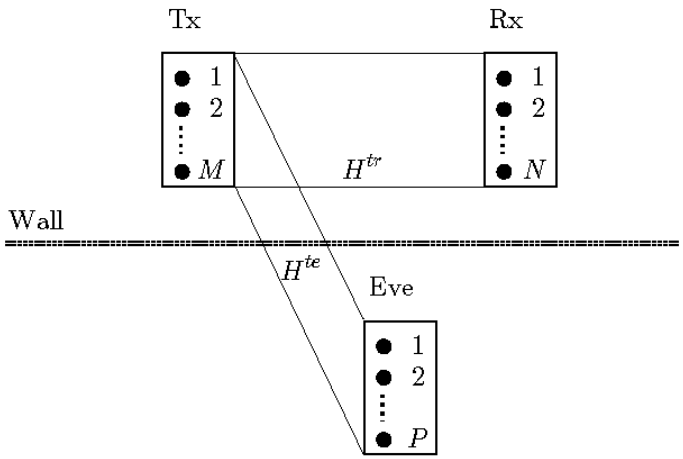
Radio Window Attack Idea



Experiment: WiFi AP in building (■), two WiFi Intel NUCs (■) outside each measure RSS on 3 antennas.

- Fool an attacker! Change TX power
- Either (a) randomly uncorrelated (b) fake line crossing
- Problem: Multiple (6) RX antennas observe mostly identical power change
- Attacker can remove median RSS change

Radio Window Attack Current Work



MIMO radio window eavesdropper can be confused by MIMO transmitter with M > P.

1. Assume legit AP has more antennas than attacker. Randomly alter precoding matrix to confuse the attacker
2. Pseudorandom frequency hopping across channels to avoid eavesdropper
3. Prototype AP which resists a radio window attack

Outline

Conclusion

- Transceiver interface: the light bulb / sensor of RF
- New transceivers provide new capabilities
- Sensing capabilities open up new attacks, we can quantify and address
- Localization solutions will use both RF and light
- We can gain intuition in RF, and imagine future technologies, by analogy to light