RF is the new Light

Sensing, Localization, and Privacy

Neal Patwari

S P A N

Sensing and Processing Across Networks
Washington University in St. Louis
span.engineering.wustl.edu
RF is the new Light
RF is the new Light

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

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

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

Neal Patwari
Washington University in St. Louis

RF is the new Light
Topics of Talk

- Localization
  1. Device-free localization
  2. Source localization

- Sensing

- Privacy
  4. Radio window attack
  5. Remote transceiver attack
RF Attacks on Privacy

- 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

Narrowband RF Sensor

Sitara: Low-cost ($25) narrowband software-defined 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

- **Sensing**

- **Privacy**
  4. Radio window attack
  5. Remote transceiver attack
RF is the new Light: Changes

Track based on changes in measured scattered light (RF)
Radio channel measurements change most due to people in environment near link
One person / object affects multiple links
Mesh network of \( N \) nodes \( \rightarrow O(N^2) \) RSS measurements
Find: Count, locations of people

Neal Patwari
Washington University in St. Louis

RF is the new Light
Radio Tomographic Imaging

We first explored radio tomographic imaging (RTI) for DFL\textsuperscript{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
  \[ y = Wx + n \]
  \[ W = \left[ [w_{l,p}] \right]_{l,p} = \text{weight of pixel } p \text{ in link } l \]
  - Pick regularization method
  - Solve inverse problem $\hat{x} = \Pi y$

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

\textsuperscript{1} N. Patwari and P. Agrawal, “Effects of Correlated Shadowing: Connectivity, Localization, and RF Tomography”, IPSN 2008.

Neal Patwari
Washington University in St. Louis
RF is the new Light
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. Estimate params. of model for each link

---


RSS-DFL: Survey of Current Capabilities

- Error: 7cm - 2m (5-35 nodes in 15-150 m²)
- Multiple people, building structure, motion vs. change, 2D & 3D, in & outdoors
- Algs: RTI, ML, statistical inversion

---

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

Neal Patwari
Washington University in St. Louis

RF is the new Light
DFL: Open Topics

- CSI+ML dominates DFL research
- Training gets stale quickly: $2 \times$ Error every 6 changes\textsuperscript{5}
- Need updates, perhaps from located sources
- Adaptive statistical models for CSI

RF is the new Light: Source Localization

Locate sources of light (RF)

Neal Patwari, Washington University in St. Louis

RF is the new Light
Powder: Open Outdoor SDR Platform

- 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](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 measurements may include multiple TXs
- Problem: Estimate number, location of TXs
- Our solution: SPLOT\(^6\)
- Outperforms SotA quasi-EM method

PocketSDR: Large Participant Studies

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

- RF spectrum $\leftrightarrow$ Sitara $\leftrightarrow$ Phone $\leftrightarrow$ Server
- Can exchange 52 kSps over BLE 5
- Participant recharges over $\mu$USB
- Otherwise, pocket and forget it

---

Outline

1. Intro
2. Localization
3. Sensing
4. Privacy
5. Conclusion
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

Breathing Localization

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

---

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

---

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 $\approx -40$ 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\(^\text{11}\)
- CSI not needed; narrowband RSS contains audio vibrations

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 $\approx \frac{20\pi}{\ln10} \frac{\Delta z}{\lambda}$
- $\Delta z = 0.2$ mm and 900 MHz results in 0.017 dB power change
- But, $\Delta z$ 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

1. Intro
2. Localization
3. Sensing
4. Privacy
5. Conclusion

Neal Patwari
Washington University in St. Louis

RF is the new Light
Security of IoT Devices

- Mirai exploited 600k IoT devices (webcams, routers) \(^\text{12}\)
- IoT device hacking: prevalent, growing problem

Breathing Monitoring: Privacy Issue

- 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

“Amazon’s Echo Spot is a sneaky way to get a camera into your bedroom”, The Verge, 28 Sep 2017.
Attack on Breathing Privacy

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

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

quantizer $Q\{}$, amplitude $A$, phase $\phi$, 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 $\omega$
- Assume noise is iid $\mathcal{N}(0, \sigma^2)$
- Offset from quantization threshold $B$ is uniform

Bound: fcn. of $\Delta$ (step size), $f_s$, $\sigma$

Assume best case for attacker: optimal interference power

---

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:

- 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

Example layout of wireless devices in a home and attacker’s receivers
Radio Window Attack Analysis

- 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)\(^\text{14}\)

Radio Window Attack Idea

- 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

Experiment: WiFi AP in building (●), two WiFi Intel NUCs (●) outside each measure RSS on 3 antennas.
Radio Window Attack Current Work

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.

MIMO radio window eavesdropper can be confused by MIMO transmitter with $M > P$. 
<table>
<thead>
<tr>
<th>#</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Intro</td>
</tr>
<tr>
<td>2</td>
<td>Localization</td>
</tr>
<tr>
<td>3</td>
<td>Sensing</td>
</tr>
<tr>
<td>4</td>
<td>Privacy</td>
</tr>
<tr>
<td>5</td>
<td>Conclusion</td>
</tr>
</tbody>
</table>
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