“Should I Work on Wireless Networks?”

Kyle Jamieson
Networks Research Group
Department of Computer Science
University College London

We gratefully acknowledge funding from the European Research Council “Ideas” Program and Proof of Concept grant
Some things are well understood...

Q: What’s the capacity of a point-to-point link?

• Before Shannon:
The only way to make $P(\text{error})$ arbitrarily small is to reduce the rate of communication.

• Shannon:
No! Up to some rate $C$, coding can make $P(\text{error})$ arbitrary small!

$$C = B \log_2 (1 + \text{SNR}) \, \text{bits/second}$$
...others aren’t understood well at all!

Q: What’s the capacity of a wireless network?

A: (information theory) ...
A: (CS community) let’s build a better medium access protocol!
The growing wireless toolbox

Link Layer and above
• MAC protocols
• Routing and handoff

Physical Layer
• Successive Interference Cancellation
• Transmit beamforming
• Receive beamforming
• MIMO spatial multiplexing
• Space-time coding
• Amplify-and-forward
Wireless network system structure

- Optimization across layers
- Optimization across the network, at each layer
Heuristic #1: Solve it better

Given a solved problem, ask yourself:

Can I take a fresh look at solving this problem?

Is there anything about the way the researchers solve this problem that I perhaps think can be improved, or even outright disagree with?
Embrace collisions in RF backscatter networks

- “Efficient and reliable low-power backscatter networks,” Wang et al., SIGCOMM 2012
Software-defined radio opens up the network to innovation

More on-board processing ➔

Faster bus to PC

- Ettus Research USRP1
- Ettus Research USRP2
- Rice WARP v2
- Rice WARP v3
- MSR Asia Sora
Heuristic #3: Take the next step

Given a solved problem, ask yourself:

What’s the next step in realizing the solution, and are there any interesting challenges in doing so?
SoftPHY: Change perspective from packets to symbols

- **Cross-layer** information flow from PHY up
- **Extract use** from high-confidence parts of packets

- Maintain layered architecture (PHY-independent use)
Partial Packet-ARQ

“Partial Packet Recovery,” Jamieson and Balakrishnan, SIGCOMM ‘07

Data bits

1\textsuperscript{st} pkt., 1\textsuperscript{st} tx.

1\textsuperscript{st} pkt., 2\textsuperscript{nd} tx.
2\textsuperscript{nd} pkt., 1\textsuperscript{st} tx.

1\textsuperscript{st} pkt., 3\textsuperscript{rd} tx.
3\textsuperscript{rd} pkt., 1\textsuperscript{st} tx.

“Good” data bits
“Bad” data bits
Checksum (32-bit)
Maranello: Practical Partial Packet Recovery

“Maranello: Practical Partial Packet Recovery for 802.11,” Han et al., NSDI ‘11

Correct

802.11 & Maranello

Corrupt

802.11

Corrupt

Maranello
To take away...

Great, you’ve decided to go into wireless networks!

TODO:
1. Solve it better
2. Hack on new hardware
3. Take the next step
4. Solve a new problem
ArrayTrack: Exploiting Angle-of-Arrival for Accurate and Responsive Indoor Location

Kyle Jamieson with Jie Xiong
Department of Computer Science
University College London

We gratefully acknowledge funding from the European Research Council “Ideas” Program and Proof of Concept grant
Mobile needs a good *indoor* location service

Augmented reality

Product information in *retail stores and supermarkets*

*Location-based wireless security*

*Location-based bandwidth allocation*

All benefit from a highly *accurate* (centimeter-level) and *responsive* (< one second latency) *indoor* location service
Indoor location systems today

- **Map- and radio modeling-based approaches:** RADAR [Bahl+00]
  - Require calibration to build signal strength map
  - RF propagation model relates signal strength, distance
  - Augmented with probabilistic models: Horus [Youssef +05] (**60 cm accuracy**)
  - Crowdsourcing calibration: EZ [Chintalapudi+10]

- **Radio modeling-based approaches**
  - No calibration needed, but accuracy suffers
  - 3 m accuracy [Lim+06], 5.4 m accuracy [Gwon+04]

- **Vision-based approaches**
  - **Highly accurate** (≈ 20 cm) [Hile+08] but computationally intensive
  - Light conditions aren’t always ideal, humans are humans
Challenge: Tightly-packed multipath reflections

Outdoor multipath

Indoor multipath

Signal strength (dBm)

Direct path

Multipath reflections

Normalized signal strength

Direct path

Multipath reflections
Two observations about WiFi access points

1. Ever-increasing number of antennas for MIMO, SDMA

2. High WiFi access point density: usually many nearby
   - UCL Department of CS
   - Client at a random location sends a packet
   - How many APs overhear it?
ArrayTrack: High-level view

- Client sends a single packet over the air
- Each access point (AP) computes the **physical angles-of-arrival** of a client’s transmission: a *pseudospectrum*
- Aggregate pseudospectra at backend server for location
Phased antenna array: Principle of operation

Array steering vector \( \mathbf{a}(\theta) = \begin{bmatrix} 1 \\ e^{j\pi\Delta \cos \theta} \end{bmatrix} \)

\[ \frac{\lambda}{2} \sin \theta \]
Generalizing to many antennas

• Input: complex baseband signals $x_1, x_2, x_3$ from antennas 1, 2, and 3, respectively

• Examine array correlation matrix:

$$R_{xx} = E \begin{bmatrix} x_1^* x_1 & x_1^* x_2 & x_1^* x_3 \\ x_2^* x_1 & x_2^* x_2 & x_2^* x_3 \\ x_3^* x_1 & x_3^* x_2 & x_3^* x_3 \end{bmatrix}$$

• Expectation is a time-average of the baseband signals

• Need just $\approx 100$ samples ($\approx 2 \mu s$) from an 802.11 packet
  - 802.11g ERP-OFDM preamble = 20 $\mu$s
MUSIC: Geometric interpretation
(Three antennas, two signals)

- **MUSIC** algorithm [Schmidt ‘79] and variants [Shan ‘85] analyze the eigenstructure of $\mathbf{R}_{xx}$

[Adapted from Schmidt, “Multiple Emitter Location and Signal Parameter Estimation”]
Challenge: Multipath propagation

- Multipath is a challenge in **two** distinct ways:

  1. MUSIC takes time-averages, gets confused when signals are *coherent*
Solution (1): Spatial smoothing

• Well-known technique [Shan\textsuperscript{+}85] to average across spatially diverse groups of antennas:

• Tradeoff: Fewer effective number of antennas
Challenge: Multipath propagation

- Multipath is a challenge in **two** distinct ways:

  1. MUSIC takes time-averages, gets confused when signals are coherent

  2. Obstacles may block the direct line of sight
Multipath fools naïve approach 18% of the time

Pick the maximum peak

Ground-truth angle (degrees)

Estimated angle (degrees)
Combining bearing likelihoods for a location likelihood at the backend server

- **Given** $N$ AP bearing likelihoods $P_1(\theta_1(x))$, $P_2(\theta_2(x))$, ..., $P_N(\theta_N(x))$

1. **Compute** location likelihood $P(x)$ for a given location $x$:

   $$P(x) = \prod_{l=1}^{N} P_l(\theta_l(x))$$

   $$= \sum_{l=1}^{N} \log P_l(\theta_l(x))$$

2. **Search** for most likely location with sampling and hill climbing
Sampling and gradient search
Additional APs can *worsen* the location estimate.

Figure 6: Heat maps showing the location likelihood of client A in Figure 4 with different numbers of APs computing its location. We denote the ground truth location of client A in each heat map with a small dot.

5. RELATED WORK

The most widely used RF-based approach for location uses average received signal strength (RSS) from packets, usually measured in units of whole decibels. While readily available from commodity WiFi hardware at this granularity, the resulting RSS measurements are very coarse compared to the physical-layer information we use in ArrayTrack, and so incur an amount of quantization error, especially when few readings are present.

There are two main lines of work using RSS; the first, pioneered by RADAR [3, 4] builds “maps” of signal strength to one or more access points, achieving an accuracy on the order of meters [18, 22]. Later systems such as Horus [32] use probabilistic techniques to improve localization accuracy to an average of 60 centimeters when an average of six access points are within range of every location in the wireless LAN converge area, but require large amounts of manual calibration. While some work has attempted to reduce the calibration overhead [9], mapping generally requires significant effort. Other map-based work has proposed using overheard GSM signals from nearby towers [25], or dense deployments of desktop clients [2]. In contrast to map-based techniques, the experimental results we show here achieve better location accuracy from very small numbers of detected packets, with no calibration steps required.

The second line of work using RSS are techniques based on mathematical models. Some of these proposals use RF propagation models [17] to predict distance away from an access point based on signal strength readings. By triangulating and extrapolating using signal strength models, TIX [8] achieves an accuracy of 5.4 meters indoors. Lim et al. [12] use a singular value decomposition method combined with RF propagation models to create a signal strength map (overlapping with map-based approaches). They achieve a localization error of about three meters indoors. EZ [5] is a system that uses sporadic GPS fixes on mobiles to bootstrap the localization of many clients indoors. EZ solves these constraints using a genetic algorithm, resulting in a median localization error of two meters indoors, without the need for any explicit pre-deployment calibration.

AoA-based approaches. Niculescu and Nath [15] use a mechanically-rotated directional antenna to triangulate clients' locations from packet-level RSS readings as base stations rotate their antennas. Their system achieves a 2.1 m median error with seven participating base stations. However, it requires an additional rotating antenna to be added to the base station, and needs to overhear hundreds of packets from each client in order to get enough RSS data to achieve that accuracy. Wong et al. [28] investigate the use of AoA and channel impulse response measurements for localization. While they have demonstrated positive results at a very high SNR (60 dB), typical wireless LANs operate at significantly lower SNRs, and the authors stop short of describing a complete system design of how the ideas would integrate with a functioning wireless LAN as ArrayTrack does. Niculescu et al. [14] simulate AoA-based localization in an ad hoc mesh network. AoA has also been proposed in CDMA mobile cellular systems [31], in particular as a hybrid approach between TDoA and AoA [6, 29], and also in concert with interference cancellation and ToA [24].

Image processing based approaches. These approaches match features extracted from images from a mobile’s camera to localize a device. Examples include work by Hile et al. [10] and vSLAM [11].
ArrayTrack achieves high localization accuracy

- 33 clients on one floor of an office space in active use

- Ground truth using architectural drawings and laser measure

- Compare with optimal AP subset of any size: ArrayTrack is within $2\times$
  - Reasons to expect even further improvement

[ACM HotMobile 2012]
Current work: A 16-antenna AP prototype

• Three independent reasons to increase the number of antennas at an AP in the future:
  1. Antenna diversity
  2. MIMO on a single link
  3. SDMA to multiple clients

• Leverage more antennas and more spatial smoothing
ArrayTrack: Latency

- Ongoing work; real-time tracking of mobile clients
- Pseudospectrum computation latency: tens of milliseconds
- Heat map search latency: highly parallel problem
To take away...

Look across system layers for an improved location service and for improved network security

- **ArrayTrack**: High accuracy (median 25 cm) and low latency indoor location system from WLAN infrastructure

- **SecureAngle**: Augmenting WLAN security with AoA signatures