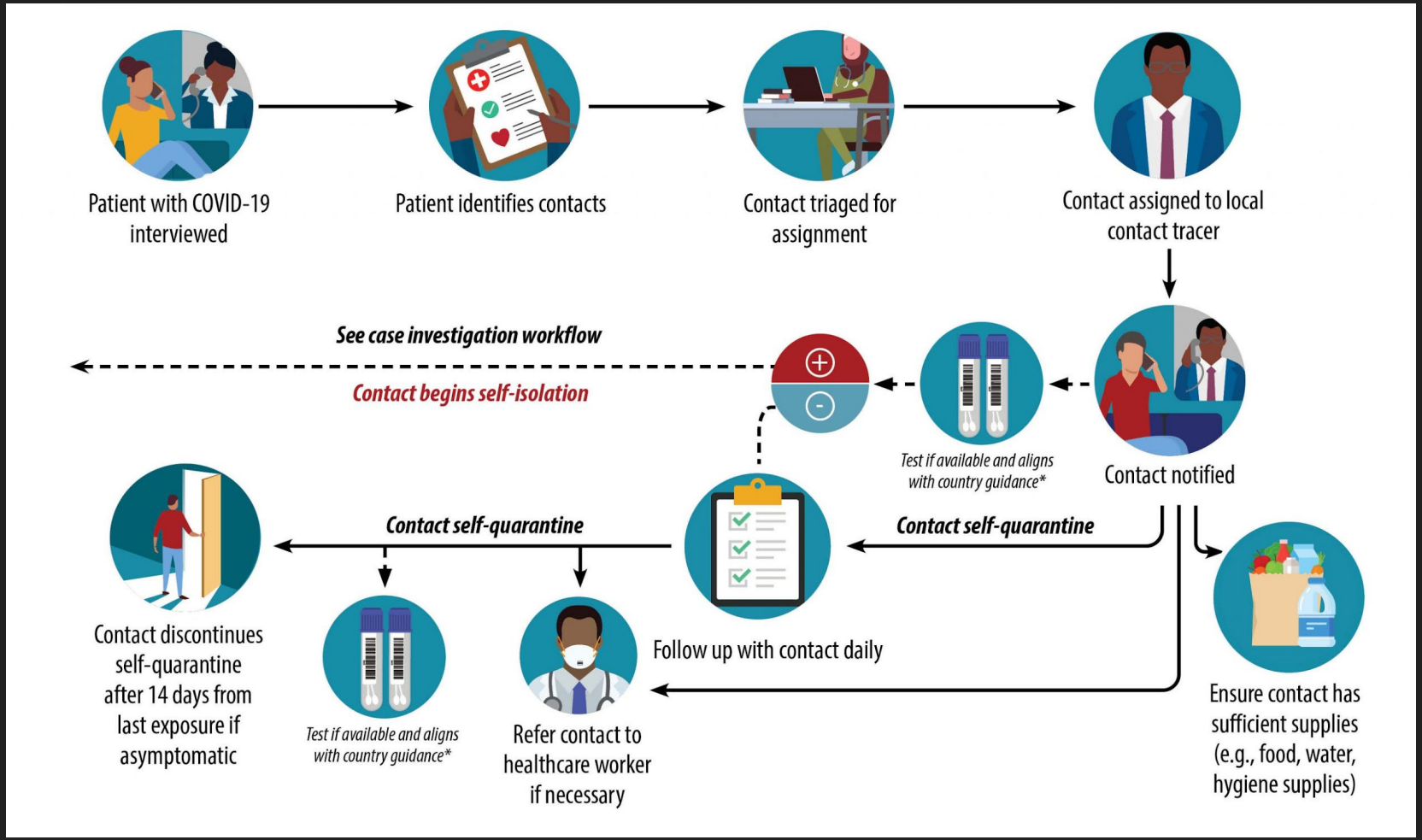
COVID-19 Contact Tracing & Prevention

Michael Specter, specter@mit.edu, Lecture for 6.808, March 2021

Introduction



Source: https://www.cdc.gov/coronavirus/2019-ncov/global-covid-19/contact-tracing-workflow.html

Contact Tracing: Limitations

Human process of contacting those who might be infected

Largely manual

Depends on “who you know you’ve infected”

Goals of Exposure Notification

Augment “classic” contact tracing

-- By --

Automatically notifying those who have been
“close enough” for “long enough” to someone infected!

Ok, fine, I solved the problem, with an app!

1. User uploads their name and contact info to government's DB
2. User uploads GPS coordinates every ~20 minutes
3. When someone is infected, government notifies all users that have been in proximity!

Boom. Done. I'll take my Nobel Prize now.

New Goal, Avoid Dystopia.

TraceTogether

Government Technology Agency Medical ★★★★☆ 15,415

Everyone

You don't have any devices

You can share this with your family. Learn more about Family Library

Add to Wishlist Install

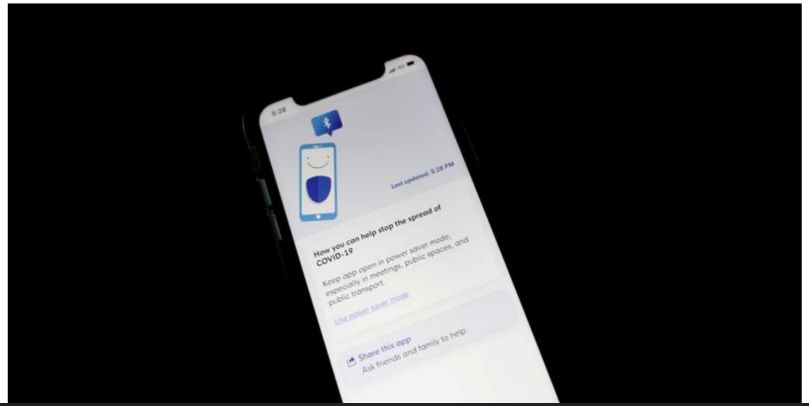
REUTERS World Business Markets Breakingviews Video More

HEALTHCARE & PHARMA JANUARY 4, 2021 / 4:44 AM / UPDATED 3 MONTHS AGO

Singapore COVID-19 contact-tracing data accessible to police

By Reuters Staff 3 MIN READ

SINGAPORE (Reuters) - Singapore said on Monday its police will be able to use data obtained by its coronavirus contact-tracing technology for criminal investigations, a decision likely to increase privacy concerns around the system.



The rest of this lecture:

1. PACT: Private Automated Contact Tracing Protocol
2. SonicPACT: Augmenting PACT with Acoustic Range Estimation

CSAIL

MASSACHUSETTS GENERAL HOSPITAL
GLOBAL HEALTH

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

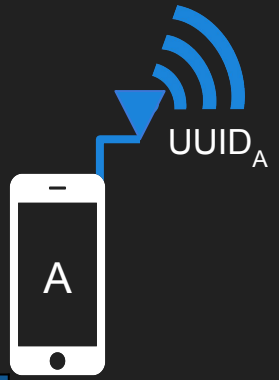
Internet Policy Research Initiative
Massachusetts Institute of Technology

PACT

Private Automated Contact Tracing

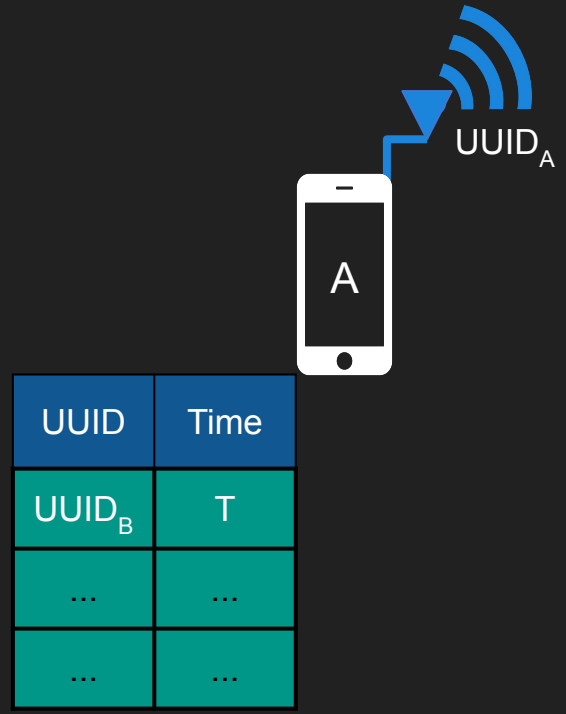
Ronald L. Rivest, Hal Abelson, Jon Callas, Ran Canetti, Kevin Esvelt, Daniel Kahn Gillmor, Louise Ivers, Yael Tauman Kalai, Anna Lysyanskaya, Adam Norige, Bobby Pelletier, Ramesh Raskar, Adi Shamir, Emily Shen, Israel Soibelman, Michael Specter, Vanessa Teague, Ari Trachtenberg, Mayank Varia, Marc Viera, Daniel Weitzner, John Wilkinson, Marc Zissman

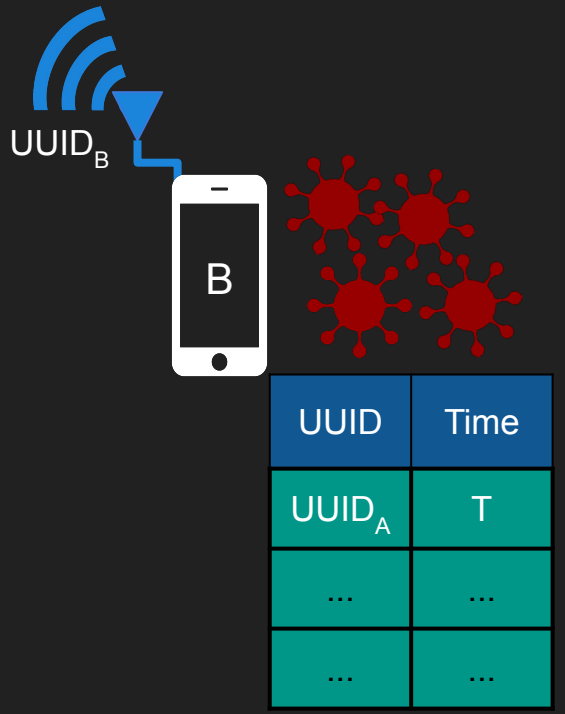
Naive solution

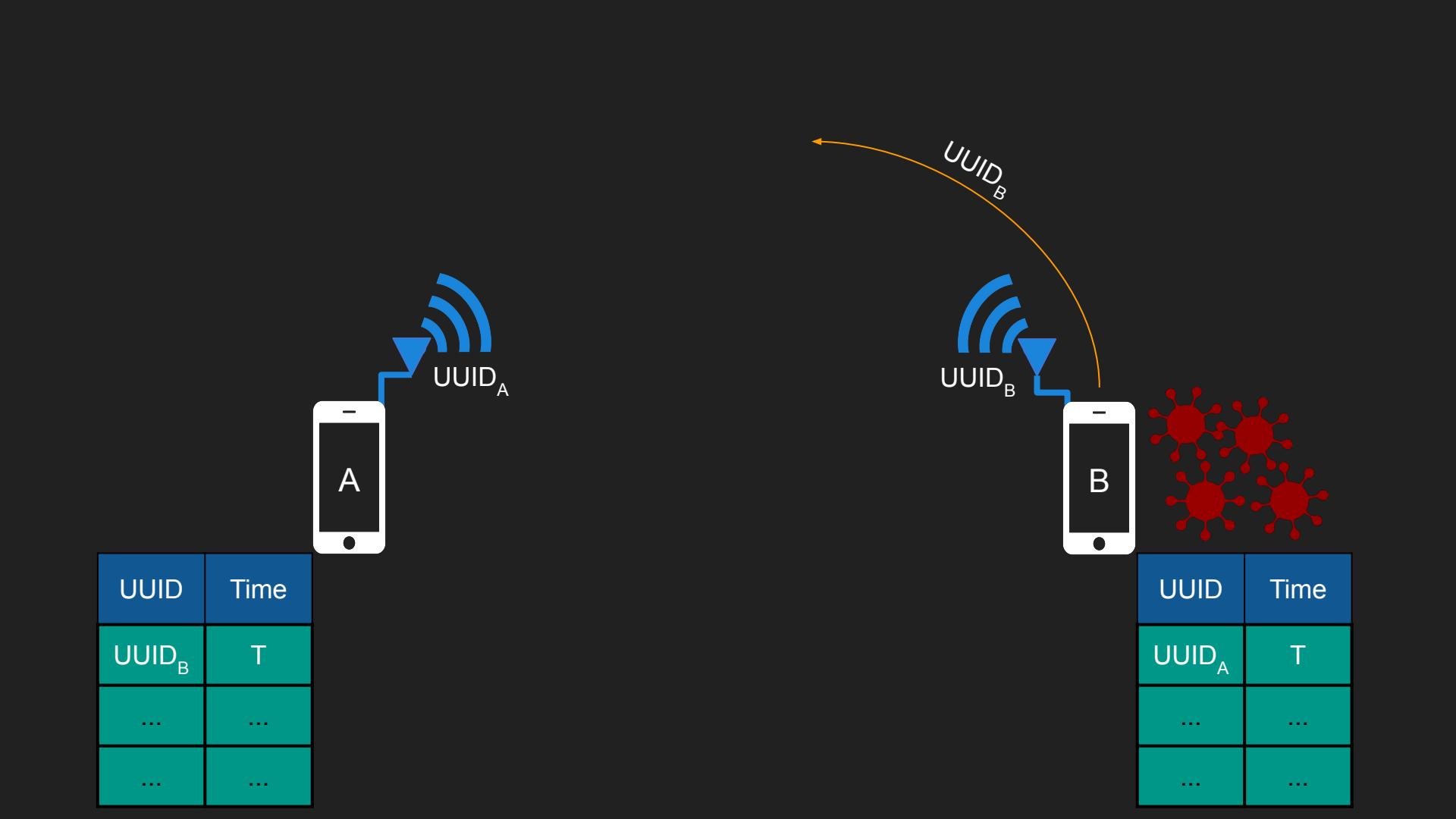


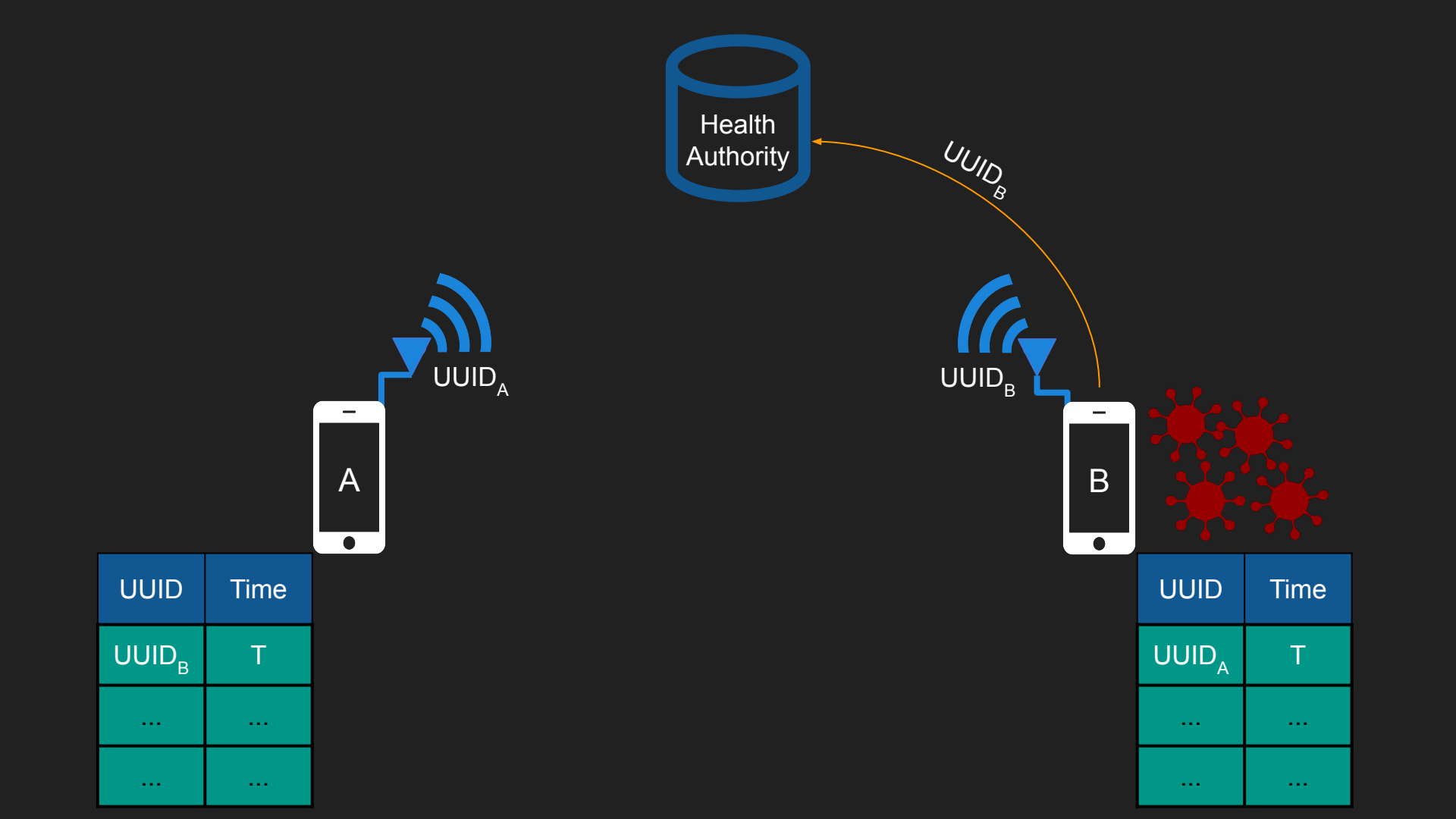
UUID	Time
UUID$_B$	T
...	...
...	...

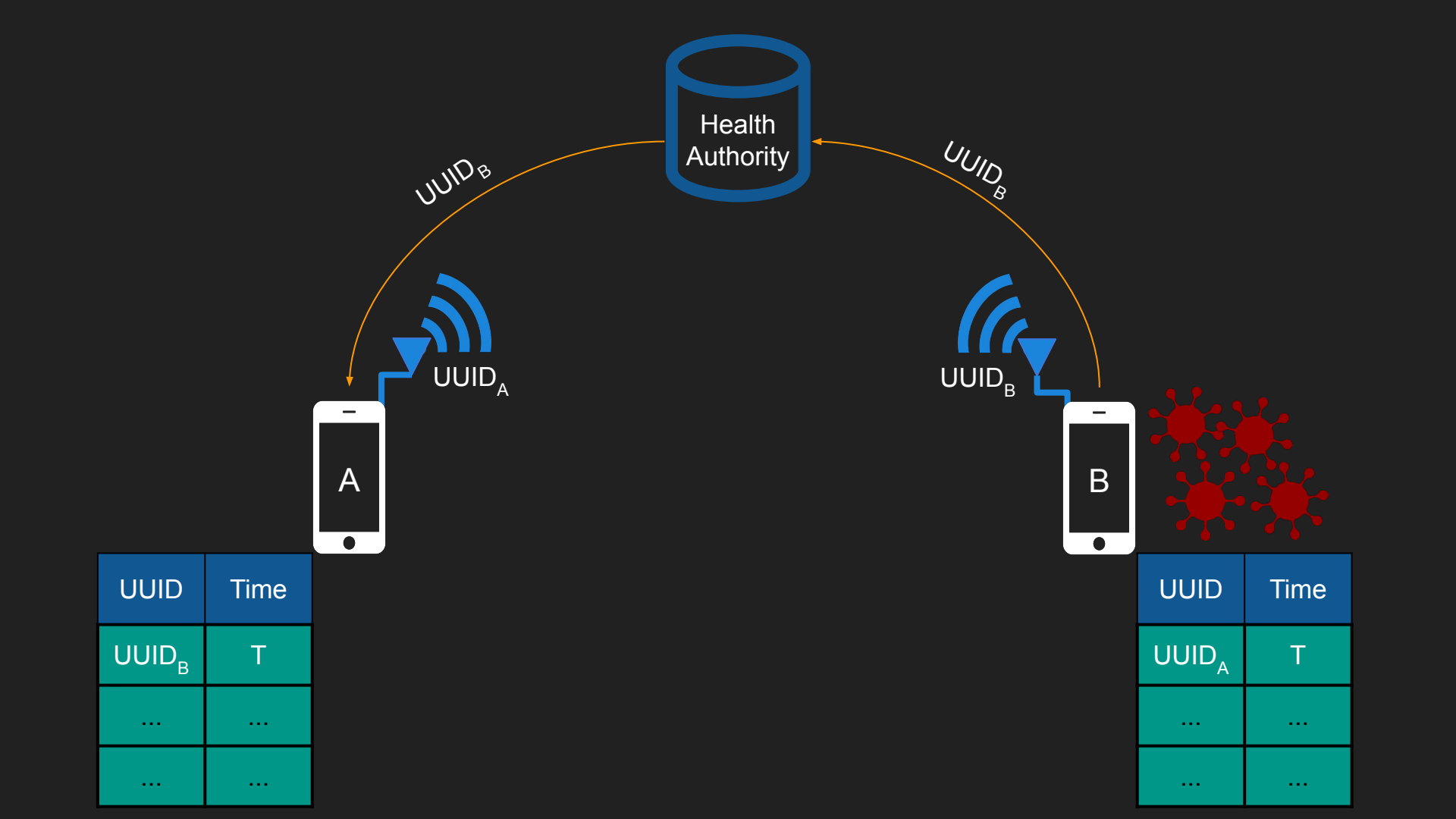
UUID	Time
UUID$_A$	T
...	...
...	...

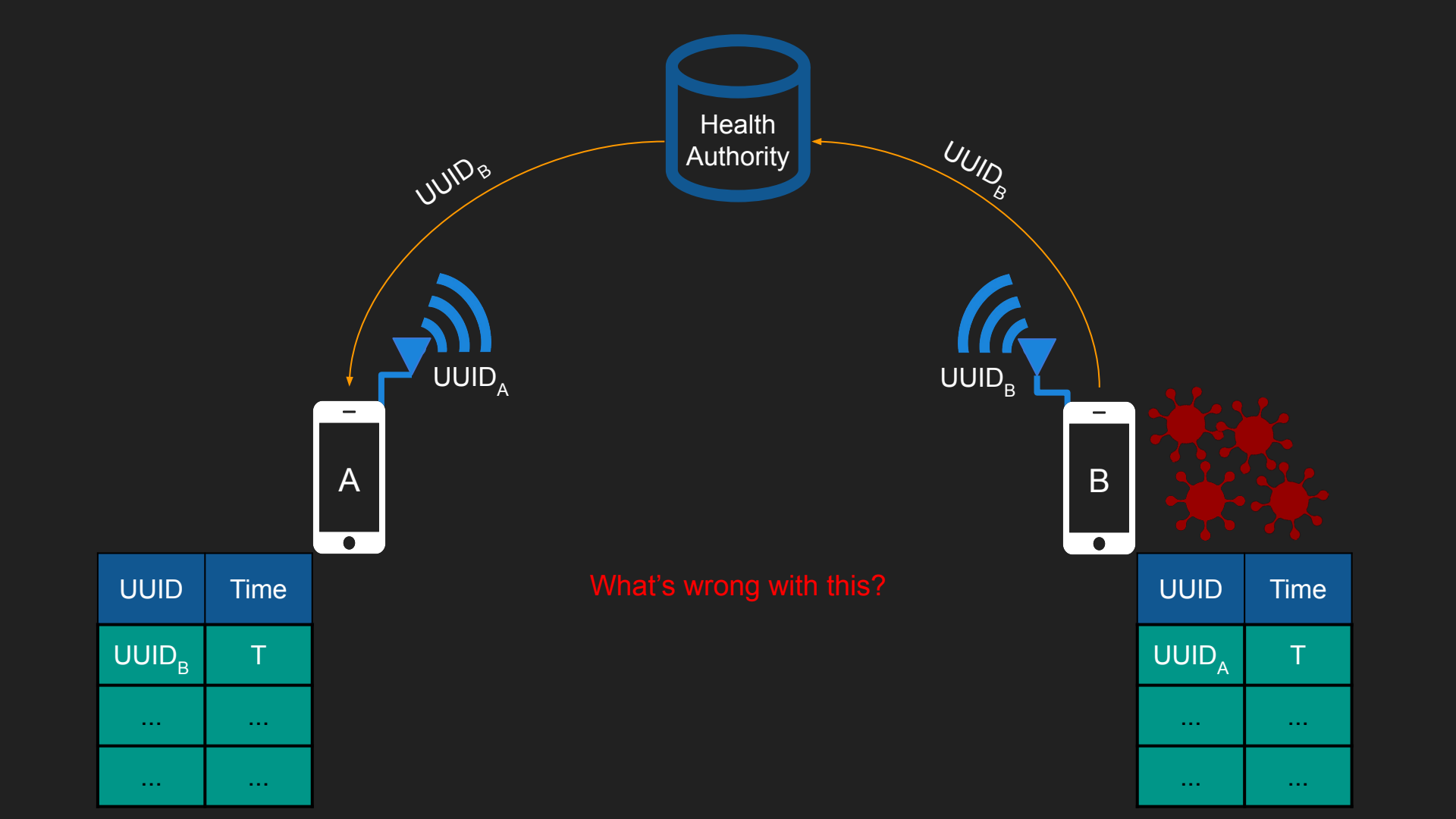

UUID$_A$
A
UUID
Time
UUID$_B$
T
...
...
...
...


UUID$_B$
B
UUID
Time
UUID$_A$
T
...
...
...
...


UUID_B
UUID_A
UUID_B
A
B
UUID
Time
UUID_B
T
...
...
...
...
UUID
Time
UUID_A
T
...
...
...
...


Health Authority
UUID$_B$
UUID$_A$
UUID$_B$
A
B
UUID
Time
UUID$_B$
T
...
...
...
...
UUID
Time
UUID$_A$
T
...
...
...
...


Health Authority
UUID$_B$
UUID$_B$
UUID$_A$
UUID$_B$
A
B
UUID
Time
UUID$_B$
T
...
...
...
...
UUID
Time
UUID$_A$
T
...
...
...
...


Health Authority
UUID$_B$
UUID$_B$
UUID$_A$
UUID$_B$
A
B
What's wrong with this?
UUID
Time
UUID$_B$
T
...
...
...
...
UUID
Time
UUID$_A$
T
...
...
...
...

Specific Goals:

1. Unlinkability
    a. An attacker should not be able to know that she saw you at time A and then later at time B
2. Ability to disavow time periods
    a. A user should be able to choose when their IDs are available at upload time

Solution: Use seeds & Time

1. Every hour, a user selects a new random “seed” S_h
2. Let uuid = sha256(S_h || Current Time)
3. The user stores a database of (S_h, time)
4. When infected, the user uploads the seeds & time period
    a. If they want to disown some time period, omit that S_h
5. All other users recalculate the uuid’s for any time period to check if they’ve been around the infected user

What’s wrong with this?

CSAIL

MASSACHUSETTS GENERAL HOSPITAL
GLOBAL HEALTH

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Internet Policy Research Initiative
Massachusetts Institute of Technology

SonicPACT

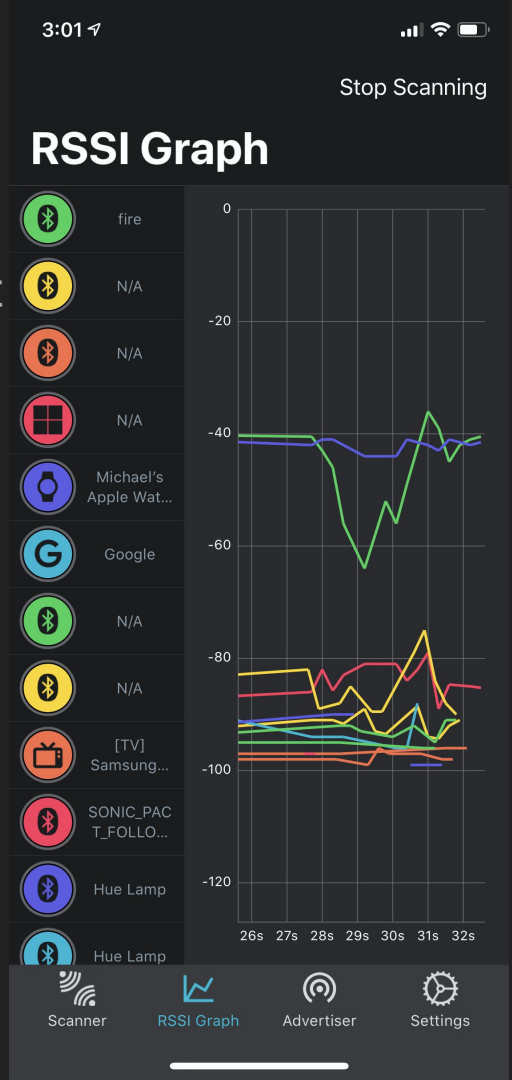
Device to Device Ultrasonic Rangefinding

Michael Specter, John Meklenburg, Michael Wentz, Hari Balakrishnan, Anantha Chandrakasan, John Cohn, Gary Hatke, Louise Ivers, Ronald Rivest, Gerald Jay Sussman, Daniel Weitzner

Problem: Bluetooth is Sadness

Why?

- Signal strength as a distance measurement is suspect
  - Attenuation happens w/ meat
  - Humans are made of meat
  - Dependent on channel, antenna, etc
- On-device clocks generally can’t measure speed
  - Kills AOA, timestamping methods
- Bluetooth goes through walls

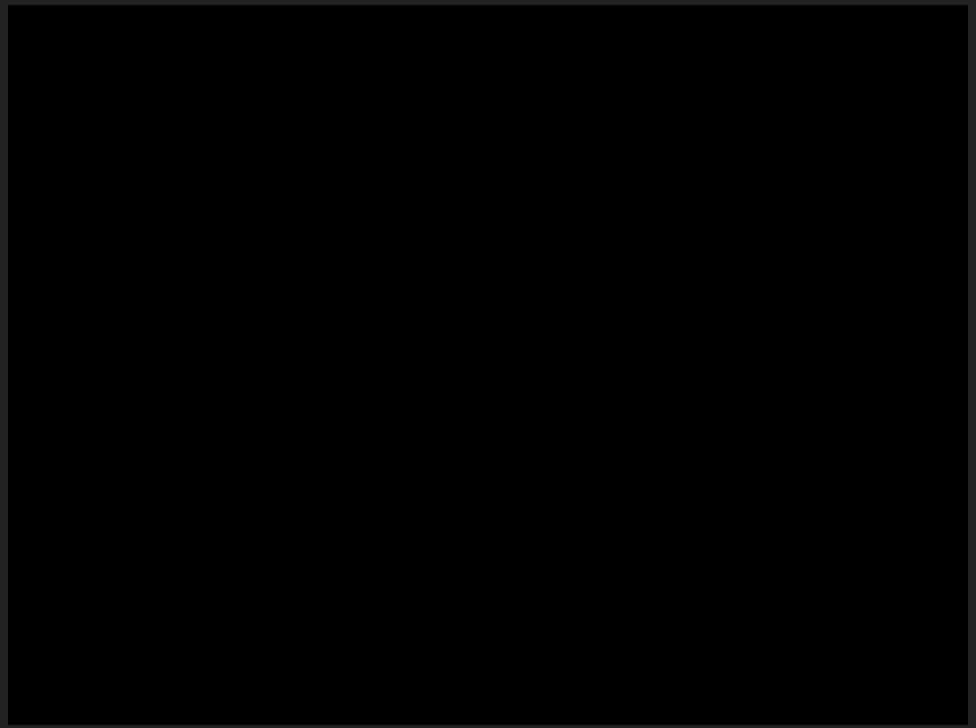


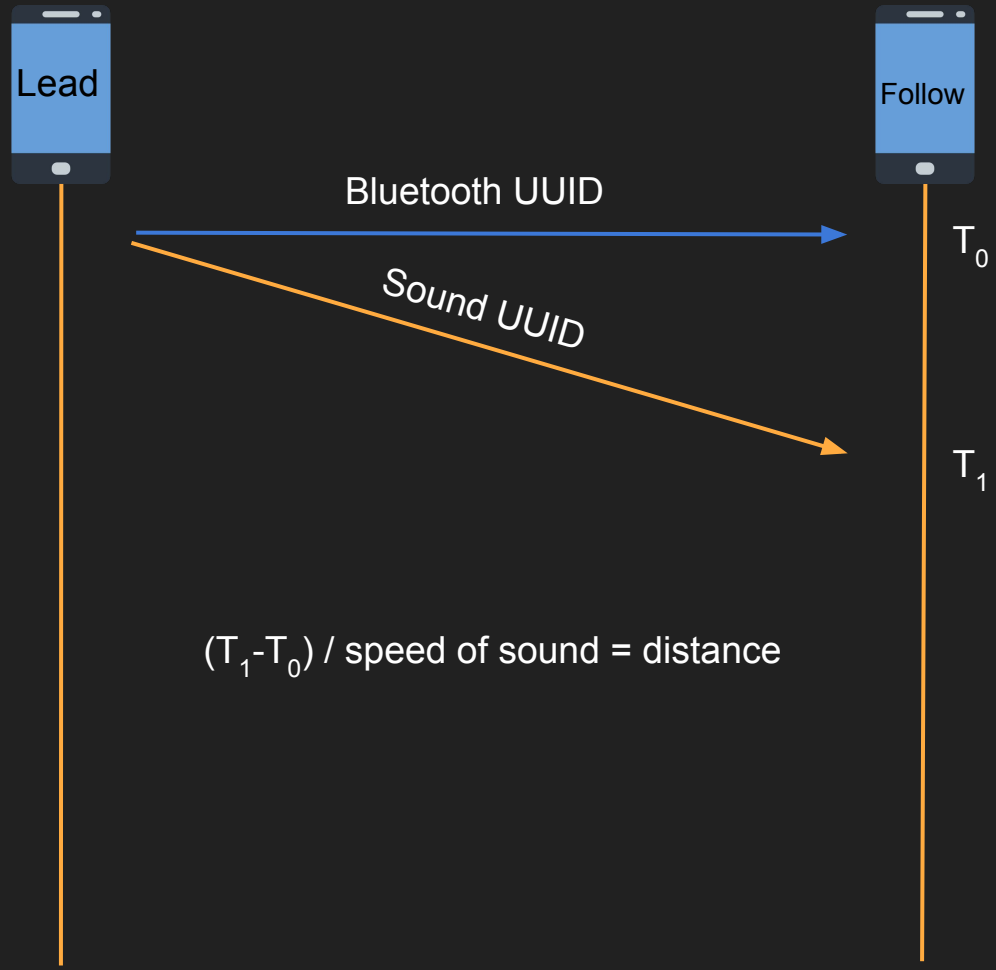
What about audio?

Ultrasonic Frequency Use on Commodity Devices

- 18-20KhZ, Generally cannot be heard by adults
- iOS and Android devices are capable of broadcasting / receiving
- Can be modulated ala RF to carry data
    - Unique random noise per device & matched filter to decide whose wave is incoming

Early tests




Lead
Follow
Bluetooth UUID
Sound UUID
T_0
T_1
(T_1-T_0) / speed of sound = distance

- Why is this not a normal smartwatch?

Pro Sports COVID-19 Sensors Trace Rise of Ultra-Wideband Tech

Bluetooth- and UWB-based contact tracing both compelling, though UWB may be poised for post-pandemic takeoff

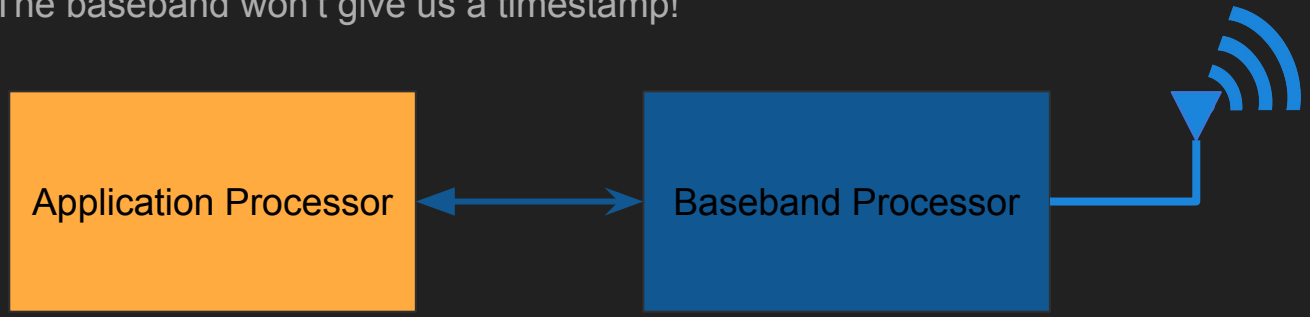
By **Jeremy Hsu**

Photo: Kinexon

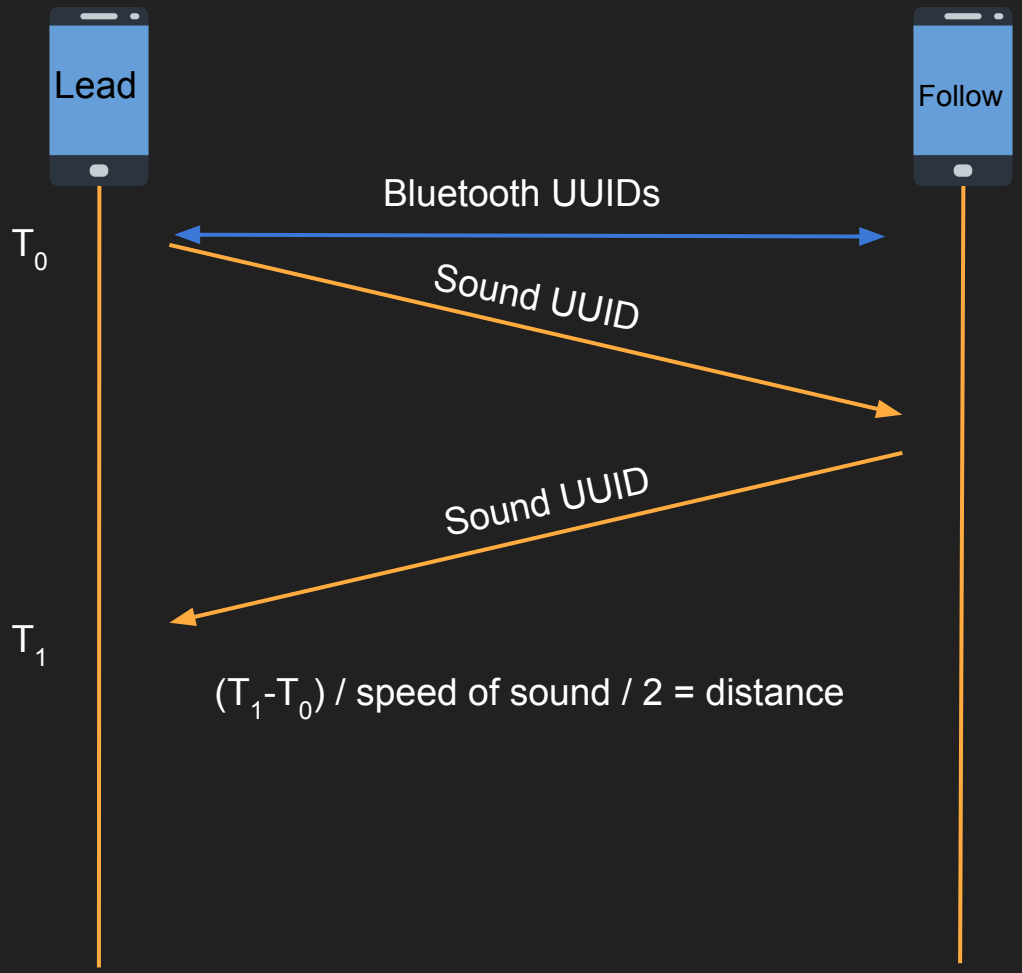
Ultra-Wideband (UWB) on the Wristband: Denver Broncos quarterback Drew Lock wears a Kinexon SafeTag featuring UWB technology for contact tracing.

You don’t control the radio!

- Path of a bluetooth packet through Android:
  a. Userspace process
  b. Kernel
  c. Userspace Bluetooth process
  d. Back to the kernel
  e. Talks to Baseband Processor (closed-source Qualcomm real-time OS)
- We have no control over when a packet is sent
  a. The baseband won’t give us a timestamp!

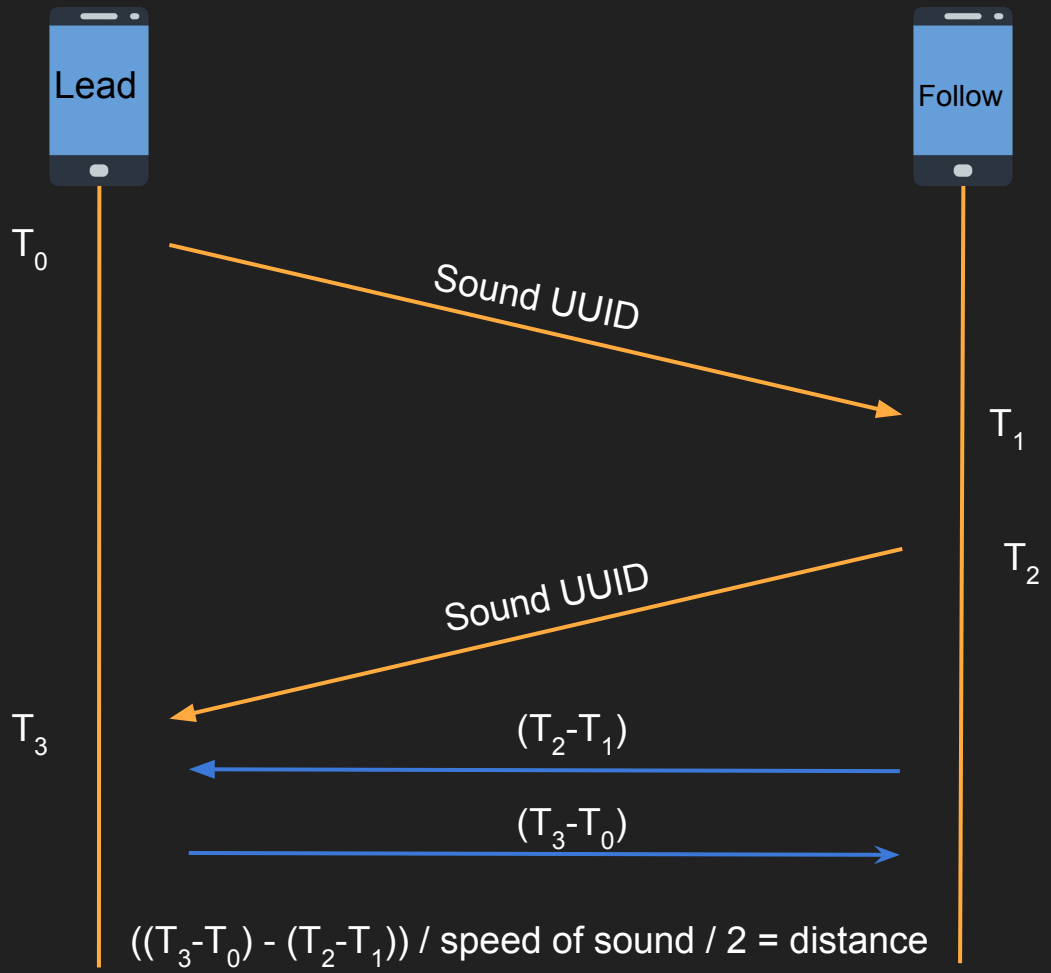


Roundtrip Protocol


Lead
Follow
Bluetooth UUIDs
T0
Sound UUID
Sound UUID
T1
(T1-T0) / speed of sound / 2 = distance

This STILL doesn’t work.

- Path of audio through Android:
  a. Current process
  b. Kernel
  c. Media process
     - Filtering, mixing, other sadness
  d. Kernel
  e. Hardware DAC
  f. Speaker
- Same thing in reverse for the other side
- We have no idea when audio is sent or received.


Lead
Follow
T_0
Sound UUID
T_1
T_2
Sound UUID
T_3
(T_2-T_1)
(T_3-T_0)
$((T_3-T_0) - (T_2-T_1)) / \text{speed of sound} / 2 = \text{distance}$

We have to control for the OS

- Use “high speed” audio
  a. Still not enough
- Use a loopback to estimate delay
  a. Whenever you broadcast, listen for our own audio
  b. ~8 MS delay to exit the device on most android devices
  c. Highly dependent on OS state!

Waveform Generation & Detection

How do we transmit a UUID?

- We need to be able to pick up on signals
  a. Random noise (e.g. a clap) *will* hit U.S. frequencies
  b. Doppler shift is a thing, can’t assume frequencies
- Initially, we used BPSK
  a. RF-like modulation!
  b. Arbitrary data!
  c. Super slow
- Moved to random noise generation

How do we transmit a UUID?

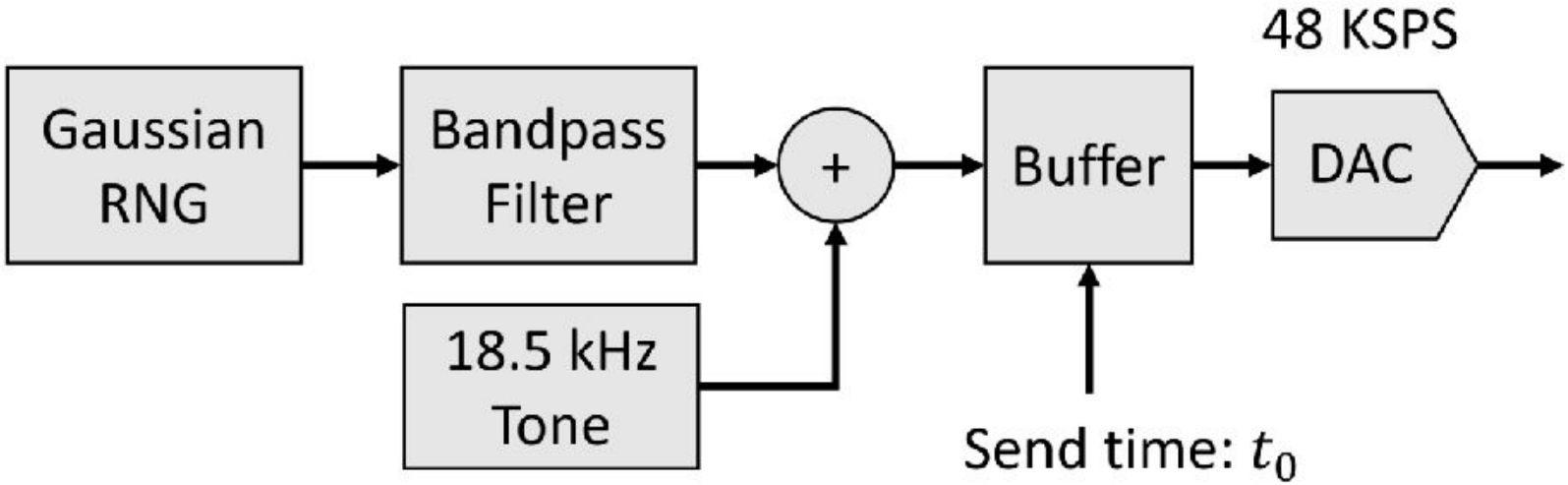
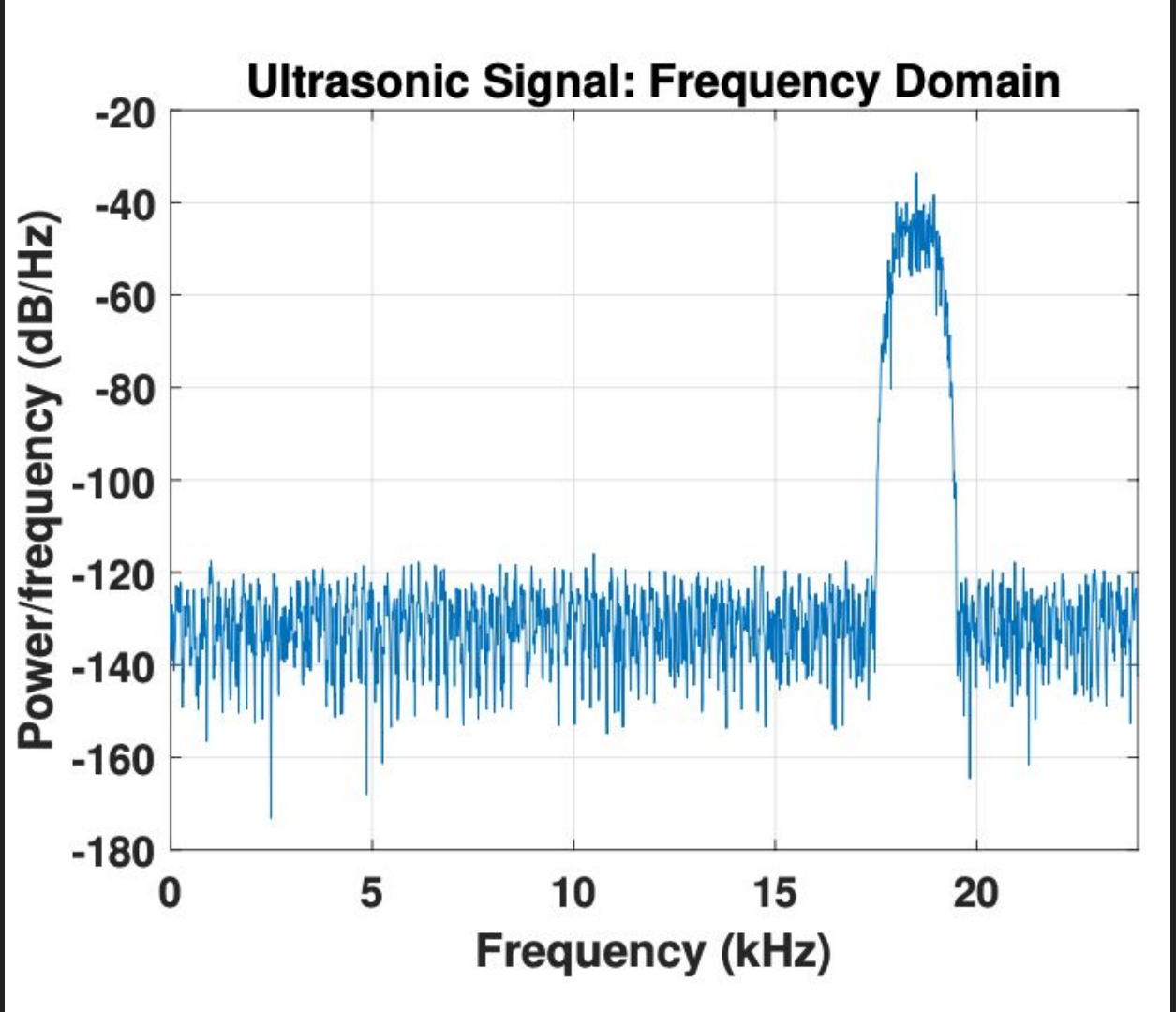


Fig. 10. Transmitter processing block diagram

```
def gen_waveform(uuid):
    samples = []
    seed ← SHA256(uuid)

   # Guassian RNG, standard deviation of 1 centered
    at 0
    generator ← GaussianRNG(seed, 0, 1)

    for i ∈ {0...WAVE_LENGTH}:
        samples[i] ← generator.next()

    samples = BandpassFilter(samples, 18Khz, 20Khz)
    samples = AddStaticPulse(samples, 18Khz)

    for i ∈ {0...ramp_len}:
        samples[i] *= i/ramp_len
        samples[len(samples)-i] *= i/ramp_len

    return samples
```

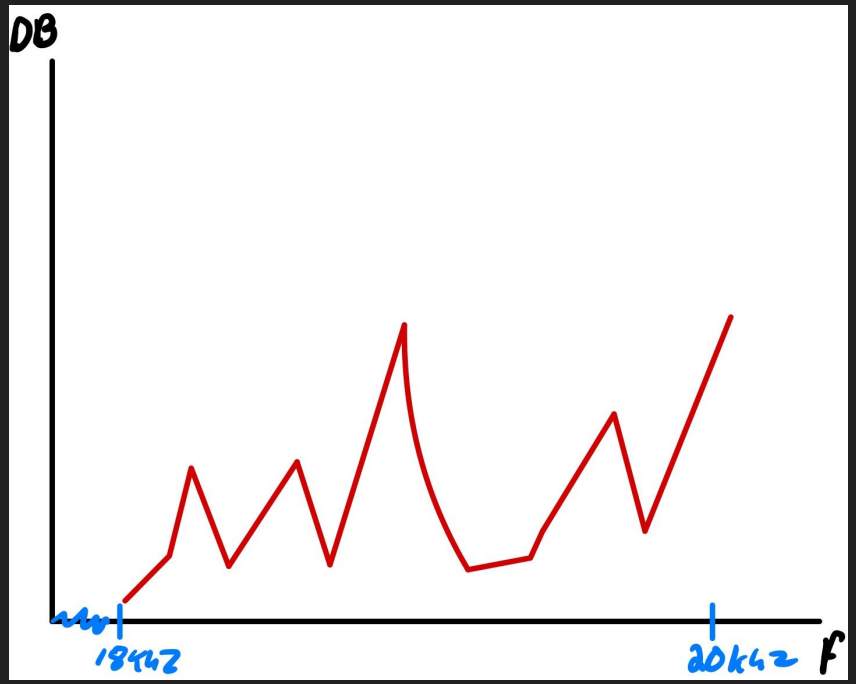
Listing 1. Waveform Generation

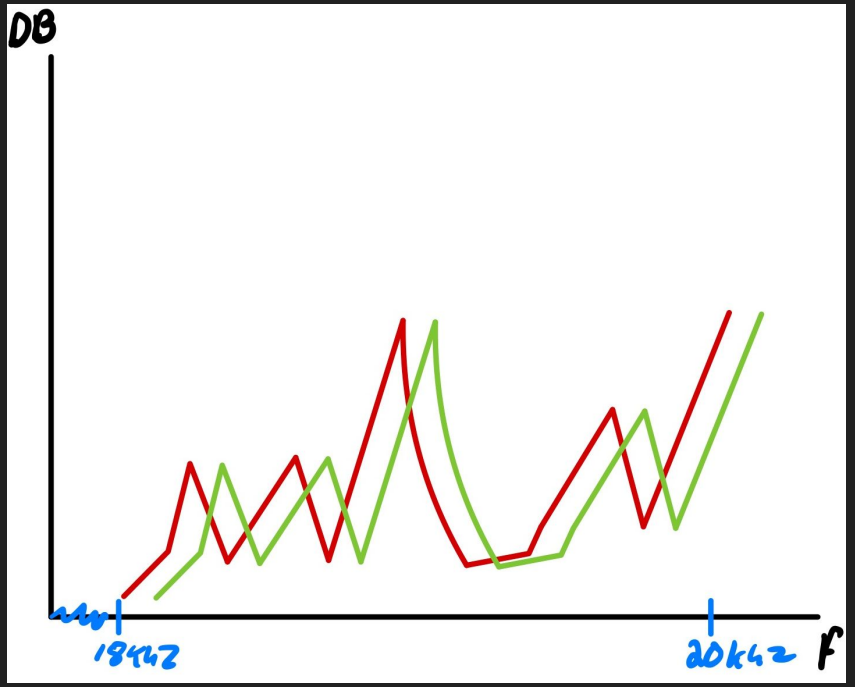

Ultrasonic Signal: Frequency Domain
Power/frequency (dB/Hz)
-20
-40
-60
-80
-100
-120
-140
-160
-180
0
5
10
15
20
Frequency (kHz)

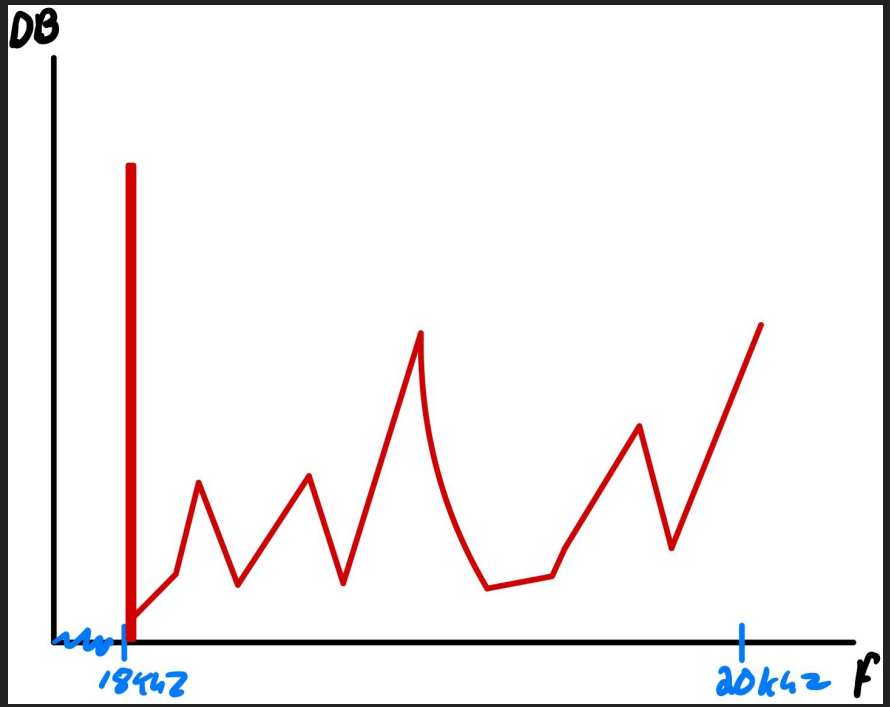
Detection

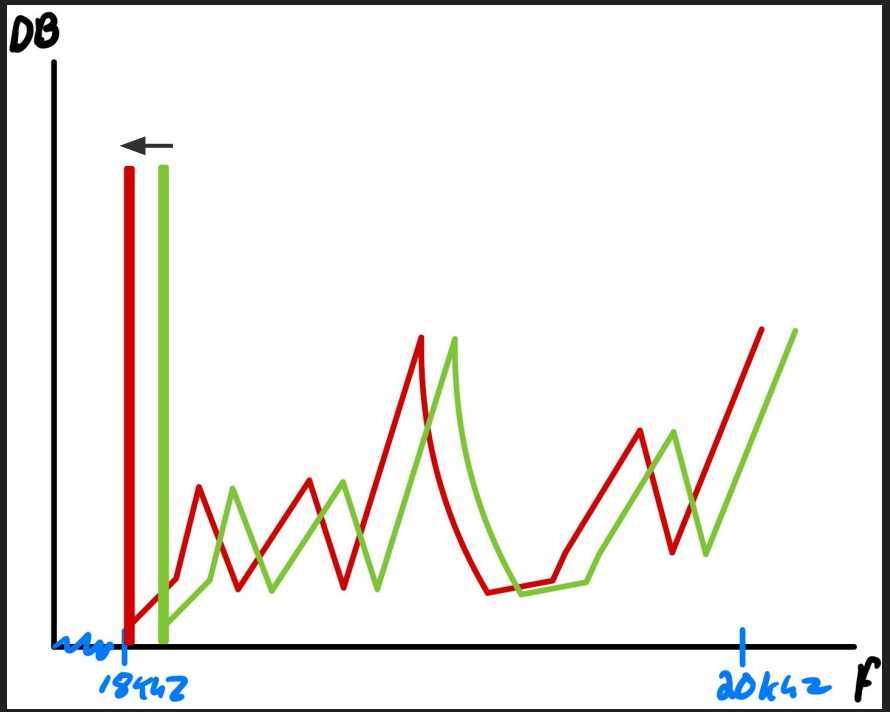
- First, check if anyone’s around using bluetooth
- Since we know everyone’s UUID from bluetooth, generate their wave!
- Use a matched filter to correlate & decide whose wave is incoming

What happened here?



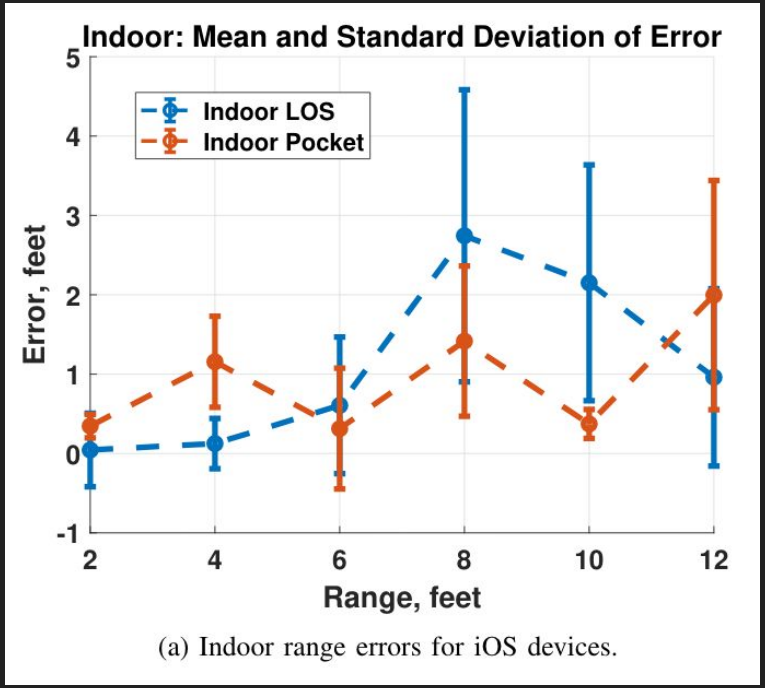



DB
18kHz
20kHz
F

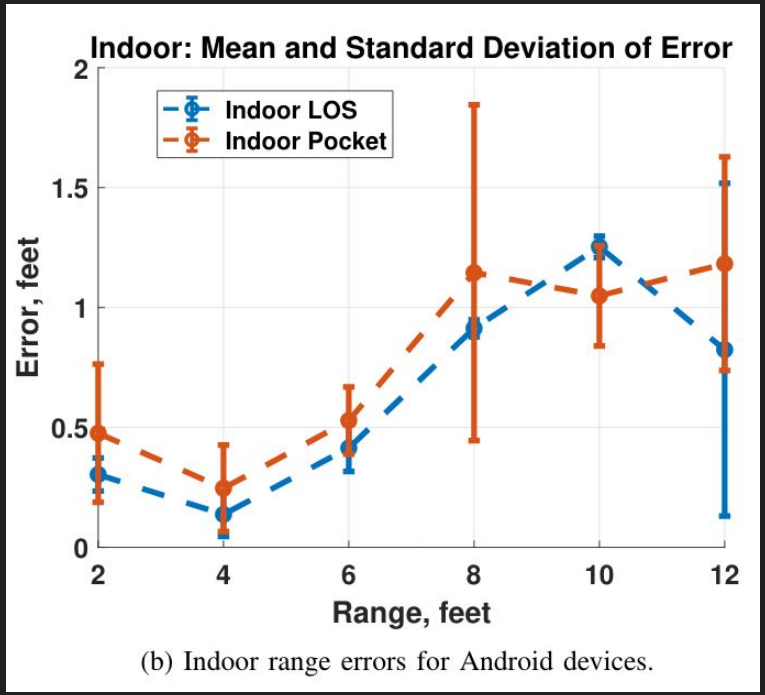

DB
18kHz
20kHz
F

Results


RESTORE
SANITY
FELLOW



(a) Indoor range errors for iOS devices.



(b) Indoor range errors for Android devices.

Test	6-ft miss %	6-ft false %	8-ft miss %	8-ft false %	Within 1 foot %
LOS Android	0.0	0.0	0.0	0.0	80.3
LOS iOS	5.1	0.0	11.9	0.0	57,6
Pocket Android	0.0	0.0	1.3	0.0	70.9
Pocket iOS	3.3	0.0	13.3	0.0	56.7

Some takeaways

- A lot of what we're doing here depends on your degrees of freedom
- Real world is limited in ways we don't expect
  a. Especially as academics
- *Still* a lot of low-hanging fruit!

Full Paper: https://pact.mit.edu/

Contact: specter@mit.edu