Carnegie Mellon University

S23 18500 Team C2: **WiSpider**

Presenter: Ethan Oh
Group: Ethan Oh, Anish Singhani, Thomas Horton King

Application / Use Case

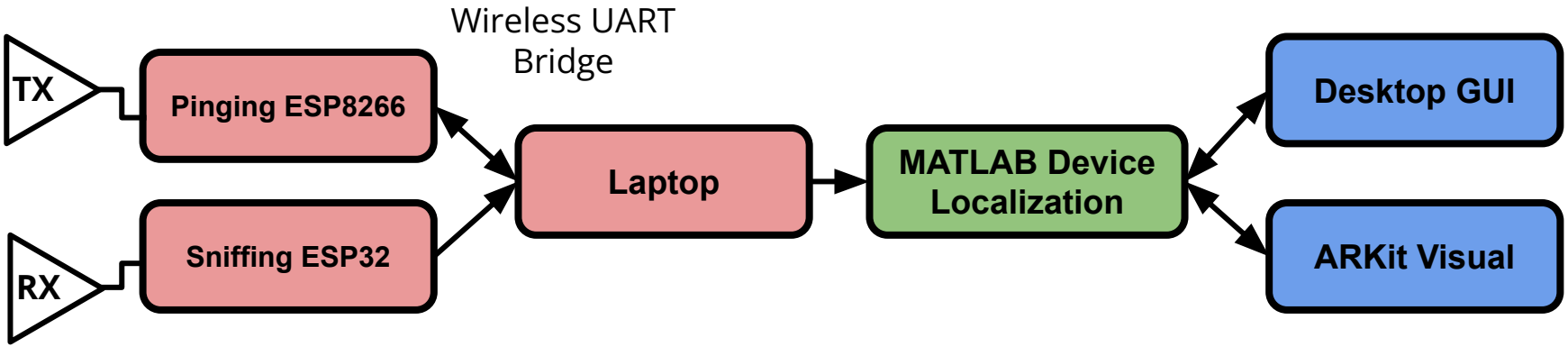
- Hidden wireless devices are infringing privacy
  - Cameras, microphones, sensors, etc.
- We want to build a product to detect and locate these hidden Wi-Fi devices indoors
- Detect devices even if user is not connected to the same Wi-Fi network

Solution Approach

- Building a product with which a user can walk around a room, and it will detect Wi-Fi devices via time-of-flight, and build a map of their locations
  - Limited to indoors, tracking non-moving devices
- Show the locations of detected devices to the end-user in an Augmented Reality visualization
  - User can then find devices manually within the ~1m detection zone

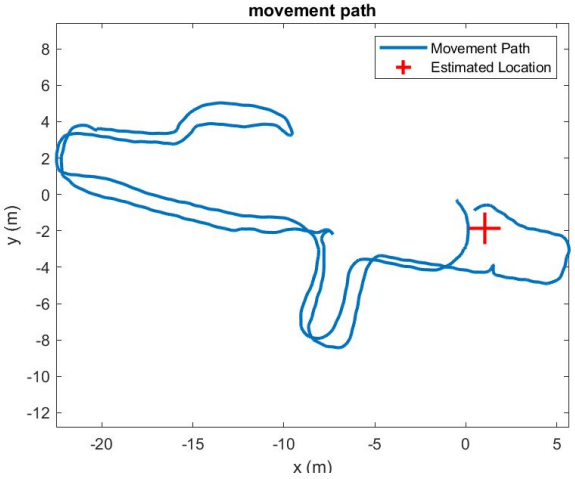
System Design - Block Diagram

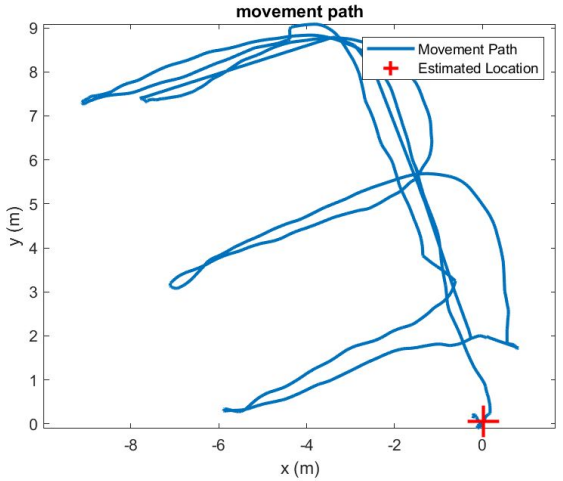
- Moved away from AX200 and towards 2 ESPs
  - Reduces cost and complexity, uses only open-source software
- No longer using any directional antennas



Testing Procedure

- De-risking: Manually sanity-testing each component before integration
  - Allows us to find workarounds to things that don’t work as expected
- Set up testbed in a room, try various different movement patterns
  - Zig-zag through the room
  - Spiraling out from center of room





Unit Testing

- Device detection
  - Put known devices on a network, check how many devices it detects
- Device pinging
  - Test via pinging known device and observing ACKs on Wireshark
- Device localization
  - Localize one known device at known position, calculate error
- Self-localization + AR visualization
  - Place objects at known location and visually verify

Unit-Test Results

Design Requirements	Metric	Result
Physical	< 10lbs, 1ft^3	*1.2 lbs, 0.1 cu ft (including user's phone)*
Sniffing rate	< 1 min	*15 seconds*
Injection rate	100 pkt/s	*~400 pkt/s*
ToF measurement rate	50 pkt/s	*~200-400 pkt/s depending on target device*
ToF accuracy	< 2m	*individually noisy, ~1m when aggregated*
Distinguish devices	Yes	*Yes, by MAC address; even across channels*
Infrequent device	Yes	*Yes, using wakeup packets*
Self-localization and AR	< 0.3m	*verified < 0.3m with occasional re-localization*

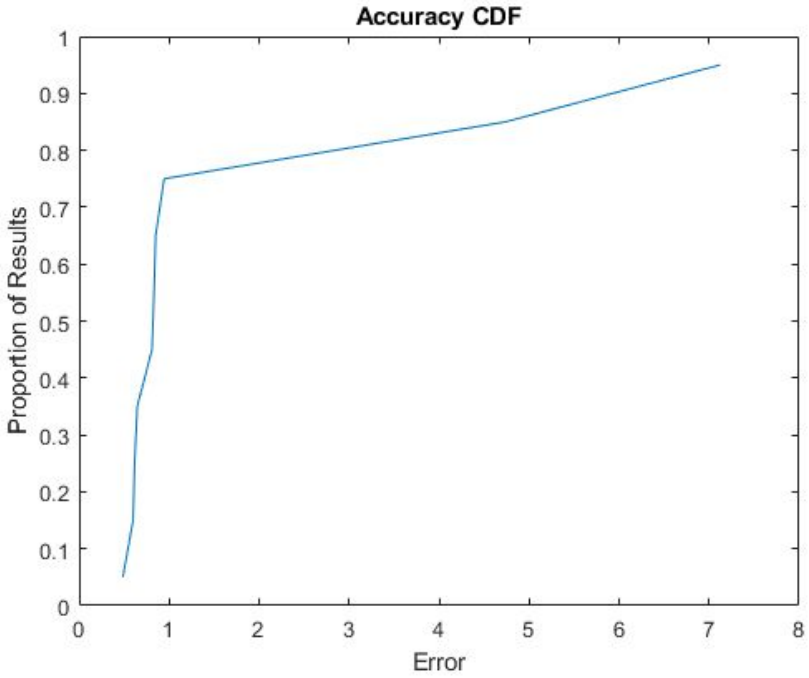
Integration Testing

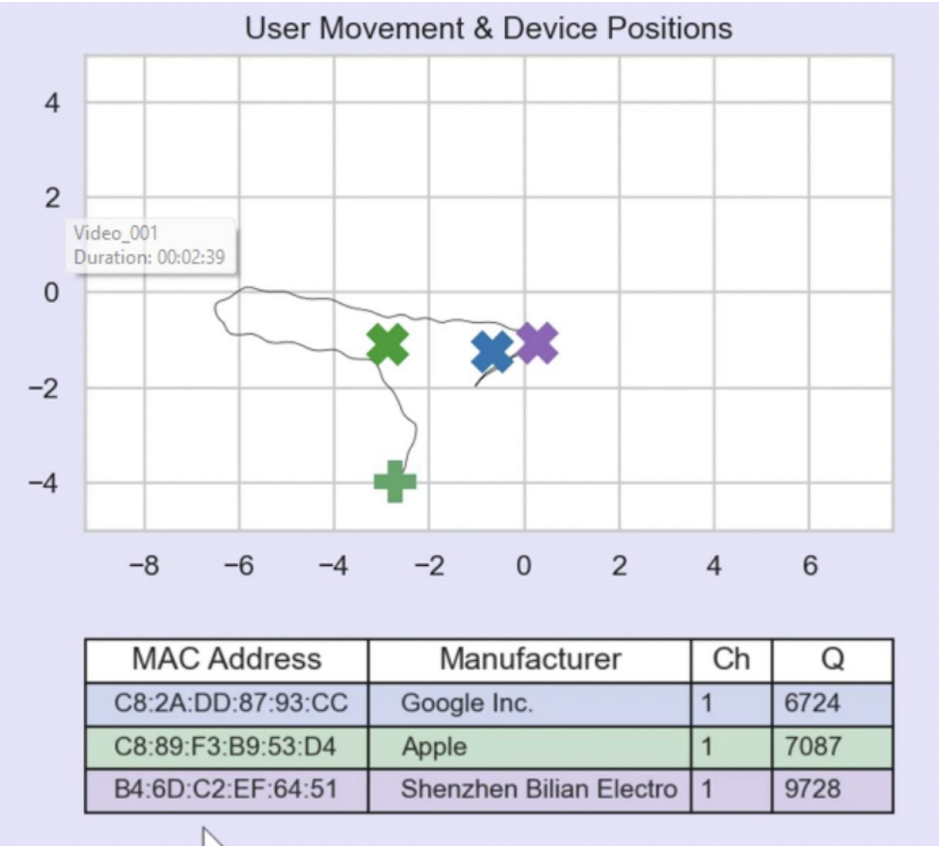
- Set up testbed with a variety of Wi-Fi devices
  - Different channels and data rates to test detection accuracy and range
  - Different kinds of devices: cameras, microphones, sensors, etc.
- Set an origin point, measure ground-truth location of each device
- Capture a variety of test traces (3min, 5min, 10min long traces)
  - Verify positional accuracy against ground-truth
  - Verify percentage of devices detected (and time taken to detect)
- Visually test that AR locations match the physical coordinates

Integration-Test Results

Use-case Requirements	Metric	Result
Cost	< $150	*$143.60*
Size/Weight	< 10lbs, 1ft^3	*1.2 lbs, 0.1 cu ft (including user's phone)*
Detection Rate	> 90%	***prelim results very good, still verifying***
Scan Time	< 5 min	*3~5 minutes*
Lateral Accuracy	< 1m	***prelim results suggest ~0.8m, still verifying***
Detection Range	> 10m	*verified at >40m range*
Detection Resolution	< 0.5m	*can distinguish devices ~0.2m apart*

Results Graphs





MAC Address	Manufacturer	Ch	Q
C8:2A:DD:87:93:CC	Google Inc.	1	6724
C8:89:F3:B9:53:D4	Apple	1	7087
B4:6D:C2:EF:64:51	Shenzhen Bilian Electro	1	9728

Current Status + ToDo’s

- Video: https://cmu.box.com/s/8x966w48auefjpds1oikymdqhz2etpzc
- TODOs
  - Finish integration
    - *Make it easy to filter out known/trusted devices*
  - Evaluate and optimize localization error
  - Refine user interface

Project Management

Anish - Integration

Thomas - Device localization

Ethan - Laptop visualization