Carnegie Mellon University

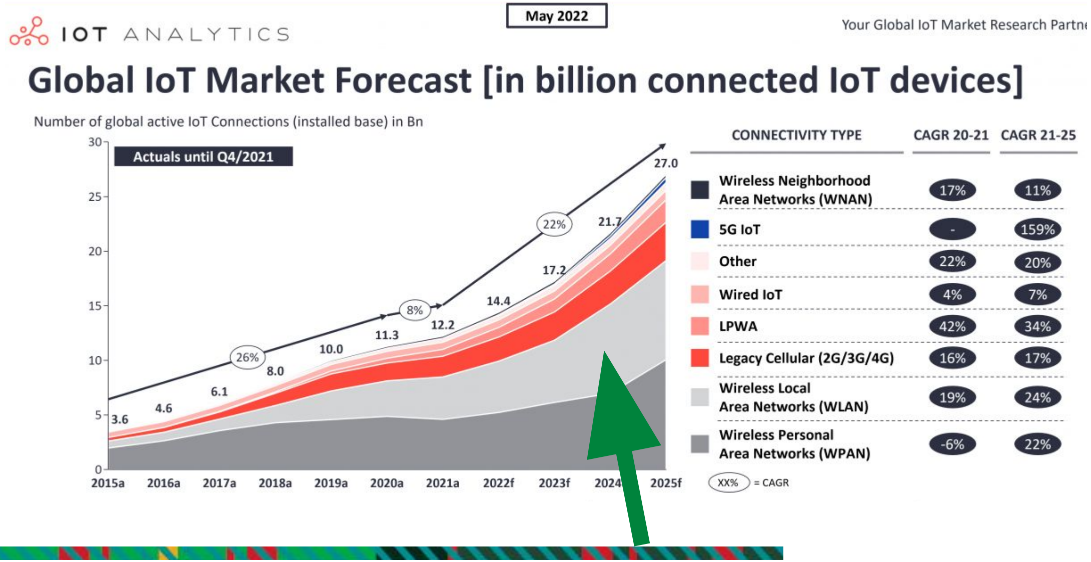
S23 18500 Team C2: **WiSpider**

Presenter: Thomas Horton King

Group: Ethan Oh, Anish Singhani, Thomas Horton King

Problem Statement / Use Case

- Hidden wireless devices are infringing privacy
- We want to build a product to find and locate them
- Design Areas:
    - Signals and Systems
    - Software Systems
    - Hardware



IOT ANALYTICS

May 2022

Your Global IoT Market Research Partne

Global IoT Market Forecast [in billion connected IoT devices]

Number of global active IoT Connections (installed base) in Bn

CONNECTIVITY TYPE	CAGR 20-21	CAGR 21-25
Wireless Neighborhood Area Networks (WNAN)	17%	11%
5G IoT	-	159%
Other	22%	20%
Wired IoT	4%	7%
LPWA	42%	34%
Legacy Cellular (2G/3G/4G)	16%	17%
Wireless Local Area Networks (WLAN)	19%	24%
Wireless Personal Area Networks (WPAN)	-6%	22%

XX% = CAGR

Use-Case Requirements 1:

Cost: < $150

- Primarily for corporate / military applications
- Still want to be accessible
- Project restrictions

Weight: < 10 lbs

Size: < 1 ft^3 volume

- Device should be carryable
- Want to be transportable and easy to use

Use-Case Requirements 2:

Device detection rate: >90%

Scanning time: <5 minutes

- Catch frequently transmitting devices
- Trade-off between measurements

Lateral accuracy: <1m

- This will allow users a small enough area to manually search for hidden devices

Use-Case Requirements 3:

Detection Range: > 10m

- Most wireless devices are passively in ‘sleep’ mode
- In-line with microphone, proximity sensors

Recognition Accuracy: > 50%

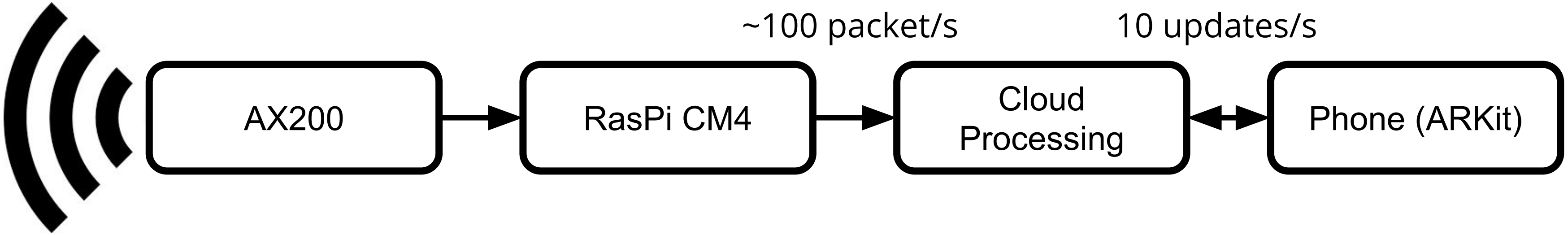
- Any accuracy is better than most commercial solutions
- Allows the user to avoid removing harmless devices

Technical Challenges

- Using mostly commodity hardware
- **Accurate** localization using WiFi/hidden signatures
- **Combined** with user movement/positioning
- Detecting possible low-power **IoT devices**
- Device identification with limited information (i.e non-cooperatively)

Design - Physical Layer

- AX200 WiFi Chip for receiving
  - PicoScenes to recover ToF and CSI
- 2 directional antennas
- Raspberry Pi for control and data uplink
- Phone for Self-Localization and AR Visualization
- Storage on AWS, Processing on MATLAB

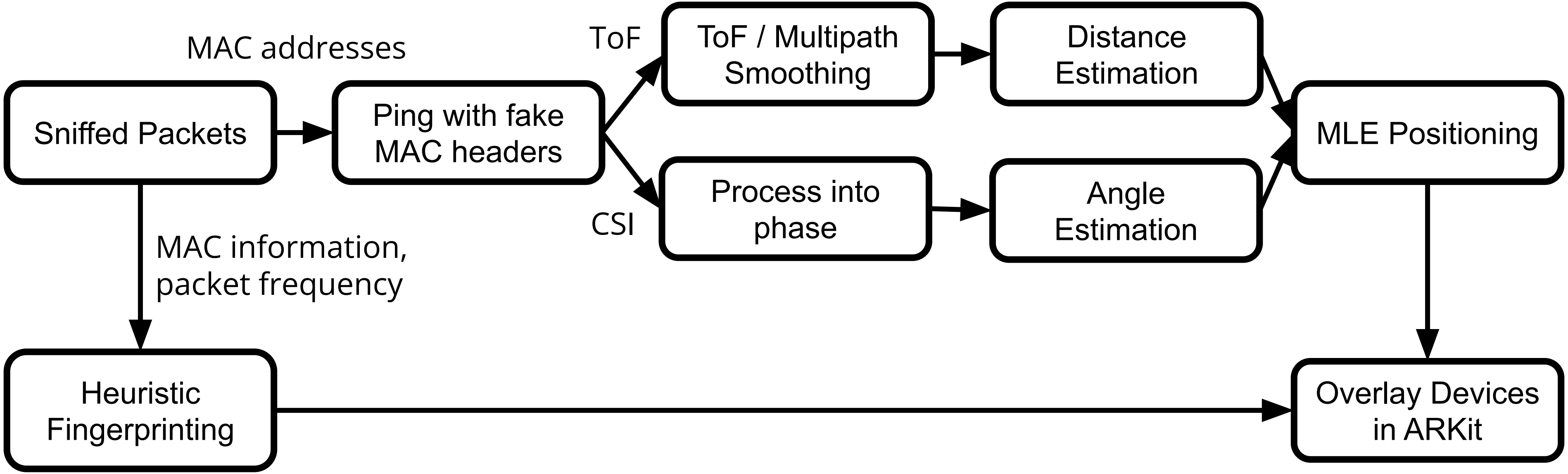


AX200 → RasPi CM4 → Cloud Processing ↔ Phone (ARKit)

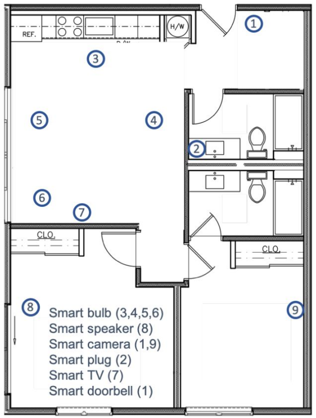
~100 packet/s

10 updates/s

Design - Algorithmic Layer



Testing and Verification



- Testbed with various IoT devices connected to their own router
- Scatter devices throughout a room and assess localization
- Multiple (5) runs with different detection times (3 min, 5 min, 10 min)
- **Device detection rate**: measure detection rate under fixed (5 min) time
- **Scanning time**: measure how long it takes to reach the target detection rate
- **Lateral accuracy**: Compare detected locations with actual locations
- **Detection range**: Place a device (5, 10, 20 m) away from the scanner and measure performance
- **Recognition accuracy:** Test if each ‘category’ of device is identified correct.

Tasks

Anish

- **Hardware**
- Antenna Selection
- PicoScenes Integration with WiFi Receiver
- ARKit self-localization
- ARKit visualization
- RPi Data Streaming
- RPi WiFi chip integration

Ethan

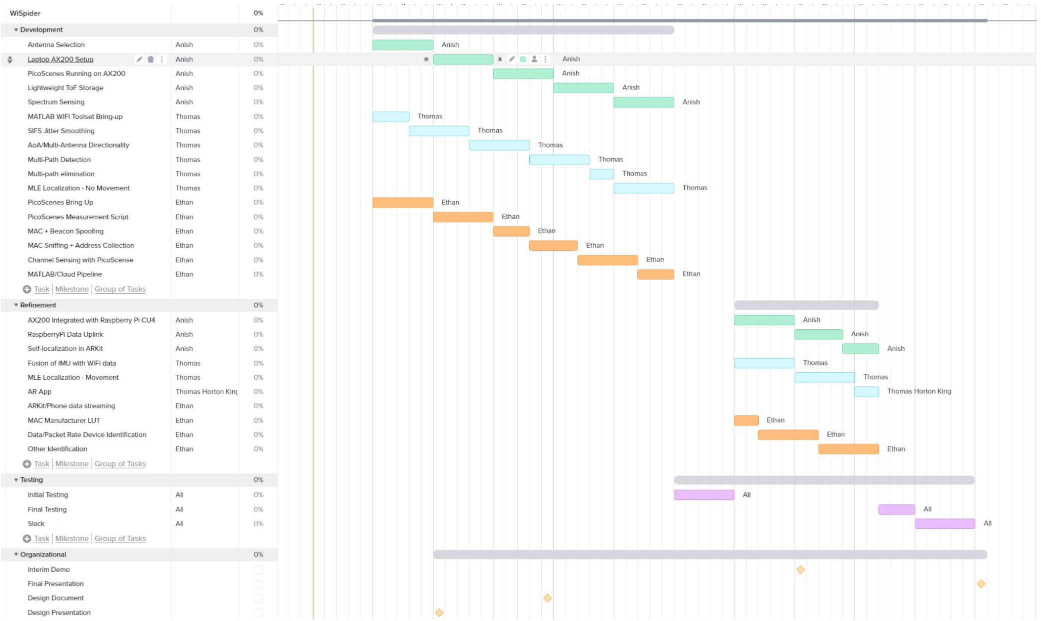
- **Software/Security**
- MAC Sniffing + Storage
- Beacon + Packet/MAC Spoofing
- Device Recognition
- Cloud (AWS) data pipeline

Thomas

- **Signals and Systems**
- MLE Localization from PDoA, ToF
- ToF measurement
- Time of Flight/SIFS smoothing
- IMU Fusion
- Multipath management

Schedule

- 5 weeks development
- 1 week testing
- 3 weeks refinement
- 1 week testing



WiSpider		0%
▾ Development		0%
Antenna Selection	Anish	0%
Laptop AX200 Setup	Anish	0%
PicoScenes Running on AX200	Anish	0%
Lightweight ToF Storage	Anish	0%
Spectrum Sensing	Anish	0%
MATLAB WIFI Toolset Bring-up	Thomas	0%
SIFS Jitter Smoothing	Thomas	0%
AoA/Multi-Antenna Directionality	Thomas	0%
Multi-Path Detection	Thomas	0%
Multi-path elimination	Thomas	0%
MLE Localization - No Movement	Thomas	0%
PicoScenes Bring Up	Ethan	0%
PicoScenes Measurement Script	Ethan	0%
MAC + Beacon Spoofing	Ethan	0%
MAC Sniffing + Address Collection	Ethan	0%
Channel Sensing with PicoScense	Ethan	0%
MATLAB/Cloud Pipeline	Ethan	0%
⊕ Task | Milestone | Group of Tasks		
▾ Refinement		0%
AX200 Integrated with Raspberry Pi CU4	Anish	0%
RaspberryPi Data Uplink	Anish	0%
Self-localization in ARKit	Anish	0%
Fusion of IMU with WiFi data	Thomas	0%
MLE Localization - Movement	Thomas	0%
AR App	Thomas Horton King	0%
ARKit/Phone data streaming	Ethan	0%
MAC Manufacturer LUT	Ethan	0%
Data/Packet Rate Device Identification	Ethan	0%
Other Identification	Ethan	0%
⊕ Task | Milestone | Group of Tasks		
▾ Testing		0%
Initial Testing	All	0%
Final Testing	All	0%
Slack	All	0%
⊕ Task | Milestone | Group of Tasks		
▾ Organizational		0%
Interim Demo		□
Final Presentation		□
Design Document		□
Design Presentation		□

Prior Works / Competitors

Paper	Contributions
Polite WiFi	Ping any Wi-Fi device using fake MAC, and get response
Wi-Peep	Non-cooperative drone-based localization of WiFi devices using ToF: Attacker perspective, built off of Polite WiFi
Lumos	Identify and locate hidden IoT devices using a rooted phone
PicoScenes	OSS framework for WiFi CSI and metadata collection