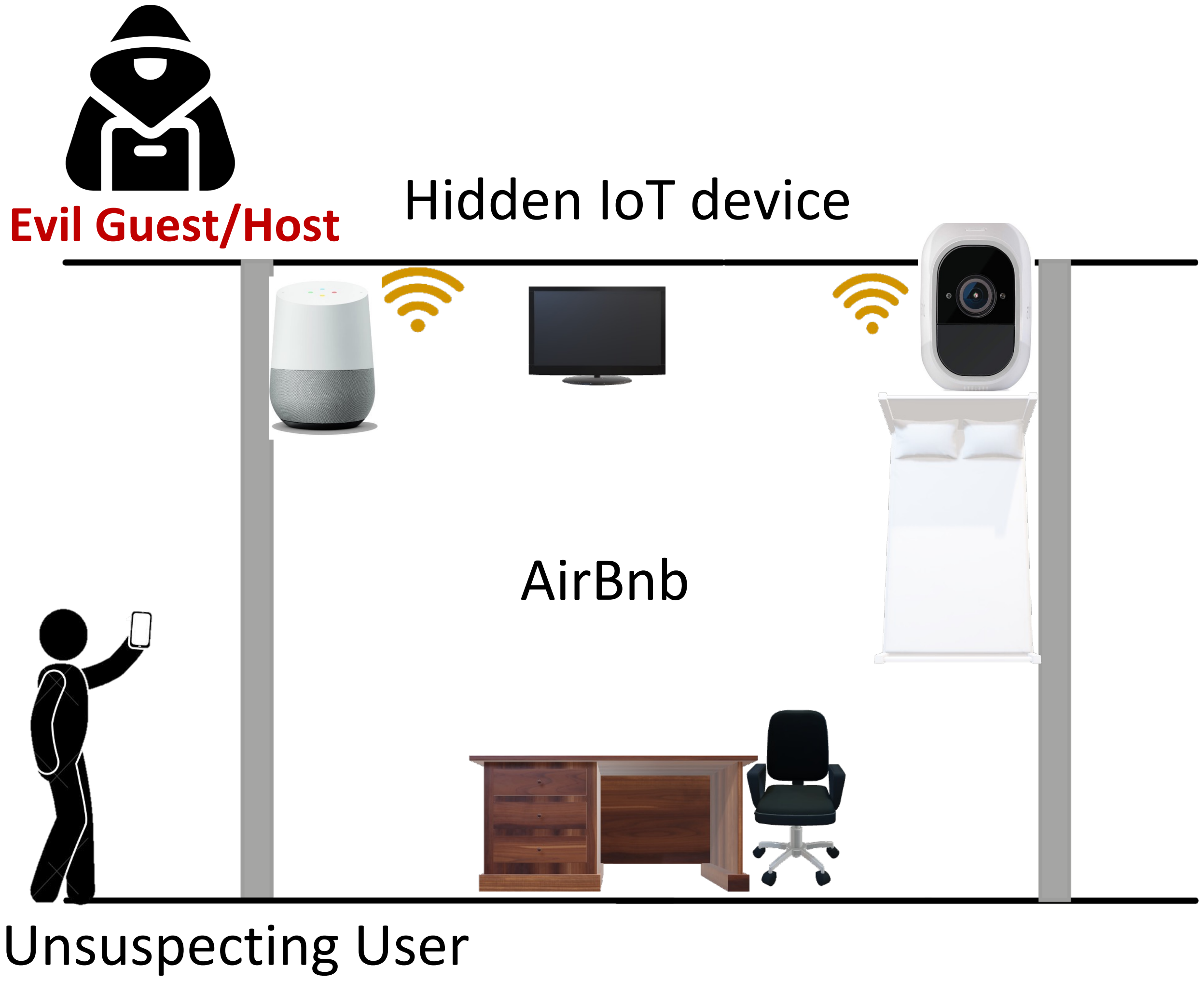
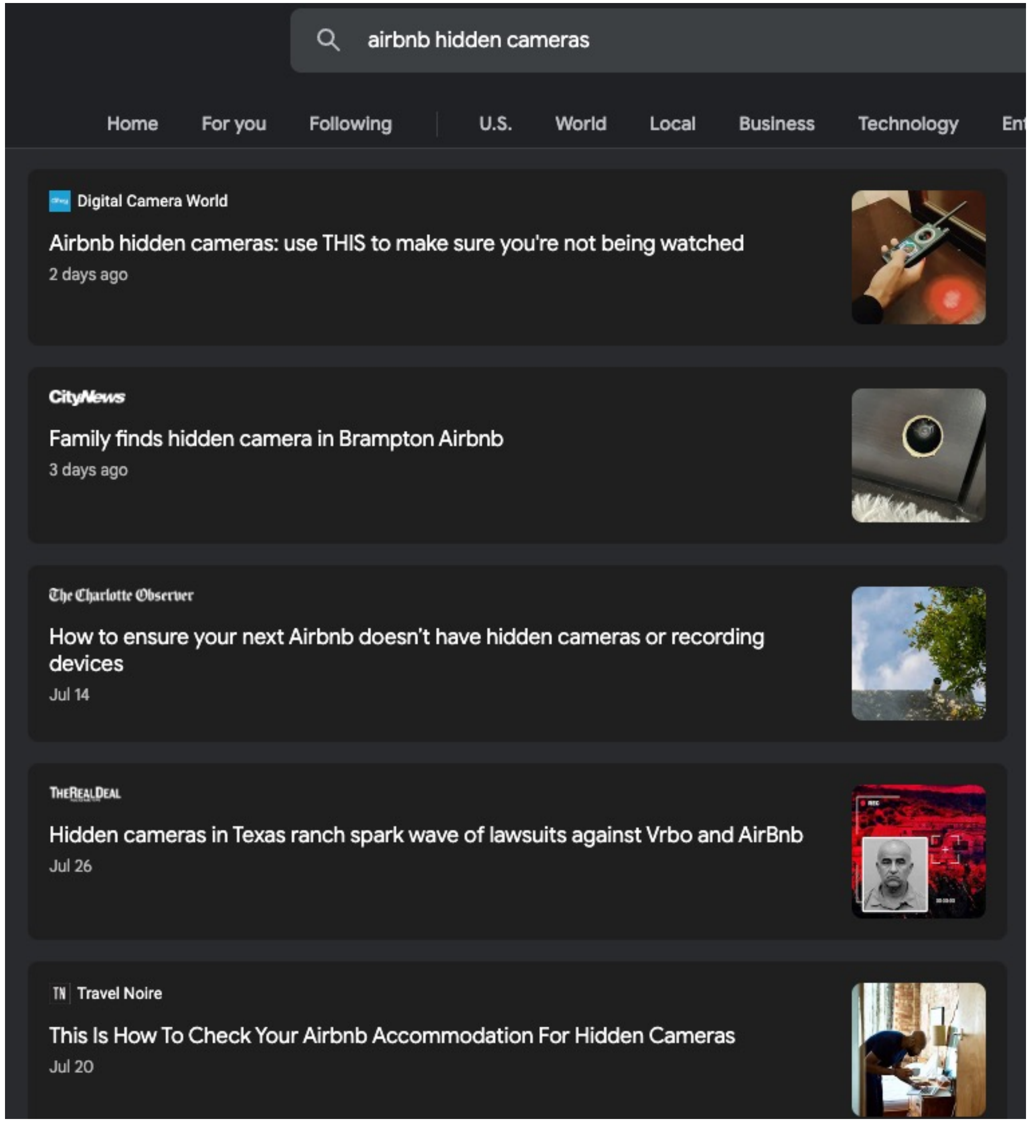
Lumos: Identifying and Localizing Diverse Hidden IoT Devices in an Unfamiliar Environment

Rahul Anand Sharma

Elahe Soltanaghaei*, Anthony Rowe and Vyas Sekar
Carnegie Mellon University, UIUC*

Evil Guest/Host attacks in an Airbnb





Digital Camera World
Airbnb hidden cameras: use THIS to make sure you're not being watched
2 days ago

CityNews
Family finds hidden camera in Brampton Airbnb
3 days ago

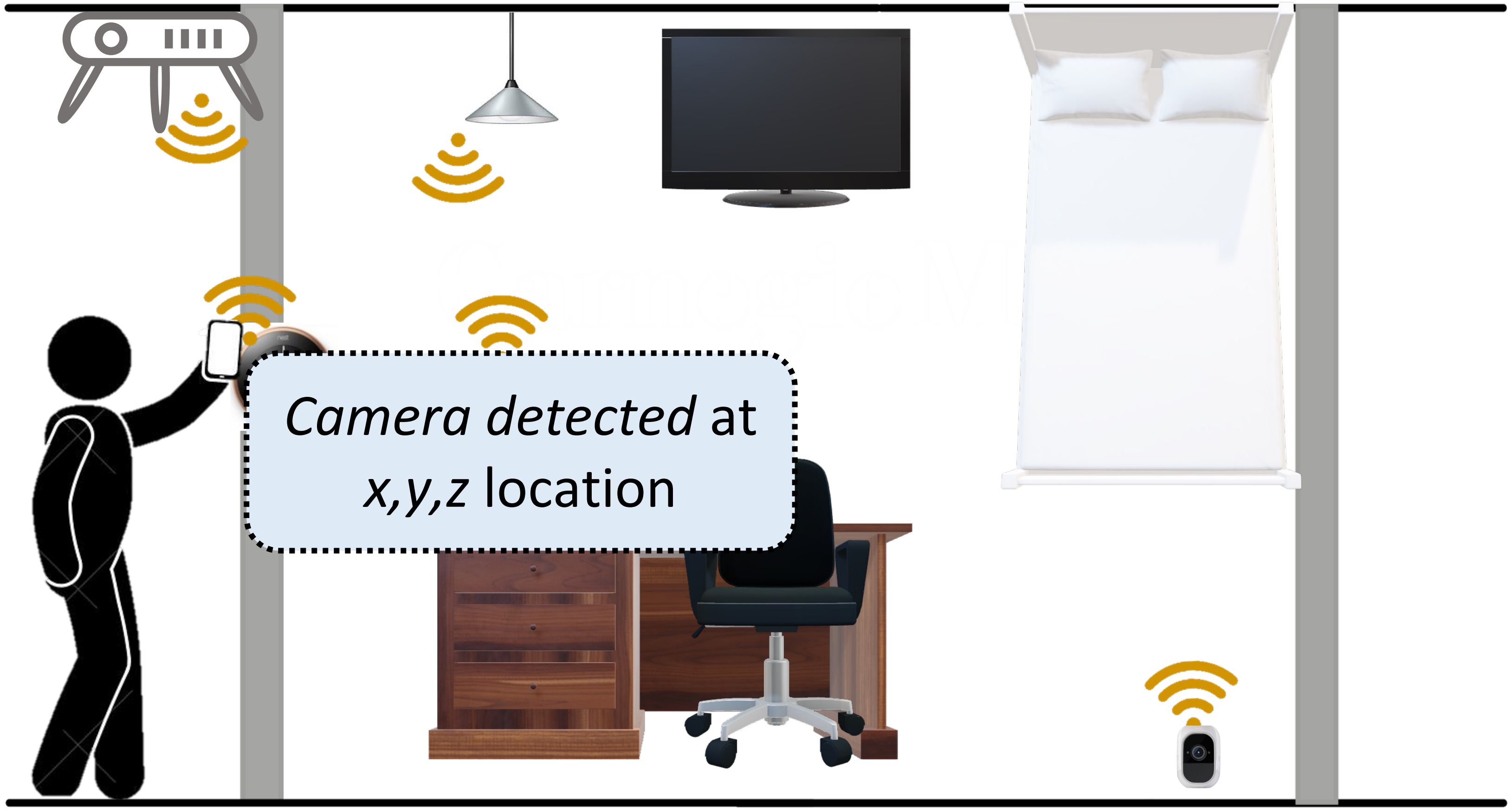
The Charlotte Observer
How to ensure your next Airbnb doesn't have hidden cameras or recording devices
Jul 14

TheRealDeal
Hidden cameras in Texas ranch spark wave of lawsuits against Vrbo and AirBnb
Jul 26

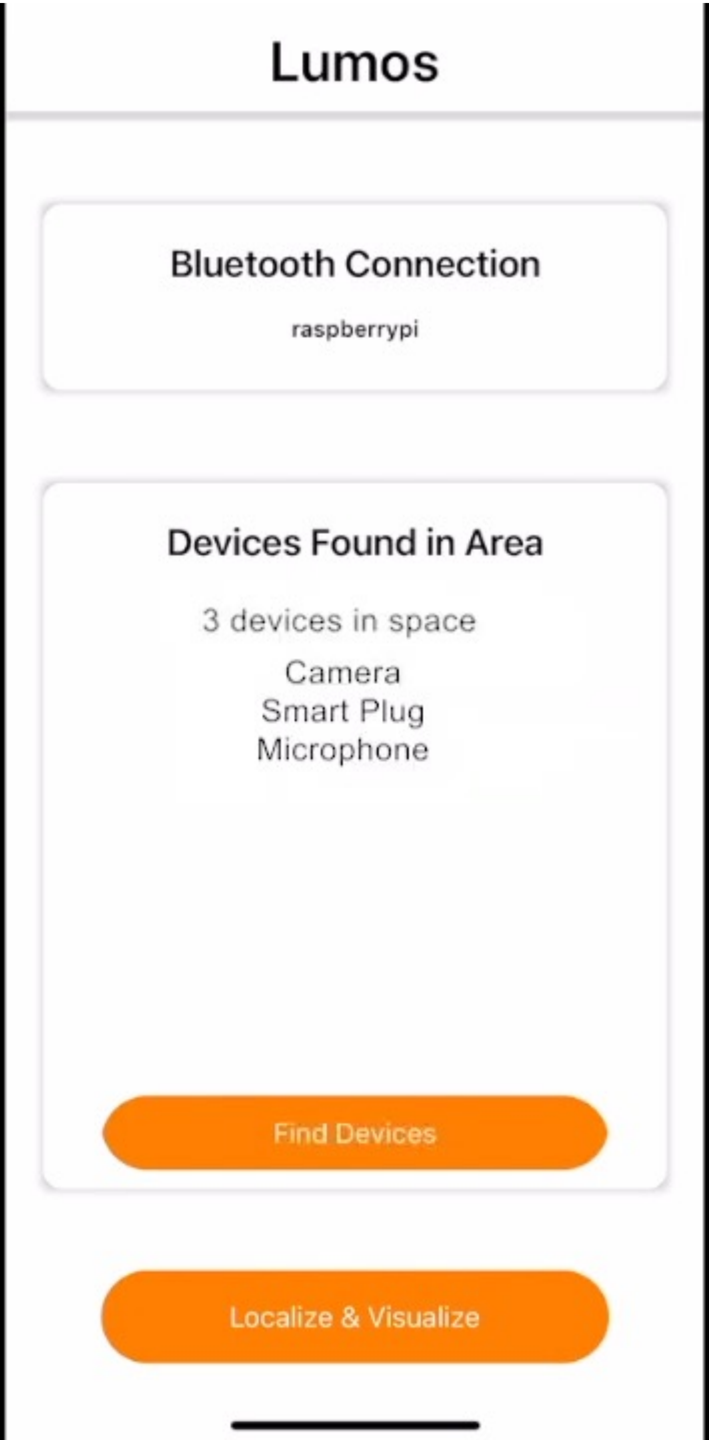
Travel Noire
This Is How To Check Your Airbnb Accommodation For Hidden Cameras
Jul 20

Source: Google News - Search

We would like to detect, identify and localize IoT devices



Camera detected at *x,y,z* location



Lumos

Bluetooth Connection

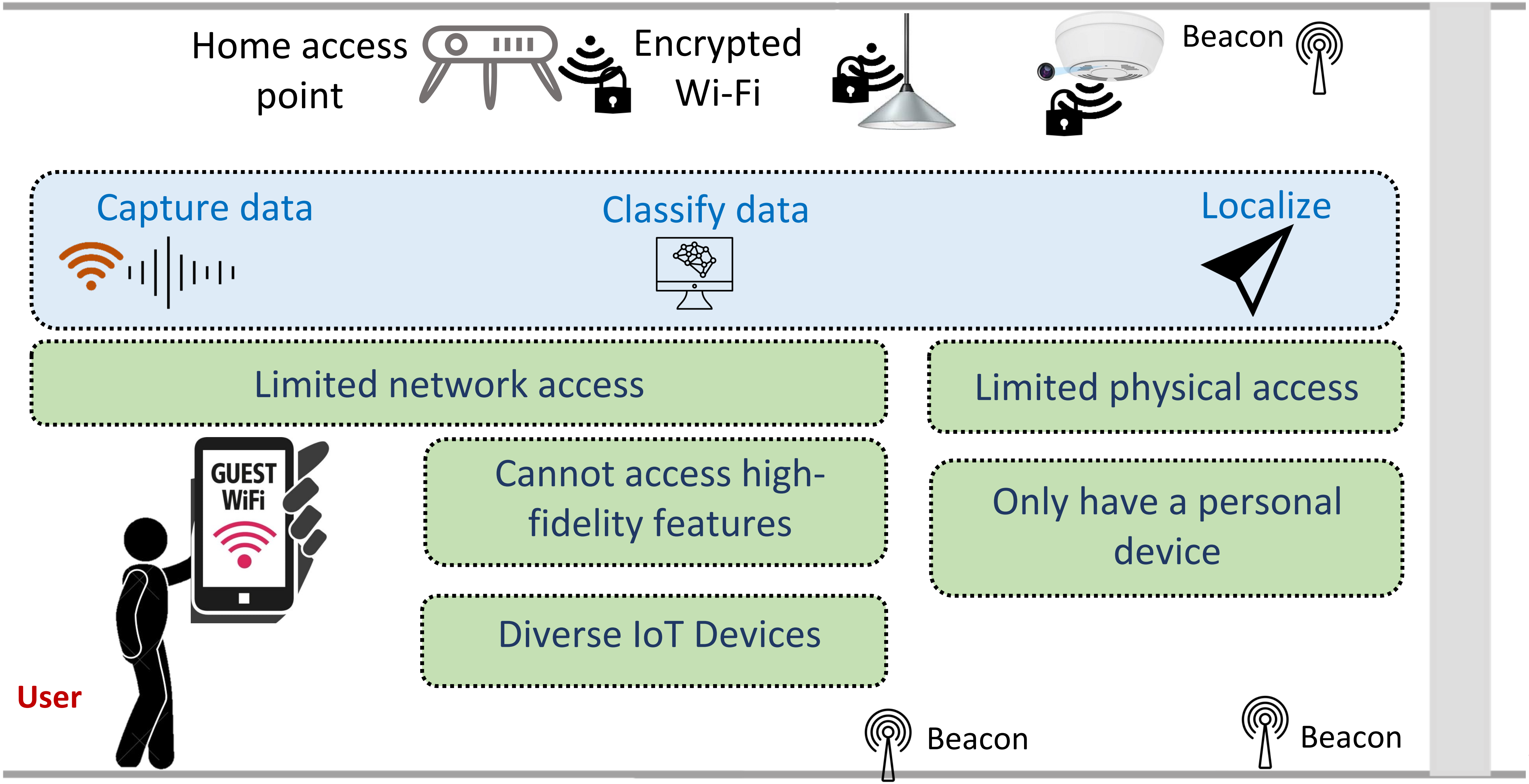
raspberrypi

Devices Found in Area

3 devices in space

Camera
Smart Plug
Microphone

Challenges: limited access + diverse devices



Home access point

Encrypted Wi-Fi

Beacon

Capture data

Classify data

Localize

Limited network access

Limited physical access

Cannot access high-fidelity features

Only have a personal device

Diverse IoT Devices

User

Beacon

Beacon

Lumos vs prior work

Approach	**Handheld**	**Limited N/W access**	**Diverse IoT devices**	**Localization**
Bug Finder	✗	✓	✗	✓
Camera Detectors	✓	✓	✗	✓
N/W traffic at the router	✓	✗	✓	✗
Lumos	✓	✓	✓	✓

Lumos: Innovations

Capture data

Classify data

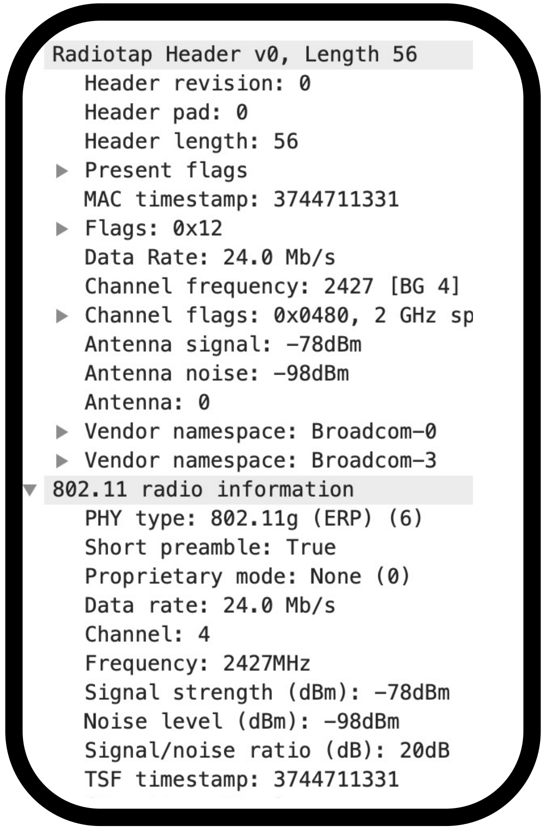
Localize

- □ A greedy multi armed bandit approach that uses packet arrival time estimates to pick what channel to sense and for how long

- □ A new feature extraction and classification algorithm by just using coarse attributes at Wi-Fi 802.11 layer

- □ An algorithm to localize IoT devices by correlating a user’s motion with RSSI of sniffed packets

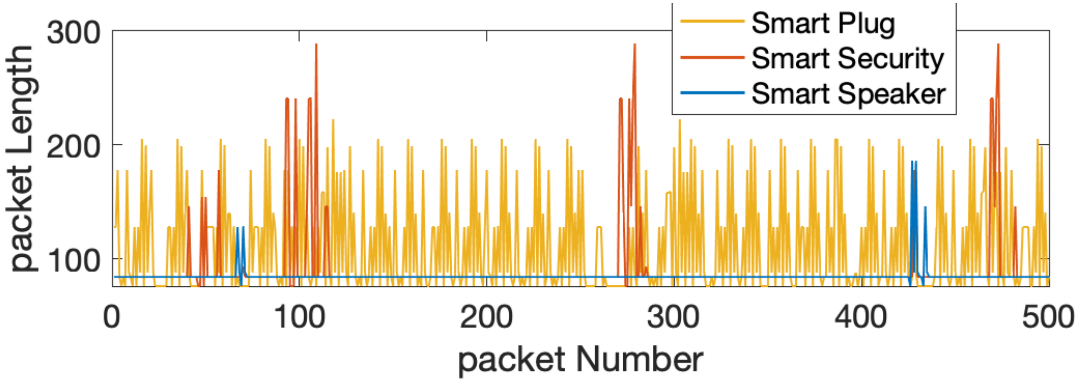
Insight 1: Even coarse attributes have signals



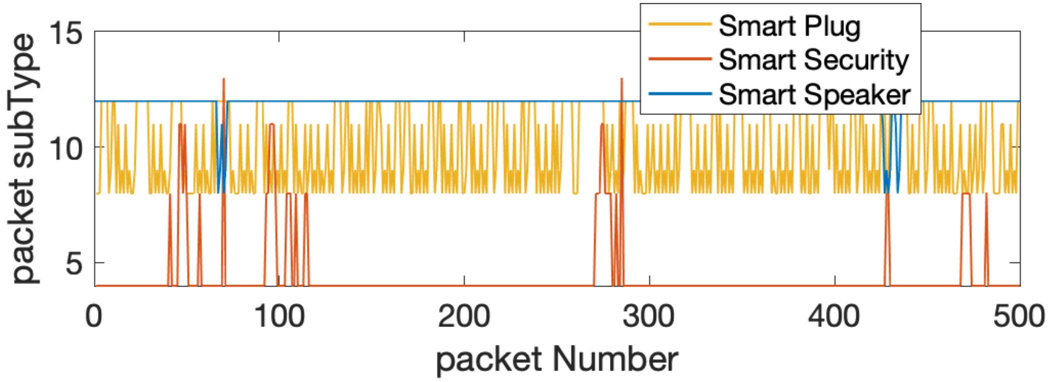
```
  Radiotap Header v0, Length 56
    Header revision: 0
    Header pad: 0
    Header length: 56
  ▶ Present flags
    MAC timestamp: 3744711331
  ▶ Flags: 0x12
    Data Rate: 24.0 Mb/s
    Channel frequency: 2427 [BG 4]
  ▶ Channel flags: 0x0480, 2 GHz sp
    Antenna signal: -78dBm
    Antenna noise: -98dBm
    Antenna: 0
  ▶ Vendor namespace: Broadcom-0
  ▶ Vendor namespace: Broadcom-3
▼ 802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: True
    Proprietary mode: None (0)
    Data rate: 24.0 Mb/s
    Channel: 4
    Frequency: 2427MHz
    Signal strength (dBm): -78dBm
    Noise level (dBm): -98dBm
    Signal/noise ratio (dB): 20dB
    TSF timestamp: 3744711331
```

Sample 802.11 Packet

Popular fingerprinting feature, packet length varying with device

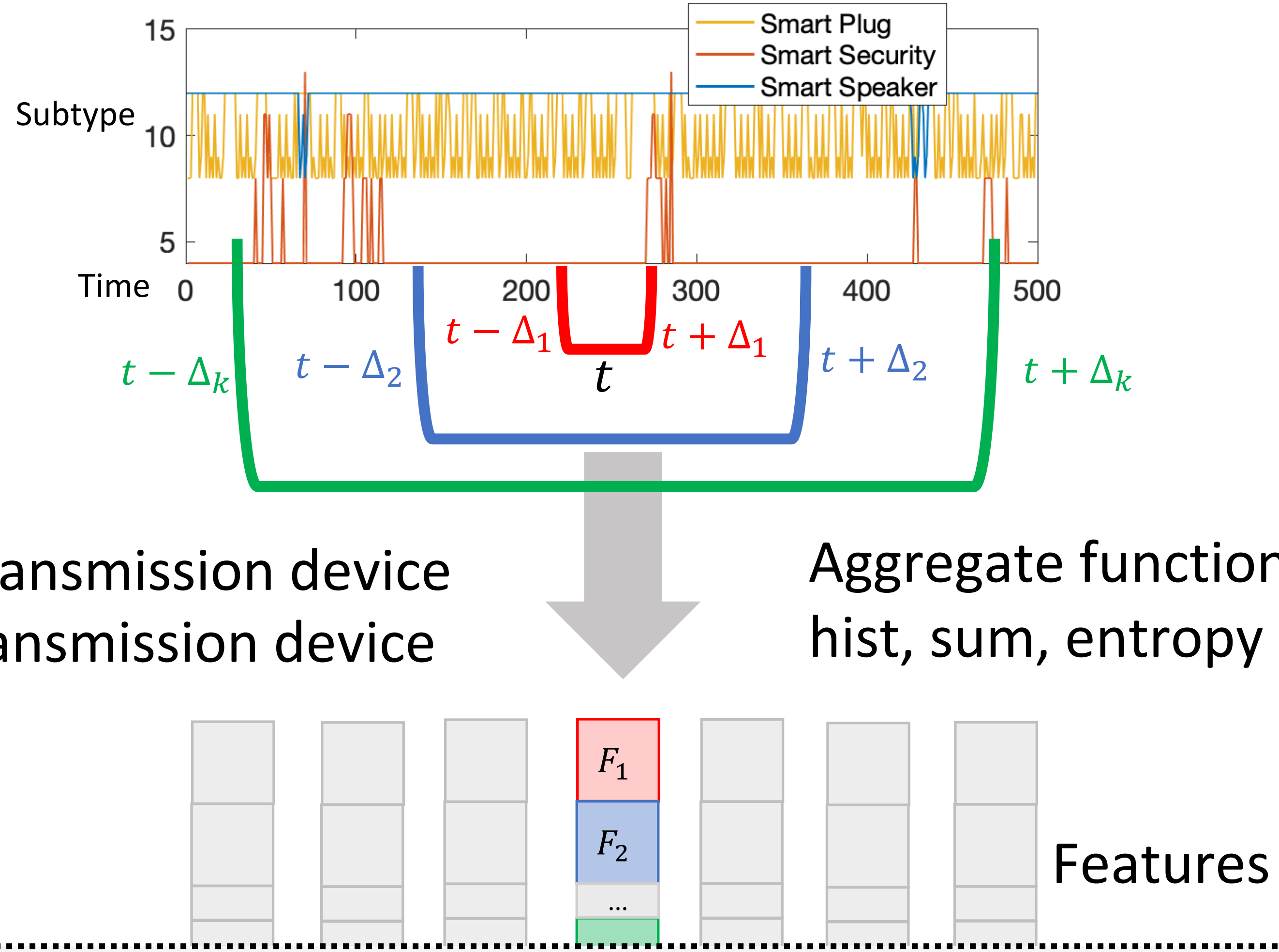


802.11 specific attribute, packet subtype varying with device



Approach: Extract **broadest** observable feature set (all headers)

Insight 2: Multi-time resolution can handle diverse IoT devices



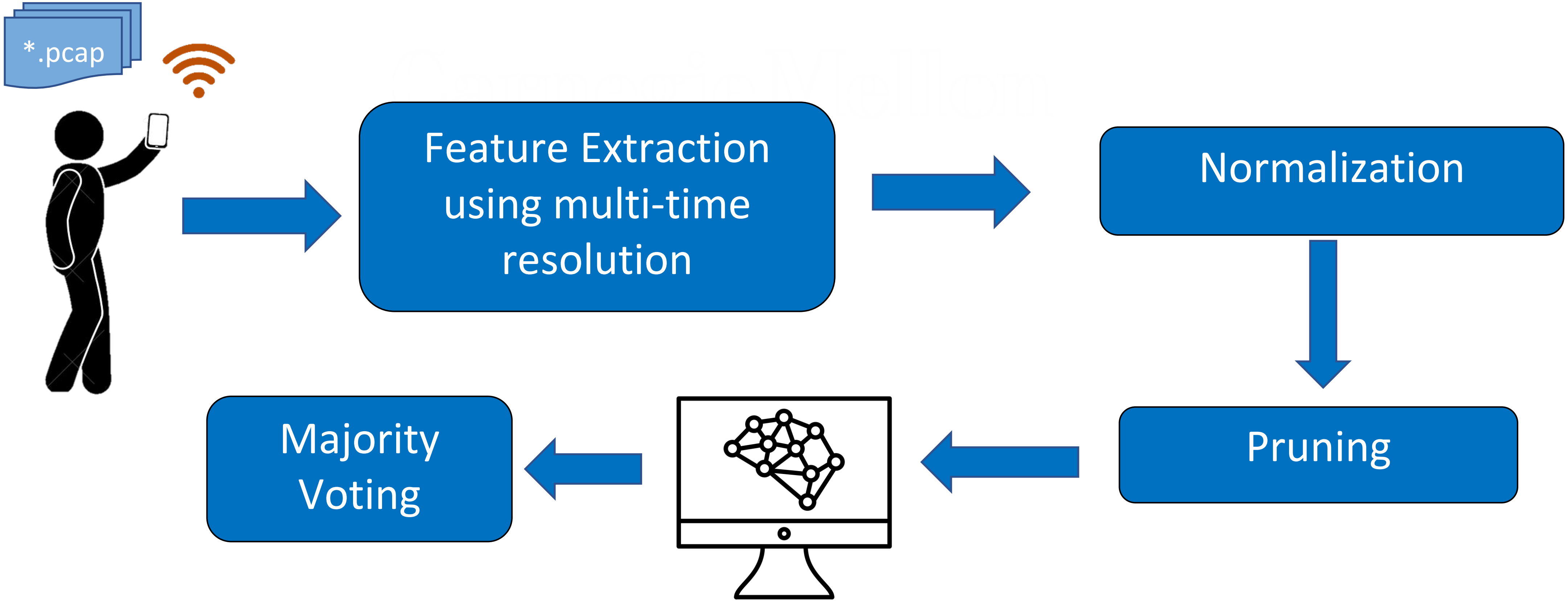
Small Δ_1 for high-transmission device
Large Δ_1 for low-transmission device

Aggregate functions (mean, hist, sum, entropy etc.)

Approach: Allow **multiple** aggregation windows for feature extraction

Workflow of Lumos device classification

Sniffed encrypted Wi-Fi 802.11 packets



*.pcap

Feature Extraction using multi-time resolution

Normalization

Pruning

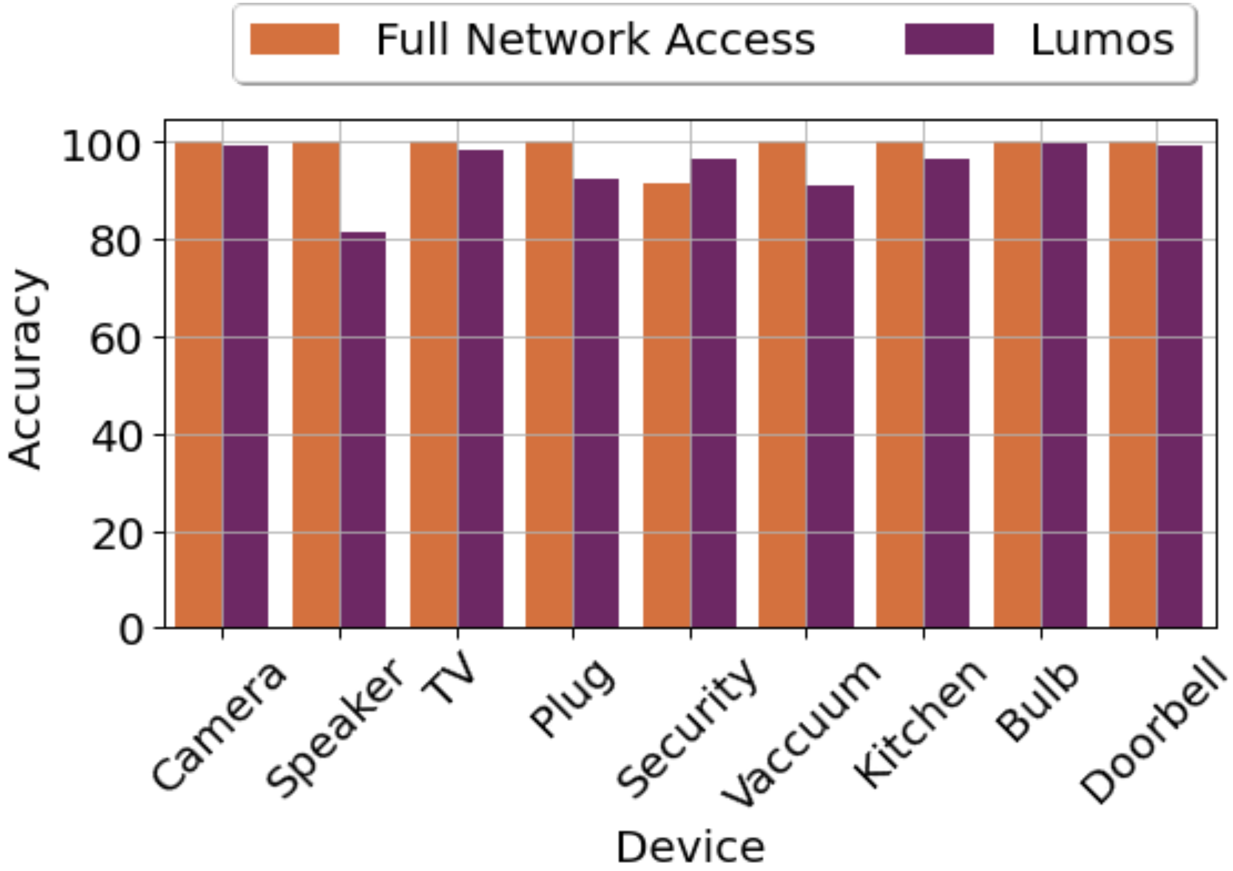
One-vs-Rest ML Classifier

Majority Voting

Evaluation: Setup (44 IoT Devices)

Category	Devices
Camera	Nest, Canary, Ring, Blink, EZVIZ, TP Link KC100, TP Link KC120, D-Link, Geeni, NightOwl, HidvCam, OVEHEL, LookCam, MiniSpy, AlphaTech
Doorbell	Nest Doorbell, Kangaroo, Ring
Security	Simplisafe, ADT, Ring
TV	Vizio, Panasonic, TCL
Microphones	Google Home, Amazon Echo, SONOS, Amazon Show, Apple HomePod, Lenovo Smartclock
Plug	Amazon, Wemo, TP Link, Jinvoo Smartplug, Gosund Power-strip, TP Link Power-strip
Kitchen	Anova Cooker, iKettle
Bulb	Wiz1, Wiz2, Wiz3, Wiz4
Vacuum	Roomba & Deebot

Lumos can achieve comparable accuracy to methods assuming full network access



Full Network Access: “Sivanathan, A et. Al . “Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics.” *IEEE Transactions on Mobile Computing* (August 2019)”

Limitation & Future Work

- Sniffing 802.11 packets is disabled by manufacturers
- An expert attacker could modify the device behavior to evade detection
- Extend to other wireless technologies

Conclusions

Lumos: In 30 minutes it can identify devices with 95% accuracy in a 1000 Sq. Ft. apartment and localize them with a median error of 1.5m

- ❑ Data capturing with limited a priori knowledge
- ❑ Device classification with limited features
- ❑ Localization with no infrastructure support

GitHub https://github.com/rahul-anand/Lumos

Email : rahulans@cmu.edu
Website: https://rahul-anand.github.io/