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

Evil Guest/Host

Hidden IoT device

AirBnb

Unsuspecting User

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

Find Devices

Localize & Visualize
Challenges: limited access + diverse devices

- Capture data
  - Limited network access
  - Cannot access high-fidelity features
  - Diverse IoT Devices

- Classify data
  - Encrypted Wi-Fi

- Localize
  - Limited physical access
  - Only have a personal device

- Home access point
- Beacon
- Beacon
- User
## Lumos vs prior work

<table>
<thead>
<tr>
<th>Approach</th>
<th>Handheld</th>
<th>Limited N/W access</th>
<th>Diverse IoT devices</th>
<th>Localization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bug Finder</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Camera Detectors</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>N/W traffic at the router</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Lumos</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Lumos: Innovations

- 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

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

Sample 802.11 Packet

**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 [8G 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

Popular fingerprinting feature, packet length varying with device

802.11 specific attribute, packet subtype varying with device
Insight 2: Multi-time resolution can handle diverse IoT devices

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

Small $\Delta_1$ for high-transmission device
Large $\Delta_1$ for low-transmission device

Approach: Allow multiple aggregation windows for feature extraction
Workflow of Lumos device classification

Sniffed encrypted Wi-Fi 802.11 packets

Feature Extraction using multi-time resolution

Normalization

Pruning

One-vs-Rest ML Classifier

Majority Voting
## Evaluation: Setup (44 IoT Devices)

<table>
<thead>
<tr>
<th>Category</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Nest, Canary, Ring, Blink, EZVIZ, TP Link KC100, TP Link KC120, D-Link, Geeni, NightOwl, HidvCam, OVEHEL, LookCam, MiniSpy, AlphaTech</td>
</tr>
<tr>
<td>Doorbell</td>
<td>Nest Doorbell, Kangaroo, Ring</td>
</tr>
<tr>
<td>Security</td>
<td>Simplisafe, ADT, Ring</td>
</tr>
<tr>
<td>TV</td>
<td>Vizio, Panasonic, TCL</td>
</tr>
<tr>
<td>Microphones</td>
<td>Google Home, Amazon Echo, SONOS, Amazon Show, Apple HomePod, Lenovo Smartclock</td>
</tr>
<tr>
<td>Plug</td>
<td>Amazon, Wemo, TP Link, Jinvoo Smartplug, Gosund Power-strip, TP Link Power-strip</td>
</tr>
<tr>
<td>Kitchen</td>
<td>Anova Cooker, iKettle</td>
</tr>
<tr>
<td>Bulb</td>
<td>Wiz1, Wiz2, Wiz3, Wiz4</td>
</tr>
<tr>
<td>Vacuum</td>
<td>Roomba &amp; Deebot</td>
</tr>
</tbody>
</table>
Lumos can achieve comparable accuracy to methods assuming full network access.

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](https://github.com/rahul-anand/Lumos)

Email: rahulans@cmu.edu
Website: [https://rahul-anand.github.io/](https://rahul-anand.github.io/)