SecurePlug: Detecting and Mitigating Behavioral Inference from Smart Home IoT Traffic Metadata

Jordy M. Rodríguez De Gracia
Advisor: Dr. Jeffrey Duffany
Graduate Project EXPO, May 2026

ABSTRACT

Smart home devices encrypt their cloud communications, but traffic metadata like timing patterns, packet frequency, and protocol cadence leaks occupant routines onto the local network. This project demonstrates that behavioral inference from IoT metadata is achievable in a real residential setting, then neutralizes it with SecurePlug: a Raspberry Pi Zero 2 deployed as an in-network privacy shield.

A pre-deployment capture from five commercial devices revealed that iHome smart plugs broadcast UDP heartbeats at a near-constant 1.7-second cadence, and that WiZ smart bulbs transmit mDNS bursts containing device fingerprints in plaintext on every state change. A Python inference pipeline reconstructed the occupant's daily routine with 75% confidence, without decrypting a single payload. SecurePlug eliminates departure detection across all four post-shield days and reduces behavioral event count by 64%.

INTRODUCTION

Nowadays, we might have used or installed some sort of smart home devices to better our way of living. Smart home usage has expanded at a faster pace, but on some occasions the security expectations set in these products rarely match the reality of residential network environments. Companies may have addressed payload privacy, most devices communicate via TLS or proprietary encrypted channels, but traffic metadata remains largely unprotected. This type of vulnerability can be troubling, because it is invisible to the homeowner and requires no exploitation of the device itself. Just an attacker with passive access to the Wi-Fi network sees enough.

THREAT MODEL & BACKGROUND

Adversary: Passive observer with local Wi-Fi access (neighbor, compromised device, or ISP monitoring broadcast traffic). No payload decryption required in Ren et al. [8] confirm this is sufficient for behavioral inference.
Target: Occupant's daily routine (wake-up, departure, arrival, sleep). Acar et al. [7] document that this information class enables burglary planning, stalking, and insurance fraud.
Key finding: No MQTT plaintext found in any capture, all devices used TLS or UDP. Metadata alone reconstructs routines.
When researching network traffic analysis of IoT devices, there is an established research history on the topic:
[1] Apthorpe et al.: A passive Wi-Fi observer can infer device states and user actions through simple traffic rate analysis
[2–3] Sivanathan et al.: Temporal regularity is the primary distinguishing factor in IoT behavioral classification.
[4] Dong et al.: Local mDNS exposes device identity to any device on the same network segment.
[6] Bezawada et al.: Traffic shaping meaningfully degrades inference accuracy; this is SecurePlug's core defense principle.
[7–8] Acar, Ren et al.: Metadata exposure holds even when encryption is correctly applied.

EXPERIMENTAL SETUP

Testbed: Real residential home network (192.168.0.x subnet), Arris router
Devices: 2× iHome Flow smart plugs, 2× Philips WiZ LED bulbs, 1× TP-Link KL125 smart plug.
Capture tool: Wireshark 4.2.4 on Windows laptop; analysis in Python 3.13.5.
Phase 1 (Before): No shield active. Phase 2 (After): Shield running.
Both phases used identical inference pipeline for fair comparison.

PRE-SHIELD TRAFFIC FINDINGS

iHome UDP Heartbeat Pattern
Both plugs broadcast to 255.255.255.255:6667 at 1.7-second intervals, alternating turns in predictable sequence. 69,468 packets over 48 hours, 99.4% of all captured traffic. Timing variance: ~0.001 s (clock like precision).
WiZ mDNS Burst Fingerprinting
Every bulb on/off fires an mDNS burst to 224.0.0.251:5353, carrying MAC address, IP, model ID, and Matter protocol metadata in plaintext. Any device listening on the subnet receives a timestamped log of every state change, zero effort required.
Behavioral Inference Rules (infer_behavior.py)

- Wake-up: First WiZ mDNS cluster in 5–11 AM window.
- Departure: All devices quiet ≥60 min during daytime.
- Arrival: WiZ burst cluster after afternoon silence.
- Sleep: Last WiZ mDNS cluster of the night.

INFERRED ROUTINE — BEFORE SHIELD

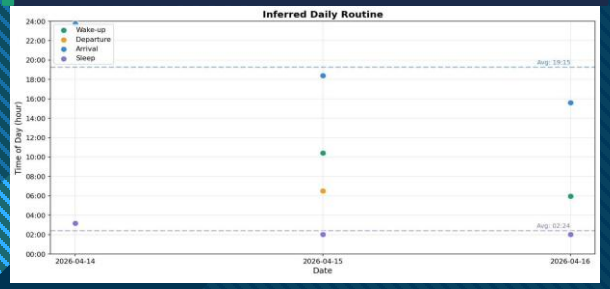

Figure 1. Inferred daily routine (before shield). Each dot represents a detected behavioral event. Departure is prominent on April 15.

28	75%	1/1
Behavioral Events	Inference Confidence	Departure Detected

The departure event on April 15 is the most significant result from this phase. A continuous 88-minute gap with no device activity during daytime hours was enough for the algorithm to flag it as a departure with HIGH confidence

SECUREPLUG: THREE-LAYER PRIVACY SHIELD

Hardware: Raspberry Pi Zero 2 W deployed as in-network shield between devices and router. Runs as a systemd service (Restart=always), no SSH session required.
Layer 1: iHome Heartbeat Jitter
Binds to 0.0.0.0:6667. Intercepts every UDP broadcast from iHome plugs and re-emits each packet after a random delay of 0.5–3.0 seconds. Payload is preserved byte-for-byte; only timing changes. Raises iHome timing variance by 2,500×.
Layer 2: WiZ Heartbeat Jitter
Applies identical jitter logic to WiZ heartbeats on port 38900 (broadcast to 192.168.0.255). 146 WiZ heartbeats intercepted and reshuffled over 55 hours.
Layer 3: WiZ mDNS Burst Suppressor
Pi joins multicast group 224.0.0.251 via IP_ADD_MEMBERSHIP, becoming the primary recipient of all mDNS traffic. Any packet from a WiZ source IP is received and dropped MAC address, IP, model ID, and Matter metadata never reach any other device. 337 mDNS bursts suppressed; 74,881 iHome packets intercepted over 55 hours.

Layer 1 iHome Jitter	Layer 2 WiZ Jitter	Layer 3 mDNS Drop
Port 6667	Port 38900	Port 5353
0.5–3.0s delay	0.5–3.0s delay	Multicast join
2,500× variance	146 intercepted	337 suppressed

INFERRED ROUTINE — AFTER SHIELD (DEPARTURE: UNDETECTED)

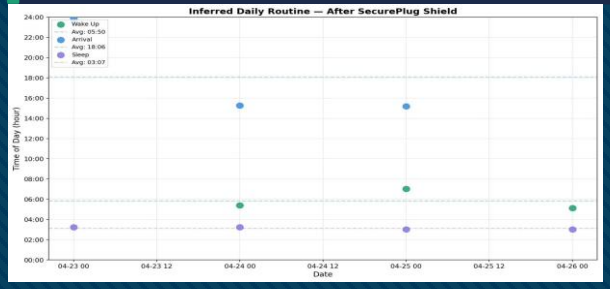

Figure 2. Inferred daily routine (after shield). Departure is absent from all four days. Wake-up and sleep show more variation.

10	62%	0/4
Behavioral Events	Inference Confidence	Departure Detected

WiZ Bulb 2 experienced intermittent Wi-Fi disconnections during the capture. During those reconnection events the bulb transmitted mDNS announcements before the shield socket could intercept them, accounting for 343 packets that appear in Wireshark despite the suppressor being active, this is a known limitation.

RESULTS: BEFORE VS. AFTER SHIELD

Table 1. Comparison of behavioral inference metrics before and after SecurePlug.

Metric	Before	After	Change
Inference confidence	75%	62%	↓ 17%
Behavioral events	28	10	↓ 64%
Departure detected	1/1 days	0/4 days	✓ Eliminated
iHome timing variance	~0.001 s	~2.5 s	↑ 2,500×
mDNS bursts (WiZ)	Plaintext	337 suppressed	✓ Blocked
iHome pkts intercepted	—	74,881	100%

Primary Success Metric: Departure was ELIMINATED, undetected across all 4 after-shield days (0/4), compared to 1/1 detected before the shield. Overall accuracy metrics alone understate this result due to WiZ_1 connectivity instability inflating some after-shield event counts.

CONCLUSIONS

SecurePlug proves that behavioral inference from IoT traffic metadata is achievable in a real home network and that it can be stopped with hardware anyone can buy.

- Before-shield: 75% inference confidence; daily routine fully reconstructed; departure detected.
- After-shield: Departure eliminated (0/4); behavioral events ↓64%; confidence ↓ to 62%.

Limitations: WiZ_1 mDNS interception was inconsistent during reconnection events (343 packets escaped); sleep inference imprecision due to residual Wi-Fi activity. Shield was validated against passive observers only.

FUTURE WORK

- Adaptive jitter: dynamically adjusts delay range based on detected inference attempts.
- Broader protocol coverage: extend suppression beyond mDNS to cover additional discovery protocols.
- Browser-based configuration UI: non-technical deployment without SSH access.

ACKNOWLEDGEMENTS

I would like to acknowledge Dr. Jeffrey Duffany, professor at the Computer Science & Engineering department, Lizbeth Hernández for guiding me and providing feedback throughout this work, and Bárbara Sweet Hansen for taking the time to review the article for this project.

REFERENCES

[1] Apthorpe et al., PETS 2017 [2] Sivanathan et al., IEEE TMC 2019
[3] Sivanathan, PhD Thesis UNSW 2020 [4] Dong et al., ACM ASIA CCS 2020
[5] Gharakheili et al., ACM Trans IoT 2023 [6] Bezawada et al., ACM ASHES 2018
[7] Acar et al., ACM IMC 2018 [8] Ren et al., ACM IMC 2019