Et Tu Alexa?
When Commodity WiFi Devices Turn into Adversarial Motion Sensors

Yanzi Zhu*, Zhujun Xiao, Yuxin Chen, Zhijing Li*, Max Liu, Ben Y. Zhao, Heather Zheng

University of Chicago, *UC Santa Barbara
Smart Devices are Everywhere

- Smart Home
- Smart Factory
- Smart Office
Attacks Enabled by Smart Devices

1. Hack the device
2. Hack the network
3. Network traffic analysis

This paper
A new form of attack via passive WiFi signal analysis
Silent Reconnaissance Attack

Continuous motion tracking:
- **13:35:00** move in server room
- **13:45:00** leave server room
- **13:45:20** move in private office
- **13:55:20** leave private office
Silent Reconnaissance Attack

Reconnaissance attack via listening to (w/o decoding) WiFi signals
Leveraging Two Facts

(1) Smart devices are filling our home/office/factory; each room has multiple devices.

(2) Smart devices transmit WiFi data regularly.

```
| Device | Packets sent per second |
|--------|-------------------------|
|        | Active | Idle |
| TV     | 200    | 6.64 |
| ≥ 3.33 | ≥ 2.44 |
| ≥ 16   | ≥ 0.5  |
| 257    | 28.6   |
|        |
```
Human Motion is “Embedded” in Ambient WiFi Signals

Ambient WiFi signals fluctuate when humans move.

Sniffer captures such fluctuation.

**Threat model:**
1. Non-intrusive
2. Undetectable
Outline

Introduction

Silent Reconnaissance Attack

Attack Implementation & Real-world Evaluation

Defense
How is Human Motion Embedded in WiFi Signals

Anchors (motion sensor)

WiFi Device A

Sniffer

sniffer’s received signal of A

Large signal variation indicates human motion.

motion

time
Measure Signal Variation via CSI

Our solution: leverage Channel State Information (CSI)
- CSI = signal strength at different sub-frequencies

1. Compute std for each sub-frequency
2. Average std across sub-frequencies

Our final metric
\( \sigma_{aCSI} \) Captures Human Motion

\( \sigma_{aCSI} \) can separate with and without human motion. \( \sigma_{aCSI} \) can tell human is moving towards or away from anchor.

\begin{itemize}
  \item \( \sigma_{aCSI} \) with motion
  \item moving away
  \item moving towards
\end{itemize}

\begin{itemize}
  \item without motion
\end{itemize}
Our Attack: End-to-end View

1. **Phase 1: bootstrapping**
   Identify and locate static WiFi devices to their individual rooms

2. **Phase 2: continuous monitoring**
   Human motion sensing by a static sniffer
Attack Implementation & Real-world Evaluation

Implementation
- Modified WiFi firmware to passively collect CSI
  - 1st to enable passive CSI collection of any commodity WiFi devices*

Experiments
- 11 homes & offices with various floorplans
- 31 WiFi devices & 5 volunteers

Measurements
- 41 hours of data (~8 hours of human motion)

*Previous work can not collect CSI continuously on commodity devices.
Attack is Effective

Human detection rate = \[ \frac{T(\text{attacker reports room has human inside})}{T(\text{room has human inside})} \]

False alarm rate = \[ \frac{T(\text{room does not have human inside})}{T(\text{attacker reports room has human inside})} \]

*LiFS: Low human-effort, device-free localization with fine-grained subcarrier information. MobiCom’16.*
Attack is Robust

How effective is our attack at low packet rate?
- Human detection rate drops only 1.5% when anchor transmits at 2 packets per second (pps), compared to full rate 11pps.

How about non-human sources of motion?

- Fans: No Impact
- Oscillating Fans: Distinguishable
- Pets: Similar to Human
Defense via Corrupting Attacker’s Received Signal

Observation: the effectiveness of this attack depends on **quantity** and **quality** of signals.

Reducing quantity
- WiFi rate limiting
- MAC randomization
- Geofencing

Reducing quality
- Signal obfuscation by smart devices
- Signal obfuscation by AP

Ineffective and/or impractical

Our defense
Our Proposal: AP-Based Obfuscation

**Spatial Obfuscation**

AP sends cover traffic on behalf of each smart device (using its MAC address).

**Temporal Obfuscation**

AP randomly vary power over time.
Our Proposal: AP-Based Obfuscation

Spatial Obfuscation

AP sends cover traffic on behalf of each smart device (using its MAC address).

Temporal Obfuscation

AP randomly vary power over time.

With defense, human detection rate drops significantly.
Conclusion

Undetectable silent reconnaissance attack
- No hacking needed, only passive WiFi signal analysis

Effective in real-world evaluations
- 11 homes/offices, 31 WiFi devices

New defenses
- AP-based obfuscation is effective

Thank you
Any questions?