Master Thesis |
Midtermpresentation

WiFi Relink: Analysis of Plaintext WiFi Sidechannels for Unique Device

Supervisors:
Prof. Dr. Bruno Rodrigues, Prof. Dr. Burkhard Stiller, Karim Khamaisi, Katharina O. E. Müller

26.10 2026 · Nils Grob

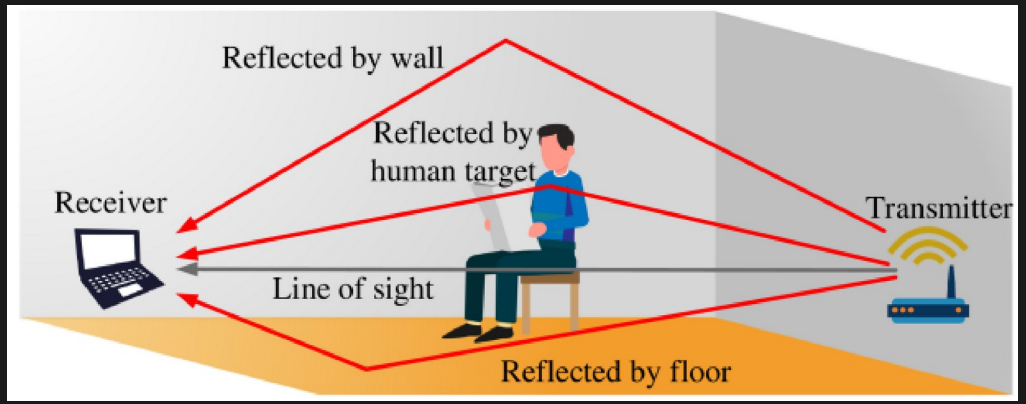
Agenda

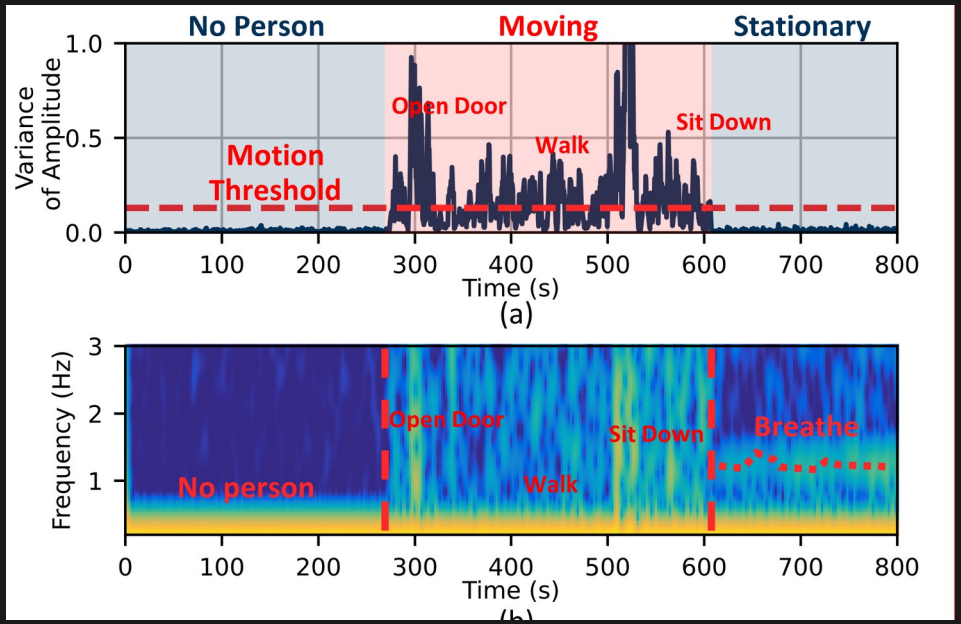
- Motivation
- Background
- Selected related work
- Design
- Preliminary results
- Outlook

Motivation

WiFi Sensing

- Occupancy, Activity Detection of Humans
- Identity Inference





Motivation

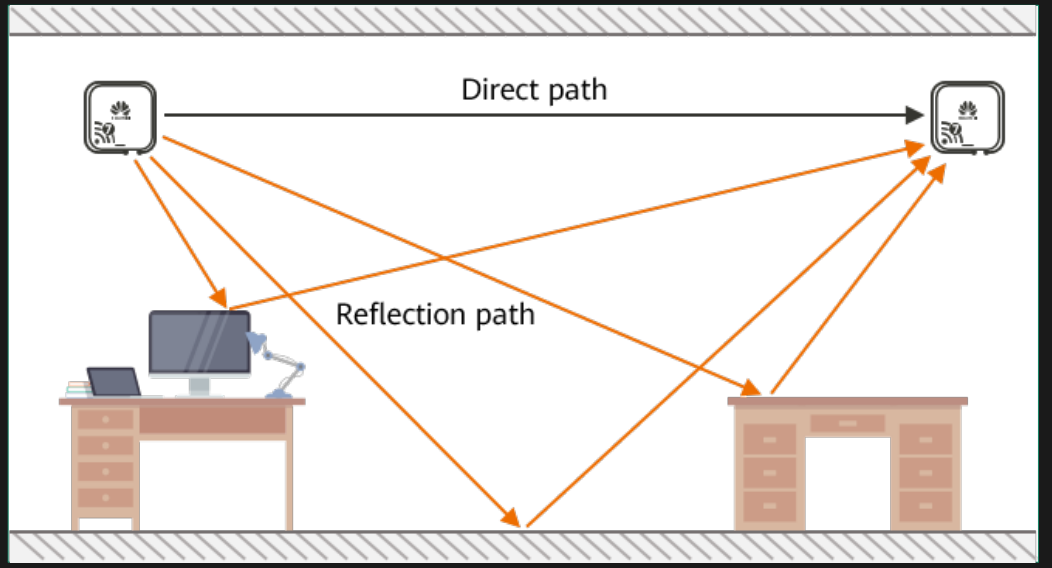
Thesis Aim

Apply WiFi Sensing side channels to relink devices which randomize their MAC address

Background

Channel State Information (CSI)

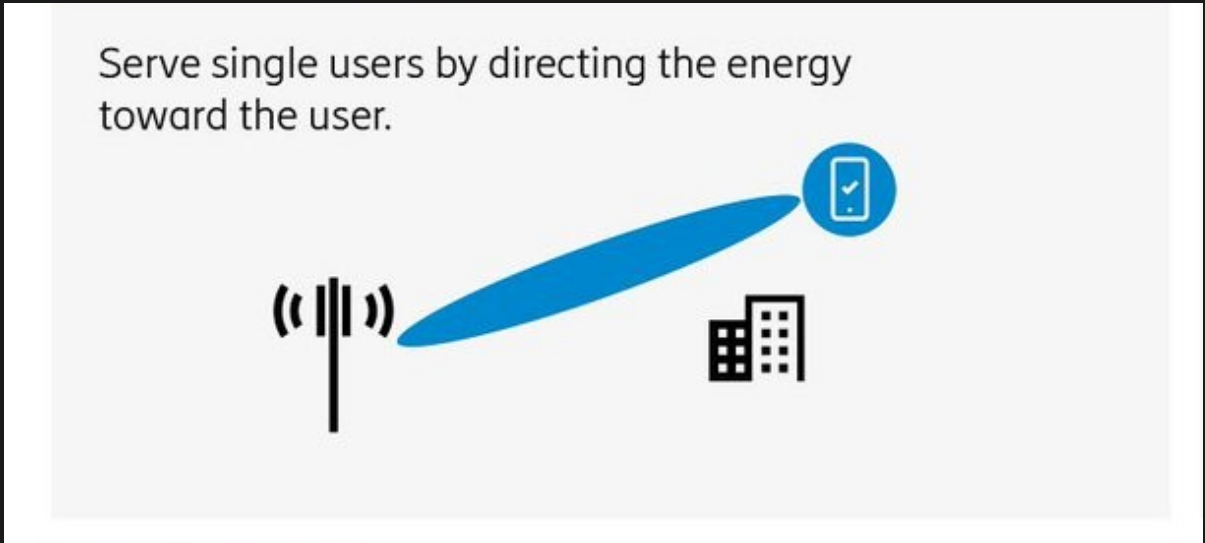
- Multipath effect
- Amplitude attenuation
- Phase offset of radio signal per subcarrier



$$H \in \mathbb{C}^{N \times M \times K}$$

Background

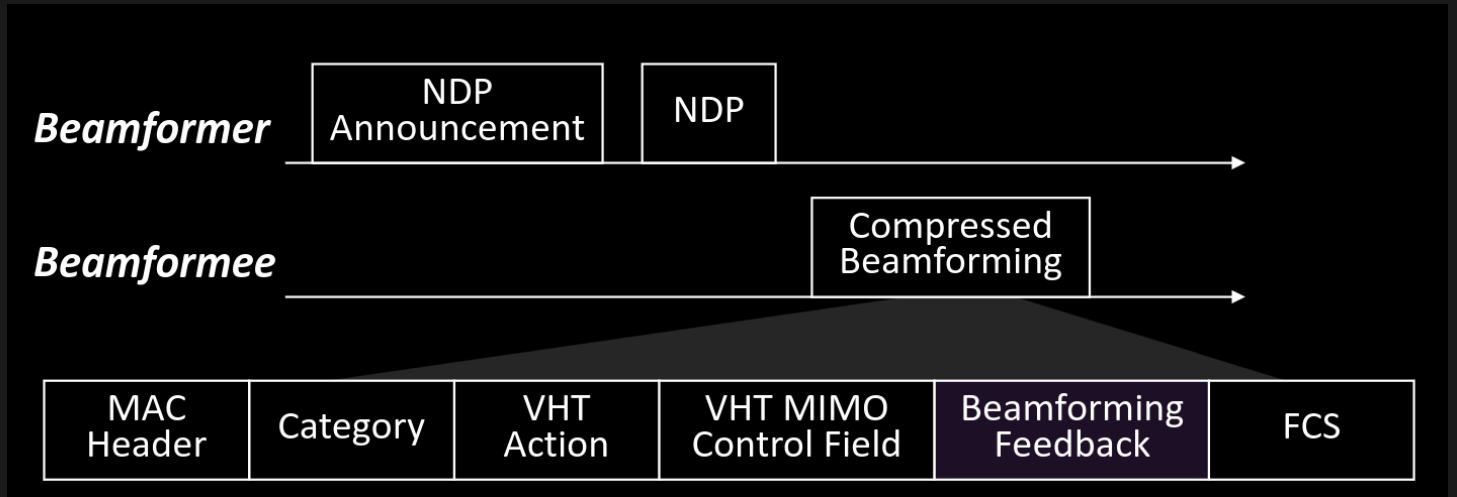
Beamforming



Background

Beamforming Information (BFI)

- Introduced in Wifi 5 802.11ac
- Access Point (AP), the Beamformer, requests BFI
- Associated devices, the beamformees calcutate BFI based on CSI and send it back to the AP in **plaintext**



Background

Beamforming Steering Matrix

$$\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{H}$$

Selected Related Work

Mac Relinking Attacks

- Utilize Probe Requests in disassociated state
- Based on content and timing of Information Elements (IE)

Selected Related Work

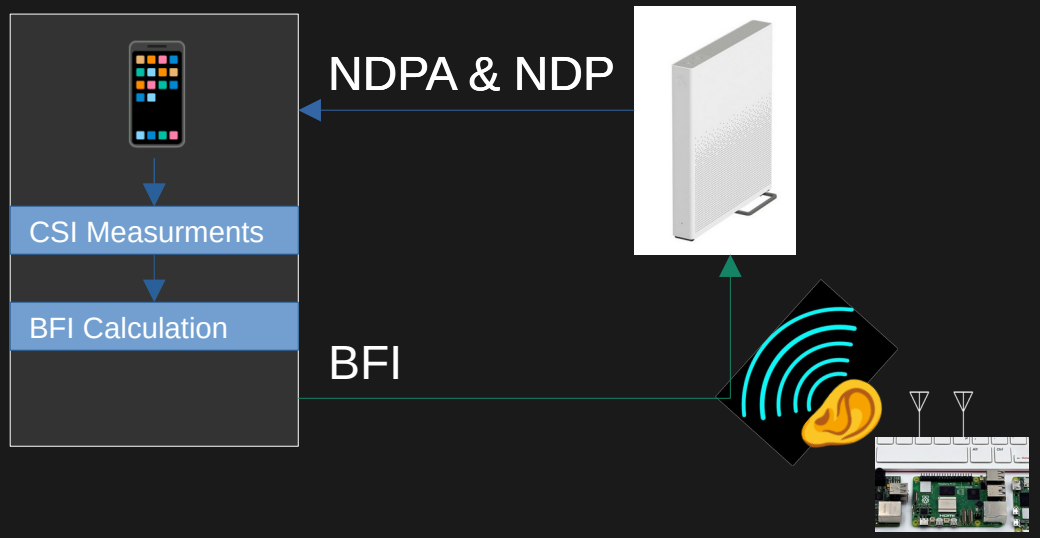
Limitations of previous work

- Mostly defeated with IE cycling on newer Operating Systems
- Can only reach disassociated devices
- Fingerprinting based on hardware imperfection assume the use of software defined radios

Design

Attack Scenario

- Low-cost
- Passive



Design

WiFi Relink: Research Prototype

- Included capture pipeline for CSI & BFI
- No MAC oracle
- No feature analysis

Design

Experiment Setup

Design

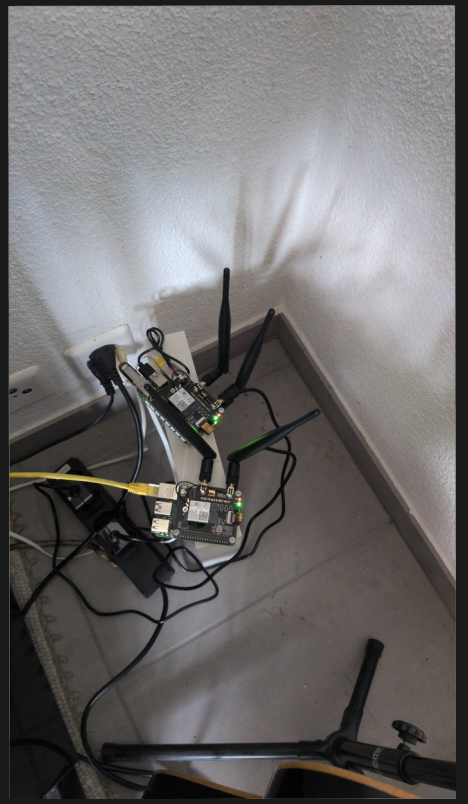
Test Devices / Mac Rotation Oracle

- Fleet of five ESP C5 with custom firmware
- Rotate mac adress every 15 minutes
- Simulate internet traffic for 10 minutes
- Use static IP pool to identify

Design

Capturing Devices (sniffers)

- 2 Rasperry Pi 5
- AX210 network card
- Connected to local network via ethernet cables.
- Sniffs only for BFI packets which are addressed to my AP

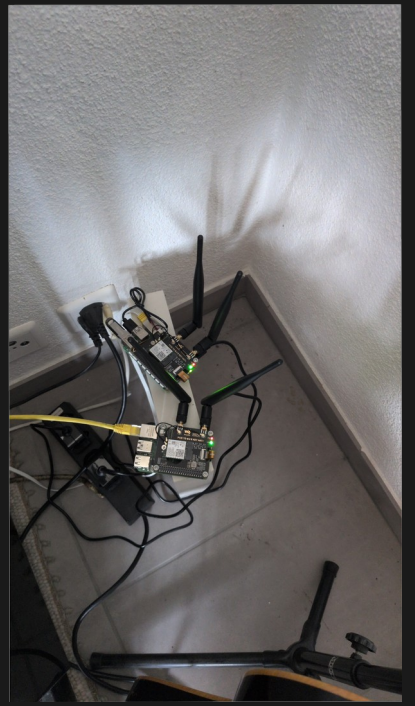


Design

Experiments

Experiment 01:

- 3 MAC rotating, stationary (non moving) C5s
- 2 sniffing pis
- 5 day observation window



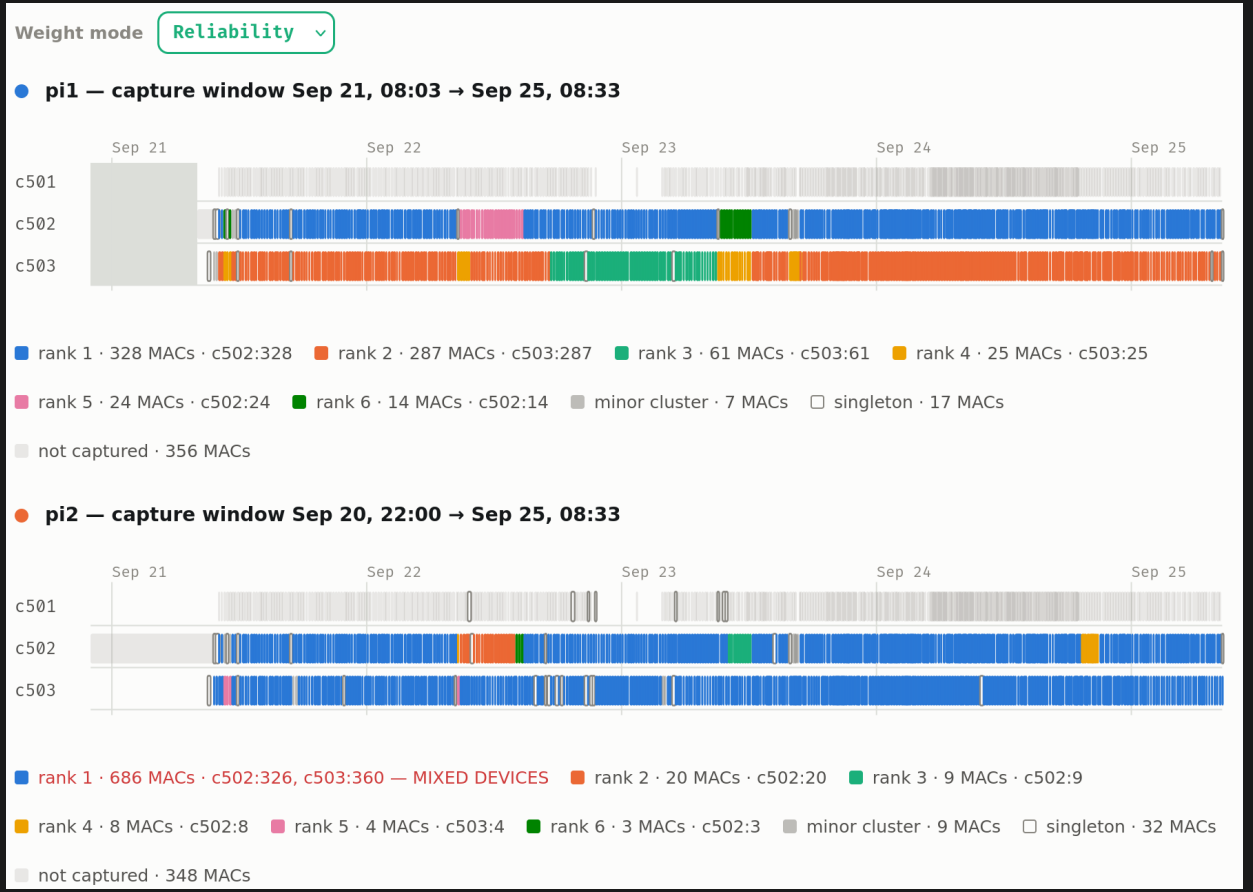
Experiment 02:

- 5 MAC rotating C5s
- 2 sniffing pis
- 8 day observation window
- 1 change in location of the C5s

Preleminary Results

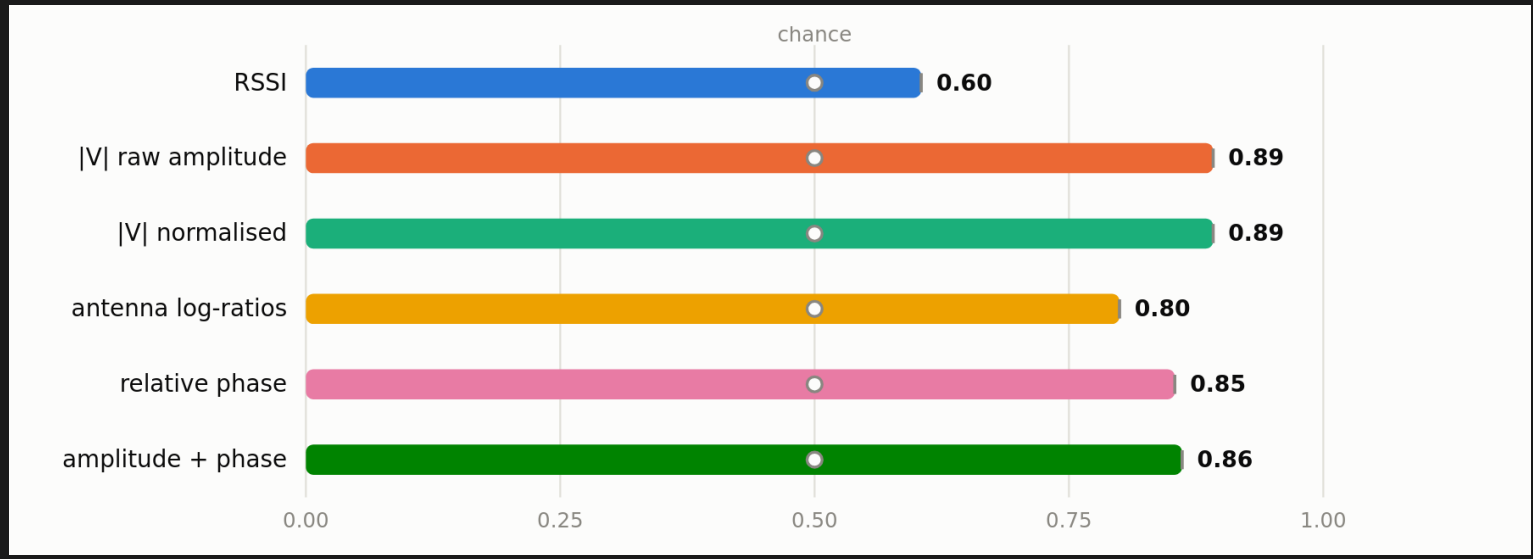
Experiment 01: Clustering

Clustering on raw BFI body bytes and RSSI



Preleminary Results

Experiment 01: BFI Features



Same-device pairs (necessarily spanning a MAC rotation) vs. different-device pairs, as the ROC-AUC
"small cosine distance ⇒ same device".

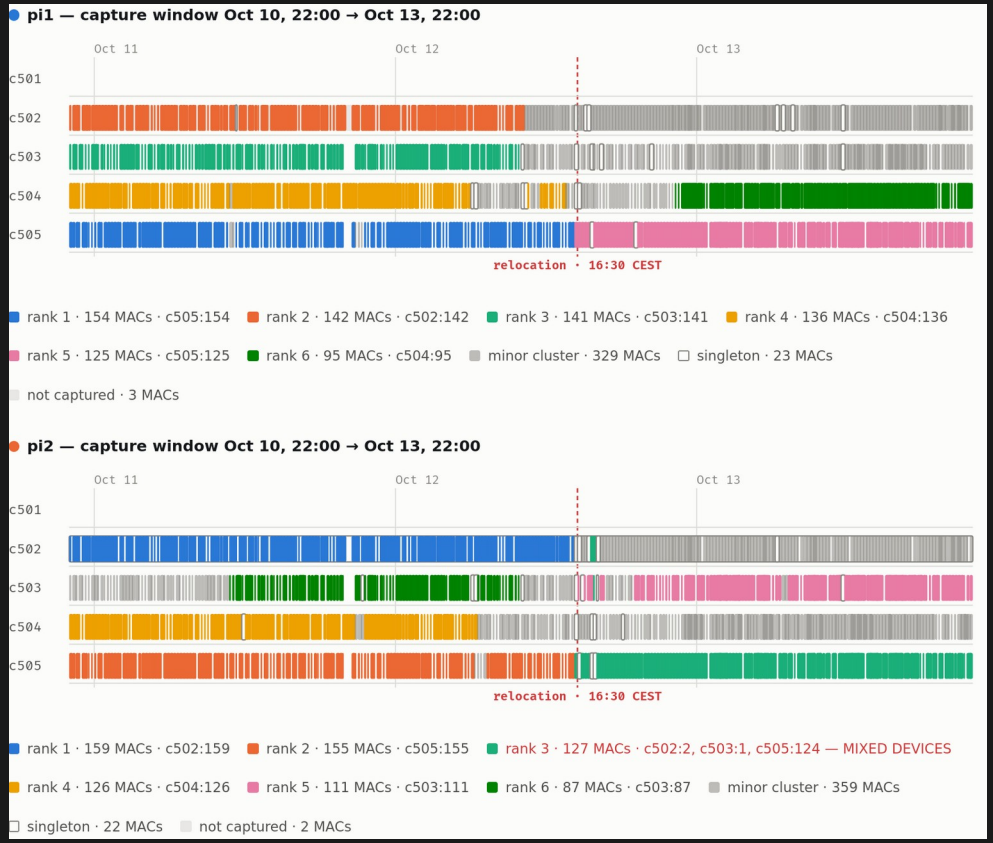
Preleminary Results

Experiment 01: Interpretation

- Clustering is decent but not perfect
- Only 2 test devices worked
- Only considers the stationary case
- RSSI is sensitive to antenna setup of sniffers

Preleminary Results

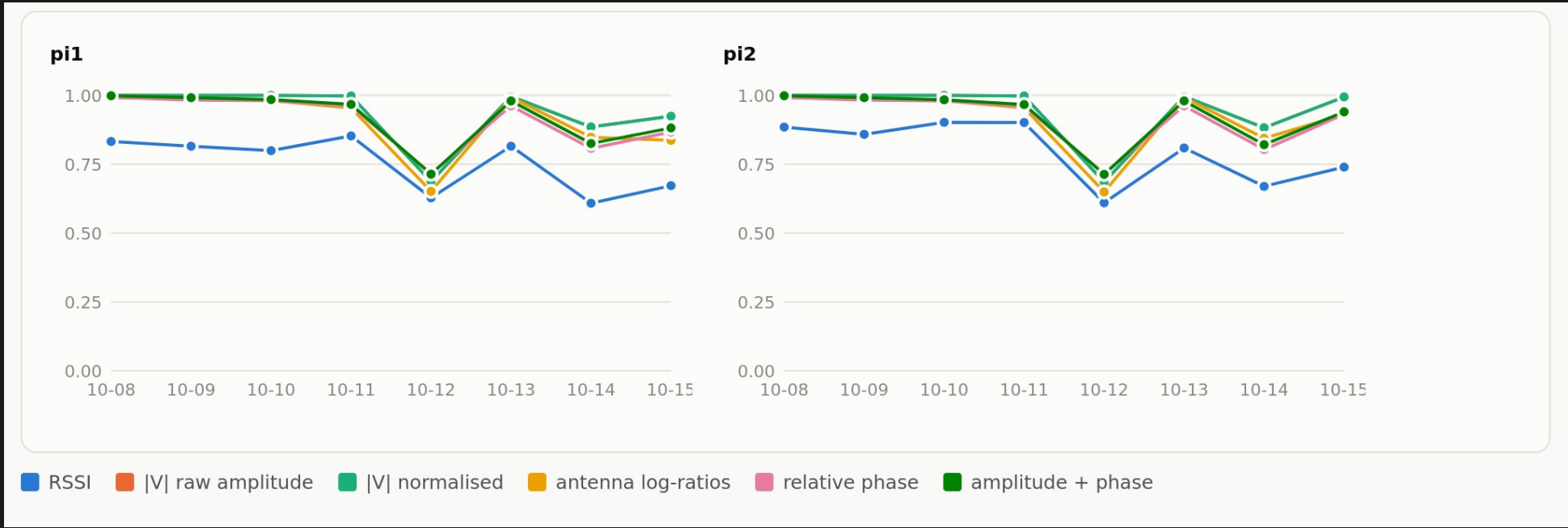
Experiment 02: Clustering



Preleminary Results

Experiment 02: BFI Features

Single day runs AUC across observed days



Preleminary Results

Experiment 02: BFI Features

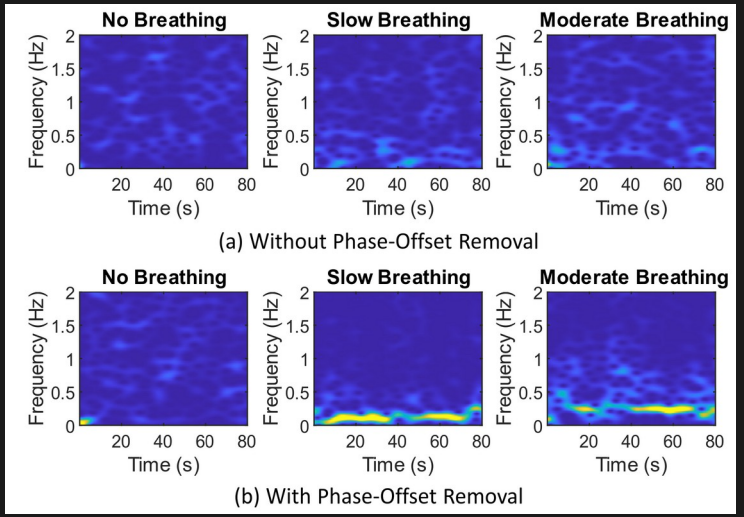
- Clustering is almost perfect before location change

- Clusters and feature surivals are location sensitive

Outlook

Next Steps

- Explore timing attacks of BFI sounding
- Do additional preprocessing of the BFI steering matrix besides simple decoding
- Run more experiments
- Document results



Q / A

Acknowledgement

- Thanks to Bruno and Karim for the excellent supervision so far
- Helpful research prototype which accelerated initial progress

References

M. Vanhoef et al., “Why MAC Address Randomization is not Enough,” ACM ASIA CCS 2016.

C. Matte et al., “Defeating MAC Address Randomization Through Timing Attacks,” ACM WiSec 2016.

J. Martin et al., “A Study of MAC Address Randomization in Mobile Devices and When it Fails,” PoPETs 2017(4).

M. Baccichet et al., “MAC Address De-Randomization using Multi-Channel Sniffers and Two-Stage Clustering,” arXiv:2408.01578, 2024.

R. Kong and T. Chen, “CSI-RFF: Leveraging Micro-Signals on CSI for RF Fingerprinting of Commodity WiFi,” IEEE TIFS, 2024, DOI 10.1109/TIFS.2024.3396375.

S. Todt, C. Morsbach, T. Strufe, “BFId: Identity Inference Attacks Utilizing Beamforming Feedback Information,” ACM CCS 2025, DOI 10.1145/3719027.3765062. See also Xiao et al., “Lend Me Your Beam,” NDSS 2026.

V. Brik et al., “Wireless Device Identification with Radiometric Signatures (PARADIS),” ACM MobiCom 2008, DOI 10.1145/1409944.1409959.