Lend Me Your Beam:
Privacy Implications of Beamforming Feedback in WiFi

Rui Xiao[1], Xiankai Chen[1], Yinghui He[2], Jun Han[3], and Jinsong Han[1]

[1] Zhejiang University, [2]Nanyang Technological University, [3]KAIST

NDSS 2025

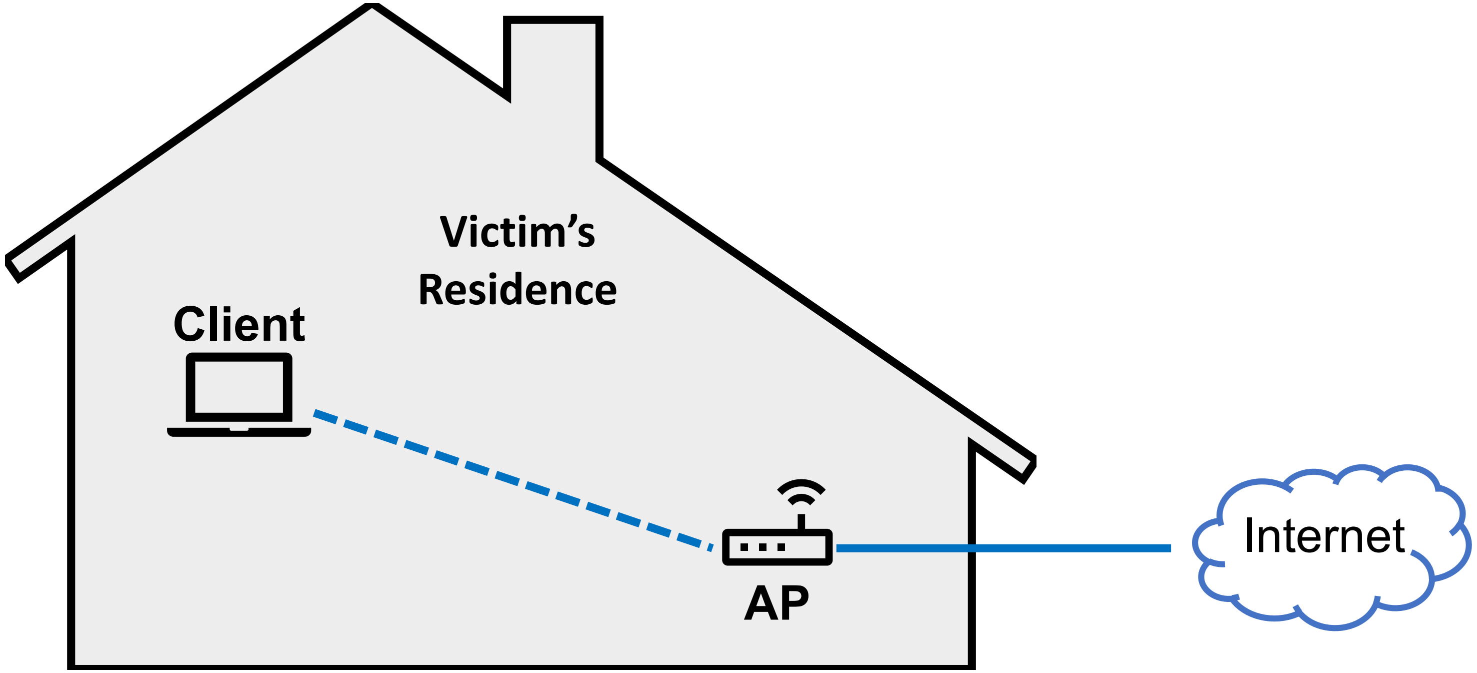
Smart WiFi Devices are Everywhere

Smart Home

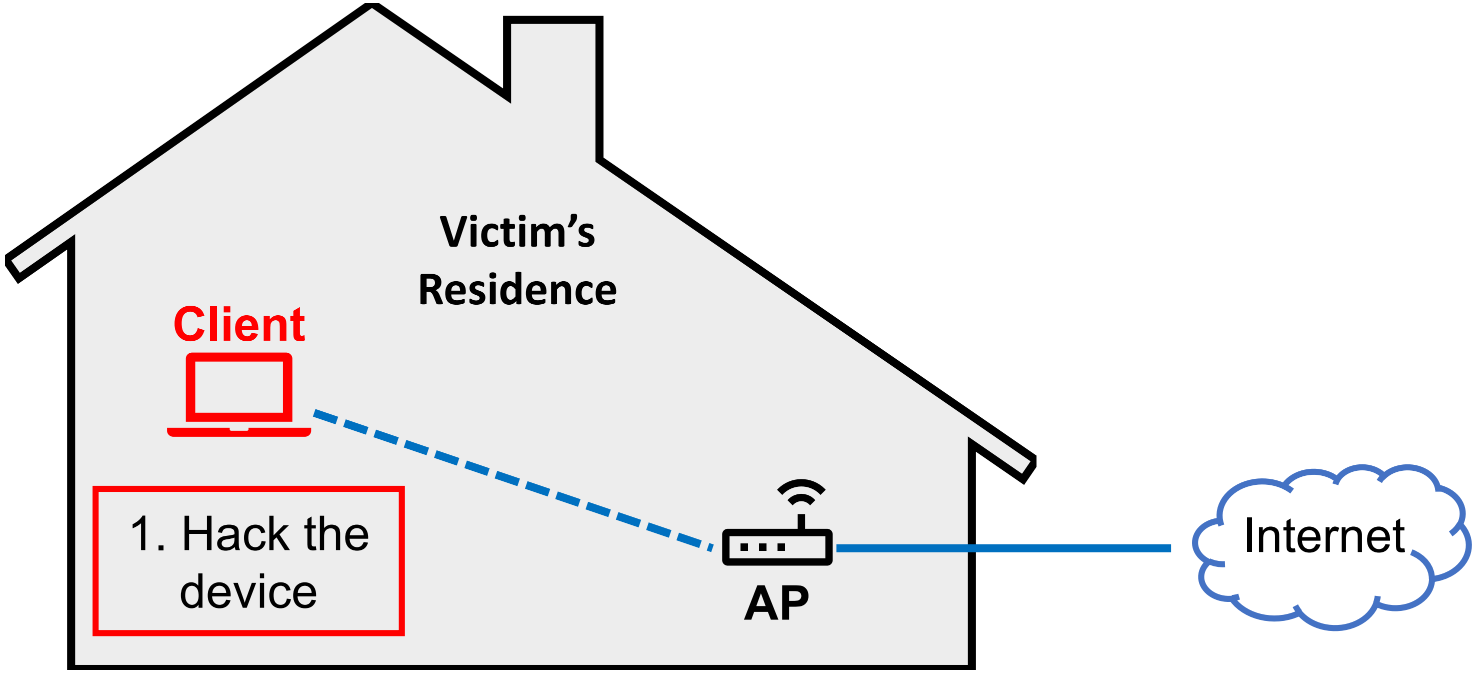
Smart Factory

Smart Office

Attacks Enabled by WiFi Devices

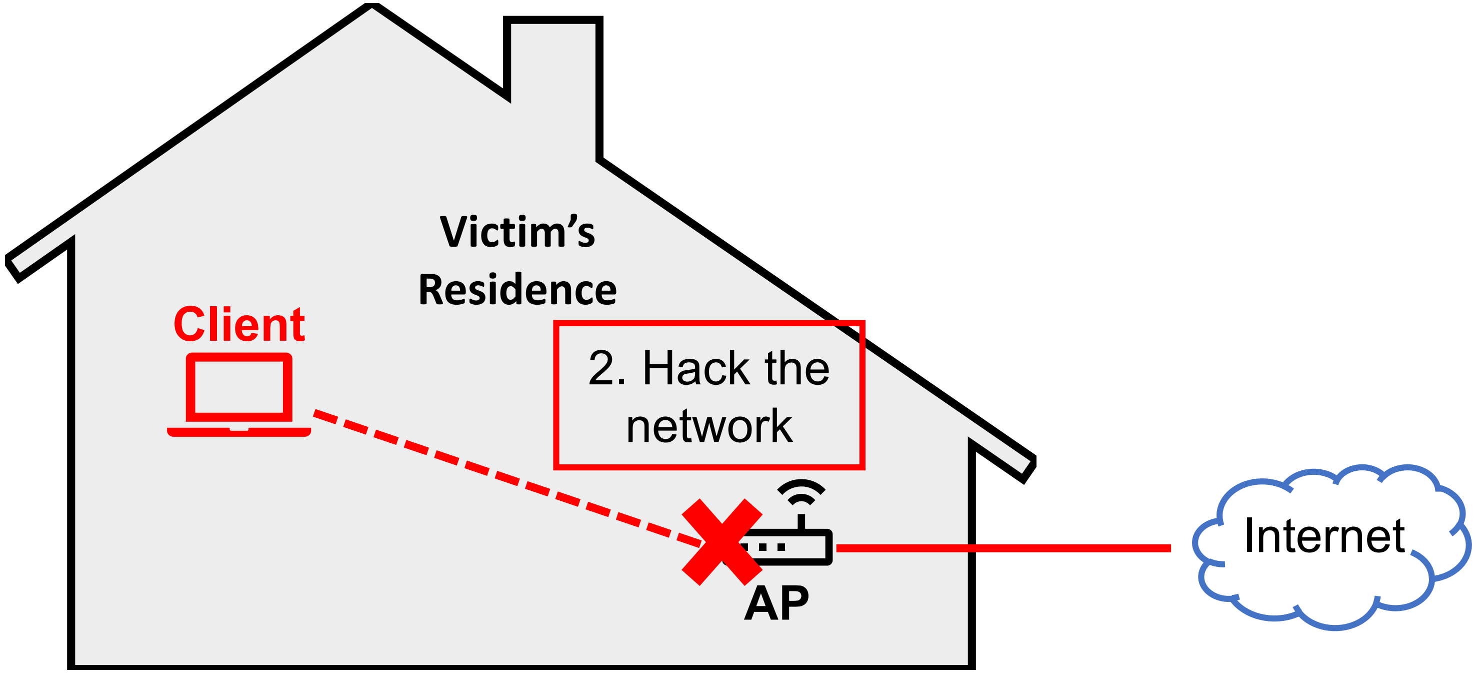


Attacks Enabled by WiFi Devices

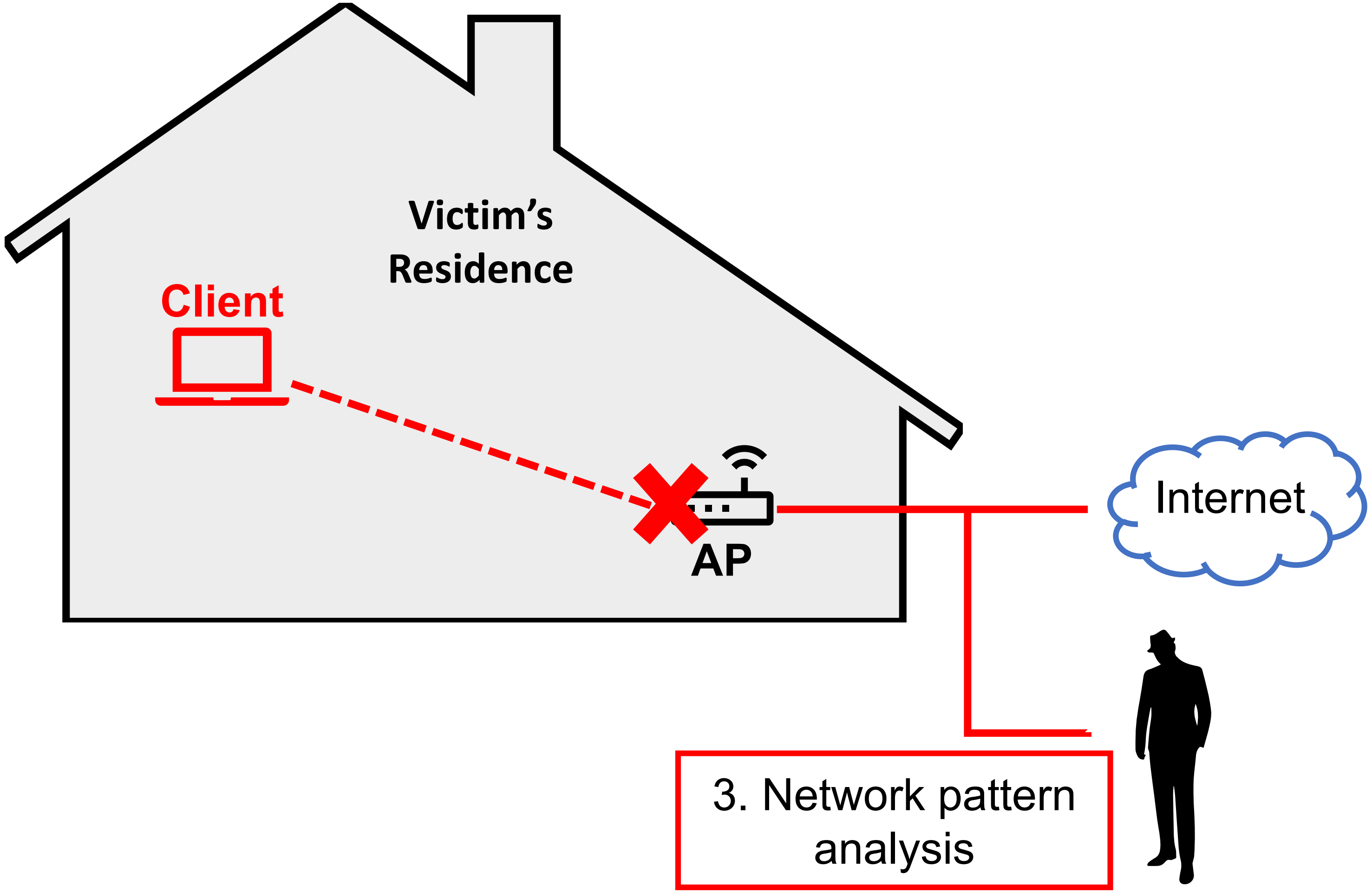


1. Hack the device

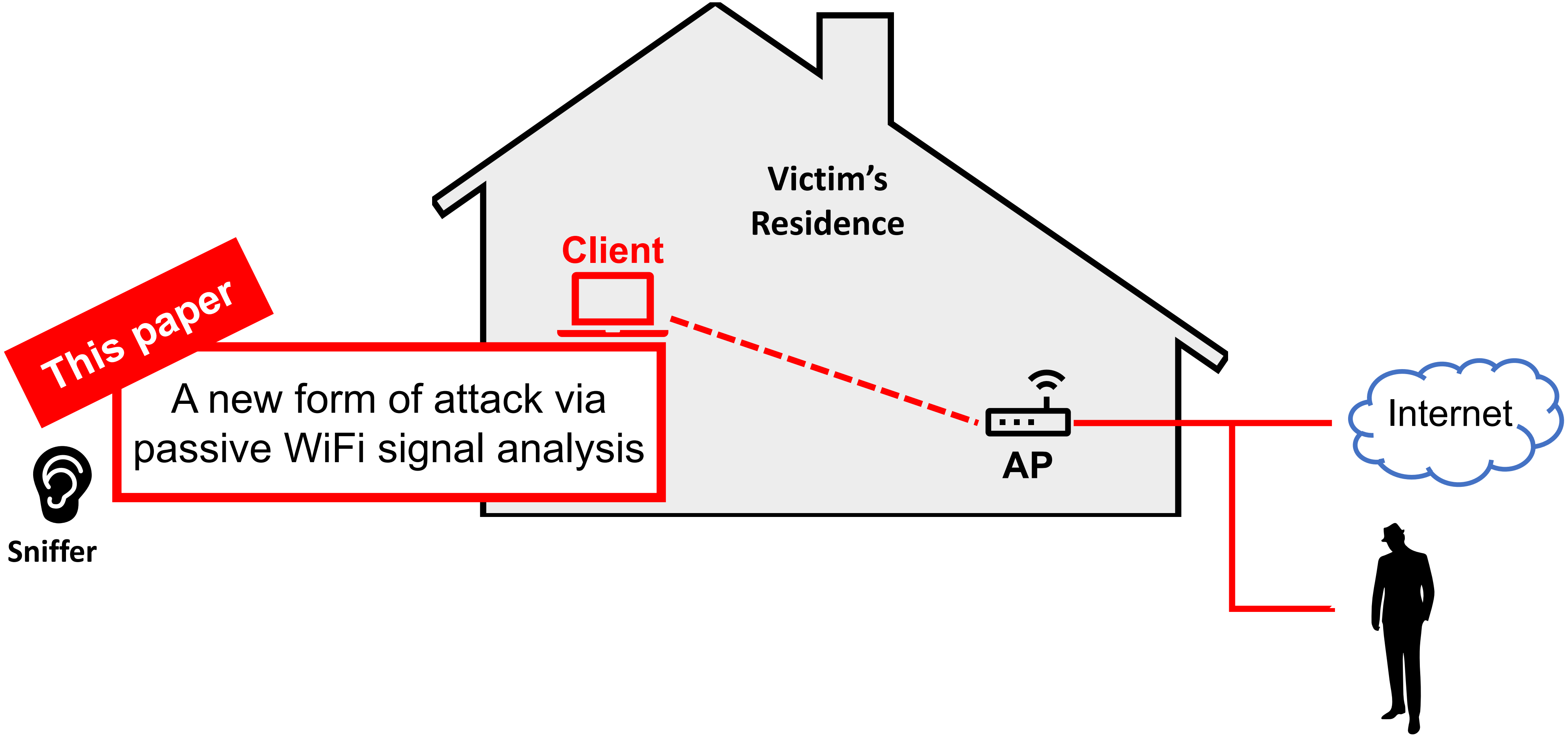
Attacks Enabled by WiFi Devices



Attacks Enabled by WiFi Devices



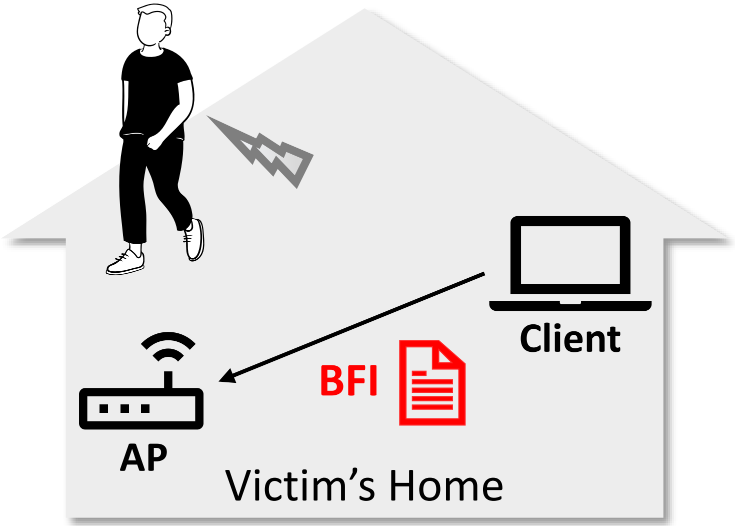
Attacks Enabled by WiFi Devices



This paper

A new form of attack via passive WiFi signal analysis

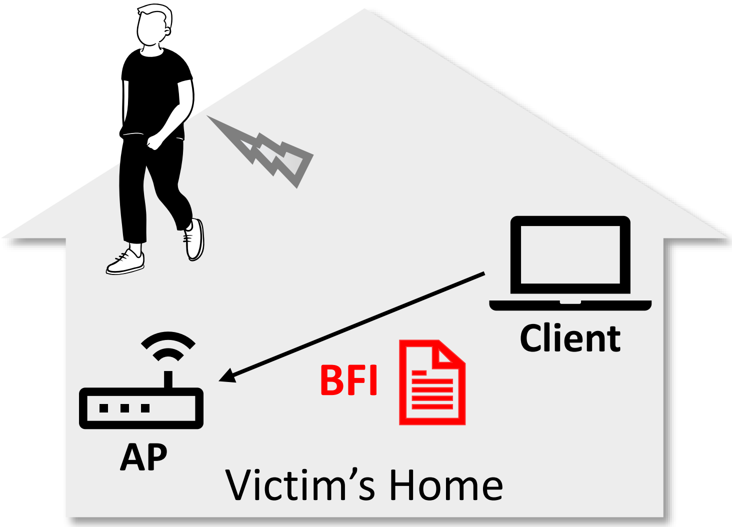
This Paper: Silent Occupancy Detection Attack



This Paper: Silent Occupancy Detection Attack

- New Side Channel from

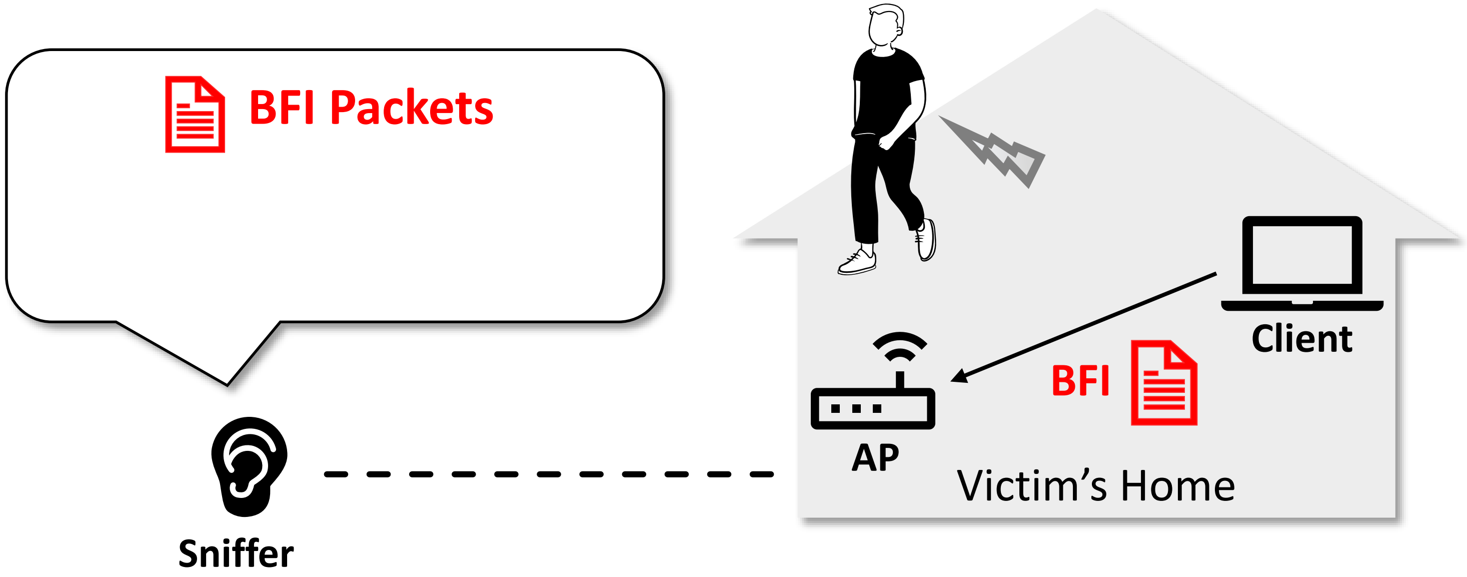
Beamforming Feedback (BFI) Packets



This Paper: Silent Occupancy Detection Attack

- New Side Channel from

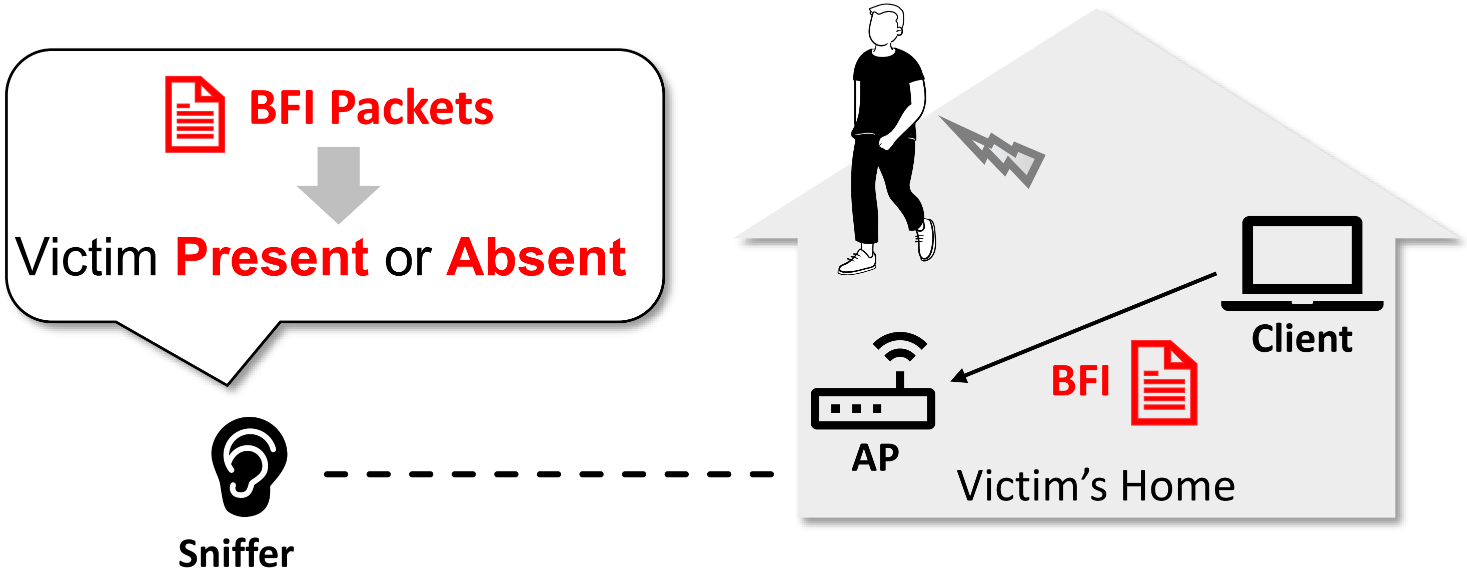
Beamforming Feedback (BFI) Packets



This Paper: Silent Occupancy Detection Attack

- New Side Channel from

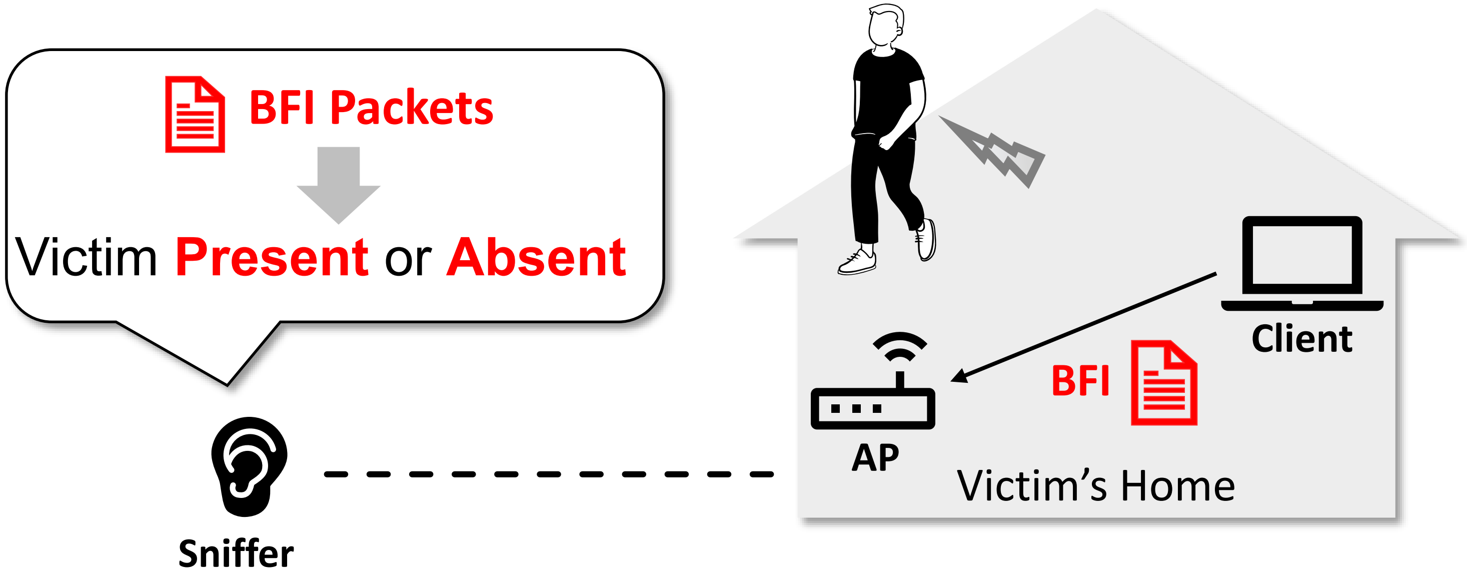
Beamforming Feedback (BFI) Packets



This Paper: Silent Occupancy Detection Attack

- New Side Channel from

Beamforming Feedback (BFI) Packets

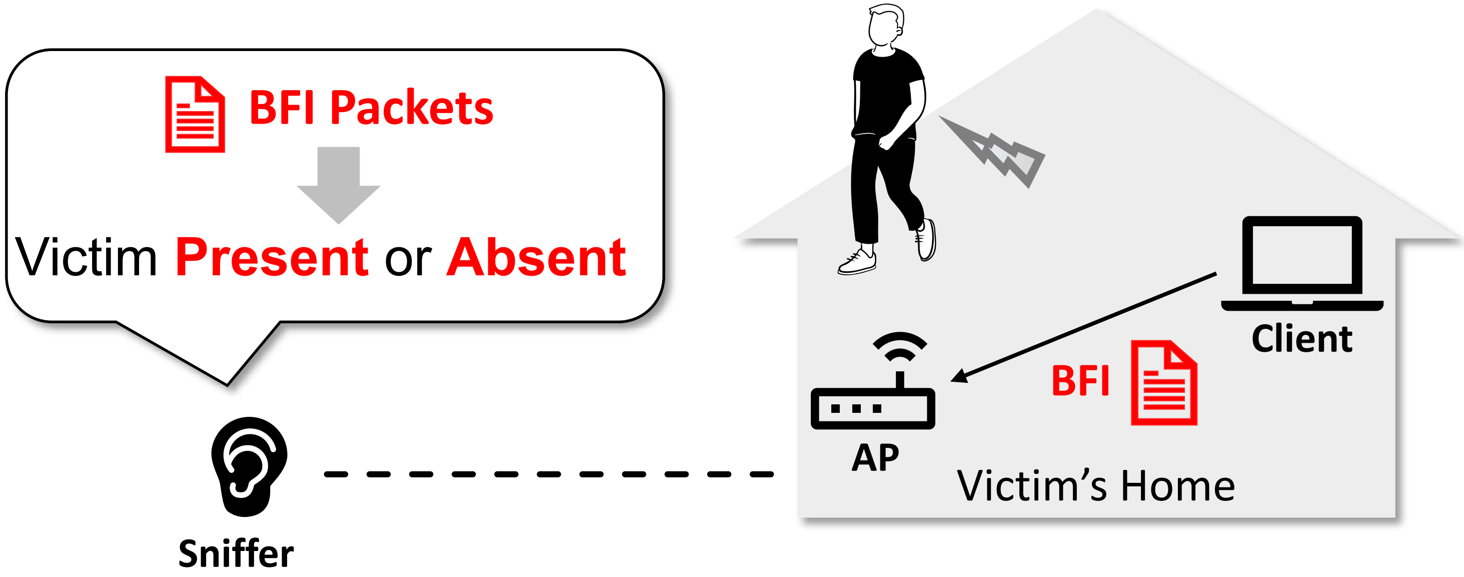


BFI Packets exists in 86% of WiFi 5/6 devices and is plaintext.

This Paper: Silent Occupancy Detection Attack

- New Side Channel from

Beamforming Feedback (BFI) Packets



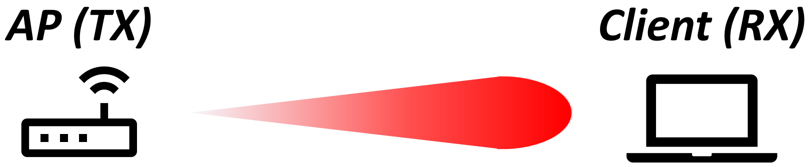
Spy Activity

Neighborhood Surveillance

BFI Packets exists in 86% of WiFi 5/6 devices and is plaintext.

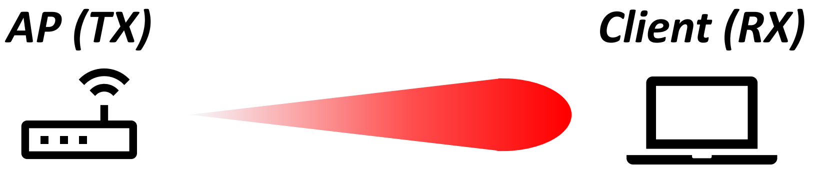
BFI’s Original Purpose: Beamforming

- Beamforming is **Directional Signal Transmission** for SNR improvement



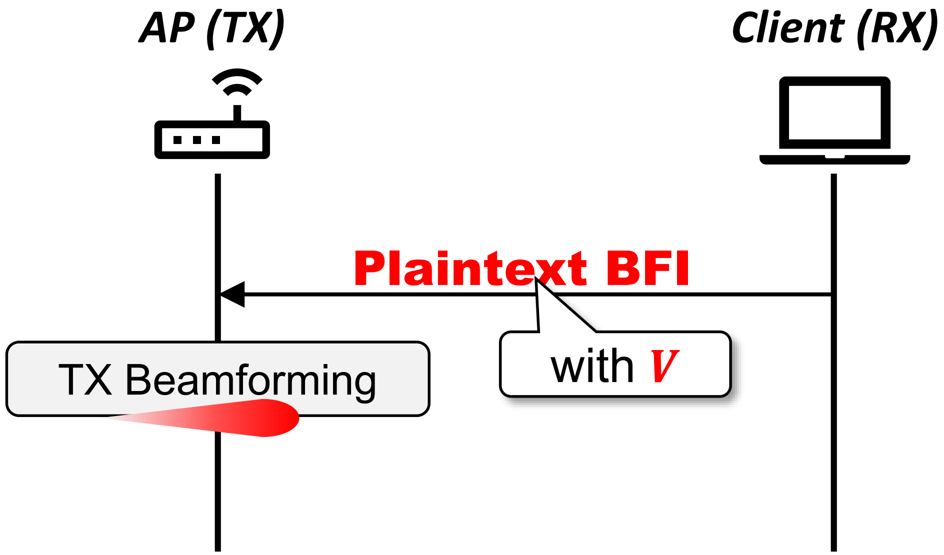
BFI’s Original Purpose: Beamforming

- Beamforming is **Directional Signal Transmission** for SNR improvement
- AP needs a **steering matrix V (spatial information)** for beam direction control



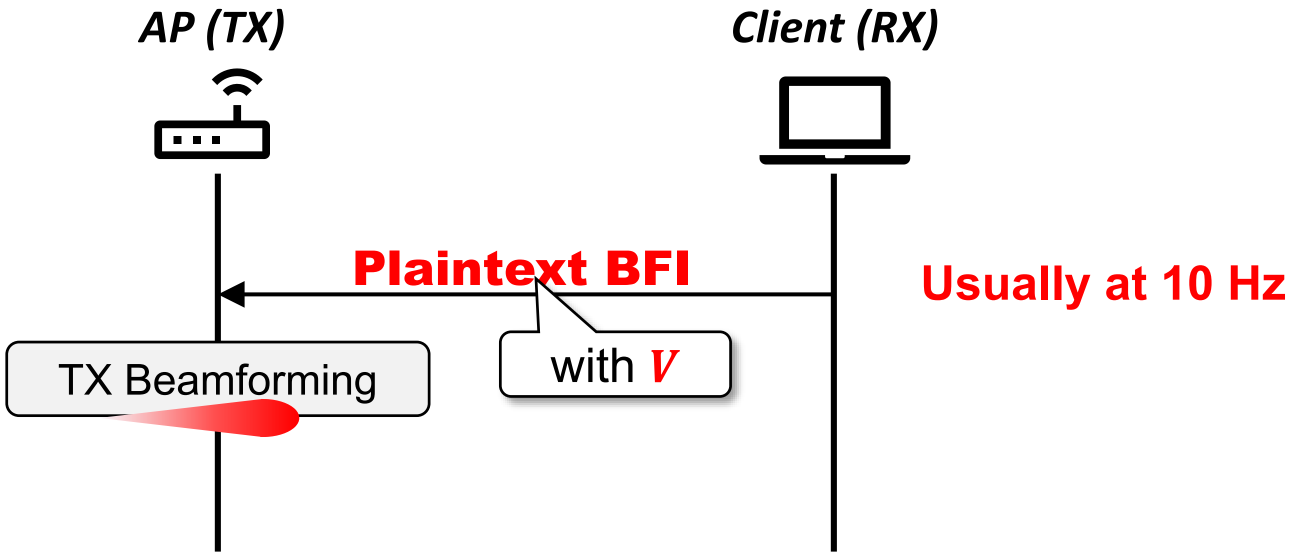
BFI’s Original Purpose: Beamforming

- Beamforming is **Directional Signal Transmission** for SNR improvement
- AP needs a **steering matrix V (spatial information)** for beam direction control



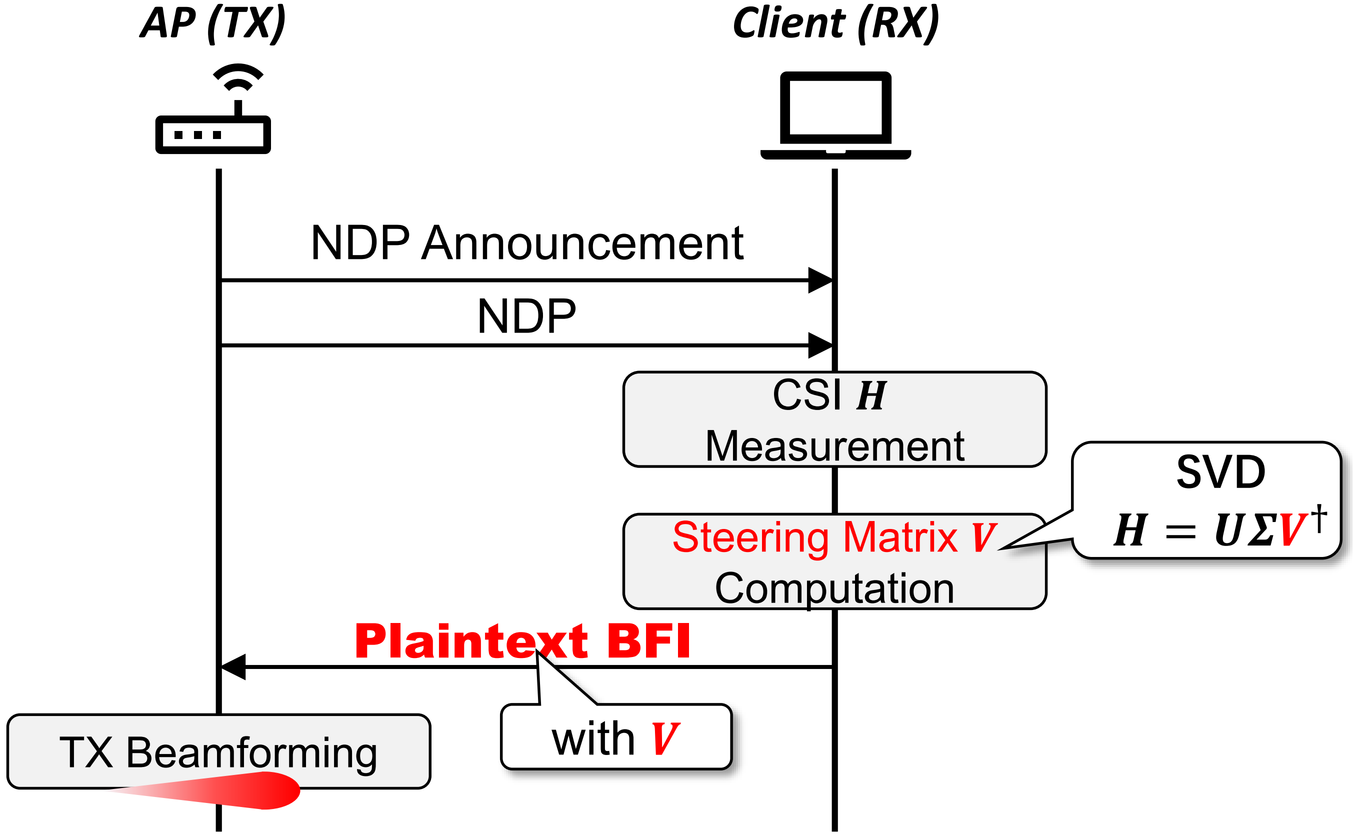
BFI’s Original Purpose: Beamforming

- Beamforming is **Directional Signal Transmission** for SNR improvement
- AP needs a **steering matrix V (spatial information)** for beam direction control



BFI’s Original Purpose: Beamforming

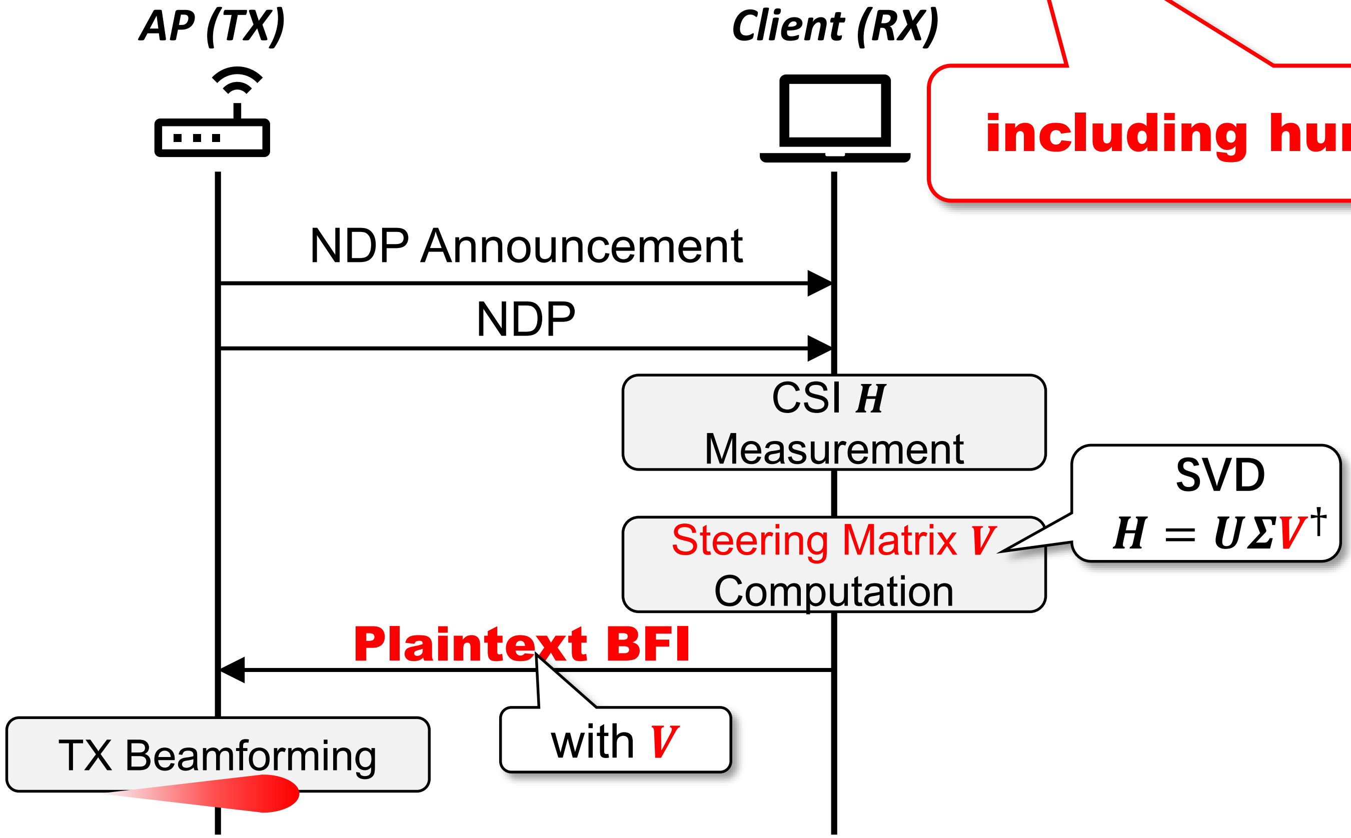
- Beamforming is **Directional Signal Transmission** for SNR improvement
- AP needs a **steering matrix V (spatial information)** for beam direction control



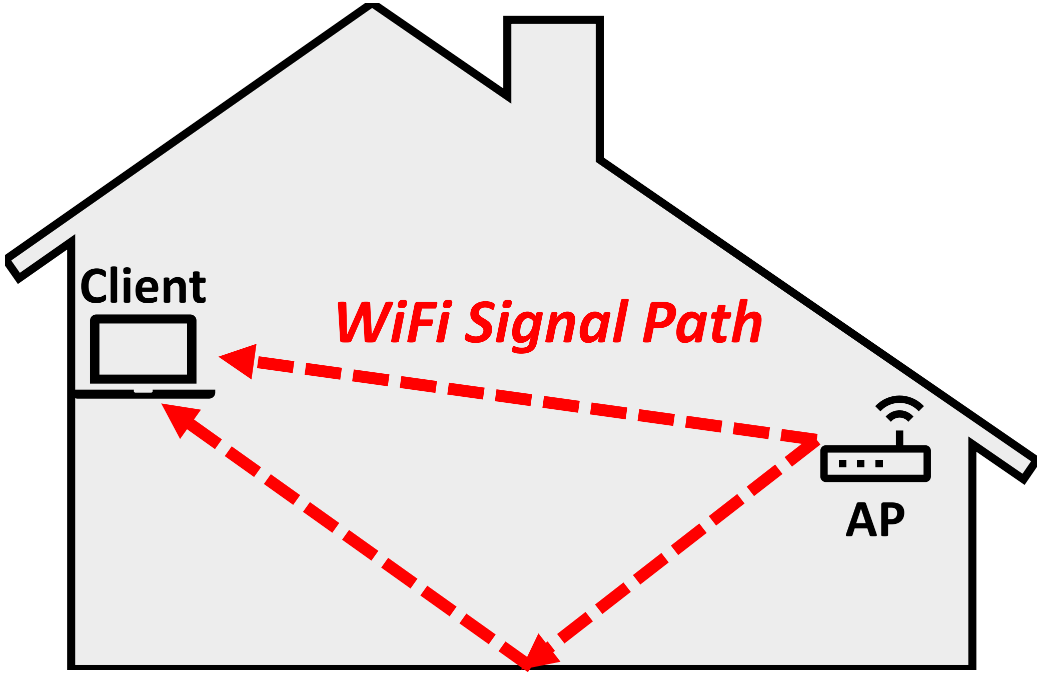
BFI’s Original Purpose: Beamforming

- Beamforming is **Directional Signal Transmission** for SNR improvement
- AP needs a **steering matrix V (spatial information)** for beam direction control

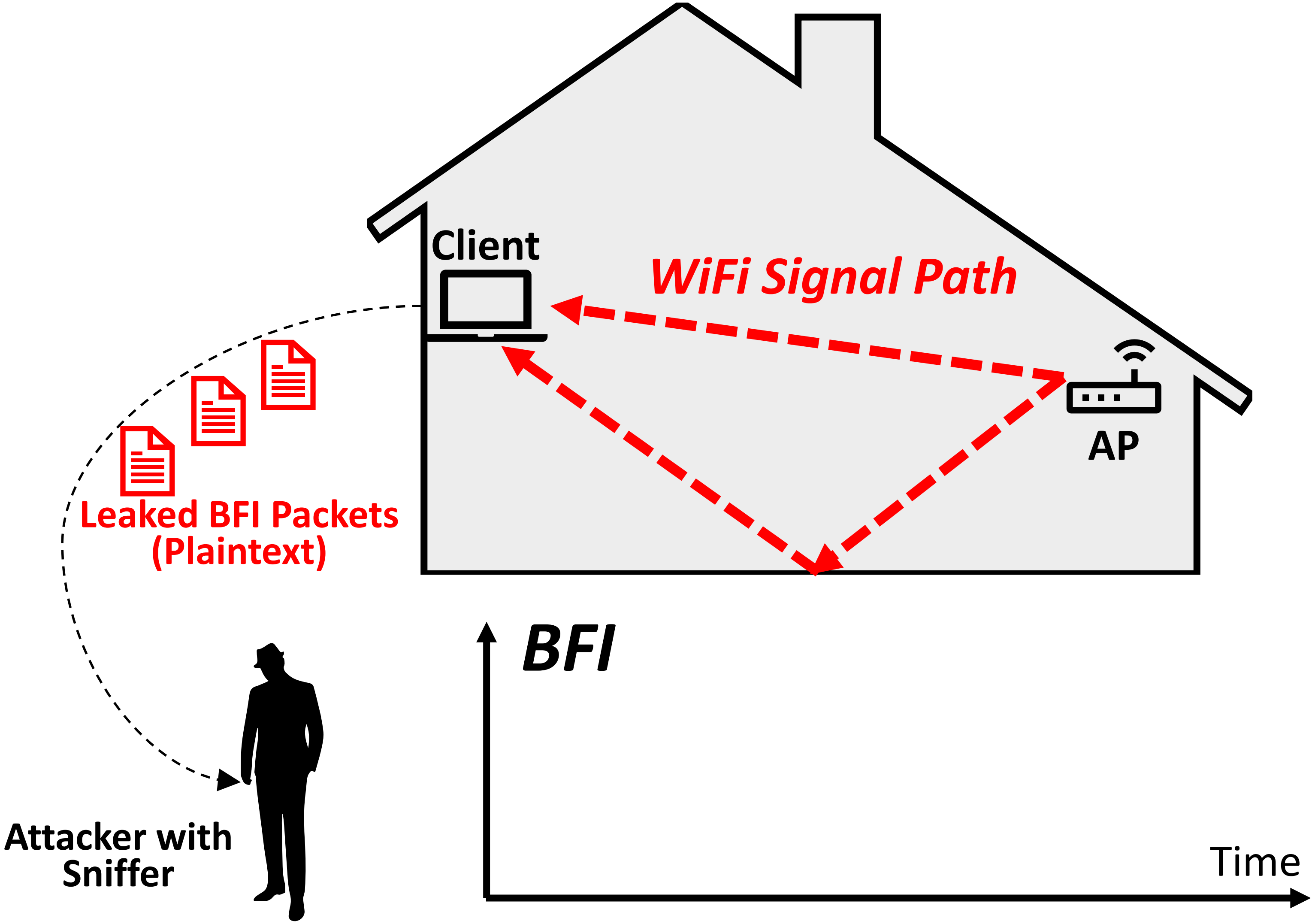
including human activity



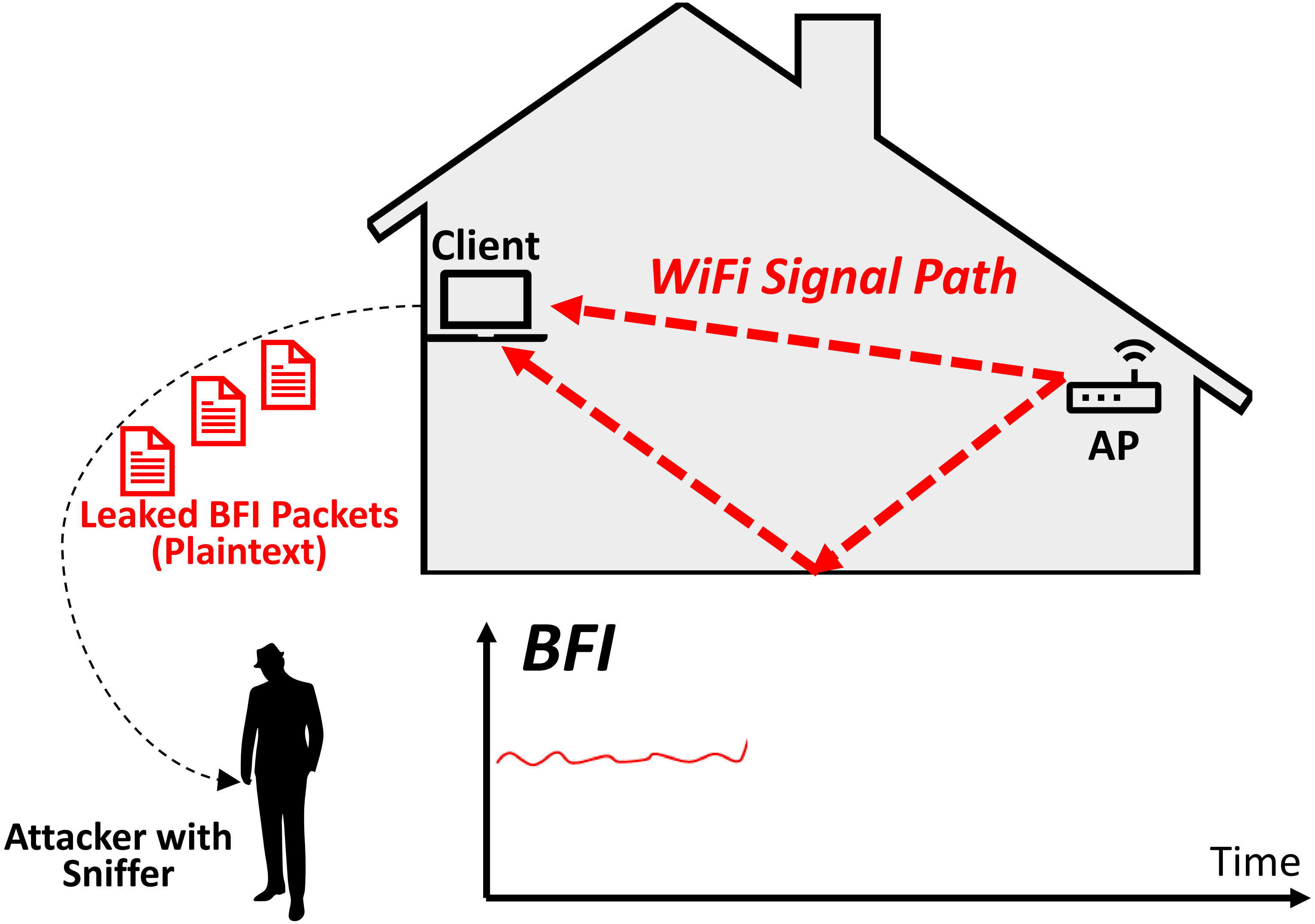
How does BFI reveal human activity?



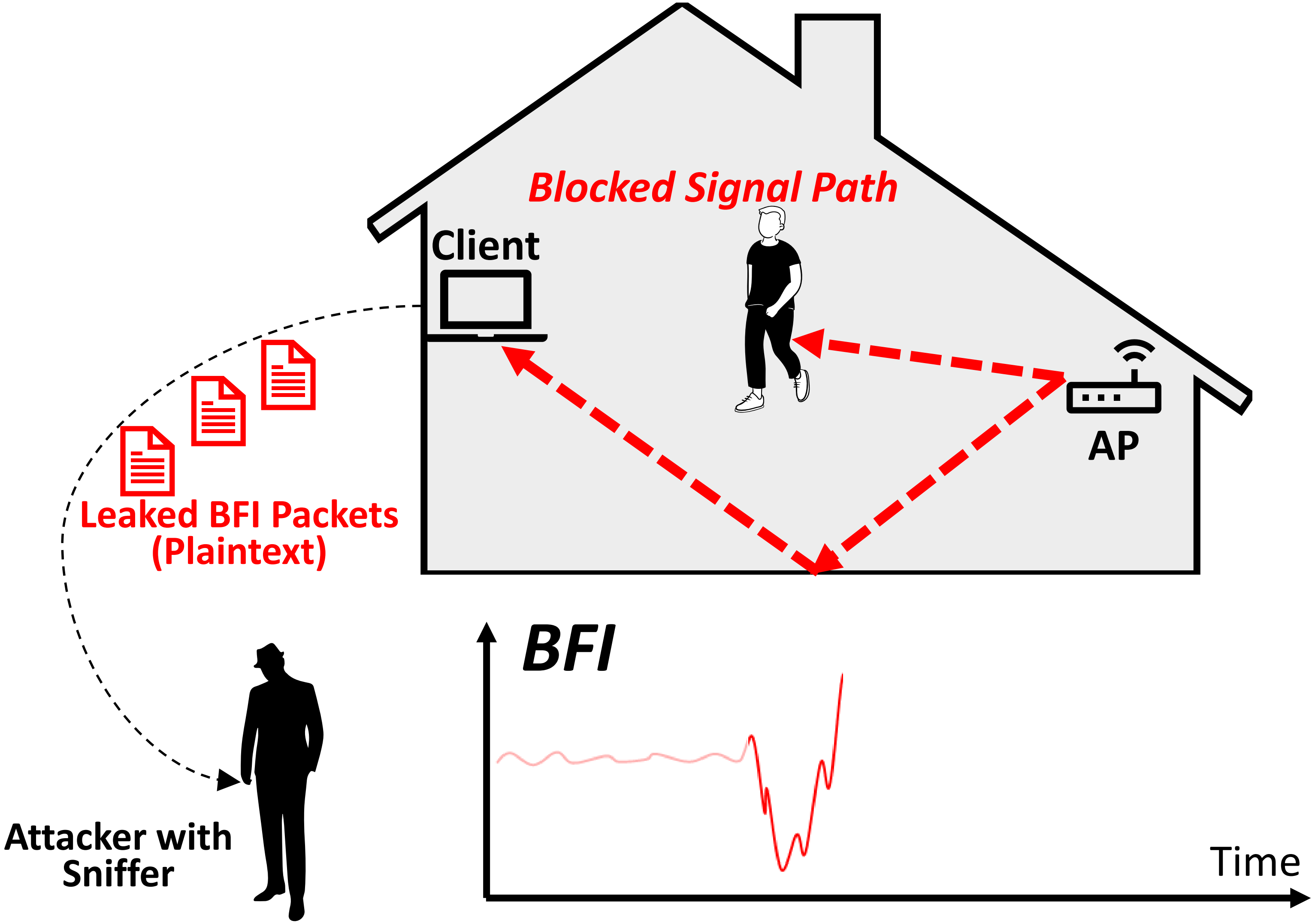
How does BFI reveal human activity?



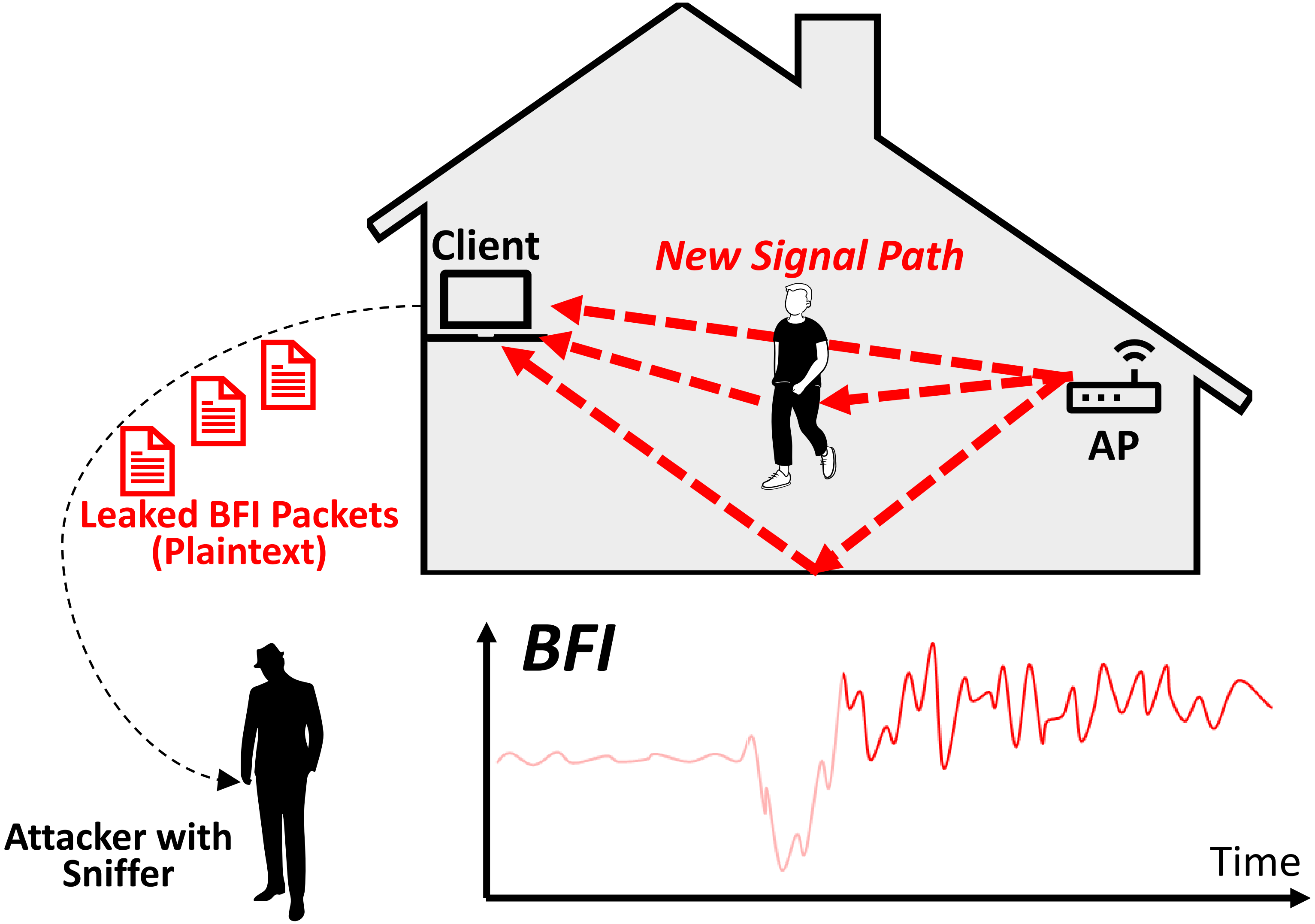
How does BFI reveal human activity?



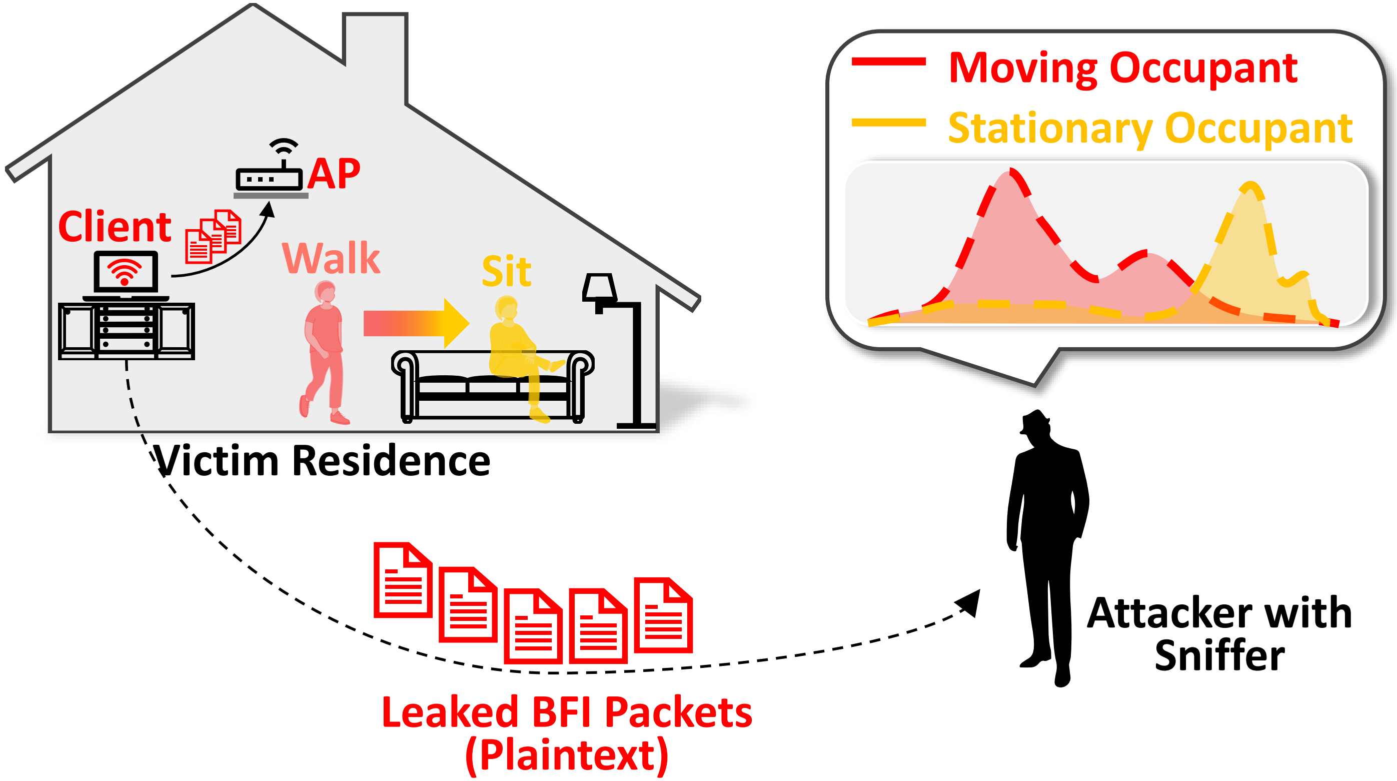
How does BFI reveal human activity?



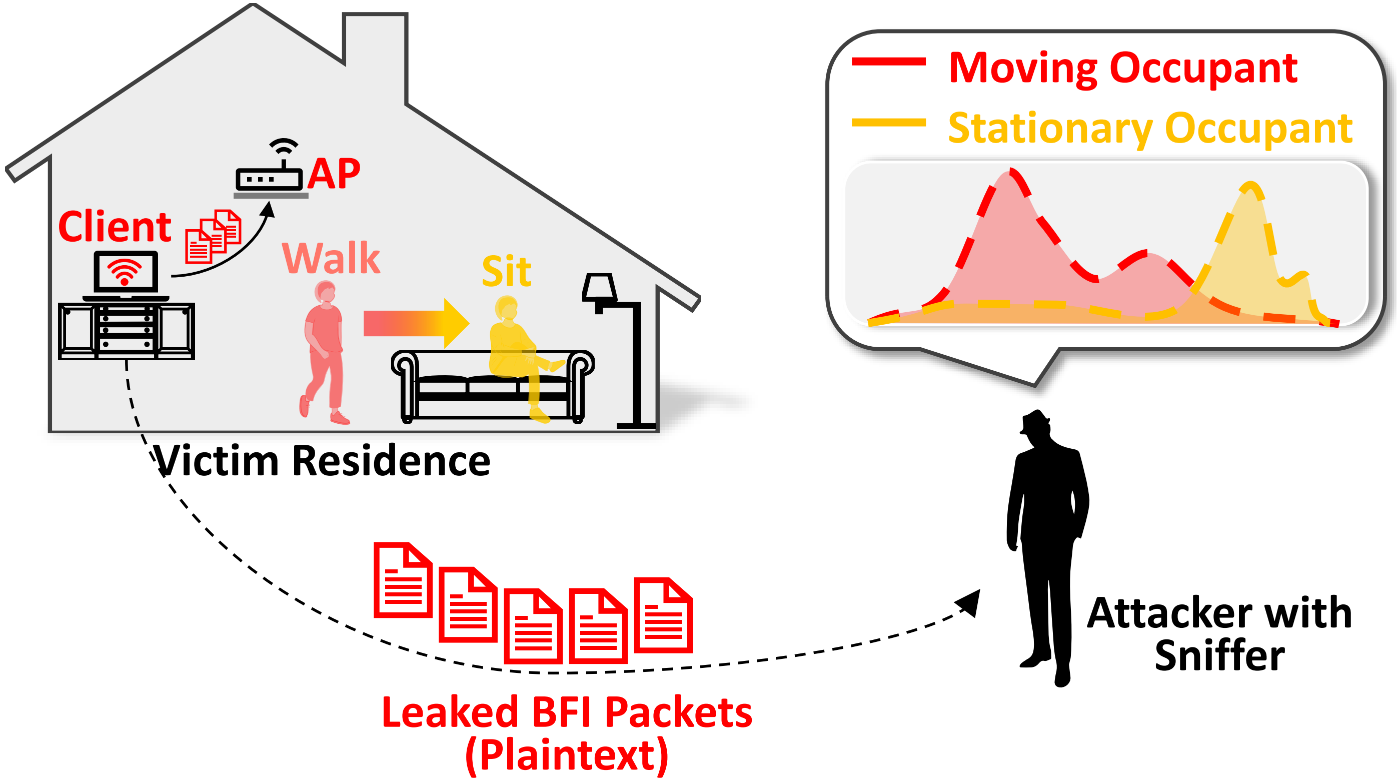
How does BFI reveal human activity?



LeakyBeam – Silent Occupancy Detection Attack



LeakyBeam – Silent Occupancy Detection Attack

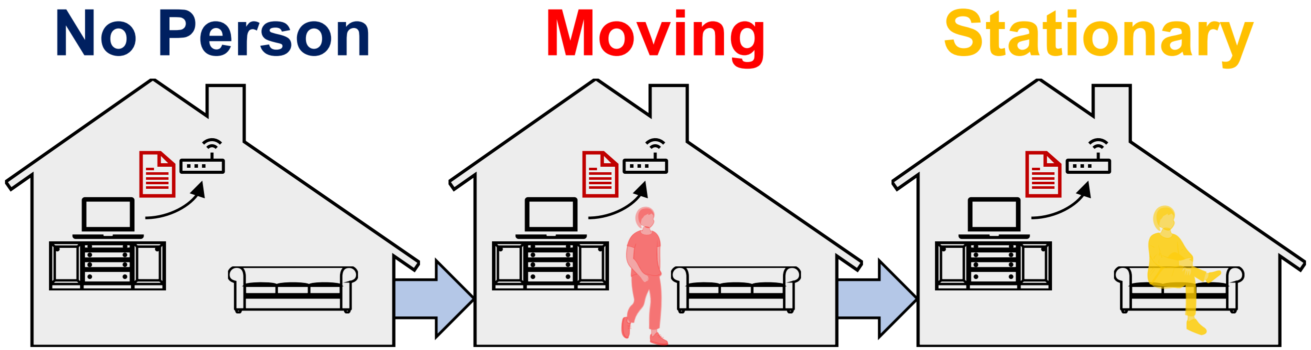


Key Features

- **High Accuracy**
  - Detect Stationary Occupant
- **Stealthiness**
  - Passive Sniffing
- **Accessibility**
  - Plaintext BFI packets
- **Long-Range**
  - Up to 20 meters

Overview: Measure Human Presence with BFI

Our Solution:

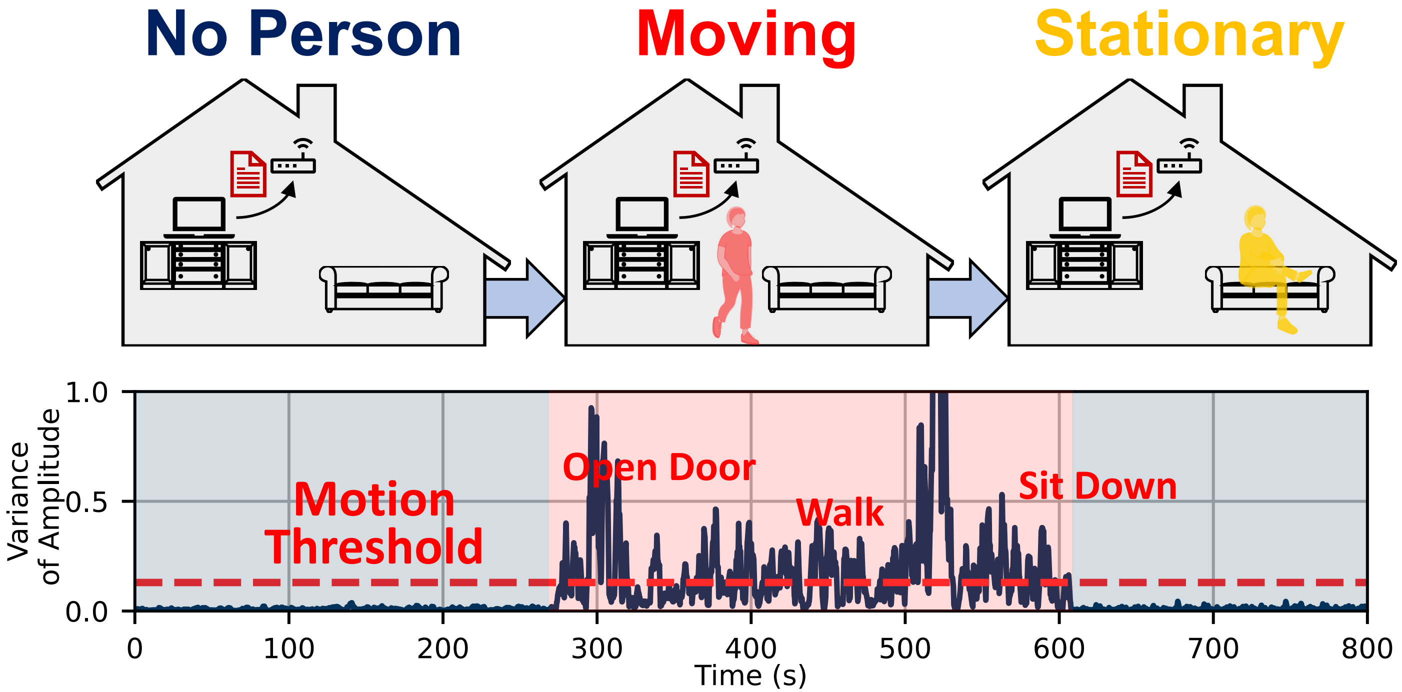


Overview: Measure Human Presence with BFI

Our Solution:

1) Motion Detection

- Using **amplitude variance**
- Detect **moving** occupants

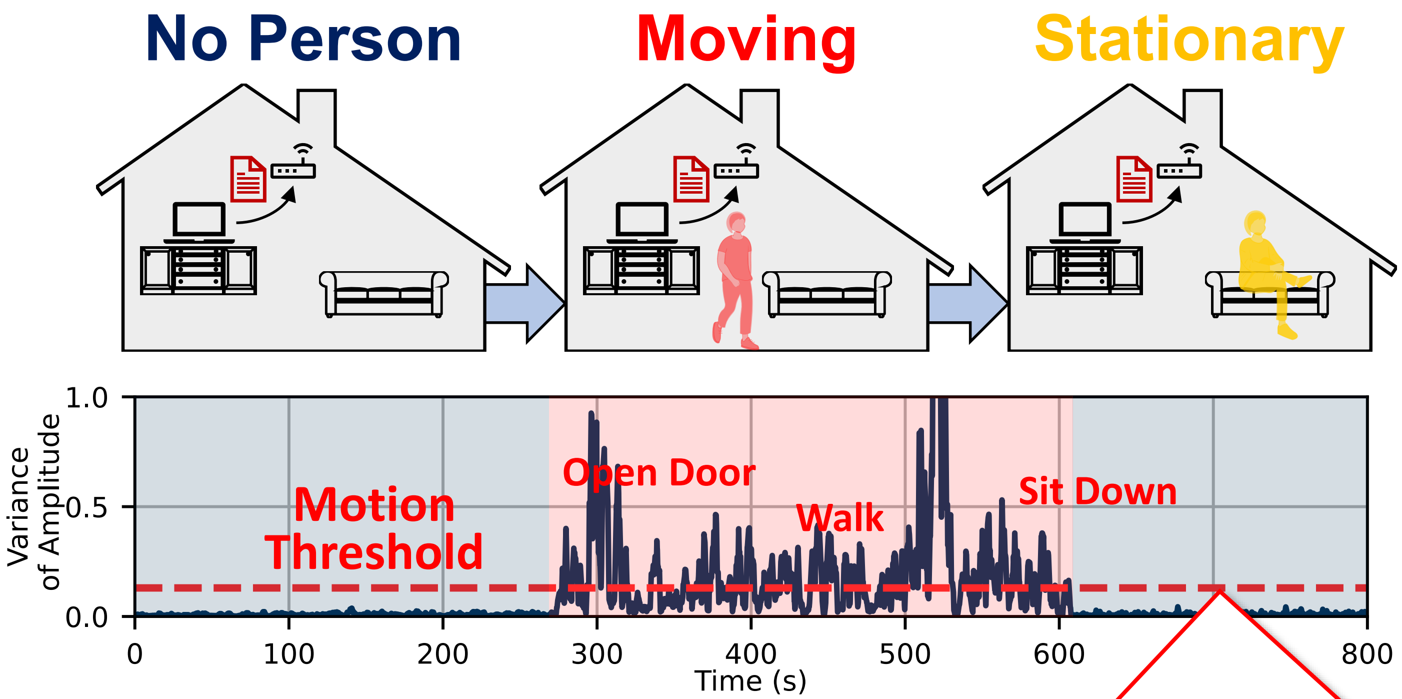


Overview: Measure Human Presence with BFI

Our Solution:

1) Motion Detection

- Using **amplitude variance**
- Detect **moving** occupants



Cannot detect stationary occupant

Overview: Measure Human Presence with BFI

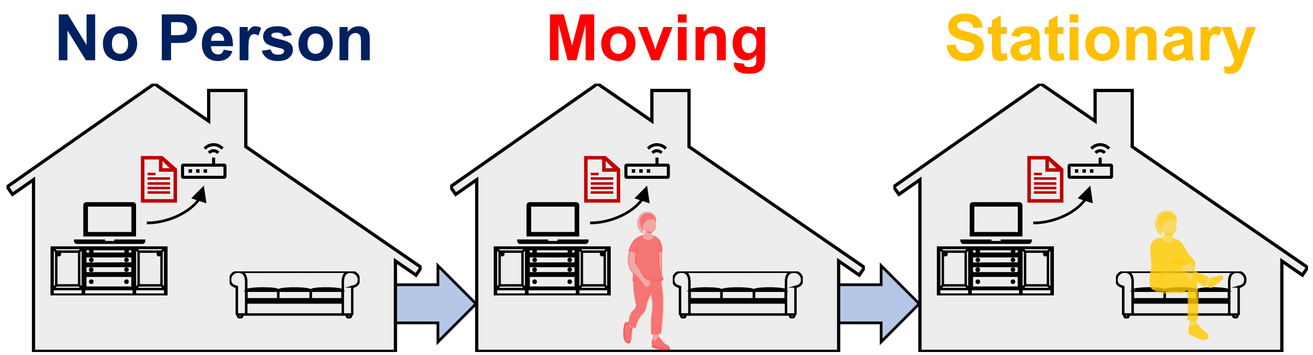
Our Solution:

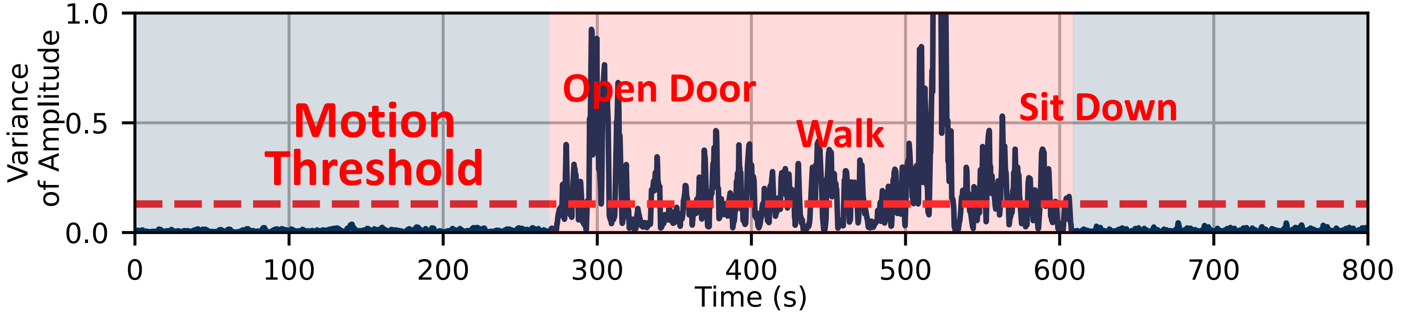
1) Motion Detection

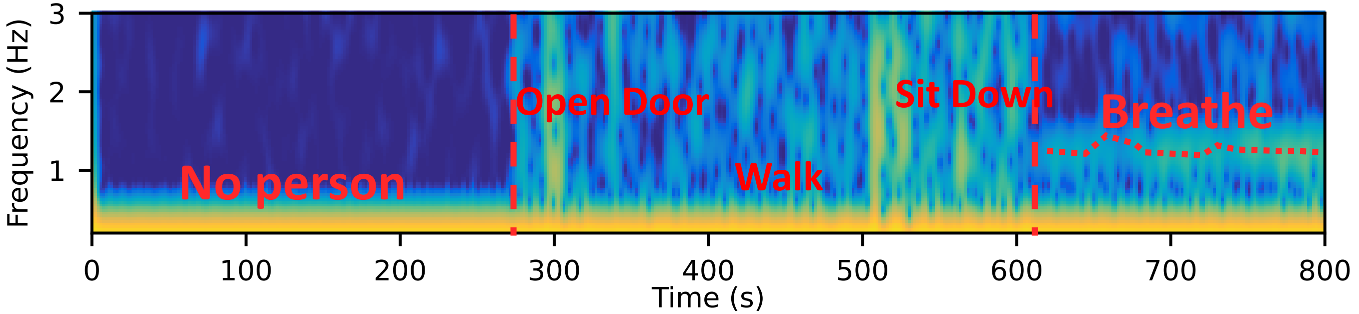
- Using **amplitude variance**
- Detect **moving** occupants

2) Breathe Detection

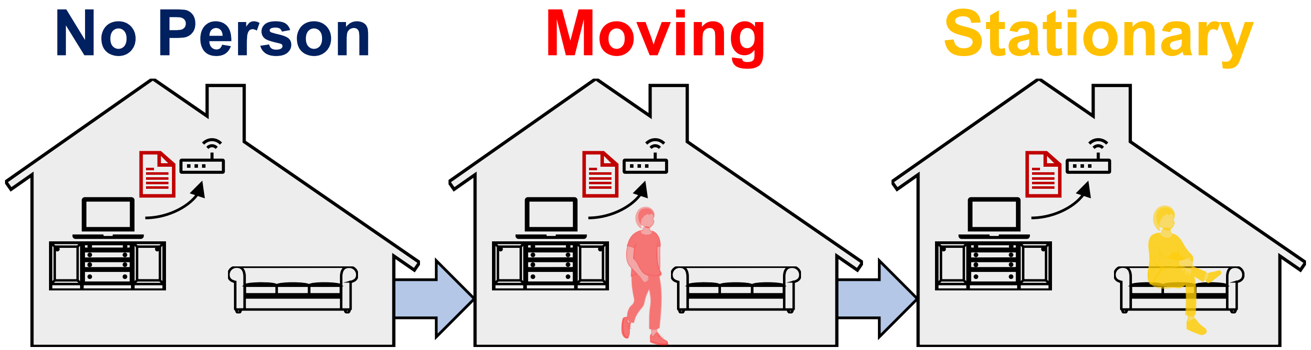
- Using **phase spectrogram**
- Detect **stationary** occupants







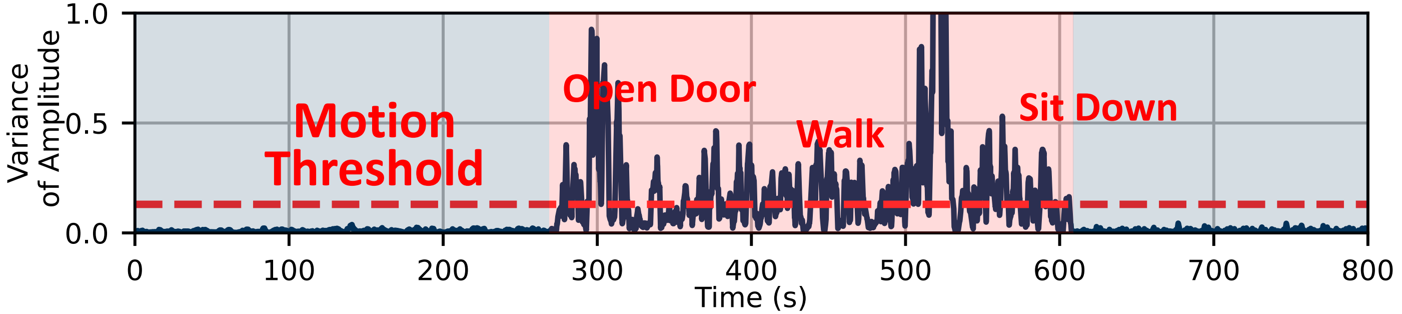
Overview: Measure Human Presence with BFI



Our Solution:

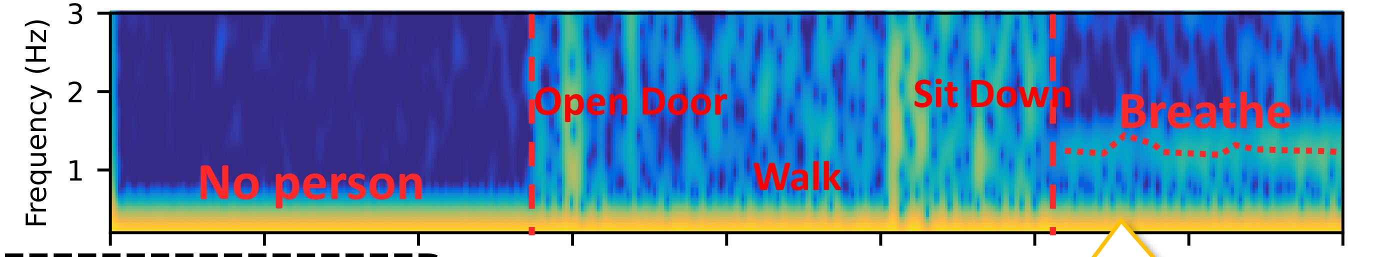
1) Motion Detection

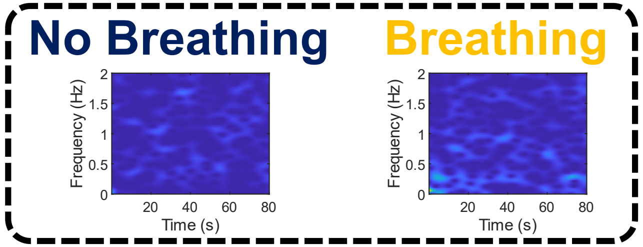
- Using **amplitude variance**
- Detect **moving** occupants



2) Breathe Detection

- Using **phase spectrogram**
- Detect **stationary** occupants





Challenge: Phase Offset

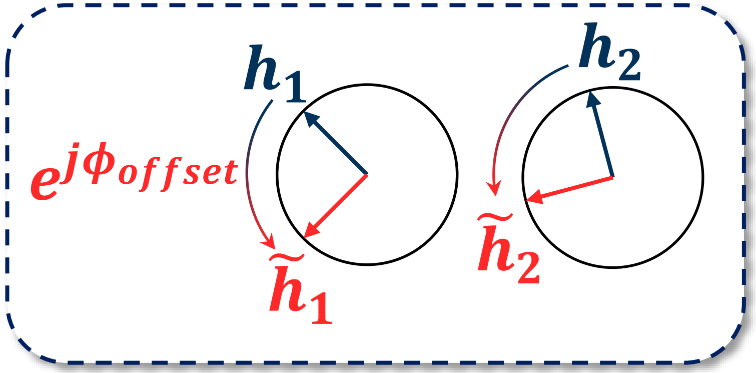
Challenge: Phase Offset from CSI to BFI

- Phase offset in CSI measurement:

$$\mathbf{H} = [\boldsymbol{h}_1, \boldsymbol{h}_2]$$

Phase Offset ϕ_{offset}

$$\widetilde{\mathbf{H}} = [\widetilde{\boldsymbol{h}}_1, \widetilde{\boldsymbol{h}}_2]$$


$\boldsymbol{h}_1$
$\boldsymbol{h}_2$
$e^{j\phi_{offset}}$
$\widetilde{\boldsymbol{h}}_1$
$\widetilde{\boldsymbol{h}}_2$

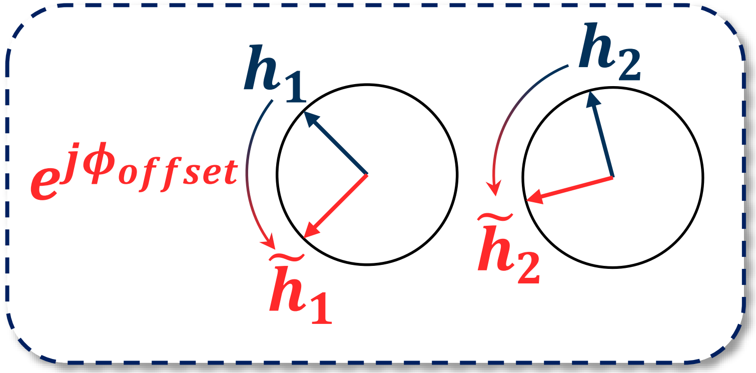
Challenge: Phase Offset from CSI to BFI

- Phase offset in CSI measurement:

$$\mathbf{H} = [\boldsymbol{h}_1, \boldsymbol{h}_2]$$

$$\Big\downarrow \quad \textit{Phase Offset } \phi_{offset}$$

$$\widetilde{\mathbf{H}} = [\widetilde{\boldsymbol{h}}_1, \widetilde{\boldsymbol{h}}_2]$$

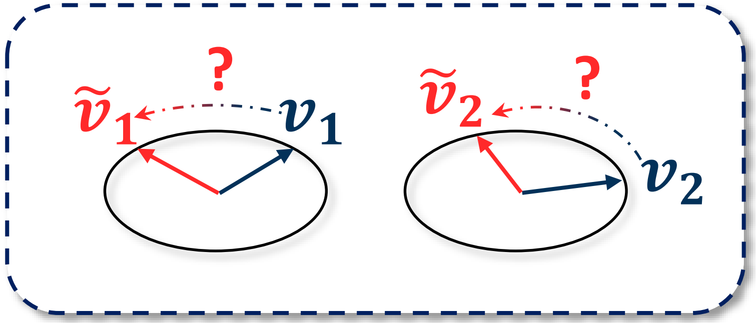

$\boldsymbol{h}_1$
$\boldsymbol{h}_2$
$e^{j\phi_{offset}}$
$\widetilde{\boldsymbol{h}}_1$
$\widetilde{\boldsymbol{h}}_2$

- BFI $\boldsymbol{V}$ is the right singular matrix of $\boldsymbol{H}$, i.e., $\boldsymbol{H} = \boldsymbol{U\Sigma V}^{\dagger}$:

$$\mathbf{V} = [\boldsymbol{v}_1, \boldsymbol{v}_2]$$

$$\Big\downarrow \quad \mathbf{V} = \left(\boldsymbol{\Sigma}^{-1}\mathbf{U}^{\dagger}\widetilde{\mathbf{H}}\right)^{\dagger}$$

$$\widetilde{\mathbf{V}} = [\widetilde{\boldsymbol{v}}_1, \widetilde{\boldsymbol{v}}_2]$$


$\widetilde{\boldsymbol{v}}_1$
?
$\boldsymbol{v}_1$
$\widetilde{\boldsymbol{v}}_2$
?
$\boldsymbol{v}_2$

Solution: Deriving a Phase-Offset-Free Feature

- New Feature $\mathrm{R} := \widetilde{\mathrm{V}}\Sigma^2\widetilde{\mathrm{V}}^\dagger$

R is phase-offset-free

Solution: Deriving a Phase-Offset-Free Feature

- **New Feature** $\mathbf{R} := \tilde{\mathbf{V}}\boldsymbol{\Sigma}^2\tilde{\mathbf{V}}^\dagger$
- Proof:

$$\boldsymbol{R} = V\Sigma U^\dagger U\Sigma V^\dagger = \left(U\Sigma V^\dagger\right)^\dagger\left(U\Sigma V^\dagger\right) = \boldsymbol{H}^\dagger\boldsymbol{H} = \begin{pmatrix} \boldsymbol{h}_1^\dagger\boldsymbol{h}_1 & \boldsymbol{h}_1^\dagger\boldsymbol{h}_2 \\ \boldsymbol{h}_2^\dagger\boldsymbol{h}_1 & \boldsymbol{h}_2^\dagger\boldsymbol{h}_2 \end{pmatrix}$$

Conjugate Multiplication
Between Antennas

⬇

Phase-Offset-Free

Solution: Deriving a Phase-Offset-Free Feature

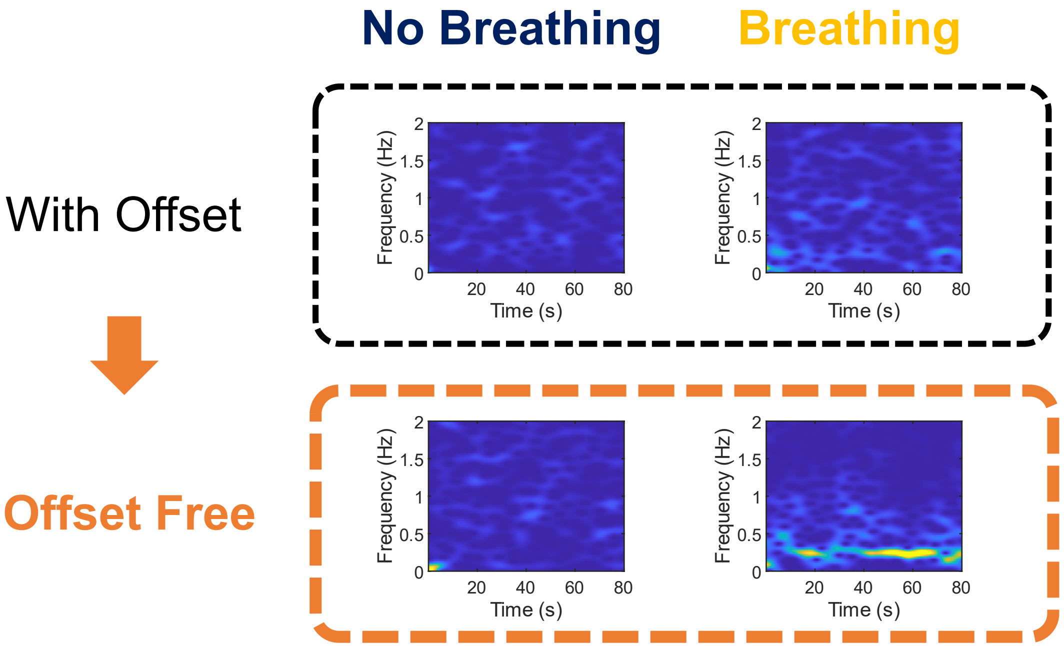
- **New Feature** $\mathbf{R}:=\tilde{\mathrm{V}}\Sigma^2\tilde{\mathrm{V}}^\dagger$
- Proof:

$$\boldsymbol{R} = V\Sigma \mathrm{U}^\dagger U\Sigma \mathrm{V}^\dagger = \left(U\Sigma \mathrm{V}^\dagger\right)^\dagger\left(U\Sigma \mathrm{V}^\dagger\right) = \boldsymbol{H}^\dagger\boldsymbol{H} = \begin{pmatrix} \boldsymbol{h}_1^\dagger\boldsymbol{h}_1 & \boldsymbol{h}_1^\dagger\boldsymbol{h}_2 \\ \boldsymbol{h}_2^\dagger\boldsymbol{h}_1 & \boldsymbol{h}_2^\dagger\boldsymbol{h}_2 \end{pmatrix}$$

Conjugate Multiplication Between Antennas

↓

Phase-Offset-Free



Evaluation Setup

Sniffer

Dell Laptop
(**no external antenna**)

with

Wireshark

Evaluation Setup

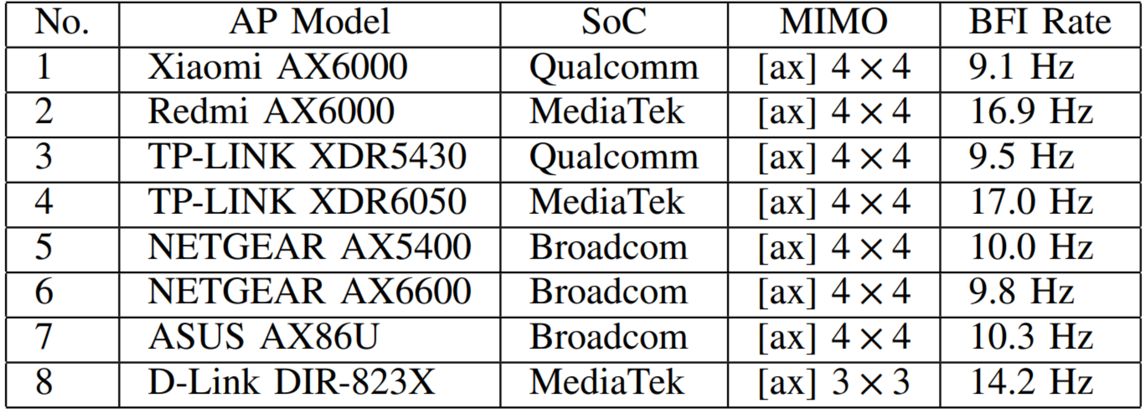
Sniffer

Dell Laptop
(no external antenna)

with

Wireshark

8 WiFi APs



No.	AP Model	SoC	MIMO	BFI Rate
1	Xiaomi AX6000	Qualcomm	[ax] 4 × 4	9.1 Hz
2	Redmi AX6000	MediaTek	[ax] 4 × 4	16.9 Hz
3	TP-LINK XDR5430	Qualcomm	[ax] 4 × 4	9.5 Hz
4	TP-LINK XDR6050	MediaTek	[ax] 4 × 4	17.0 Hz
5	NETGEAR AX5400	Broadcom	[ax] 4 × 4	10.0 Hz
6	NETGEAR AX6600	Broadcom	[ax] 4 × 4	9.8 Hz
7	ASUS AX86U	Broadcom	[ax] 4 × 4	10.3 Hz
8	D-Link DIR-823X	MediaTek	[ax] 3 × 3	14.2 Hz

Evaluation Setup

Sniffer

Dell Laptop
(no external antenna)

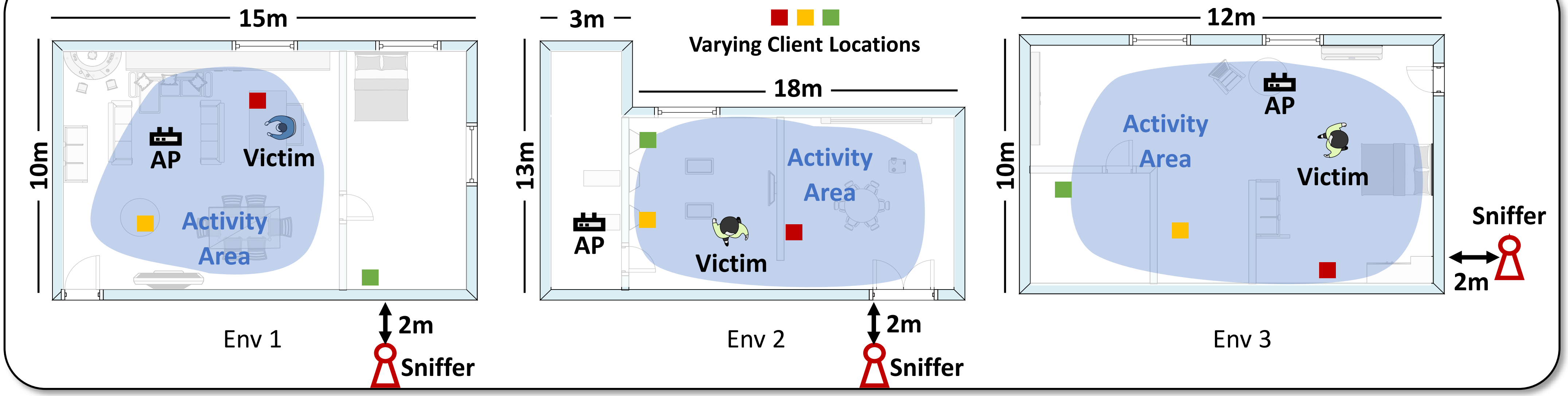
with

Wireshark

8 WiFi APs

No.	AP Model	SoC	MIMO	BFI Rate
1	Xiaomi AX6000	Qualcomm	[ax] 4 × 4	9.1 Hz
2	Redmi AX6000	MediaTek	[ax] 4 × 4	16.9 Hz
3	TP-LINK XDR5430	Qualcomm	[ax] 4 × 4	9.5 Hz
4	TP-LINK XDR6050	MediaTek	[ax] 4 × 4	17.0 Hz
5	NETGEAR AX5400	Broadcom	[ax] 4 × 4	10.0 Hz
6	NETGEAR AX6600	Broadcom	[ax] 4 × 4	9.8 Hz
7	ASUS AX86U	Broadcom	[ax] 4 × 4	10.3 Hz
8	D-Link DIR-823X	MediaTek	[ax] 3 × 3	14.2 Hz

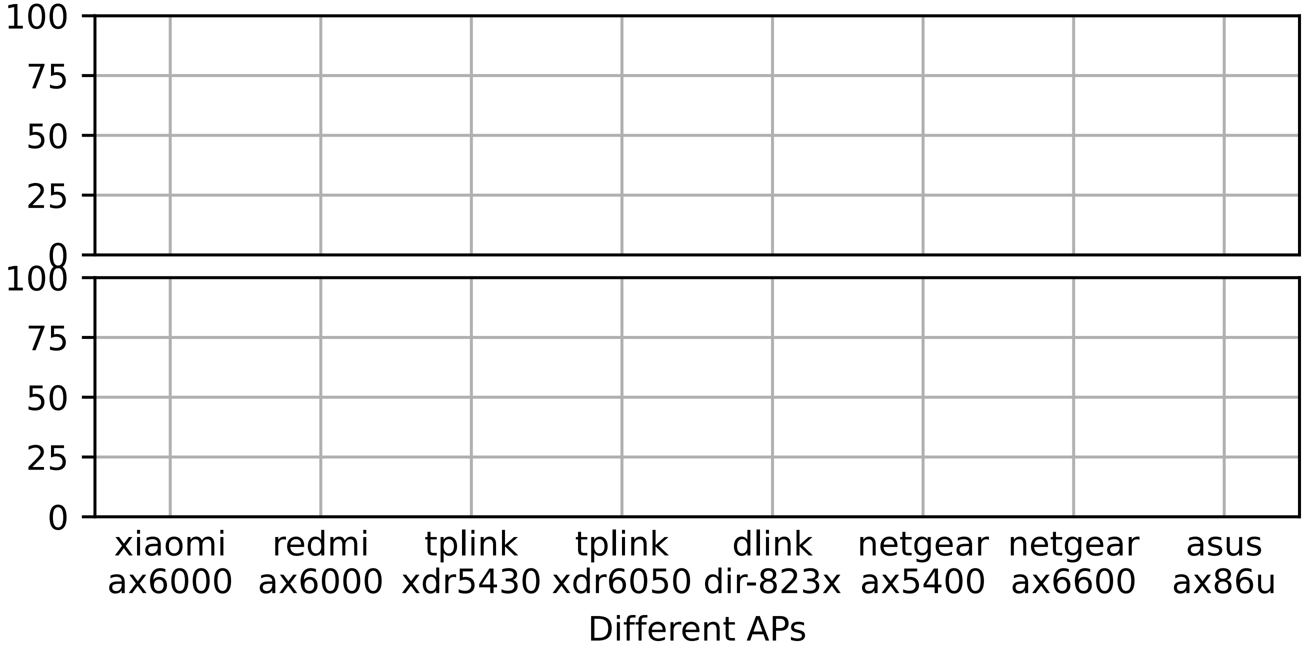
3 Environments with 9 Layouts



Summary of Evaluation Results

True Positive Rate (TPR)

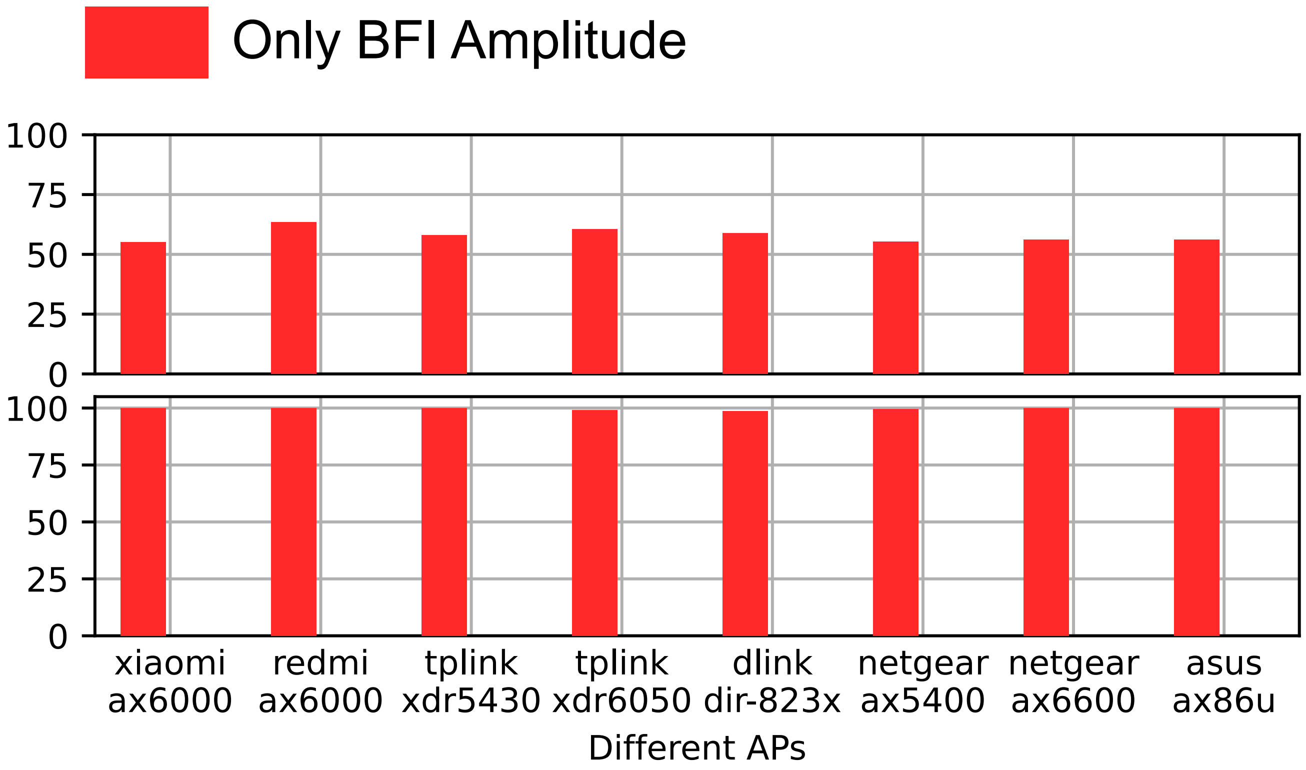
True Negative Rate (TNR)



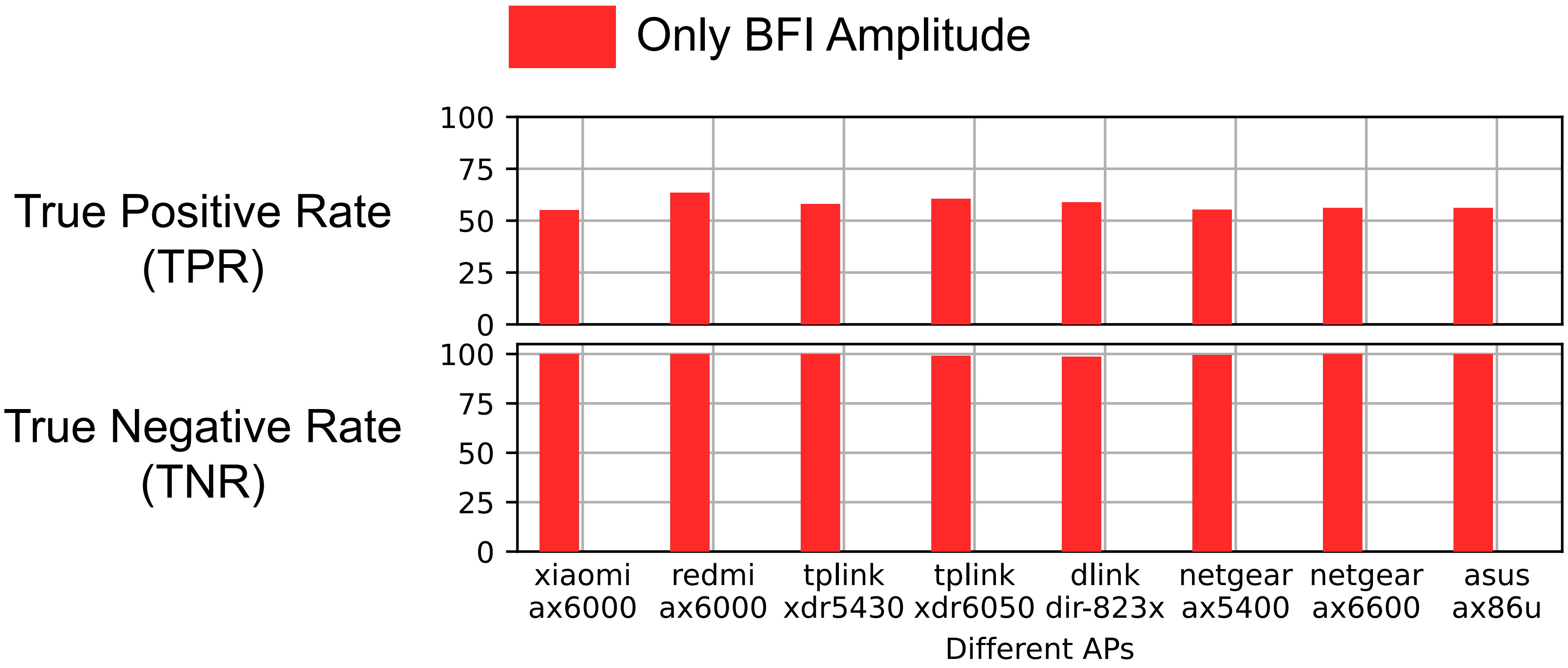
Summary of Evaluation Results

True Positive Rate (TPR)

True Negative Rate (TNR)

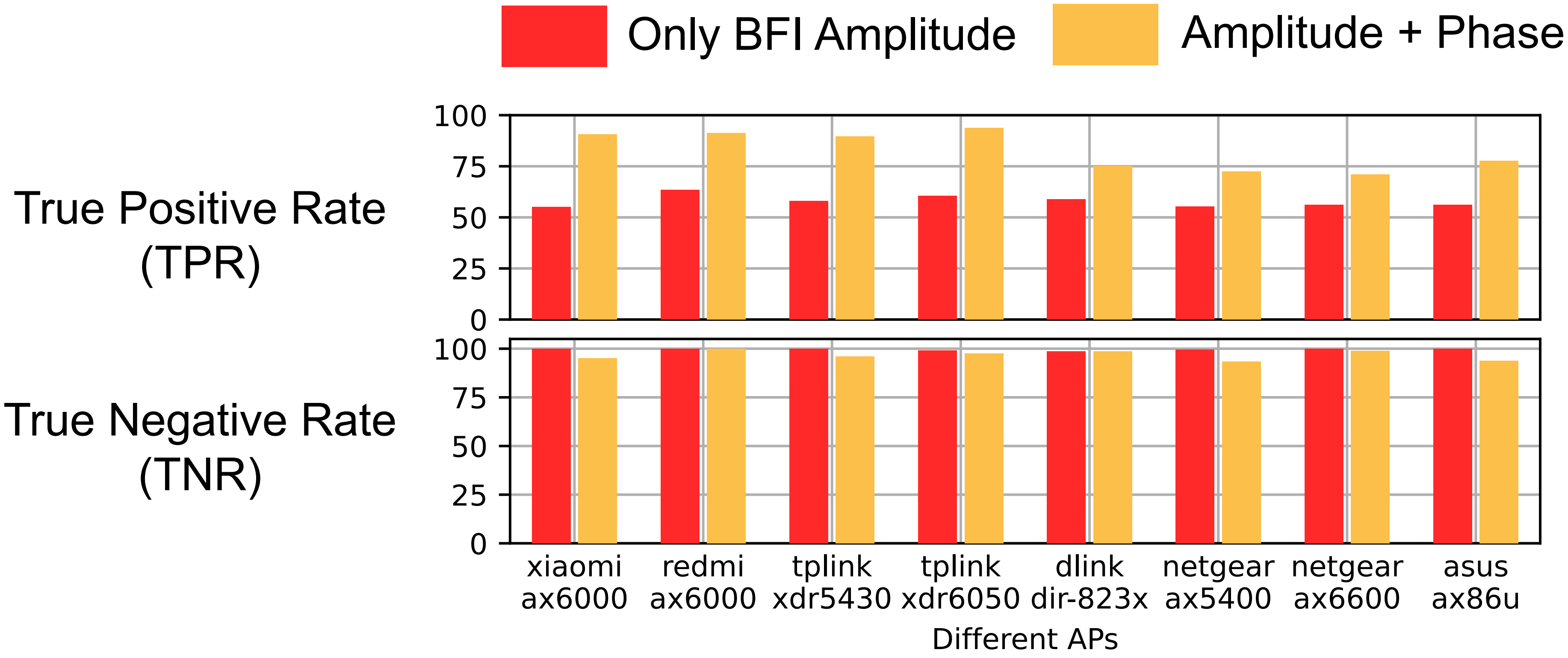


Summary of Evaluation Results



- Detecting **occupancy** states with 58% TPR and 99% TNR ☹

Summary of Evaluation Results



- Detecting **occupancy** states with **83%** TPR and **97%** TNR

Summary of Evaluation Results

- Accurate at detecting **occupancy** states (**83%** TPR and **97%** TNR)

Summary of Evaluation Results

- Accurate at detecting **occupancy** states (**83%** TPR and **97%** TNR)

- Works across **different client devices**

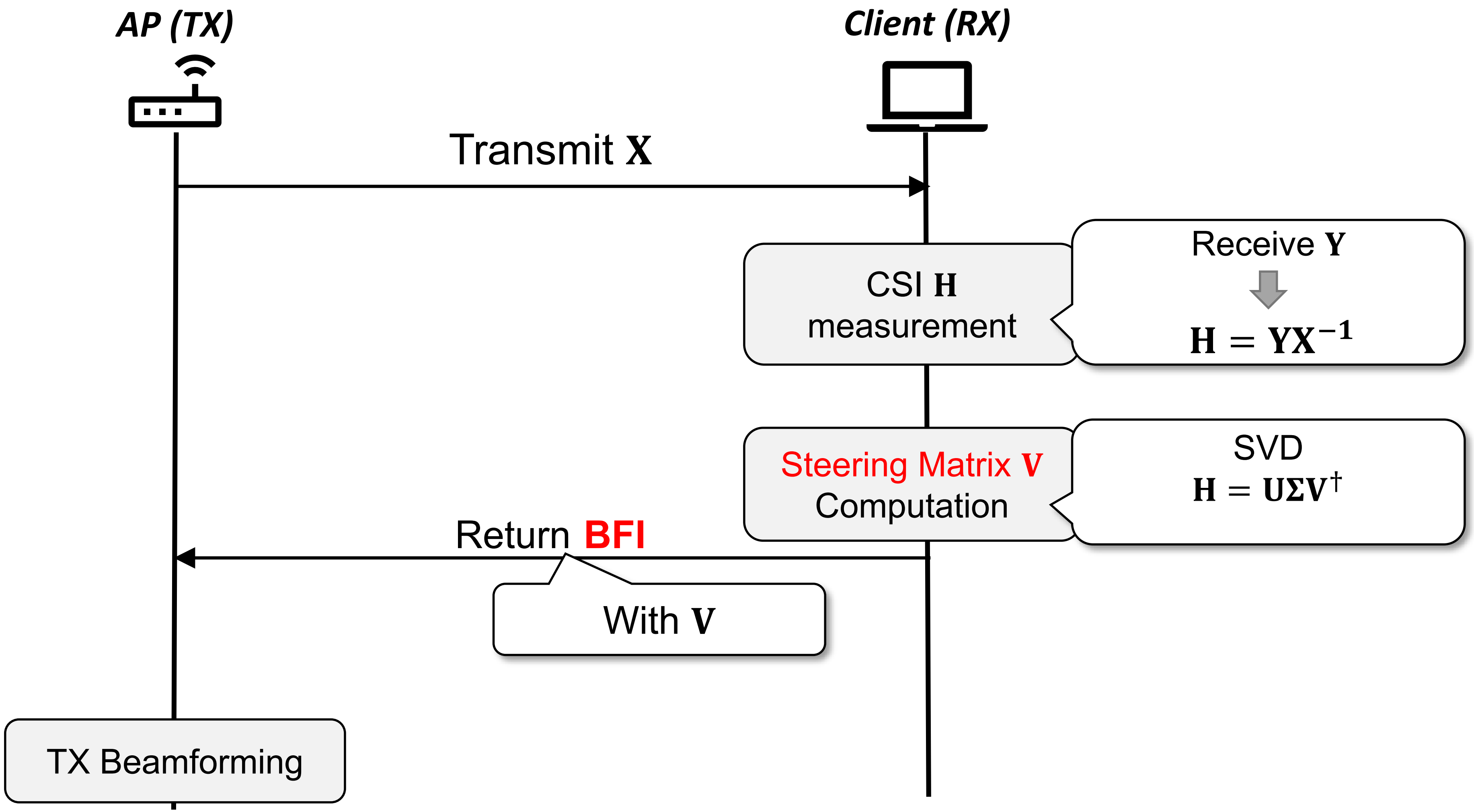
- Performs well with varying **background traffic types**, even when **idle**

- **88.3%** accuracy at a distance up to **20 meters**

Our Defense: Stay Plaintext But Preserve Privacy

Our Defense: Stay Plaintext But Preserve Privacy

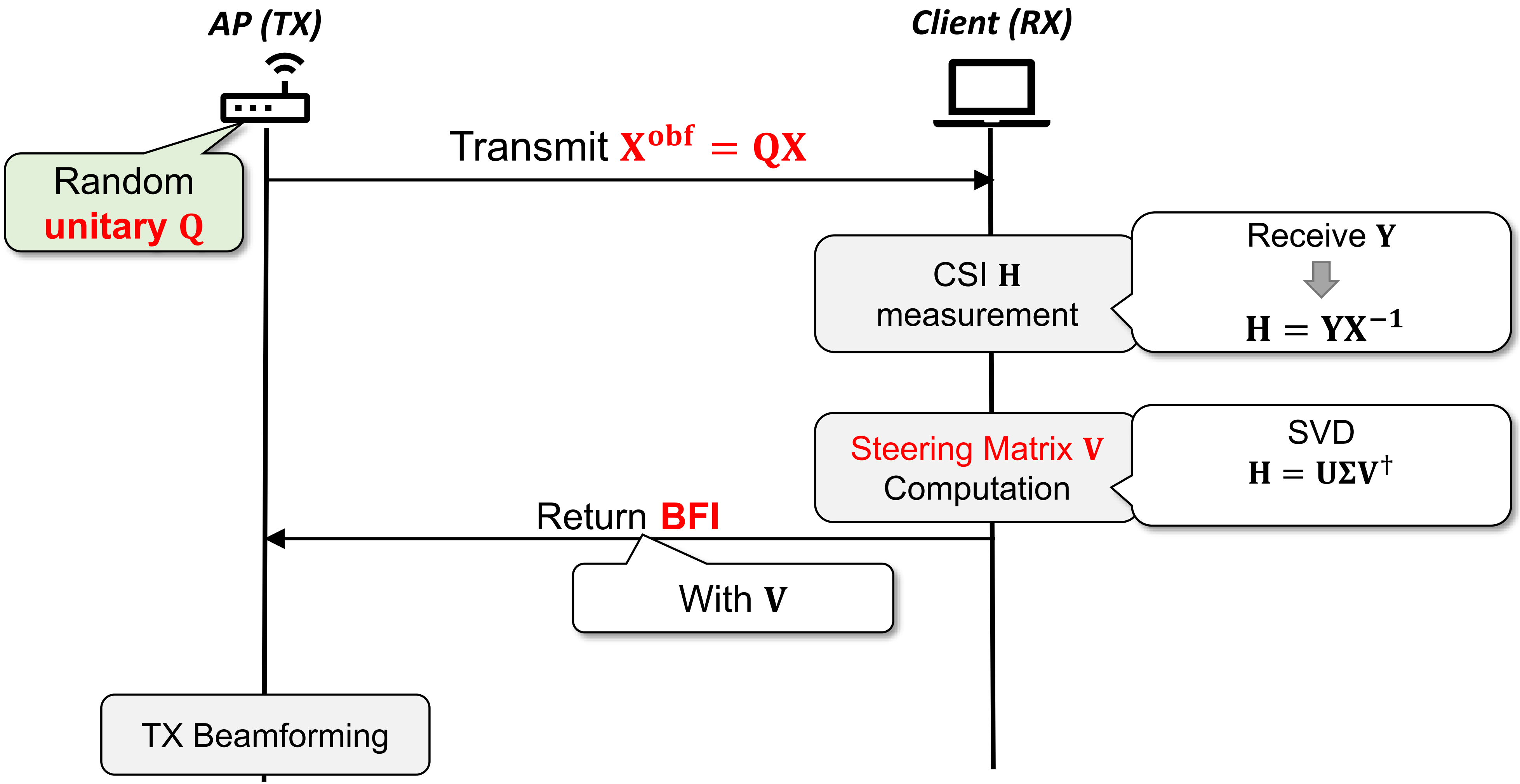
- Original BFI Measurement:



AP (TX)
Client (RX)
Transmit $\mathbf{X}$
Receive $\mathbf{Y}$
$\mathbf{H} = \mathbf{Y}\mathbf{X}^{-1}$
CSI $\mathbf{H}$ measurement
SVD
$\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{\dagger}$
Steering Matrix $\mathbf{V}$ Computation
Return BFI
With $\mathbf{V}$
TX Beamforming

Our Defense: Stay Plaintext But Preserve Privacy

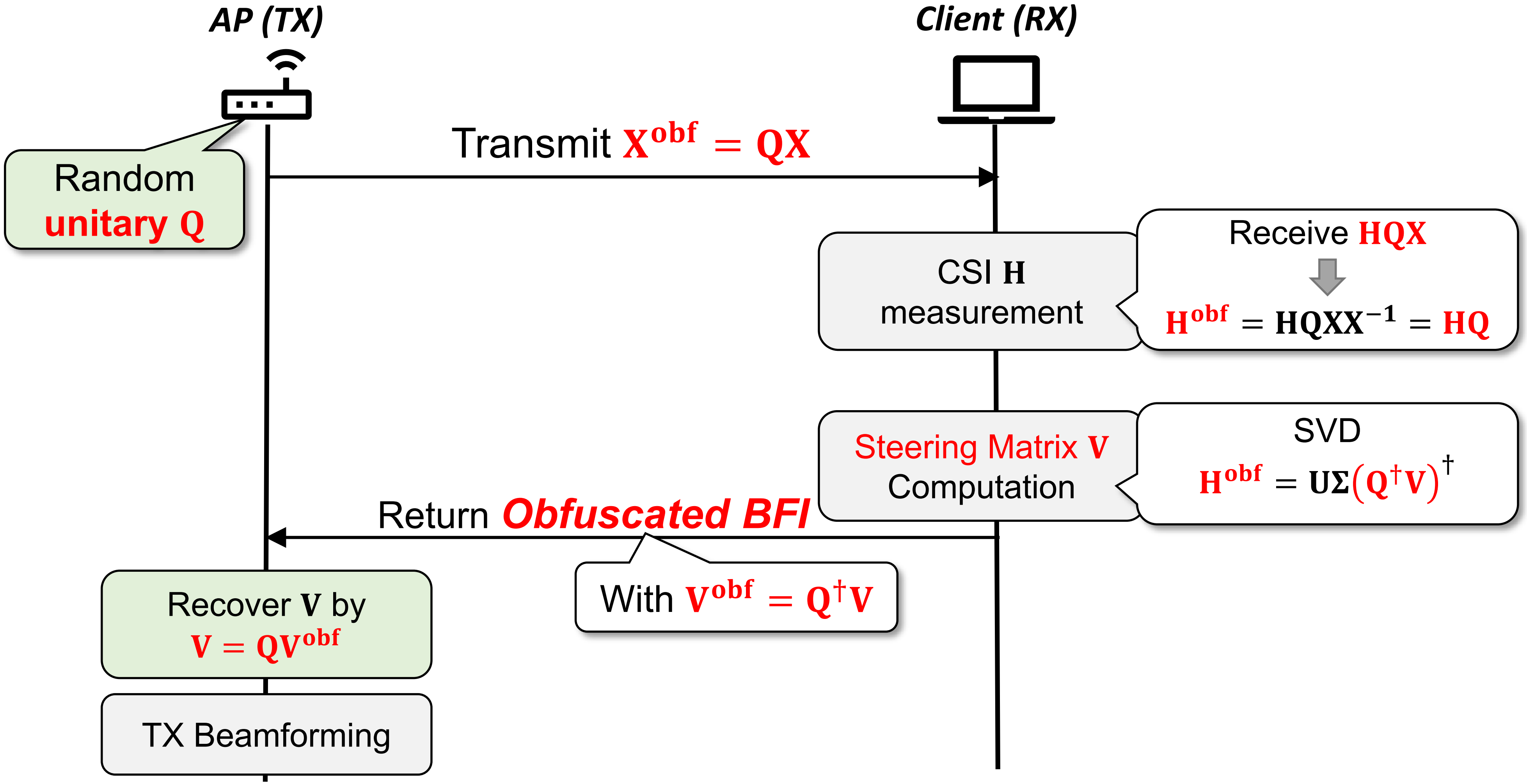
- BFI Measurement with **a random mapping $\mathbf{Q}$ on training symbol $\mathbf{X}$:**



AP (TX)
Client (RX)
Random unitary $\mathbf{Q}$
Transmit $\mathbf{X}^{\mathbf{obf}} = \mathbf{QX}$
CSI $\mathbf{H}$ measurement
Receive $\mathbf{Y}$
$\mathbf{H} = \mathbf{YX}^{-1}$
Steering Matrix $\mathbf{V}$ Computation
SVD
$\mathbf{H} = \mathbf{U\Sigma V}^{\dagger}$
Return BFI
With $\mathbf{V}$
TX Beamforming

Our Defense: Stay Plaintext But Preserve Privacy

- BFI Measurement with **a random mapping $\mathbf{Q}$ on training symbol $\mathbf{X}$:**



AP (TX)

Client (RX)

Random **unitary $\mathbf{Q}$**

Transmit $\mathbf{X}^{\mathbf{obf}} = \mathbf{QX}$

CSI $\mathbf{H}$ measurement

Receive $\mathbf{HQX}$

$\mathbf{H}^{\mathbf{obf}} = \mathbf{HQXX}^{-1} = \mathbf{HQ}$

Steering Matrix $\mathbf{V}$ Computation

SVD

$\mathbf{H}^{\mathbf{obf}} = \mathbf{U\Sigma}\left(\mathbf{Q}^{\dagger}\mathbf{V}\right)^{\dagger}$

Return ***Obfuscated BFI***

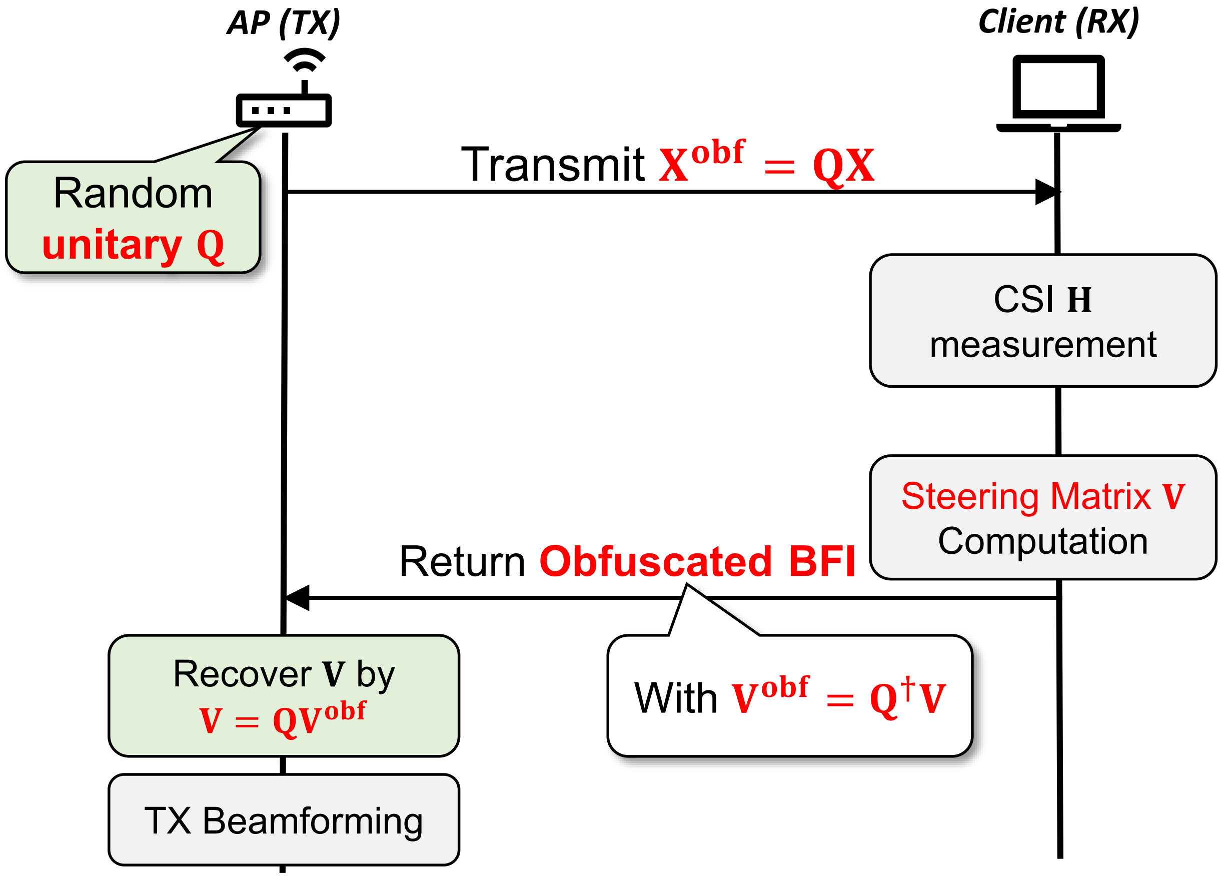
With $\mathbf{V}^{\mathbf{obf}} = \mathbf{Q}^{\dagger}\mathbf{V}$

Recover $\mathbf{V}$ by $\mathbf{V} = \mathbf{QV}^{\mathbf{obf}}$

TX Beamforming

Our Defense: Stay Plaintext But Preserve Privacy

- BFI Measurement with **a random mapping $\mathbf{Q}$ on training symbol $\mathbf{X}$:**



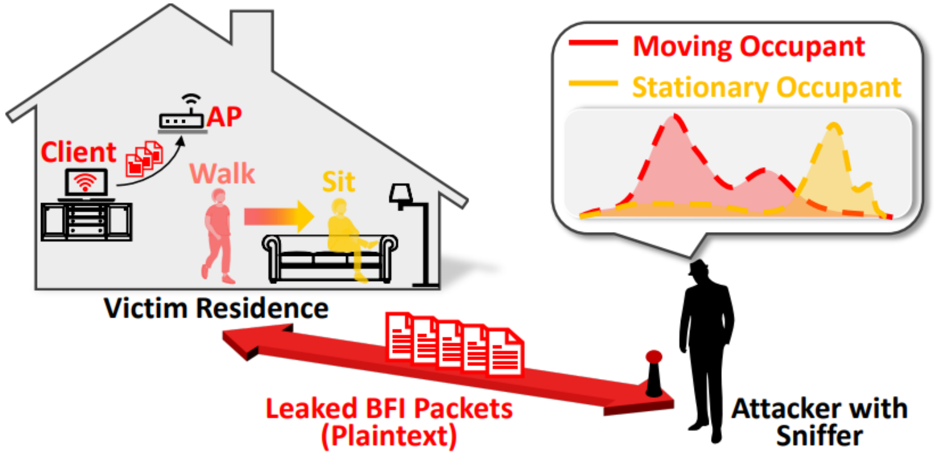
AP (TX)
Client (RX)
Random unitary $\mathbf{Q}$
Transmit $\mathbf{X}^{\mathrm{obf}} = \mathbf{QX}$
CSI $\mathbf{H}$ measurement
Steering Matrix $\mathbf{V}$ Computation
Return Obfuscated BFI
With $\mathbf{V}^{\mathrm{obf}} = \mathbf{Q}^{\dagger}\mathbf{V}$
Recover $\mathbf{V}$ by $\mathbf{V} = \mathbf{QV}^{\mathrm{obf}}$
TX Beamforming

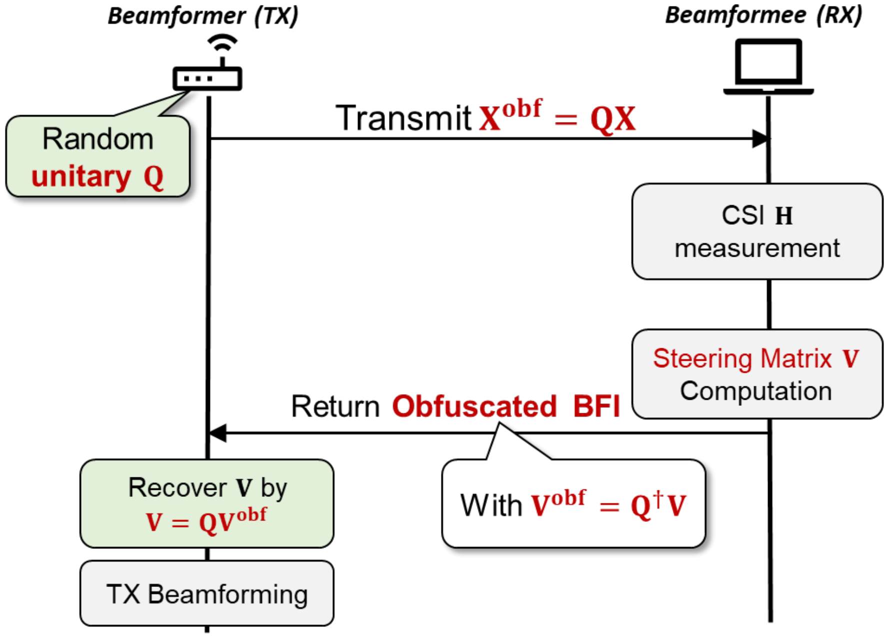
Key Features:

- **Minimal Hardware Modification**
  - Client: Unaffected
  - AP: Reusing Spatial Mapping Mechanism
- **Minimal Impact on Communication**
  - Beamforming is still effective.
- **Effective Privacy Preserving**
  - Obfuscated BFI cannot infer occupancy state.

Conclusion

- We introduce LeakyBeam, **a practical adversarial occupancy detection attack** utilizing the **BFI side channel**.
- We propose **a novel defense mechanism** to potential attacks with plaintext BFI packets.





Beamformer (TX)
Beamformee (RX)
Random unitary $\mathbf{Q}$
Transmit $\mathbf{X}^{\mathrm{obf}} = \mathbf{QX}$
CSI $\mathbf{H}$ measurement
Steering Matrix $\mathbf{V}$ Computation
Return Obfuscated BFI
With $\mathbf{V}^{\mathrm{obf}} = \mathbf{Q}^{\dagger}\mathbf{V}$
Recover $\mathbf{V}$ by $\mathbf{V} = \mathbf{QV}^{\mathrm{obf}}$
TX Beamforming

Thank you!

Homepage

Mail: ruixiao24@zju.edu.cn

Rui Xiao

PhD candidate at Zhejiang University

Wireless, Mobile, Sensing, Security

I’m seeking a ***post-doctoral position*** starting in ***Fall 2025***.
Please feel free to contact me!