Exploiting and Securing WiFi for Pervasive Human Sensing

Rui Xiao @ Zhejiang University

Pervasive WiFi Devices

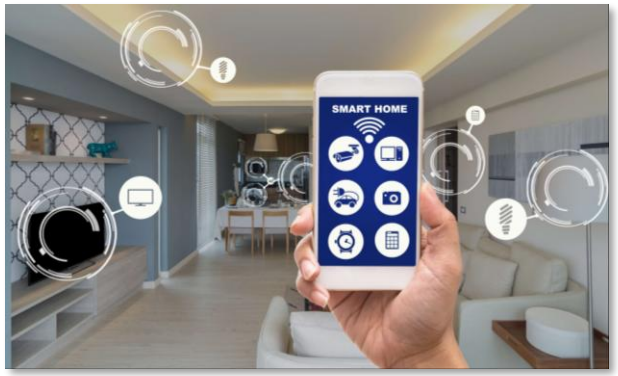
➢Commercial WiFi Devices:

Phone & Smart Watch

Smart Speaker

Smart TV

➢WiFi-enabled Applications:

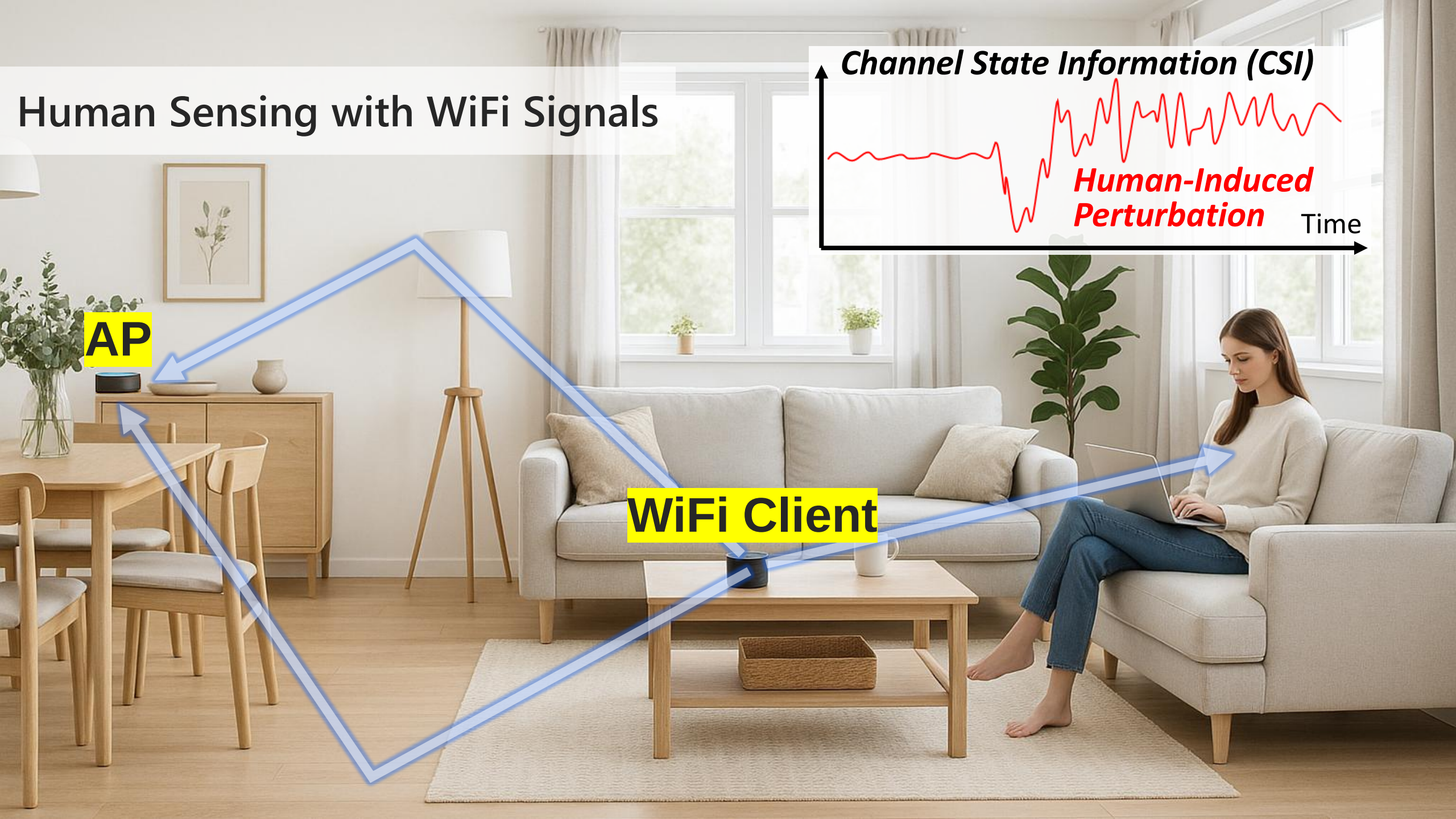


Smart Home

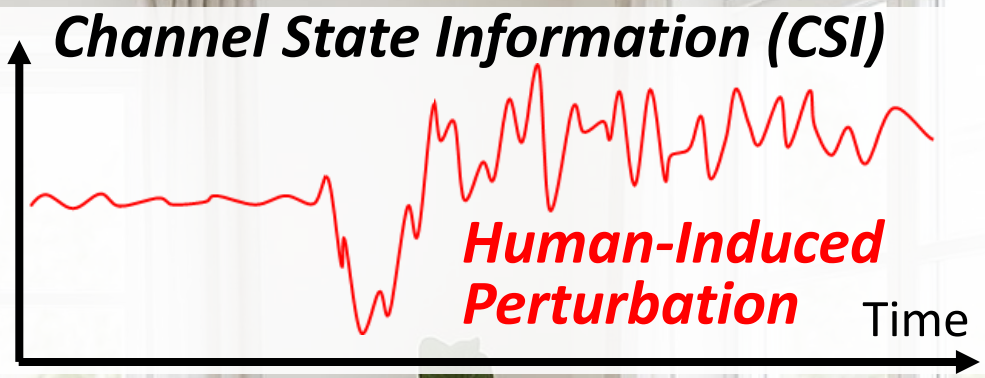
Smart Factory

Smart Office

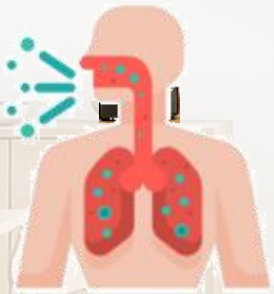
Human Sensing with WiFi Signals



Human Sensing with WiFi Signals



Sensing Applications



Vital Sign Monitoring

Activity Recognition

Tracking

However, WiFi Signal ***leaks beyond intended boundary****...*

Human Sensing with WiFi Signals

The Sensing Capability of WiFi is _____

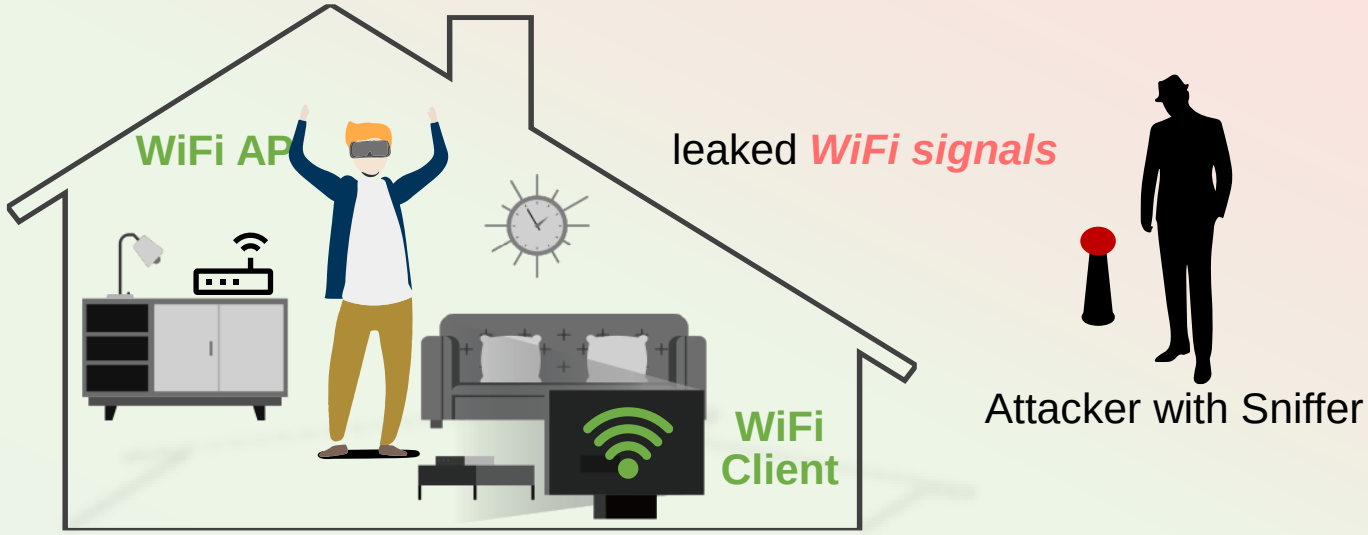
I. A novel enabler for pervasive human sensing

- *OneFi, a few-shot solution for generalizability [SenSys'21]*
- *Platform: Traditional Analog CSI*

II. A new vector for privacy leakage

- *LeakyBeam, an adversarial attack [NDSS'25]*
- *Platform: New Digital BFI Packets*

New Possibility?



The Sensing Capability of WiFi is _____

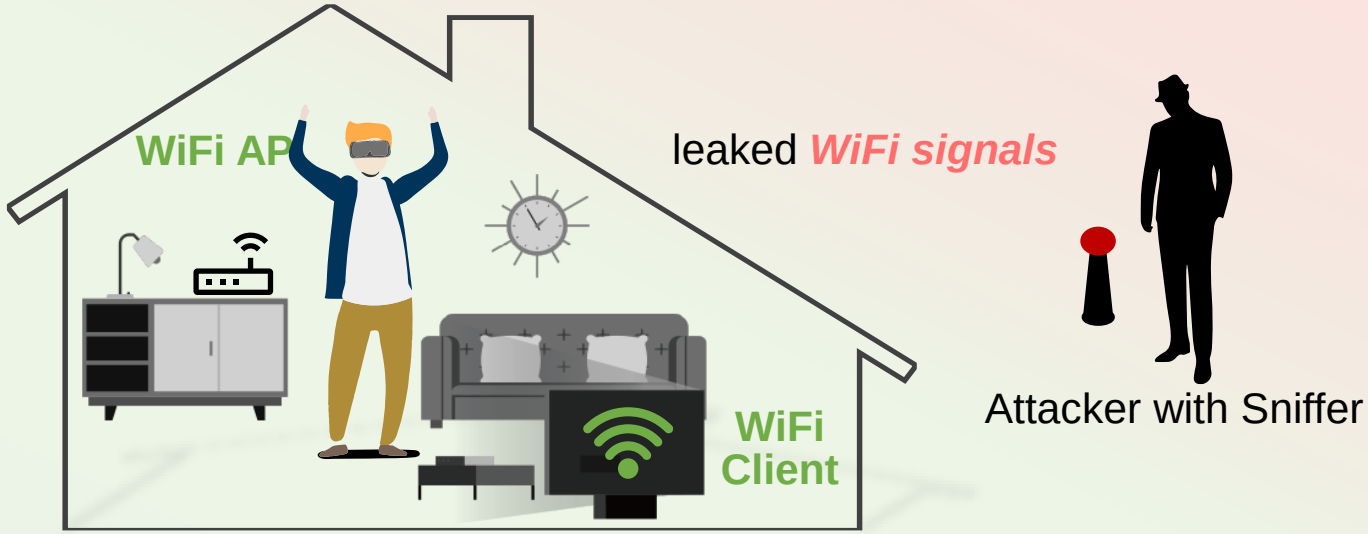
I. A novel enabler for pervasive human sensing

- *OneFi, a few-shot solution for generalizability [SenSys'21]*
- *Platform: Traditional Analog CSI*

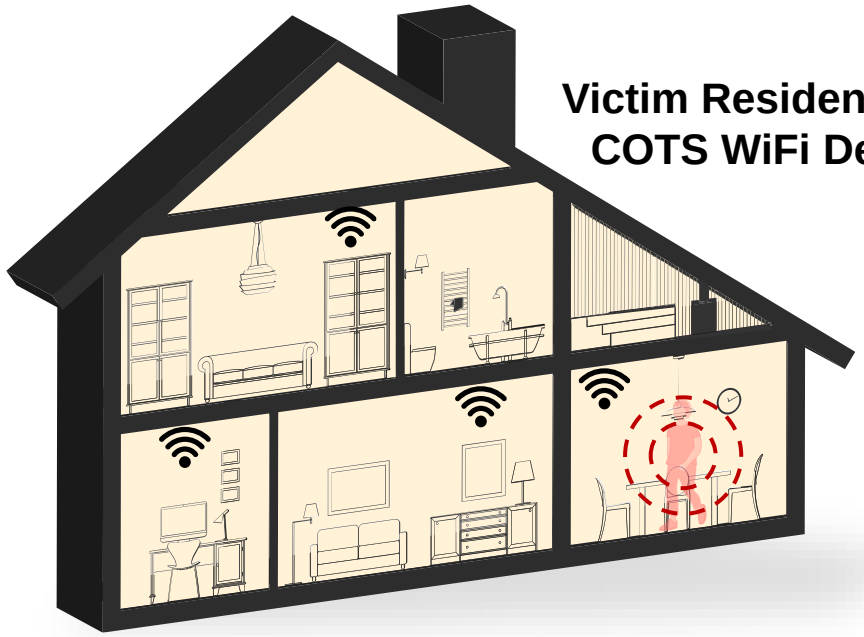
II. A new vector for privacy leakage

- *LeakyBeam, an adversarial attack [NDSS'25]*
- *Platform: New Digital BFI Packets*

New Possibility?



Adversarial Human Sensing: Motivation Scenario



Victim Residence with COTS WiFi Devices

Distant WiFi Sniffer

Adversarial Human Sensing: Motivation Scenario

Victim Residence with COTS WiFi Devices

Distant WiFi Sniffer

Adversarial Human Sensing: Motivation Scenario

Victim Residence with COTS WiFi Devices

Distant WiFi Sniffer

Adversarial Human Sensing: Motivation Scenario

Victim Residence with COTS WiFi Devices

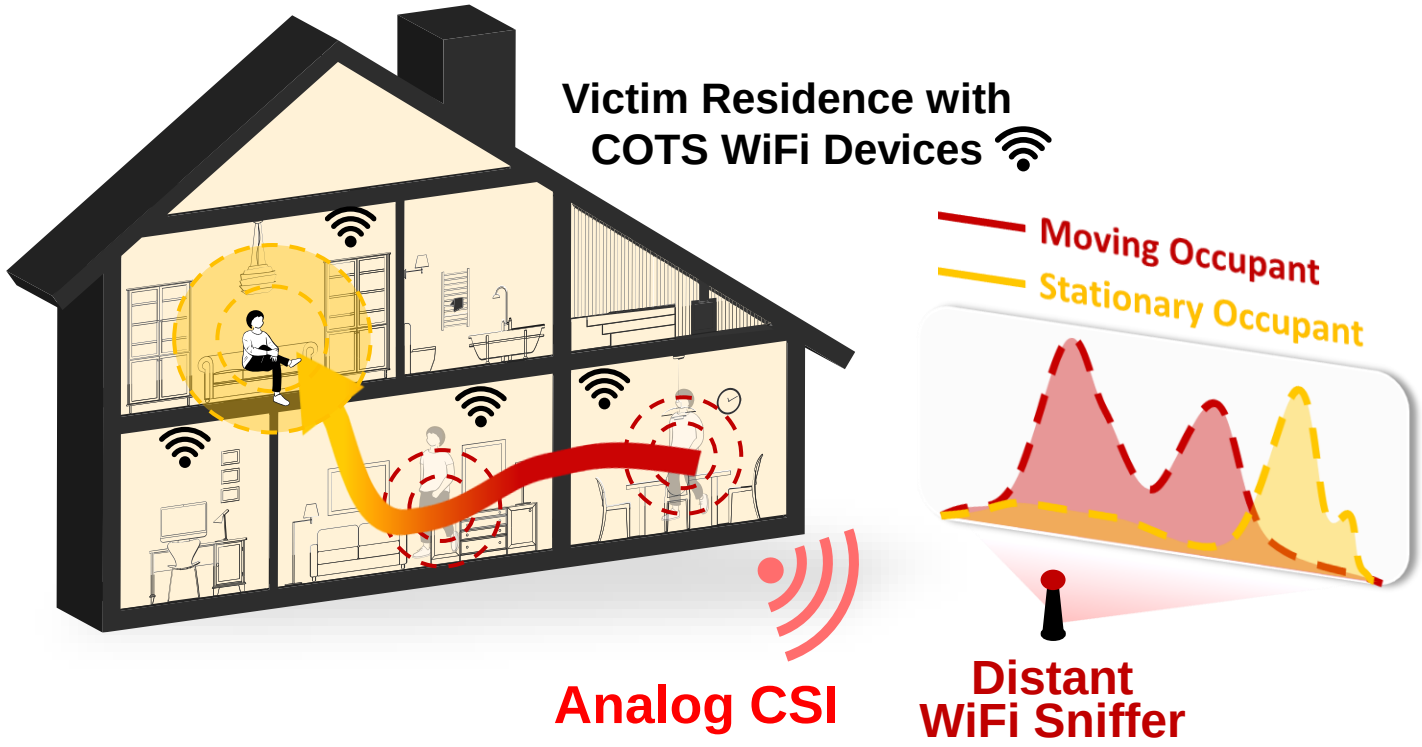
Distant WiFi Sniffer

Adversarial Human Sensing: Motivation Scenario

Victim Residence with COTS WiFi Devices

Distant WiFi Sniffer

Adversarial Human Sensing: Motivation Scenario



Continuous, Passive
Monitoring!

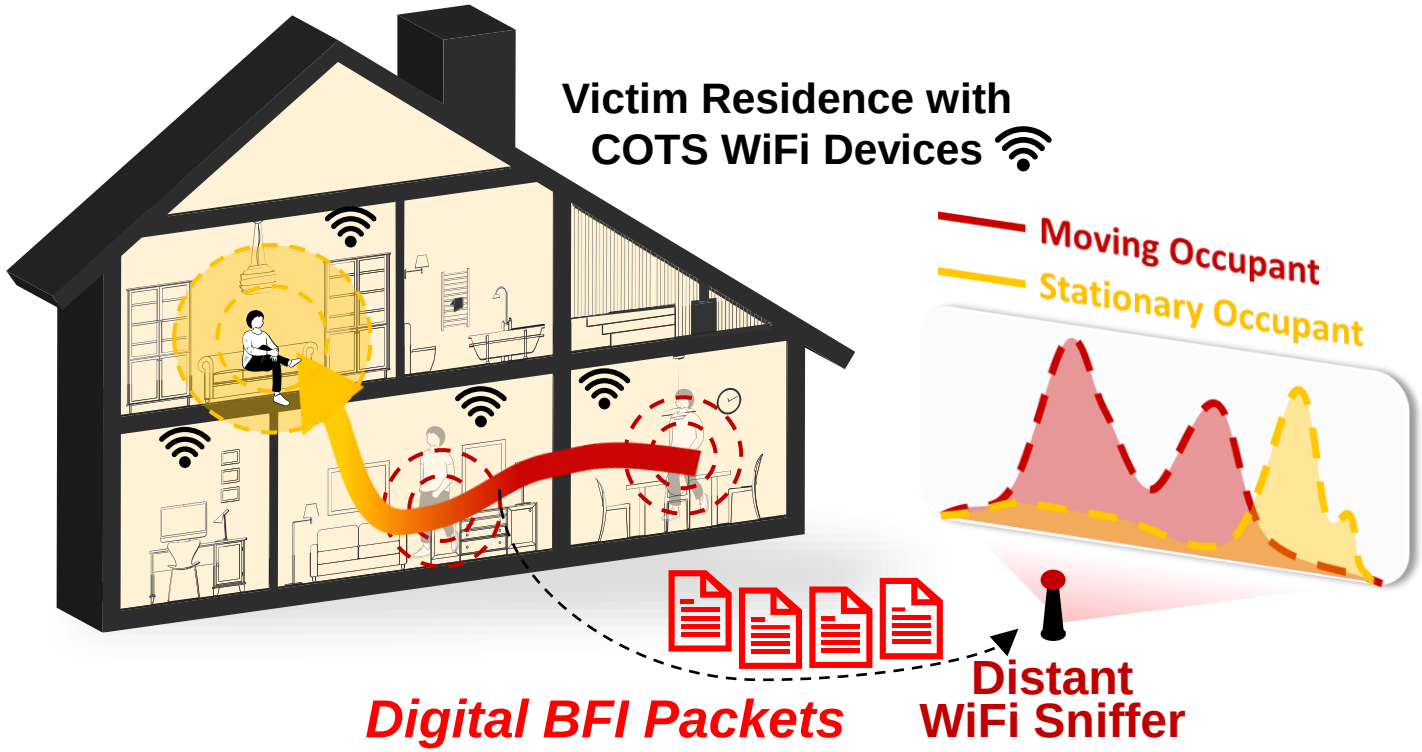
Spy Activity

Neighborhood Surveillance

- Problem: Signal Attenuation → **Limited Attack Distance** using **analog CSI**

Side-Channel: *CSI from* ***Beamforming Feedback Information (BFI) Packets***

Adversarial Human Sensing: Motivation Scenario



Continuous, Passive Surveillance!

Spy Activity

Neighborhood Surveillance

- Problem: Signal Attenuation → **Limited Attack Distance** using **analog CSI**

Side-Channel: *CSI from* ***Beamforming Feedback Information (BFI) Packets***

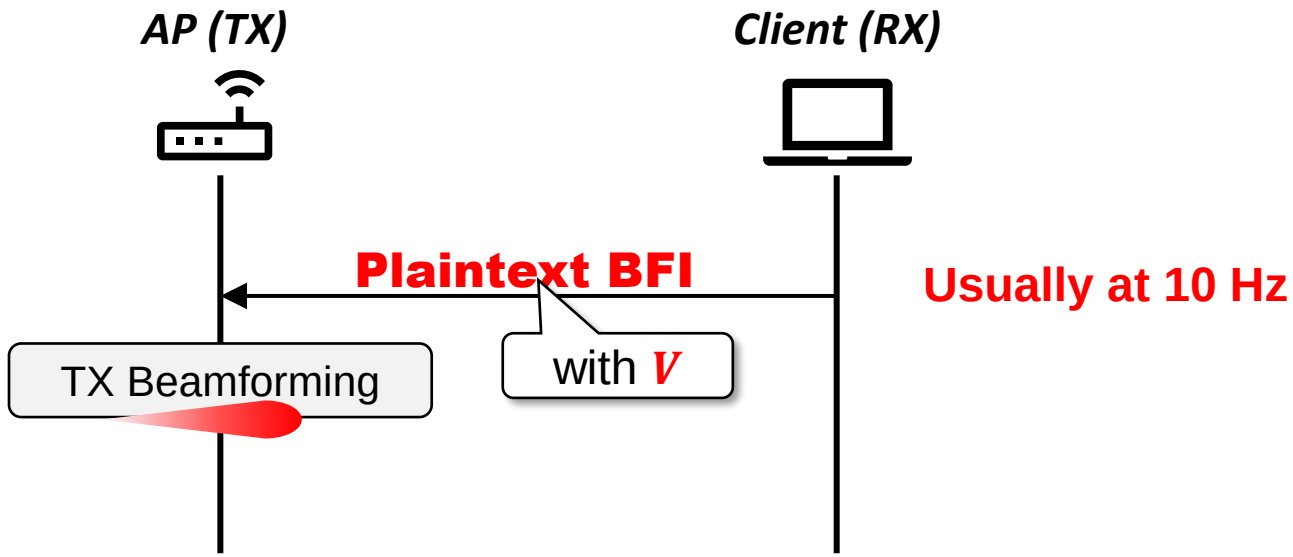
- CSI in digital BFI packets will not be distorted by signal attenuation.
- BFI Packets exist in 86% of WiFi 5/6 devices and are plaintext.

BFI: Control Frame with Compressed CSI

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

BFI: Control Frame with Compressed CSI

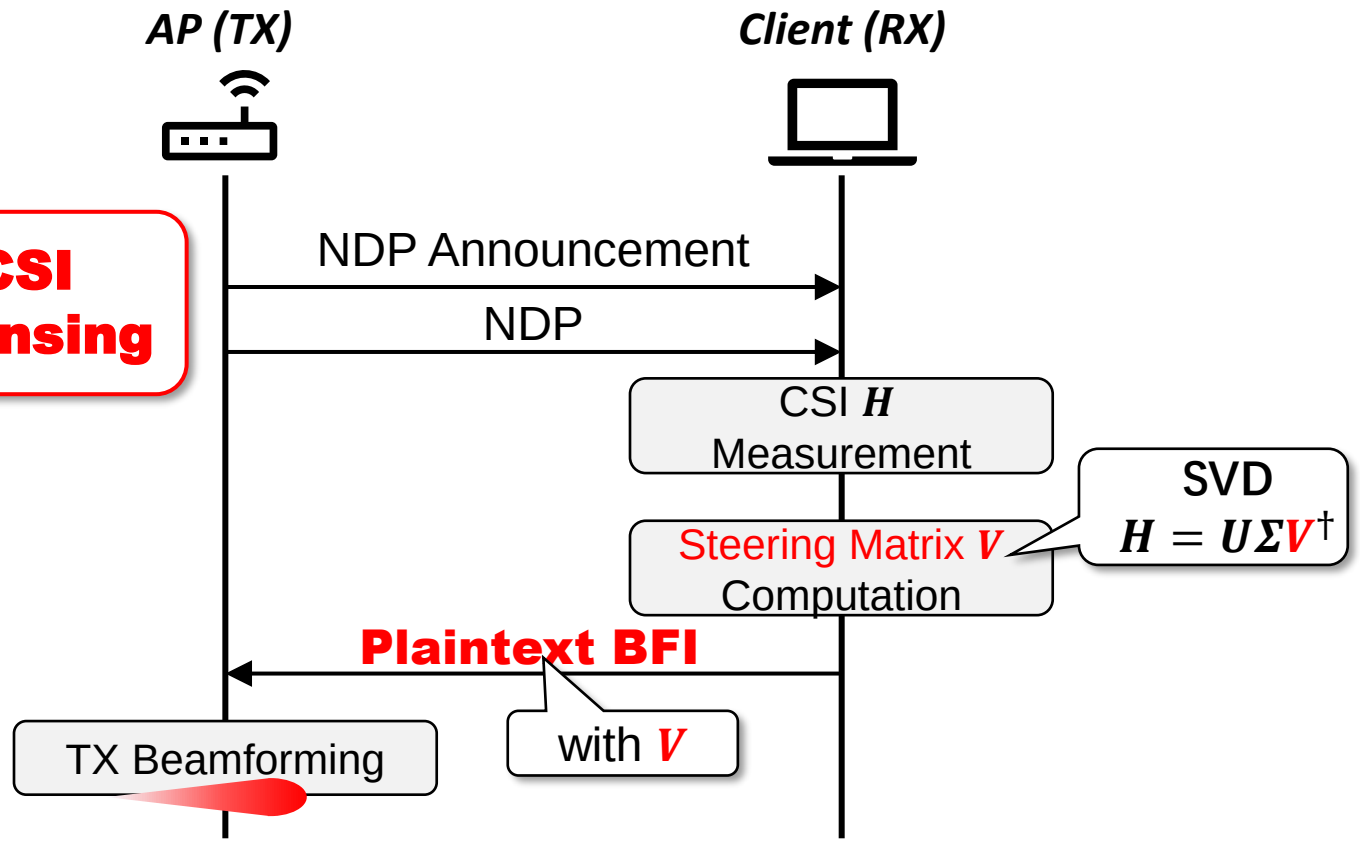
- BFI is for beamforming -- **Directional Signal Transmission** for SNR improvement
- AP needs a **steering matrix V (spatial information)** for beam direction control



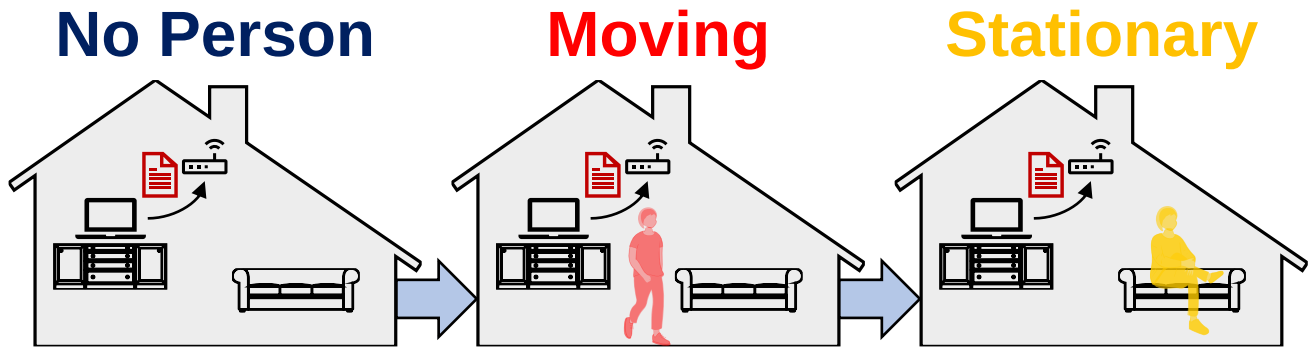
BFI: Control Frame with Compressed CSI

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

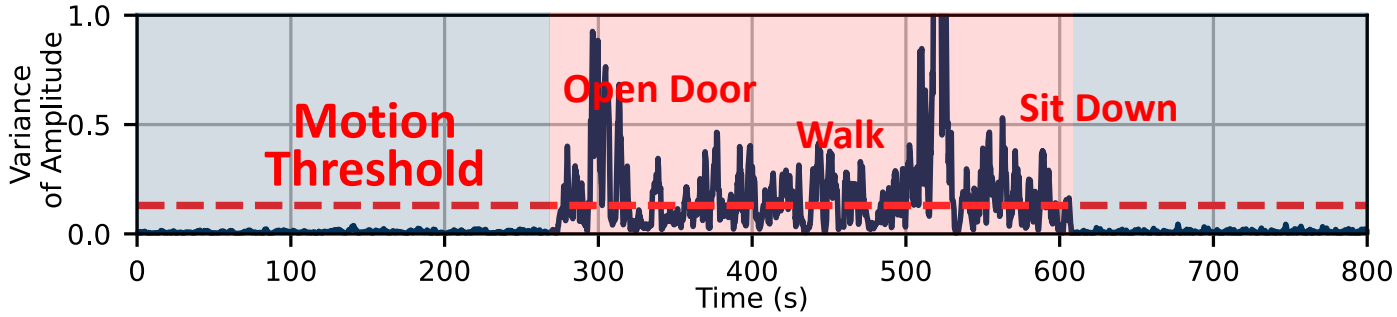
BFI is compressed CSI and can be used for sensing



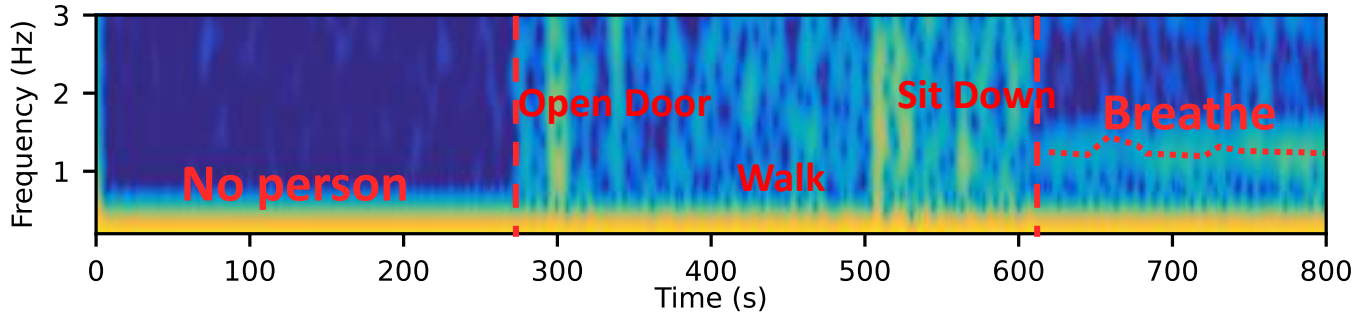
(Adversarial) Human Sensing with BFI



- Scenario 1: Motion Detection
  - Using **BFI amplitude**

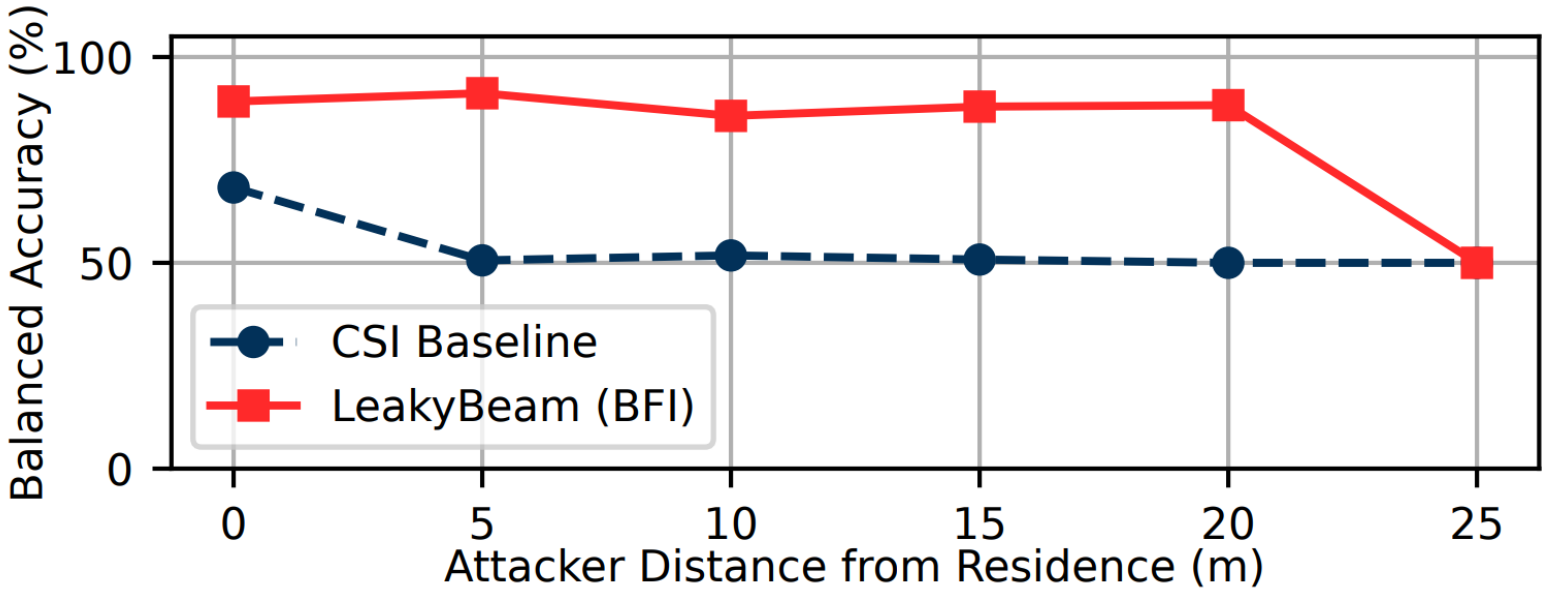


- Scenario 2: Breathe Detection
  - Using **BFI phase**



Implementation and Evaluation

- Sniffer: Dell Laptop (no external antenna) + Wireshark
- Detecting Breathing and Motion states with **90%** accuracy
- Compared with CSI Baseline, BFI is effective at a distance of **20 m**



The Sensing Capability of WiFi is _____

I. A novel enabler for pervasive human sensing

- *OneFi, a few-shot solution for generalizability [SenSys'21]*
- *Platform: Traditional Analog CSI*

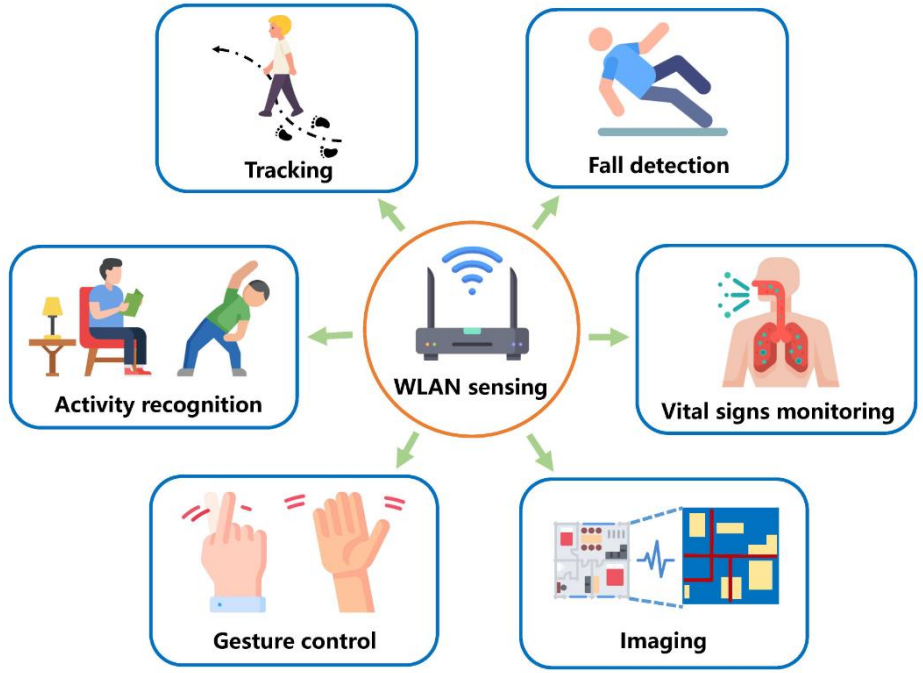
II. A new vector for privacy leakage

- *LeakyBeam, an adversarial attack [NDSS'25]*
- *Platform:* ***New Digital BFI Packets***

New Possibility?

Future Works…

Future Works



- ➢ Pervasive WiFi Sensing Platform with BFI
  - Privacy Enhancement for BFI
  - Novel BFI Sensing Methodology
  - Dual-purpose BFI design for Integrated sensing and communication
- Open Challenge: Environmental Ambiguity

Providing novel wireless sensing solution that is pervasive, robust and secure?

Thank you!

Homepage

Mail: ruixiao24@zju.edu.cn

Rui Xiao

Wireless, Mobile, Sensing, Security

Start in **Fall 2025**, I'll join ***Shanghai University of Finance and Economics*** as an **Assistant Professor**.