ActListener: Imperceptible Activity Surveillance by Pervasive Wireless Infrastructures

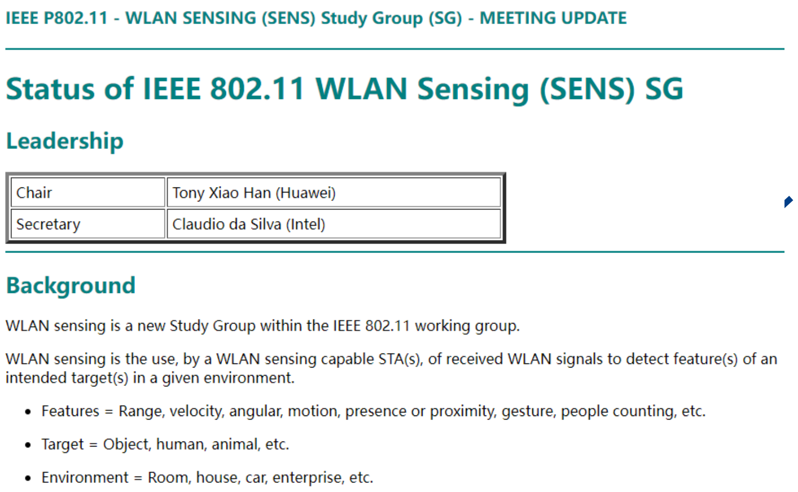
Presenter: Wenjin Zhang

Li Lu, Zhongjie Ba, Feng Lin, Jinsong Han, Kui Ren
School of Cyber Science and Technology
Key Laboratory of Blockchain and Cyberspace Governance of Zhejiang Province
Zhejiang University

浙江大学 网络空间安全学院
SCHOOL OF CYBER SCIENCE AND TECHNOLOGY
ZHEJIANG UNIVERSITY

ICDCS 2022
42nd IEEE International Conference on Distributed Computing Systems
July 10 - July 13, 2022 // Bologna, Italy

WiFi-based Sensing



IEEE P802.11 - WLAN SENSING (SENS) Study Group (SG) - MEETING UPDATE

Status of IEEE 802.11 WLAN Sensing (SENS) SG

Leadership

Chair	Tony Xiao Han (Huawei)
Secretary	Claudio da Silva (Intel)

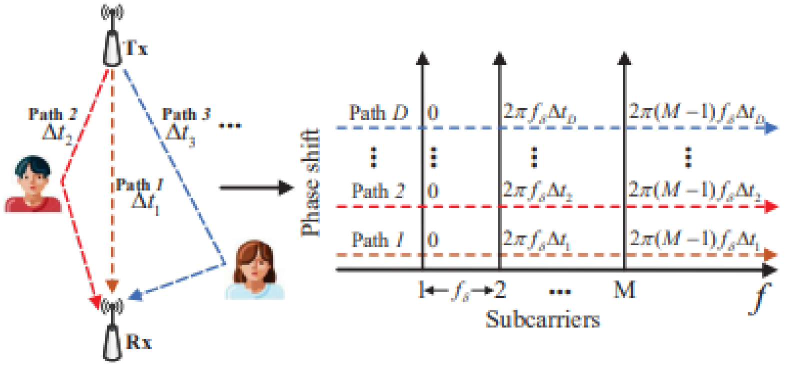
Background

WLAN sensing is a new Study Group within the IEEE 802.11 working group.

WLAN sensing is the use, by a WLAN sensing capable STA(s), of received WLAN signals to detect feature(s) of an intended target(s) in a given environment.

- Features = Range, velocity, angular, motion, presence or proximity, gesture, people counting, etc.
- Target = Object, human, animal, etc.
- Environment = Room, house, car, enterprise, etc.

Upcoming WiFi standard

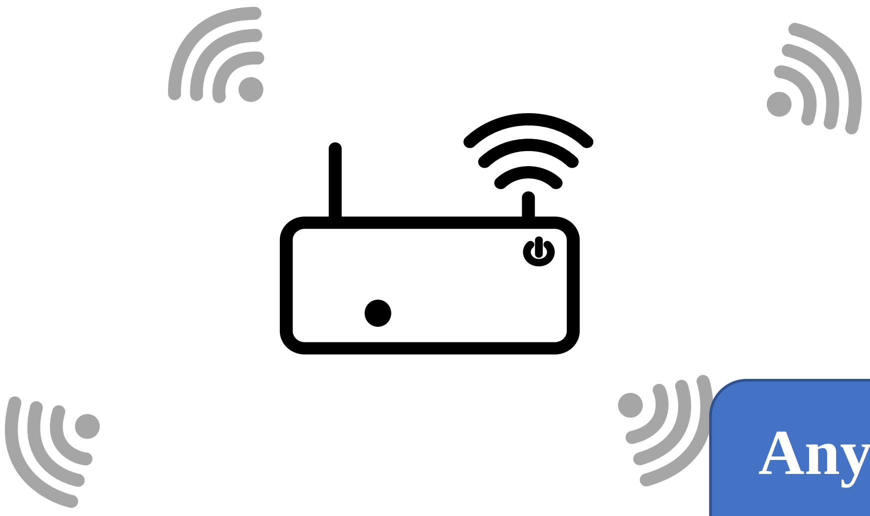


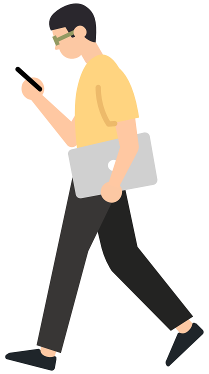
Active research efforts

Relative enterprises

[1] E. Au. New standards initiative for using wi-fi for sensing [standards]. IEEE Vehicular Technology Magazine, vol. 15, no. 1, pp. 119–119, 2020.
[2] H. Kong, L. Lu, J. Yu, Y. Chen, X. Xu, F. Tang, Y.-C. Chen. MultiAuth: Enable Multi-User Authentication with Single Commodity WiFi Device. Proceedings of ACM MobiHoc. Shanghai, China. 2021.
[3] Perspicace Intelligent Technology - AI creates Happy Life. https://www.perspicace-china.com, 2021.

Broadcasting Manner vs. Leakage Threat





…asting

…in any

position

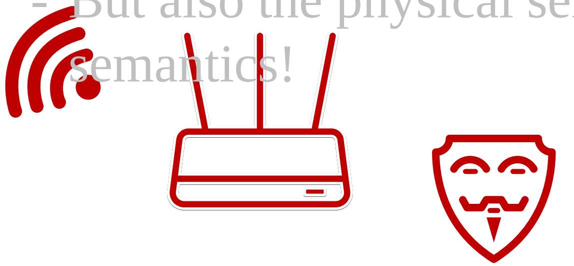
- Non-intrusive communication and sensing

Any security problem underlying the broadcasting manner?

Broadcasting Manner vs. Leakage Threat

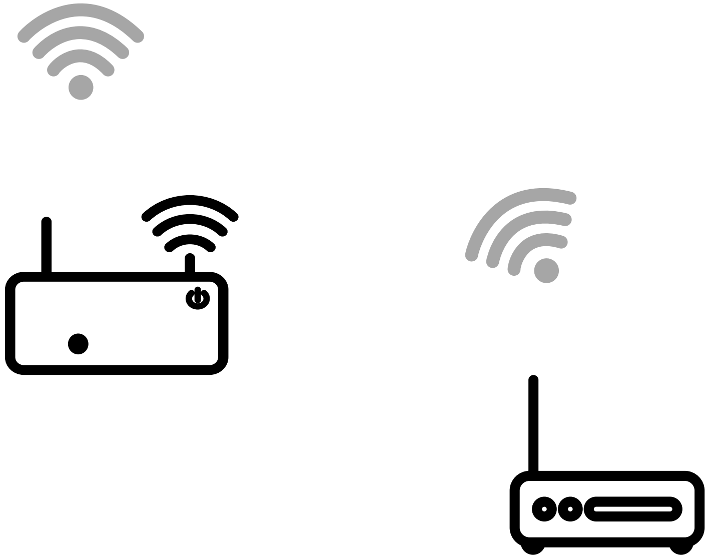
- Information leakage with broadcasting signals during sensing
  - Not only the traditional token and files in the cyber world
  - But also the physical sensed activity semantics!

Victim typing sensitive documents



Adversary compromising any AP

Privacy concerns appear while we enjoy the convenience brought by WiFi sensing!



Multiple AP sensing

Goal & Challenges

Goal:

- **Investigate the feasibility of eavesdropping on the omni-directional broadcasting signal to retrieve the activity semantics**
- **Reveal the threat of activity surveillance by pervasive WiFi infrastructures**

➢ Challenges:

- Only compromise a single device for eavesdropping
- Have no prior knowledge of the compromised device's location
- Retrieve activity semantics under unknown activity recognition models

Outline

- System and Threat Models
- Attack Design
- Evaluation
- Conclusion

System and Threat Models

➢ WiFi Activity Recognition

WiFi Router

Smart appliances

Activities

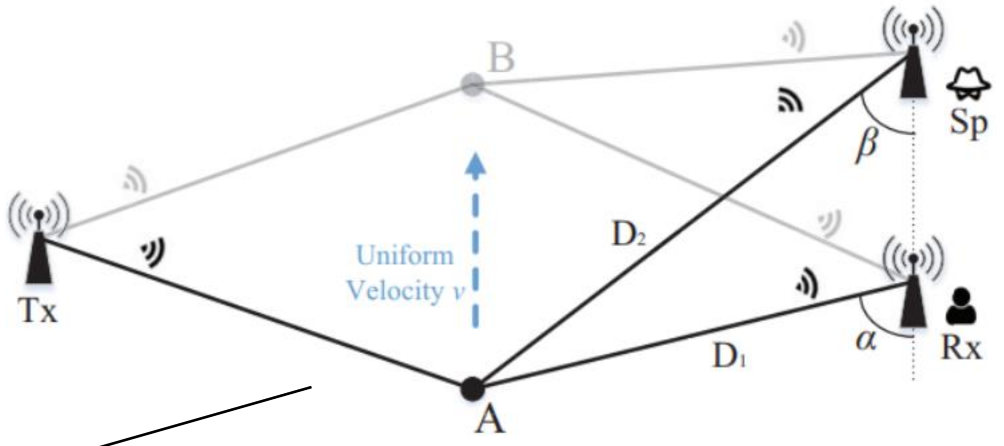
- Data collection
- Signal processing
- Feature extraction
- Classification model training
- Activity recognition

➢ Activity Surveillance Attack

- Victim’s Rx is compromised
- Adversary has no prior knowledge of model details

Feasibility Study

- Ideal case



Signal: $Y(f,t) = a(f,t)\,e^{-j2\pi\frac{D(t)}{\lambda}}$

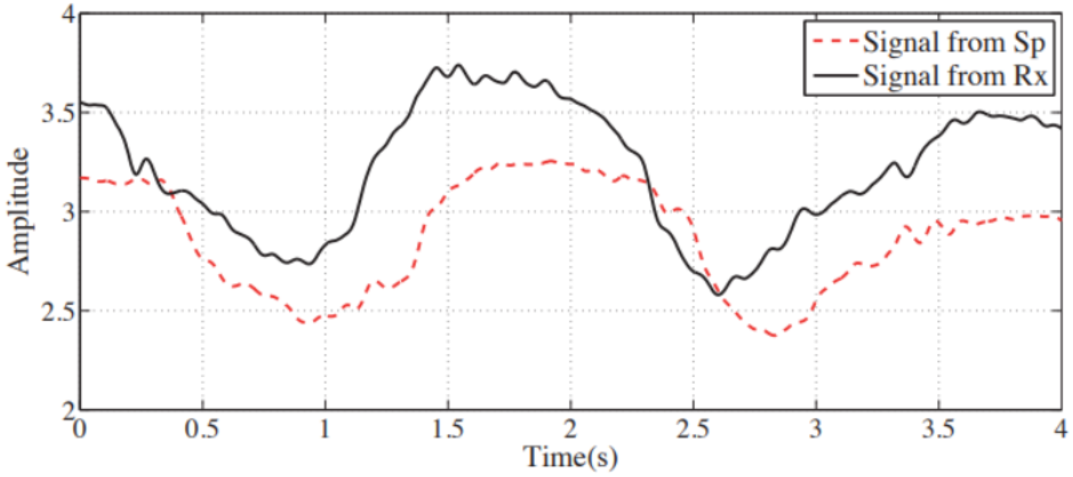
- $j2\pi\frac{D(t)}{\lambda}$

$a(f,t) = \frac{\quad}{D(t)^2}$

Hence, the CSI is: $H(f,t) = \frac{k}{D(t)^2}e^{-j2\pi\frac{D(t)}{\lambda}}$

Feasibility Study

➢ Experimental Validation



- Observation:

  Though Rx and Sp in different positions, their received signals exhibit similar trend

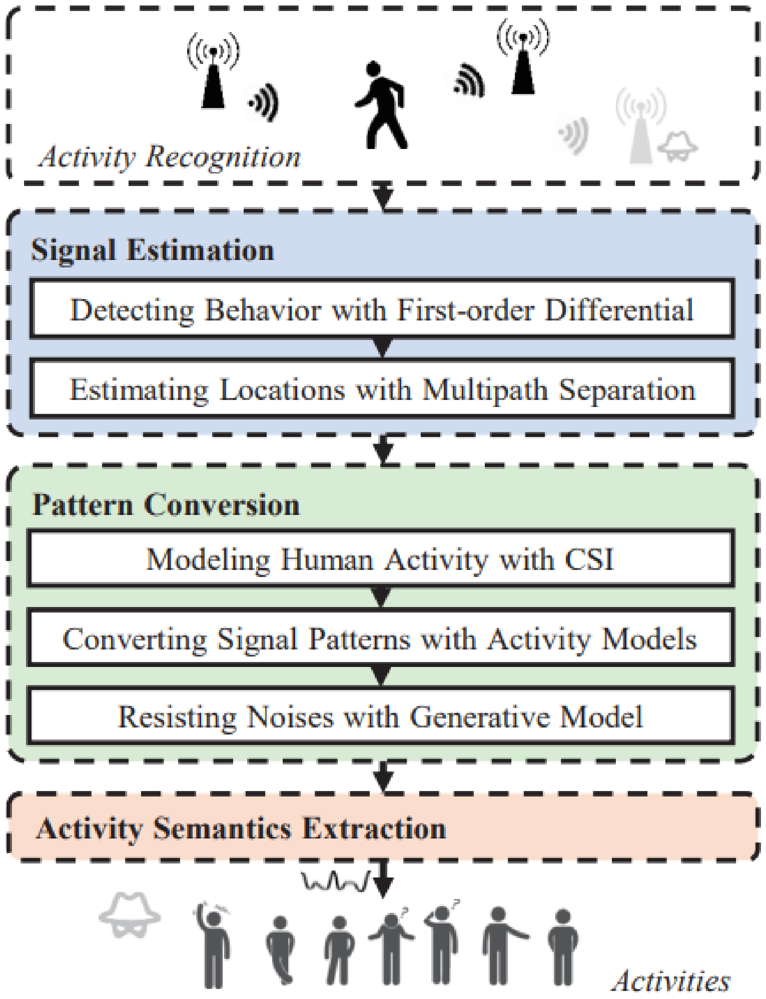
Outline

- System and Threat Models
- Attack Design
- Evaluation
- Conclusion

Overview

Basic idea: ***Recovering the WiFi signals received by legitimate receiver from that by a compromised one in any position***

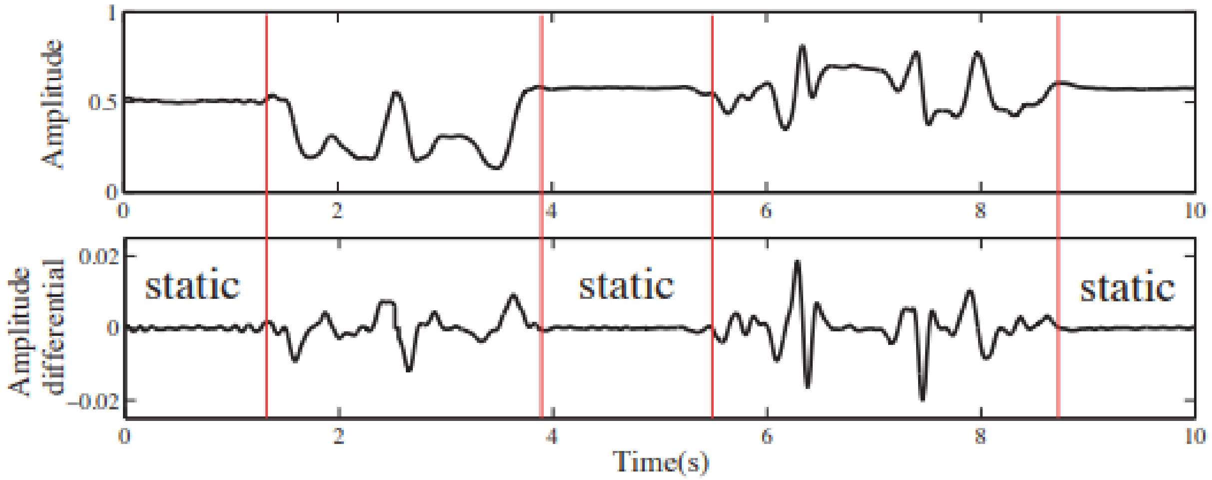
- Three Processings
  - Signal estimation
  - Pattern conversion
  - Activity semantics extraction



Signal Estimation

➢ Detecting Activity with First-Order Differential

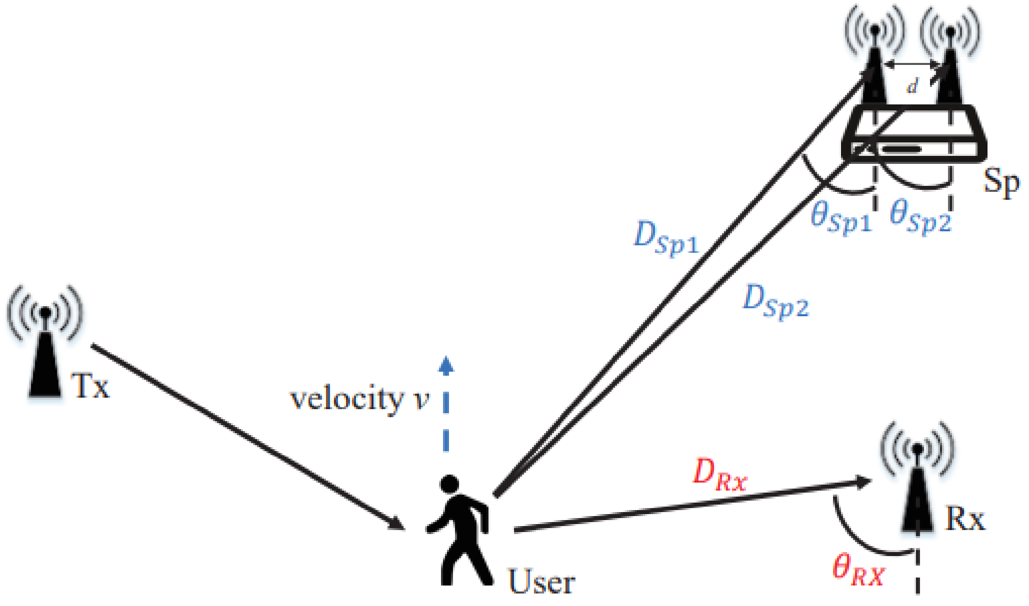
- Both user behavior and static environments reflect in the signal
  - Interfere with the conversion
- Threshold-based detection
  - A sudden variance in CSI amplitudes at the start and end of an activity
  - First-order differential of CSI amplitudes representing the variance
  - Employ a sliding window to detect whether all signal points are within a threshold



Signal Estimation

➢ Estimating Locations with Multipath Separation

- Premise of signal conversion
  - Estimated relative locations between Rx and Sp
- AoA and ToA estimation
  - MUlti SIgnal Classification (MUSIC) and its derivation[1]



[1] H. Xue, J. Yu, Y. Zhu, L. Lu, S. Qian, and M. Li, “Wizoom: Accurate multipath profiling using commodity wifi devices with limited bandwidth,” in Proceedings of IEEE SECON, 2019.

Pattern Conversion

➢ Modeling Human Activity with CSI

- Linear behavior modeling
  - Ideal case:

$$H(f,t) = \frac{k}{D(t)^2} e^{-j2\pi \frac{D(t)}{\lambda}} + N$$

  - Practical case:

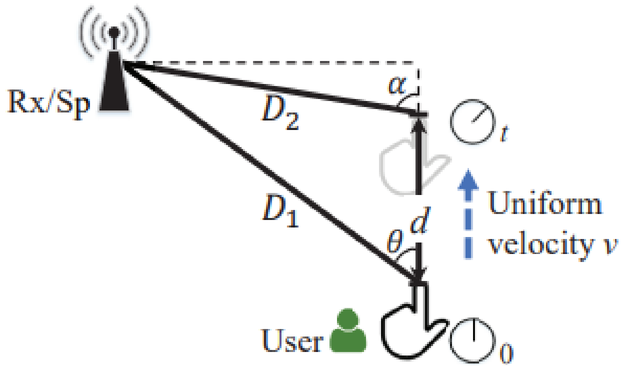
$$H_T(f,t) = \int_0^t \frac{kv \cdot e^{-j2\pi \frac{D_2}{\lambda}}}{(D_1)^2(1 + (\frac{v\Delta t}{D_1})^2 - 2\frac{v\Delta t}{D_1}\cos\theta)} d\Delta t + N.$$

  - Eliminating unseen value:

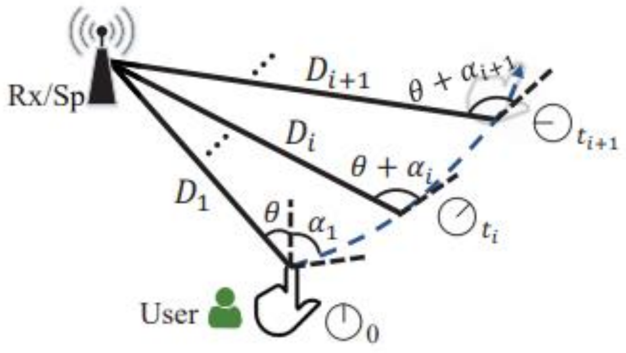
$$dH_T(f,t) = \frac{kv}{(D_1)^2(1 + (\frac{vt}{D_1})^2 - 2\frac{vt}{D_1}\cos\theta)}$$

- Non-linear behavior modeling

$$dH(f,t_{i+1}) = \frac{kv}{D_i^2(1 + (\frac{d}{D_i})^2 - 2\frac{d}{D_i}\cos(\theta + \alpha_i))}$$



(a) Linear behavior.



(b) Non-linear behavior.

Pattern Conversion

➢ Converting Signal Patterns with Activity Models

- Main task:
  - Recover $dH_{Rx}(f,t)$ based on $H_{Sp}(f,t)$
- How to?
  - Perform polynomial expansion on $dH_{Sp}(f,t)$ and obtain $dH_{Sp}(f,t) \approx \frac{k_{Sp}v}{D_{Sp}^2}(1+\frac{2v}{D_{Sp}}\cos\theta_{Sp}\cdot t)$
  - Derive the constant and first-order coefficient

$$a_1 = \frac{k_{Sp}v}{D_{Sp}^2}, \quad a_2 = \frac{k_{Sp}v}{D_{Sp}^2}\cdot\frac{2v}{D_{Sp}}\cos\theta_{Sp}$$

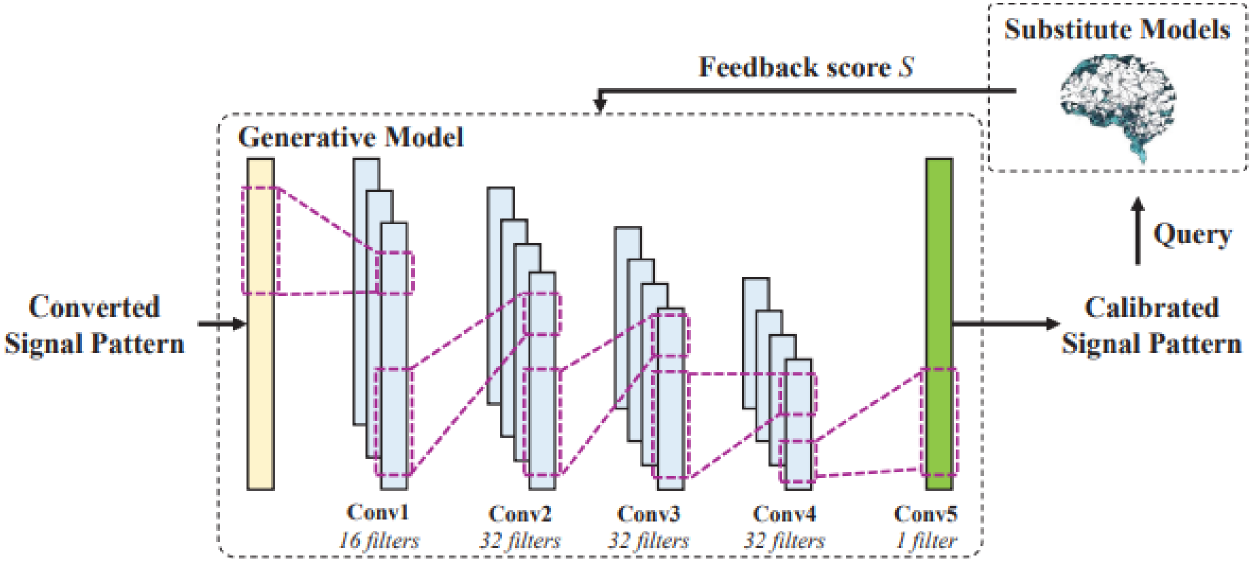
  - Using the measured $dH_{Sp}(f,t)$, derive the behavior measurement v by solving the above equation
  - Replace v into the following equation, to derive the WiFi CSI received from legitimate Rx

$$dH_{Rx}(f,t) = \frac{k_{Rx}v}{D_{Rx}^2\left(1+\left(\frac{vt}{D_{Rx}}\right)^2 - 2\frac{vt}{D_{Rx}}\cos\theta_{Rx}\right)}$$

Pattern Conversion

➢ Resisting Noises with Generative Model

- Ever-existing noises in CSI of WiFi channels
- Time-Delay Neural Network (TDNN)
  - 5-layer 1D Convolution blocks
  - One leaky ReLU as the activation function
- Multiple substitute recognition models
  - Provide recognition score as feedback for signal calibration



Activity Semantics Extraction

- Query-based semantics extraction
  - Compromised device's received signal → Legitimate one's received signal
    - Retrieve semantics of the converted signals
  - How to know specific models?
    - Sniff packets sent from legitimate device and retrieve destination IP address of cloud-based models
    - Reconstruct the packet containing the generated signal pattern as the payload and the destination IP address
    - Query the targeted cloud-based model

Outline

- System and Threat Models
- Attack Design
- Evaluation
- Conclusion

Experimental Setup

Implementation

- Tx: an AP TP-Link WDR5620
- Rx: a desktop Dell E6430 with Intel 5300 NIC
- Sp: a laptop HP Pavilion 14 with Intel 5300 NIC
- CSI of WiFi signals are extracted by CSI Tool

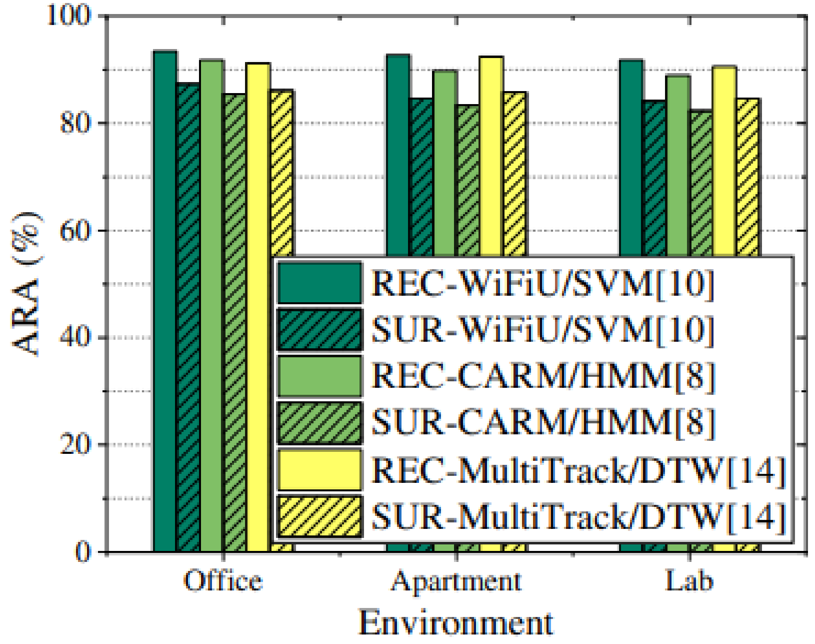
Setup

- 15 volunteers and 5 activities for human-computer interactions
  - Age: 19~43, heights: 1.59~1.80m, weights: 48~74kg
  - Push, pull, bend arm, zigzag, slide
- Three environments
  - Office (3.2m*2.8m), apartment (4.1m*3m), lab (5.8m*4.2m)

Performance of Activity Modeling-based Conversion

➢ Activity Recognition Accuracy (ARA)

- Sp's ARAs all above 80%
- Sp's ARA are all smaller than Rx's ARA within 10%
- ARAs of attacking different models exhibit minute difference
- ARAs under different environments also show subtle variance



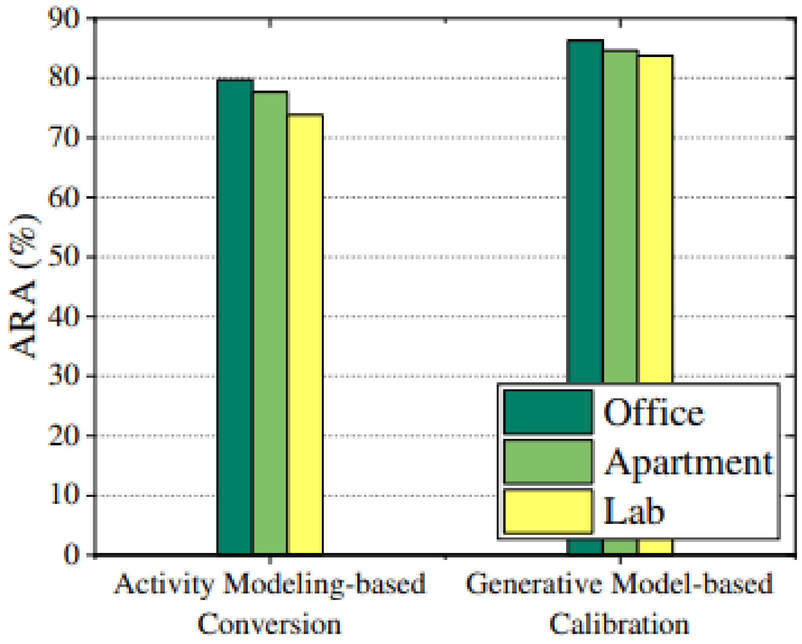
Performance of Generative Model-based Calibration

➢ Activity Recognition Accuracy (ARA)

- Average ARA of generative model-based calibration is 7.9% larger than activity modeling-based conversion
- Standard deviation of ARA:

  3.0% (activity modeling-based conversion)

  → 1.3% (generative model-based calibration)



Impact of Distances and Angles

➢ Activity Recognition Accuracy (ARA)

- ARA decreases as the increase of distance
- ARA could be larger than 80% within the distance of 1.8m
- ARAs decrease below 55% on average under the angle of $-60\circ$ and $-30\circ$
- ARA could be above 75% for other angles

Table I
ARA OF *ActListener* UNDER DIFFERENT DISTANCES ON DIFFERENT MODELS.

	WiFiU/SVM[10]	CARM/HMM[8]	MultiTrack/ DTW[14]
REC	92.8%	92.6%	91.6%
SUR-1.5m	85.3%	83.7%	85.5%
SUR-1.6m	84.4%	82.8%	84.3%
SUR-1.8m	81.8%	80.2%	80.8%
SUR-2m	74.3%	73.1%	72%

Table II
ARA OF *ActListener* UNDER DIFFERENT ANGLES ON DIFFERENT MODELS.

	WiFiU/SVM[10]	CARM/HMM[8]	MultiTrack/ DTW[14]
REC	92.8%	92.6%	91.6%
SUR-60°	86.8%	84%	84.8%
SUR-30°	86.4%	83.9%	85.3%
SUR-0°	85.3%	83.7%	85.5%
SUR-−30°	54.8%	49.5%	53.4%
SUR-−60°	55.8%	49.5%	53.4%

Outline

- System and Threat Models
- Attack Design
- Evaluation
- Conclusion

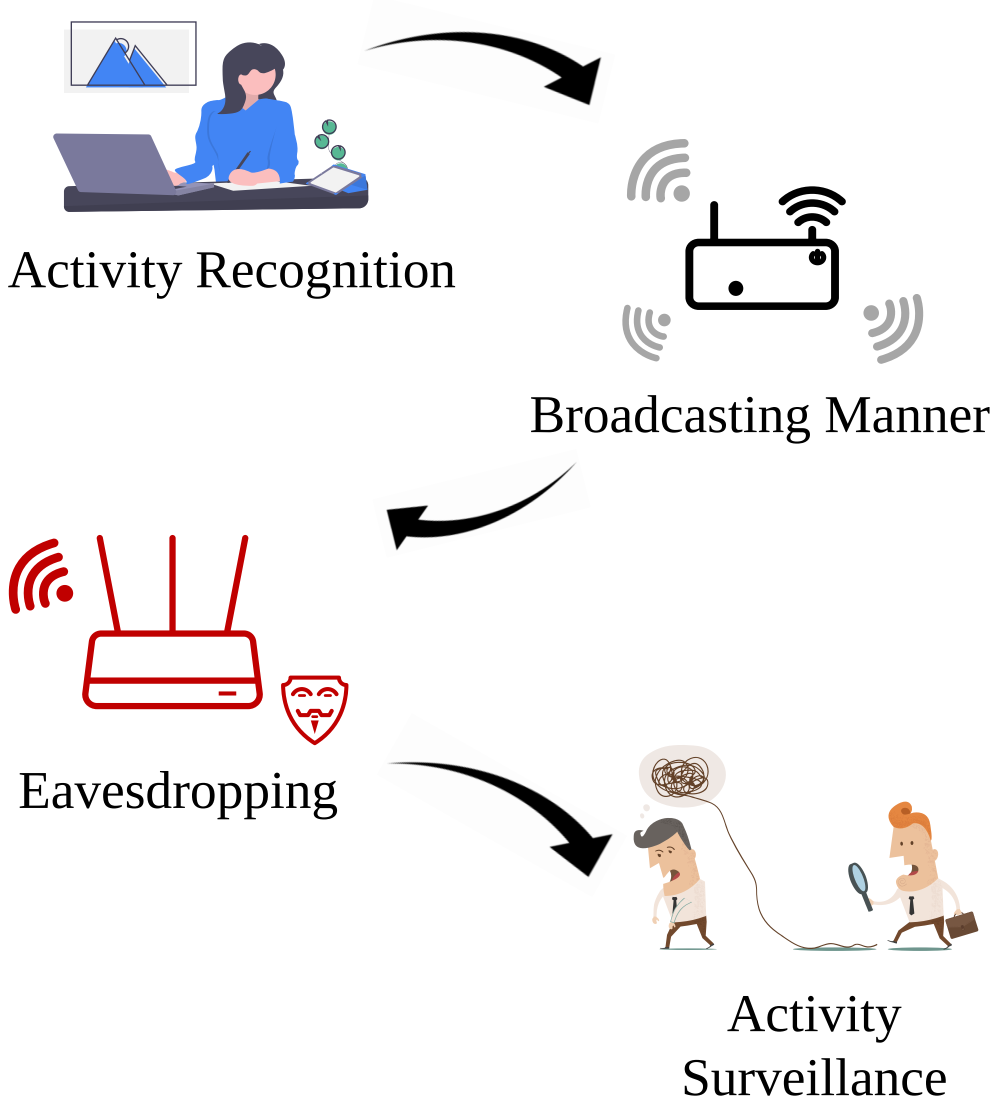
Conclusion

Contribution

- Demonstrate an eavesdropping attack on WiFi-based activity recognition
- Design an activity modeling-based signal conversion method
- Develop a generative model-based signal calibration approach

Evaluation

- Achieve 88.4% α-similarity with legitimate signals
- Achieve over 90% ARA in activity recognition



Thank you!

Contact: Li Lu
li.lu@zju.edu.cn