The Eighteenth International Conference on Wireless and Mobile Communications ICWMC 2022

Spear and Shield: gesture recognition and obfuscates sensing with the communication signal

Presenter: Dr. Ouyang Zhang
Google LLC
formerly Ohio State University, U.S.
Communications Systems
& Networking Research Group (CoSyNe)

email: zhang.4746@osu.edu

Presenter Bio

Ouyang Zhang currently works at Google. During his studies he interned with IBM and Facebook. Ouyang Zhang completed his PhD in Computer Science at OSU working with Prof. Kannan Srinivasan where his research interests include wireless sensing, mobile computing, networking, and applied machine learning. His work on protecting user privacy against wireless sensing (PhyCloak) received the Best Student Paper Award in NSDI. You can find his publications here (https://scholar.google.com/citations?hl=en&user=wdFXYjoAAAAJ).

His dissertation focused on two major challenges in wireless sensing: fine-grain gesture recognition and obfuscate sensing with communication signal. One challenge is to break the boundary of sensitivity in the status quo with wireless signal. The other is to disable all possibilities of leaking user privacy with signals in the air. Like spear and shield: sensing and protection.

Dr. Zhang also serves as a reviewer for Asia-Pacific Conference on Communications (APCC), IEEE GLOBECOM, FTC, etc. He completed his undergraduate in Electrical Engineering at University of Science and Technology of China in 2014 with a major in communication and information science. His dissertation was about resource allocation of multi-cell OFDMA.

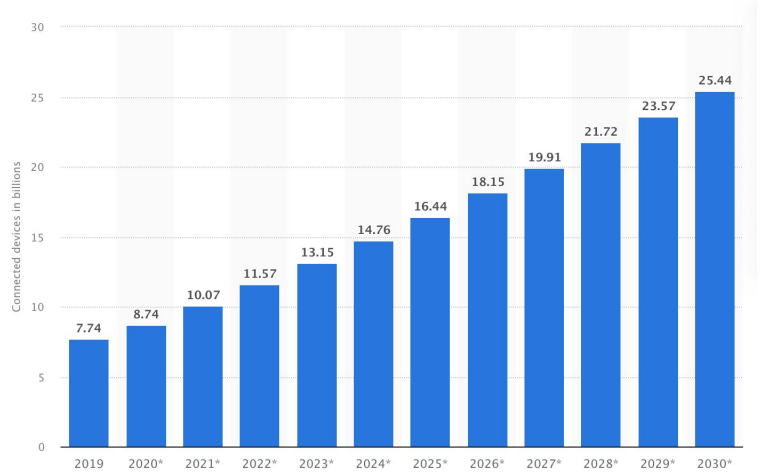
Outline

- Wireless sensing with communication signal (Opportunity, Principle & Challenges)
- Reliability and robustness of wireless sensing
- Protect user privacy against malicious sensing
- Conclusions

Wireless sensing with communication signal

Opportunity

- Up to now, 11.57 billion connected IoT devices worldwide
- By 2030, the number would be boosted to 25.44 billion (Statista Report)
- Standard-supported availability of the channel information
- In 802.11n protocol, a transmitter can trigger CSI estimation at
- a receiver by setting an sounding flag in the transmitted packet
- Source: Ieee 802.11n-2012 standard. 2012, 2016, Link: http://standards.ieee.org/findstds/standard/802.11n-2012.html.

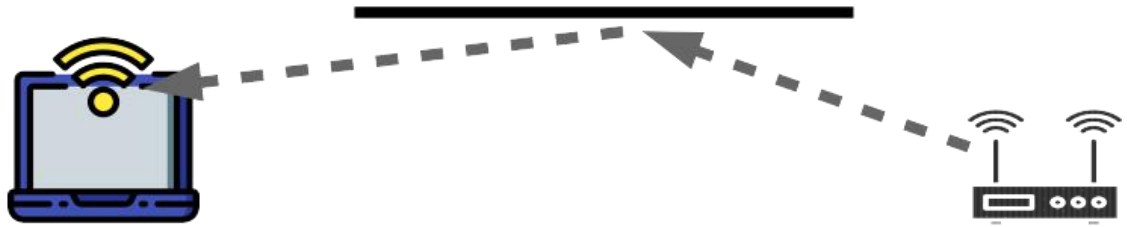


Wireless sensing with communication signal

Principle

- Physical world will change the channel that the signal go through from the transmitter to the receiver, which is the fundation of wireless sensing.
- Channel coefficients of the signal propagation process captures the characteristics of the physical world.

$$r(t,f)=ae^{-j2\pi f\delta t}s(t-\delta t,f)$$

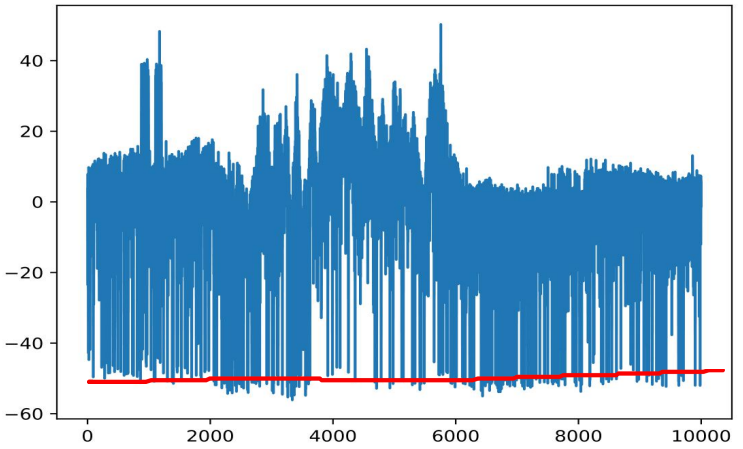


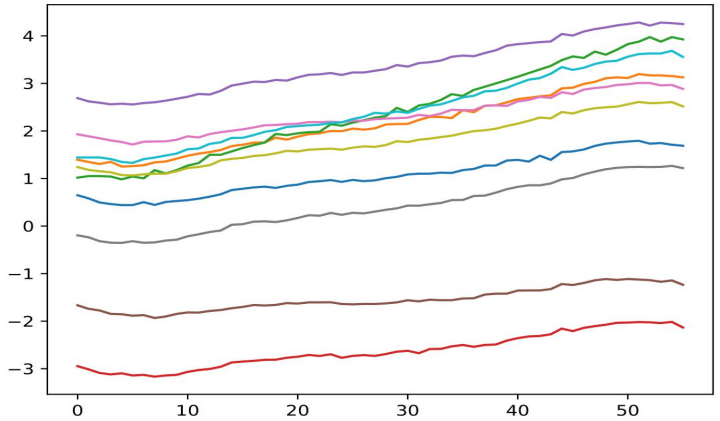
- There are three dimensions in signal r(t, f), i.e., attenuation, phase and frequency. They are three degrees of information freedom.

Wireless sensing with communication signal

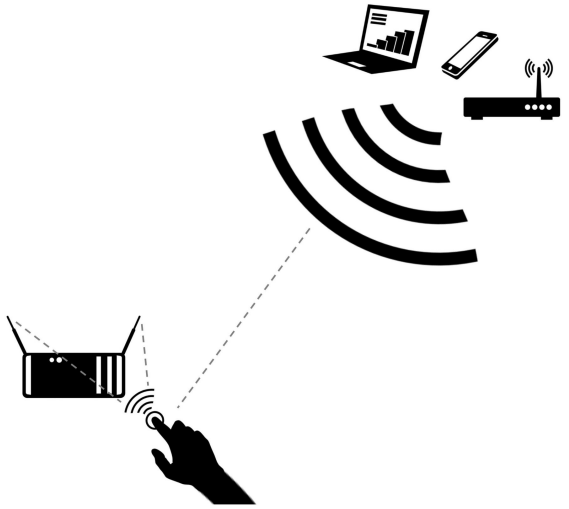
Challenges

- Noisy channel
  - Environmental variation
  - Device imperfection
  - Device internal state transition
- Phase randomness
  - Unsynchronized clock – frequency offset
- Consistency against environment dynamics
- Heterogeneous link conditions
- User privacy protection





Reliability and robustness of wireless sensing



Finger gesture recognition

- Near-field
- Mobile handheld device
- Finger gestures
- User motility

Human activity recognition

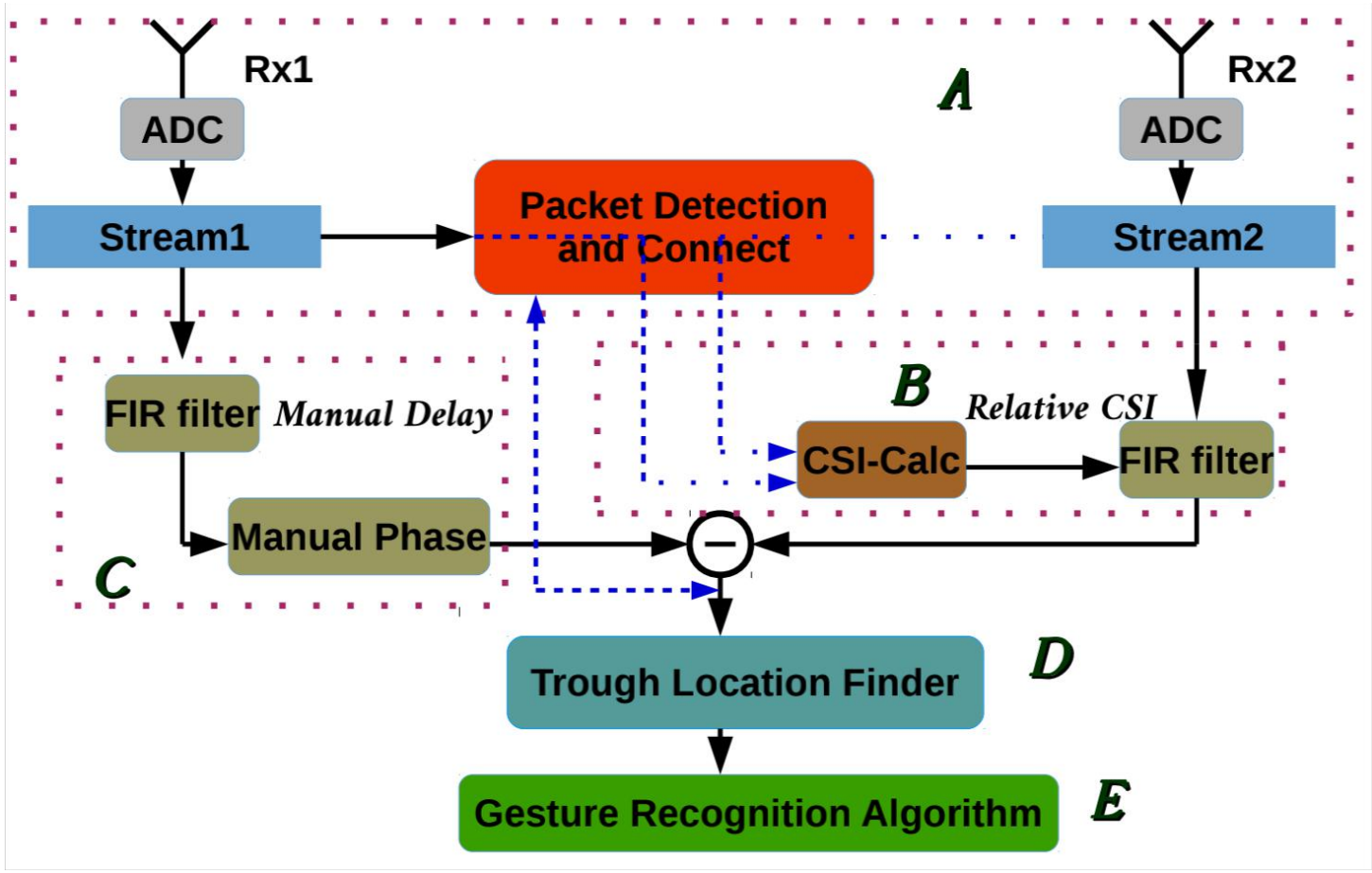
- Far-field
- Home-installed WiFi infrastructure/device
- Human activity
- Passive detection

Reliability and robustness of wireless sensing

Finger gesture recognition

System architecture

- Packet detect/connect
- Channel estimator/signal equilization
- Manual delay/phase injector
- Trough location finder
- Gesture recognition algorithm

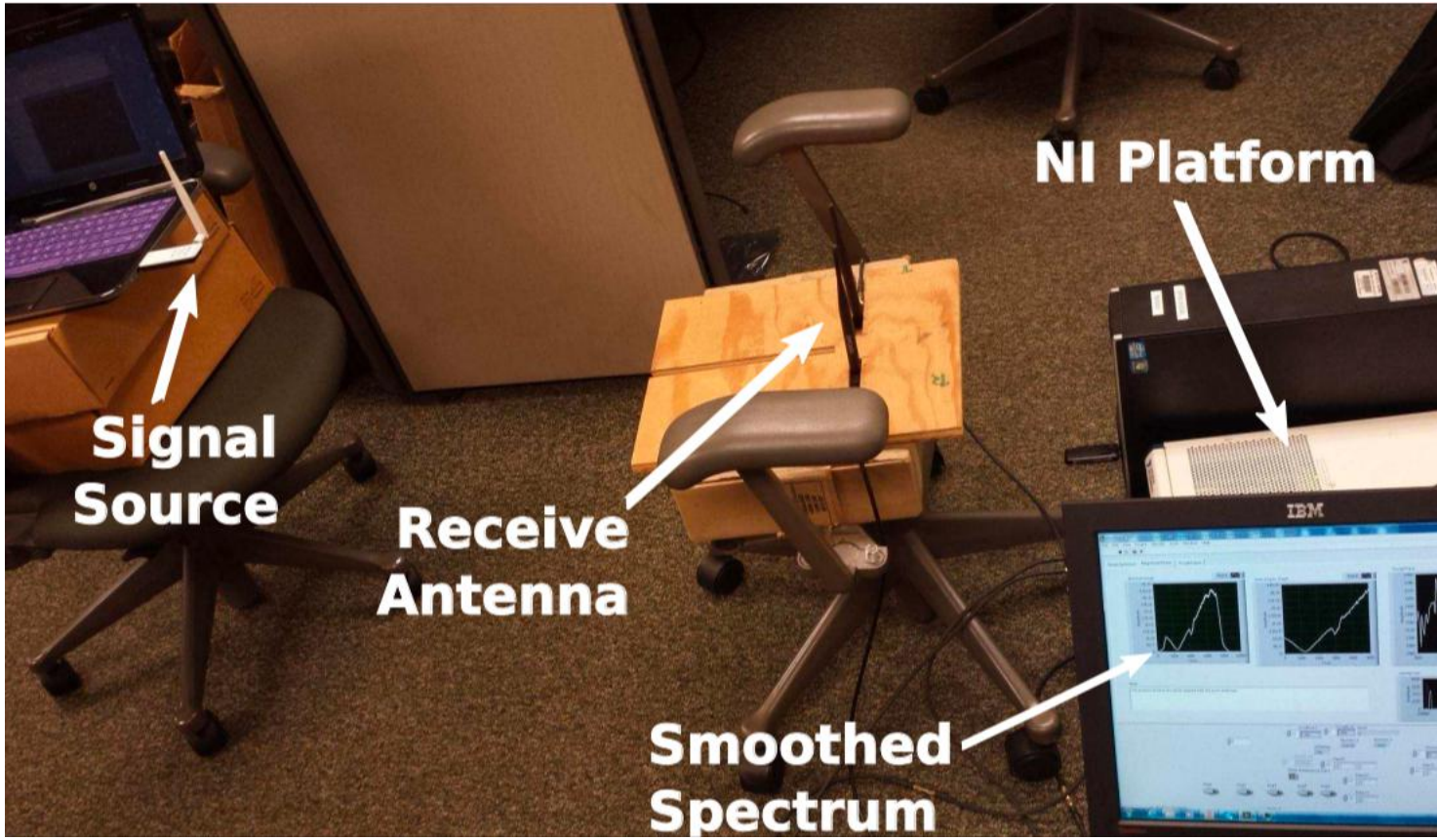


Reliability and robustness of wireless sensing

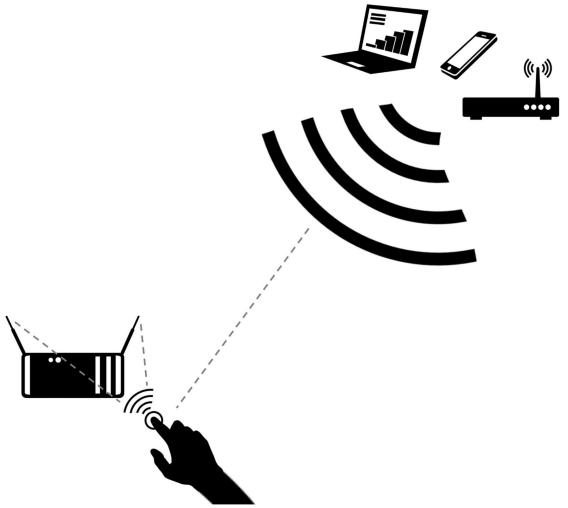
Finger gesture recognition

Test bed

- NI PXIe-1082 SDR platform
- NI-5791 FlexRIO adapters with VERT2450 3dBi gain antenna
- Virtex-5 based FPGA, DSP decimation after ADC with resolution of 14 bits generates 20MHz baseband samples
- Direct Memory Access is built to transfer baseband samples from Rx1 to Rx2
- Central controller is built on RTOS based PXIe-8133
- TP-LINK TL-WN722N with output power peak at 17.8 dBm [5], and NET_x0002_GEAR WNDA3100 adapter as WiFi receiver



Reliability and robustness of wireless sensing



Finger gesture recognition

Signal cancellation

- Channel Estimation

$$t(t) - T(\omega), s_1(t) - S_1(\omega), s_2(t) - S_2(\omega) \quad (1)$$

$$H_1(\omega) = \frac{S_1(\omega)}{T(\omega)}, H_2(\omega) = \frac{S_2(\omega)}{T(\omega)} \quad (2)$$

$$Relative\ Channel\ Coefficient - \frac{H_1(\omega)}{H_2(\omega)} \quad (3)$$

- Equalization

$$\overline{S_1(\omega)} = S_2(\omega) * \frac{H_1(\omega)}{H_2(\omega)} \quad (1)$$

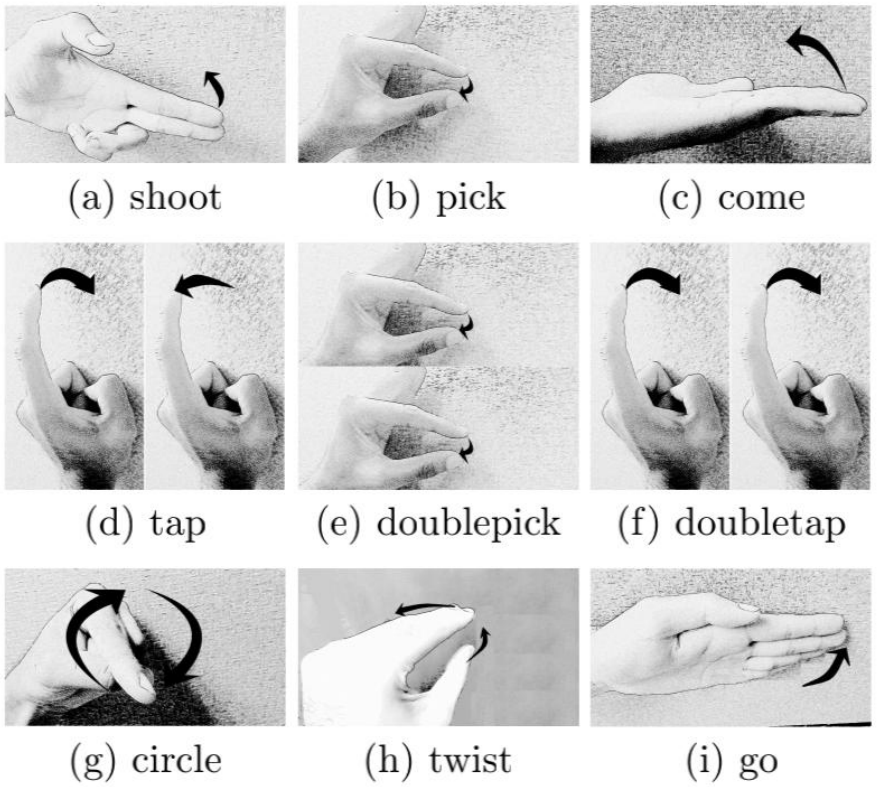
$$Time\ -\ domain : \overline{s_1(t)} = s_2(t) \bigotimes h_r(t) \quad (2)$$

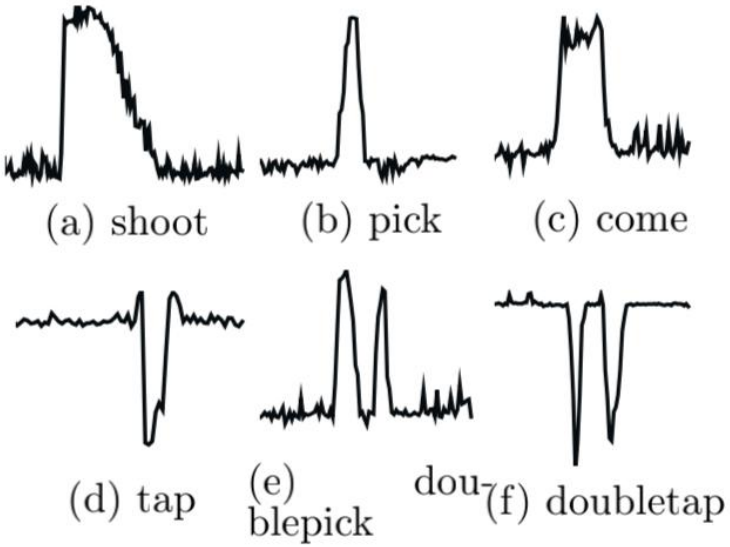
- Subtraction

$$Cancellation\ residule : r_1(t) = s_1(t) - \overline{s_1(t)} \quad (3)$$

Reliability and robustness of wireless sensing

Finger gesture recognition

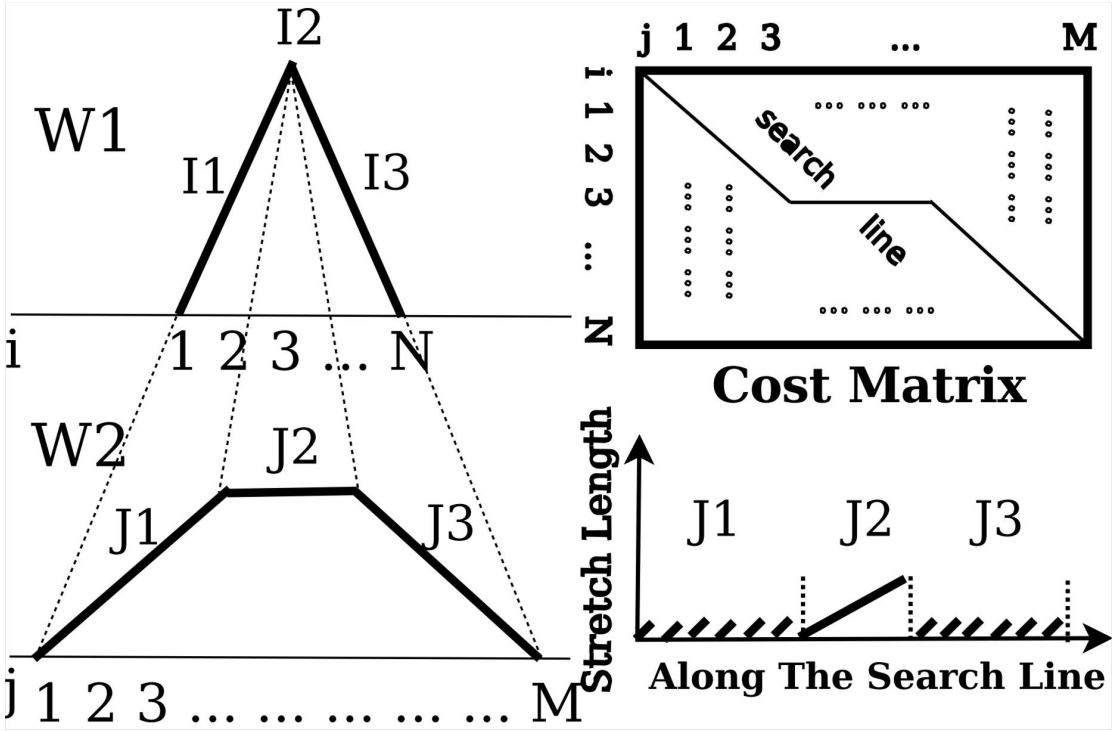


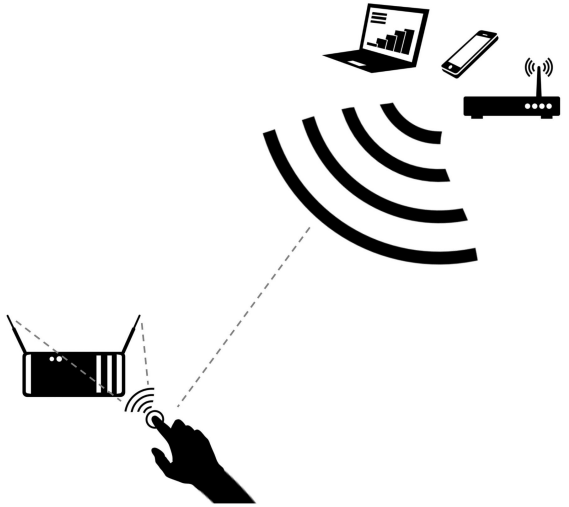


Reliability and robustness of wireless sensing

Finger gesture recognition

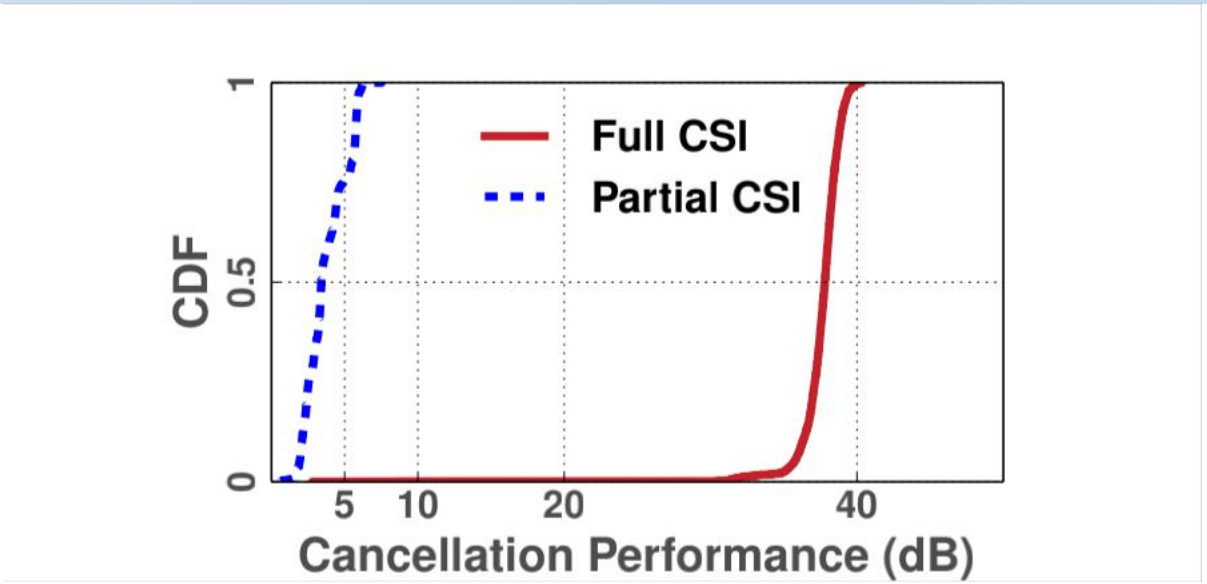
Stretch Limited DTW schematic diagram. The left plots show two waveform figures and how DTW map each part of them. The right plots show the walk through cost matrix and stretch length along the search
line.

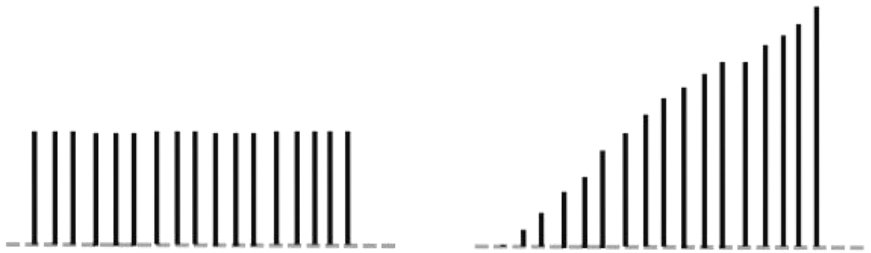


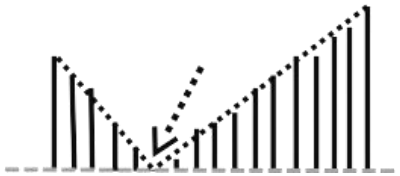


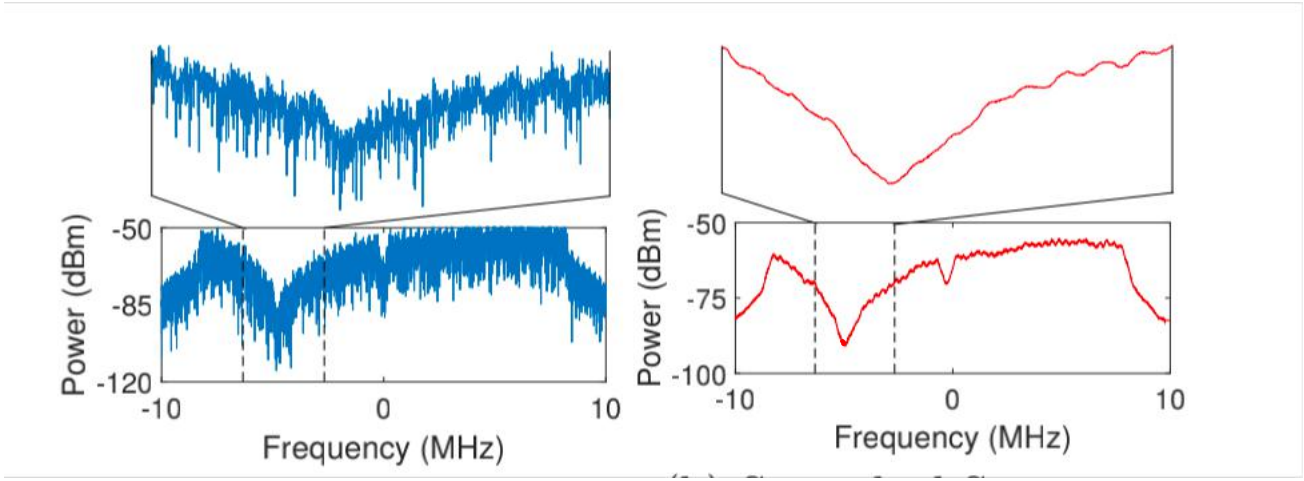
Reliability and robustness of wireless sensing

- Signal cancellation performance
- Partial CSI estimation vs full CSI estimation
- Phase injection
- Irritable signal across signal spectrum vs smoothed signal



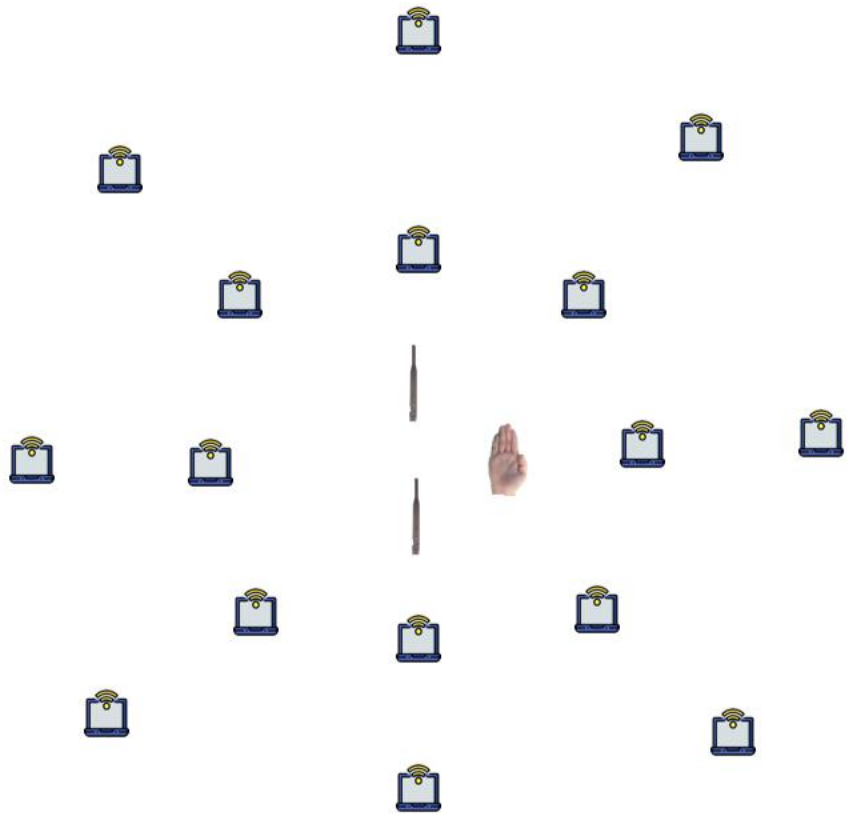


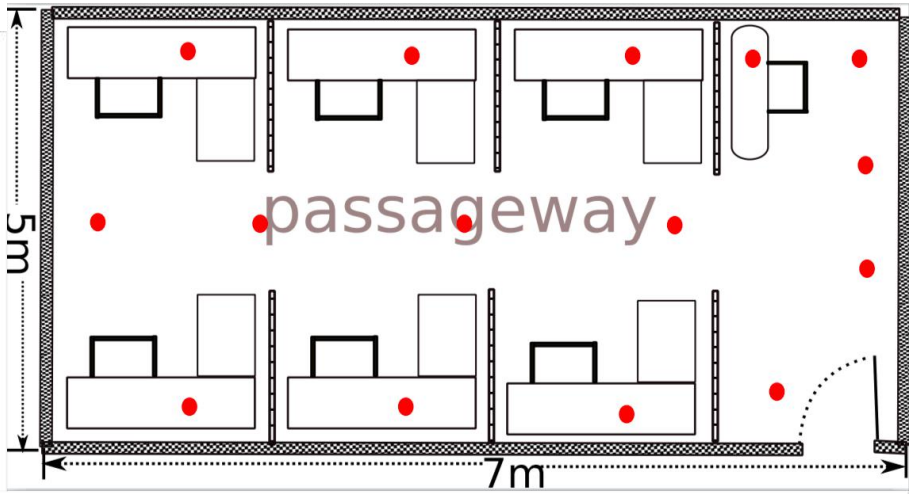


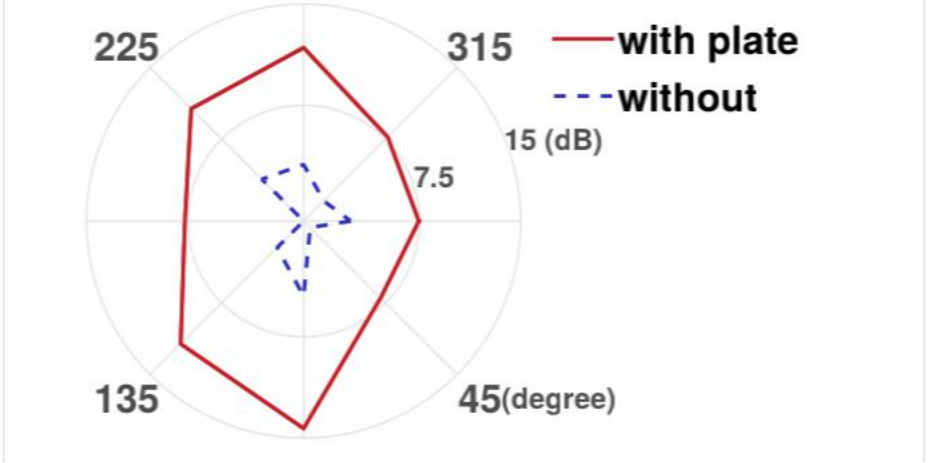


Reliability and robustness of wireless sensing

Consistency study - reliability and robustness





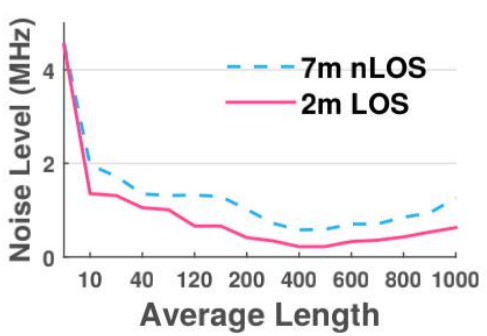


Reliability and robustness of wireless sensing

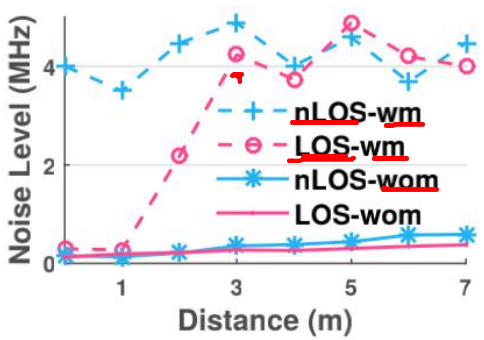
Consistency study - reliability and robustness

Position	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16
0degree	+	⋆,-	+,⋆,-	+,⋆,-	⋆,-	+,⋆,-	+,⋆	+,⋆,-	+,⋆	+,-	+,⋆,-	+,⋆	+,⋆	⋆,-	+,-	+,⋆,-
45degree	+	+,⋆,-	+,⋆	+,⋆,-	+,⋆	+,⋆,-	⋆,-	⋆,-	+,⋆,-	⋆,-	+,-	+,⋆,-	+,⋆,-	+,⋆	+	⋆,-
90degree	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

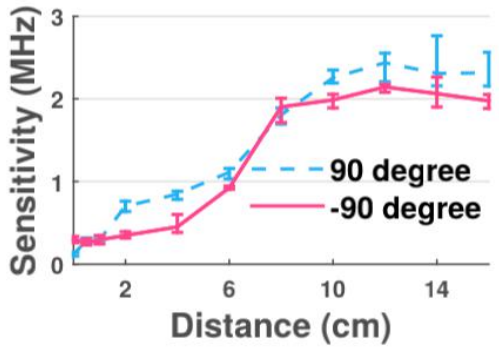
Table 1: Consistency study of gesture waveforms with various signal source locations.



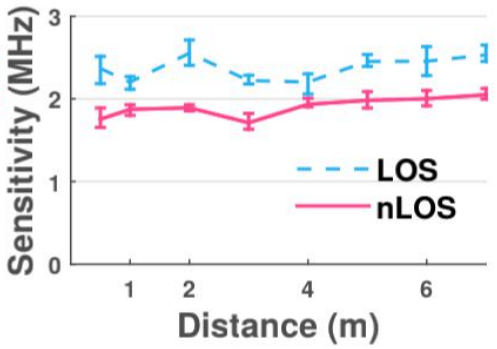
(a) Noise vs Length



(b) Noise vs Distance



(a) Antenna Distance



(b) Source Distance

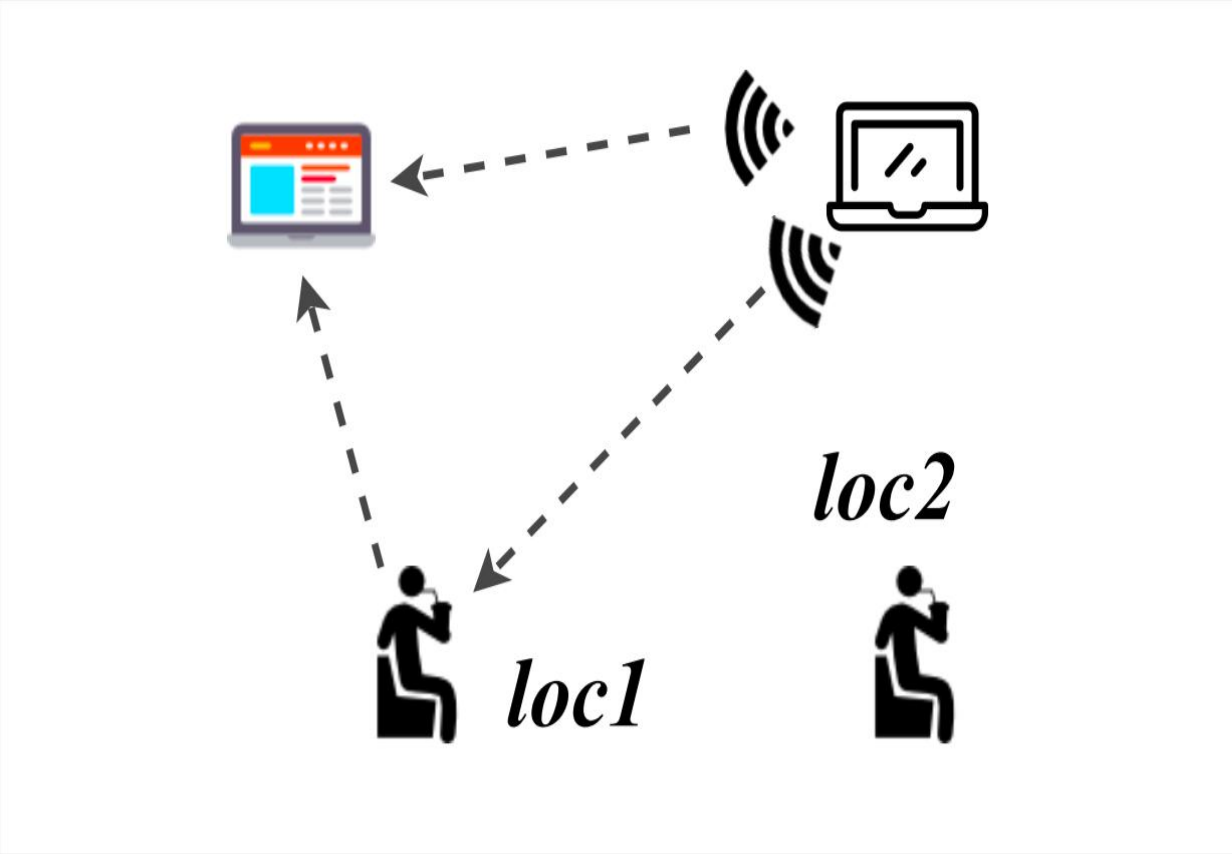
Reliability and robustness of wireless sensing

Whole-home Human Activities Recognition

- Large-scale movement (e.g., apartment ~ 10m x 10m.)
- Human object may be away from the antennas.
- The antenna setting is consistent (e.g., WiFi router, desktop, etc.)

Commodity devices.

- Dynamics in the environment settings (movement of furnitures.)



Reliability and robustness of wireless sensing

Status of the quo

Using statistics of amplitudes on each subcarrier (E-eyes MobiCom'14)

It collects CSI information as the data. CSI is the channel state information which are the channel properties on each subcarrier in the WiFi band. As there are 56 subcarriers in 20MHz WiFi band, the CSI vector has 56 dimensions.

Each activity may generate a specific amplitude distribution on WiFi subcarriers. This approach includes two steps:

In the first step, the system collects samples for each activity. Calculate the distribution of amplitude on each subcarrier and store to database as the fingerprints.

As the second step, in the testing stage, for each new collected activity data, the distribution of amplitude as histogram is compared with the database fingerprints and the activity is classified with the minimum distance.

Reliability and robustness of wireless sensing

Status of the quo

Using variation on CSI amplitudes (CARM Mobicom'15, WiSee Mobicom'13, WiFinger MobiHoc '16)

Doppler shift (WiSee) $\delta f = f * \frac{v}{c}$

CSI variation pattern (WiFinger) – Using MD-DTW to match the pattern

Speed model (CARM) – Extract speed pattern across time from CSI traces

Insights

- Human activities are mostly loosely defined.
- There is no strict order of motion, speeds, directions.
- Previous approaches: Fit into well-defined short-time gestures. WiSee, WiFinger, CARM
- The motion needs strict sequence and speed for each user.

Reliability and robustness of wireless sensing

Insights

Both profiles are critical for recognizing human activities

- The statistics of CSI represents the position, orientation and posture of the person during a period of timean activities
- The variation of CSI represents how the target moves during a period of time.

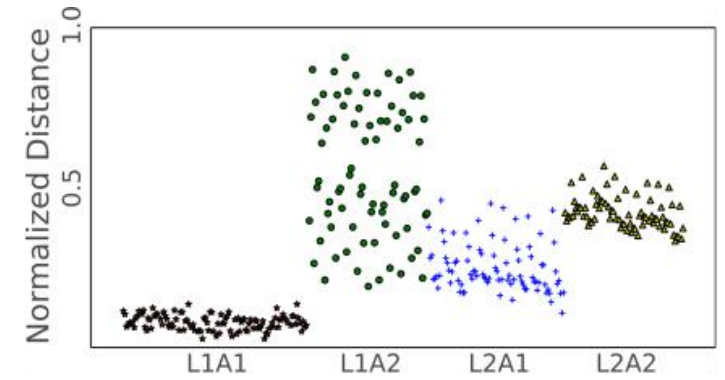
These profiles are complementary to each other

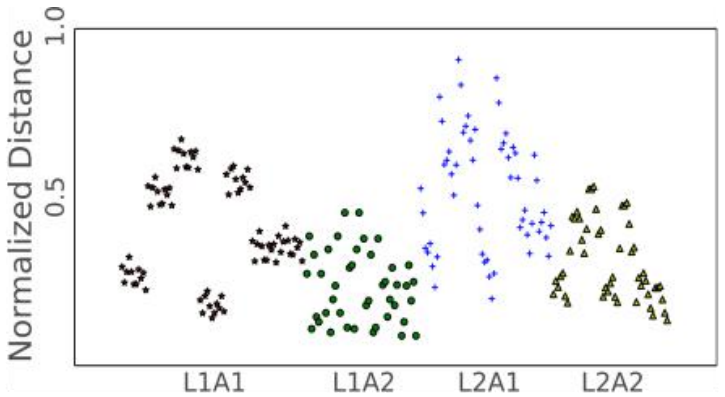
- For two activities, they could have similar CSI statistics but has different variations during the activities.
- On the other hand, in some cases these two activities have similar CSI variations but different CSI statistics.

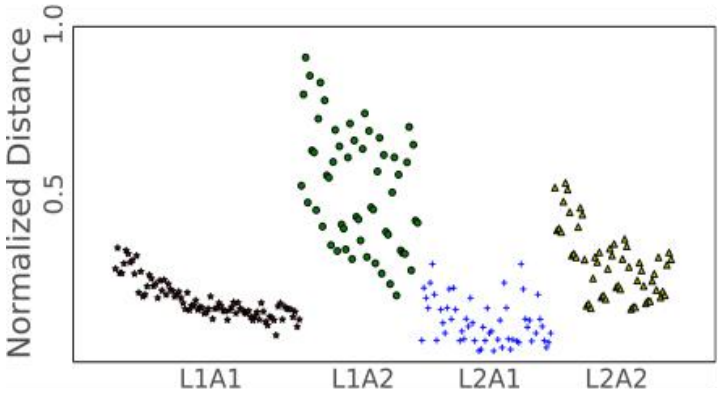
Reliability and robustness of wireless sensing

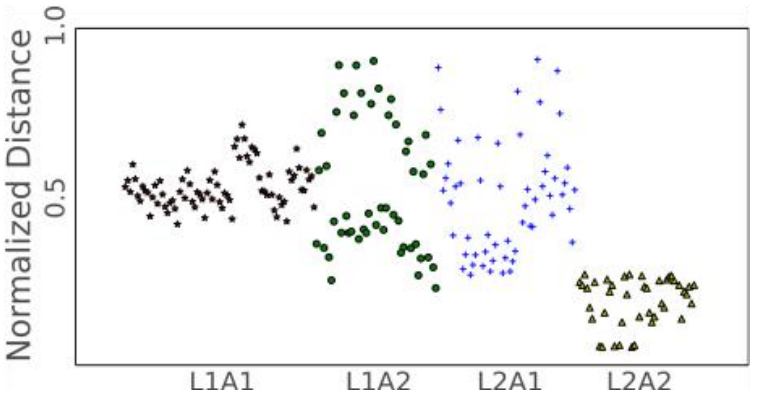
Preliminary study

Activities performed with the same position and orientation have similar distributions of CSI values.





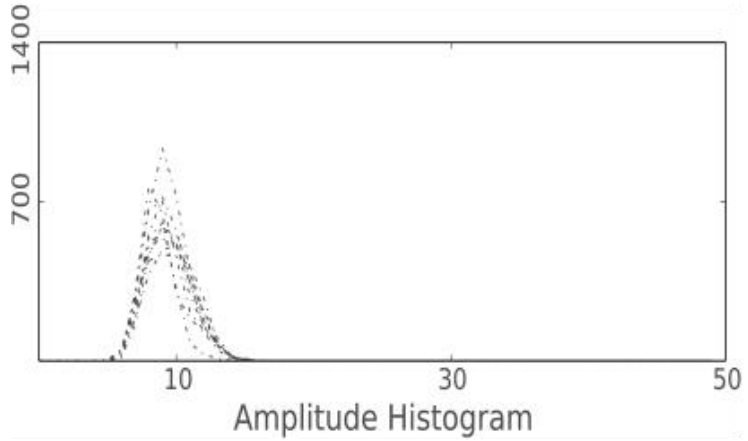


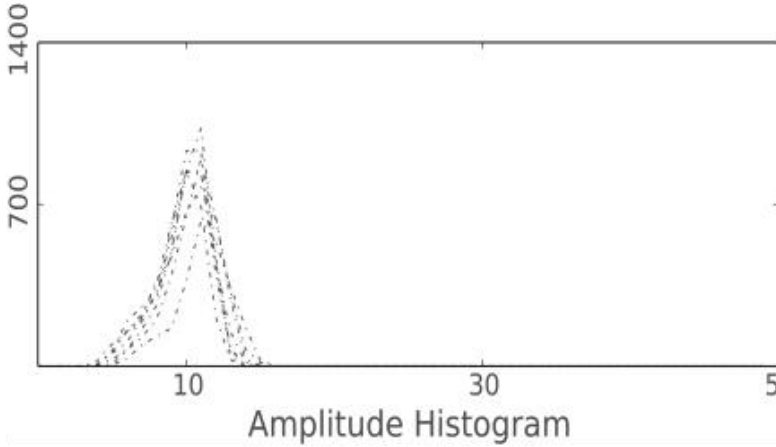


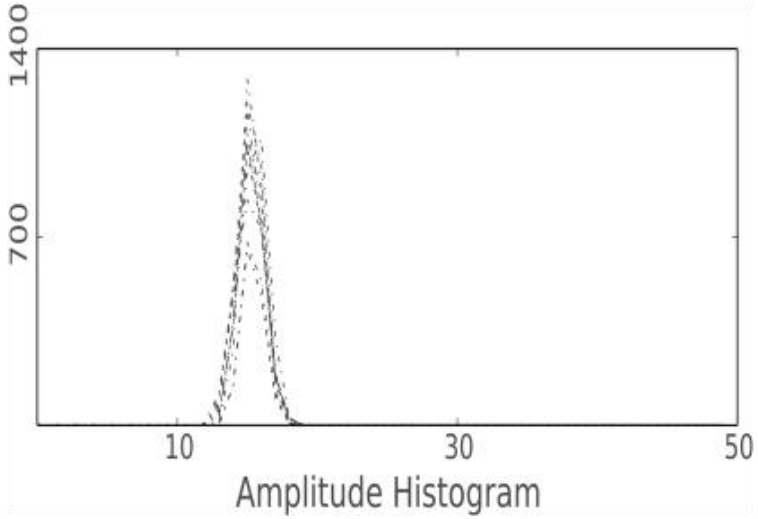
Reliability and robustness of wireless sensing

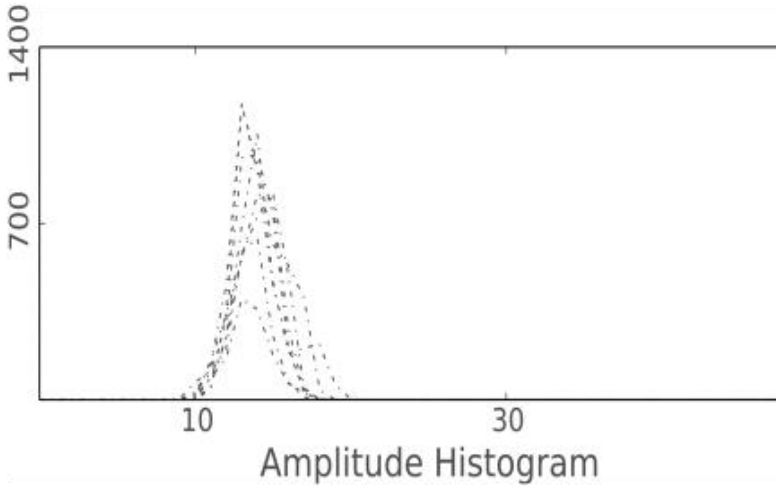
Preliminary study

Activities performed at different places may also have similar motions, i.e., moving speed, of body parts.









Reliability and robustness of wireless sensing

Dual-profile recognition framework

System architecture

- ❑ Multipath-profile analysis.
- ❑ Motion-profile analysis.
- ❑ Profile integration mechanism.
- ❑ Activity detection algorithm.

Reliability and robustness of wireless sensing

Multipath-profile analysis. This component constructs a multipath profile from CSI data. Then, it analyzes the profile for recognition using a dual-statistics model.

CSI to Robust Multipath Profile
Localization - feature is one CSI vector
Activity - feature is time series of CSI vectors

Existing work - module trained on time series of CSI on one subcarriers

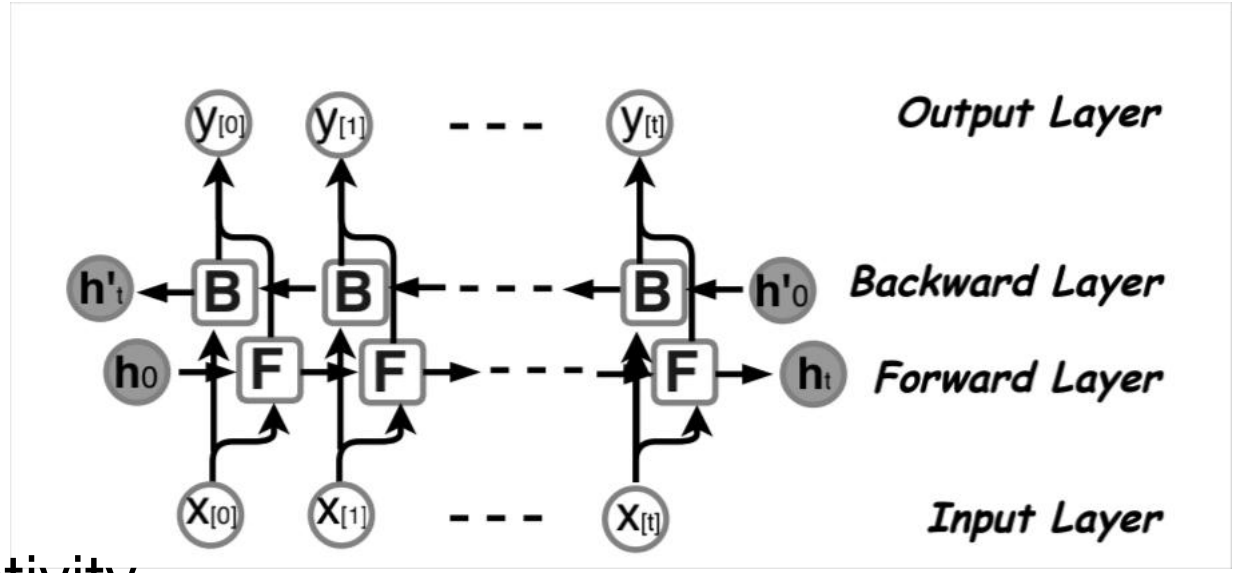
The challenge - require a model to analyze dual statistics, i.e., across multiple subcarriers and sampling time points.

Reliability and robustness of wireless sensing

Multipath-profile analysis.

$$F = [f_1, f_2, ..., f_t, ..., f_T]$$

$$f_t = [|h_1|, |h_2|, ..., |h_{56}|]^T$$



Apart from the variation across different activity instances (i.e., each time the participant does the activity slightly differently), the model needs to extract the statistics of CSI values in the collection of one instance.

~~Earth mover's distance (EMD) algorithm.~~

Reliability and robustness of wireless sensing

Motion-profile analysis.
This component constructs a motion profile from CSI data.
Then, it applies statistical analysis to the profile for loosely-defined human activity.

CSI to Motion Profile

Relation between CSI values and object's speed

$$h(f,t) = e^{-j2\pi\Delta f t}(h_s(f,t) + \sum_{k=1}^{K} a_k(f,t)e^{-j2\pi l_k(t)/\lambda})$$

$$|h(f,t)|^2 = \sum_{k=1}^{K} 2|h_s(f)a_k(f,t)|cos(\frac{2\pi v_k t}{\lambda} + \frac{2\pi l_k(0)}{\lambda} + \phi_{sk})$$

$$+ \sum_{\substack{k,l=1 \\ k\neq l}}^{K} 2|a_k(f,t)a_l(f,t)|cos(\frac{2\pi(v_k - v_l)t}{\lambda} + \frac{2\pi(l_k(0) - l_l(0))}{\lambda}$$

$$+ \phi_{kl}) + \sum_{k=1}^{K} |a_k(f,t)|^2 + |h_s(f)|^2$$

Reliability and robustness of wireless sensing

Motion-profile analysis.

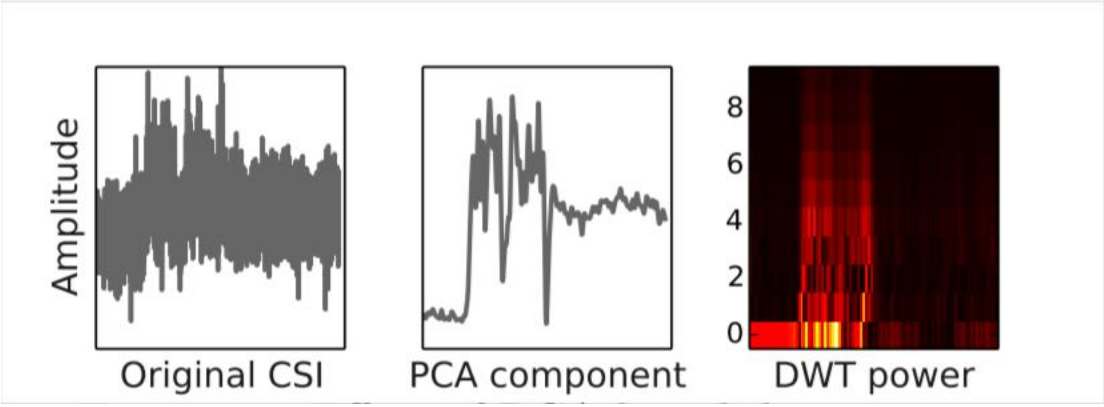
Challenge
noisy CSI data from
commodity WiFi cards

Motion Profile Construction.
Discrete wavelet transform (DWT) has advantages in obtaining high-frequency value with high time resolution and low-frequency value with high frequency resolution.

Transmission Rate and PCA-based Denoising

150 Hz is the upper bound of variation frequency caused by human speed less than 8 m/s

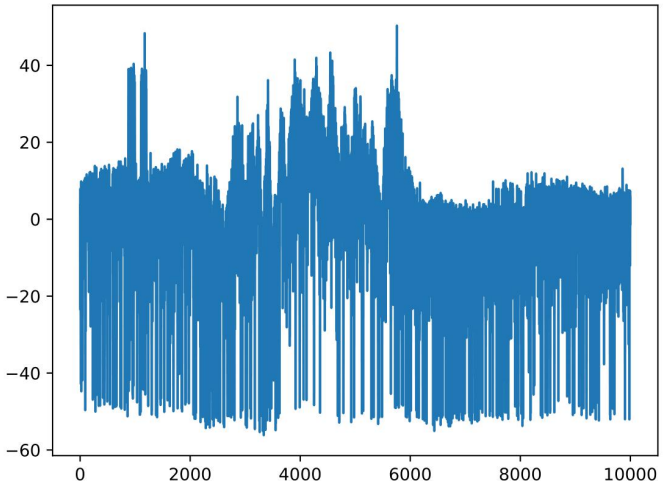
PCA-based de-noising technique

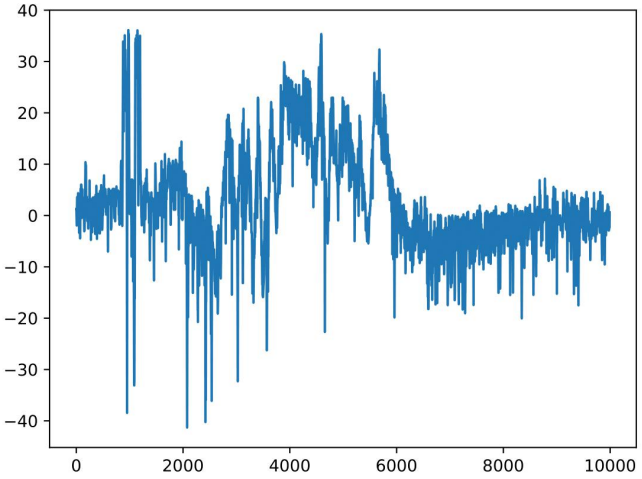


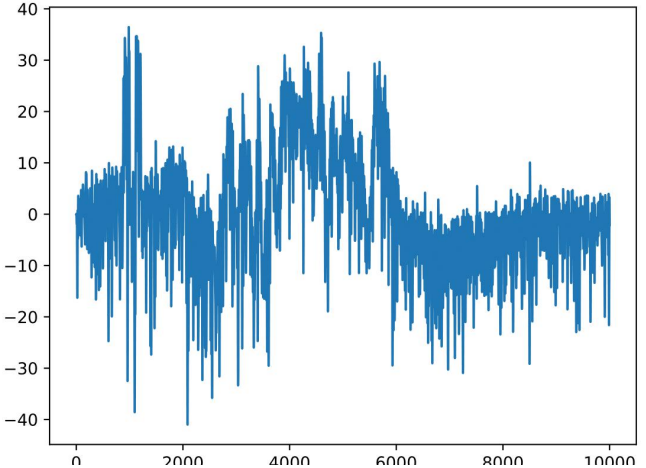
Reliability and robustness of wireless sensing

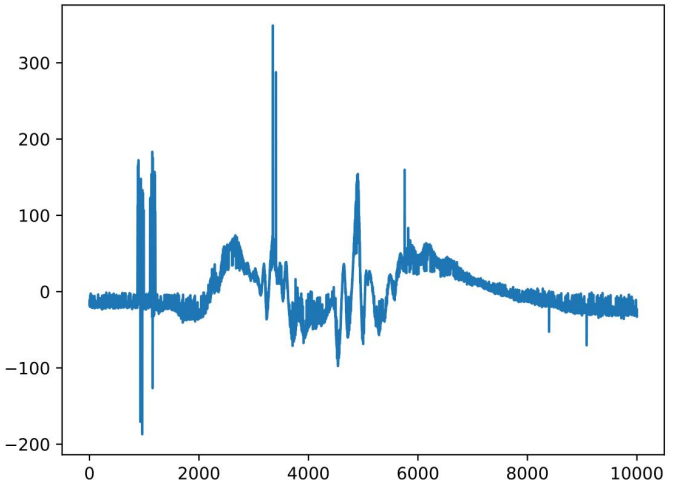
Motion-profile analysis.

Denoising processing - Low-pass filter vs median filter vs principle component analysis (PCA)









Reliability and robustness of wireless sensing

Profile integration mechanism. This part integrates the analysis result from two profile. We make use of the insight on individual strength of each profile to design the integration strategy to enhance the overall performance.

Transmission Rate and PCA-based Denoising

maximum probability based decision (MPD)

priority based decision (PBD)
PBD approach can combine the advantages of these two profiles and boost the recognition accuracy,

Reliability and robustness of wireless sensing

Activity detection algo.
This part is responsible for detecting and segmenting the CSI data for each activity. It is at the beginning of the workflow. Since our activity detection scheme utilized both multipath and motion profile, we put it in the later section.

The strategy of activity detections in TifWiFi goes in two steps.
In the first step, we first obtain the reference profile with ‘Empty’ activity (code ‘a’ in Table.1), which means no human in the test area. Then, with the multipath profile at the current time, the activity is detected with a large deviation from the reference profile by calculating the Euclidean distance.

We detect the motion activity if the motion intensity reaches 2 times of the maximum value during static period.

Reliability and robustness of wireless sensing

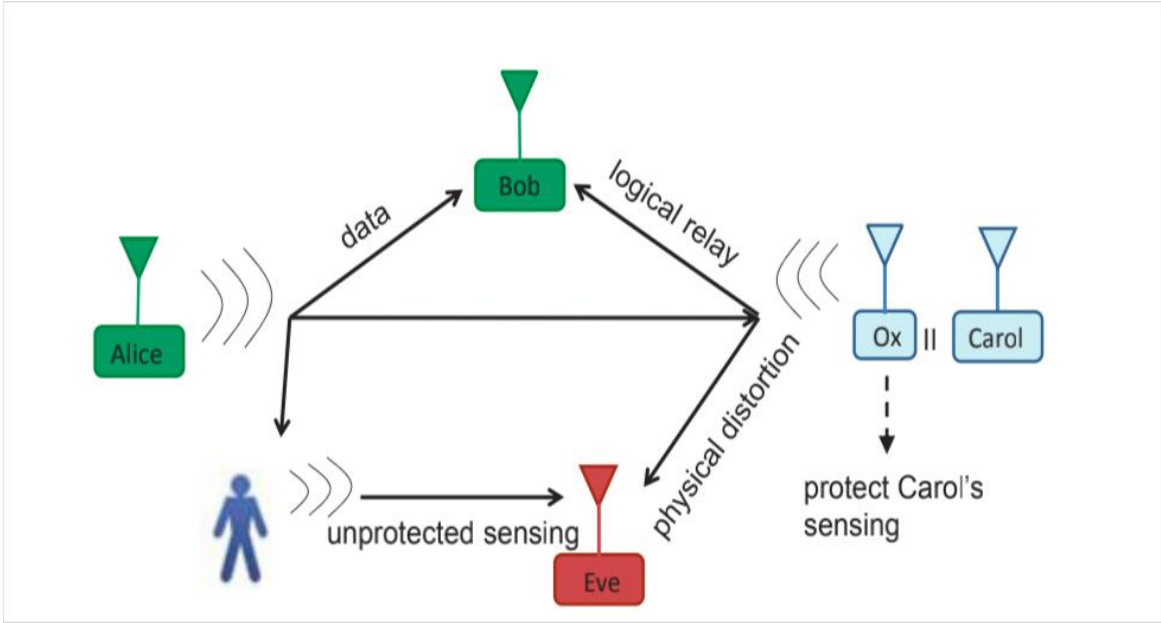
Testbed

- Qualcomm Atheros chipsets (i.e., Atheros AR9382 and Atheros AR9462)
- HP laptops as transmitter and receiver
- Wi-Fi PCIe card can support two antennas. Thus, with 802.11n Wi-Fi protocol, the signal transmission can support 2x2 MIMO stream
- 802.11 Wi-Fi standard specifies the requirement of setting the sounding flag to enable the CSI calculation and reporting functionality of the Wi-Fi card
- the linux kernal is modified with Atheros CSI tool in Ubuntu 14.04 LTS environment

Protect user privacy against malicious sensing

Obfuscating Sensing from Communication Signal

- counter the threat of unwanted or even malicious communication based sensing
- preserve data in the communication signal
- preserve sensing of legitimate sensors

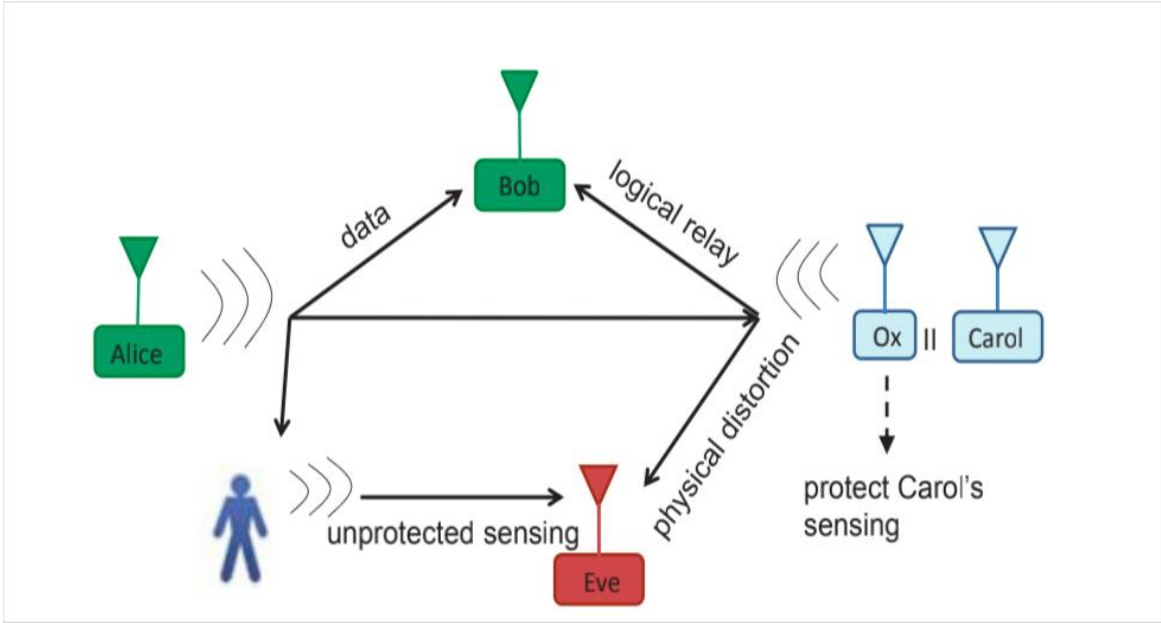


Protect user privacy against malicious sensing

Naive Approach: Jam the signal

- Communication is also disabled.
  - Two layers of information
  Physical layer
  Logical layer

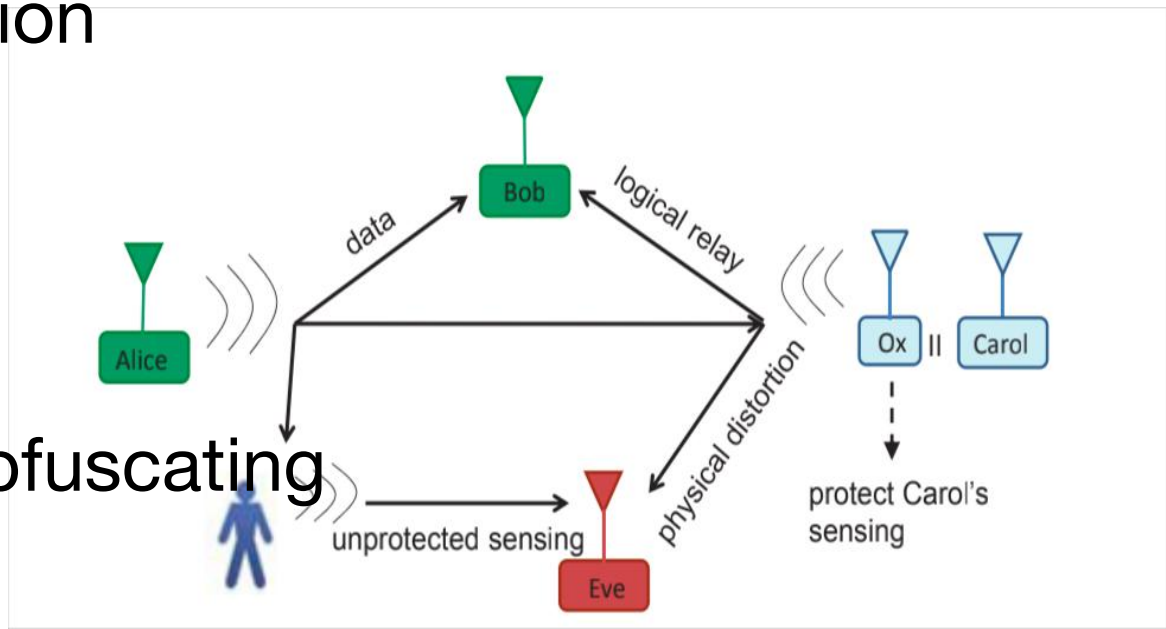
- Legitimate sensing is also disabled.
  - Random jam signal distorts all signals in the covered area.



Protect user privacy against malicious sensing

Proposed Approach: Signal Obfuscation

- Only distort physical-layer information
  - Two layers of information
  Physical layer
  Logical layer

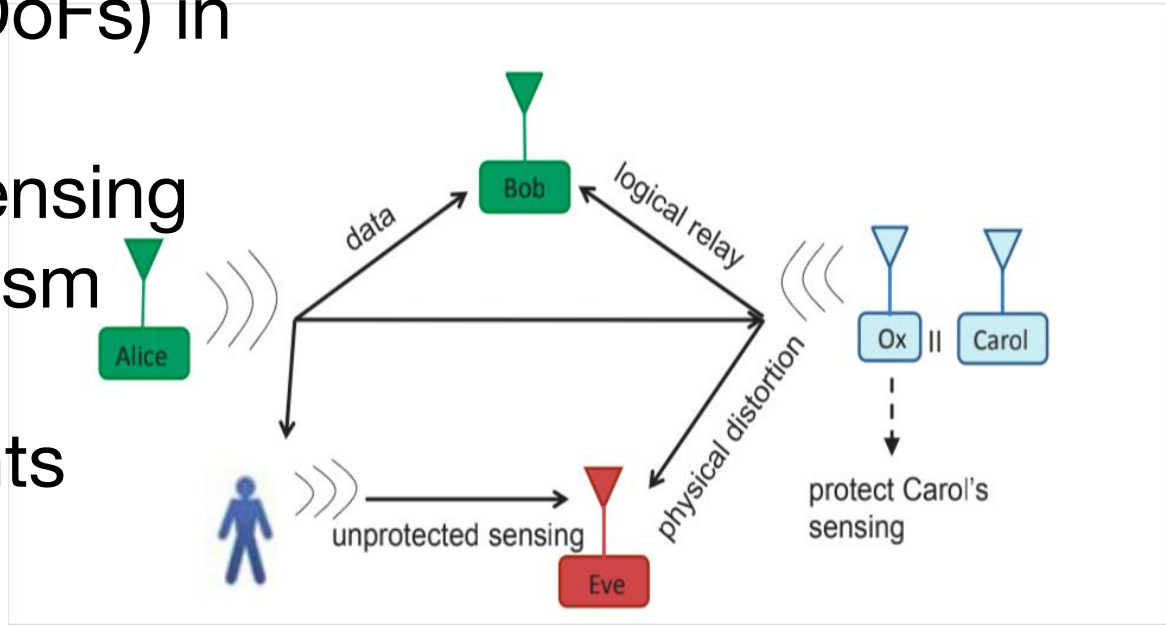


- Enable legitimate sensing on the obfuscating node
  - Since the obfuscating node has the knowledge of the obfuscation signal, it has the power to restore the original signal to maintain the sensing service.

Protect user privacy against malicious sensing

System Overview

- Distort three degrees of freedom (DoFs) in the signal
  - Disable the unauthenticated sensing regardless of the RF-sensing mechanism
- Ox performs as a relay node
  - Introduce multipath components
  - Preserve logical information
- Full-duplex cancellation
  - Restore the original signal



Protect user privacy against malicious sensing

Distort three degrees of freedom (DoFs) in the signal

- Summary of recent SISO sensing systems.

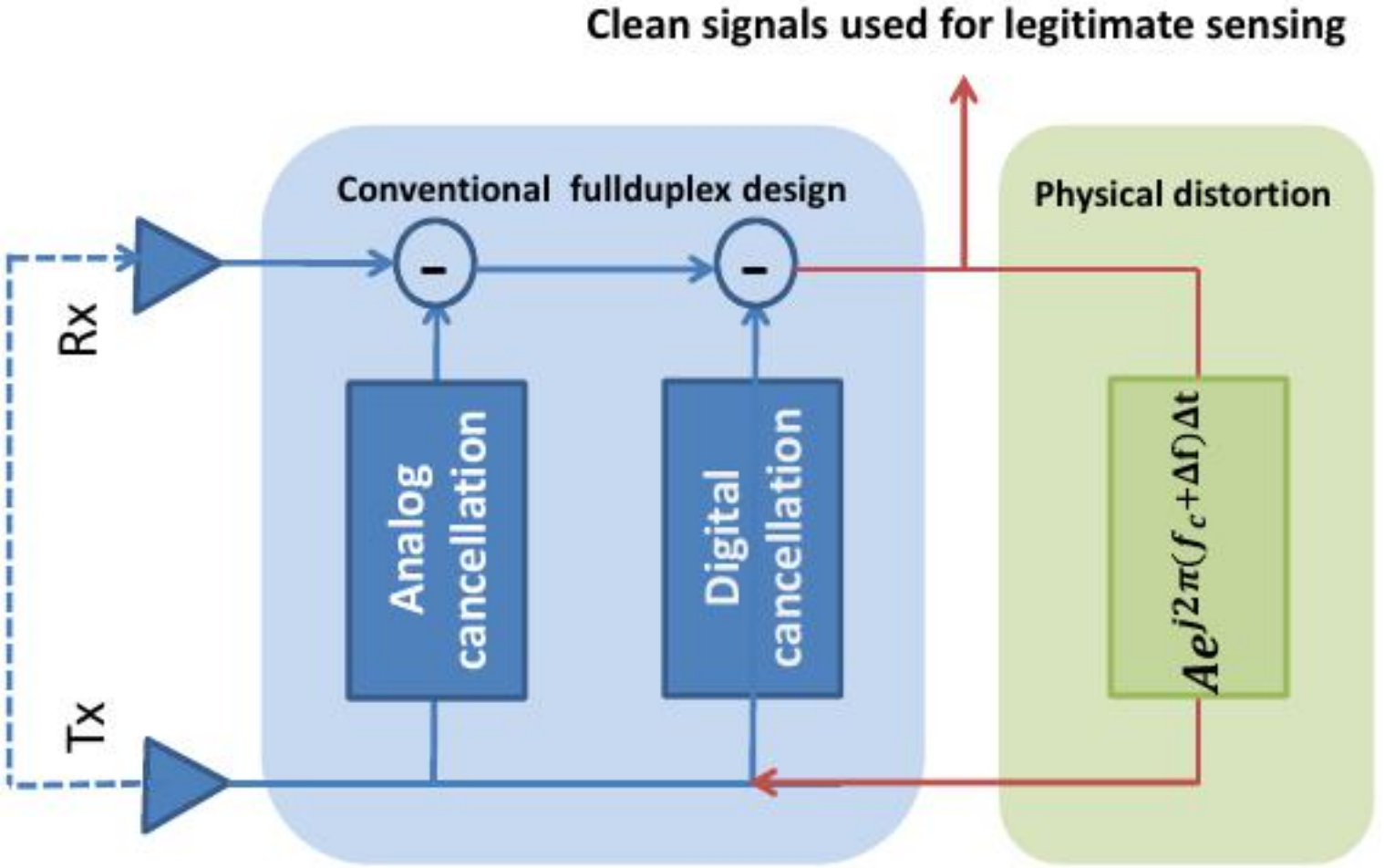
Existing Work	Feature Basis	Device	Sensing Task
WiSEE: Pu et al.	Doppler Shift	USRP-N210	Gesture recognition
Wi-Vi: Adib and Katabi	Phase	USRP-N210	Gesture based communication,tracking
E-eyes: Wang et al.	RSSI, CSI	802.11n devices	Activity classification
Gonzalez-Ruiz et al.	RSSI	802.11g wireless card	Obstacle mapping
Wang et al.	Phase, CSI	802.11ac devices	Activity classification
WiKey: Ali et al.	CSI	802.11n devices	Key recognition
RSA: Zhu et al.	RSS	Gigalink radios	Object imaging

$$r(t,f)=ae^{-j2\pi f\delta t}s(t-\delta t,f)$$

Protect user privacy against malicious sensing

Full-duplex relay node

- Analog cancellation
- Digital cancellation
- Physical distortion



Protect user privacy against malicious sensing

Online maintenance of self-channel estimates

- Wireless channel is changing over time
  - Coherence time ~ 100ms
- External transmission
  - Distort self-channel estimation and interfere with data reception
- Superposition of training signal and external transmission

$$\begin{Bmatrix} b_0 \\ b_1 \\ \dots \\ b_m \end{Bmatrix} = \begin{Bmatrix} a_0 & \dots & a_{-m} \\ a_1 & \dots & a_{-m+1} \\ \dots & \dots & \dots \\ a_m & \dots & a_0 \end{Bmatrix} \times \begin{Bmatrix} h_0 \\ h_1 \\ \dots \\ h_m \end{Bmatrix} + \begin{Bmatrix} s_0 & \dots & s_{-m} \\ s_1 & \dots & s_{-m+1} \\ \dots & \dots & \dots \\ s_m & \dots & s_0 \end{Bmatrix} \times \begin{Bmatrix} h_0' \\ h_1' \\ \dots \\ h_m' \end{Bmatrix}$$

Protect user privacy against malicious sensing

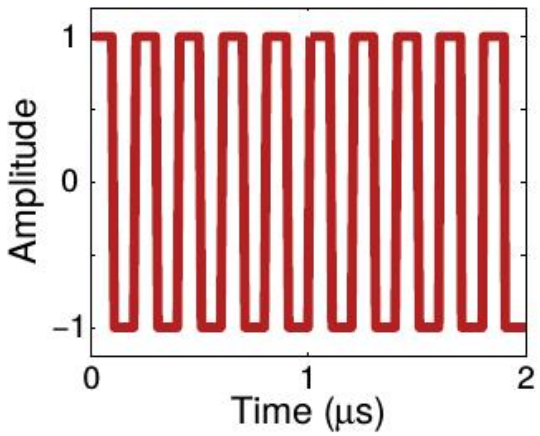
Online maintenance of self-channel estimates

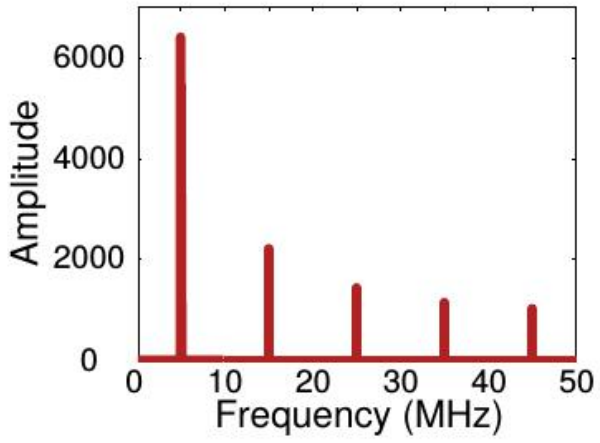
- Oversampling and differentiation

$$\begin{Bmatrix} b_1-b_0 \\ b_2-b_1 \\ \dots \\ b_m-b_{m-1} \end{Bmatrix} = \begin{Bmatrix} a_1-a_0 & \dots & a_{-m+1}-a_{-m} \\ a_2-a_1 & \dots & a_{-m+2}-a_{-m+1} \\ \dots & \dots & \dots \\ a_m-a_{m-1} & \dots & a_0-a_{-1} \end{Bmatrix} \times \begin{Bmatrix} h_0 \\ h_1 \\ \dots \\ h_m \end{Bmatrix}$$

- Special training sequence

$$a_{-m}=a_{-m+1}=\dots=a_0=a_1+c=\dots=a_m+c$$



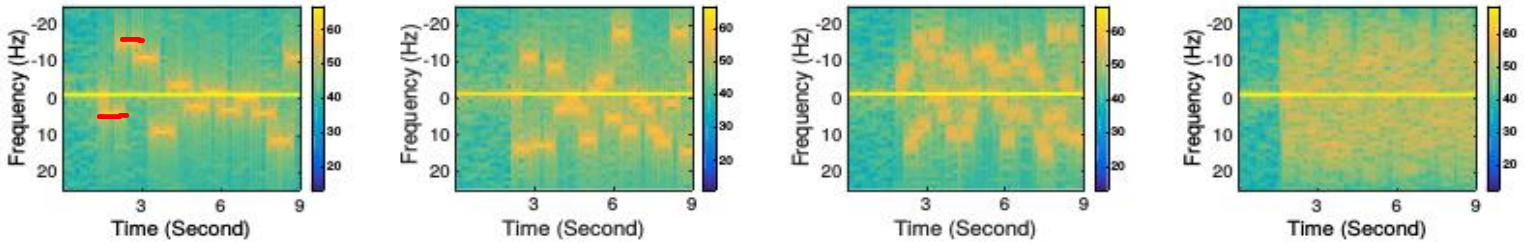


Protect user privacy against malicious sensing

Obfuscation of Patterns in 3 DoFs

$$\hat{r}(t) = a_1 \times s(t) \times e^{j2\pi(f_c+\Delta f_1)(t+\Delta t_1)} + a_2 \times s(t) \times e^{j2\pi(f_c+\Delta f_2)(t+\Delta t_2)}$$

$$\hat{R}(f) = a_1 e^{j2\pi(f_c+\Delta f_1)\Delta t_1} S(f - f_C - \Delta f_1) + a_2 e^{j2\pi(f_c+\Delta f_2)\Delta t_2} S(f - f_C - \Delta f_2)$$



(a) 1s (b) 0.5s (c) 0.125s (d) 0.05s

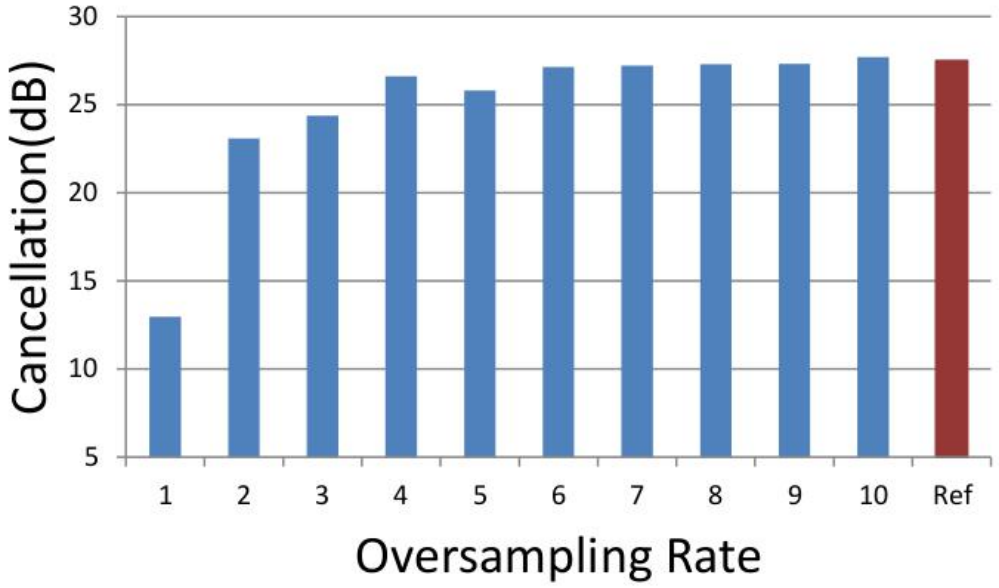
Protect user privacy against malicious sensing

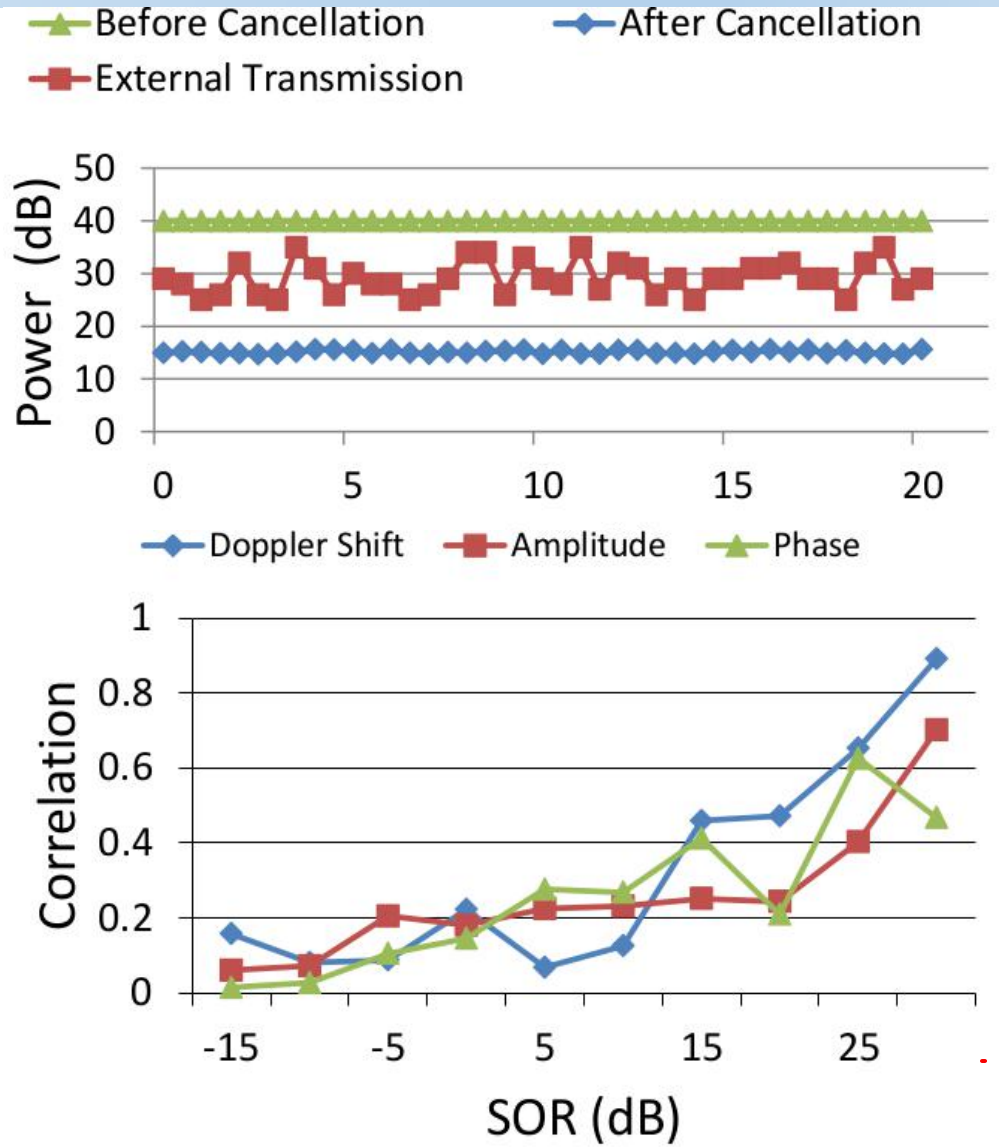
Testbed

- PXIe 1082 SDR platform
- NI PXIe-7965R (FPGA)
  - Self-channel estimation, digital cancellation and physical-layer distortion
- Distortion processing – 100ns latency

Protect user privacy against malicious sensing

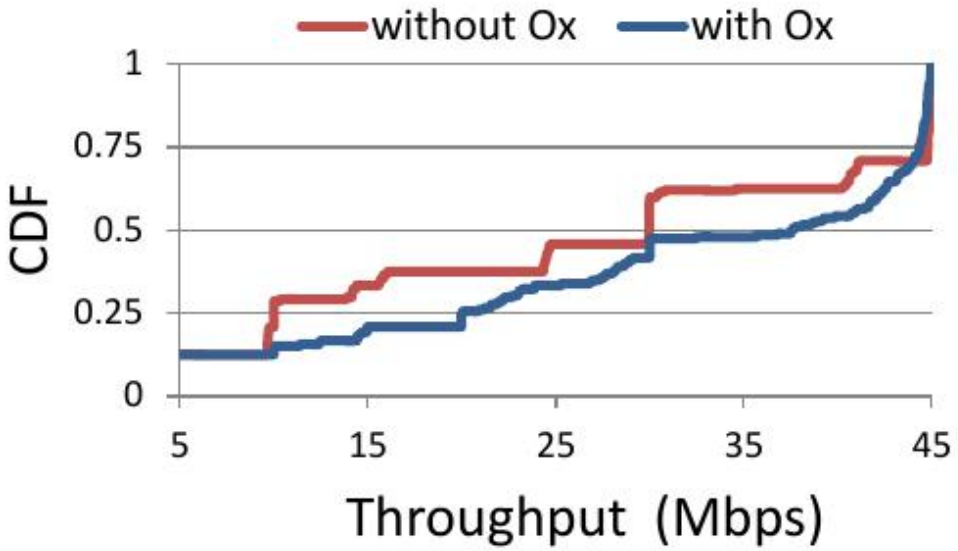
Evaluation - cancellation

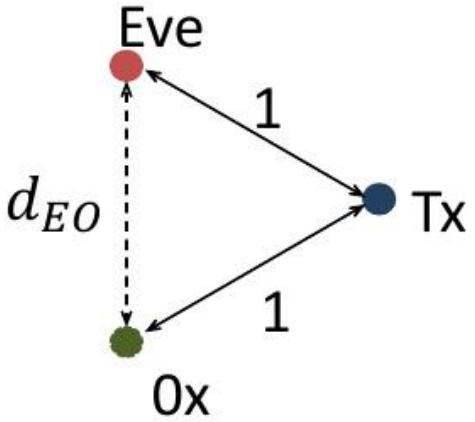


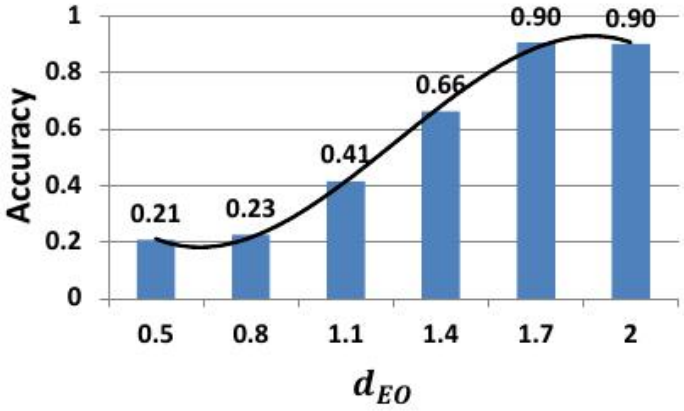


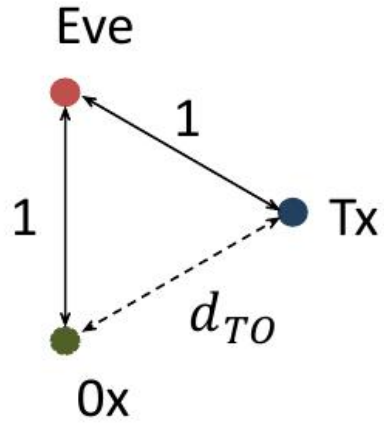
Protect user privacy against malicious sensing

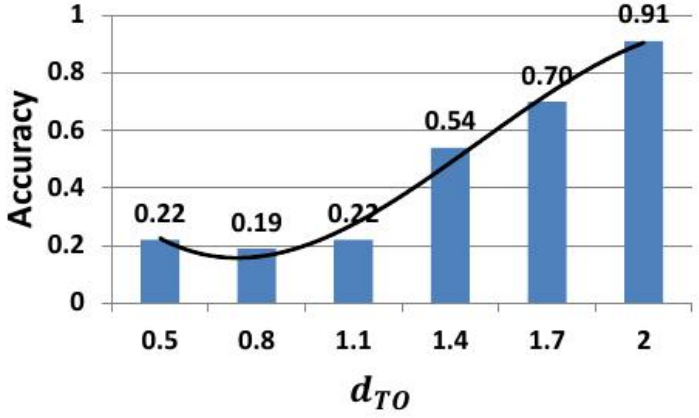
Evaluation - performance











Conclusions & Future works

Gesture recognition - reliable and robust

- Fine-grain finger gesture
- Whole-home human activity
- Explore 3+ antenna setting for more use cases

Sensing protection - works without side effects

- blackbox sensor obfuscation technique
- Explore multple obfuscators for more use cases

Acknowledgements

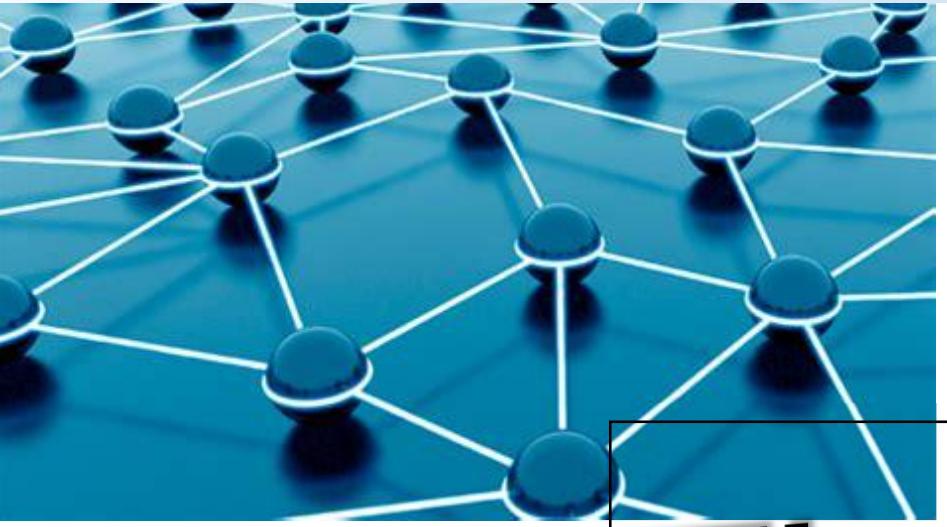
- Collaborators

  Yue Qiao, Wenjie Zhou, Yifan Mao, Kannan Srinivasan, Anish Arora

- Research funding

  NSF grants CNS-1547306, CNS-1514260, CNS-1254032 and CNS-1302620.

Thank you



Thank You!