IEEE INFOCOM

RFnoID: Protecting RFID Motion Privacy via Metasurface

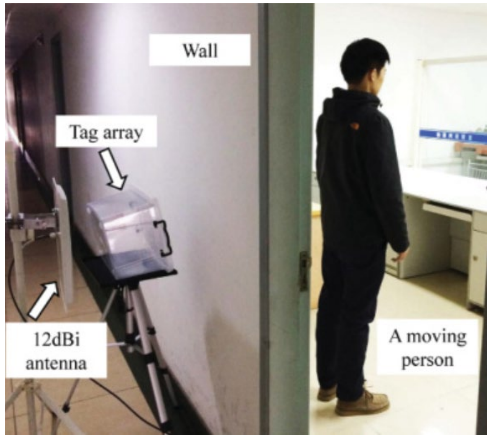
Yanni Yang[1], Zheng Shi[1], Zhenlin An[2], Runyu Pan[1],
Yanling Bu[3], Guoming Zhang[1], Pengfei Hu[1], Jiannong Cao[4]

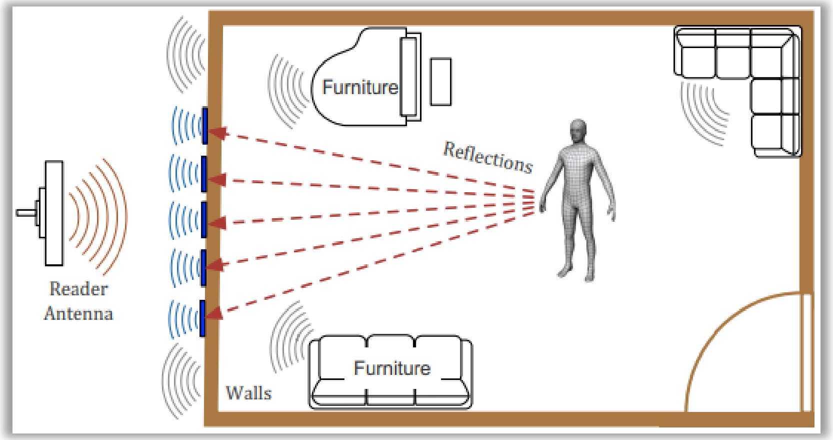
[1]Shandong University, China
[2]University of Pittsburgh, USA
[3]Nanjing University of Aeronautics and Astronautics, China
[4]The Hong Kong Polytechnic University, China

山东大学 SHANDONG UNIVERSITY
University of Pittsburgh

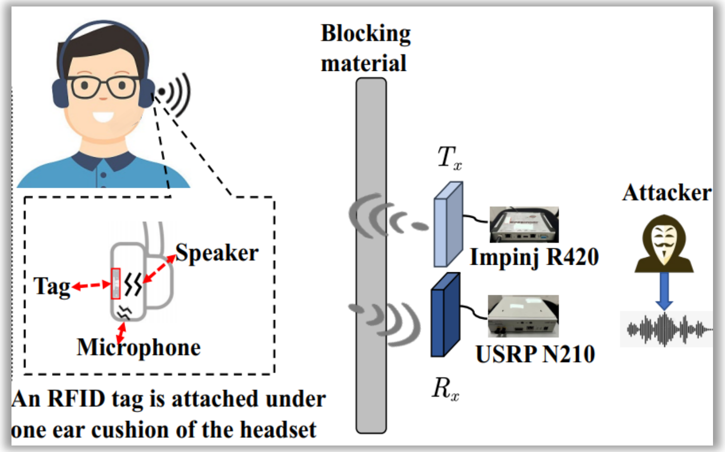
Motivation

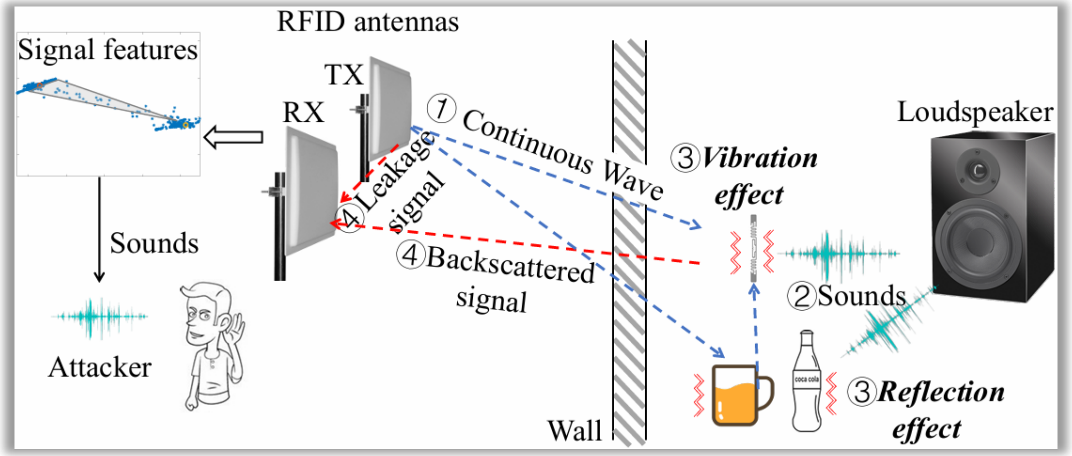
Through-wall walking detection and positioning [1][2]





Through-wall speech eavesdropping [3] [4]

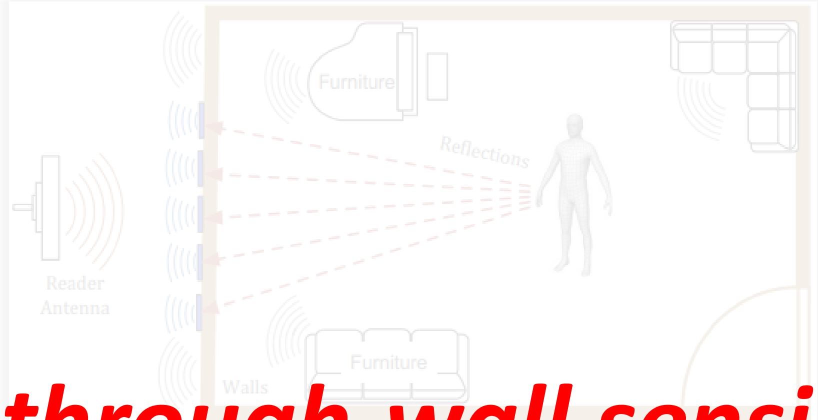




[1] Wang, Z., et al. A See-through-Wall System for Device-Free Human Motion Sensing Based on Battery-Free RFID. TECS, 2018.
[2] Yang, L., et al. See Through Walls with COTS RFID System! MobiCom, 2015.
[3] Wang, C., et al. Thru-the-wall Eavesdropping on Loudspeakers via RFID by Capturing Sub-mm Level Vibration. IMWUT, 2021
[4] Chen, Y., et al. RFSpy: Eavesdropping on Online Conversations with Out-of-Vocabulary Words by Sensing Metal Coil Vibration of Headsets Leveraging RFID. MOBISYS, 2024

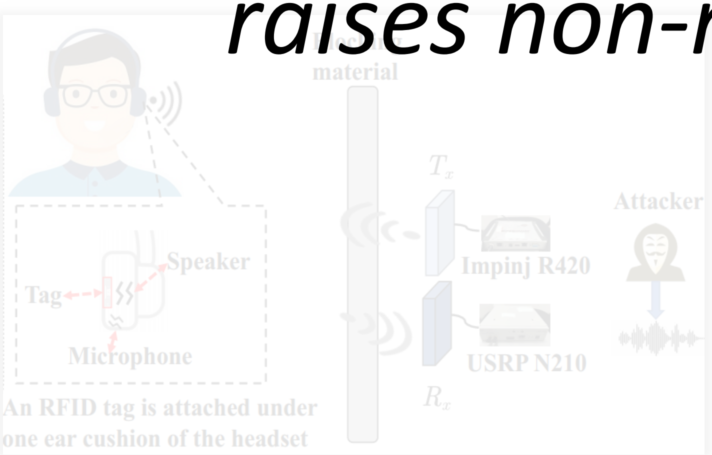
Motivation

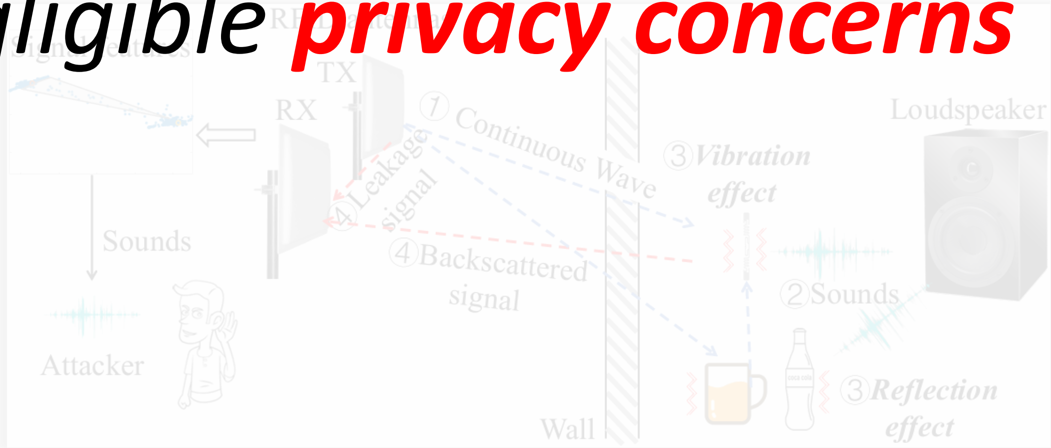
Through-wall *walking* detection and *positioning* [1][2]



The strong *through-wall sensing ability* raises non-negligible *privacy concerns*

Through-wall *audio* eavesdropping [3] [4]





[1] Wang, Z., et al. A See-through-Wall System for Device-Free Human Motion Sensing Based on Battery-Free RFID. TECS, 2018.
[2] Yang, L., et al. See Through Walls with COTS RFID System! MobiCom, 2015.
[3] Wang, C., et al. Thru-the-wall Eavesdropping on Loudspeakers via RFID by Capturing Sub-mm Level Vibration. IMWUT, 2021
[4] Chen, Y., et al. RFSpy: Eavesdropping on Online Conversations with Out-of-Vocabulary Words by Sensing Metal Coil Vibration of Headsets Leveraging RFID. MOBISYS, 2024

Existing Solutions

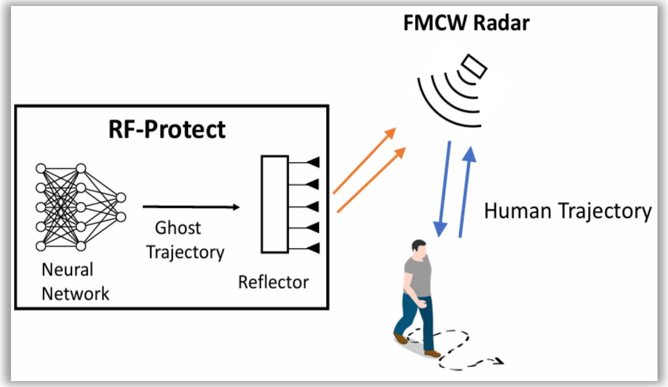
Communication security:

[NSDI'15]

RFID-based

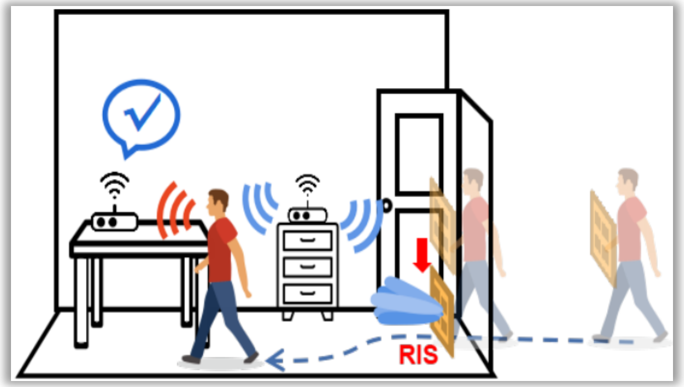
Incompatible with existing systems

Other wireless sensing security:



[SIGCOMM'22]

FMCW radar-based



[Sensys'23]

WiFi-based

Inherent different protocols and sensing models

Existing Solutions

Communication security:

Other wireless sensing security:

*Existing literature **lacks** an efficient way to safeguard **RFID motion sensing***

[NSDI'15]

[SIGCOMM'22]

[Sensys'23]

RFID-based

FMCW radar-based

WiFi-based

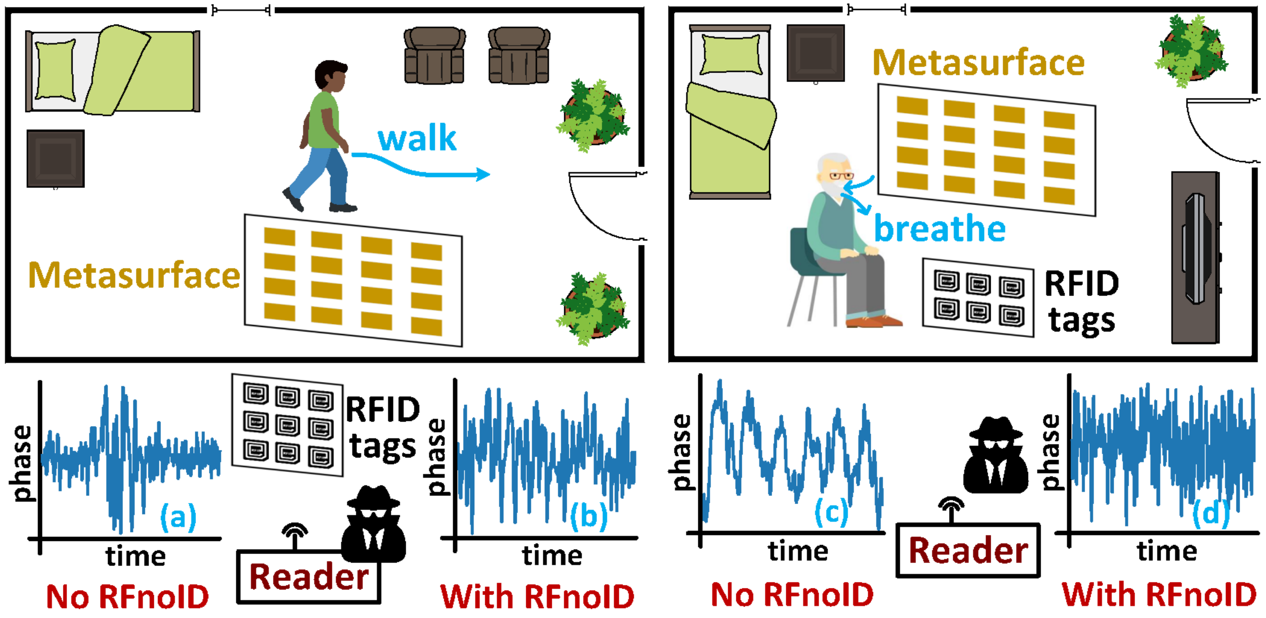
Incompatible with existing systems

Inherent different protocols and sensing models

Our Solution

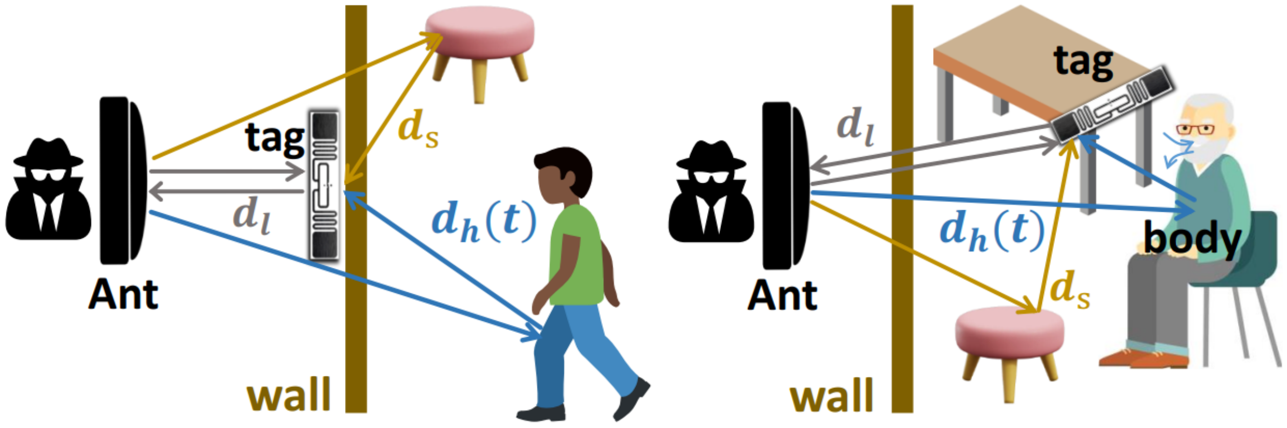
*Key Idea – **passively** introduce **motion-irrelevant noise** in the **physical channel** to obfuscate the motion-induced signals*

1) *Design of a low-cost metasurface*
2) *Signaling mechanism, obfuscation strategy*



Primer on Through-Wall RFID Motion Sensing

- *Adversarial Sensing Model*

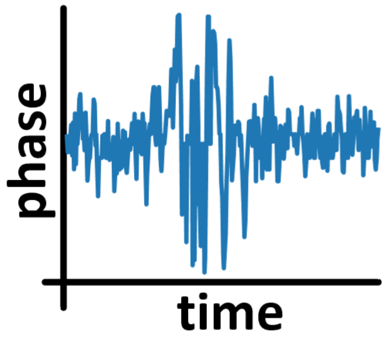


(a) tag outside the room (b) tag inside the room

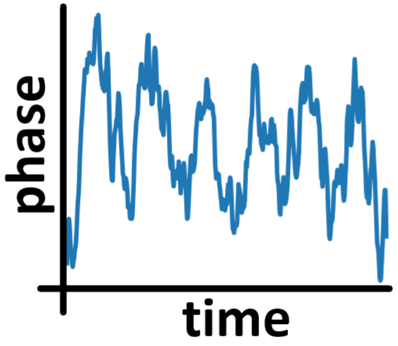
$$R(t) = \alpha_l e^{-j\frac{2d_l}{\lambda}} + \alpha_s e^{-j\frac{d_s+d_l}{\lambda}} + \alpha_h(t) e^{-j\frac{d_h(t)+d_l}{\lambda}}$$

Human-reflected

$$\Delta\phi_h(t) = \frac{d_h(t)}{\lambda} \ mod\ 2\pi$$



Walking



Breathing

- *Adversarial Sensing Tasks and Algorithms*

Walking Detection
- Variance-based [1]
- Learning-based [2]
  - Hand-crafted statistical features
  - Neural network latent vector

Respiration Eavesdropping [3]
- Band-pass filter -> FFT peak

[1] Wang, Z., et al. A see-through-wall system for device-free human motion sensing based on battery-free RFID. ACM Transactions on Embedded Computing Systems, 2017.
[2] Jiang, S., et al. RF-Gait: Gait-based person identification with COTS RFID. Wireless Communications and Mobile Computing, 2022.
[3] Zhao, R., et al. CRH: A contactless respiration and heartbeat monitoring system with COTS RFID tags. Proc. of IEEE SECON, 2018.

Preliminaries: Metasurface Design and Modelling

- *Fabrication of the Reflective Metasurface*

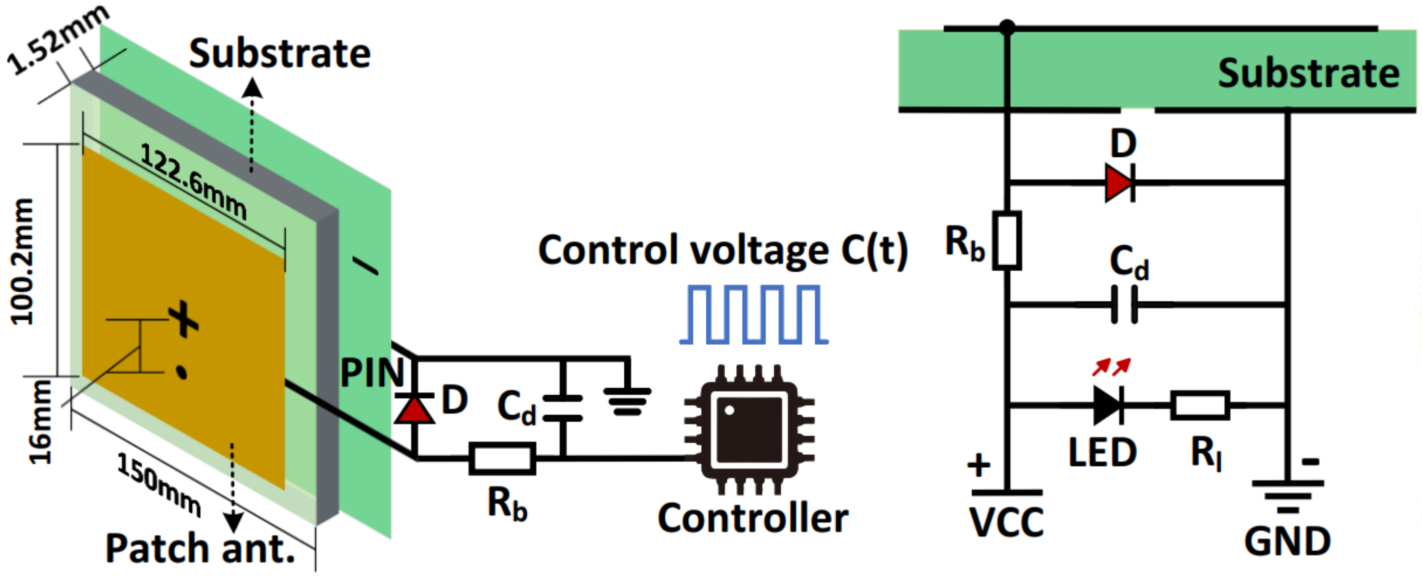
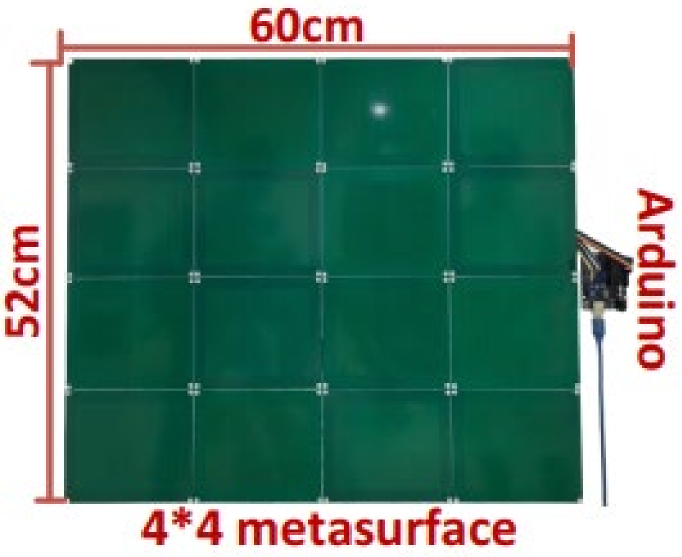
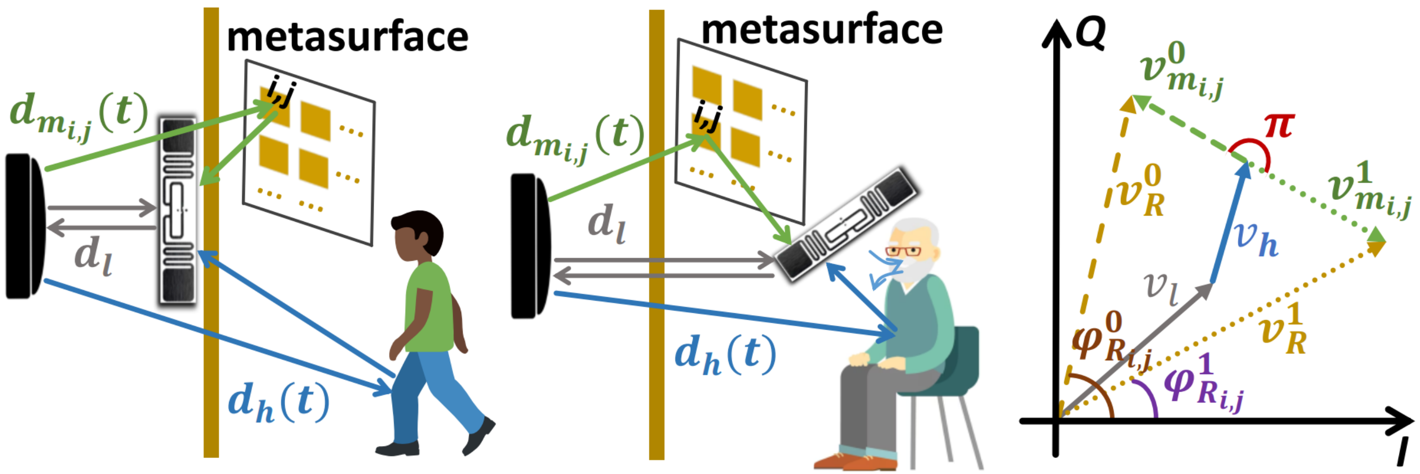


Diagram of the unit structure



RFnoID prototype

Preliminaries: Metasurface Design and Modelling



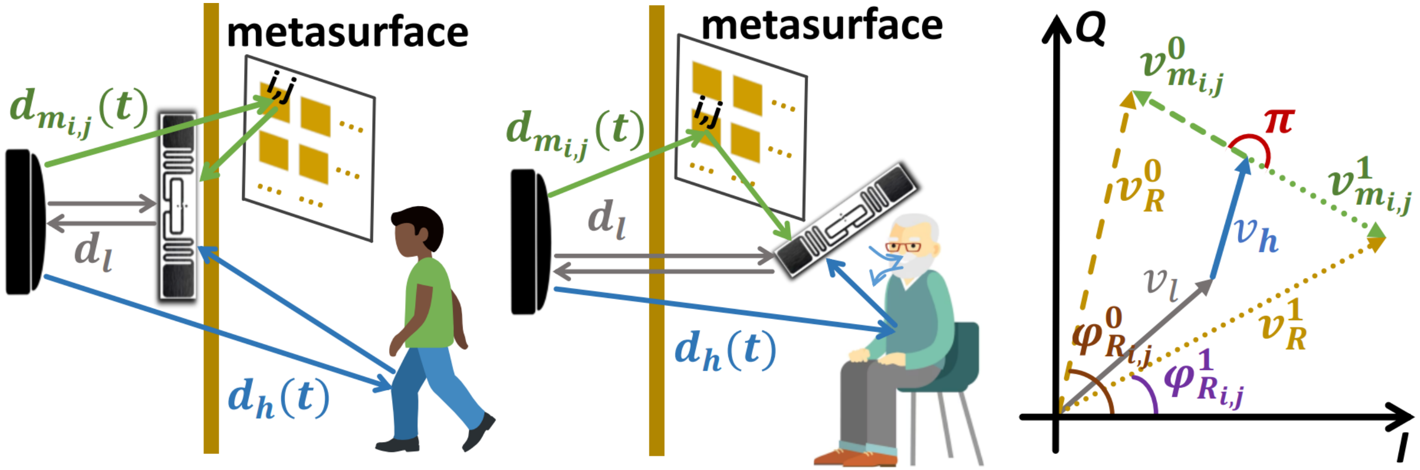
(a) signal path by metasurface (b) I-Q signal vector

1) How does the surface affect the original sensing?

- $R(t)=\alpha_l e^{-j\frac{2d_l}{\lambda}} + \alpha_s e^{-j\frac{d_s+d_l}{\lambda}} + \alpha_h(t)e^{-j\frac{d_h(t)+d_l}{\lambda}} + \sum_{i=1}^{N}\alpha_{m_i}(t)e^{-j\frac{d_{m_i}(t)+d_l}{\lambda}}$
- $v_R^{0/1}=v_l + v_s + v_h + \sum_{i=1}^{N} v_{m_i}^{0/1}$

Human-reflected *Metasurface-induced*

Preliminaries: Metasurface Design and Modelling



(a) signal path by metasurface (b) I-Q signal vector

1) How does the surface affect the original sensing?

- $R(t)=\alpha_l e^{-j\frac{2d_l}{\lambda}} + \alpha_s e^{-j\frac{d_s+d_l}{\lambda}} + \alpha_h(t)e^{-j\frac{d_h(t)+d_l}{\lambda}} + \sum_{i=1}^{N}\alpha_{m_i}(t)e^{-j\frac{d_{m_i}(t)+d_l}{\lambda}}$
- $v_R^{0/1}=v_l + v_s + v_h + \sum_{i=1}^{N} v_{m_i}^{0/1}$

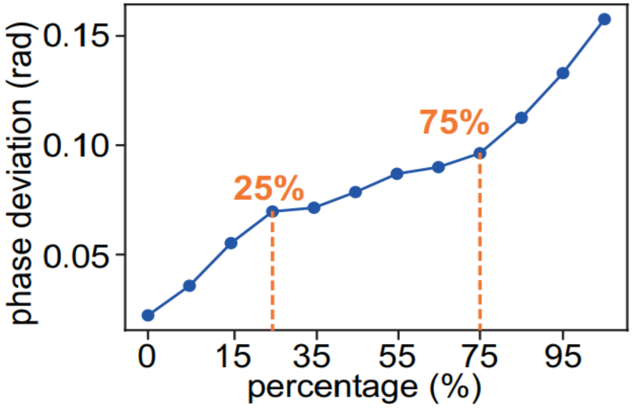
Human-reflected *Metasurface-induced*

2) Can the 1-bit surface obfuscate motion signal in various ways?

- *N* = 16, phase can exhibit 2^{16} = 65536 unique values

Preliminaries: Observation 1

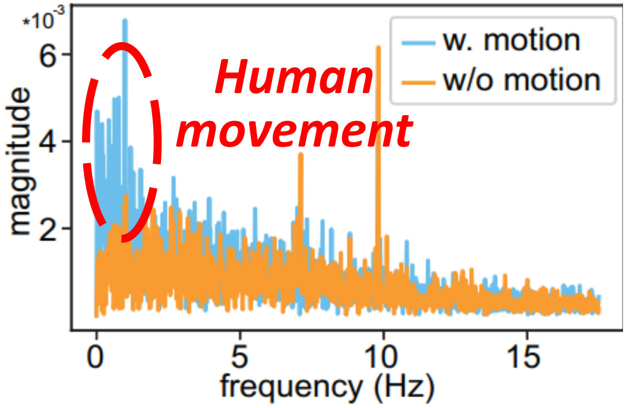
- *The **phase variation** is positively correlated to the **number of units flipped***



Naïve Solution – *construct a set-flipping scheme:*

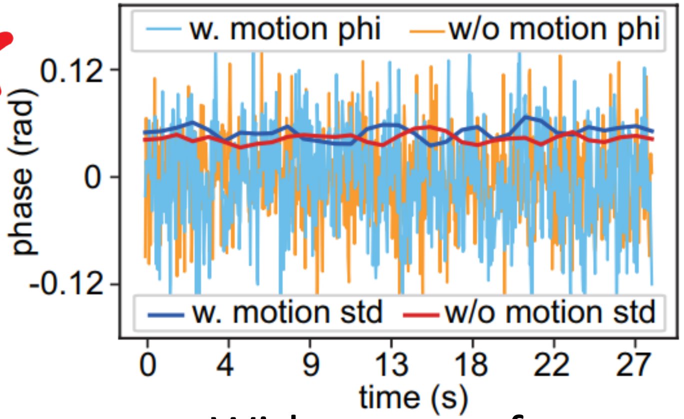
1) *max-set (0 - 15% units on)*
2) *min-set (85 - 100 % units on)*

- ***Issue 1**: fails to obfuscate the motion signal in the spectral domain*

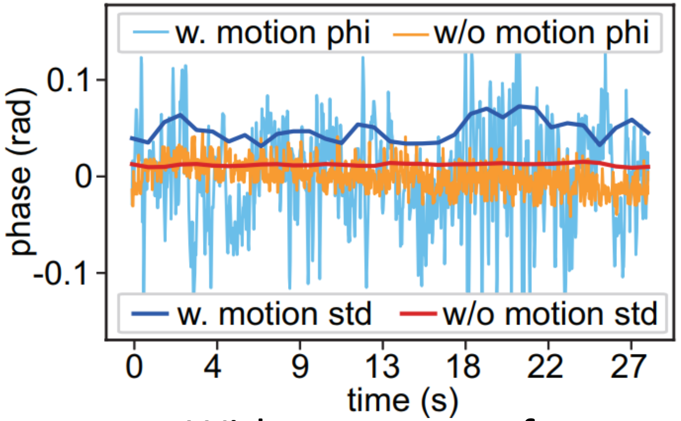


FFT results

~~Spectral domain~~



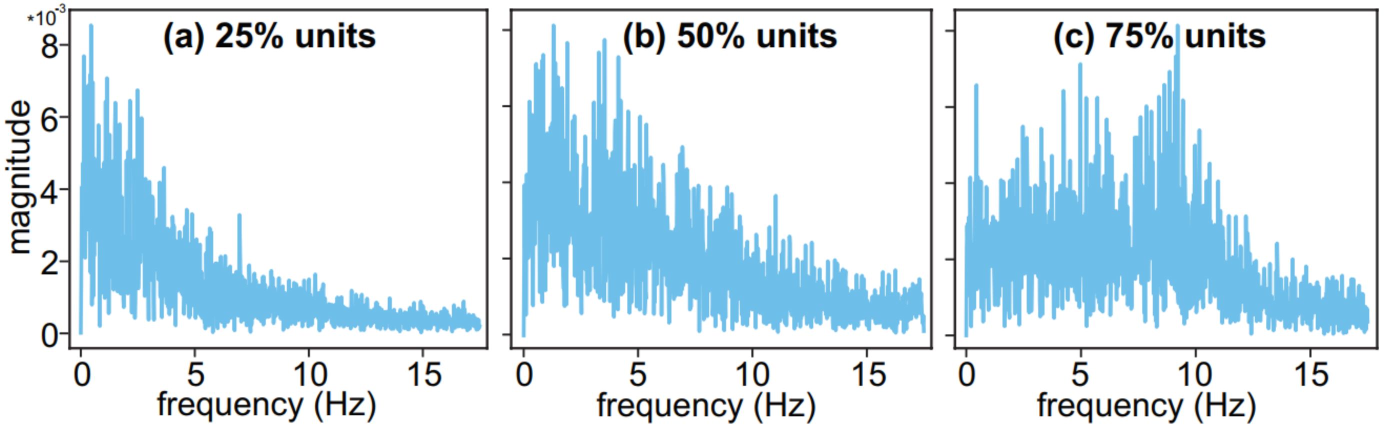
With metasurface



Without metasurface

Preliminaries: Observation 2

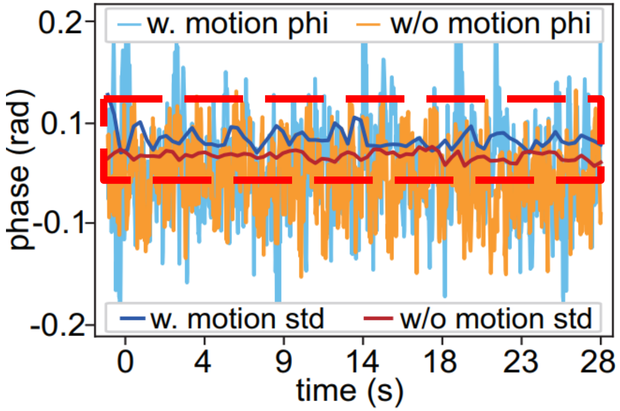
- ***Component frequency*** *is positively correlated to the* ***number of units flipped***



Naïve Solution – why not flipping less units?

e.g., 25% units

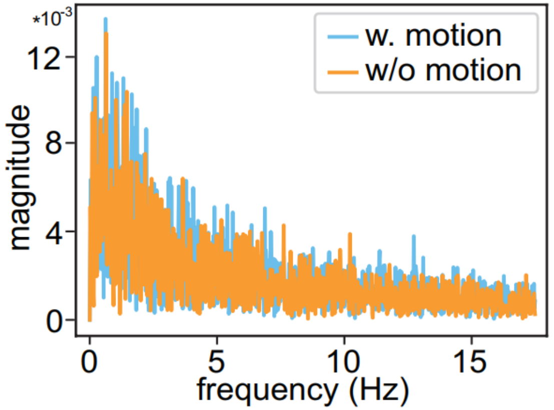
- ***Issue 2:*** *insufficient signal obfuscation in the temporal domain*



Phase and std

~~Temporal domain~~

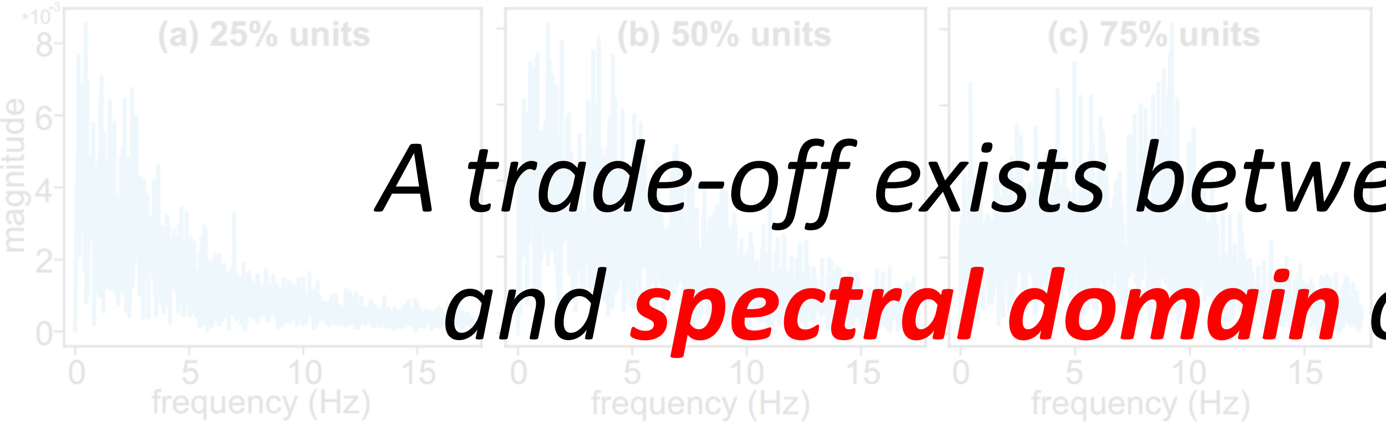
Human motion can be detected easily



Phase spectrum

Preliminaries: Observation 2

- *Component frequency is positively correlated to the number of units flipped*



Naïve Solution – *why not flipping less units?*

e.g., 25% units

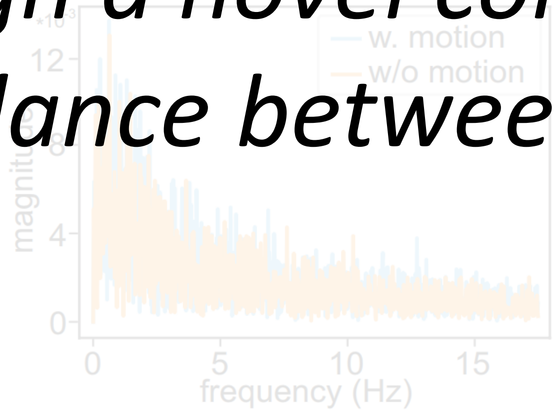
*A trade-off exists between **temporal** and **spectral domain** obfuscation*

- ***Issue 2:*** *insufficient signal obfuscation in the temporal domain*

Phase and std

~~*Temporal domain*~~

Human motion can be detected easily



Phase spectrum

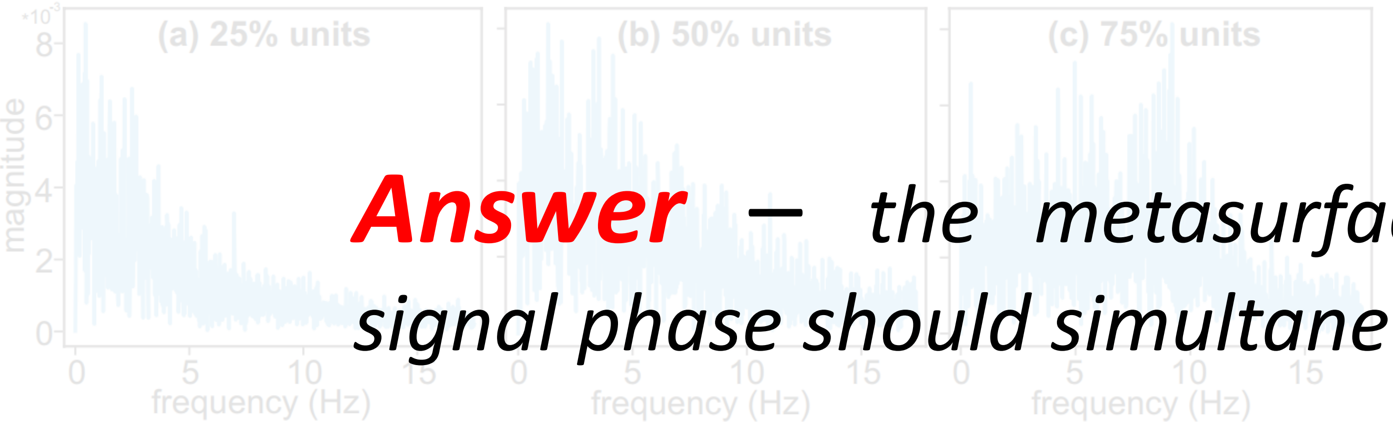
Question: *Can we design a novel controlling approach to strike a balance between them?*

Key Goals for obfuscating Motion Signal

Answer – *the metasurface-affected signal phase should simultaneously have*

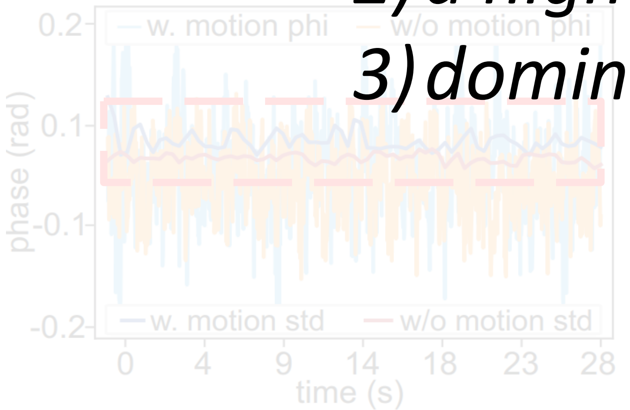
*1) a high signal **entropy***
*2) a high temporal **variance***
*3) dominant **frequencies** around the motion frequencies*

- *Component frequency is positively correlated to the number of units flipped*



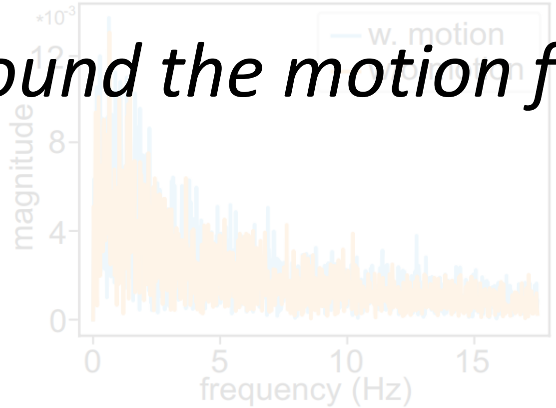
Naïve Solution – *why not flipping less units?*
e.g., 25% units

- ***Issue 2:*** *insufficient signal obfuscation in the temporal domain*



Phase and std

Temporal domain
Human motion can be detected easily



Phase spectrum

Obfuscation Controlling Strategy

- ***Base strategy***: *randomly select the number of units X_n to flip from {0, 1, 2, ..., N}, then flip a random combination of X_n units among all units*

Maximizing the phase entropy

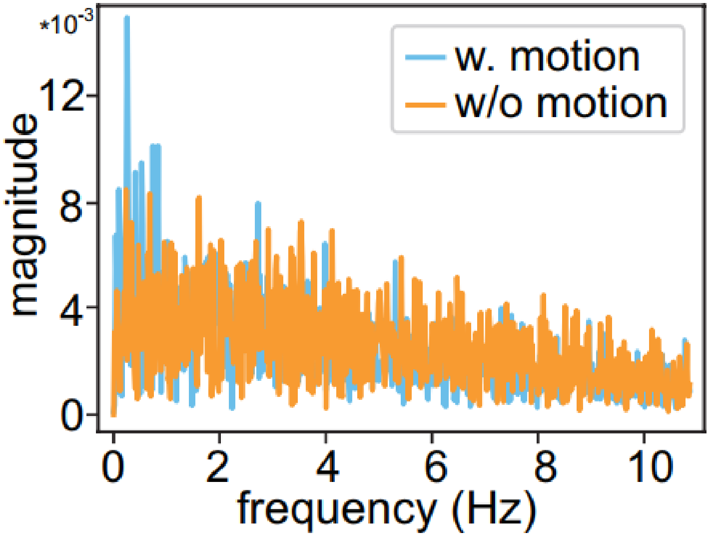
$$v_R^{0/1} = v_l + v_s + v_h + \sum_{i=1}^{N} v_{m_i}^{0/1}$$

$$\Updownarrow$$

Maximizing the entropy in selecting the unit state

1) *select an integer X_n in [0, N]*
2) *select a set X_s from $C_N^{X_n}$ combinations*

Uniform distribution

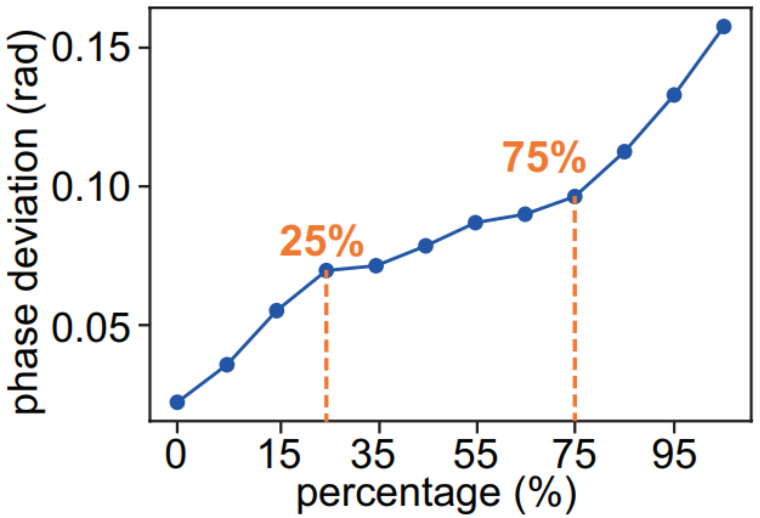


Phase spectrum with Base strategy

Goal 1: Achieving High Phase Entropy ✔

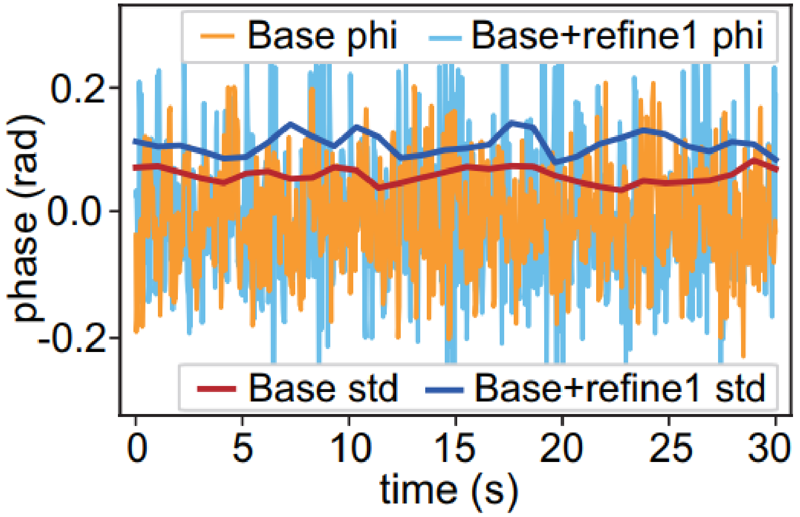
Obfuscation Controlling Strategy

- ***Refinement 1**: if a random flip resulted in a $N_{on} < \boldsymbol{\sigma_s} \times N$ or $N_{on} > \boldsymbol{\sigma_l} \times N$ $(\sigma_s < \sigma_l)$, we switch on or off all units at the next timestamp respectively*



Phase deviation of increasing units

$$\sigma_s = 25\%$$
$$\sigma_l = 75\%$$

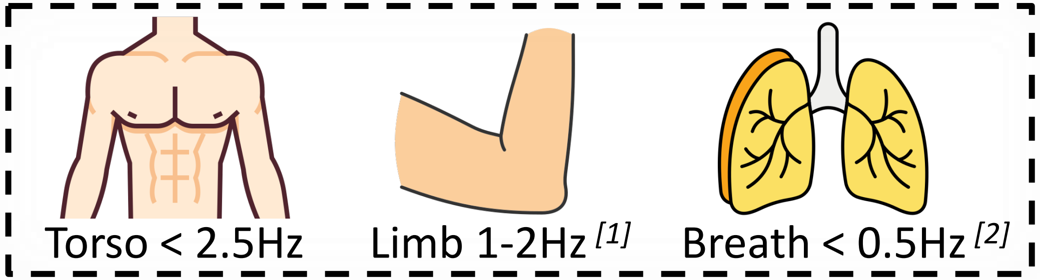


Temporal phase with/without Refinement1

Goal 2: Achieving High Phase Variance ✔

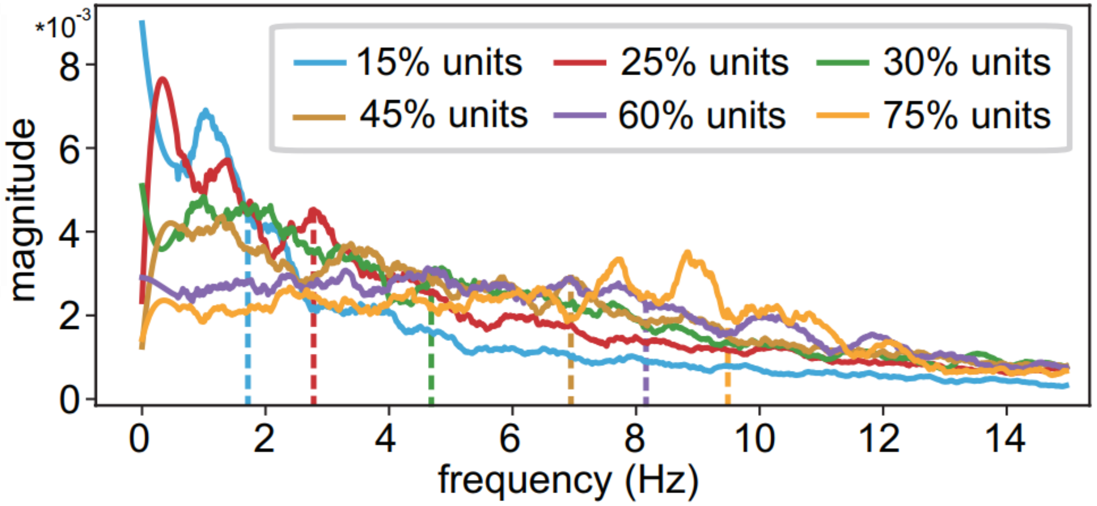
Obfuscation Controlling Strategy

- ***Refinement 2**: attach a higher likelihood $\boldsymbol{w}$ to choosing a number less than $\boldsymbol{\sigma_f} \times N$ as the number of units to flip X_n in the Base strategy*



Compare the spectrum and calculate similarity

$\boldsymbol{\sigma_f = 0.25}$ $\boldsymbol{w = 0.6}$



The spectrum for different numbers of flipped units

Goal 3: Achieving Strong Spectral Components Around the Human Motion Frequency Band ✔

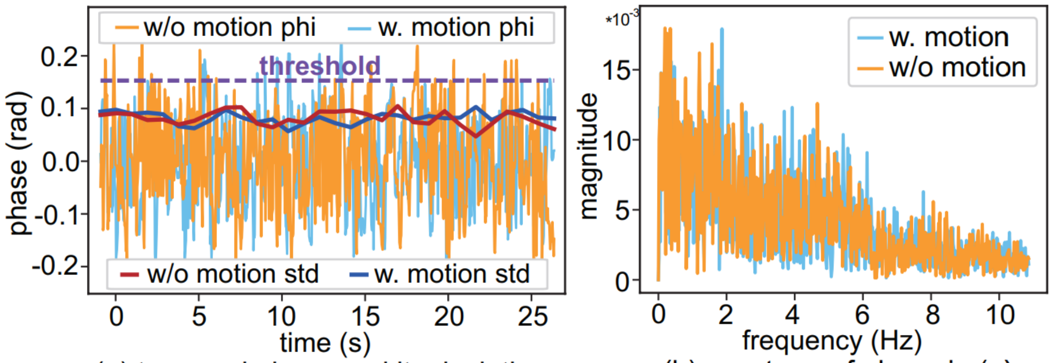
[1] Fulk, G.D., et al. *Predicting home and community walking activity poststroke.* Stroke, 2017.
[2] Lockett, E., et al. *Normal respiratory rate for adults and children.* Healthline Media, 2022.

Controlling Strategy as a Whole

Algorithm 1 Metasurface Controlling Strategy in RFNOID

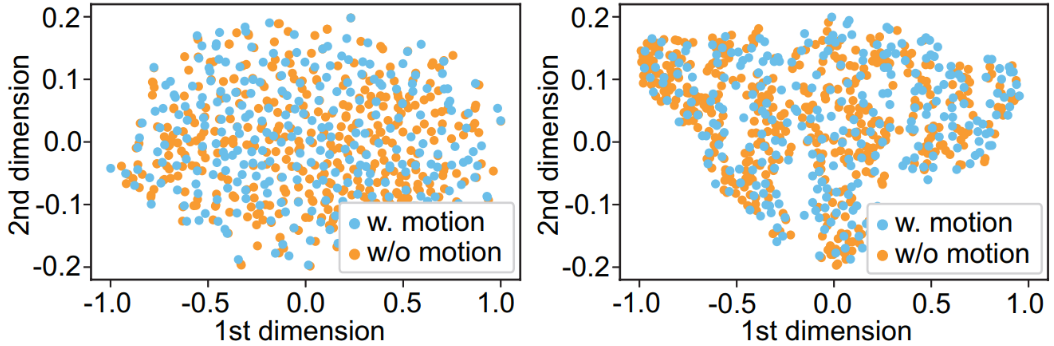
```
Require: N, t_r, σ_s, σ_l, w, σ_f, all units off
  srand(t_r); flipSet = [ ]; keepSet = [U_1, ..., U_N]; flag = RAND
  while True do
    if n_on < σ_s × N and flag = FLIP then                ▷ Refine 2
      writeToPins(allpins, ON); flag = RAND;
    else if n_on > σ_l × N and flag = FLIP then;
      writeToPins(allpins, OFF); flag = RAND;
    else
      randomNum = getRandom(0, 1);
      if randomNum < w then                                ▷ Refine 1
        percentage = getRandom(0, σ_f);                    ▷ Base
      else
        percentage = getRandom(σ_f, 1);
      end if
      switchNum = percentage × N
      for i = 0, i < switchNum, i++ do                     ▷ Base
        ind = getRandom(0, 1) % (length(keepSet));
        flipSet.append(U_ind); keepSet.delete(U_ind);
      end for
      writeToPins(flipSet, FLIP); flag = FLIP;
    end if
  end while
```

✓ *Walking: variance-based*



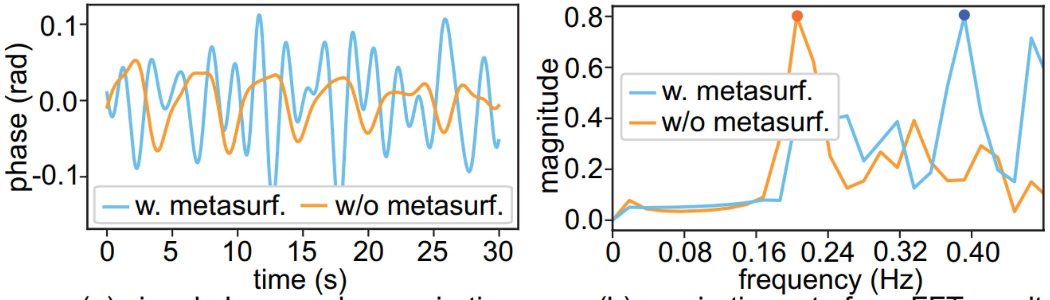
(a) temporal phase and its deviation (b) spectrum of phase in (a)

✓ *Walking: learning-based*



(a) t-SNE on temporal features (b) t-SNE on spectral features

✓ *Respiration eavesdropping*



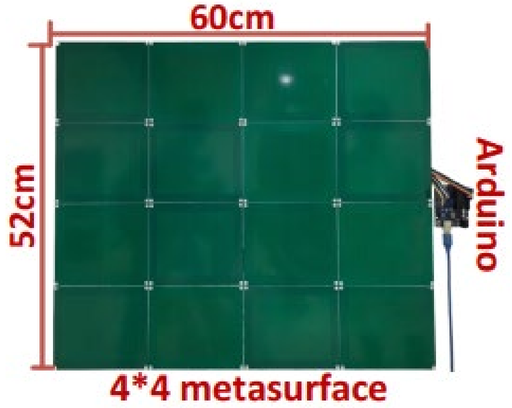
(a) signal phase under respiration (b) respiration rate from FFT result

Whole strategy (RFnoID) *can obfuscate both the* ***raw signal*** *and the* ***high-level features***

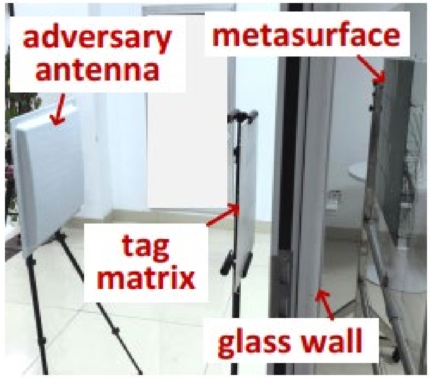
Experimental Setup

Device:

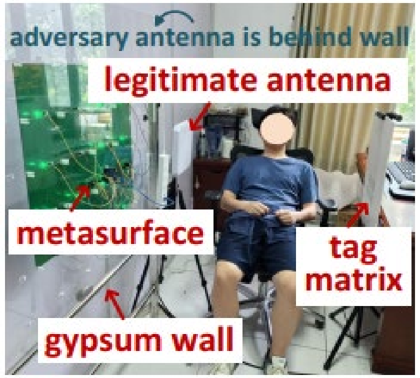
- Impinj R420 reader
- 12 dBi antenna
- 3×2 tag matrix
- RFID Metasurface



Metasurface sketch



Through glass wall



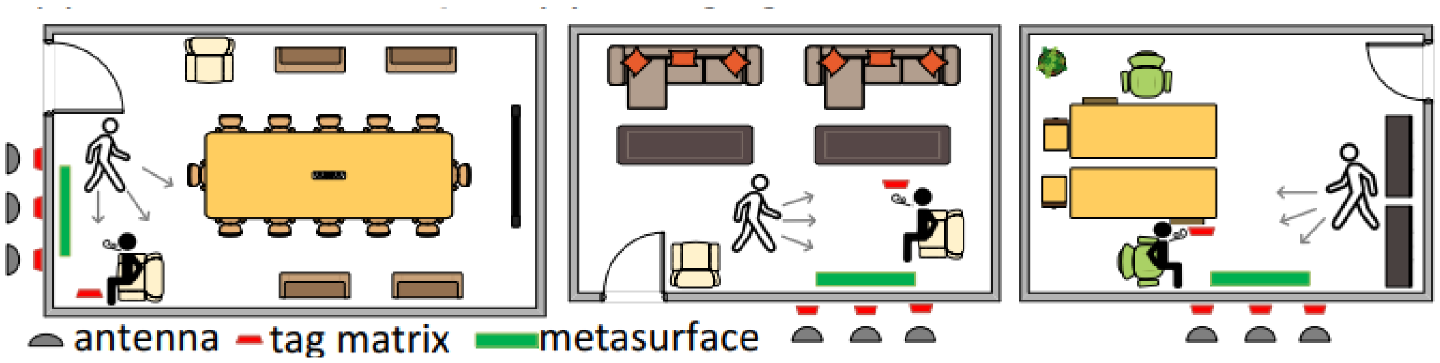
Through gypsum wall

Metrics:

- TP
- FP
- MAE

Scenario:

- gypsum wall
- wooden wall
- glass wall



Walking, breathing as usual

Overall Performance

1) Walking Motion Detection

WALKING MOTION DETECTION PERFORMANCE WITH AND WITHOUT RFNOID IN DIFFERENT ENVIRONMENTS

Method	Environment (1)				Environment (2)				Environment (3)			
	w/o metasurface		**w. metasurface**		w/o metasurface		**w. metasurface**		w/o metasurface		**w. metasurface**	
	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP
Variance threshold	1.00	0.00	0.00	0.00	1.00	0.00	0.013	0.00	1.00	0.00	0.00	0.00
Handcrafted features	1.00	0.02	0.028	0.032	0.98	0.056	0.08	0.007	0.89	0.047	0.09	0.02
Auto-encoder	1.00	0.089	0.039	0.008	1.00	0.028	0.003	0.007	1.00	0.015	0.08	0.00

Motion detection rate decreased to

less than 6%

2) Respiration Rate Estimation

RESPIRATION RATE ESTIMATION WITH AND WITHOUT RFNOID

	Environment (1)		Environment (2)		Environment (3)	
	w/o MS	**w. MS**	w/o MS	**w. MS**	w/o MS	**w. MS**
MAE	0.026	0.087	0.022	0.081	0.019	0.085

Compared with no *RFnoID*

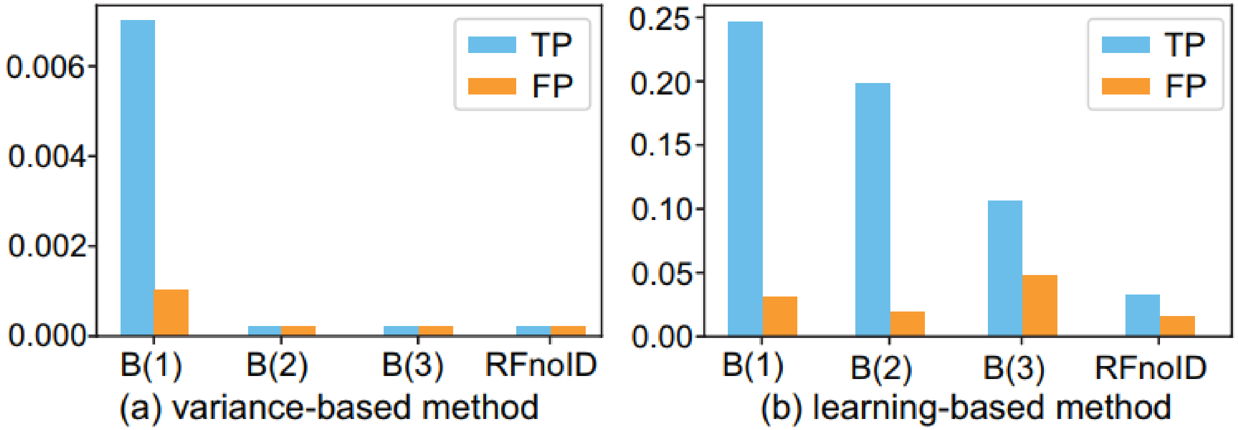
more than 3×

Increase the MAE

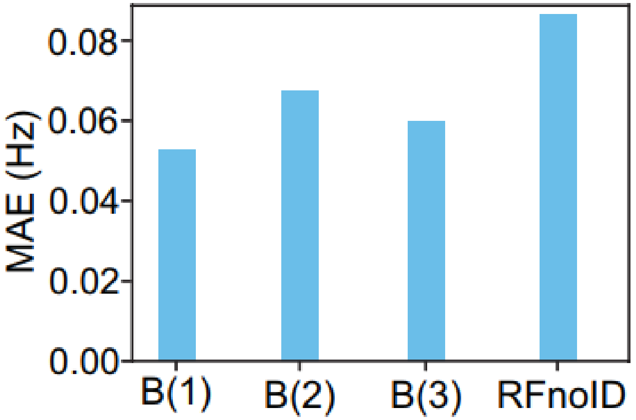
Evaluation Results

Compare with:

- B(1): Base strategy
- B(2): Base strategy + Refinement 1
- B(3): IRShield [1]



Walking motion detection

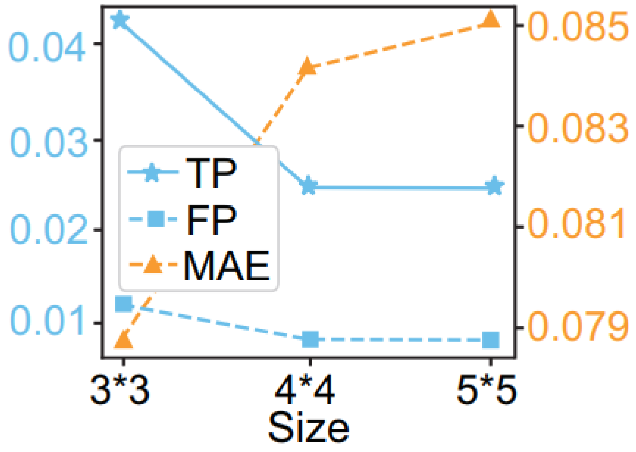


Respiration eavesdropping

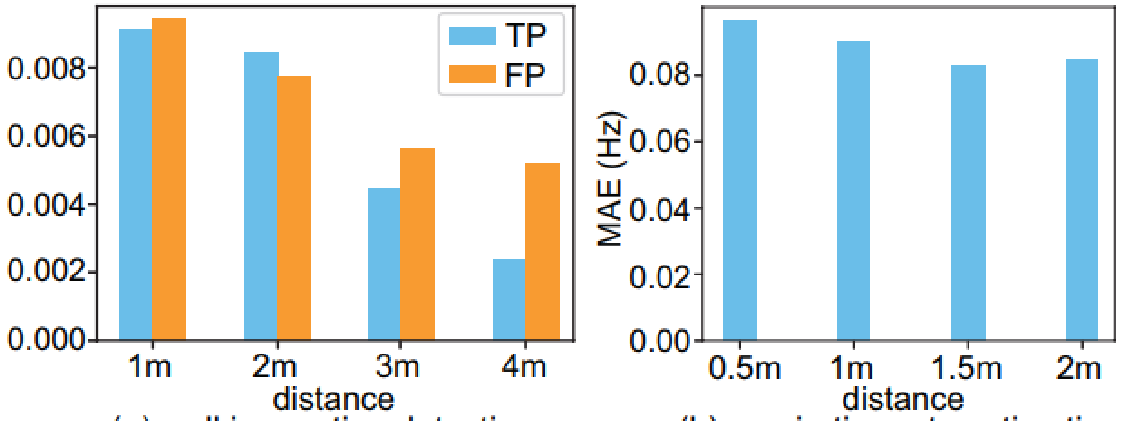
[1] P. Staat, et al. Irshield: A countermeasure against adversarial physical-layer wireless sensing. S&P 2022.

Evaluation Results

Impact of Practical Factors：



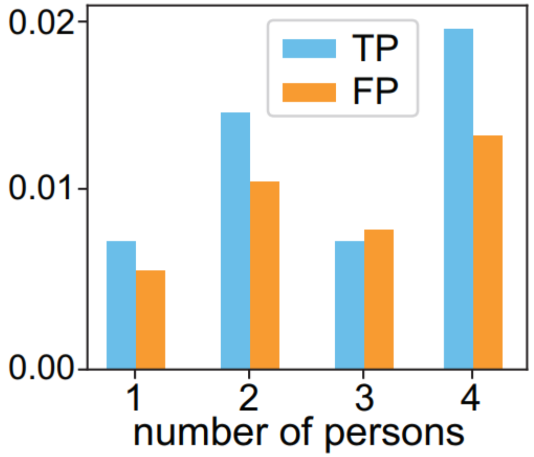
Metasurface size



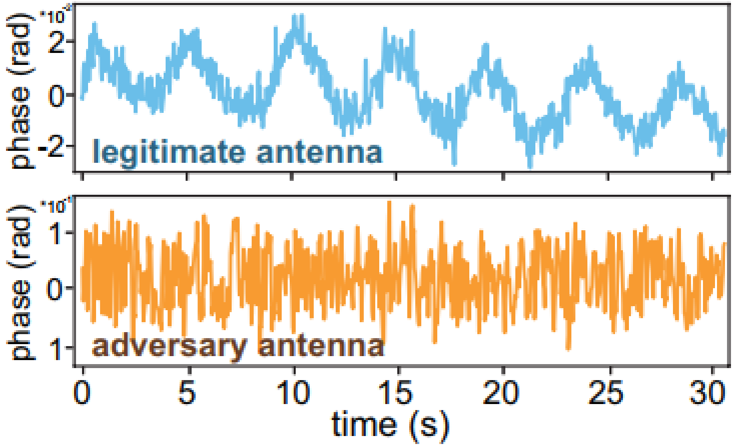
(a) walking motion detection

(b) respiration rate estimation

Distance between human and metasurface



Number of moving persons



Legitimate sensing

Conclusion

-Propose RFnoID, a first metasurface system designed for protecting RFID human motion privacy from adversary sensing.

-Theoretically model and characterize the metasurface's effect on human-reflected signal both temporally and spectrally.

-Design a novel controlling strategy to achieve a balanced obfuscation across both temporal and spectral domains.

-Develop a prototype system and conduct extensive experiments showing significant performance.

Thank you!

Q&A

Yanni Yang, Zheng Shi, Zhenlin An, Runyu Pan,

Yanling Bu, Guoming Zhang, Pengfei Hu, Jiannong Cao