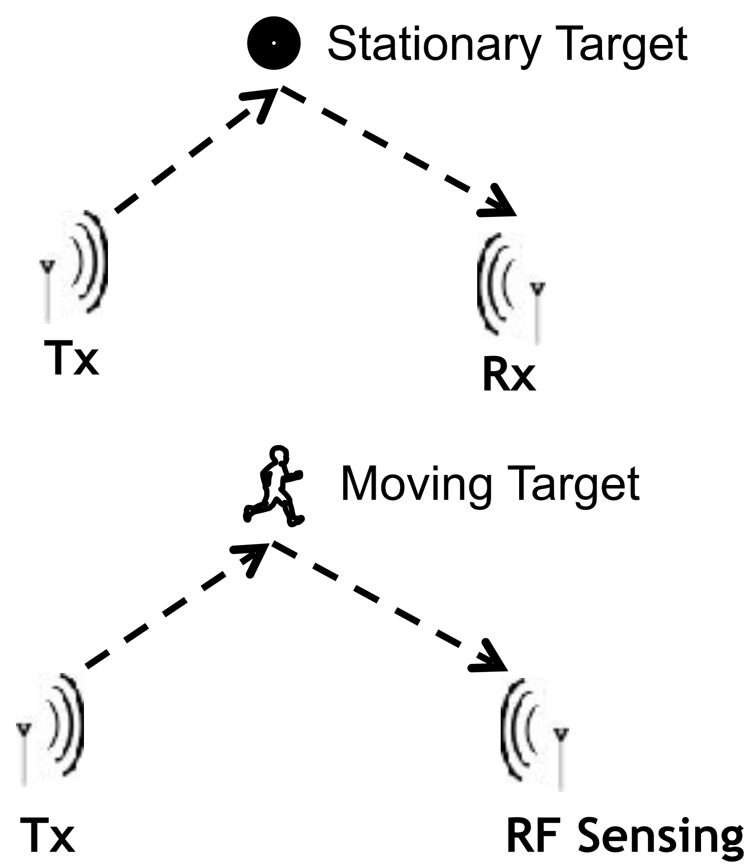
Obfuscating Sensing from Communication Signal [1]

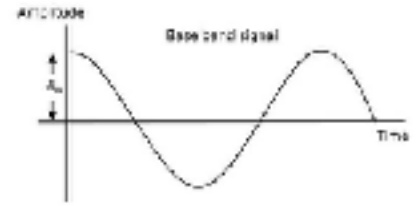
Present by Bowen Song
Based on paper: Y. Qiao et al. *NSDI'16*

BOSTON UNIVERSITY

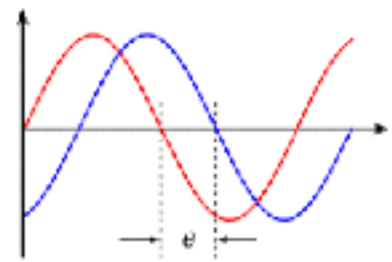
Radar



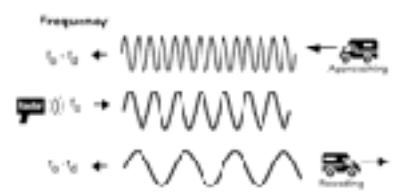
Amplitude



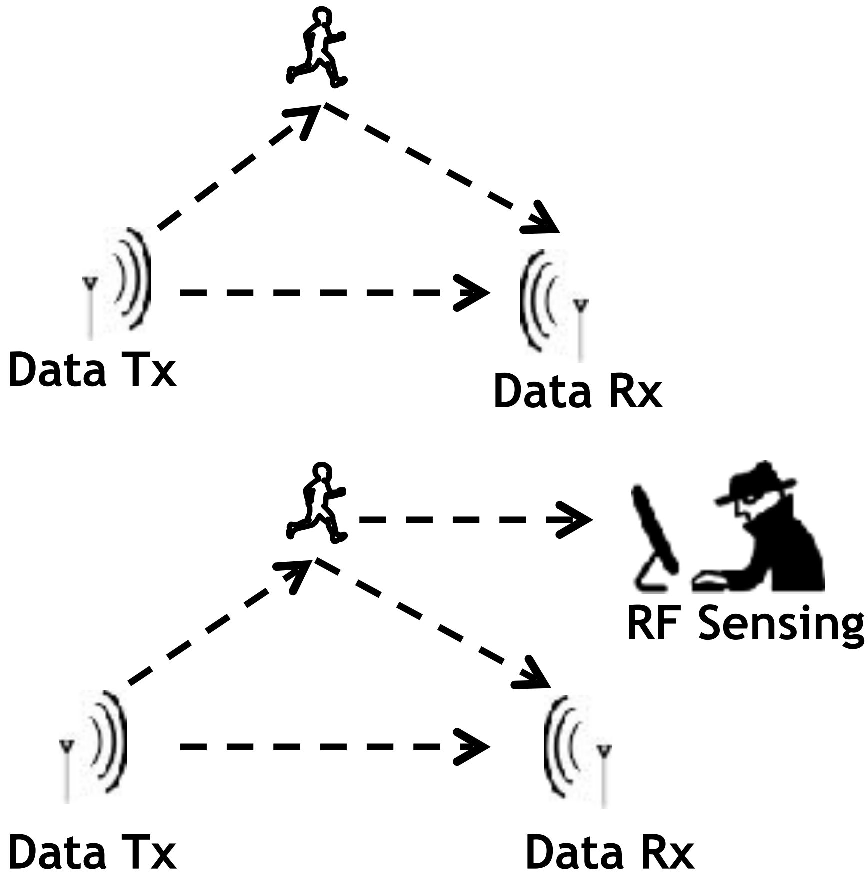
Phase shift



Doppler shift



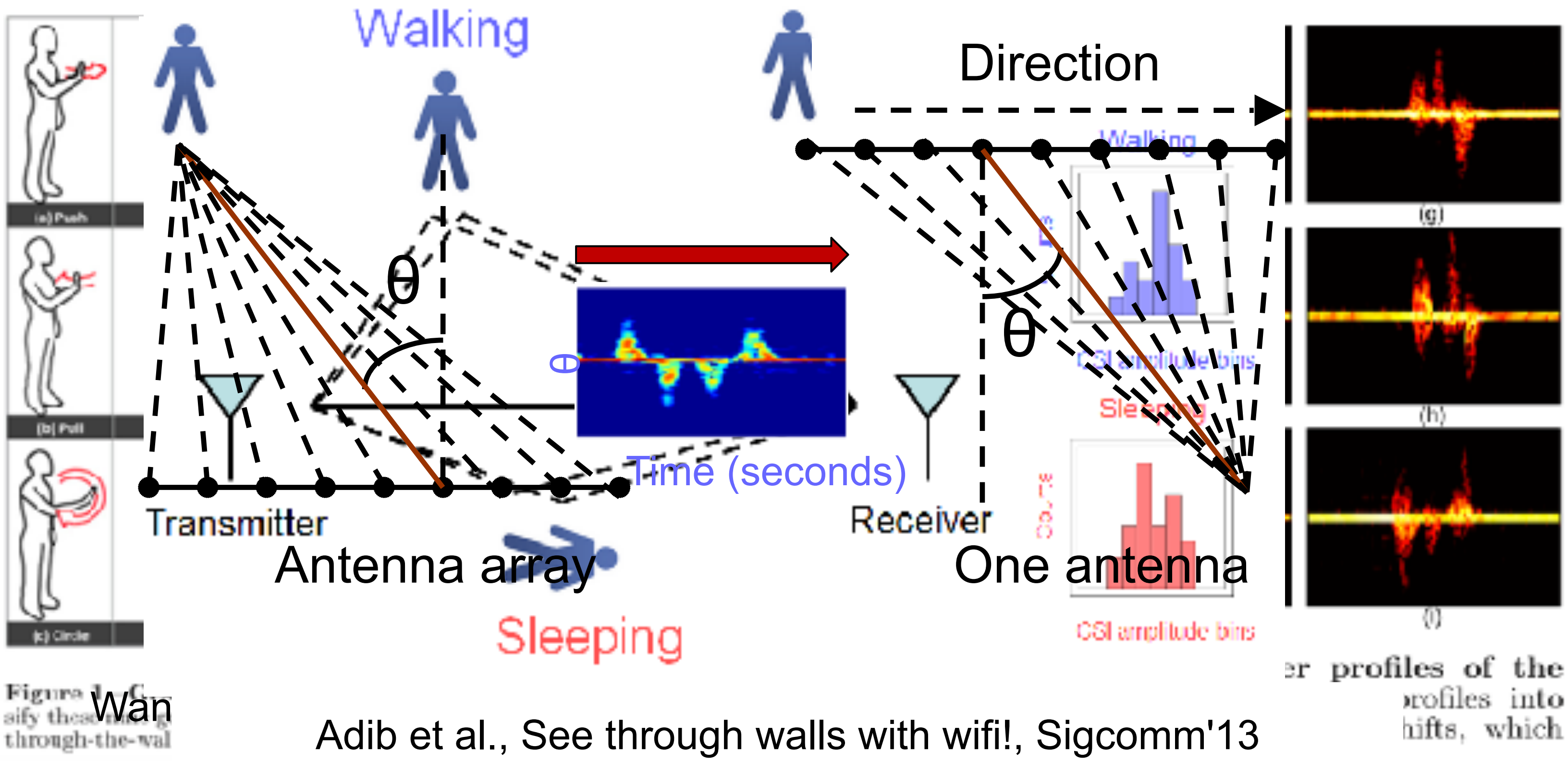
Sensing - Wifi - channel status information (CSI)



- Broadcasting nature of wireless communication

- Attackers does not need to decode message

Why do we care?
- Passive sensing: Hard to discover
- Cipher for CSI without decoding messages



Adib et al., See through walls with wifi!, Sigcomm'13

Keystroke Inference Framework

- Finger motion

(a) IKI Model (b) OKI Model

Figure 1: WiFi-based Keystroke Inference Models

Presentation Outline

1. Problem Definition and Challenges
2. Contribution
3. Countermeasures
    A. Superposition
    B. Hiding Doppler Shift
4. Allowing Legitimate Sensing
5. Performance and Limitation
6. Conclusion and Future Work
7. Reference

1. Problem Statement & Challenges

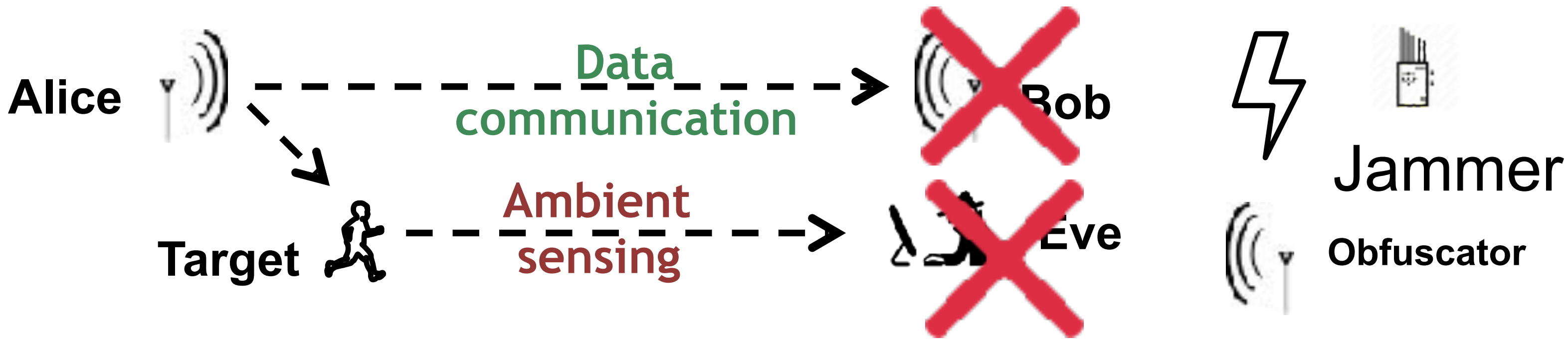
- Wifi Signal carry CSI

- Protect privacy from Wifi sensing

- Obfuscating all ambient sensing -> unknown sensing technique

- No effect on data communication -> fitting all data transmission protocols

2. Contribution



- Stronger signal
- Confusing CSI signature (a, Δf, $\Delta\phi$)
- Cover up (Obfuscate) the target signature

3. Transmitted Signal

$$r(t) = a \times s(t) \times e^{j2\pi(f_c+\Delta f)(t+\Delta t)}$$

$s(t)$: transmitted signal
$r(t)$: received signal
f_c: carrier frequency
a : amplitude
Δf: Doppler shift
$2\pi f_c \Delta t$: phase

3A. Solution Concept - Superposition

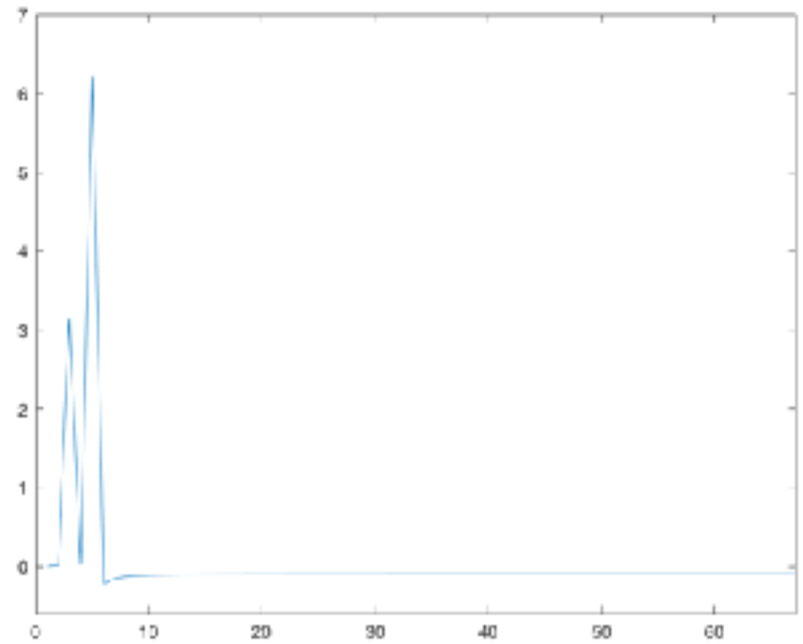
$$r(t) = a_1 s(t) e^{j2\pi(f_c+\Delta f_1)(t+\Delta t_1)} + a_2 s(t) e^{j2\pi(f_c+\Delta f_2)(t+\Delta t_2)}$$

Amplitude gain a

Phase Δt

Doppler shift Δf

Ox- Obfuscator Signal



3B. Doppler Shift - Frequency Domain

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

- Human motion: ± 20Hz Doppler shifts (2.4GHz)

- Δf continuous t seconds to show 1/t Hz Doppler shift

- Changes at least about every 0.1s

Obfuscating All 3 Sensing Techniques

- Amplitude, Phase, and Doppler shift

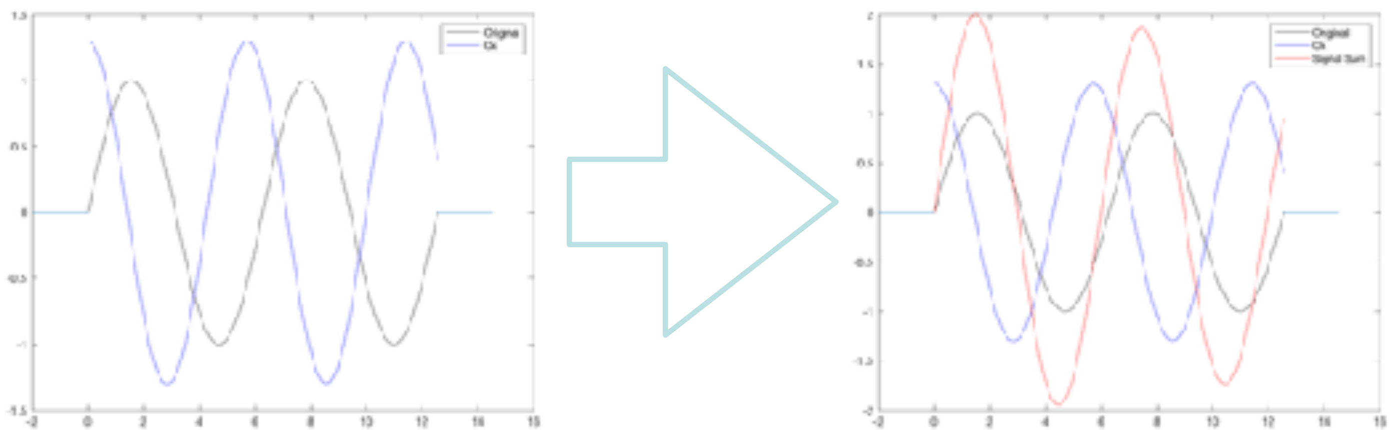
Preserving Communication Throughput

- Don’t Change of $\{a, \Delta f, \Delta\varphi\}$ in the middle of packet transmission

3. Countermeasure - PhyCloak

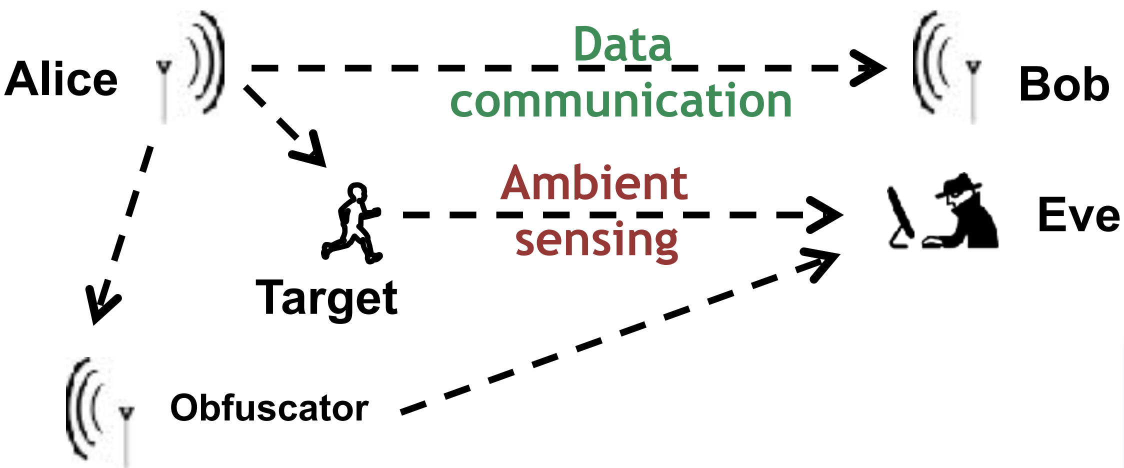
- Learning: learn signal

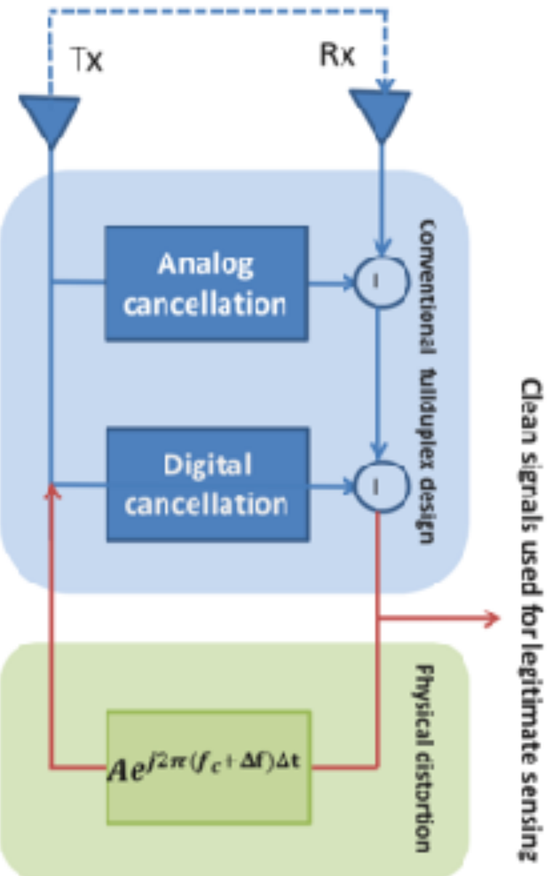
- Forwarding: applies distortions $\{a, \Delta f, \Delta\phi\}$



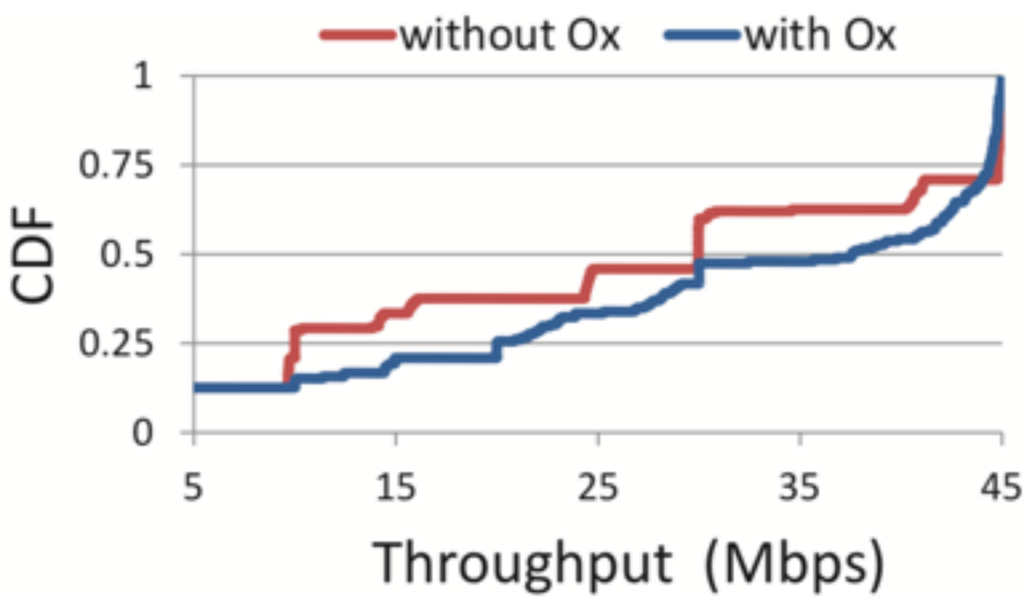
- Changes $\{a, \Delta f, \Delta\phi\}$: channel is **free** and **0.1s+**. (randomly changing $\{a, \Delta f, \Delta\phi\}$ on a per packet basis)

4. Allowing Legitimate Sensing

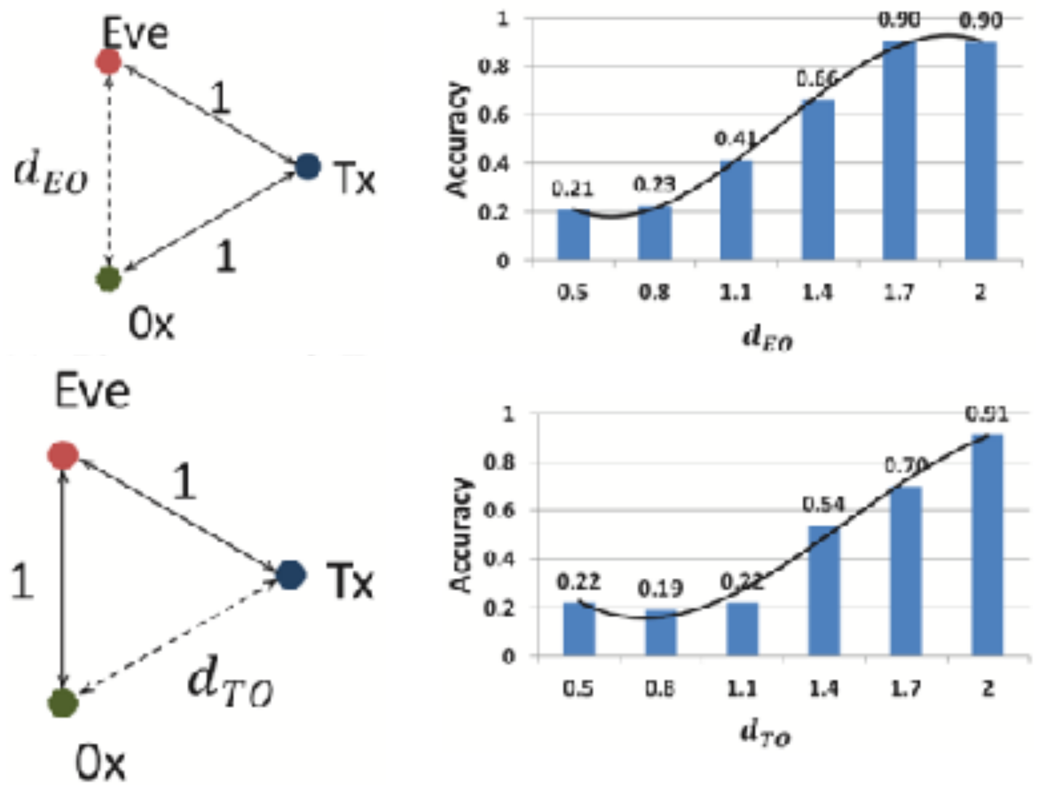




5. Performance - Throughput



5. Performance - Positioning



(a) Placement of Tx, Ox and Eve with all three channels LoS.

(b) Classification accuracy of Eve in the presence of PhyCloak increases as d_{TO} increases

5. Limitations

- High cost full-duplex hardware

- Single antenna sensing obfuscation

- Designed merely to obfuscate human activity

- Fails against multiple transmitting sources

- Signal needs to be stronger than the source

6. Conclusion:

- One of the first protection systems against comm-based sensing
- Obfuscate illegitimate single-antenna sensing
- Not degrading data throughput
- Allowing legitimate sensing
- Implemented on SDR platform

6. Future work:

- Other band than 2.4G or human activity
- Obfuscate multi-antenna sensors
- Cooperation among multiple obfuscators
- Build-in to Wifi

7. References

[1] Qiao, Yue, et al. "PhyCloak: Obfuscating Sensing from Communication Signals." *USENIX Annual Technical Conference*. 2016.

[2] Li, Mengyuan, et al. "When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals." *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016.

[3] Tan, Bo, et al. "Exploiting WiFi Channel State Information for Residential Healthcare Informatics." *IEEE Communications Magazine* 56.5 (2018): 130-137.