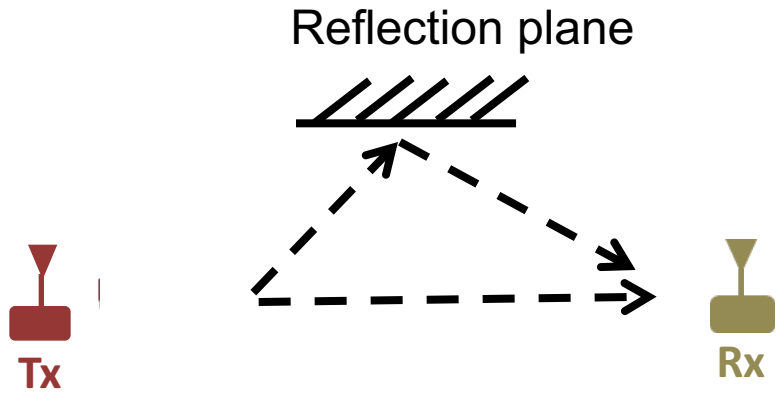
PhyCloak: Obfuscating Sensing from Communication Signals

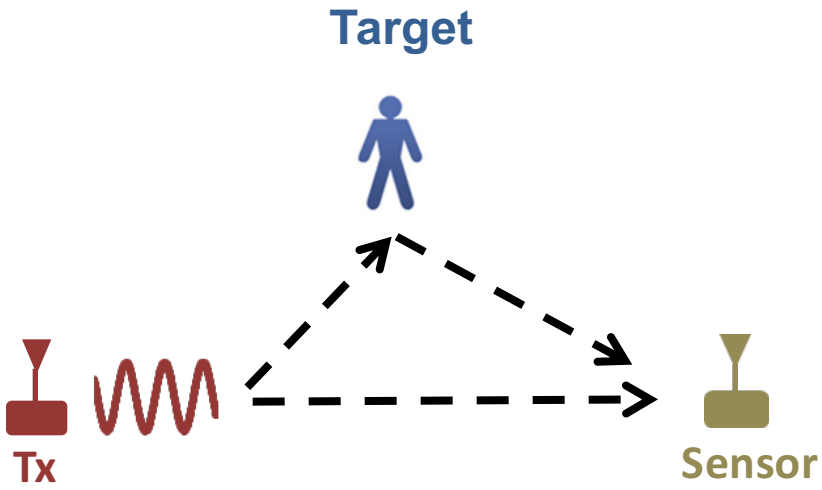
Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan and Anish Arora

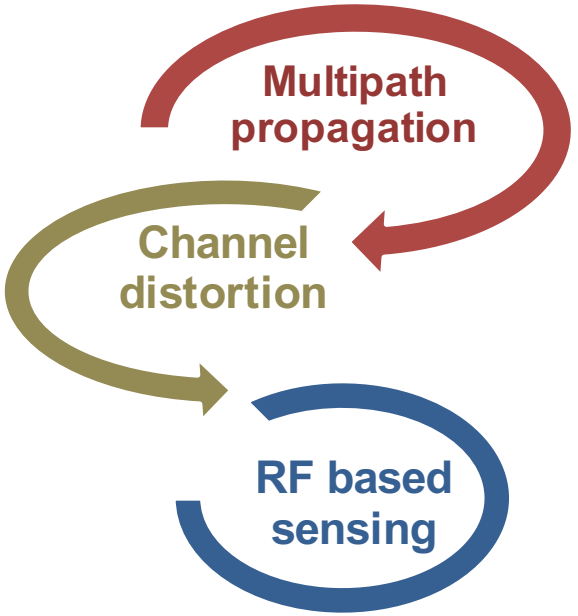
Department of Computer Science and Engineering



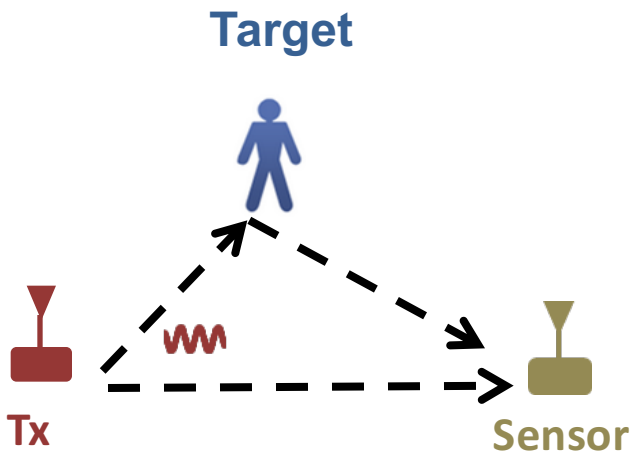
RF Based Sensing



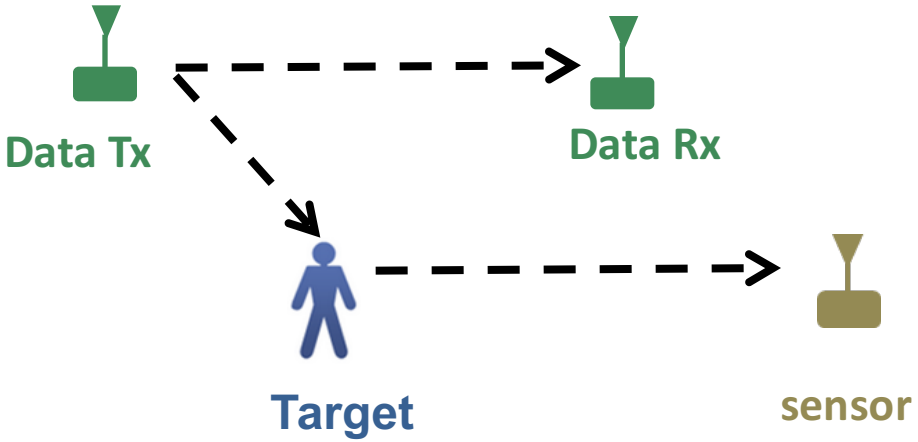




A New Threat

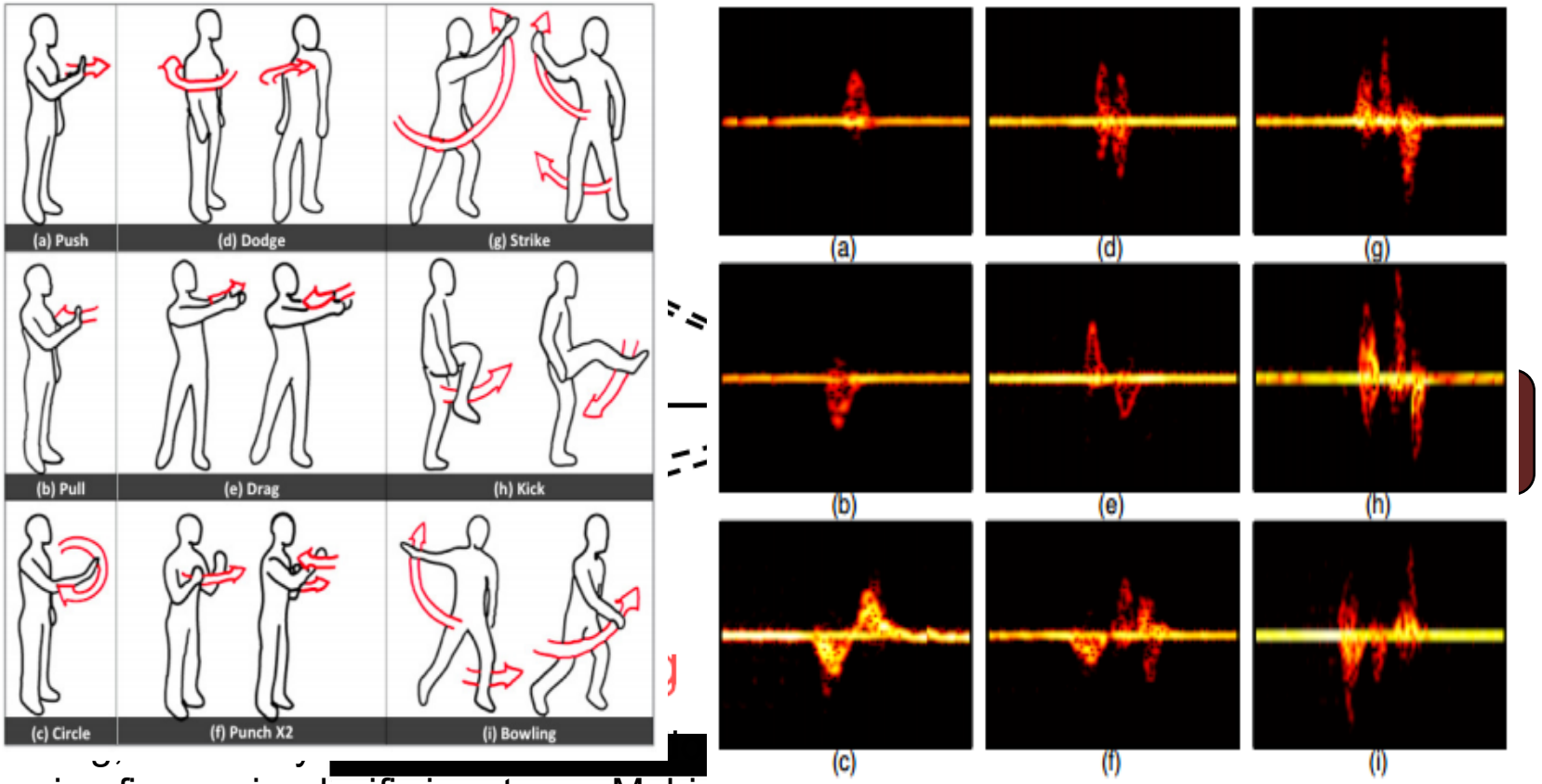


Traditional RF sensing



Comm-based RF sensing

Comm-based Sensing: Examples

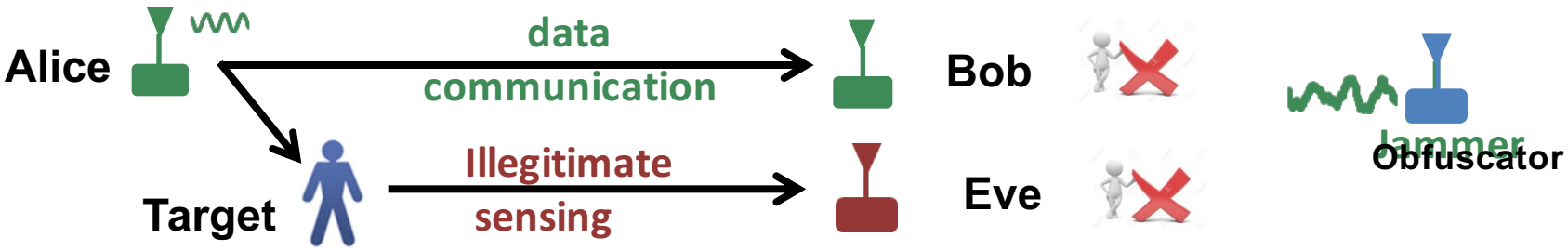


using fine-grained wifi signatures, Mobicom'14

Pu et al., whole home gesture recognition using wireless signals, Mobicom'13

see-through capabilities using laser and wireless channel measurements, Sensors Journal, IEEE, 2014.

Problem Statement



A stand-alone **black-box** obfuscator:

- Obfuscate **all** illegitimate single-antenna sensors
  - No knowledge of the sensing technique
- Not degrade **any** wireless data receivers
  - No knowledge of the data transmission protocol

Requirements

1. Obfuscate all sensors without knowing their techniques?

2. Do not degrade data links no matter what transmission protocols are being used?

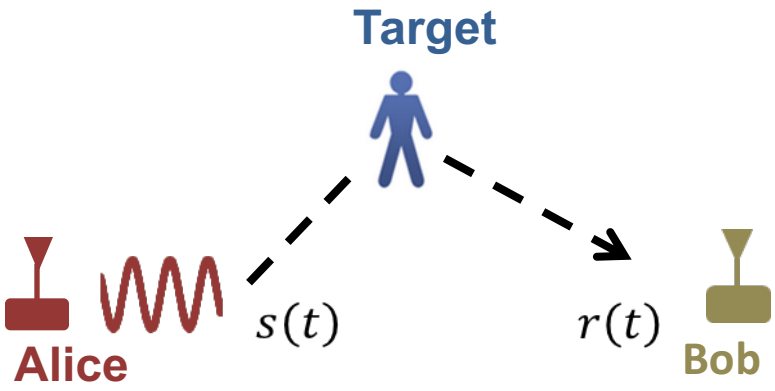
Three Degrees of Freedom

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

$s(t)$: transmitted signal
$r(t)$: received signal

Obfuscating the 3 DoFs is sufficient!

Δf: Doppler shift
$2\pi f_c \Delta t$: phase

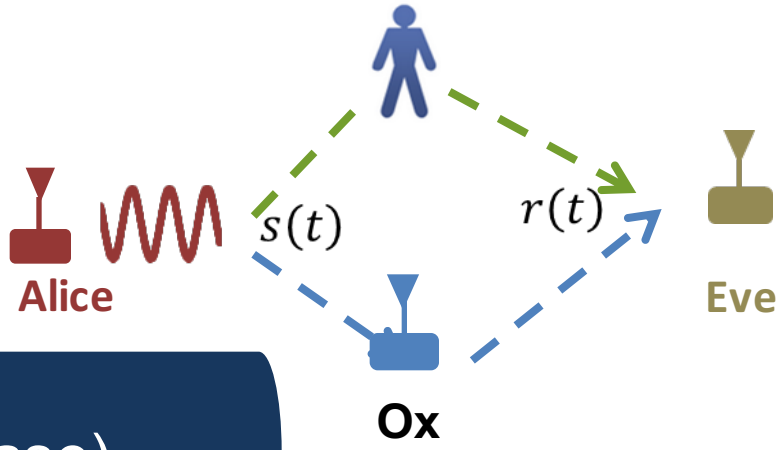


Effect of Superposition

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

passive reflected copy

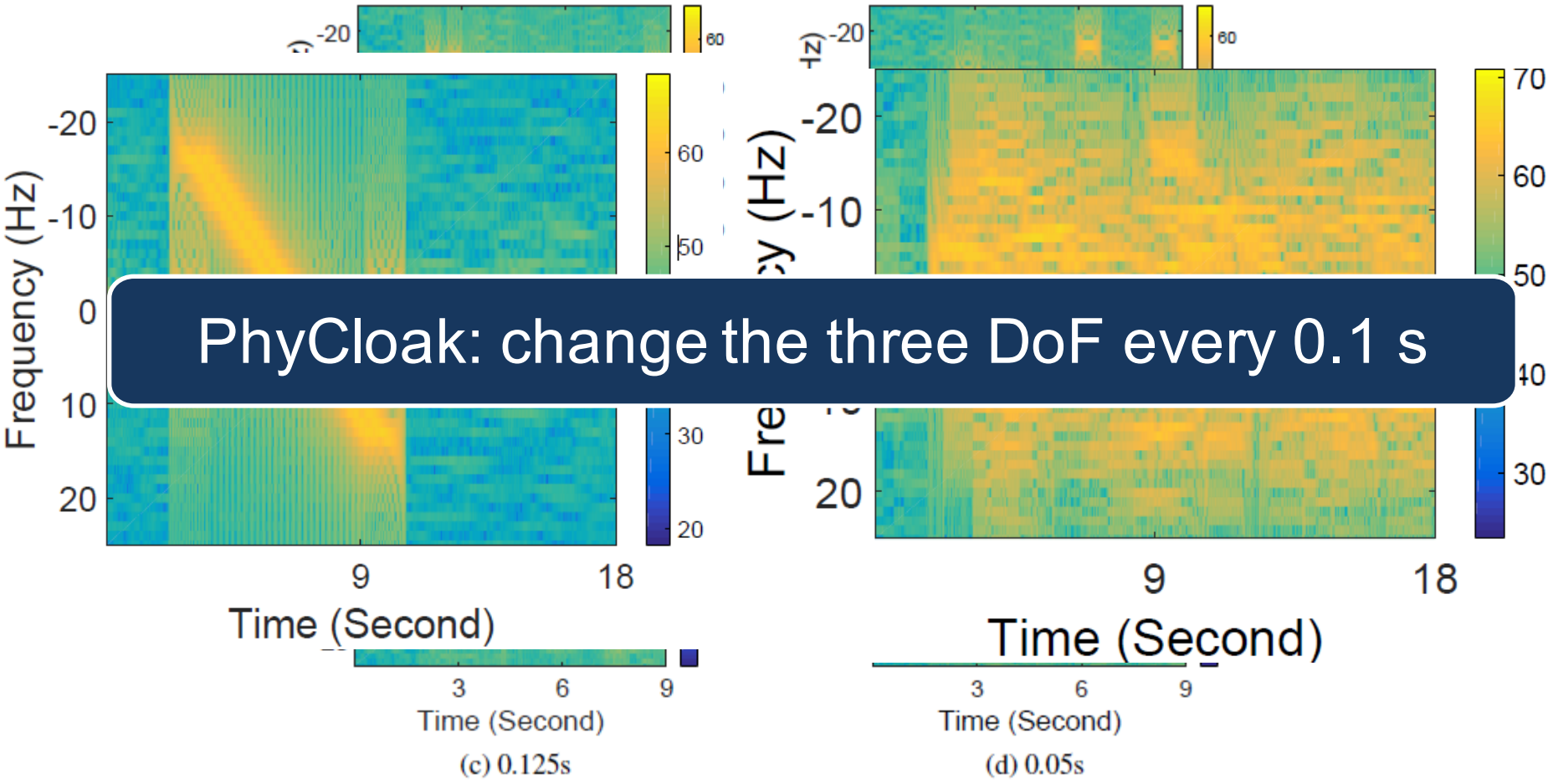
actively reflected copy



- Time domain (amplitude and phase)
  - Instantaneously obfuscated
- Frequency domain (Doppler shift)
  - Still distinguishable after superposition

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

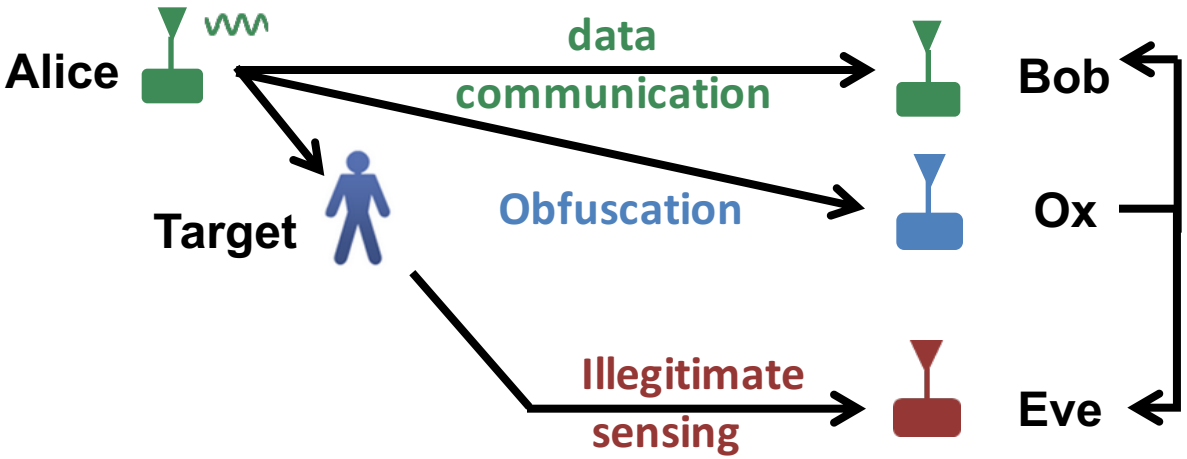
How Often to Change



PhyCloak: change the three DoF every 0.1 s

The granularity of the spectralgrams decreases as the Doppler shifts change from every 1s to every 0.05s

Full-duplex Operation



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

Instantaneously forward the received copy

Full-duplex forwarding: transmit and receive simultaneously

Eve: obfuscator

Bob: relay

Requirements

1. Obfuscate all sensor without knowing their techniques?

2. Do not degrade data links no matter what transmission protocols are being used?

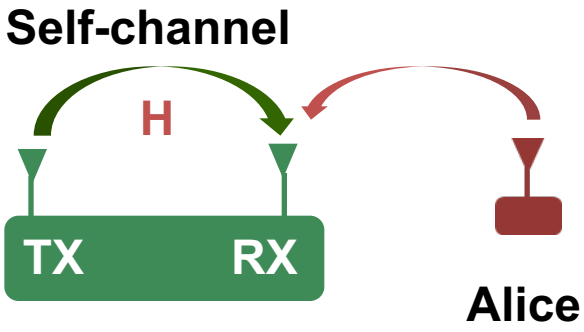
Self-channel Estimation

Self-channel training takes air time

External data transmission

Every 100 ms!

A novel scheme: parallel self-channel training and external data transmission



Ox

received

Self-interference cancellation: R - S*H

self-channel estimate

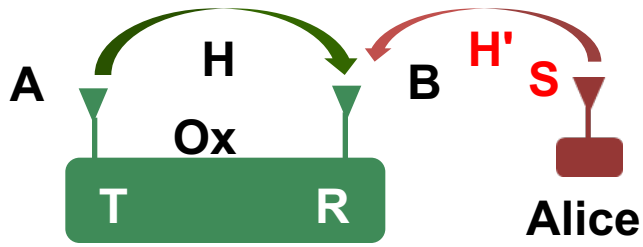
transmitted

Self-channel Estimation

Training without external interference

B = A x H

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



Basic idea: Oversample to make external interference constant over several slots

B = A x H + S C x H'

$$\begin{Bmatrix} b_0 \\ b_1 \\ \dots \\ b_m \end{Bmatrix} = \begin{Bmatrix} a_0 & \dots & a_{-m} \\ a_1 & \dots & a_{-m+1} \\ \dots & \dots & \dots \\ a_m & \dots & a_0 \end{Bmatrix} \times \begin{Bmatrix} h_0 \\ h_1 \\ \dots \\ h_m \end{Bmatrix} + \begin{Bmatrix} s_0 \times (h'_0 + \dots + h'_m) \\ s_0 \times (h'_0 + \dots + h'_m) \\ \dots \\ s_0 \times (h'_0 + \dots + h'_m) \end{Bmatrix}$$

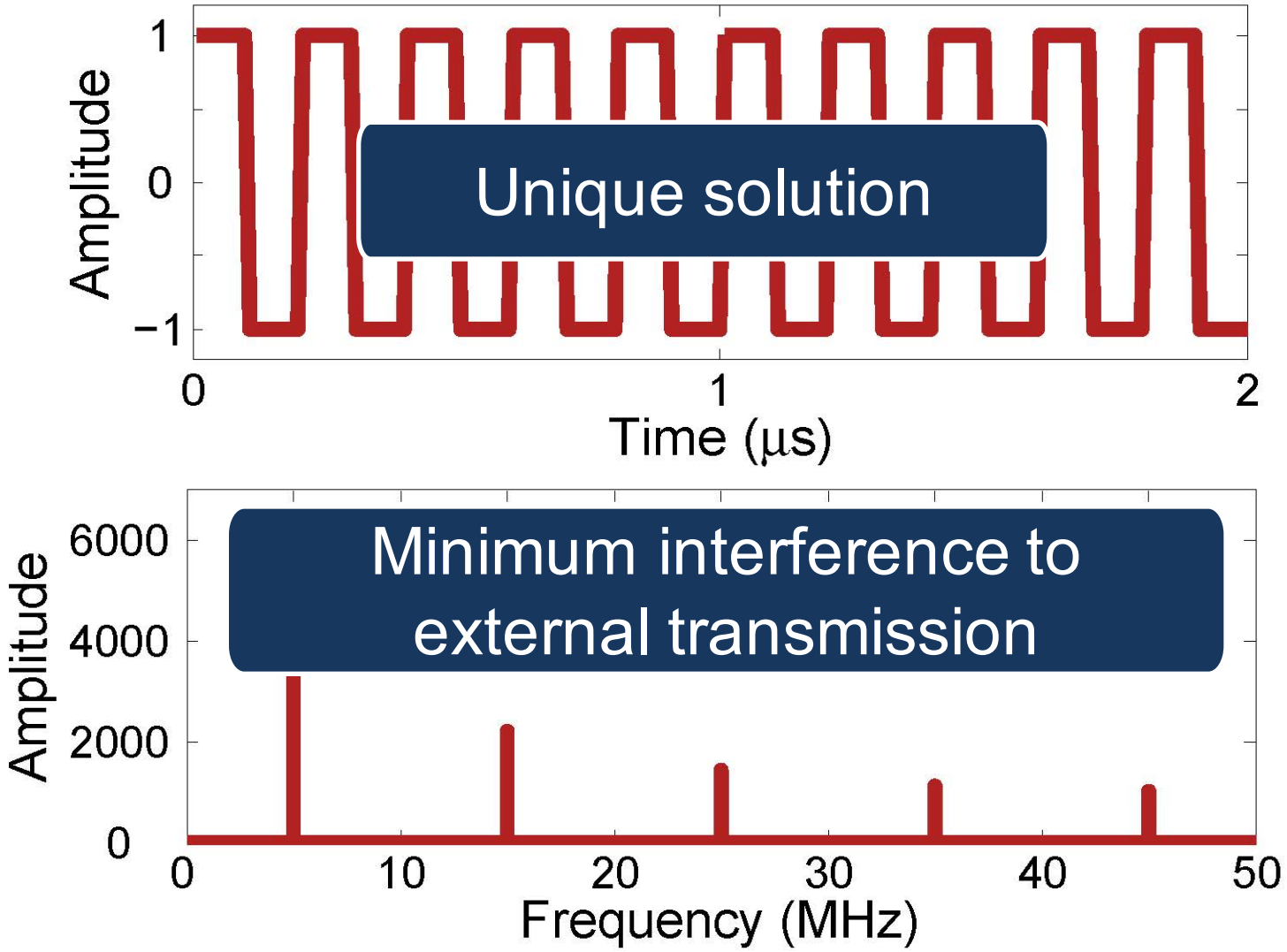
Self-channel Estimation

B = A x H + C

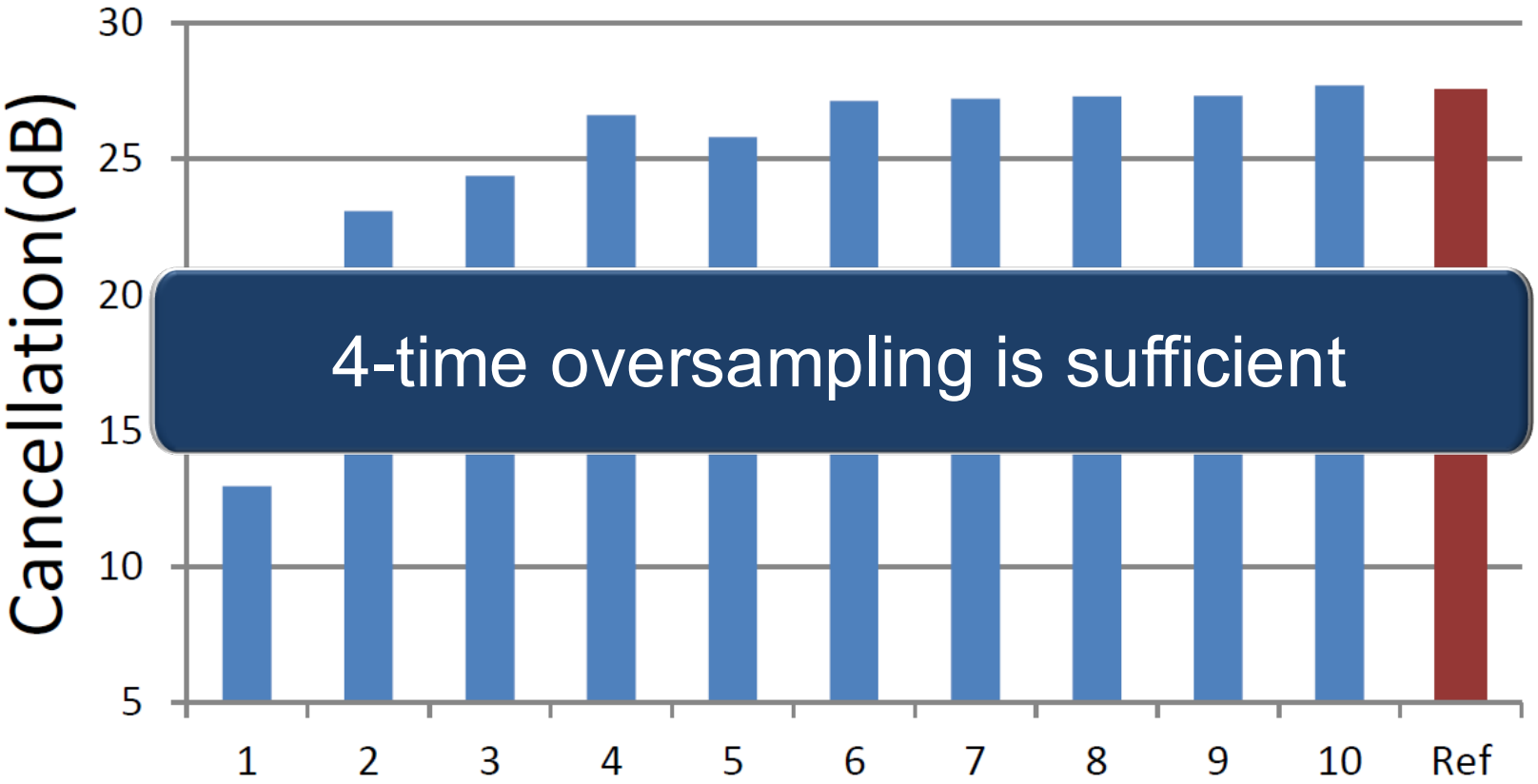
$$\begin{Bmatrix} b_0 \\ b_1 \\ \dots \\ b_m \end{Bmatrix} = \begin{Bmatrix} a_0 & \dots & a_{-m} \\ a_1 & \dots & a_{-m+1} \\ \dots & \dots & \dots \\ a_m & \dots & a_0 \end{Bmatrix} \times \begin{Bmatrix} h_0 \\ h_1 \\ \dots \\ h_m \end{Bmatrix} + \begin{Bmatrix} s_0 \times (h'_0 + \dots + h'_m) \\ s_0 \times (h'_0 + \dots + h'_m) \\ \dots \\ s_0 \times (h'_0 + \dots + h'_m) \end{Bmatrix}$$

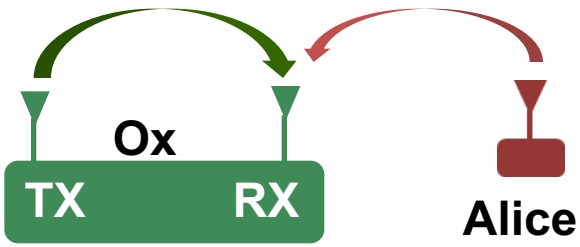
$$\begin{Bmatrix} b_1 - b_0 \\ b_2 - b_1 \\ \dots \\ b_m - b_{m-1} \end{Bmatrix} = \begin{Bmatrix} a_1 - a_0 & \dots & a_{-m+1} - a_{-m} \\ a_2 - a_1 & \dots & a_{-m+2} - a_{-m+1} \\ \dots & \dots & \dots \\ a_m - a_m & \dots & a_1 - a_0 \end{Bmatrix} \times \begin{Bmatrix} h_0 \\ h_1 \\ \dots \\ h_m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

A Special Training Sequence

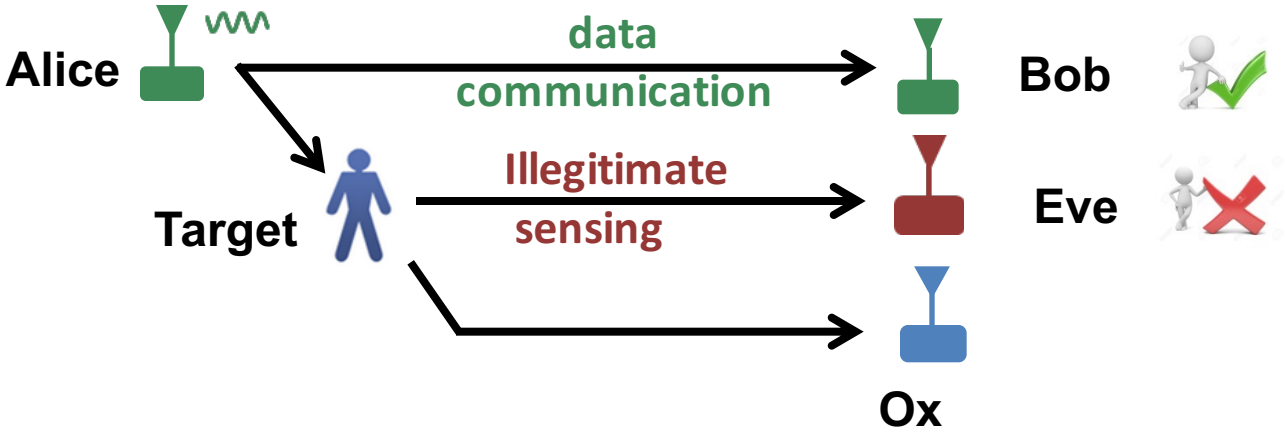


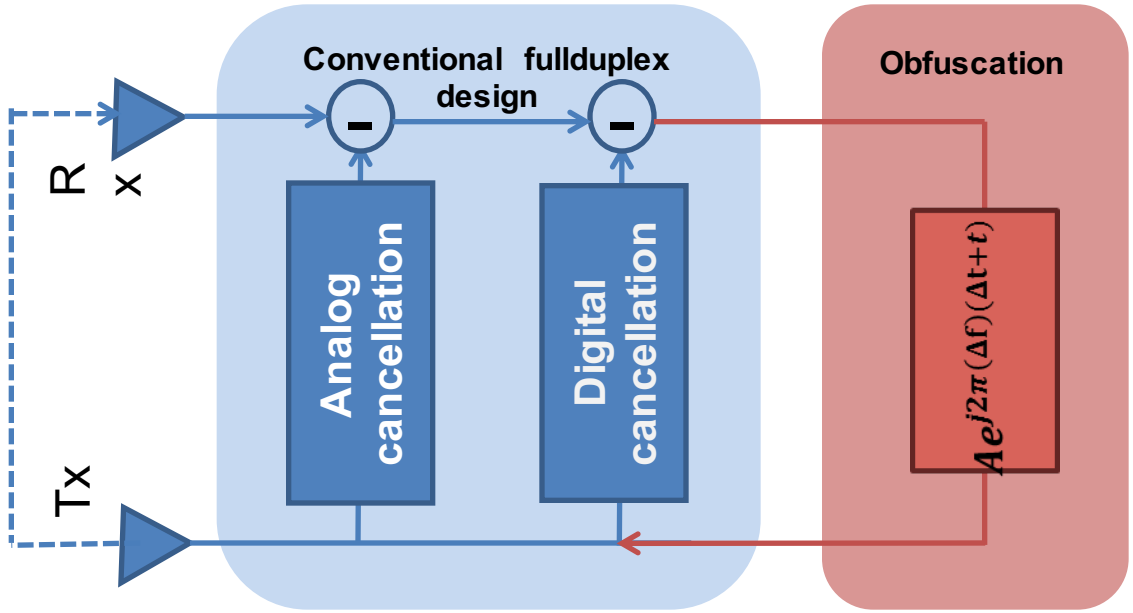
Cancellation Performance





PhyCloak


Alice
data
communication
Bob
Target
Illegitimate
sensing
Eve
Ox


Conventional fullduplex
design
Obfuscation
R
x
Tx
Analog
cancellation
Digital
cancellation
$Ae^{j2\pi(\Delta f)(\Delta t+t)}$

Evaluation

SDR Platform: NI Pxie 1082

PhyCloak

- 2.4GHz
- 50MHz

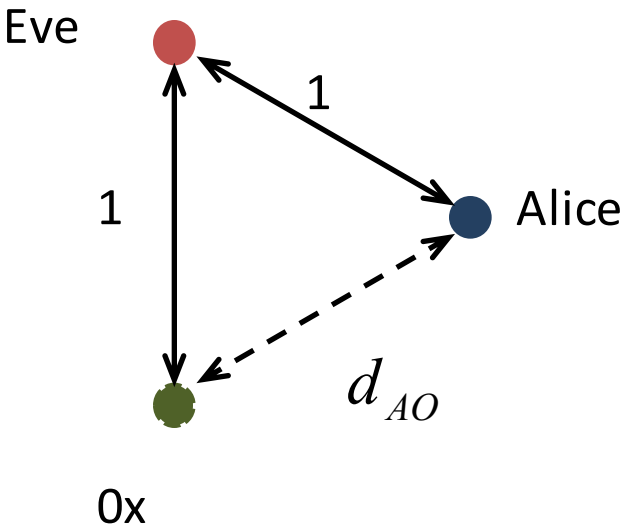
Data Tx/Rx

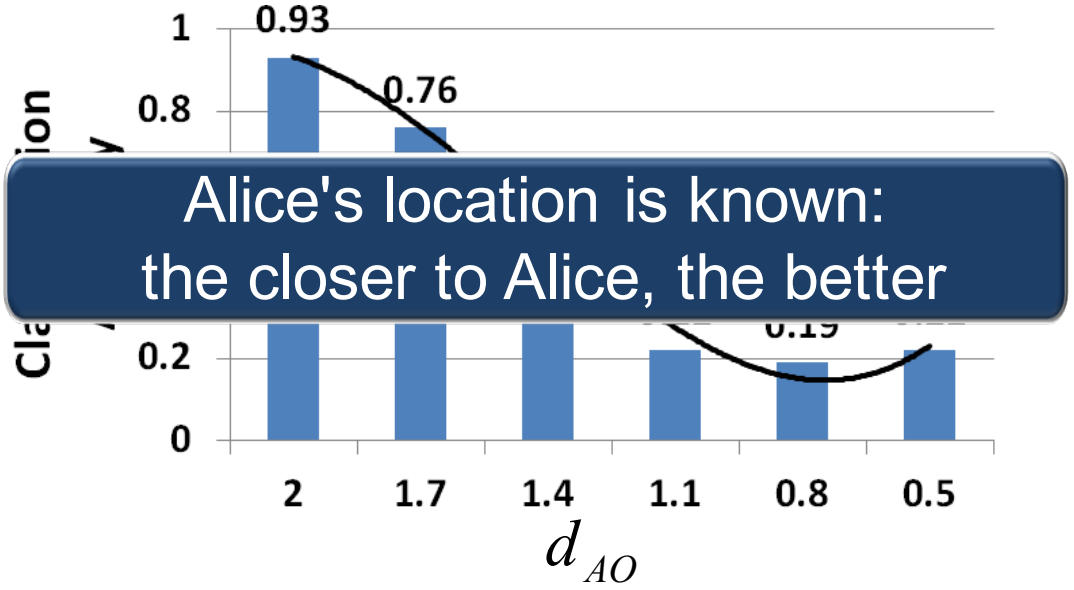
- 802.11g
- 2.4GHz
- 16.25MHz

WiSee Sensor

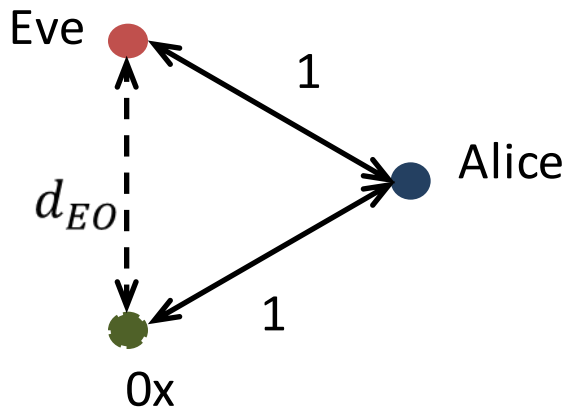
- Gesture recognition
- Doppler shift

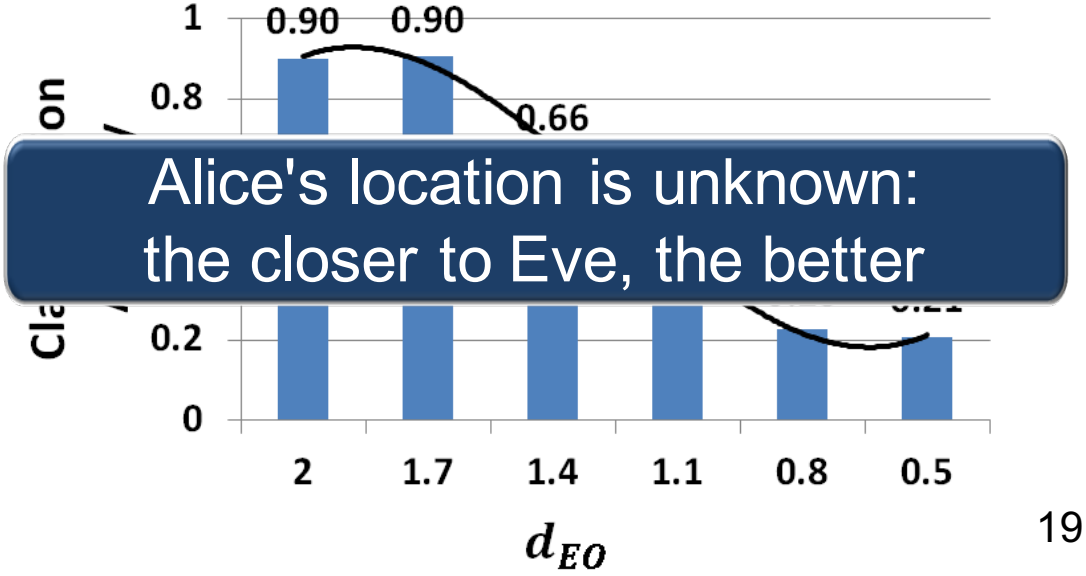
Illegitimate Sensing





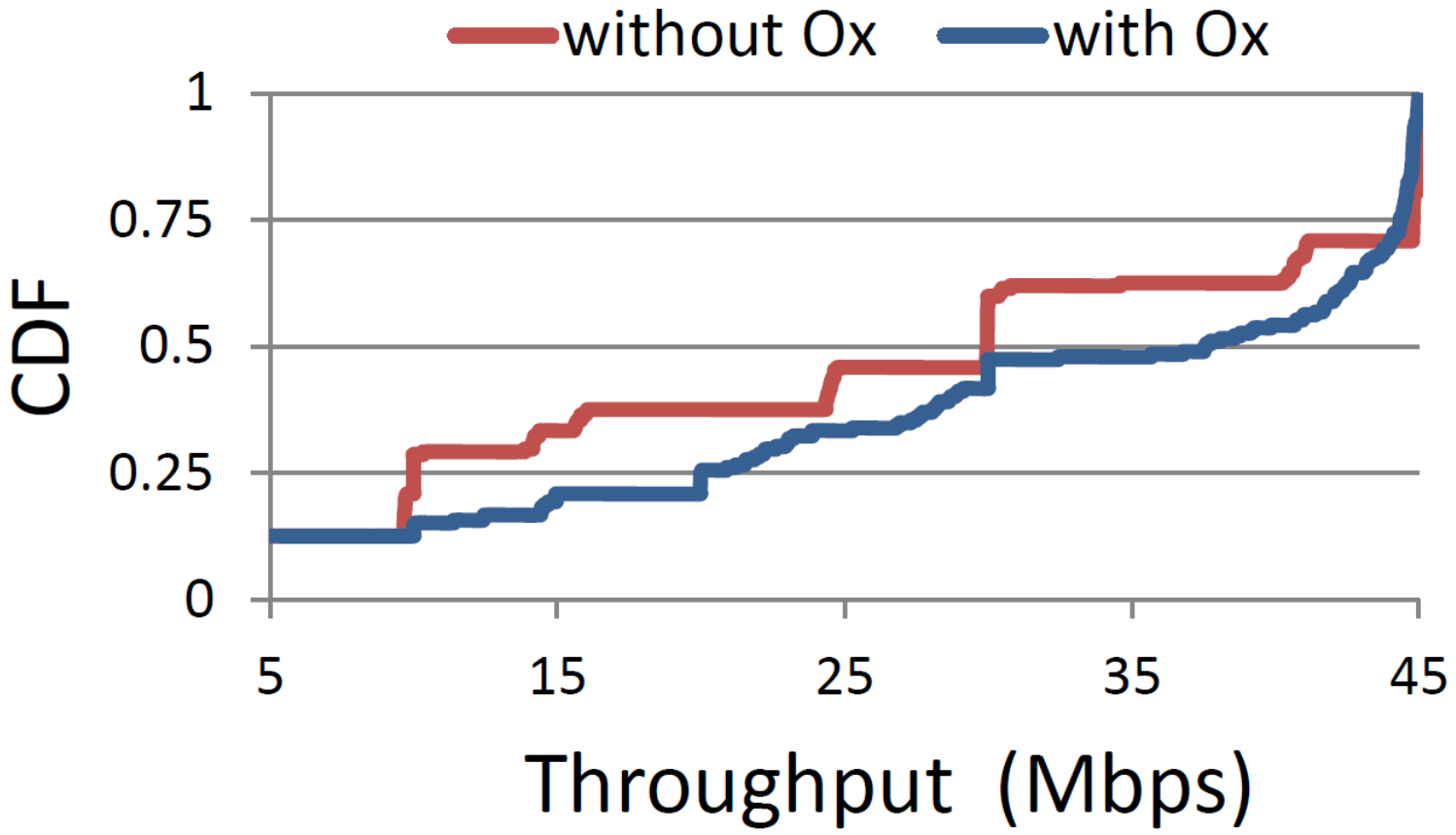
Alice's location is known:
the closer to Alice, the better





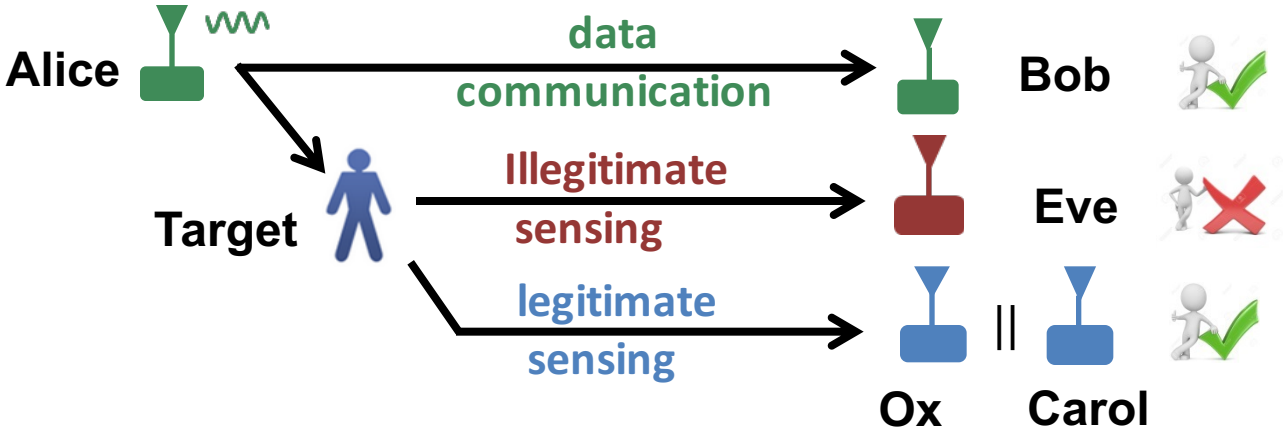
Alice's location is unknown:
the closer to Eve, the better

Throughput

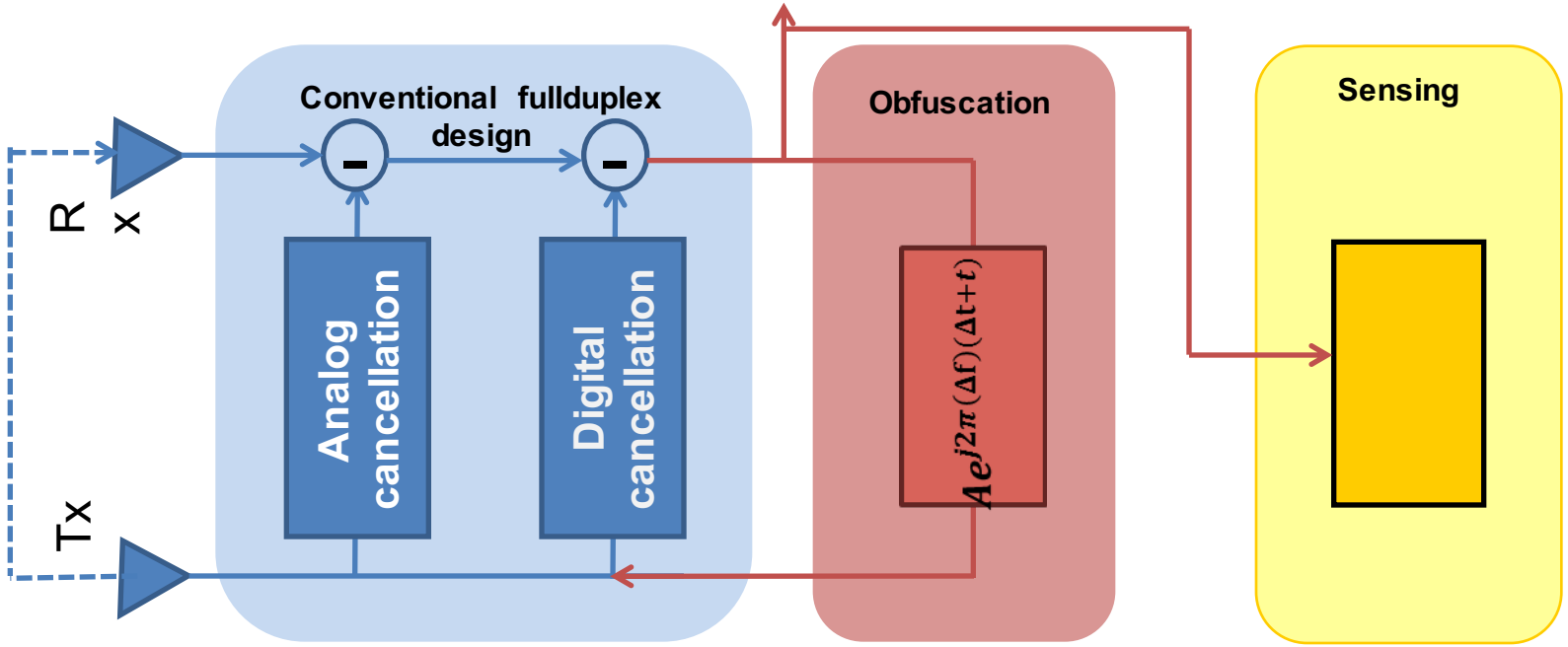


The average throughput increases with the help of PhyCloak

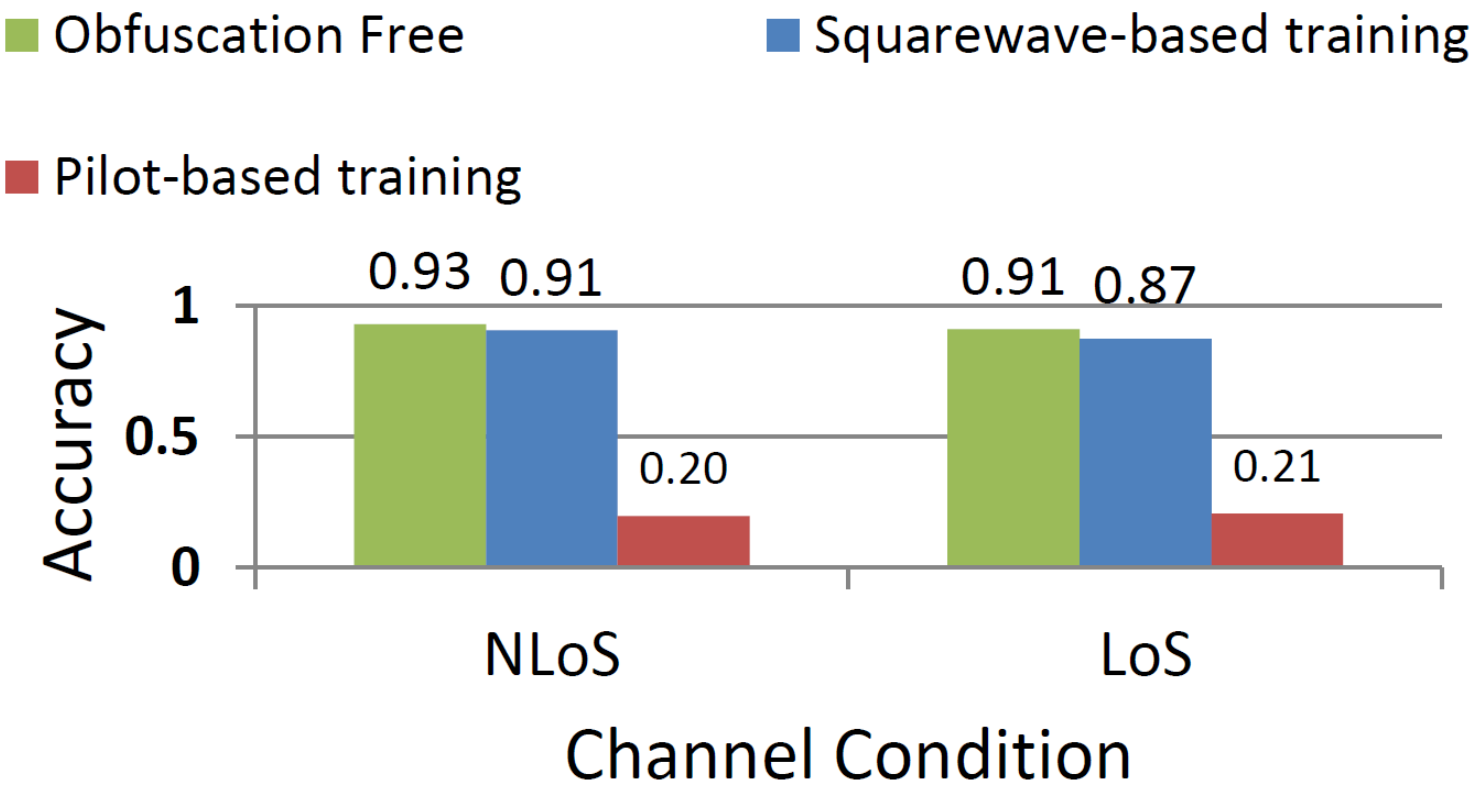
Legitimate Sensing



Clean signals used for legitimate sensing

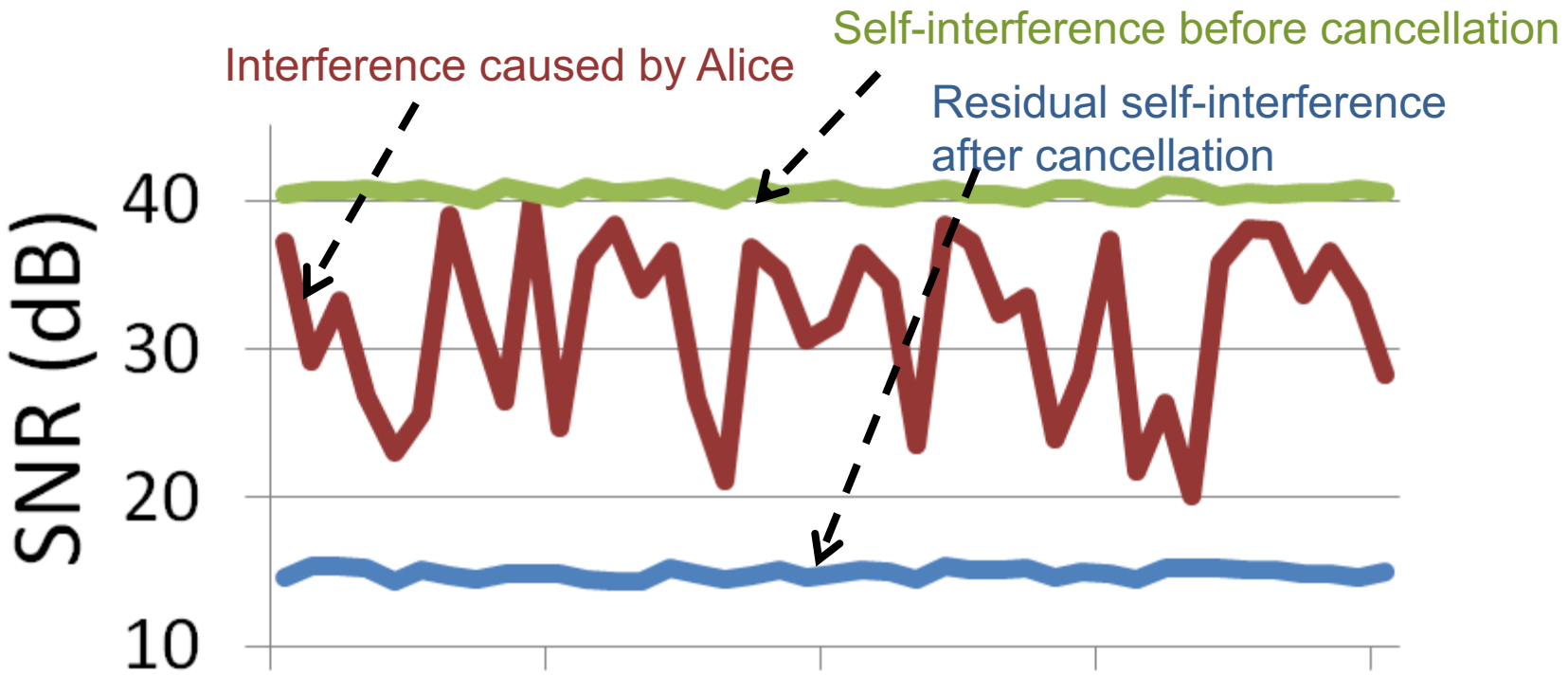


Legitimate Sensing



Squarewave based training preserves legitimate sensing

Cancellation under Varying Interference



External interference variation does not affect cancellation performance



Conclusions and Future Work

Conclusion:

- **The first protection system against comm-based sensing**
- **Obfuscate illegitimate single-antenna sensing, not degrade data throughput, and preserve legitimate sensing**
- **Implementation on SDR platform**

Future work:

- **Obfuscate multi-antenna sensors using multi antenna obfuscators?**
- **Coverage provided by obfuscators?**
- **Cooperation among multiple obfuscators?**

Q&A

Thanks