Ghostbuster: Detecting the Presence of Hidden Eavesdroppers

Anadi Chaman, Jiaming Wang, Jiachen Sun

Romit Roy Choudhury, Haitham Hassanieh

UIUC

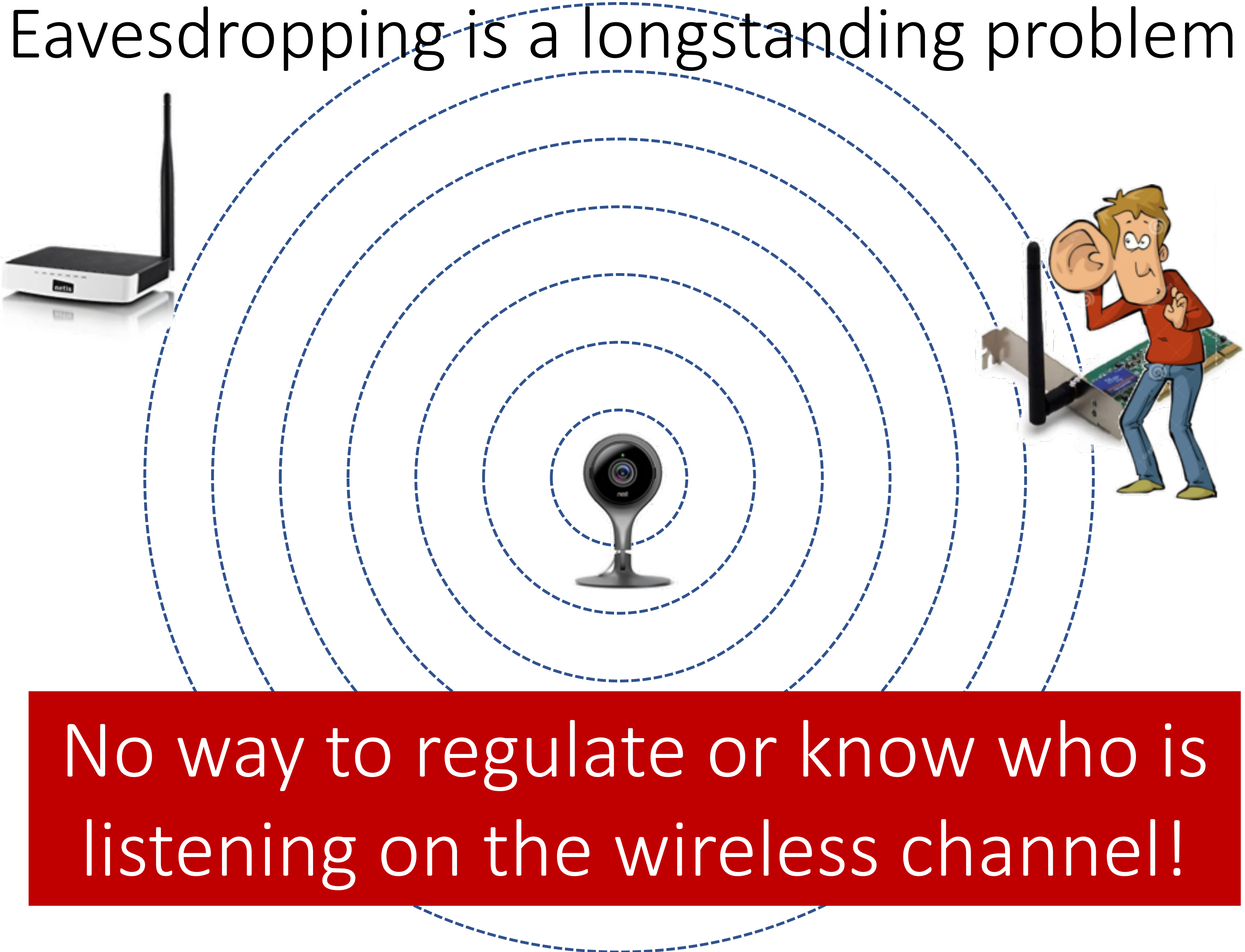
ILLINOIS

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

SyNRG

Systems & Networking
Research Group

Eavesdropping is a longstanding problem!



No way to regulate or know who is listening on the wireless channel!

Defense Against Eavesdropping: Encryption

Encryption breaks due to security loopholes.

Vulnerability in WPA2

[SIGSAC'17]

Side Channel Attacks

[CRYPTO'14, CHES'15, CCS'16, RSA'16, MobiCom'15]

Low power devices employ weak or no encryption.

Ultra-Low Power RFIDs

[S&P'09, CCS;09, Usenix'12, Defcon'13, NSDI'15]

Medical Implants

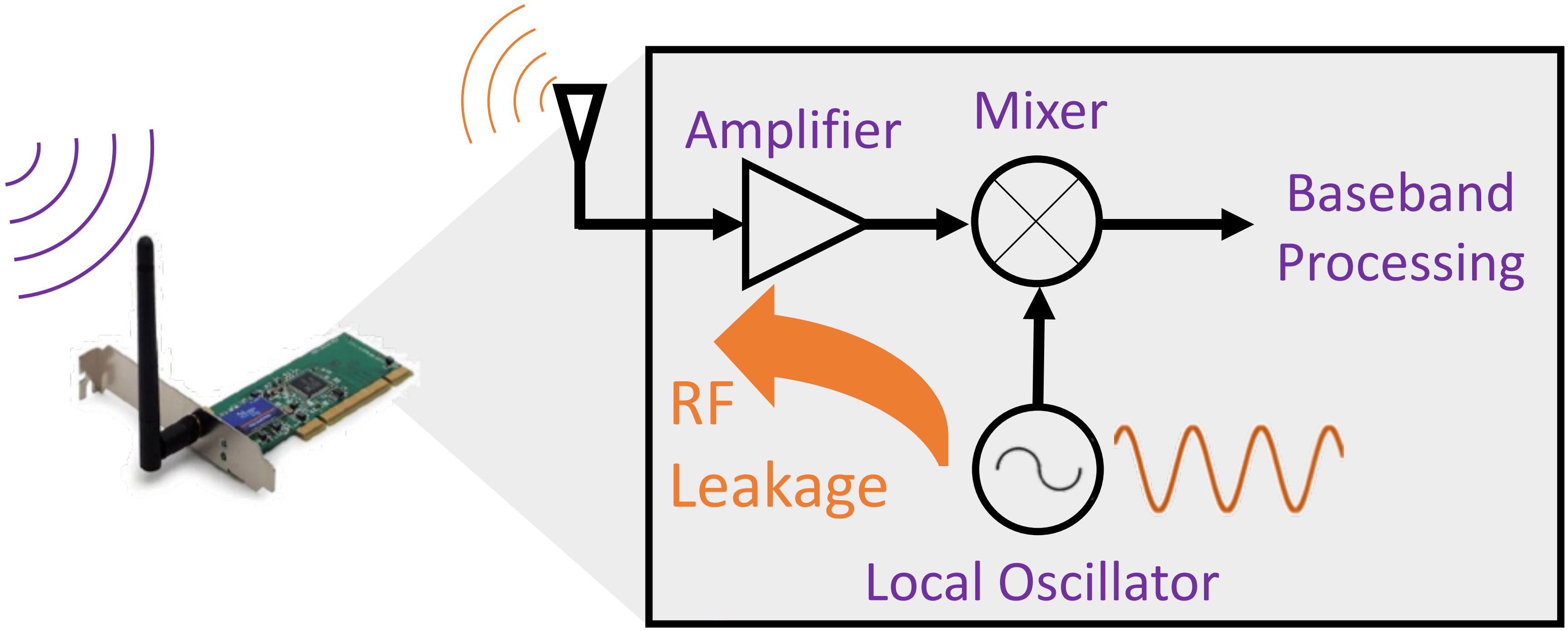
[S&P'10, SIGCOMM'11]

Can we detect the hidden presence of wireless eavesdroppers?

Ghostbuster

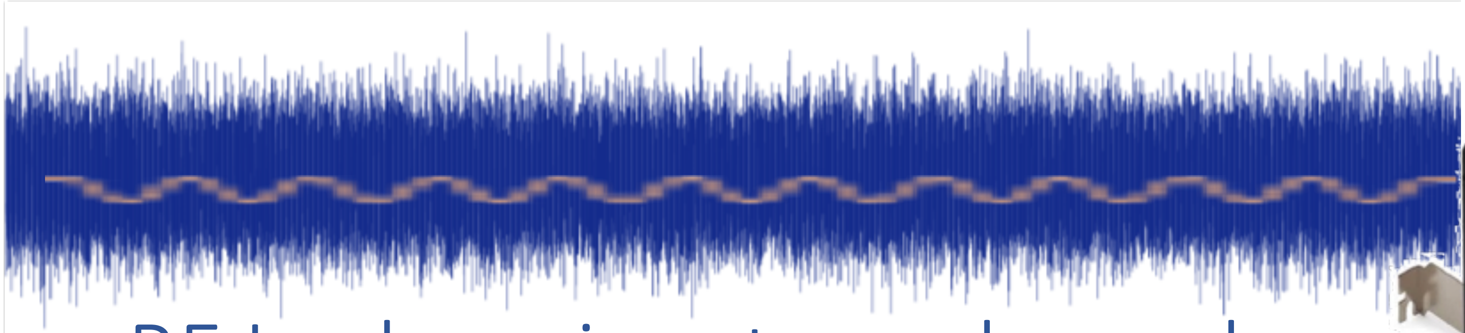
- A system that can reliably detect an eavesdropper in the presence of ongoing transmissions.
- Does not require any modifications to current transmitters and receivers.
- Implemented and empirically tested against SDR & WiFi cards based eavesdroppers.

Key Observation: Even passive receivers leakage RF signals on to the wireless medium



Eavesdropper’s Digital Receiver

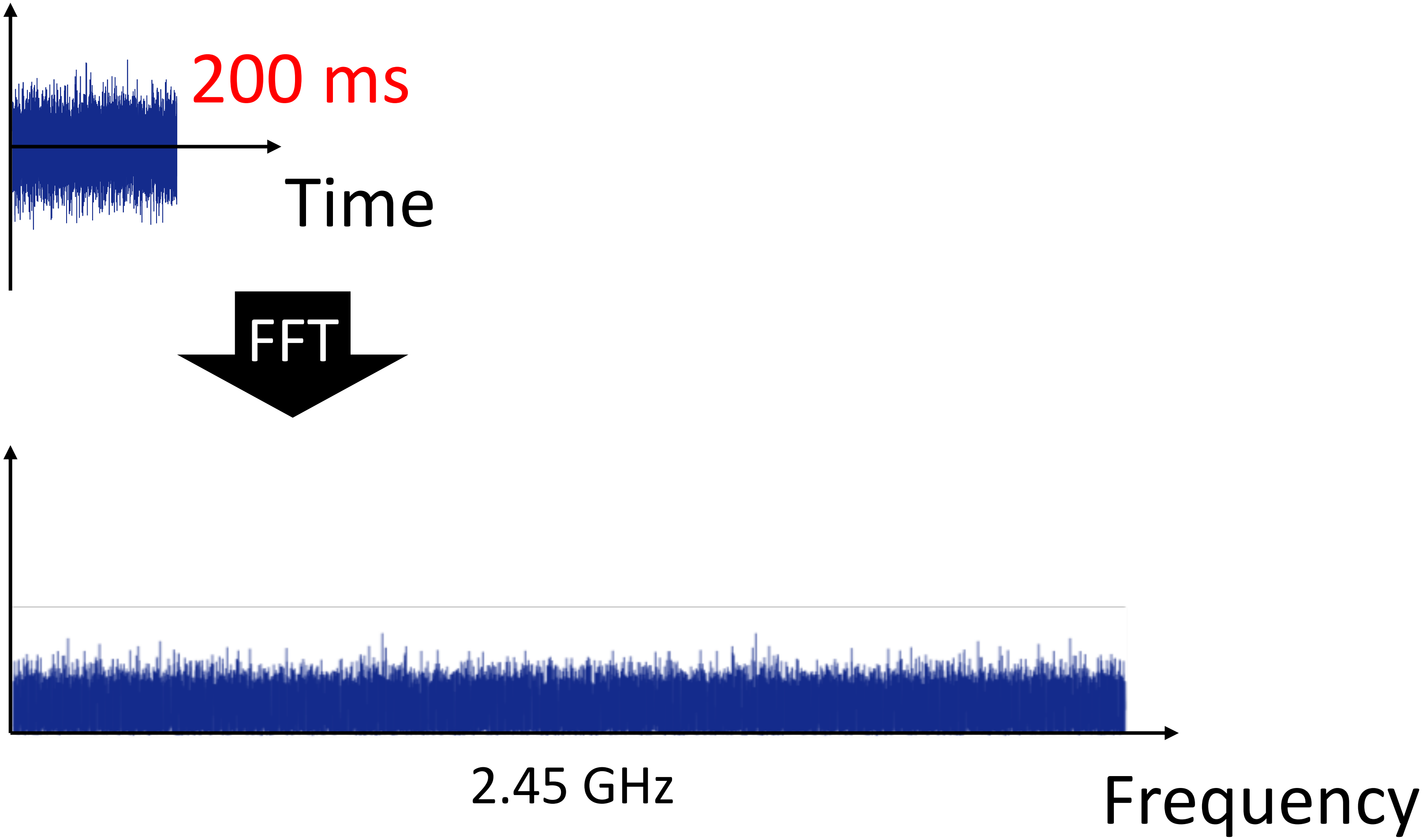
Receiver’s oscillator creates a sinusoid signal at the carrier frequency of operation



RF Leakage is extremely weak:
buried under noise floor

Hard to detect with today’s receivers

Average noise by taking an FFT over a large time window



200 ms

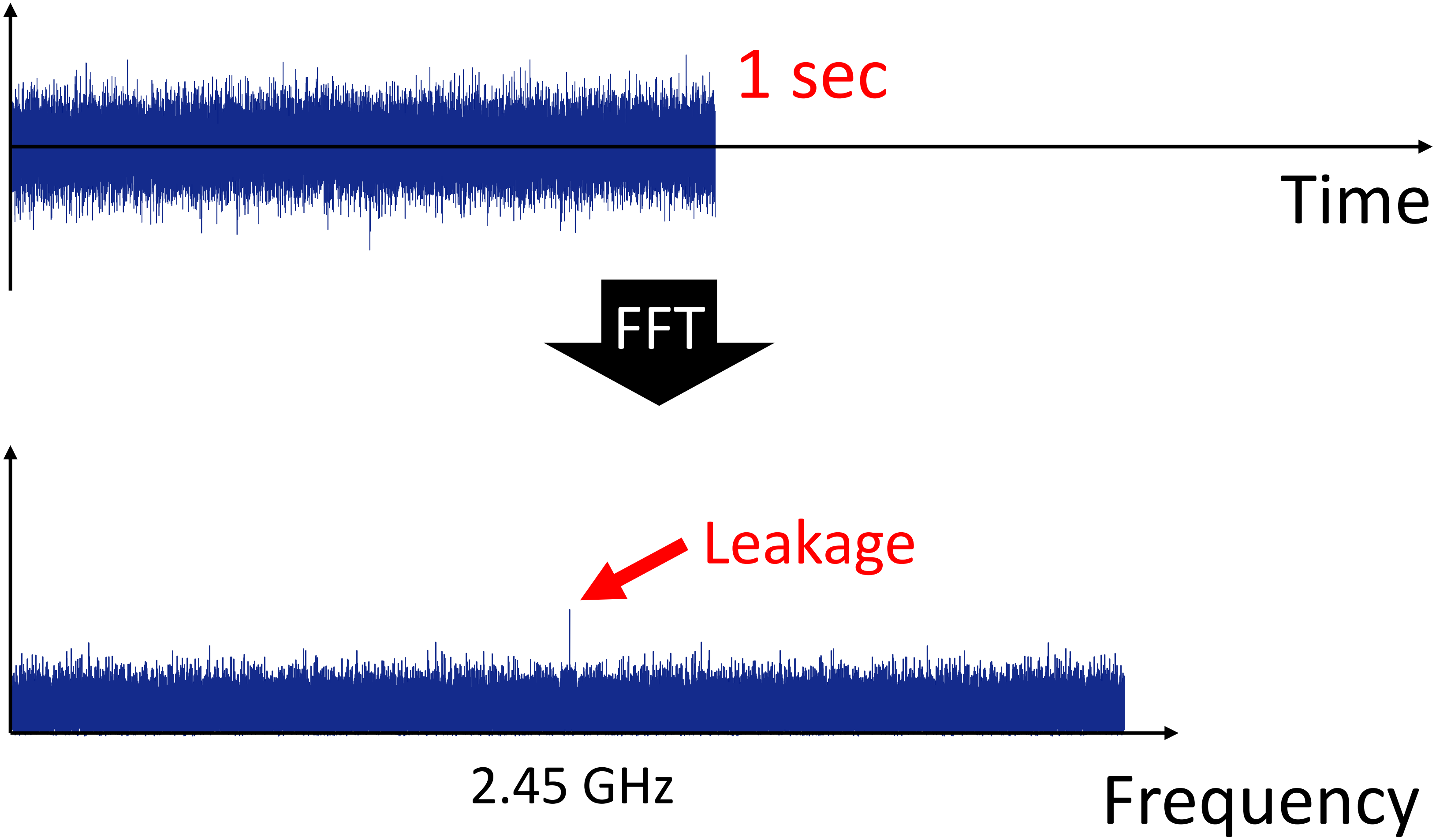
Time

FFT

2.45 GHz

Frequency

Average noise by taking an FFT over a large time window



1 sec

Time

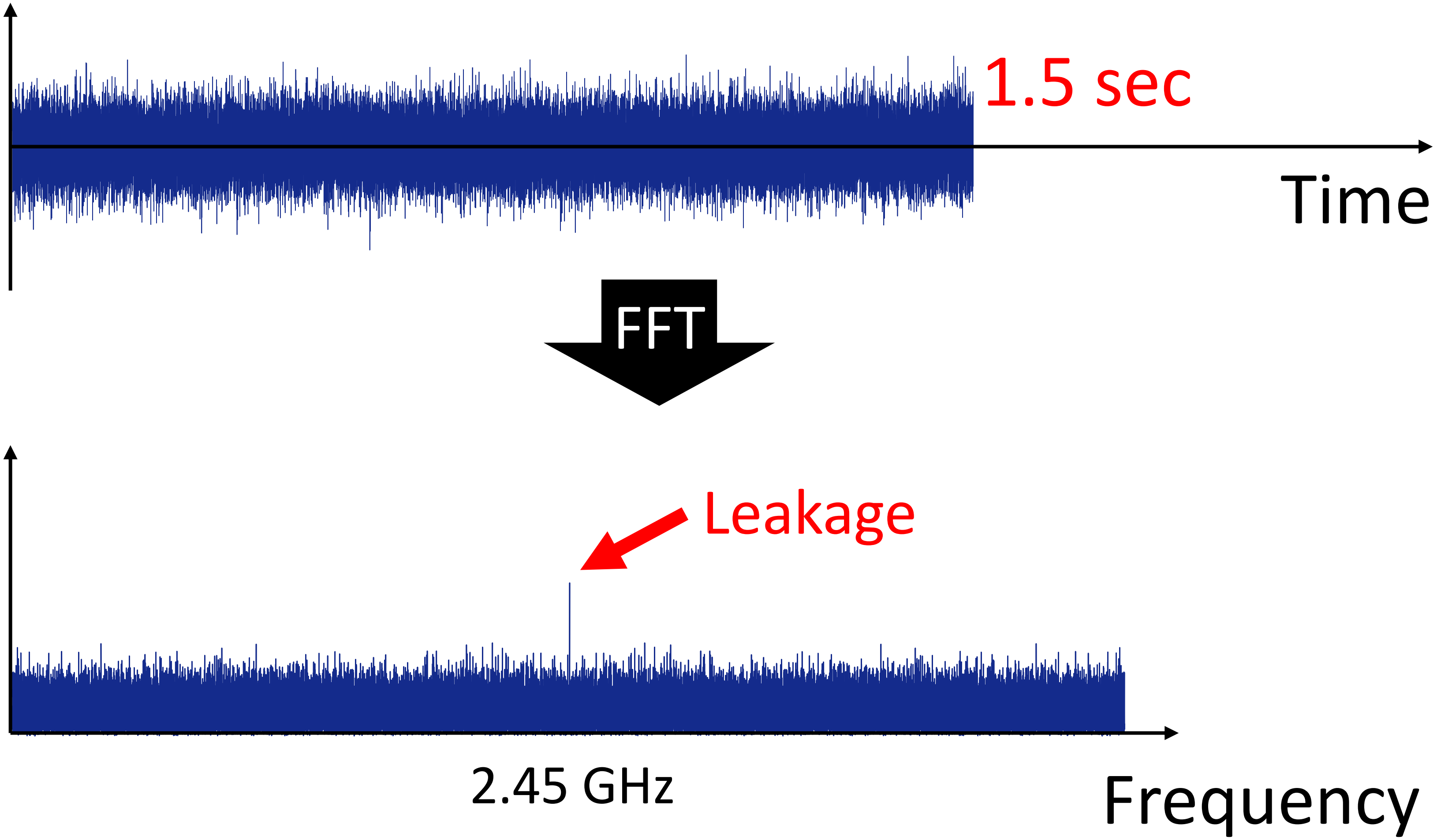
FFT

Leakage

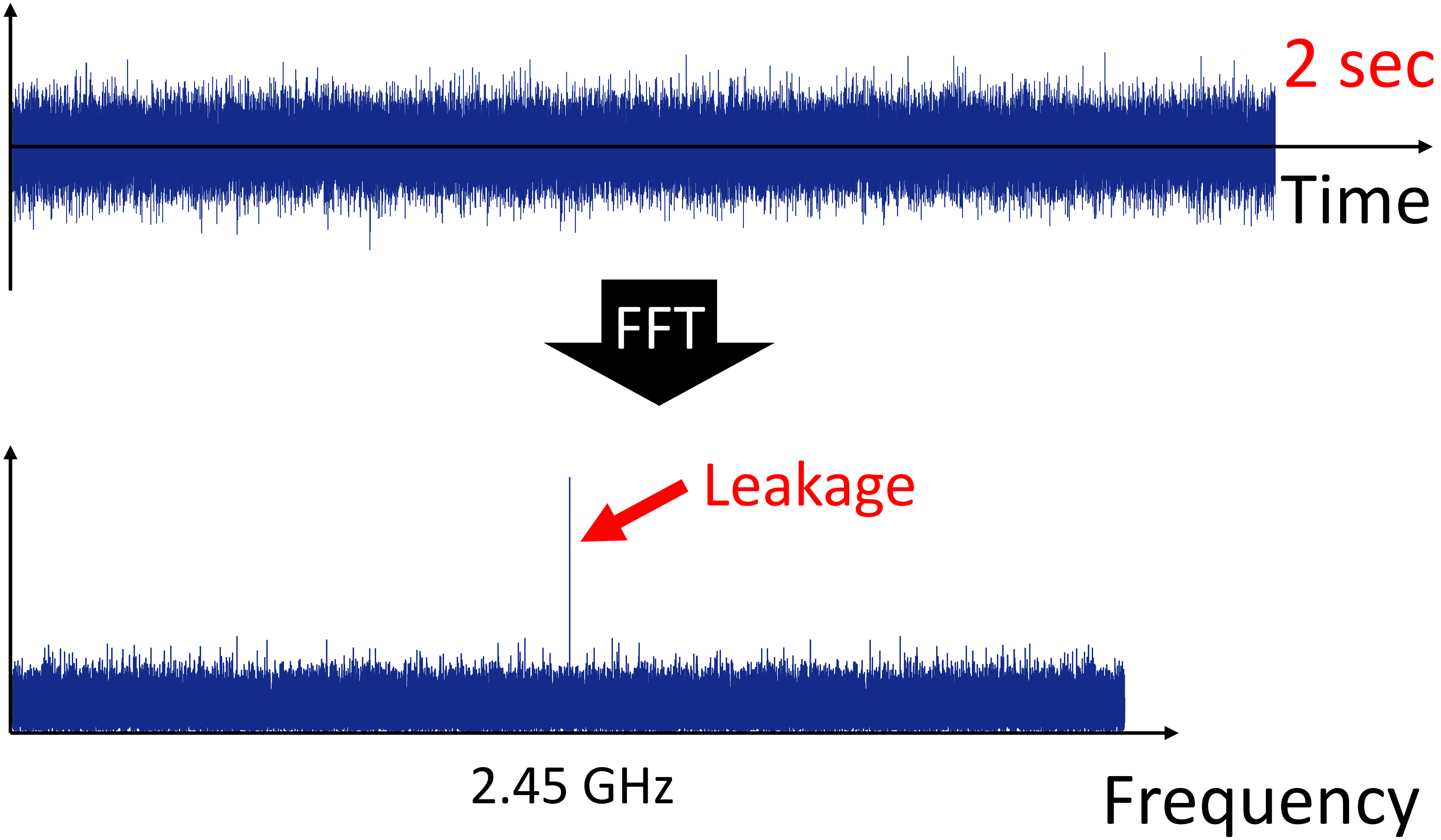
2.45 GHz

Frequency

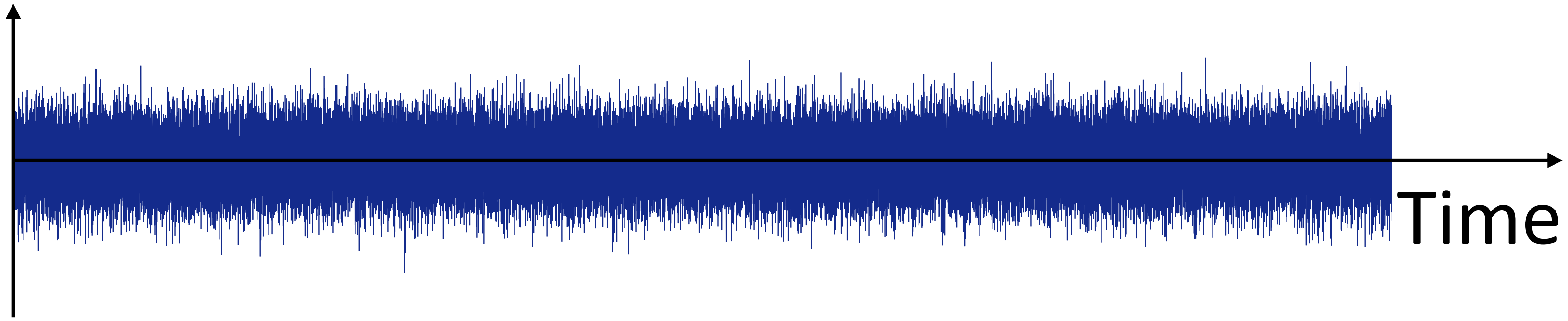
Average noise by taking an FFT over a large time window



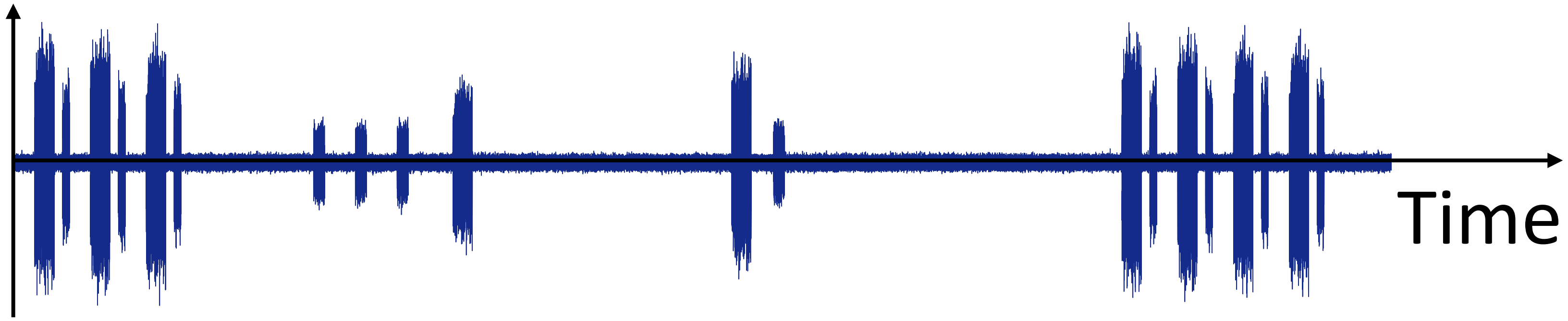
Average noise by taking an FFT over a large time window



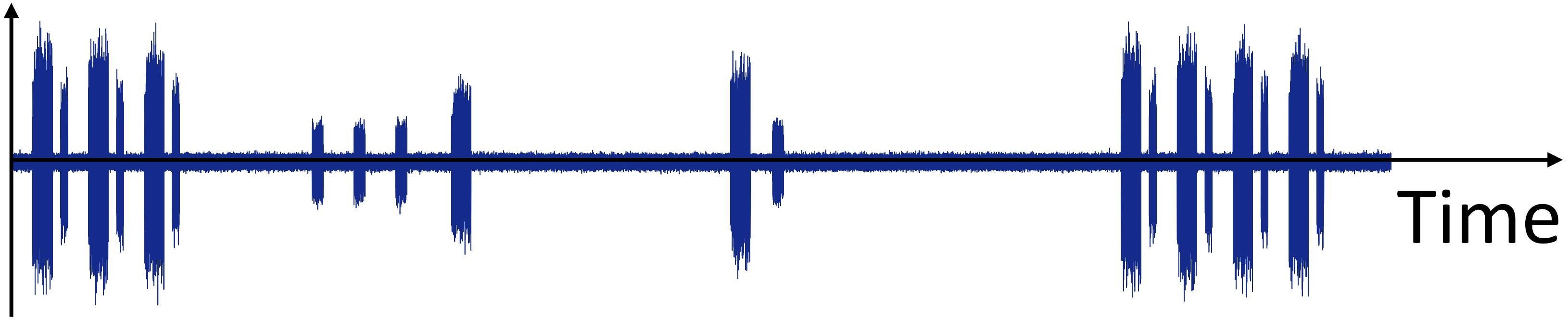
However, large time windows are bound to include transmitted packets!

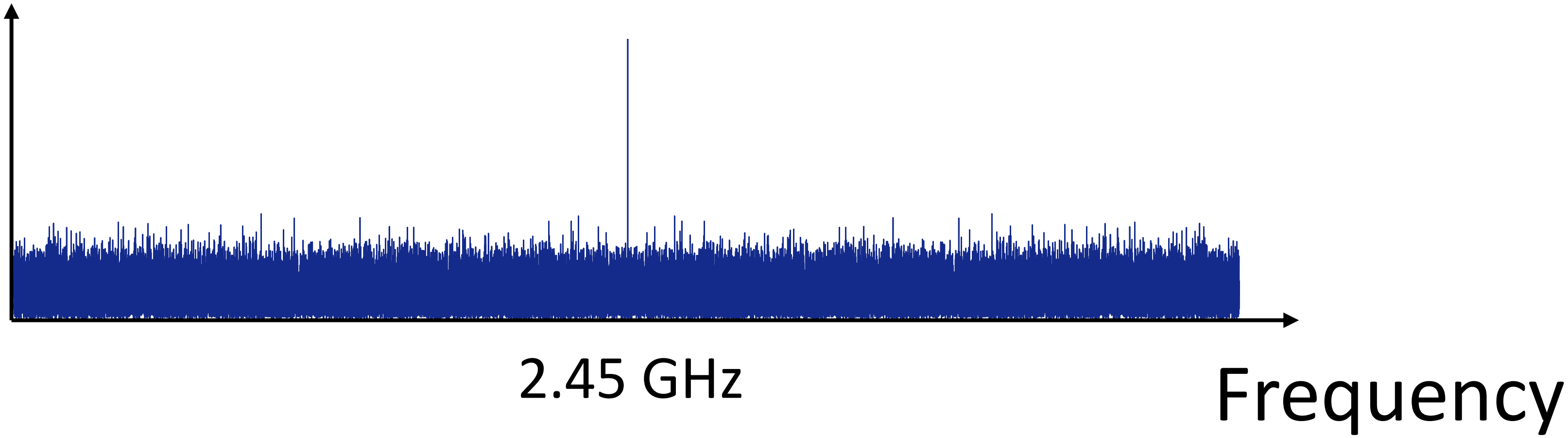


However, large time windows are bound to include transmitted packets!

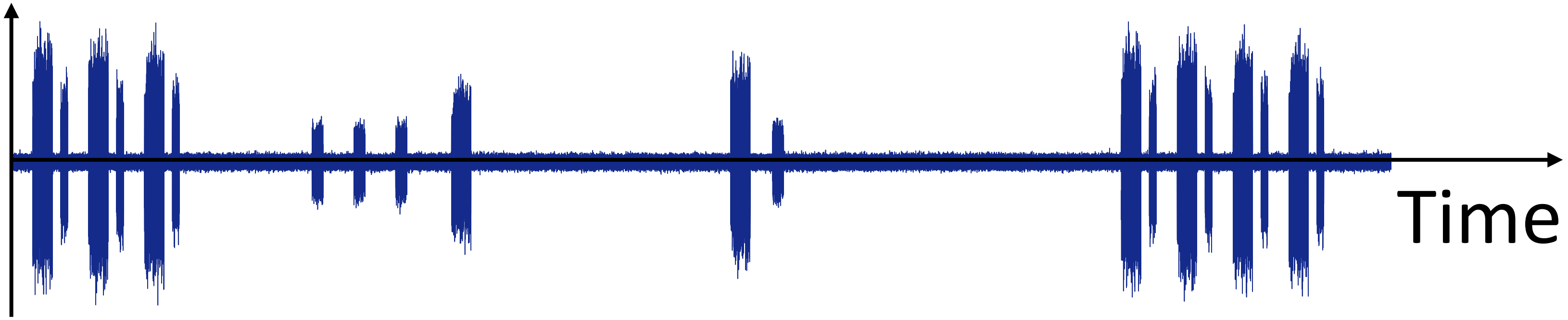


However, large time windows are bound to include transmitted packets!

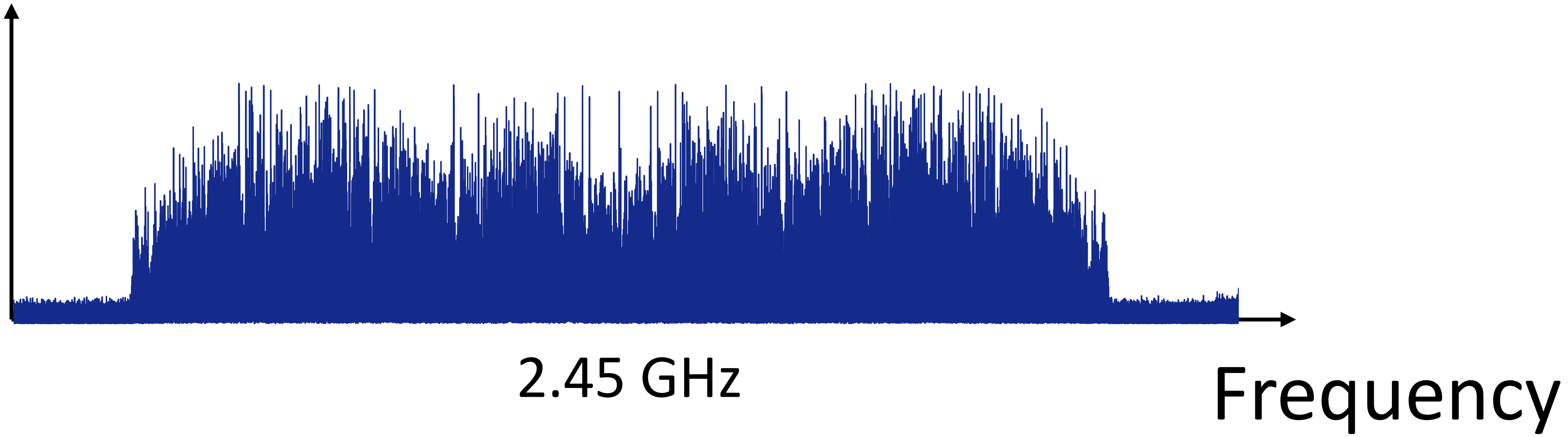




However, large time windows are bound to include transmitted packets!



Leakage is orders of magnitude weaker than TX signals.



However, large time windows are bound to include transmitted packets!

Leakage is orders of magnitude weaker than TX signals.

Other legitimate receivers also create RF leakage.

How to extract the eavesdropper's leakage in the presence of ongoing transmissions and leakage from other receivers?

Ghostbuster

Null On Going Transmissions

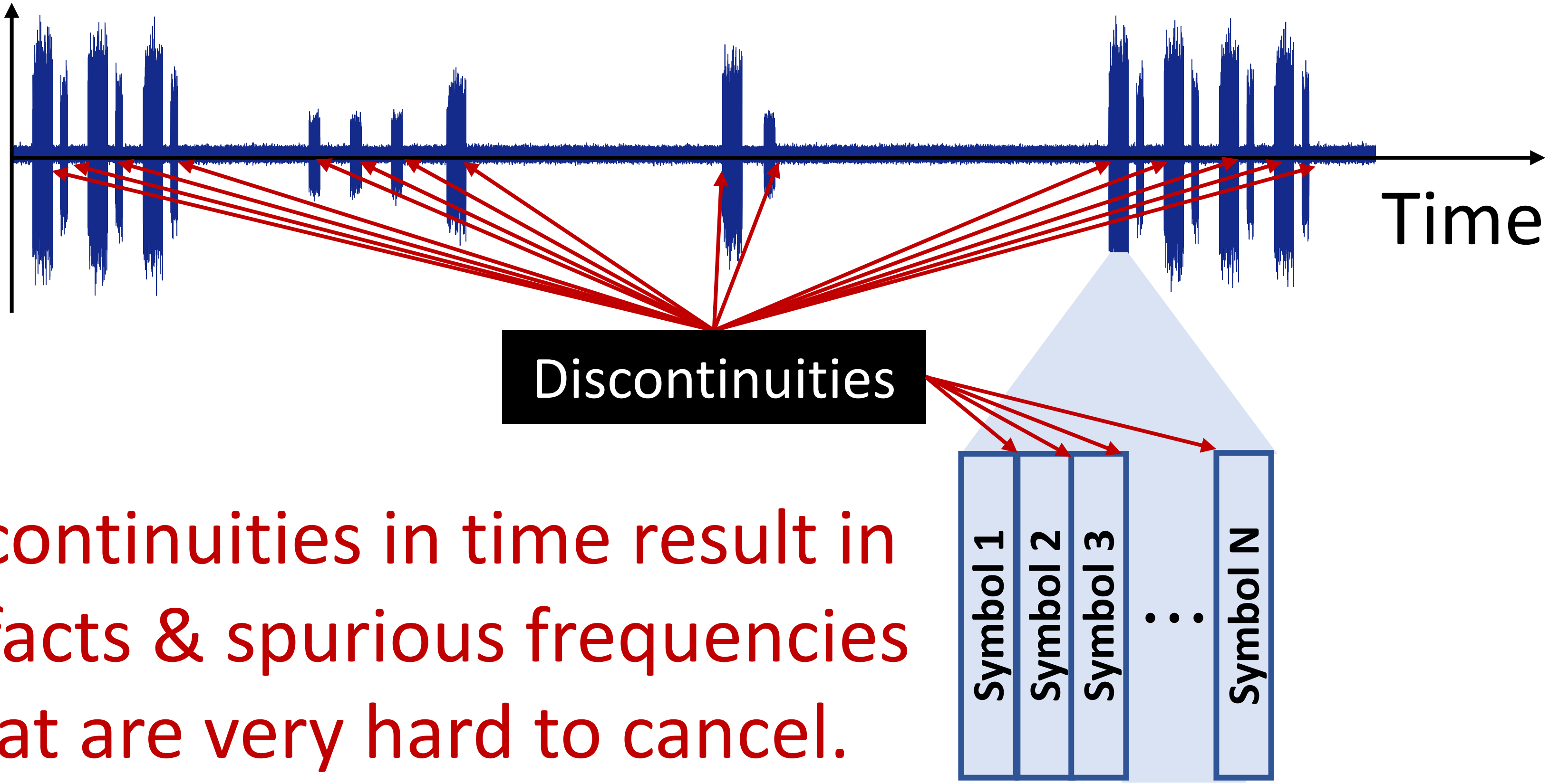
Spatial Domain

Frequency Domain

MIMO

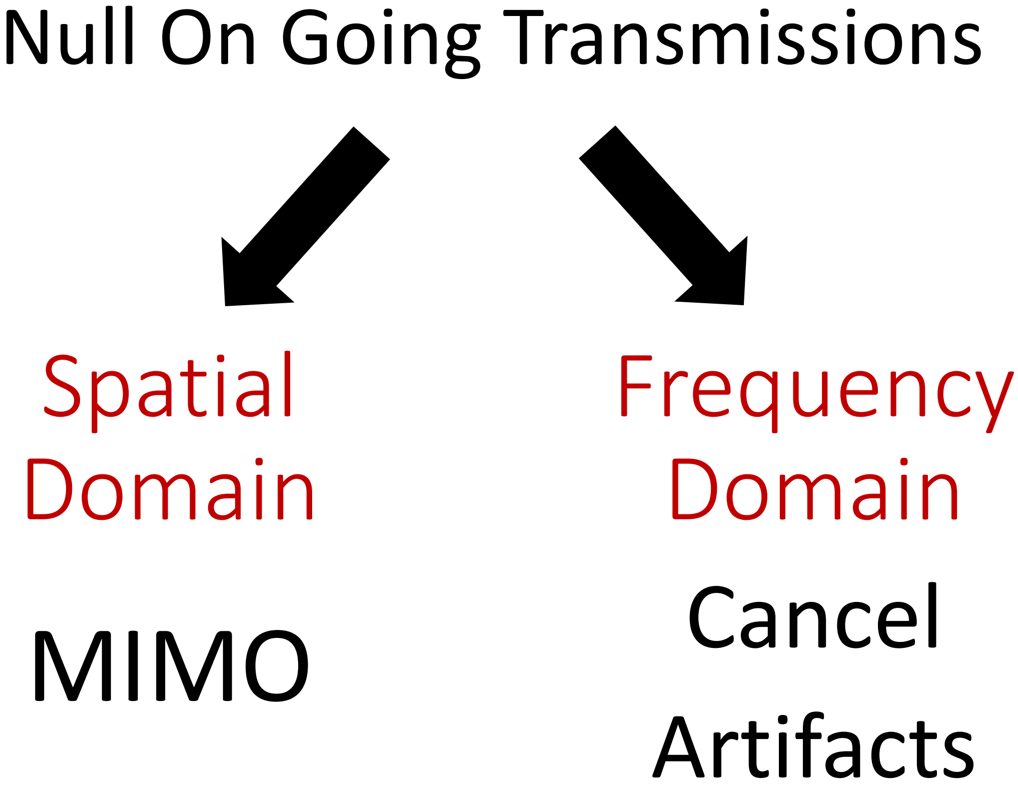
Ghostbuster

MIMO alone is not sufficient.



Discontinuities in time result in artifacts & spurious frequencies that are very hard to cancel.

Ghostbuster



Null On Going Transmissions

Spatial Domain

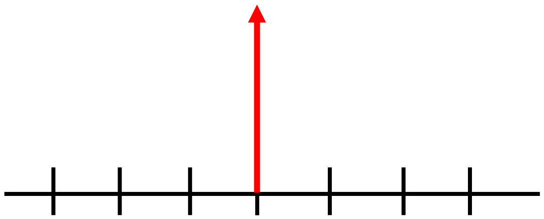
MIMO

Frequency Domain

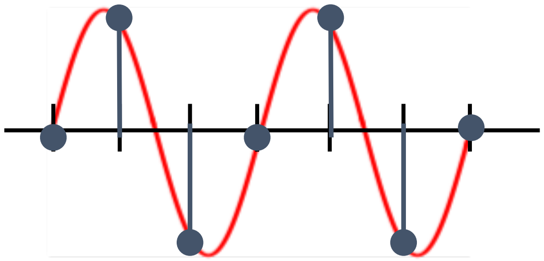
Cancel Artifacts

Discontinuities & Artifacts

Consider a single frequency

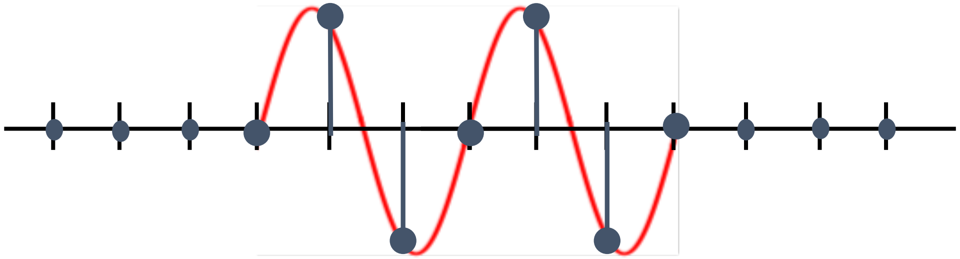


Frequency



Time

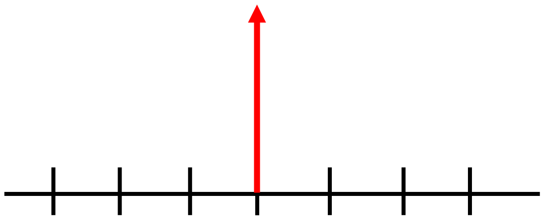
More samples



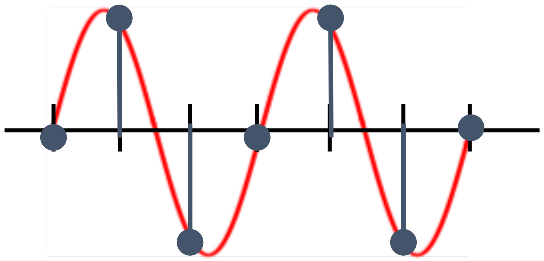
Large Time Window

Discontinuities & Artifacts

Consider a single frequency

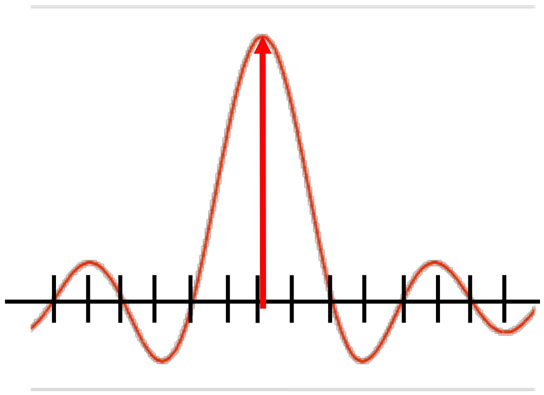


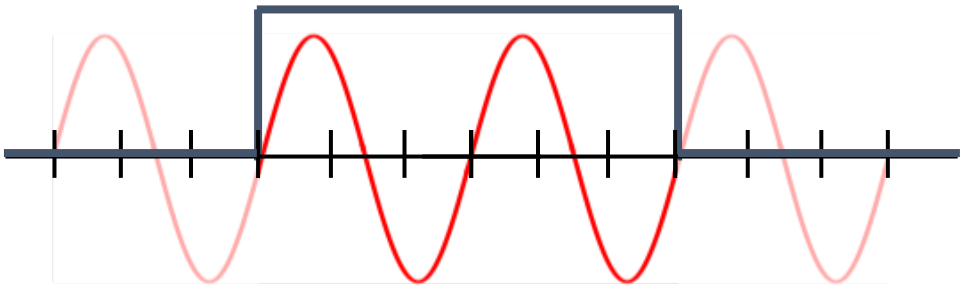
Frequency



Time

More samples

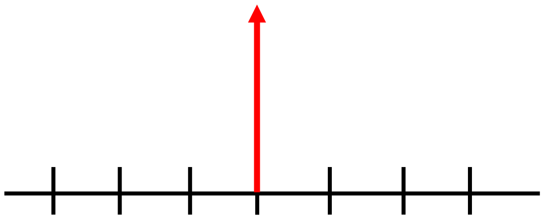




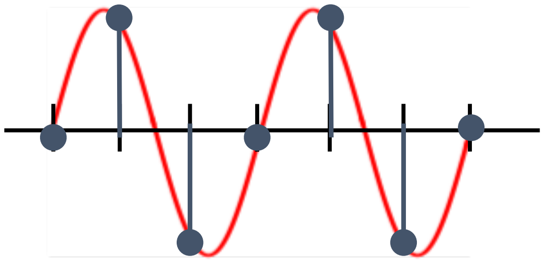
Large Time Window

Discontinuities & Artifacts

Consider a single frequency

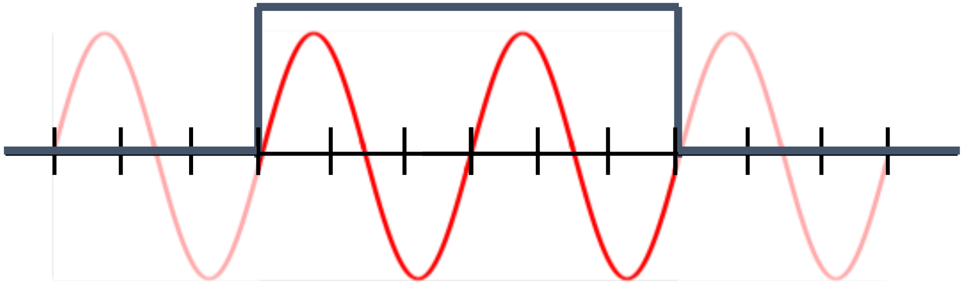


Frequency



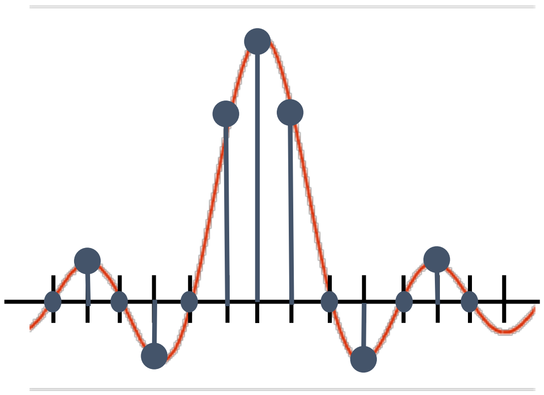
Time

More samples



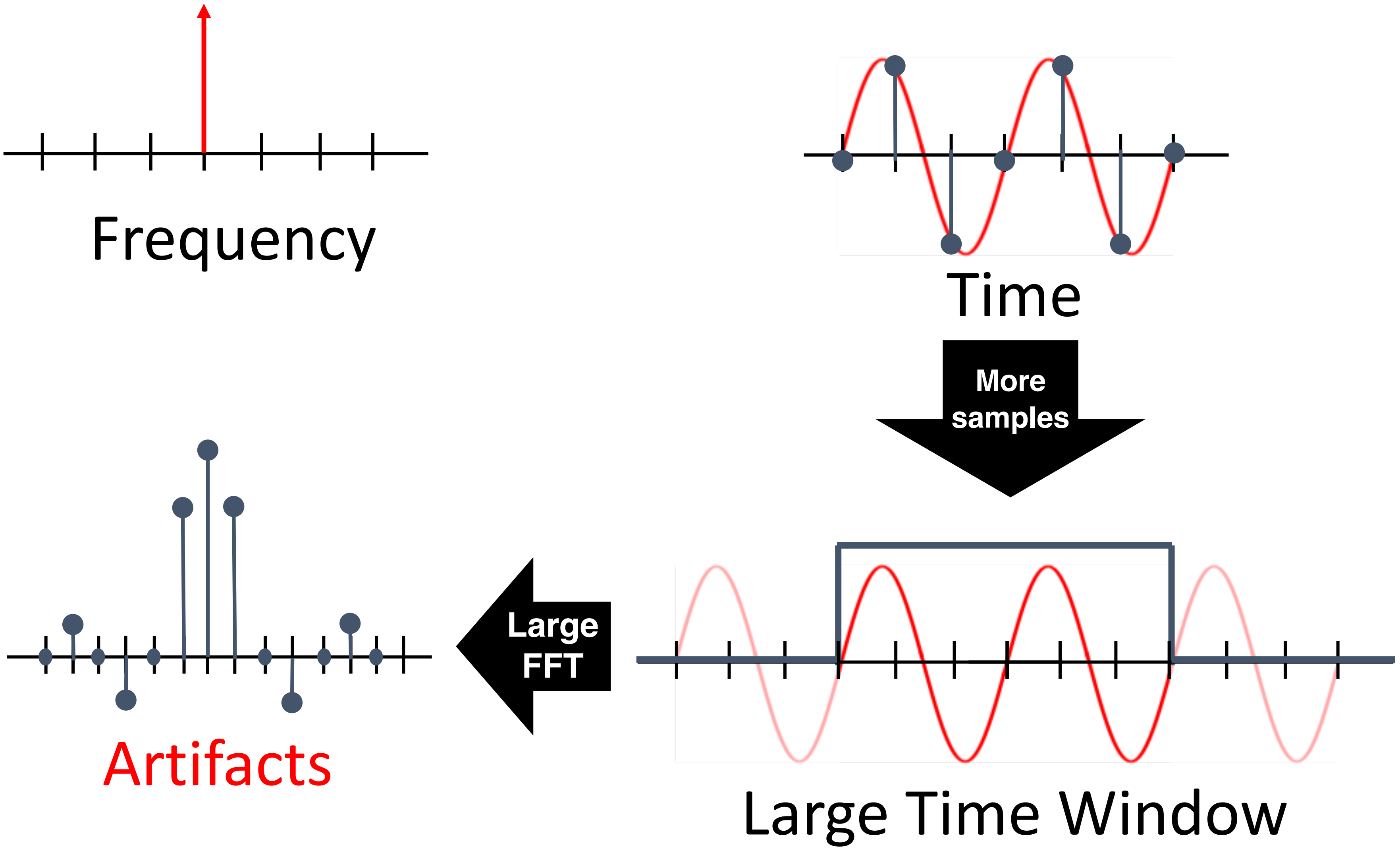
Large Time Window

Large FFT



Discontinuities & Artifacts

Consider a single frequency



Frequency

Time

More samples

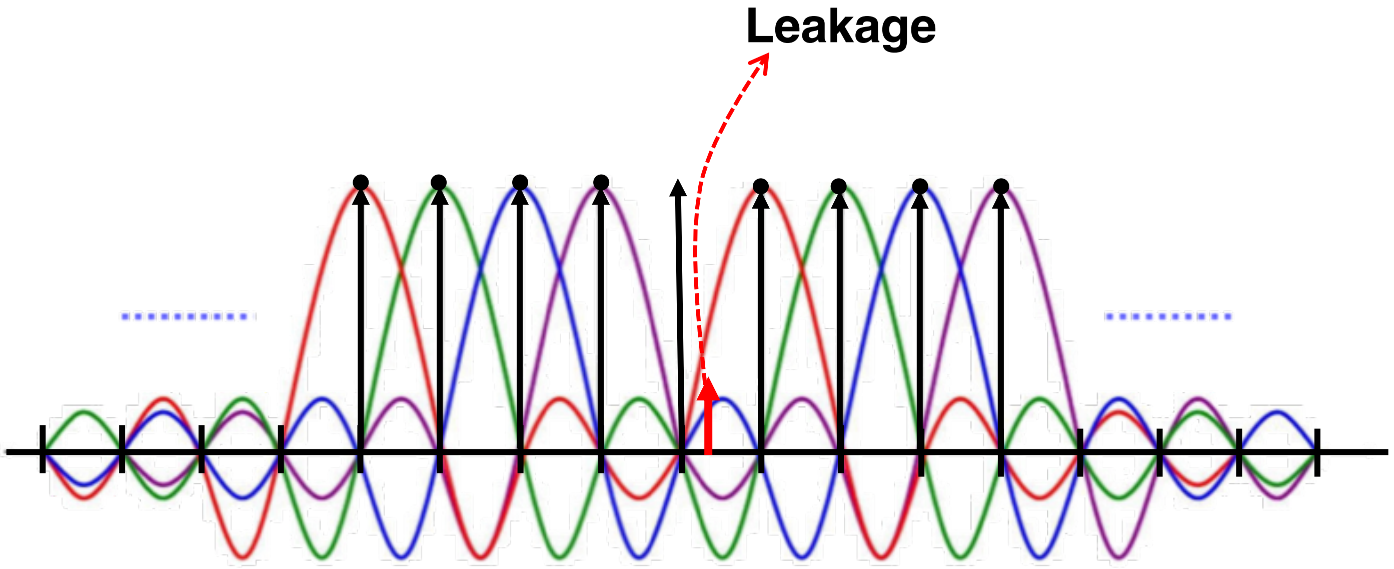
Large FFT

Artifacts

Large Time Window

Discontinuities & Artifacts

Artifacts add up from all frequencies & symbols



Artifacts add up from all packets in the time window

Canceling Artifacts

Need to estimate the continuous **(Off-Grid)** frequency positions & coefficients

Solve: $$\underset{\tilde{f}_k,\tilde{a}_k}{\operatorname{argmin}} \sum_{t=0}^{N-1} \left| x(t) - \sum_{k=0}^{N-1} \tilde{a}_k e^{j2\pi \tilde{f}_k t/N} \right|^2$$

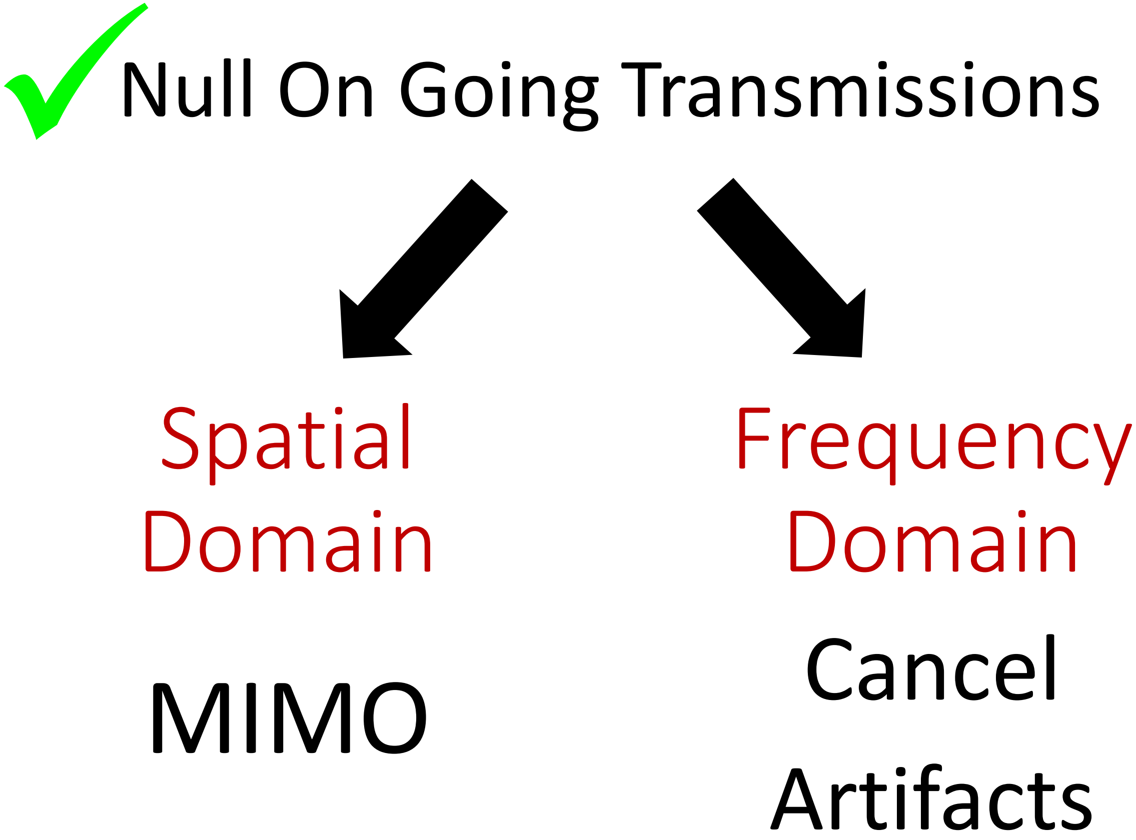
Fix $\tilde{f}_k$, solve for $\tilde{a}_k$: Weighted Least Squares

Fix $\tilde{a}_k$, solve for $\tilde{f}_k$: Convex for good initial estimates of $\tilde{f}_k$

↓

Solve using gradient descent.

Ghostbuster



✓ Null On Going Transmissions

Spatial Domain

MIMO

Frequency Domain

Cancel Artifacts

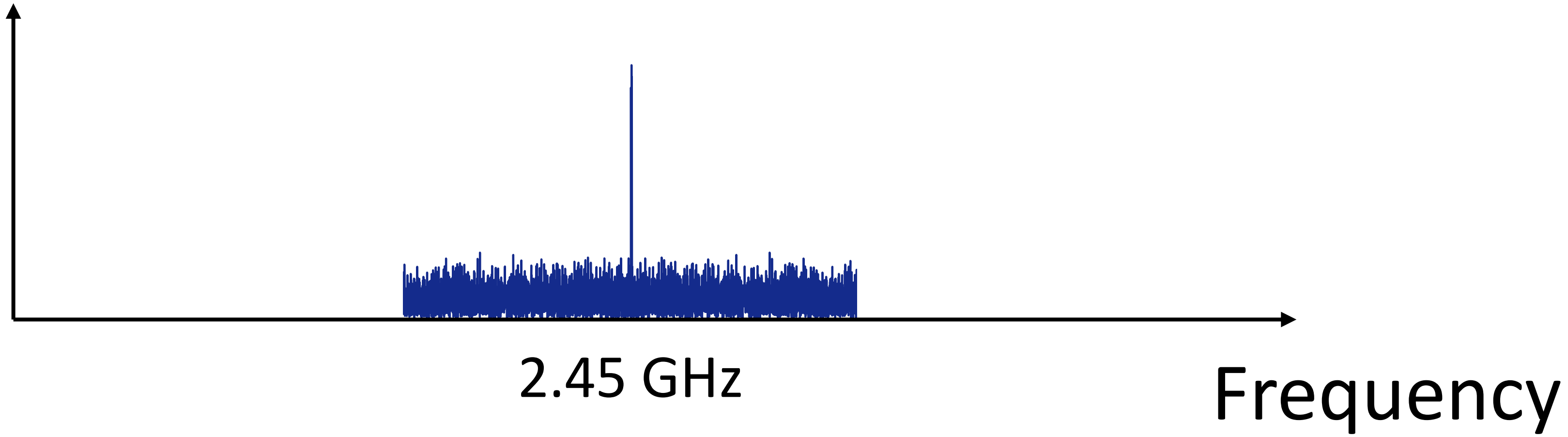
But what about leakage from other receivers?

Ghostbuster

✓ Null On Going Transmissions

But what about leakage from other receivers?

Leverage carrier frequency offset (CFO) between receivers

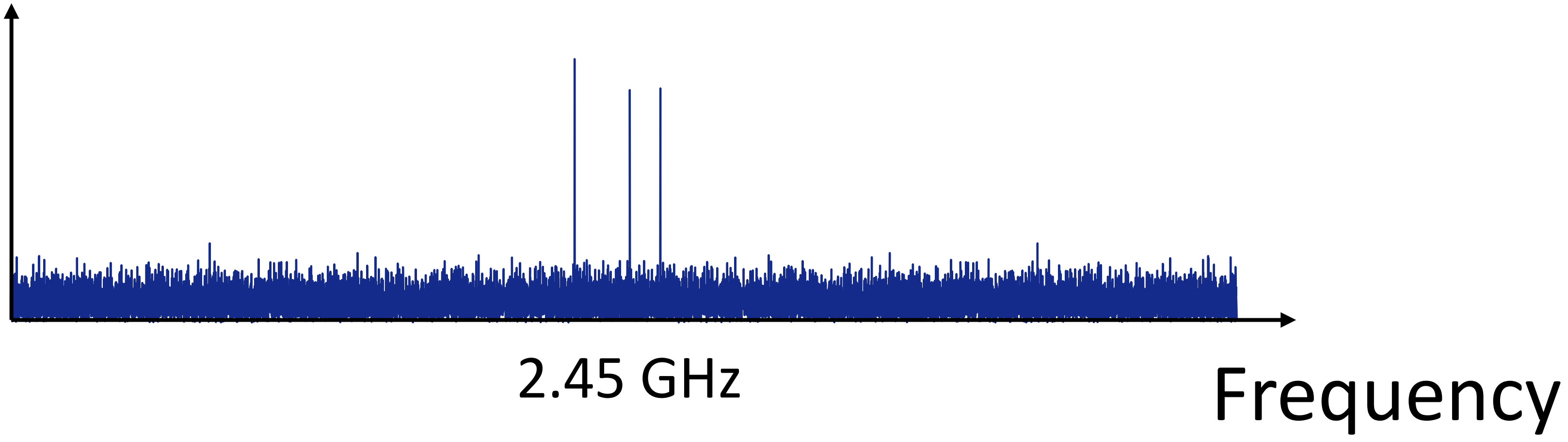


Ghostbuster

✓ Null On Going Transmissions

✓ But what about leakage from other receivers?

Leverage carrier frequency offset (CFO) between receivers



Implementation

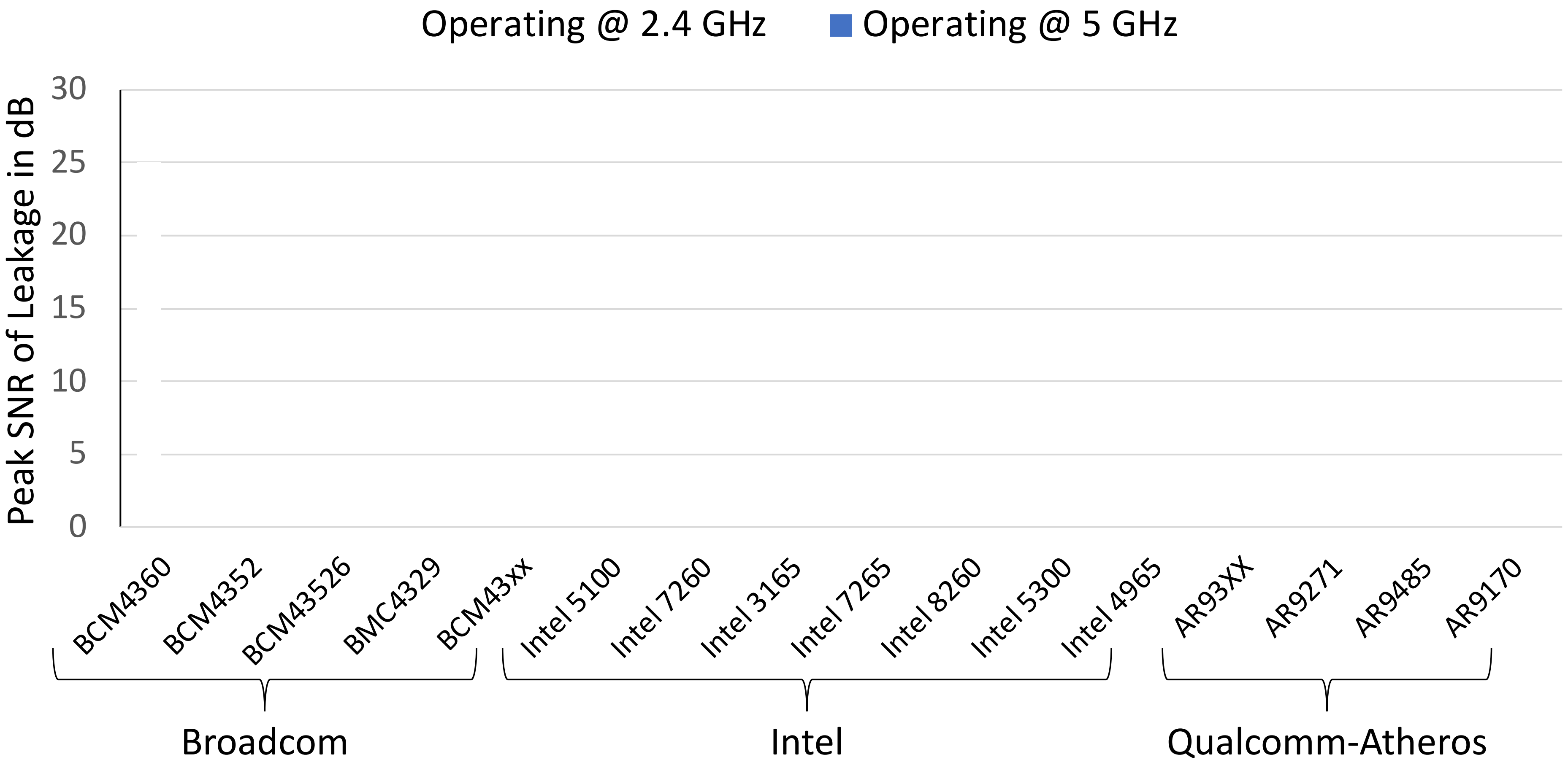
- Implemented Ghostbuster Using USRP Software Radios.

- Tested 16 WiFi Cards & 4 USRP daughterboards as eavesdroppers.

- More implementation details in the paper.

WiFi Cards placed in monitor mode

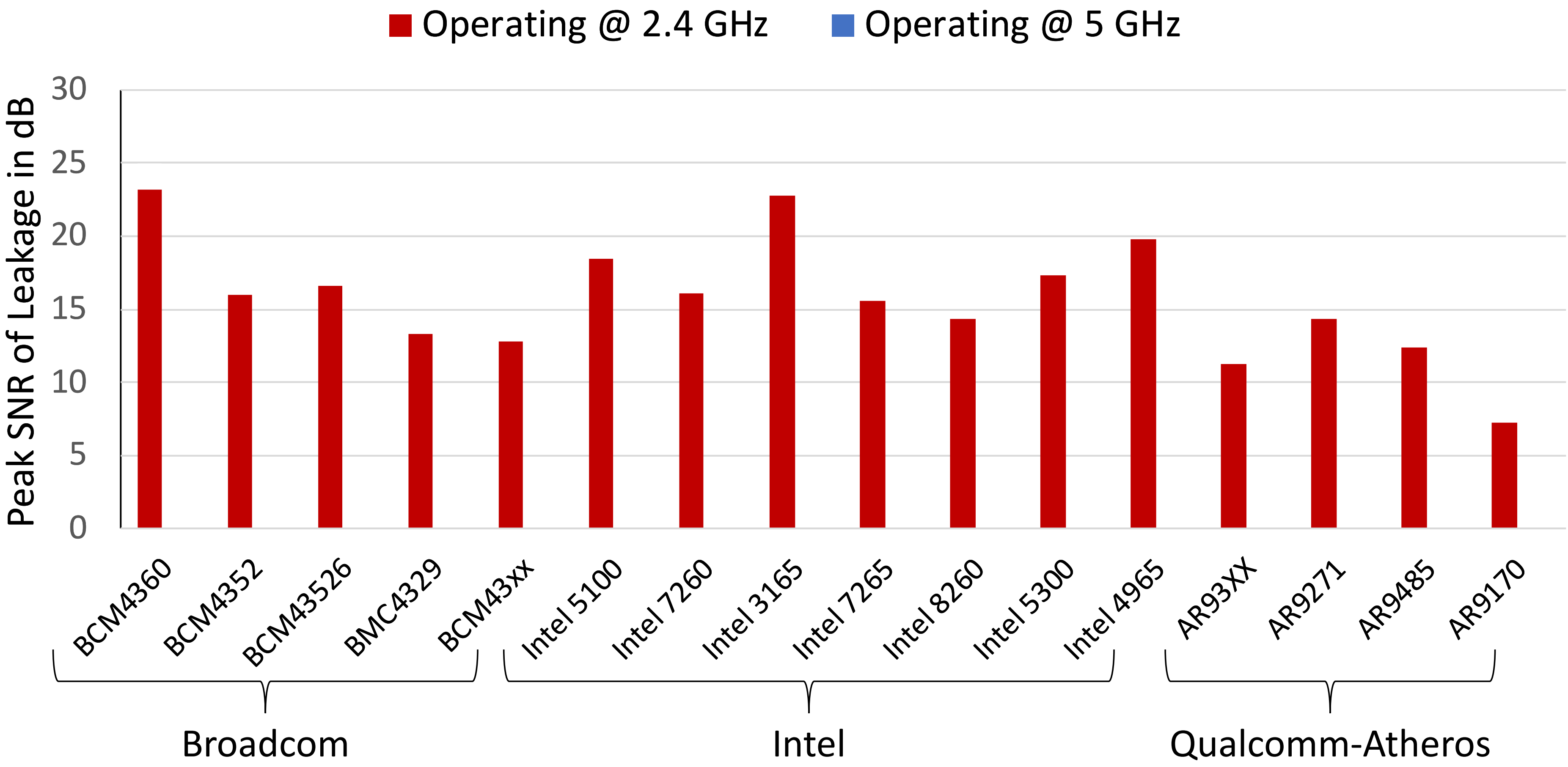
Leakage measured 1m away using 1 sec FFT Window



Chipsets cover range of hardware architectures & WiFi protocols: 802.11a/b/g/n/ac

WiFi Cards placed in monitor mode

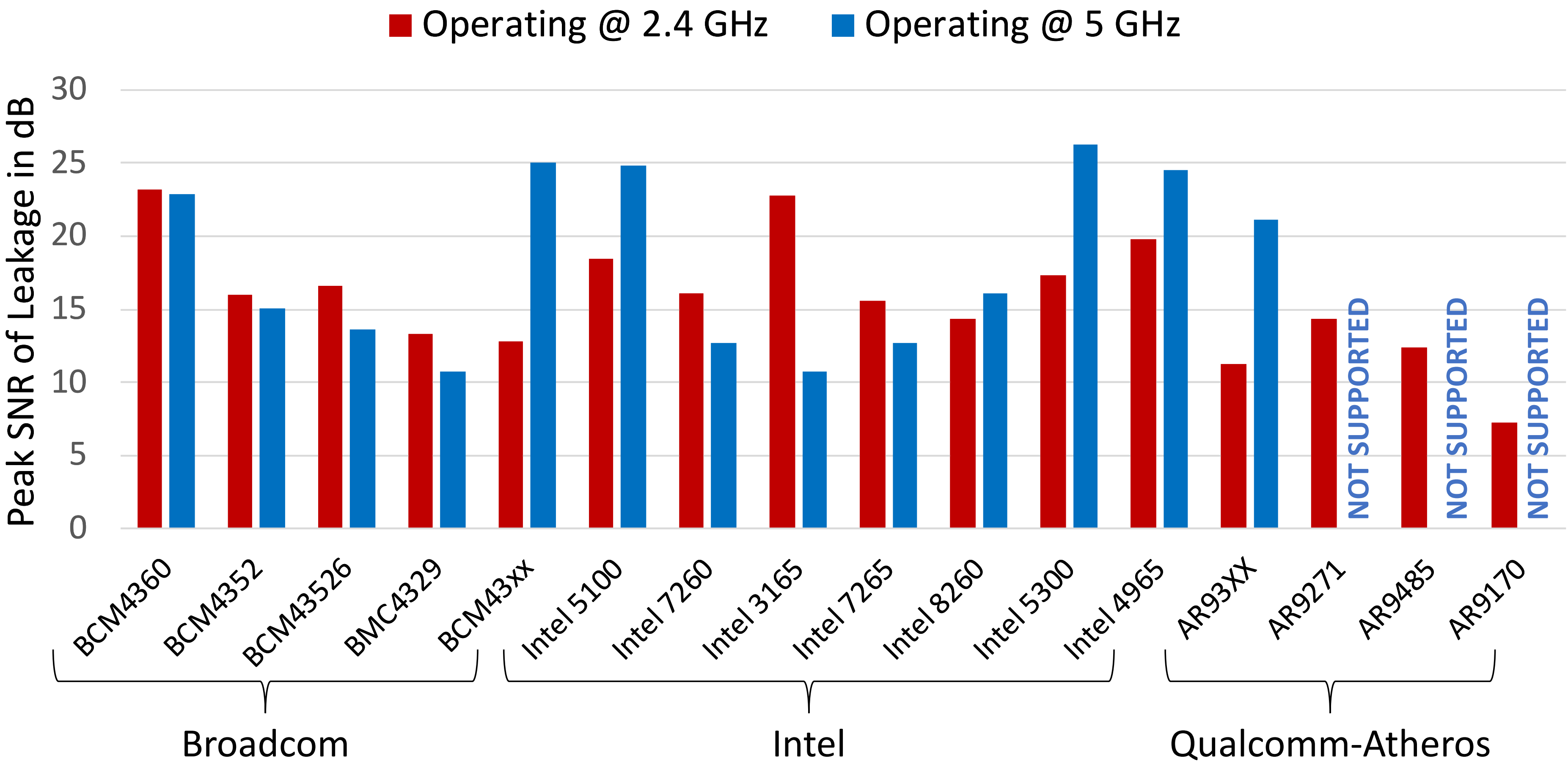
Leakage measured 1m away using 1 sec FFT Window



Chipsets cover range of hardware architectures & WiFi protocols: 802.11a/b/g/n/ac

WiFi Cards placed in monitor mode

Leakage measured 1m away using 1 sec FFT Window



Chipsets cover range of hardware architectures & WiFi protocols: 802.11a/b/g/n/ac

Summary of Results

- Ghostbuster can detect:
  - WiFi Card eavesdroppers up to 7 meters away.
  - USRP eavesdroppers up to 14 meters away.
- Detection Accuracy & Range improves with:
  - Larger time windows. (10 ms < 100 ms < 1 sec)
  - More MIMO chains. (2 MIMO < 3 MIMO < 4 MIMO)
- Ghostbuster can detect eavesdropper in the presence of transmissions & other receivers:
  - With 95% accuracy with 1 other receivers.
  - With 89.9% accuracy with 3 other receivers.

Conclusion

- Ghostbuster can detect eavesdroppers in the presence of ongoing transmissions & other receivers without requiring any modifications to current transmitters and receivers.

- Take first step towards detecting eavesdroppers

  but a lot of future work:

  - ➢ What if number of legitimate RXs is not known?
  - ➢ Can we localize the eavesdropper?
  - ➢ Can we reduce computational complexity?

- Opens the door for more practical applications:

  - ➢ Detecting Remote Explosives
  - ➢ More Efficient Carrier Sense
  - ➢ Synchronizing Clocks through Leakage