Research Presentation Exam:

"Ghostbuster: Detecting the Presence of Hidden Eavesdroppers"

Cesar Arguello

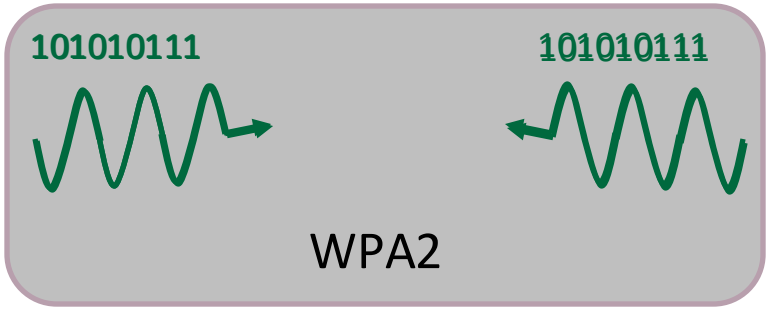
Nov 5th, 2024

DARTMOUTH

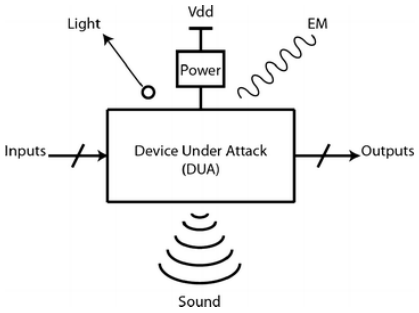
Motivation

802.11n
(Wi-Fi 4)

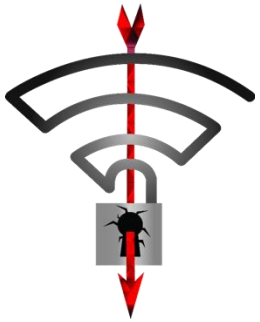
Tim



Dave



Cesar



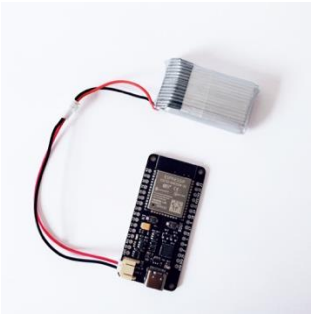
What *exactly* is Ghostbuster?

System based on radio receivers (one or more) that **detects** other passive receivers (**eavesdroppers**) in a physical area.

Detecting Eavesdroppers is **HARD**! Why?

- **No detectable footprint** in the wireless medium (e.g., no active transmissions).

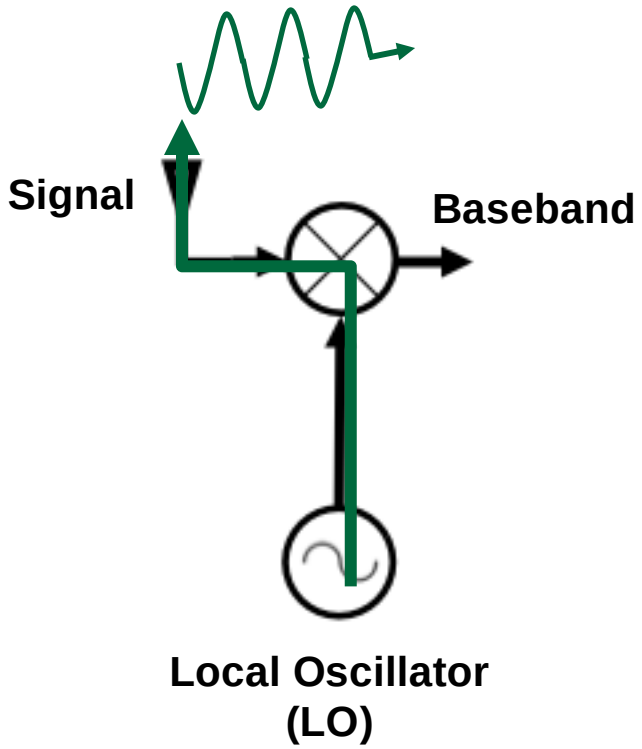
- **Can be physically concealed**, making visual detection difficult.



Ghostbuster Detection: Listening to the Ghosts

- **No dete[illegible]print** in the wireless m[illegible]e.g., no active t[illegible]

LO's signal **leaks** through the antenna

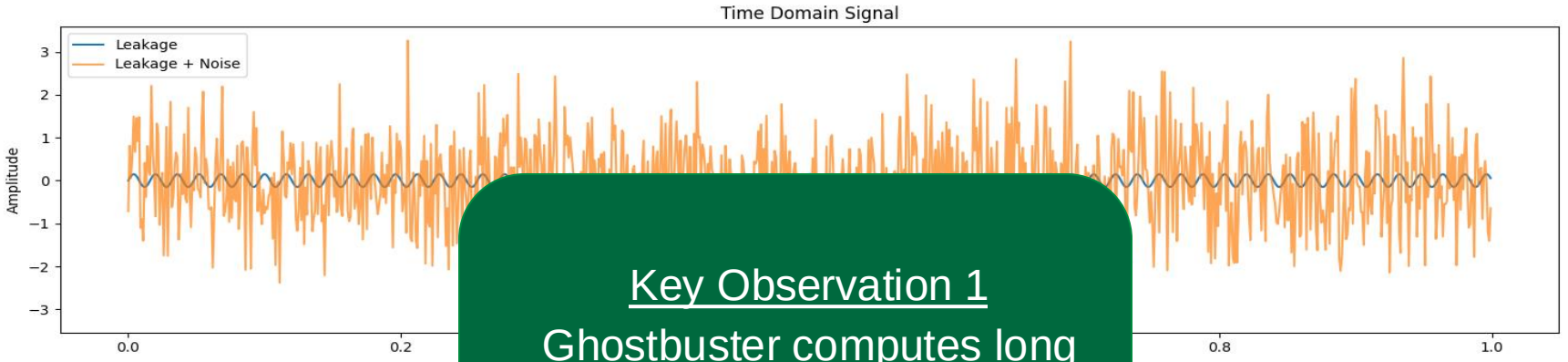


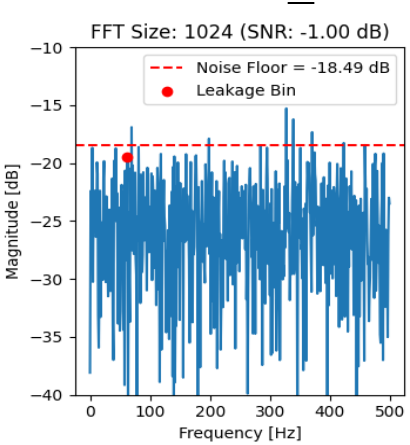
Ghostbuster Detection: Simplified Scenario I

Isolated System*

*system does not exchange matter or energy with surroundings

Ghostbuster Detection: Simplified Scenario I





Key Observation 1

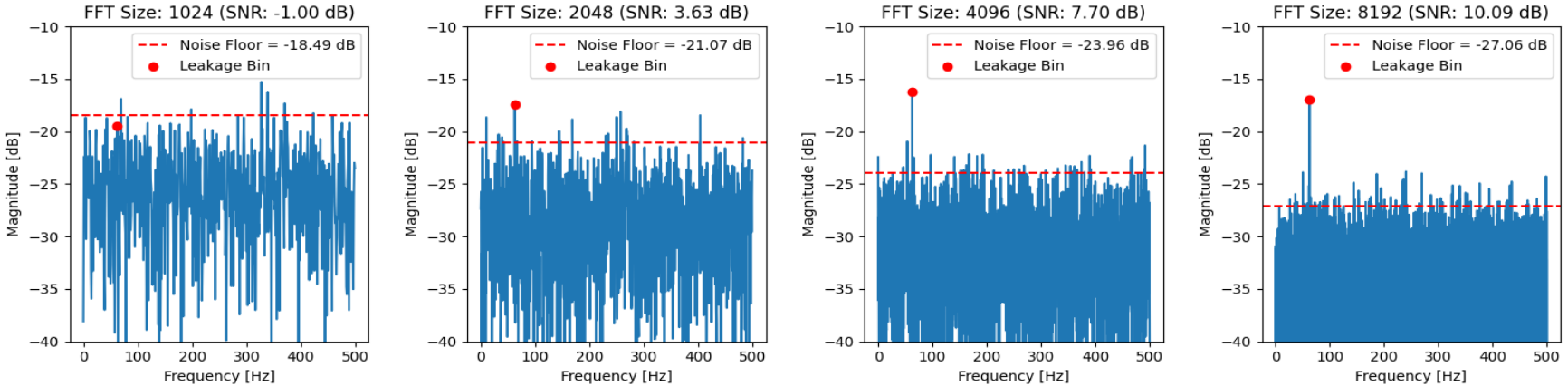
Ghostbuster computes long FFTs to bring leaked signal above the noise floor

Ghostbuster Detection: **Long DFTS**

- Power remains **constant** for **noise** (and signal*).

$$\frac{1}{N}\sum_{n=0}^{N-1}|x[n]|^2$$

- Same noise power is distributed over more bins = **SNR per bin increases**.



*signal must be a sinusoid

Ghostbuster Detection: **Long DFTS**

WiFi Chipset/ USRP Daughterboard	Frequency Band @ f_c = 2.437 GHz			Frequency Band @ f_c = 5.745 GHz		
	Design	Leakage freq. in GHz	Leakage SNR @ 1m in dB	Design	Leakage freq. in GHz	Leakage SNR @ 1m in (dB)
Broadcom: BCM43xx, BCM4329, BCM4360, BCM4352, BCM43526	a	2.437	12.8 −23.0	a	5.745	10.7−25.01
Intel: 4965	c	3.514	19.8	a	5.745	10.7
Intel: 3165, 5100, 5300	b	4.874	12.6−19.7	d	3.65	20.4−22.2
Intel: 7260, 7265, 8260	b	4.874	10.1−13.1	a	5.745	12.6−16.0
Qualcomm: AR93XX	b	4.874	11.3	d	3.65	21.1
Qualcomm: AR9271, AR9485, AR9170	b	4.874	7.2−14.3	N/A	N/A	N/A
USRP N210: SBX board	a	2.437	50.8	N/A	N/A	N/A
USRP N210: CBX board	a	2.437	50.2	a	5.745	56.7
USRP N210: UBX board	a	2.437	53.4	a	5.745	57.5

Table 1: Leakage measured 1 meter away for different WiFi eavesdroppers.

Signal length = 1 sec

FFT Size = 20×10^6 (assuming 802.11 OFDM sampling rate)

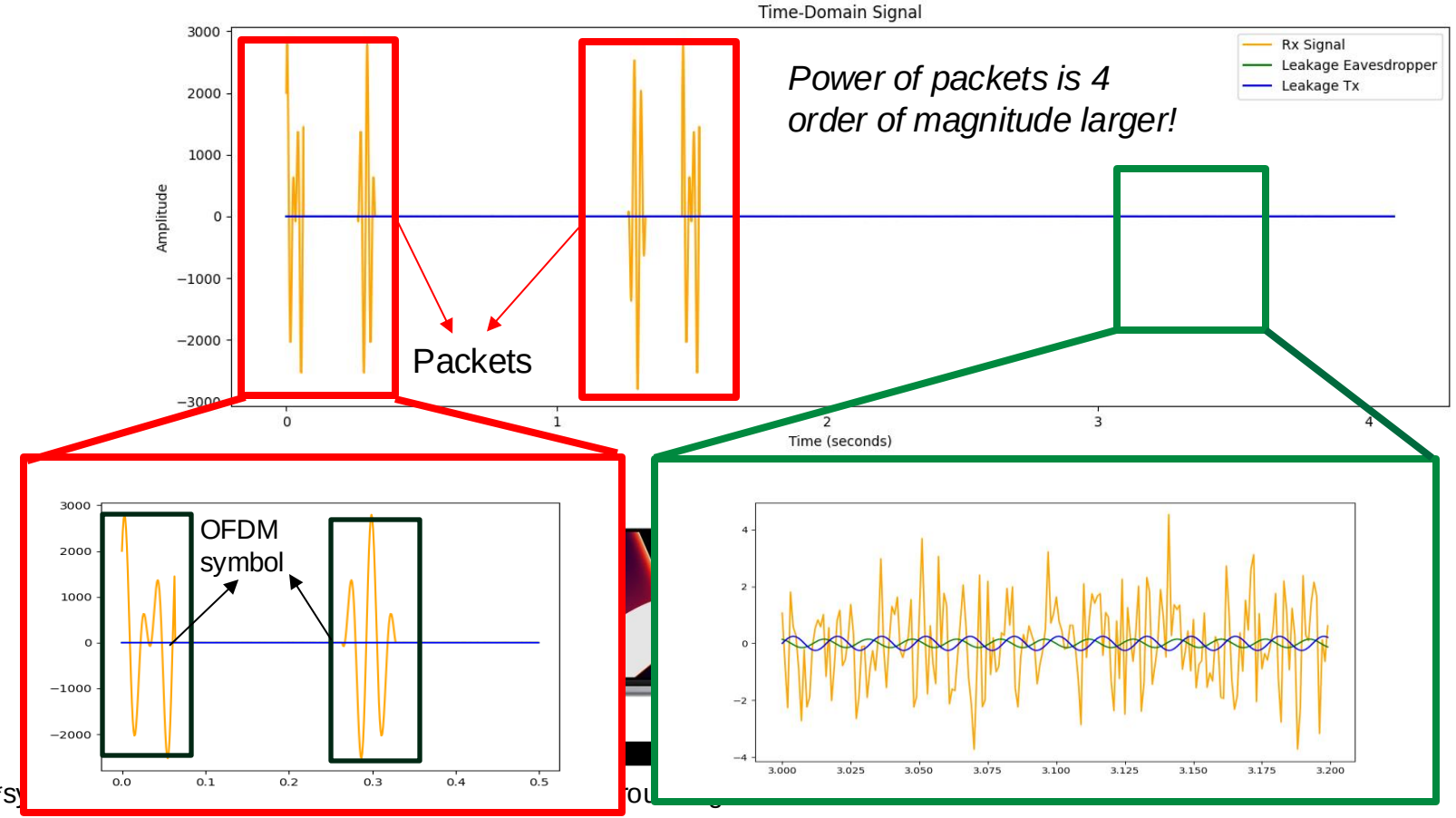
Ghostbuster Detection: Simplified Scenario II

Isolated System*

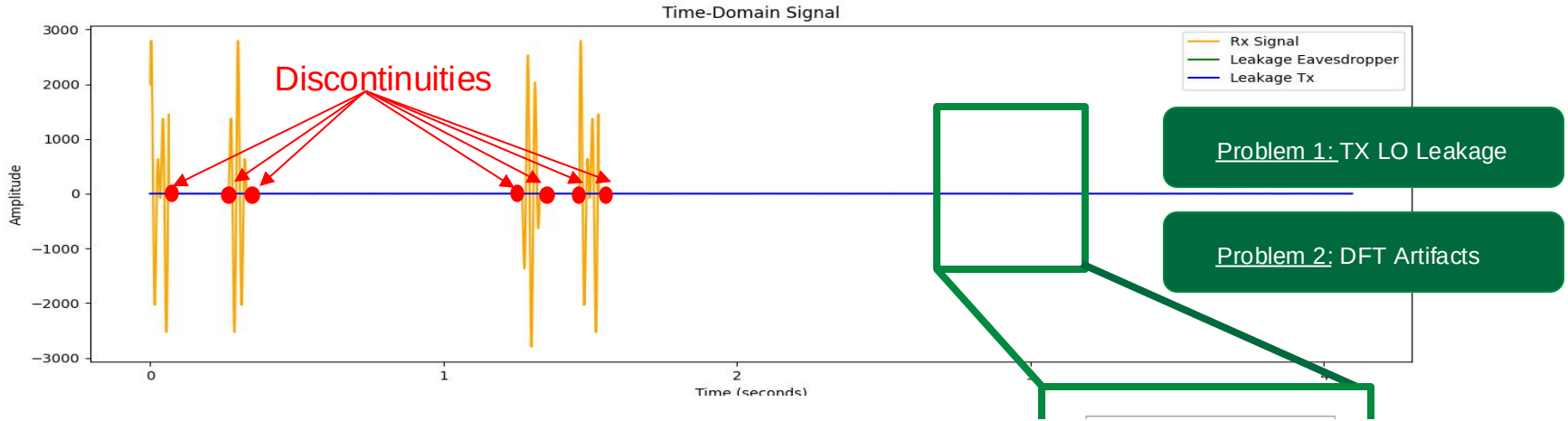
Tx

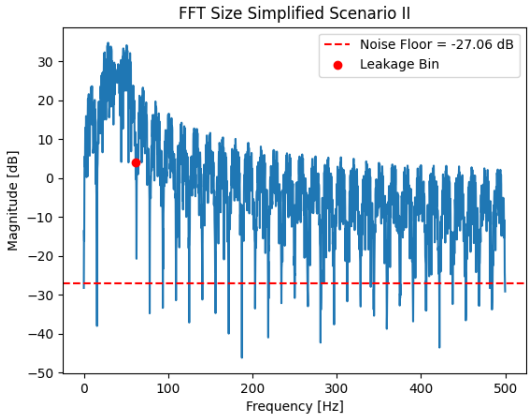
*system does not exchange matter or energy with surroundings

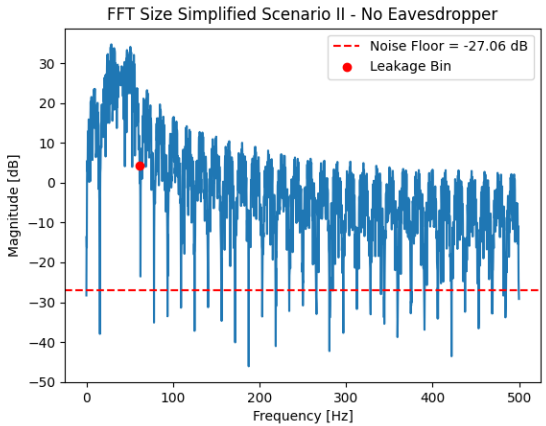
Ghostbuster Detection: Simplified Scenario II

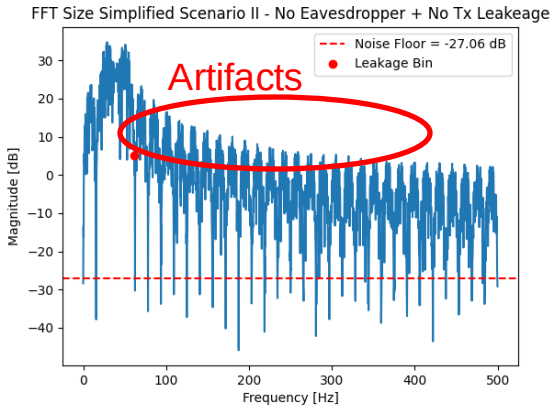


Ghostbuster Detection: Simplified Scenario II

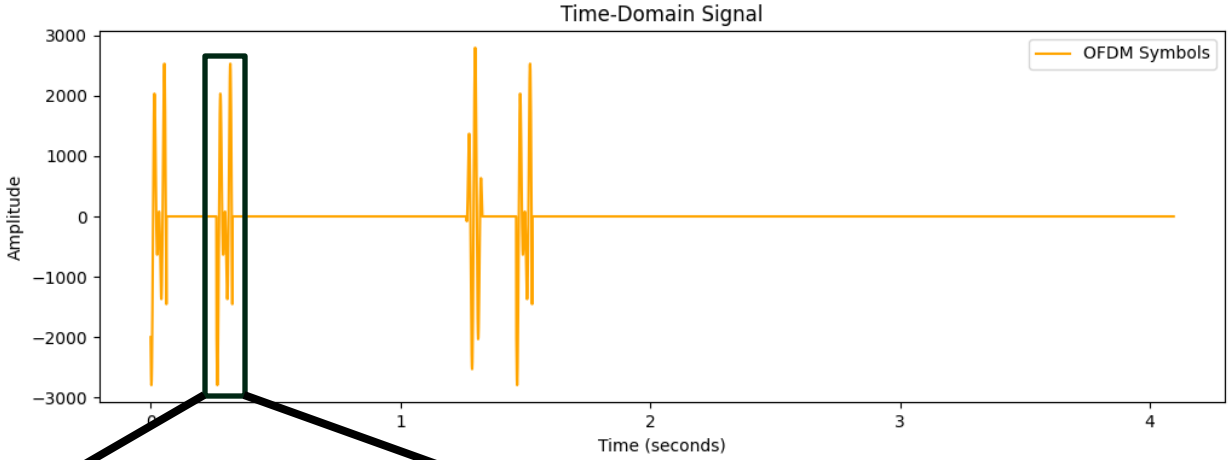


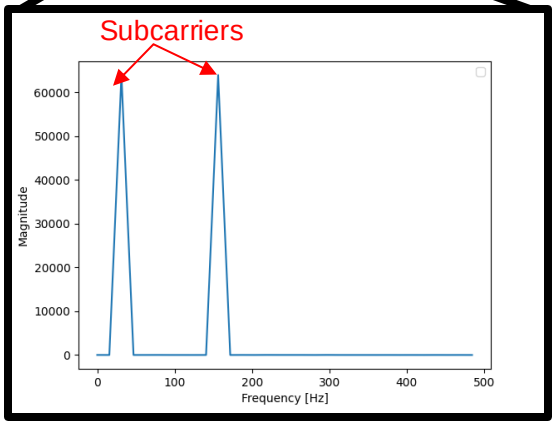






Ghostbuster Detection: Artifacts and Discontinuities





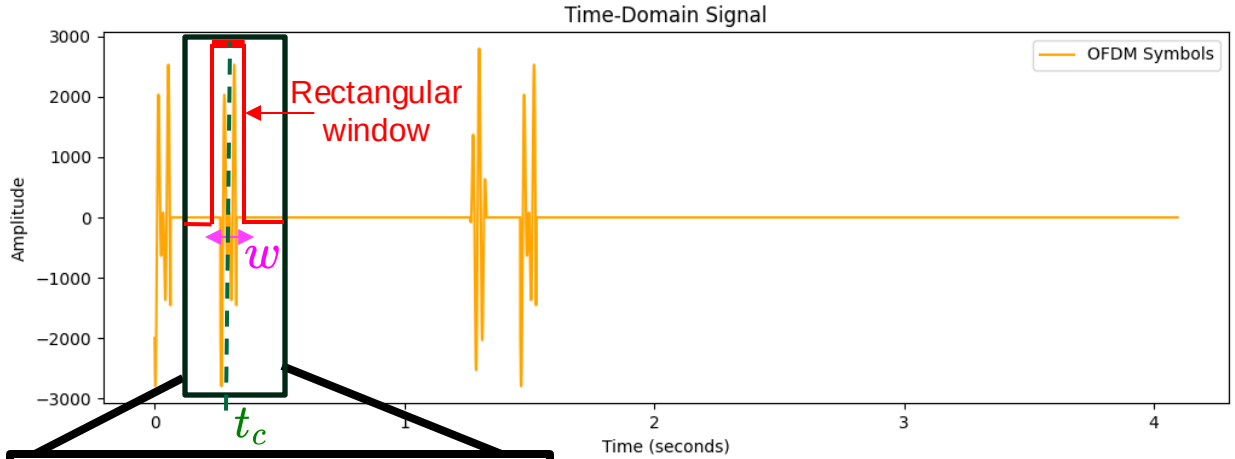
Frequency Domain

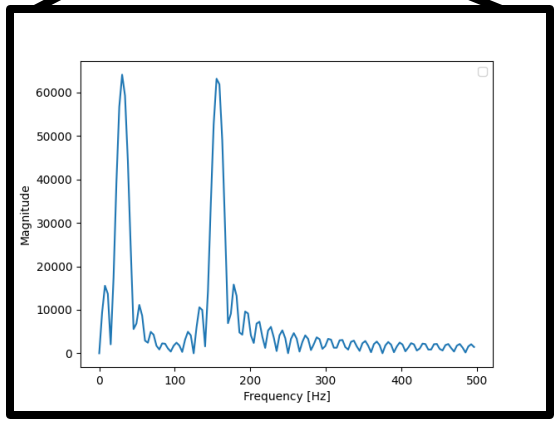
$$X[k] = \sum_{i=0}^{N} A_k \delta_{ik}$$

Subcarrier Amplitude

Kronecker Delta

Ghostbuster Detection: Artifacts and Discontinuities





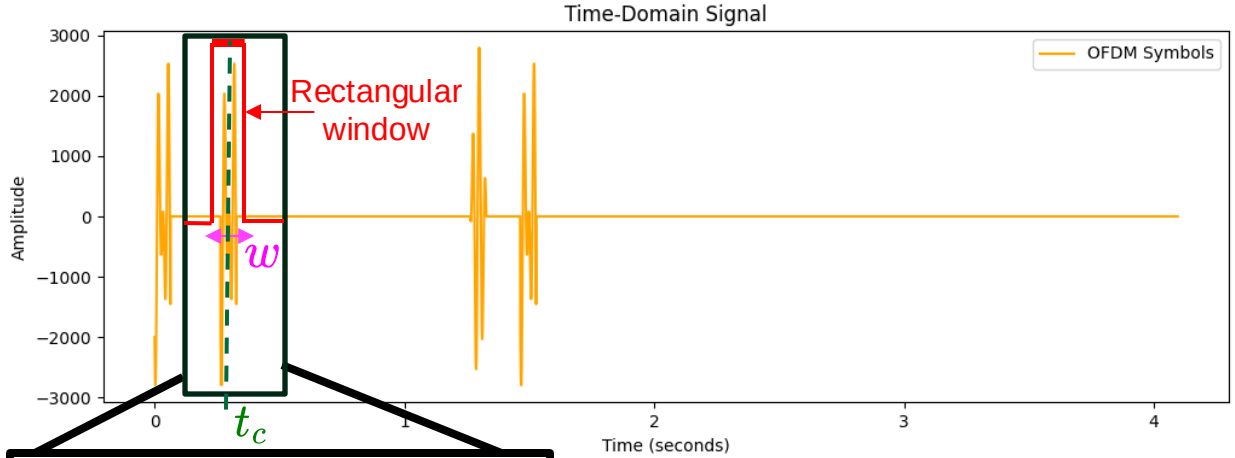
Time Domain $\longrightarrow$ $x[n] \cdot rect\left(\frac{n - t_c}{w}\right)$

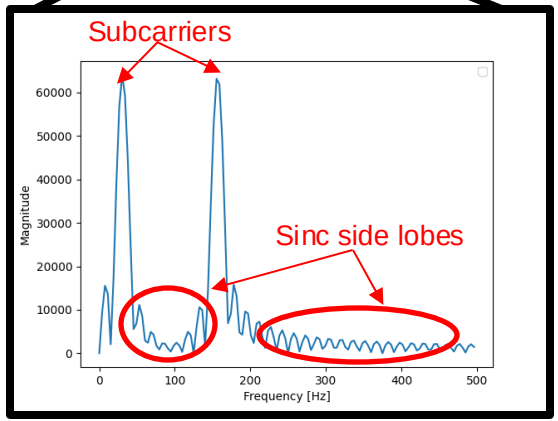
Frequency Domain $\longrightarrow$ $X[k] * D_{2w+1}[k]$

Sum of Kronecker Deltas

Dirichlet Kernel (Discrete sinc)

Ghostbuster Detection: Artifacts and Discontinuities





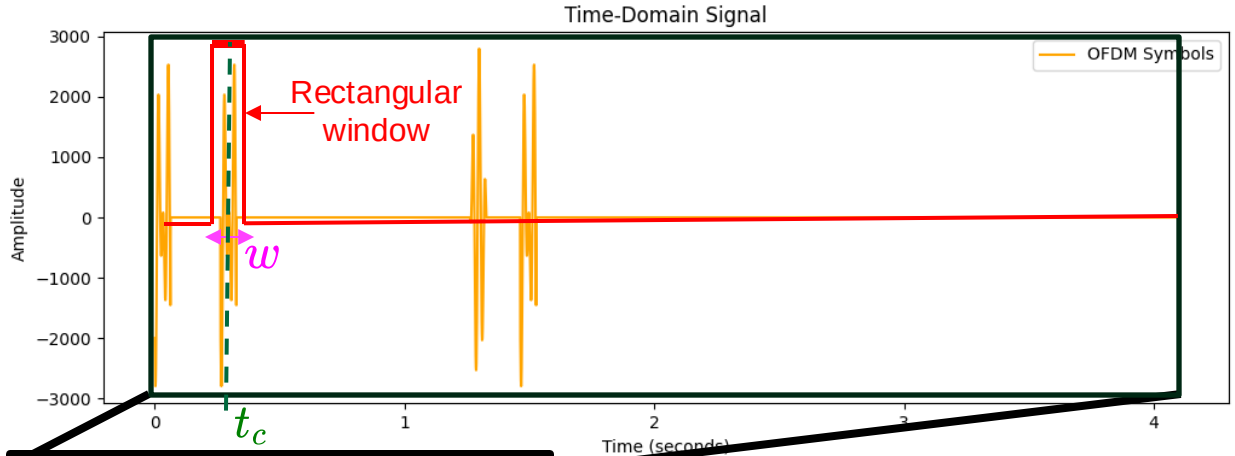
Time Domain → $x[n] \cdot rect\left(\frac{n - t_c}{w}\right)$

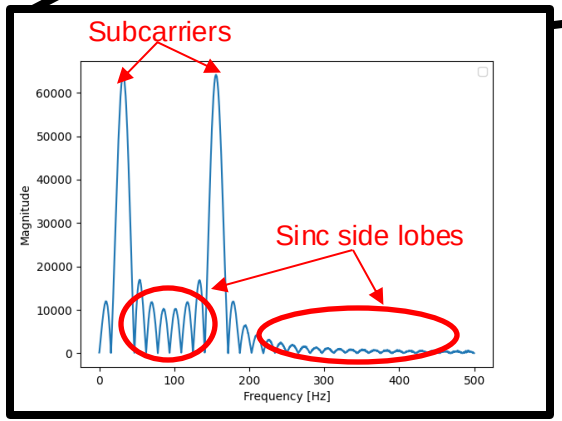
Frequency Domain → $\sum_{i=0}^{N} A_k D_{2w+1}[k - i]$

Subcarrier Amplitude

Dirichlet Kernel (Discrete sinc)

Ghostbuster Detection: Artifacts and Discontinuities





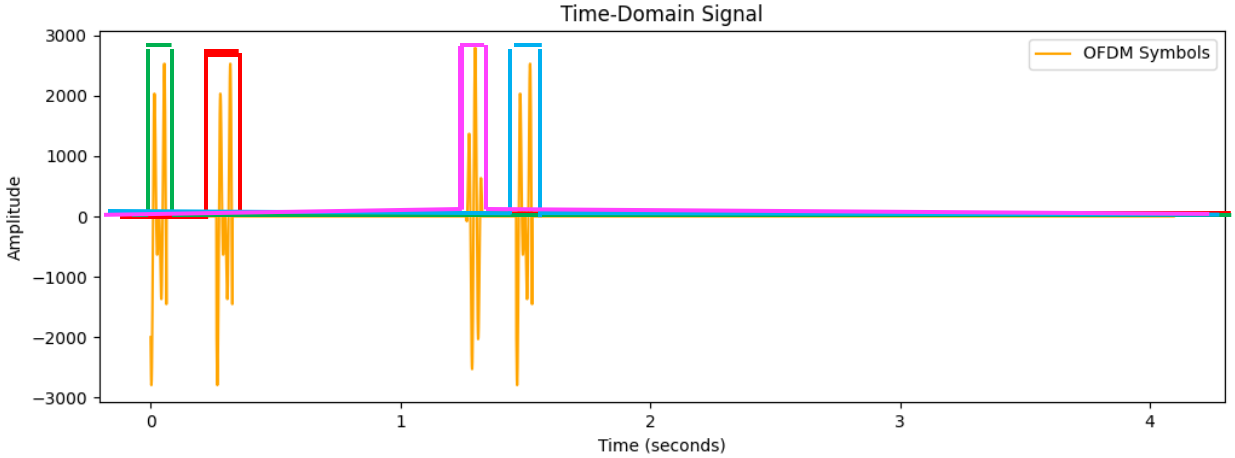
Time Domain $\longrightarrow$ $x[n] \cdot rect\left(\frac{n - t_c}{w}\right)$

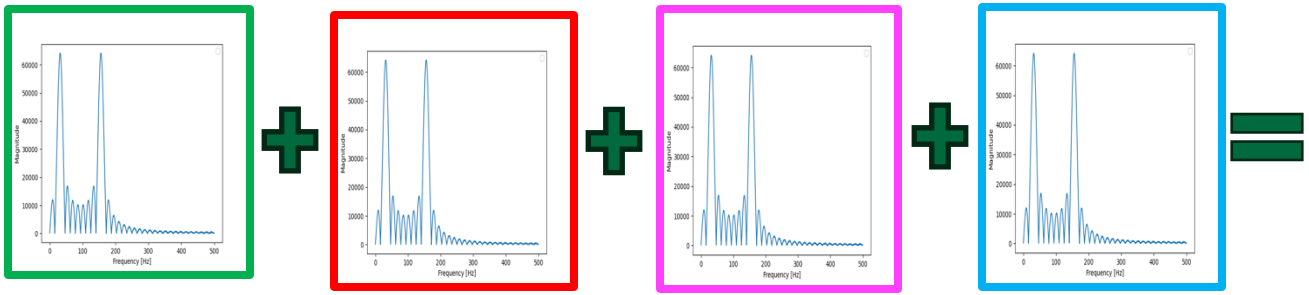
Frequency Domain $\longrightarrow$ $\sum_{i=0}^{N} A_k D_{2w+1}[k - i]$

Subcarrier Amplitude

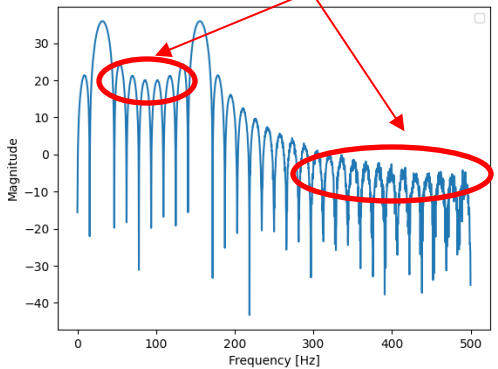
Dirichlet Kernel (Discrete sinc)

Ghostbuster Detection: Artifacts and Discontinuities





Sinc side lobes / Artifacts



Ghostbuster Detection: Simplified Scenario II

Isolated System*

Problem 1: TX LO Leakage

Problem 2: DFT Artifacts

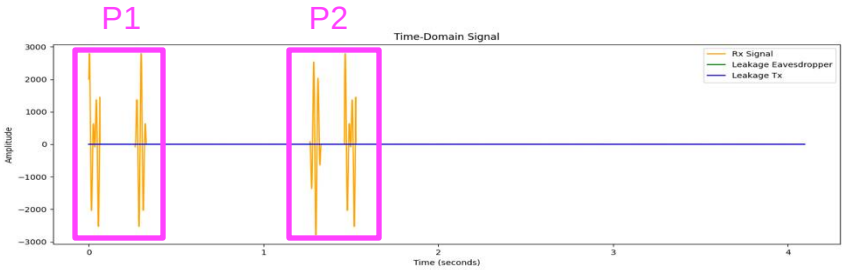
Tx

*system does not exchange matter or energy with surroundings

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.

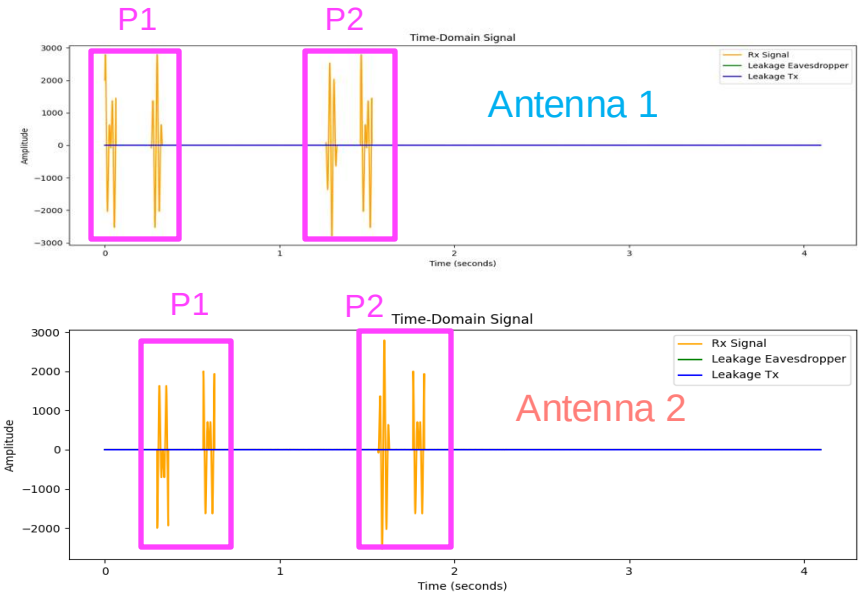


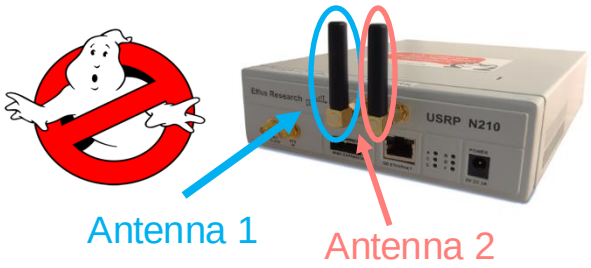
Easy! → **Ethernet Preamble**

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.

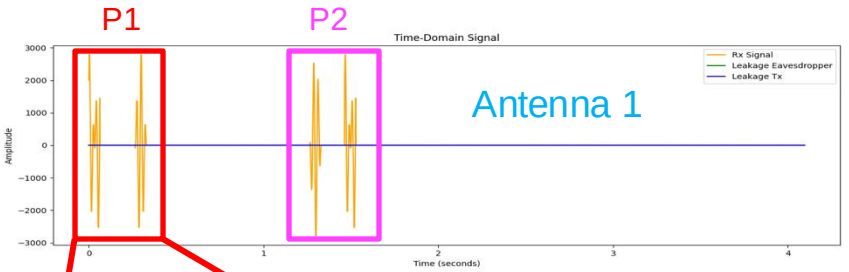


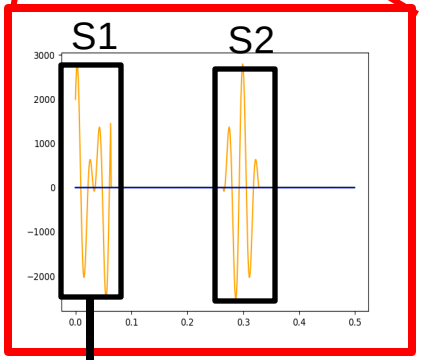


Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.





More steps to get bits

$$c_k = \frac{1}{N}\sum_{n=0}^{N-1} \hat{x}[n] e^{-2\pi i \frac{n f_k}{N}}$$

Corrected Signal

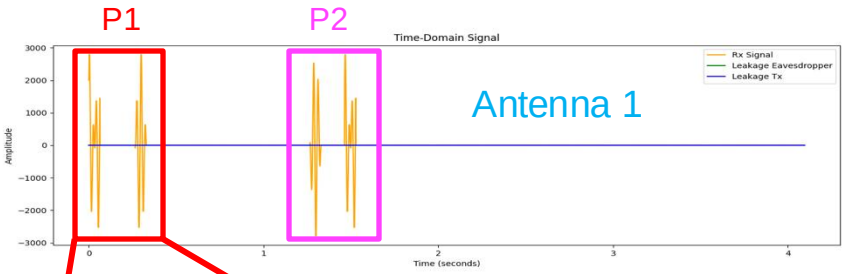
CFO Correction

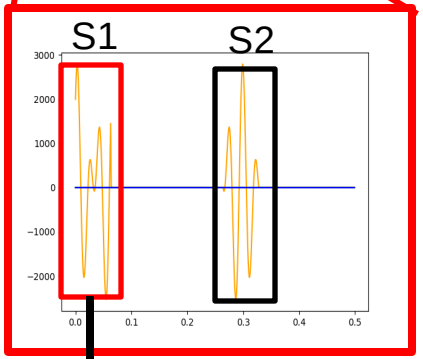
CP Removal

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

```
for k^th packet do
    for m^th MIMO Receiver do
        Decode packet using standard OFDM decoder.
        for Each OFDM Symbol do
            f^(0) ← CFO coarse & fine estimates
            i ← 1
            while E(f̃^(i−1), ã^(i−1)) ≥ Threshold do
                ã^(i) ← WeightedLeastSq(f̃^(i−1), x_m(t))
                f̃^(i) ← GradientDescent(ã^(i), x_m(t))
                i ← i + 1
            end while
            x̃_m(t) ← ã*, f̃* (other than the DC bin)
            r_m(t) ← x_m(t) − x̃_m(t)
        end for
        p_m(t) ← combination of r_m(t) from all symbols
        P_m(f) ← FFT(p_m(t))
        H_m(f_DC) ← P_m(f_DC)
    end for
    s_k(t) ← spatial cancellation using each H_m(f_DC)
end for
s(t) ← combination of s_k(t) from all packets
S(f) ← FFT(s(t))
Find spike of eavesdropper's RF leakage.
```





Only OFDM symbol (no leakage):

$$x(t) = \sum_{k=0}^{N-1} a_k e^{j2\pi f_k t/N}$$

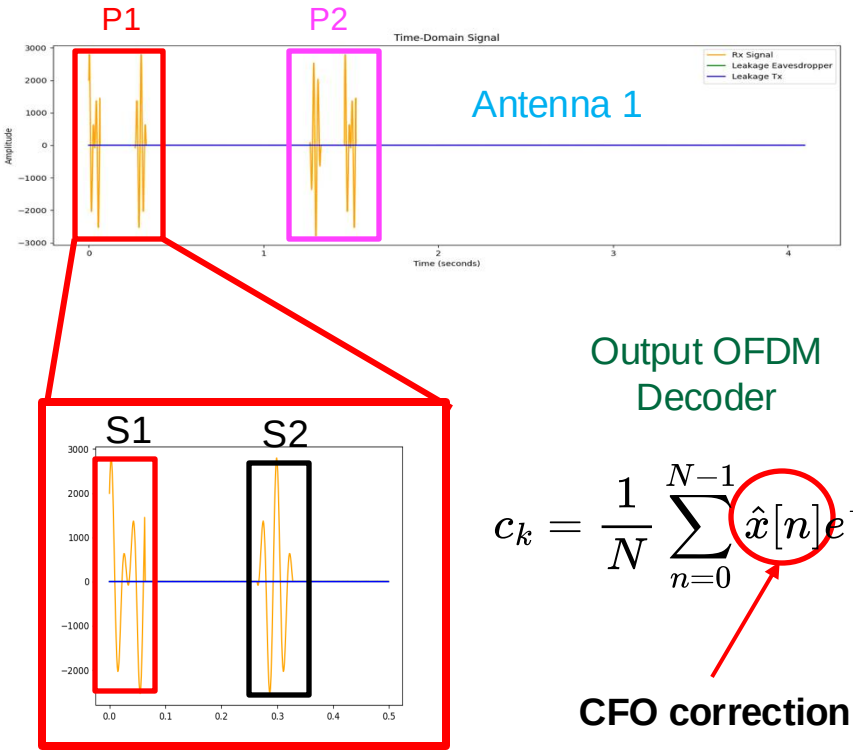
Fourier Decomposition

$$c_k = \frac{1}{N} \sum_{n=0}^{N-1} \hat{x}[n] e^{-2\pi i \frac{n f_k}{N}}$$

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.



Output OFDM Decoder

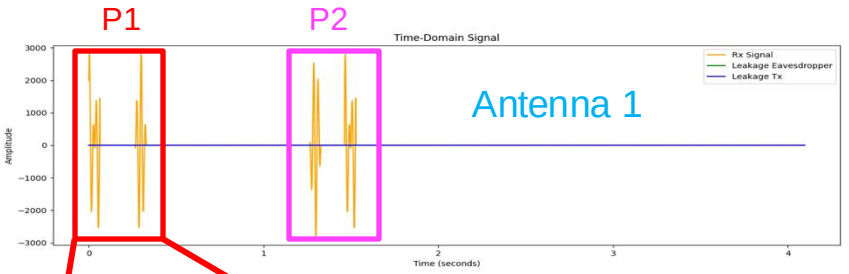
$$c_k = \frac{1}{N} \sum_{n=0}^{N-1} \hat{x}[n] e^{-2\pi i \frac{n f_k}{N}}$$

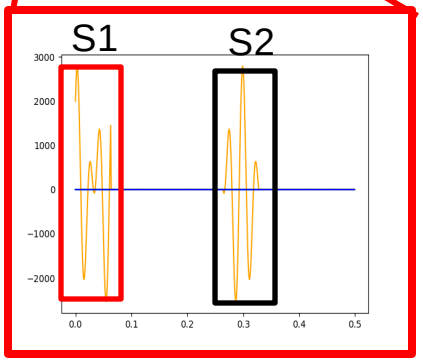
CFO correction

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\mathbf{f}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.





Output OFDM Decoder

$$c_k = \frac{1}{N}\sum_{n=0}^{N-1} x[n] e^{-2\pi i \frac{n f_k}{N}}$$

$$f_k = \frac{N(f_{subcarrier} + f_{CFO})}{F_s}$$

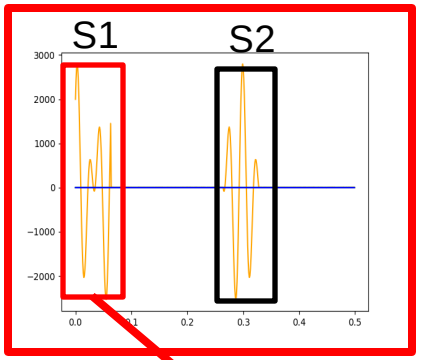
Good enough for data recovery!

Not good for Accurate Fourier Reconstruction!

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\mathbf{f}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Only OFDM symbol (no leakage):

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

Best Estimates

Error function (SSE):

$$E(\tilde{\mathbf{a}}, \tilde{\mathbf{f}}) = \sum_{t=0}^{N-1} |x(t) - \tilde{x}(t)|^2$$

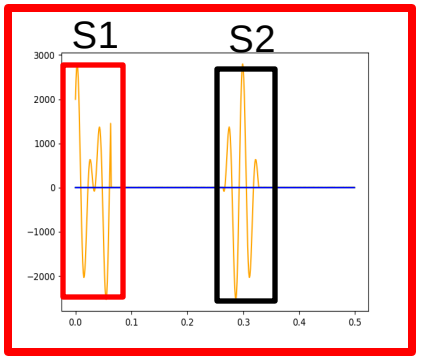
Minimize

$$\nabla E = 0$$
$$\nabla^2 E > 0$$

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Only OFDM symbol (no leakage):

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

Best Estimates

Error function (SSE):

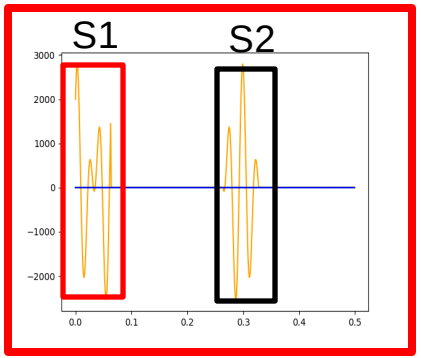
$$E(\tilde{\mathbf{a}}, \tilde{\mathbf{f}}) = \sum_{t=0}^{N-1} |x(t) - \tilde{x}(t)|^2$$

Initialize $\tilde{\mathbf{f}}$ $\longrightarrow$ $\tilde{f}_k = \dfrac{N(f_{subcarrier} + f_{CFO})}{F_s}$

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) >$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Only OFDM symbol (no leakage):

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

Best Estimates

Error function (SSE):

$$E(\tilde{\mathbf{a}}, \tilde{\mathbf{f}}) = \sum_{t=0}^{N-1} |x(t) - \tilde{x}(t)|^2$$

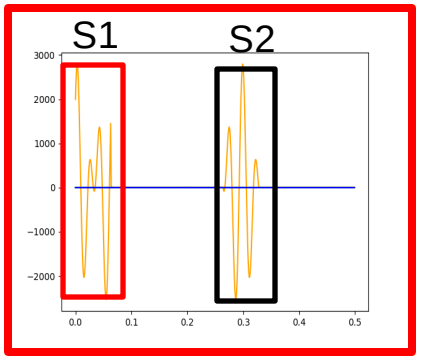
Initialize $\tilde{\mathbf{f}}$ → $\tilde{f}_k = \dfrac{N(f_{subcarrier} + f_{CFO})}{F_s}$

Solve for $\tilde{\mathbf{a}}$ (fixed $\tilde{\mathbf{f}}$) → $\dfrac{1}{N} \sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N}$

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Only OFDM symbol (no leakage):

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

Best Estimates

Error function (SSE):

$$E(\tilde{\mathbf{a}}, \tilde{\mathbf{f}}) = \sum_{t=0}^{N-1} |x(t) - \tilde{x}(t)|^2$$

Gradient Descent

Update $\tilde{\mathbf{f}}$

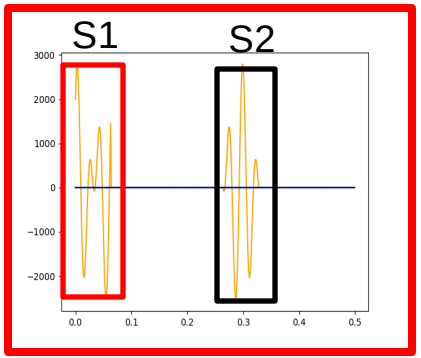
Solve for $\tilde{\mathbf{a}}$ (fixed $\tilde{\mathbf{f}}$) $\longrightarrow$ $\frac{1}{N} \sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N}$

Solve for $\frac{\partial E}{\partial \tilde{\mathbf{f}}}$

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Only OFDM symbol (no leakage):

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

Best Estimates

Error function (SSE):

$$E(\tilde{\mathbf{a}}, \tilde{\mathbf{f}}) = \sum_{t=0}^{N-1} |x(t) - \tilde{x}(t)|^2$$

Update $\tilde{\mathbf{f}}$

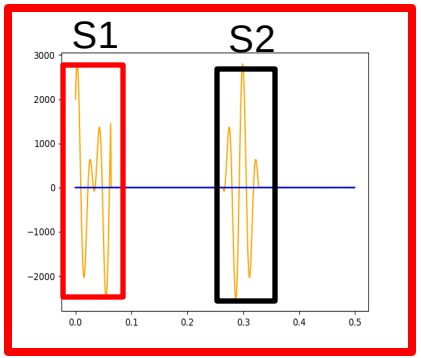
Solve for $\tilde{\mathbf{a}}$ (fixed $\tilde{\mathbf{f}}$)

$$\frac{1}{N} \sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N}$$

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \mathbf{f}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Only OFDM symbol (no leakage):

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

Best Estimates

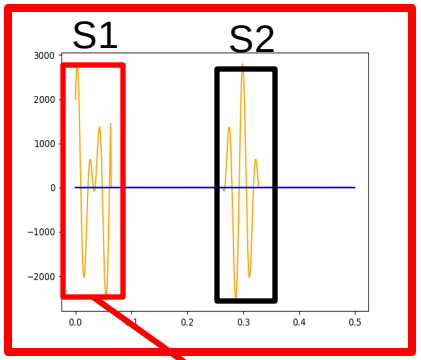
Remove DC bin from $\tilde{x}(t)$ (i.e., $\tilde{a}_0$):

- Represents NULL subcarrier (i.e., has no data)
- Contains Tx and Eavesdropper Leakage

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Only OFDM symbol (no leakage):

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

Best Estimates

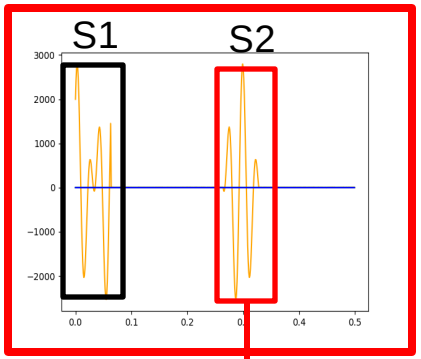
$$r(t) = x_i(t) - \tilde{x}_i(t)$$

Only LO leakages in S1

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $F(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow \text{WeightedLeastSq}(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow \text{GradientDescent}(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Only OFDM symbol (no leakage):

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

Best Estimates

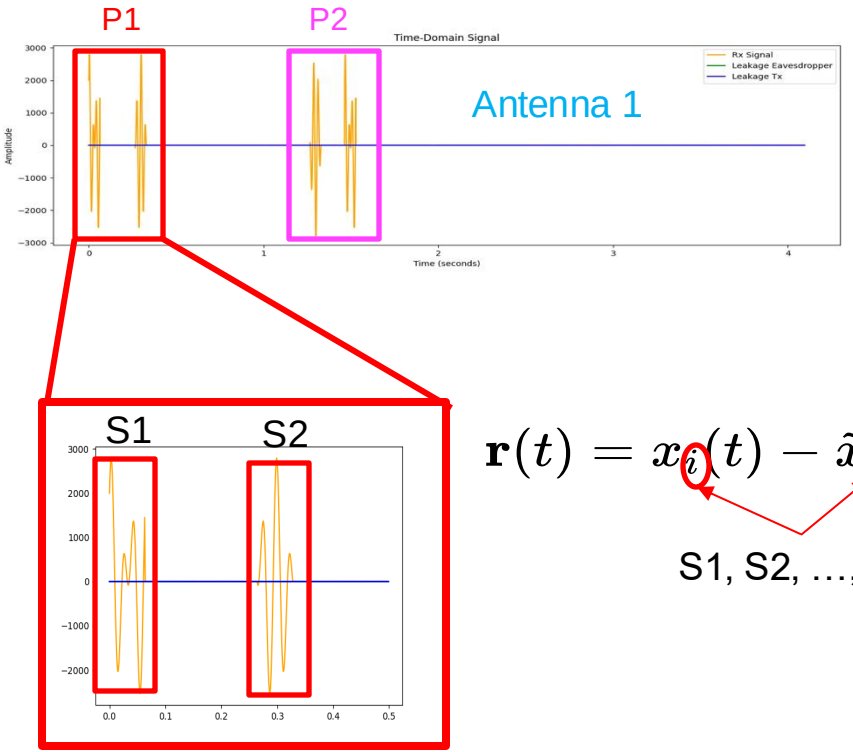
$$r(t) = x_i(t) - \tilde{x}_i(t)$$

Only LO leakages in S2

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.



$$\mathbf{r}(t) = x_i(t) - \tilde{x}_i(t)$$

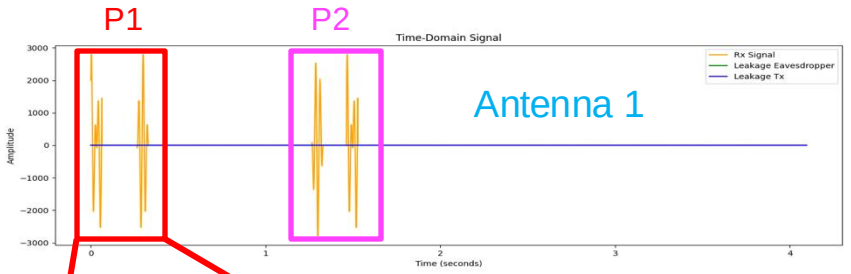
S1, S2, …, SN

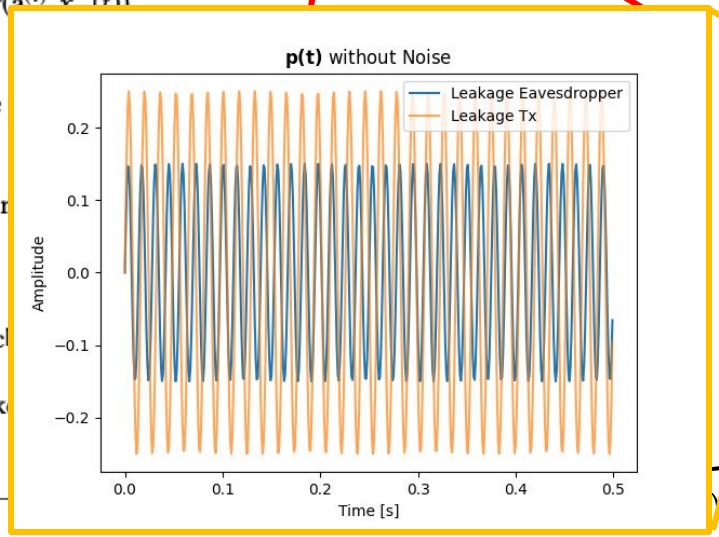
$$p(t) = [r_{S1}(t), r_{S2}(t), \ldots, r_{SN}(t)]$$

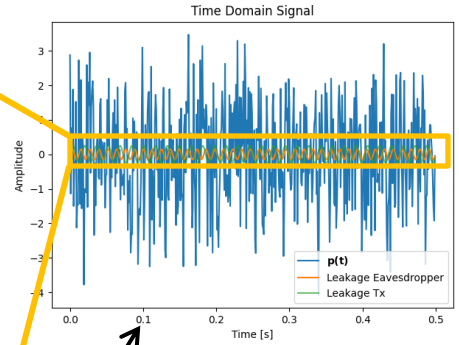
Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ fror
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using eacl
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all pack
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.





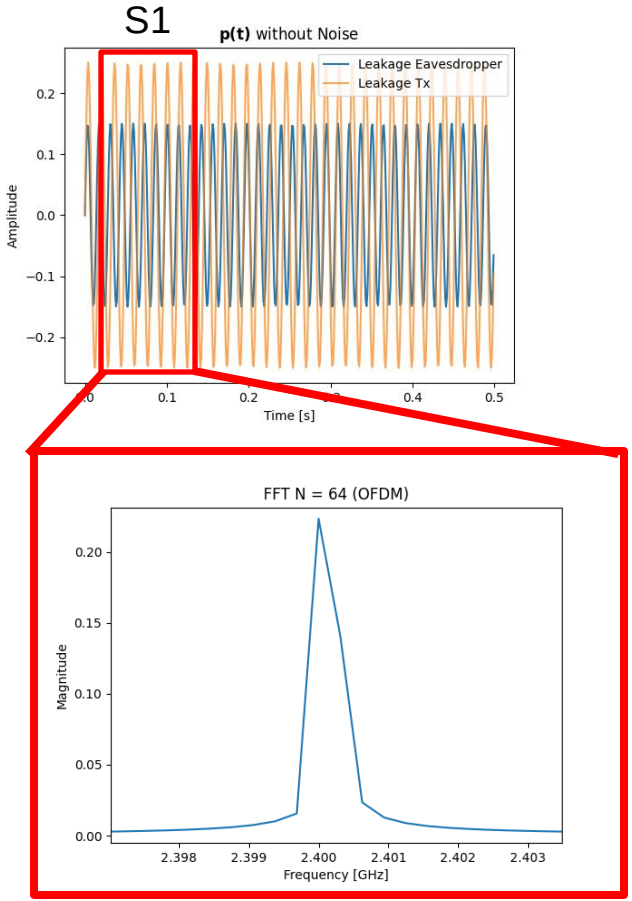


$\ldots, r_{S2}(t), \ldots, r_{SN}(t)]$

Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

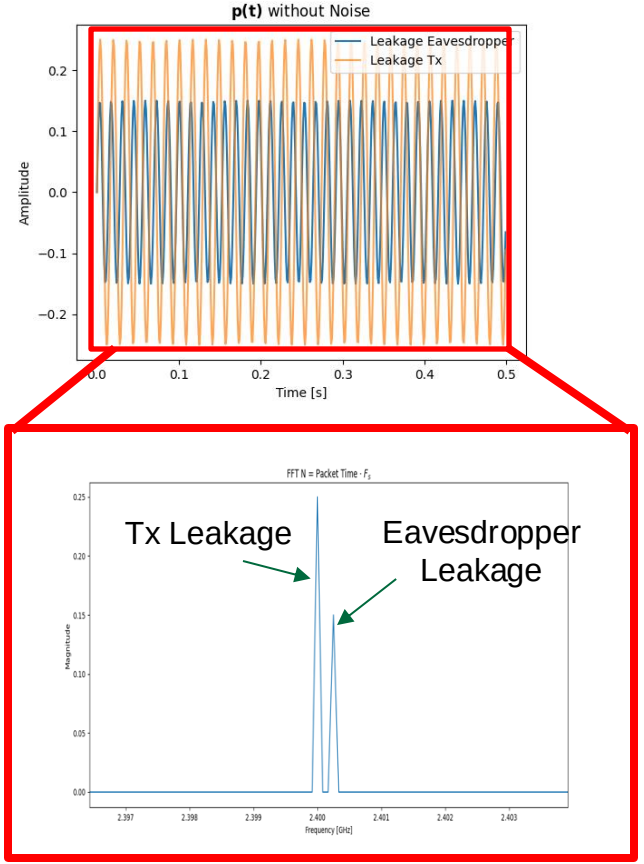
1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow \text{WeightedLeastSq}(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow \text{GradientDescent}(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.

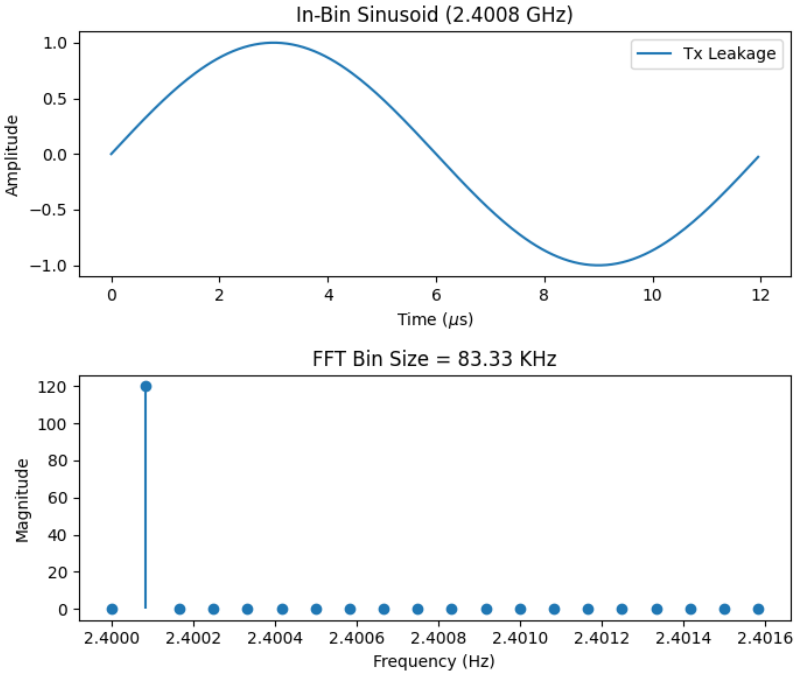


Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $F(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow \text{WeightedLeastSq}(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow \text{GradientDescent}(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.

"in-bin" sinusoid

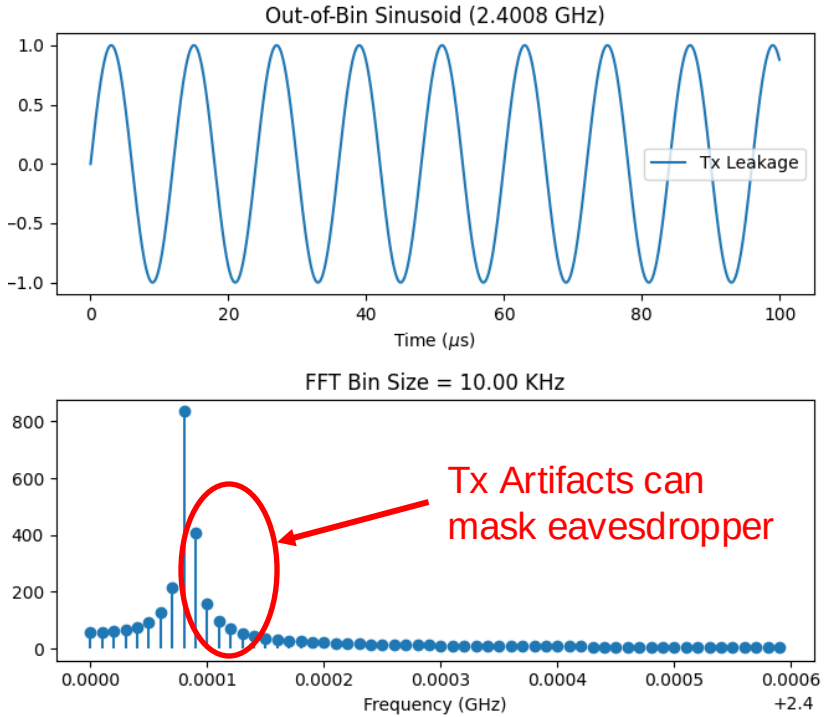


Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow \text{WeightedLeastSq}(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow \text{GradientDescent}(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.

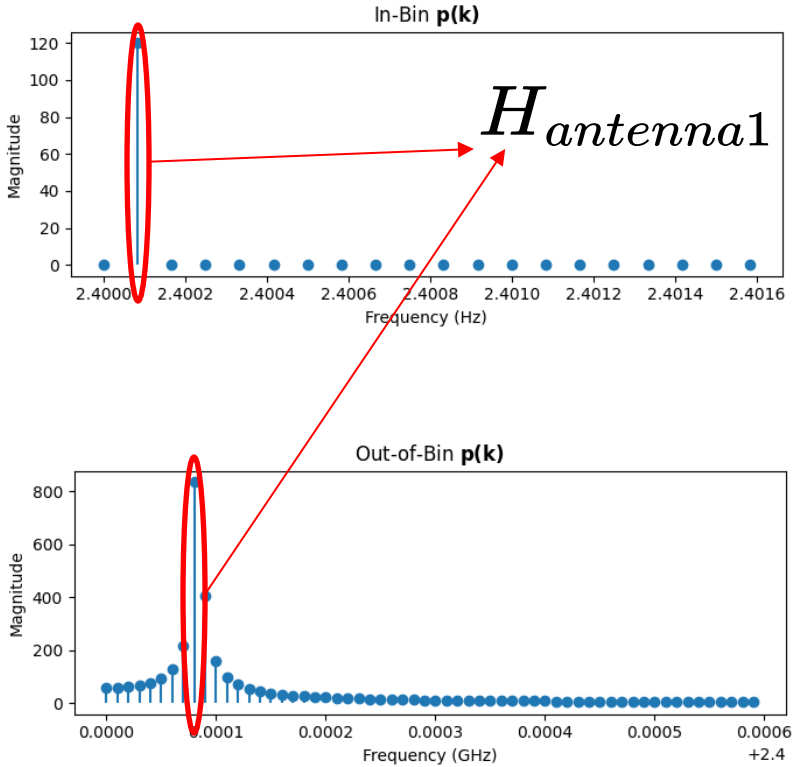
"out-of-bin" sinusoid



Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

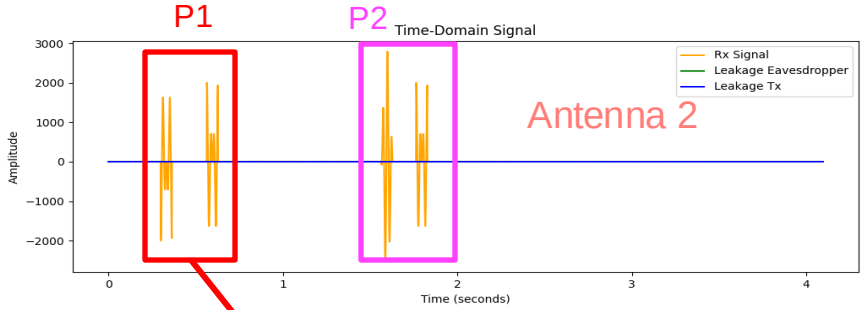
1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow \textsc{WeightedLeastSq}(\tilde{\mathbf{f}}^{(i\ 1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow \textsc{GradientDescent}(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



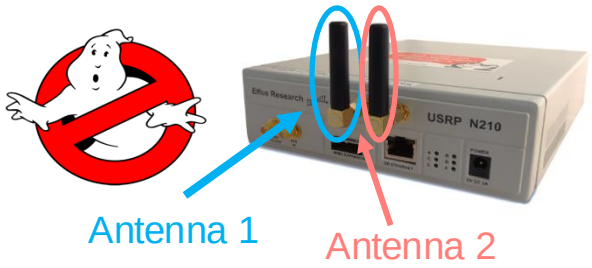
Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



$H_{antenna2}$



Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.

Only **Eavesdropper** signal!

$$Y_1(f) - \frac{H_{antenna1}}{H_{antenna2}} Y_2(f) = CE(f)$$

FFT

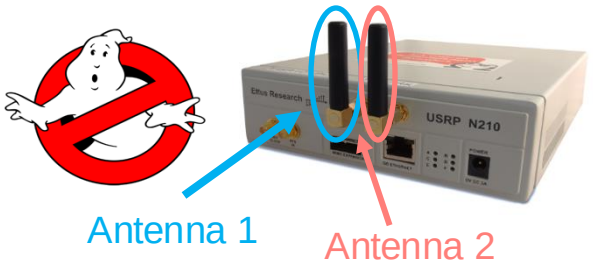
FFT

$p(t) = [r_{S1}(t), r_{S2}(t), \ldots, r_{SN}(t)]$

Antenna 1

$p(t) = [r_{S1}(t), r_{S2}(t), \ldots, r_{SN}(t)]$

Antenna 2



Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

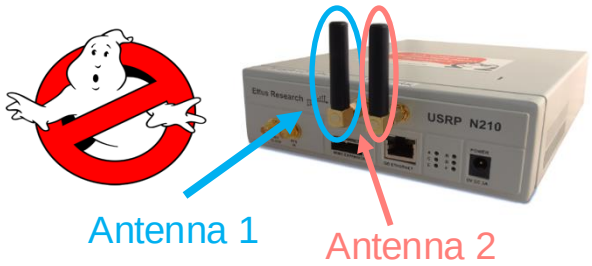
1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.

Only **Eavesdropper** signal!

$$Y_1(f) - \frac{H_{antenna1}}{H_{antenna2}} Y_2(f) = CE(f)$$

IFFT

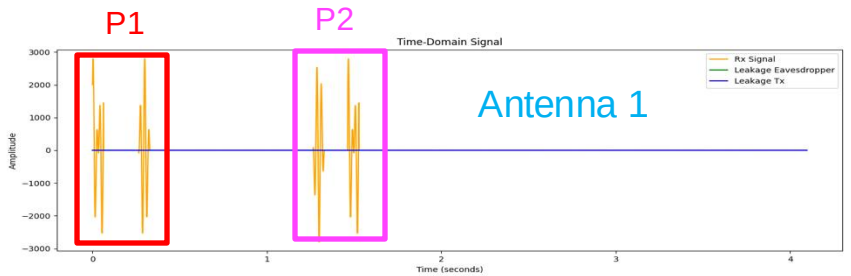
s_1

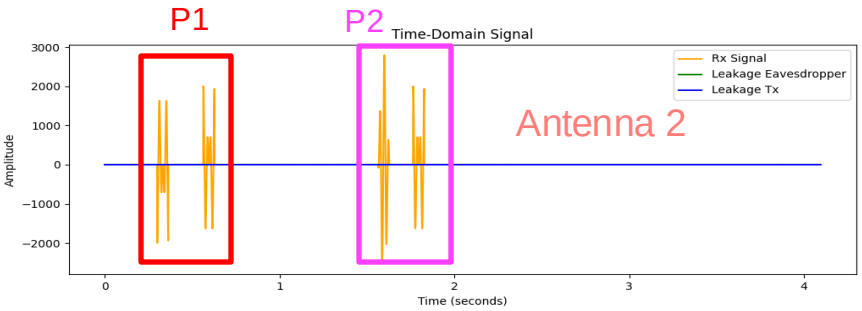


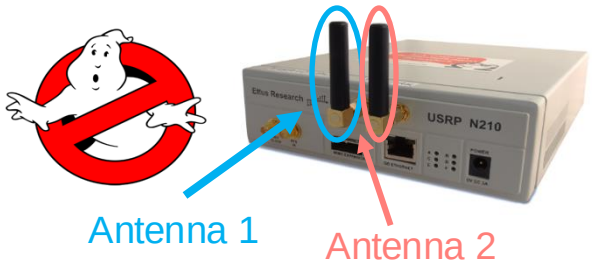
Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.



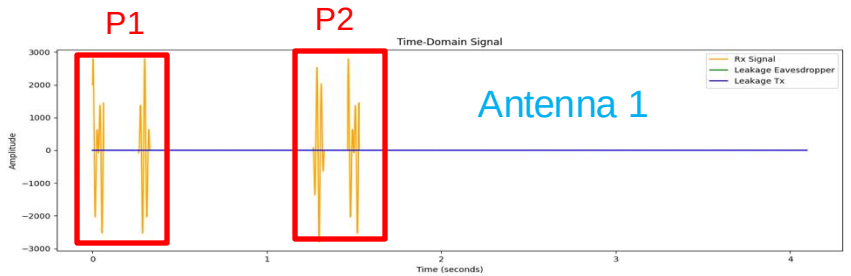


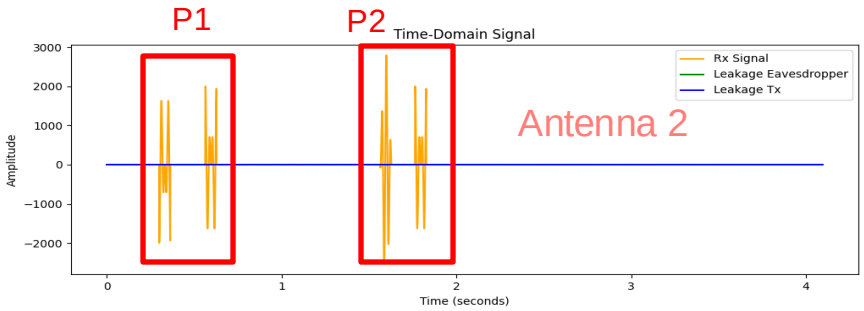


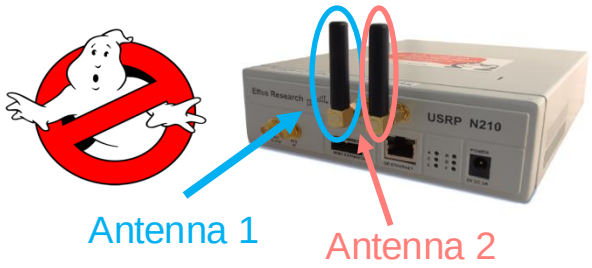
Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.



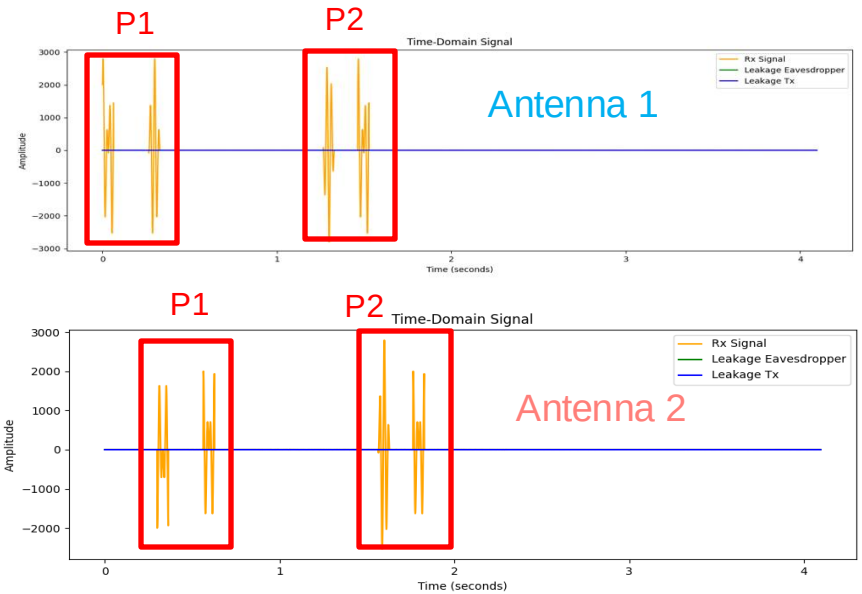




Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.



$$\mathbf{s} = [s_1, s_2, \ldots, s_i]$$

Only **Eavesdropper** Leakage!

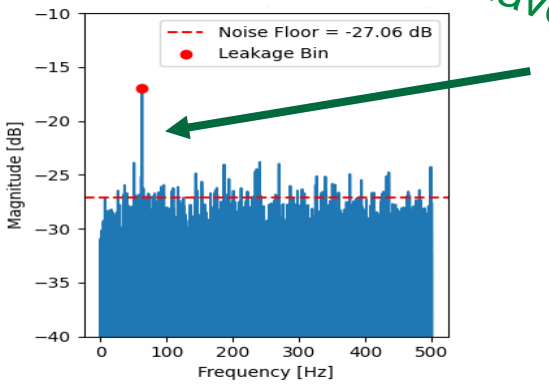
Ghostbuster Detection: The Algorithm

Algorithm 1 Ghostbuster's Cancellation Algorithm

1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.

$$\mathbf{s} = [s_1, s_2, \ldots, s_i]$$

FFT



Eavesdropper!

Ghostbuster Detection: Simplified Scenario II

Isolated System*

Key Observation 1

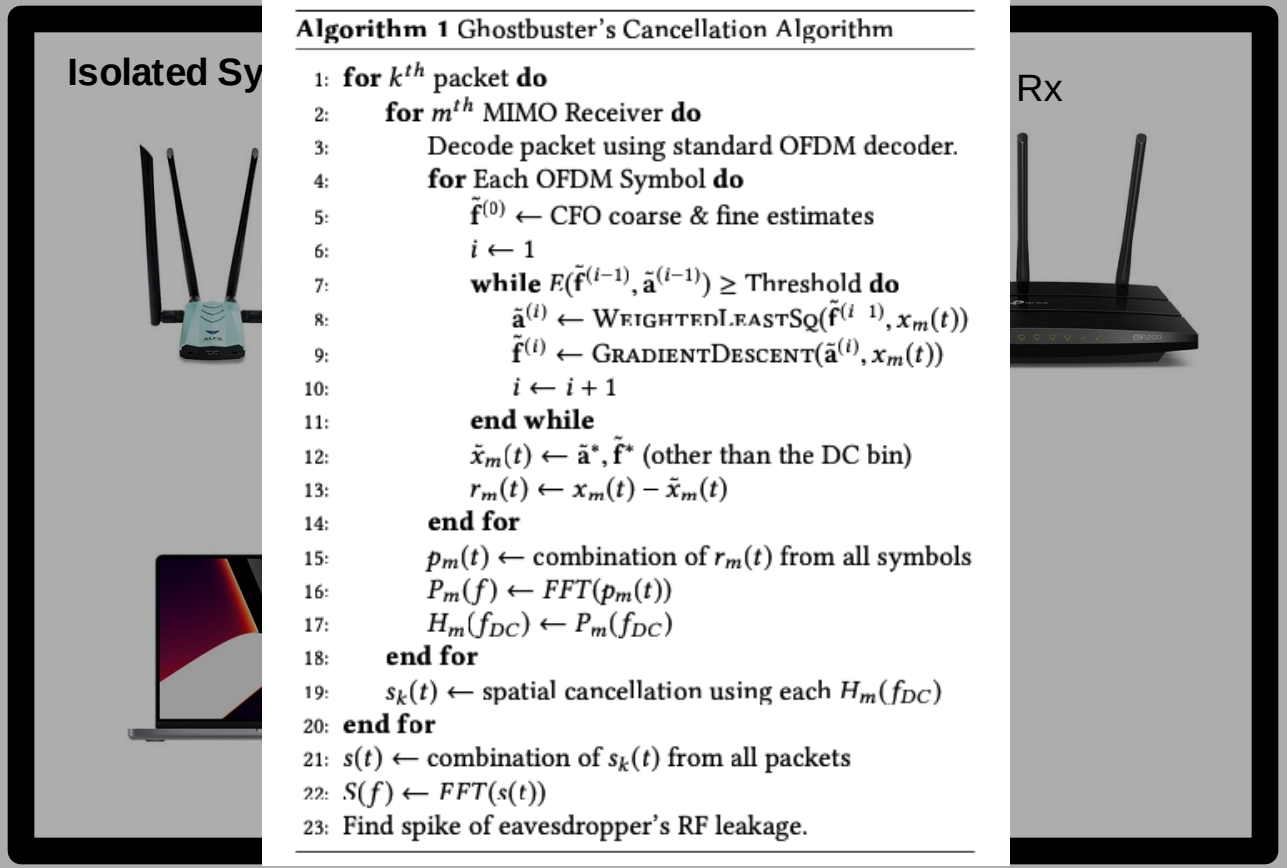
Ghostbuster computes long FFTs to bring leaked signal above the noise floor

Key Observation 2

DFT artifacts (found in long DFTs) can be eliminated through Spatial & Frequency Cancellation

*system does not exchange matter or energy with surroundings

Ghostbuster Detection: Realistic Scenario



Algorithm 1 Ghostbuster's Cancellation Algorithm

for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $F(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow \textsc{WeightedLeastSq}(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow \textsc{GradientDescent}(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.

*system does not exchange matter or energy with surroundings

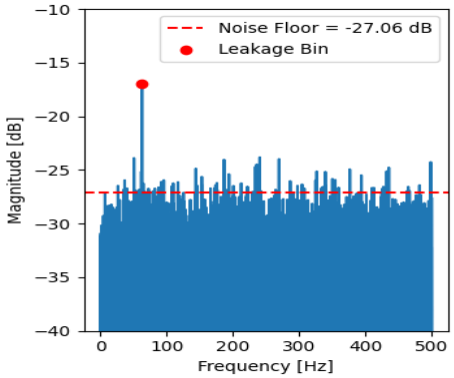
Ghostbuster Detection: Realistic Scenario

Algorithm 1 Ghostbuster's Cancellation Algorithm

for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $E(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.

$$\mathbf{s} = [s_1, s_2, \ldots, s_i]$$

FFT



Count Num Peaks:

$$N_{legitimate\_recv} = N_{peaks}$$

NO Eavesdropper!

$$N_{legitimate\_recv} \neq N_{peaks}$$

Eavesdropper!

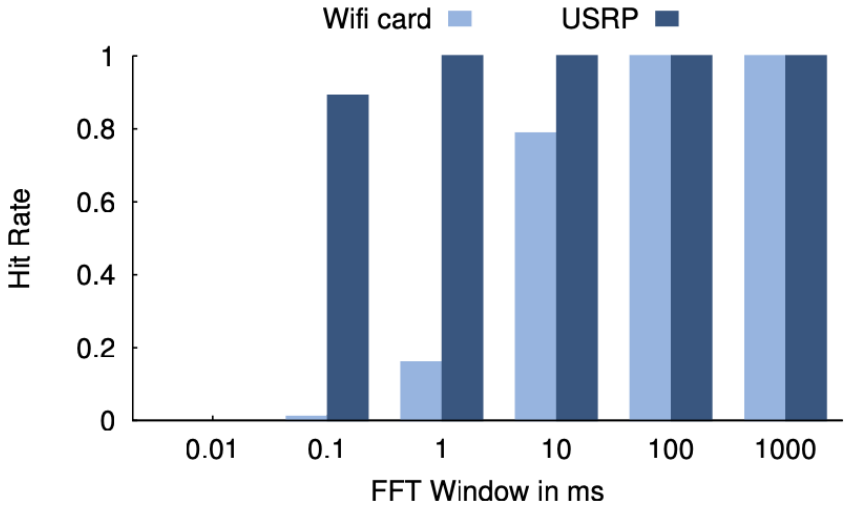
Ghostbuster Implementation

- USRPN210 SDR
- NO-MIMO, 2-MIMO, 3-MIMO, 4-MIMO
- Detection if SNR per bin > 6 dB

Ghostbuster Evaluation: Only Eavesdropper

- **Eavesdropper**: MacBook Pro in monitor mode and USRP N210.
- **Frequency Carrier**: 5.745 GHz (Channel 149).

- Eavesdroppers placed **1 m** from Ghostbuster.



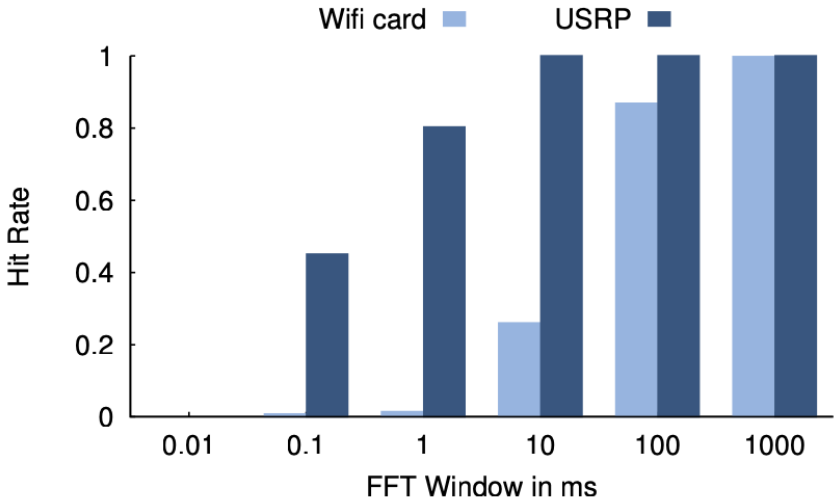
SNR > 6dB

$$Hit\ Rate = \frac{\#\ runs\ with\ correct\ detection}{total\ \#\ runs\ eavesdropper\ present}$$

Ghostbuster Evaluation: Only Eavesdropper

- **Eavesdropper**: MacBook Pro in monitor mode and USRP N210.
- **Frequency Carrier**: 5.745 GHz (Channel 149).

- Eavesdroppers placed **5 m** from Ghostbuster.



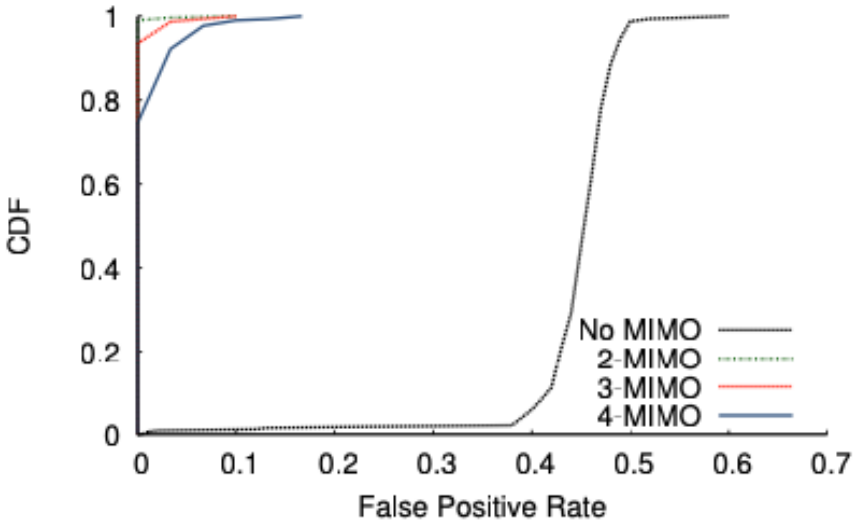
SNR > 6dB

$$Hit\ Rate = \frac{\#\ runs\ with\ correct\ detection}{total\ \#\ runs\ eavesdropper\ present}$$

Ghostbuster Evaluation: Eavesdropper and Tx

- **Tx:** USRP N210 transmitting ODFM Wi-Fi packets
- **Eavesdropper**: USRP N210 and MacBook Pro in monitor mode?

- **FFT Length:** 5 ms
- Eavesdropper placed at 350 different location between 1m - 5m from GB.

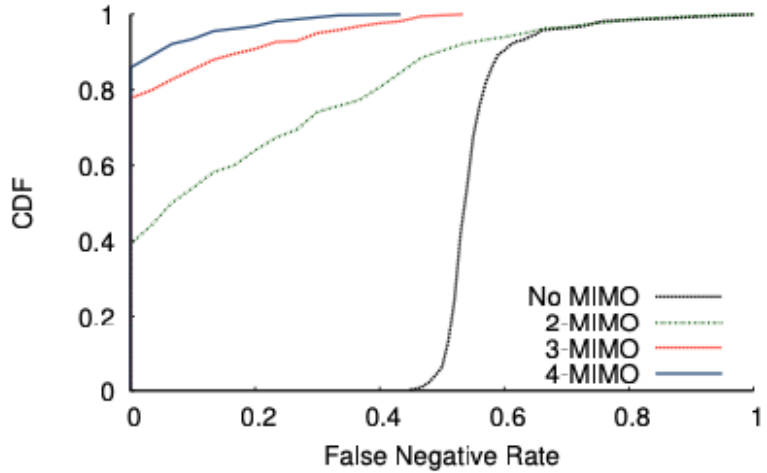


$$FPR = \frac{\#\ runs\ eavesdropper\ falsy\ detected}{total\ \#\ runs\ eavesdropper\ NOT\ present}$$

Ghostbuster Evaluation: Eavesdropper and Tx

- **Tx:** USRP N210 transmitting ODFM Wi-Fi packets
- **Eavesdropper**: USRP N210 and MacBook Pro in monitor mode?

- **FFT Length:** 5 ms
- Eavesdropper placed at 350 different location between 1m - 5m from GB.

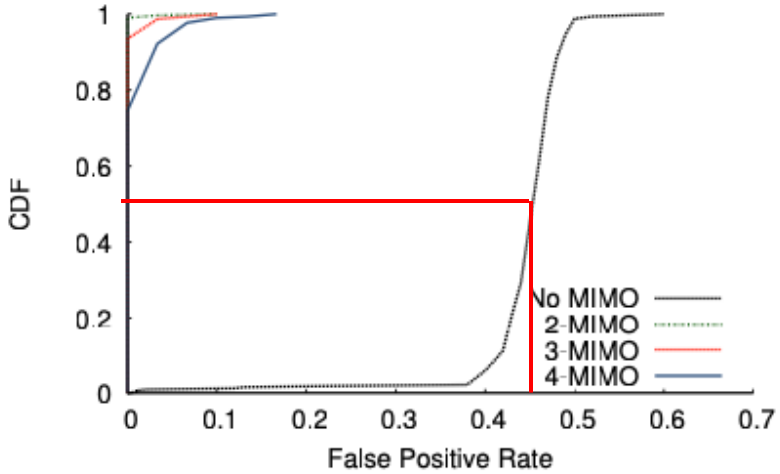


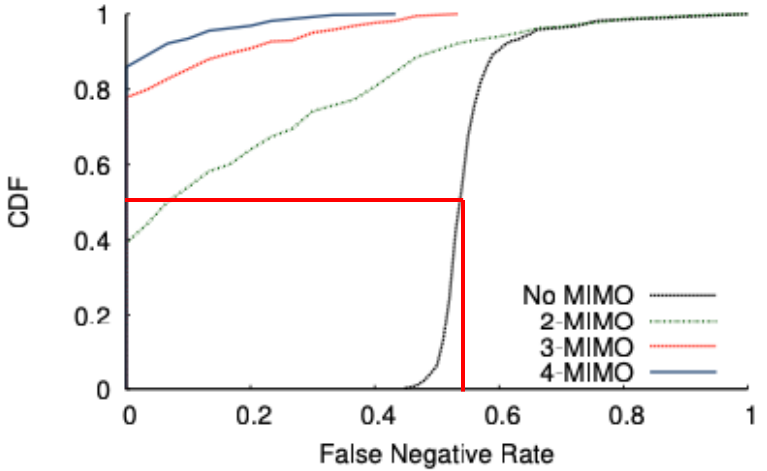
$$FNR = \frac{\#\ runs\ failed\ to\ detect\ eavesdropper}{total\ \#\ runs\ eavesdropper\ present}$$

Ghostbuster Evaluation: Eavesdropper and Tx

$$FPR = \frac{\#\ runs\ eavesdropper\ falsy\ detected}{total\ \#\ runs\ eavesdropper\ NOT\ present}$$

$$FNR = \frac{\#\ runs\ failed\ to\ detect\ eavesdropper}{total\ \#\ runs\ eavesdropper\ present}$$



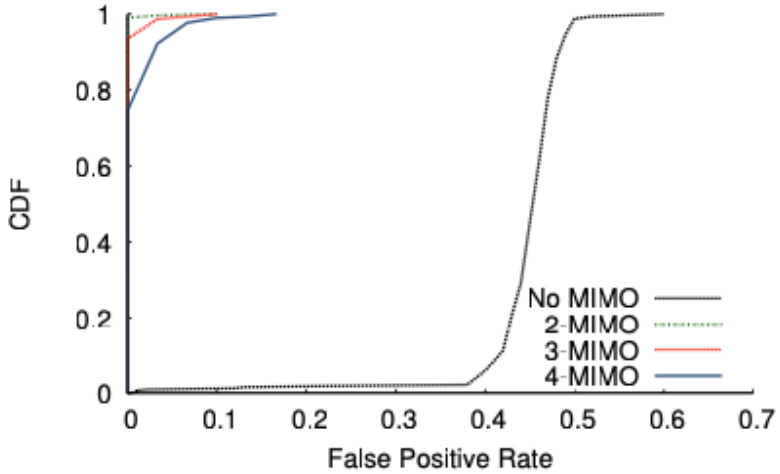


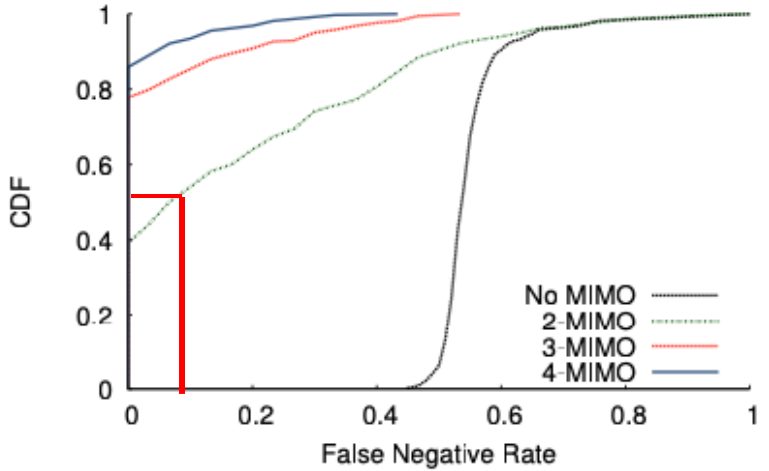
NO MIMO = Random Guess

Ghostbuster Evaluation: Eavesdropper and Tx

$$FPR = \frac{\#\ runs\ eavesdropper\ falsy\ detected}{total\ \#\ runs\ eavesdropper\ NOT\ present}$$

$$FNR = \frac{\#\ runs\ failed\ to\ detect\ eavesdropper}{total\ \#\ runs\ eavesdropper\ present}$$



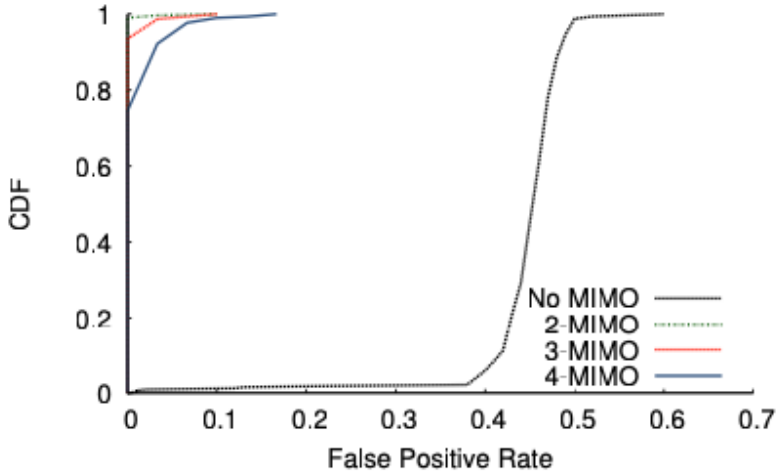


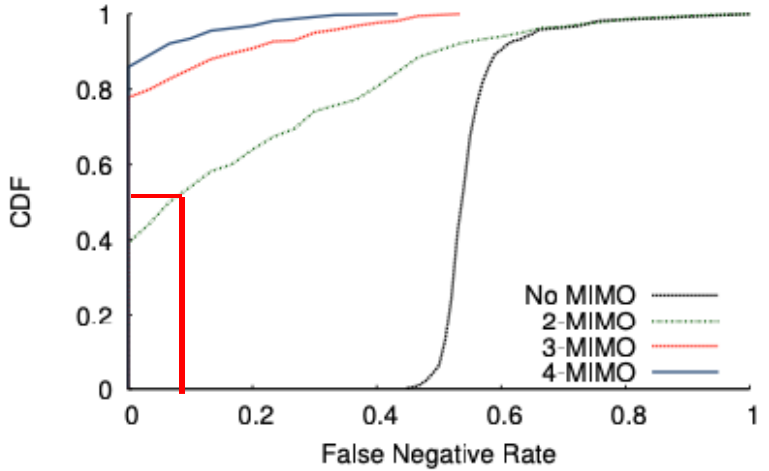
2-MIMO = 0 FPR (Median) & 0.10 FNR (Median)

Ghostbuster Evaluation: Eavesdropper and Tx

$$FPR = \frac{\#\ runs\ eavesdropper\ falsy\ detected}{total\ \#\ runs\ eavesdropper\ NOT\ present}$$

$$FNR = \frac{\#\ runs\ failed\ to\ detect\ eavesdropper}{total\ \#\ runs\ eavesdropper\ present}$$

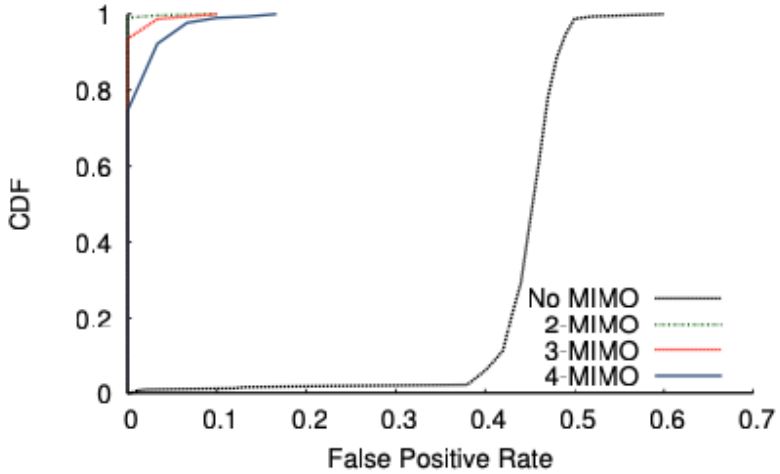




2-MIMO = 0 FPR (Median) & 0.10 FNR (Median)

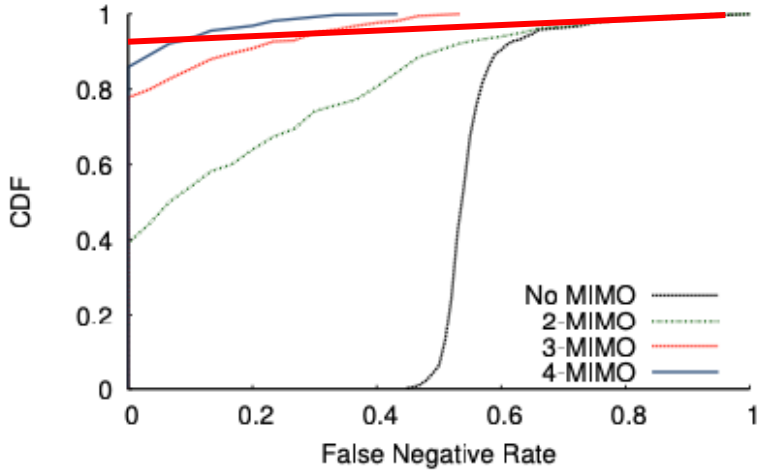
Ghostbuster Evaluation: Eavesdropper and Tx

$$FPR = \frac{\#\ runs\ eavesdropper\ falsy\ detected}{total\ \#\ runs\ eavesdropper\ NOT\ present}$$



95th Percentile FPR **increases** with more MIMO

$$FNR = \frac{\#\ runs\ failed\ to\ detect\ eavesdropper}{total\ \#\ runs\ eavesdropper\ present}$$



95th Percentile FNR **decreases** with more MIMO

Ghostbuster Evaluation: Eavesdropper and Tx

$$FPR = \frac{\#\ runs\ eavesdropper\ falsy\ detected}{total\ \#\ runs\ eavesdropper\ NOT\ present}$$

95th Percentile FPR **increases** with more MIMO

$$FNR = \frac{\#\ runs\ failed\ to\ detect\ eavesdropper}{total\ \#\ runs\ eavesdropper\ present}$$

95th Percentile FNR **decreases** with more MIMO

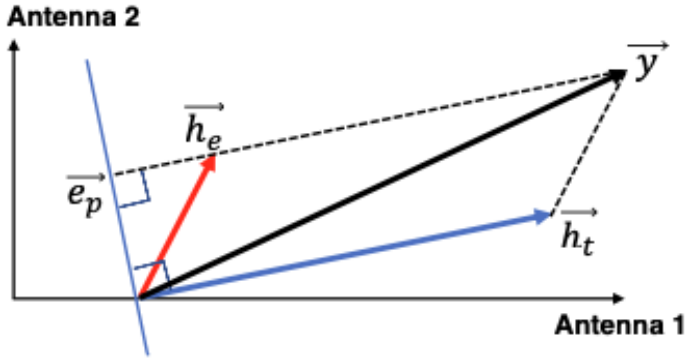
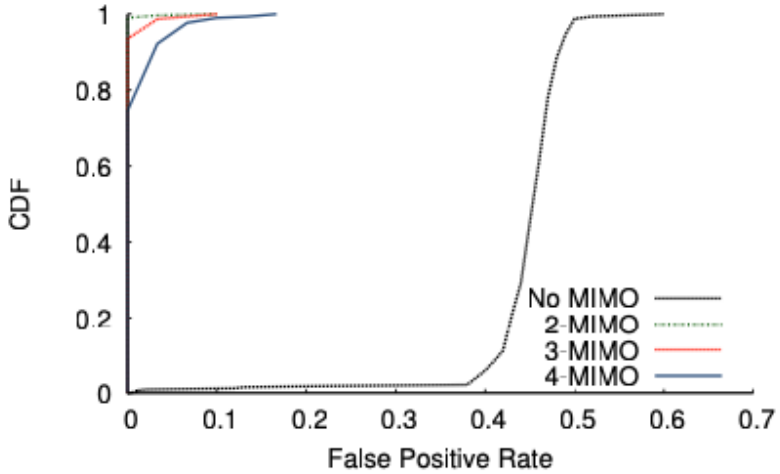


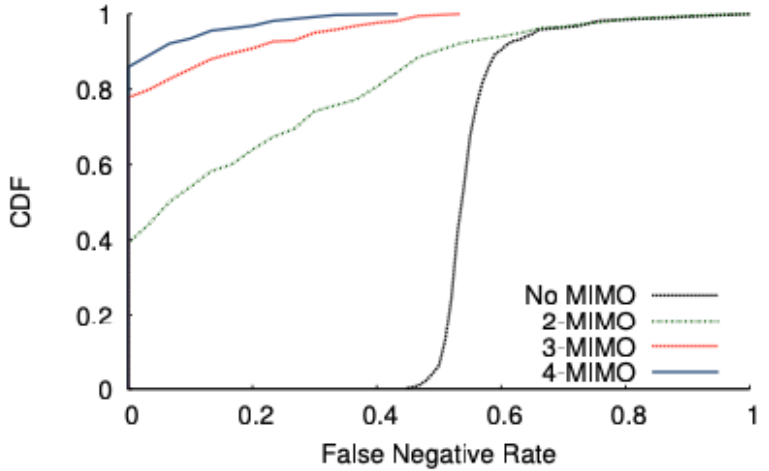
Figure 3: Ghostbuster leverages MIMO to cancel the signal from the transmitter in the Antenna Space.

Ghostbuster Evaluation: Eavesdropper and Tx

$$FPR = \frac{\#\ runs\ eavesdropper\ falsy\ detected}{total\ \#\ runs\ eavesdropper\ NOT\ present}$$

$$FNR = \frac{\#\ runs\ failed\ to\ detect\ eavesdropper}{total\ \#\ runs\ eavesdropper\ present}$$





FNR decrease > FPR increase

Ghostbuster Evaluation: Eavesdropper and Tx

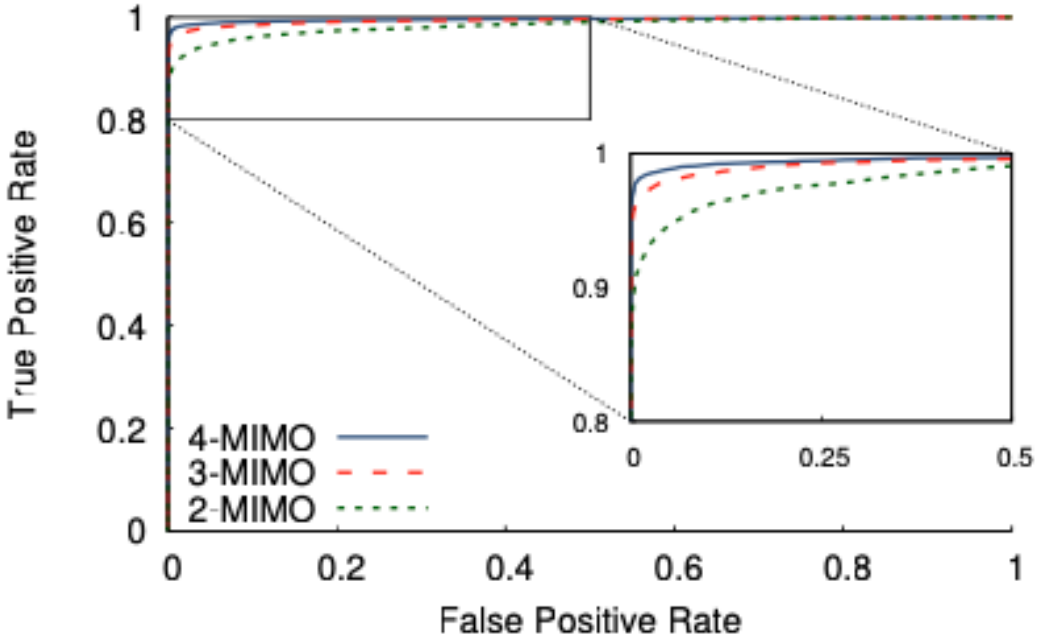


Figure 12: ROC curves for varying MIMO chain length.

More MIMO is better!

Ghostbuster Evaluation: Eavesdropper, Tx, and Rx

- **Tx:** USRP N210 transmitting ODFM Wi-Fi packets
- **Rx**: 4 USRP (max) N210 placed 1 – 5 m from GB

- **FFT Length:** 750 ms
- 2-MIMO Ghostbuster

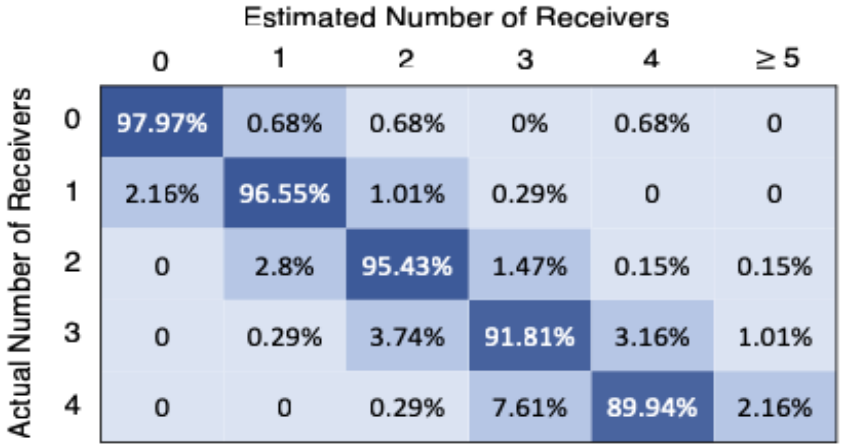


Figure 13: Confusion matrix of classification probabilities obtained on experiments on USRP receivers in the range 1 m to 5 m.

Ghostbuster Evaluation: Eavesdropper, Tx, and Rx

- **Tx:** USRP N210 transmitting ODFM Wi-Fi packets
- **Rx**: 2 MacBook Pro (monitor mode)

- **FFT Length:** 1.25 s
- 2-MIMO Ghostbuster

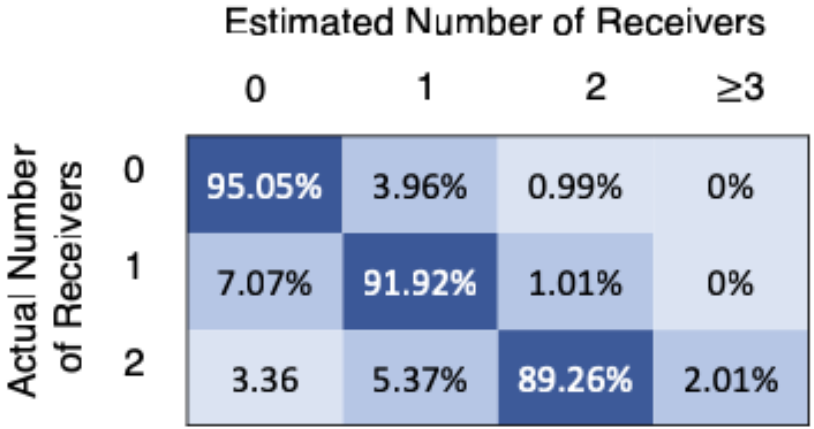
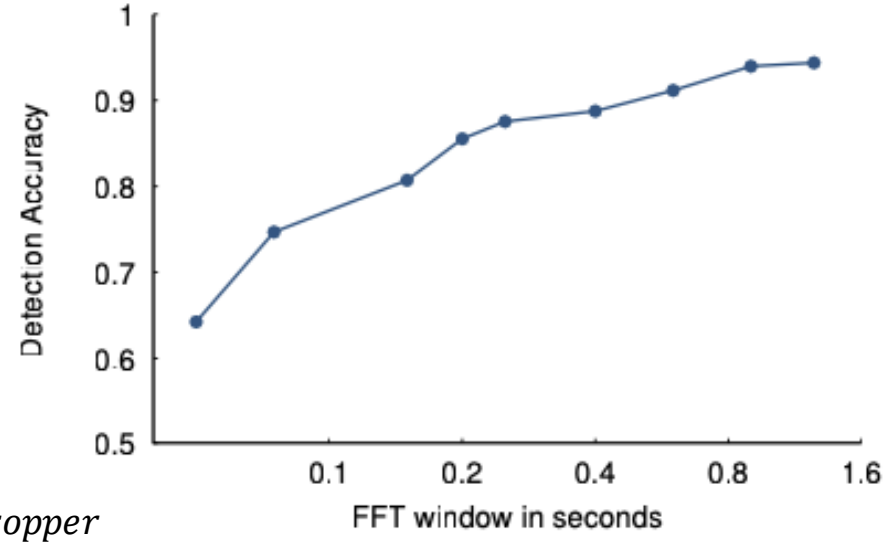


Figure 14: Confusion matrix of classification probabilities obtained on experiments on WiFi cards.

Ghostbuster Evaluation: Eavesdropper, Tx, and Rx

- **Tx:** USRP N210 transmitting ODFM Wi-Fi packets
- **Rx**: 1 MacBook Pro (monitor mode)
- **Eavesdropper**: 1 MacBook Pro (monitor mode)



$$Accuracy = \frac{\#\ runs\ GB\ correctly\ \ detected\ eavesdropper}{total\ \#\ runs}$$

94 % accuracy with 1.25 s FFT window!

Ghostbuster Limitations

- Ghostbuster requires knowing the number of legitimate receivers a priori

***Possible Solution**: Exploit duality of device as Tx/Rx (Correlate leakages)*

- Ghostbuster detection range is 5 m for USRP and 1 m for Wi-Fi cards

***Possible Solution:** Deploy multiple GB, decrease Tx power, or use larger FFT windows*

- Ghostbuster assumes **no** packet collision and **no** MIMO Tx

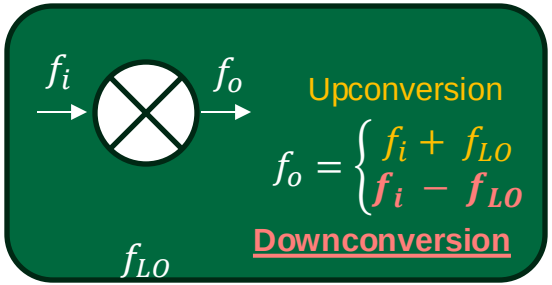
***Possible Solution:** Use MIMO to separate packets (k+1 antennas needed for k collision or k MIMO Tx)*

Thank You!

Q&A

Supplemental Material

RX Architecture -- Off-the-shelf Wi-Fi Cards



f_b : Baseband Frequency. Zero Hz/DC.

f_c : Carrier Frequency. Wi-Fi Channel frequency.

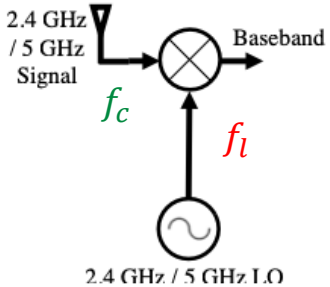
f_l : Leakage Frequency. A function of the LO frequency.

20 Wi-Fi cards were examined:

- *Device Types:* Desktops, laptops, cellphones, and access points.
- *Supported Protocols*: 802.11a,b,g,n,ac
- *Manufacturers*: Intel, Qualcomm, and Broadcom

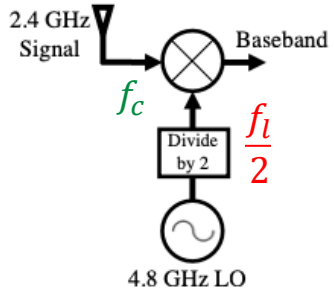
Only 4 RX architectures found!

RX Architecture -- Off-the-shelf Wi-Fi Cards



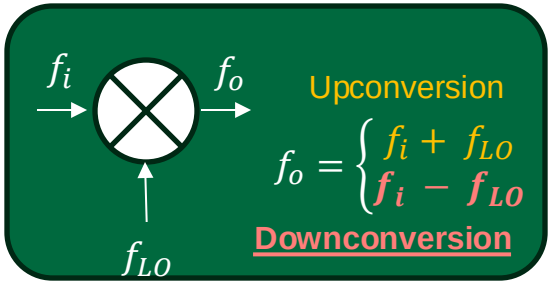
(a)

$$f_b = f_c - f_l$$
$$0 = f_c - f_l$$
$$f_c = f_l$$



(b)

$$f_b = f_c - \frac{f_l}{2}$$
$$0 = f_c - \frac{f_l}{2}$$
$$2 f_c = f_l$$

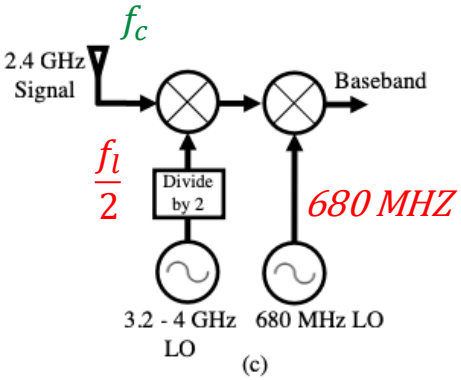


f_b : Baseband Frequency. Zero Hz/DC.

f_c : Carrier Frequency. Wi-Fi Channel frequency.

f_l : Leakage Frequency. A function of the LO frequency.

RX Architecture -- Off-the-shelf Wi-Fi Cards

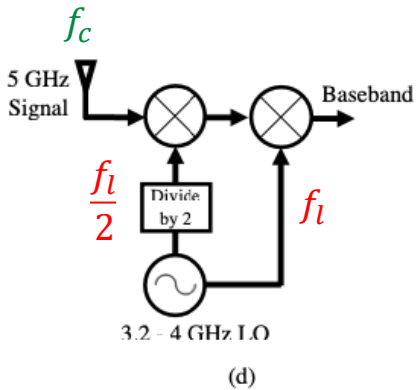


$$f_b = f_c - \frac{f_l}{2} - 680\ MHz$$

$$0 = f_c - \frac{f_l}{2} - 680\ MHz$$

$$f_c + 680\ MHz = \frac{f_l}{2}$$

$$2\ (f_c + 680\ MHz) = f_l$$

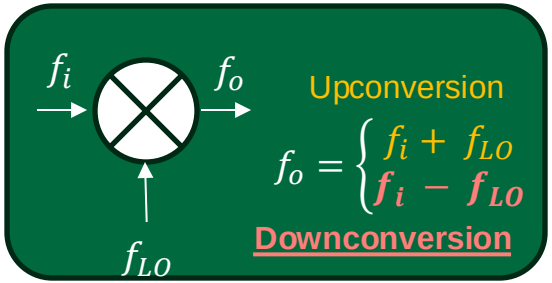


$$f_b = f_c - \frac{f_l}{2} - f_l$$

$$0 = f_c - \frac{3\ f_l}{2}$$

$$f_c = \frac{3\ f_l}{2}$$

$$\frac{2}{3} f_c = f_l$$



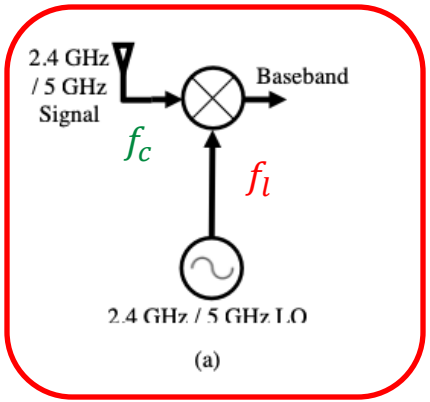
f_b : Baseband Frequency. Zero Hz/DC.

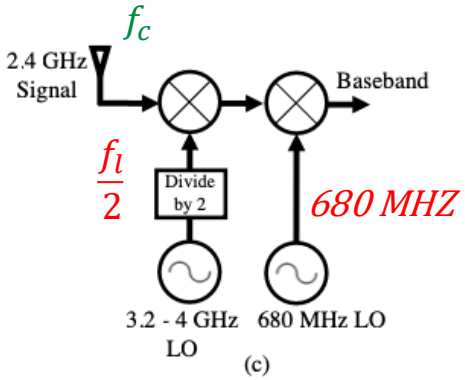
f_c : Carrier Frequency. Wi-Fi Channel frequency.

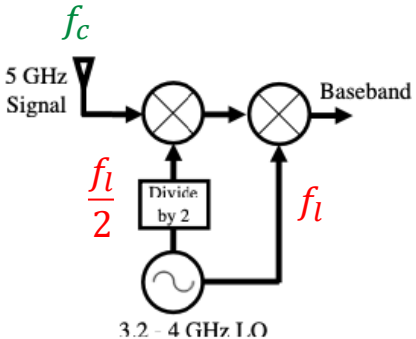
f_l : Leakage Frequency. A function of the LO frequency.

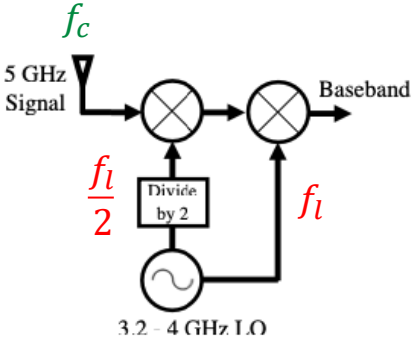
RX Architecture -- Implications

TX & Eavesdropper









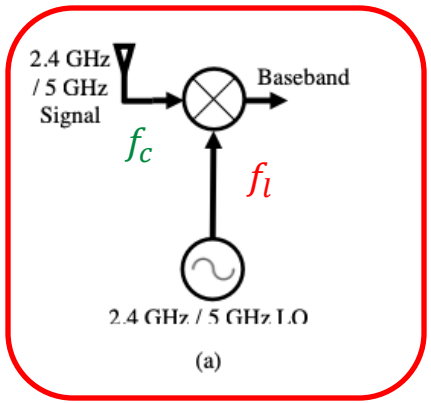
Full Ghostbuster Needed

Algorithm 1 Ghostbuster's Cancellation Algorithm

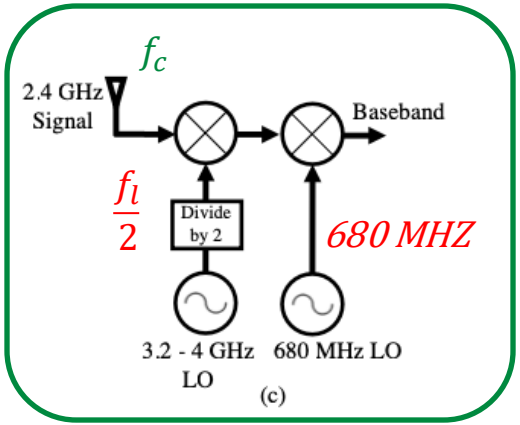
for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $F(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.

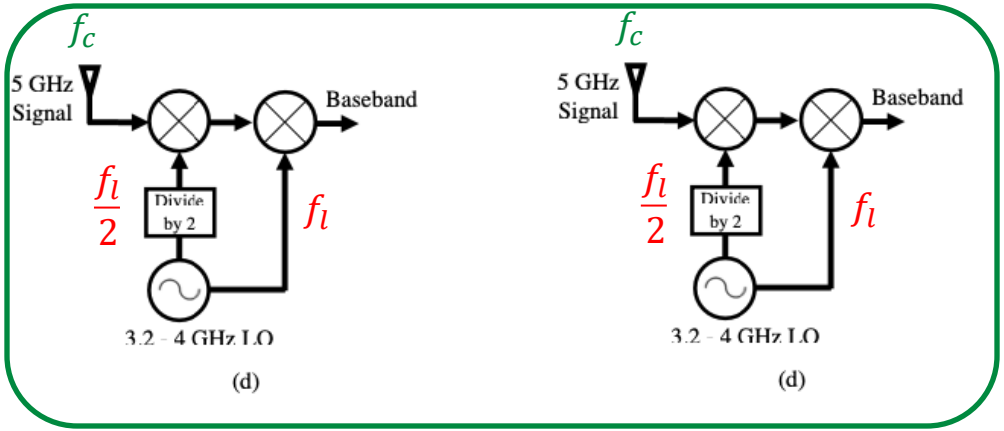
RX Architecture -- Implications

Eavesdropper



Tx





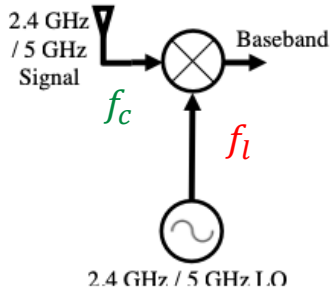
No spatial cancellation needed

Algorithm 1 Ghostbuster's Cancellation Algorithm

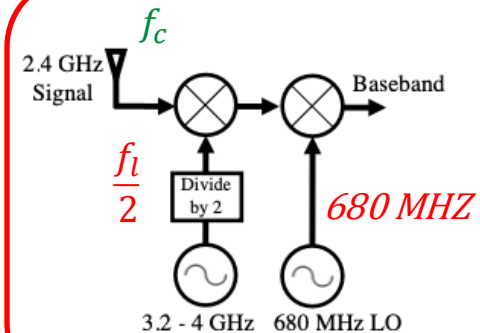
for k^{th} packet **do**
  for m^{th} MIMO Receiver **do**
    Decode packet using standard OFDM decoder.
    for Each OFDM Symbol **do**
      $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
      $i \leftarrow 1$
      while $F(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
        $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
        $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
        $i \leftarrow i + 1$
      end while
      $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
      $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
    end for
    $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
    $P_m(f) \leftarrow FFT(p_m(t))$
    $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
  end for
  $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
end for
$s(t) \leftarrow$ combination of $s_k(t)$ from all packets
$S(f) \leftarrow FFT(s(t))$
Find spike of eavesdropper's RF leakage.

RX Architecture -- Implications

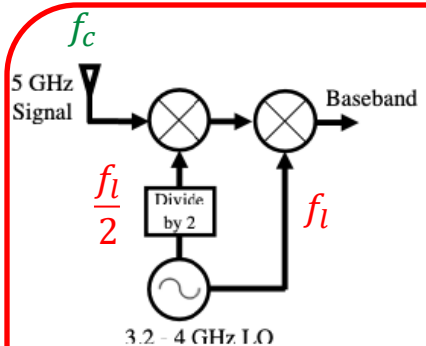
Eavesdropper



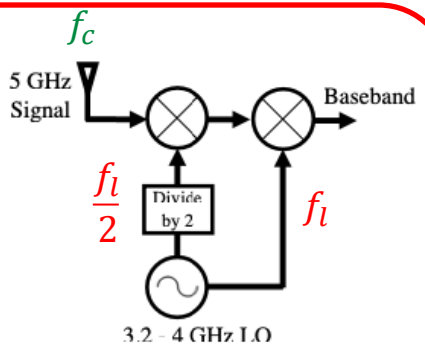
(a)



(c)



(d)

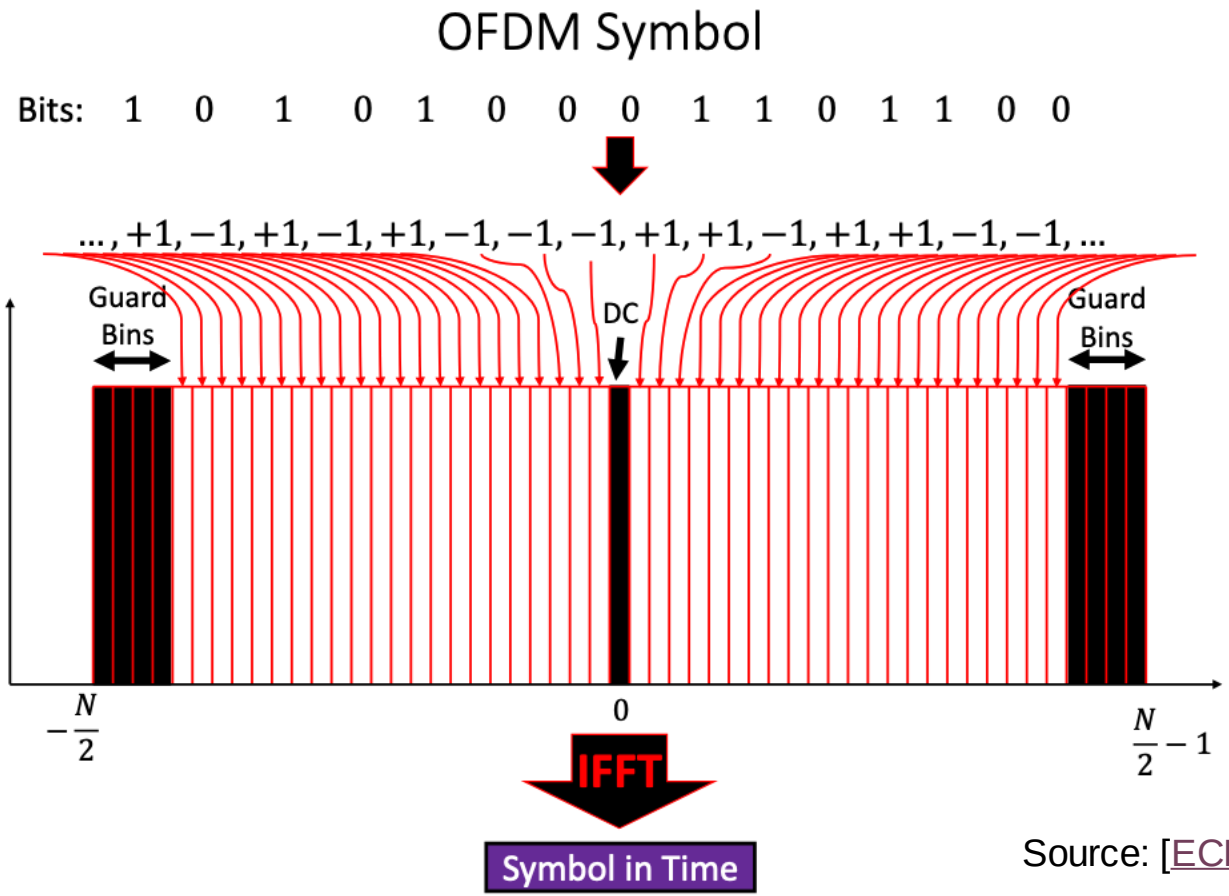


(d)

Algorithm 1 Ghostbuster's Cancellation Algorithm

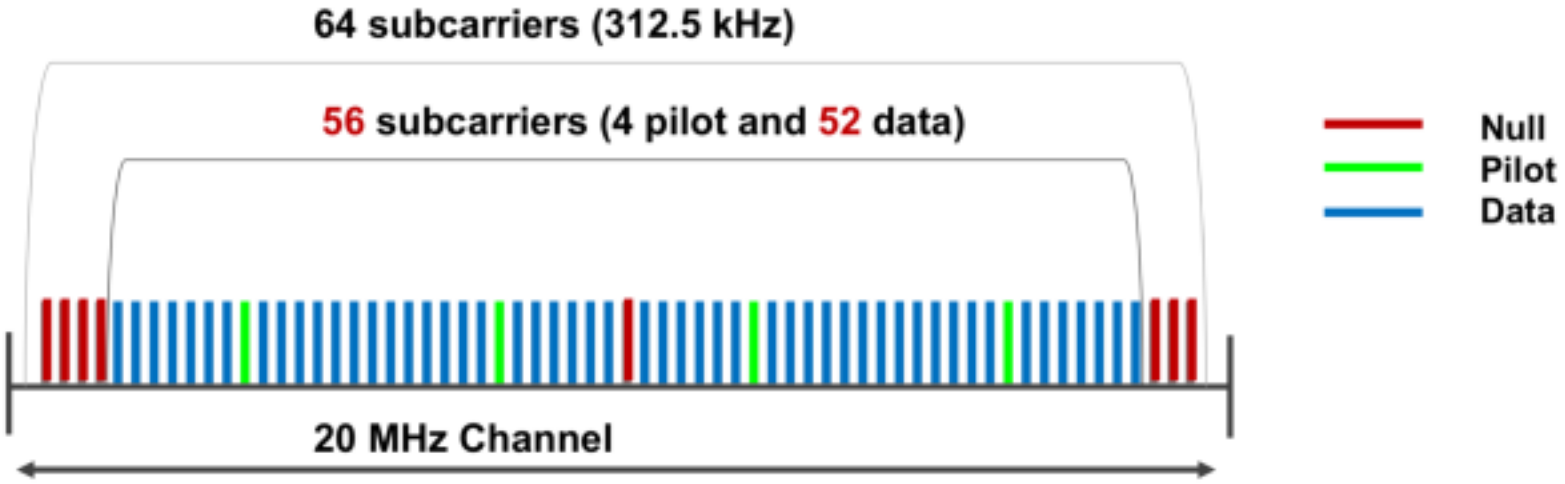
1: **for** k^{th} packet **do**
2: **for** m^{th} MIMO Receiver **do**
3: Decode packet using standard OFDM decoder.
4: **for** Each OFDM Symbol **do**
5: $\tilde{\mathbf{f}}^{(0)} \leftarrow$ CFO coarse & fine estimates
6: $i \leftarrow 1$
7: **while** $F(\tilde{\mathbf{f}}^{(i-1)}, \tilde{\mathbf{a}}^{(i-1)}) \geq$ Threshold **do**
8: $\tilde{\mathbf{a}}^{(i)} \leftarrow$ WeightedLeastSq$(\tilde{\mathbf{f}}^{(i-1)}, x_m(t))$
9: $\tilde{\mathbf{f}}^{(i)} \leftarrow$ GradientDescent$(\tilde{\mathbf{a}}^{(i)}, x_m(t))$
10: $i \leftarrow i + 1$
11: **end while**
12: $\tilde{x}_m(t) \leftarrow \tilde{\mathbf{a}}^*, \tilde{\mathbf{f}}^*$ (other than the DC bin)
13: $r_m(t) \leftarrow x_m(t) - \tilde{x}_m(t)$
14: **end for**
15: $p_m(t) \leftarrow$ combination of $r_m(t)$ from all symbols
16: $P_m(f) \leftarrow FFT(p_m(t))$
17: $H_m(f_{DC}) \leftarrow P_m(f_{DC})$
18: **end for**
19: $s_k(t) \leftarrow$ spatial cancellation using each $H_m(f_{DC})$
20: **end for**
21: $s(t) \leftarrow$ combination of $s_k(t)$ from all packets
22: $S(f) \leftarrow FFT(s(t))$
23: Find spike of eavesdropper's RF leakage.

Orthogonal Frequency Division Multiplexing (OFDM)



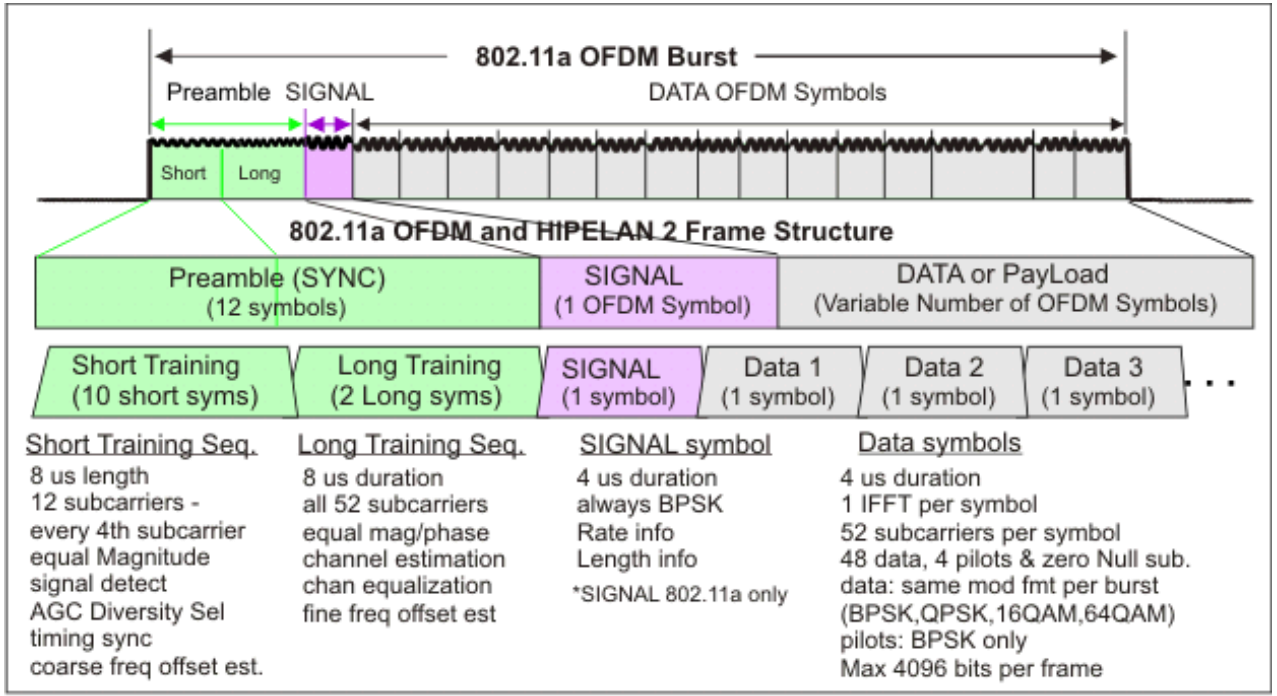
Source: [ECE 463 @ UIUC]

Wi-Fi OFDM



Source: [cradtech]

Wi-Fi OFDM



Source: [Tektronix]

Wi-Fi OFDM

- EEE 802.11a (Wi-Fi 2)
- IEEE 802.11g (Wi-Fi 3)
- IEEE 802.11n (Wi-Fi 4)
- IEEE 802.11ac (Wi-Fi 5)

Source: [Tektronix]

OFDM: CFO Estimation

$$z_1(t) = x(t)e^{-2\pi i f_{CFO} t}$$ First Preamble Symbol

$$z_2(t) = x(t)e^{-2\pi i f_{CFO}(t+NT_s)}$$ Second Preamble Symbol

$$A = \sum_{t=1}^{N} z_1 z_2^*$$ Cross-correlation of adjacent symbols

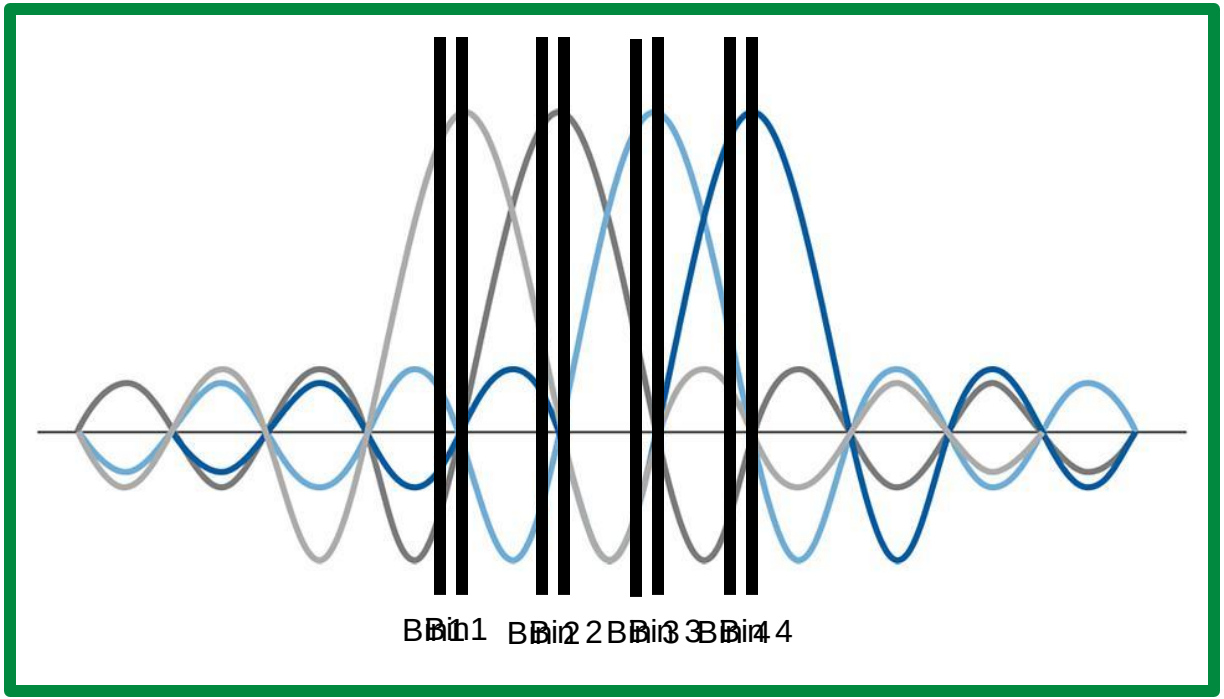
$$A = \sum_{t=1}^{N} x(t)x^*(t)e^{2\pi i f_{CFO} NT_s}$$

$$A = e^{2\pi i f_{CFO} NT_s} \sum_{t=1}^{N} |x(t)|^2$$

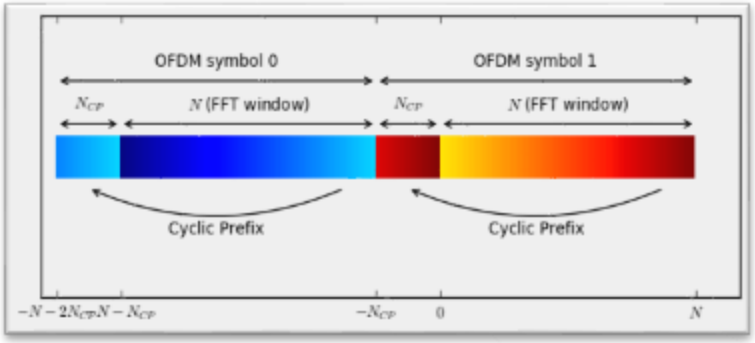
$$f_{CFO} = \frac{arg(A)}{2\pi NT_s}$$

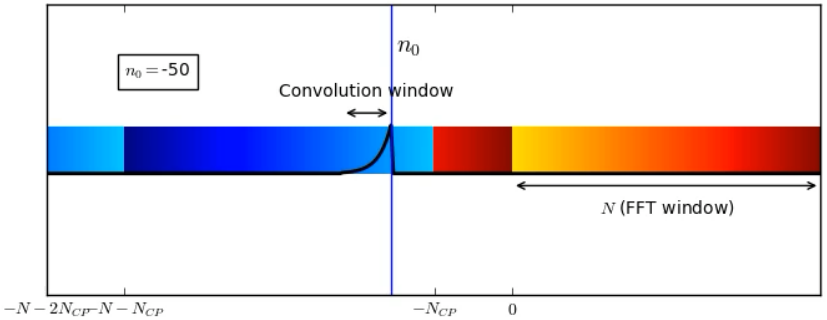
Source: [ECE 463 @ UIUC]

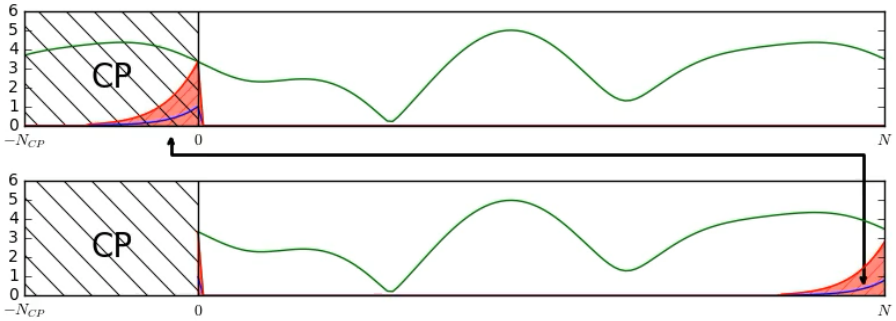
OFDM: CFO Correction



OFDM: Cyclic Prefix







Convolution with Channel's Impulse Response

Source: [Tektronix & DSP Illustrations]

Dealing with Cyclic Prefix

- CP needs to be eliminated too.
- Running algorithm on $N+N_{CP}$ symbols breaks orthogonality (i.e., initial estimates of f_k are outside convex region).
- Reconstruct from algorithm on N samples yields poor result.

Solution:

Run algorithm over this N samples

Run algorithm over this N samples

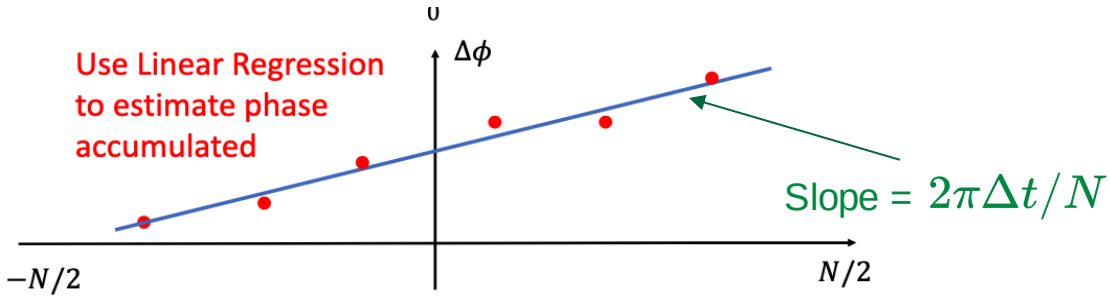
Use this result to estimate CP

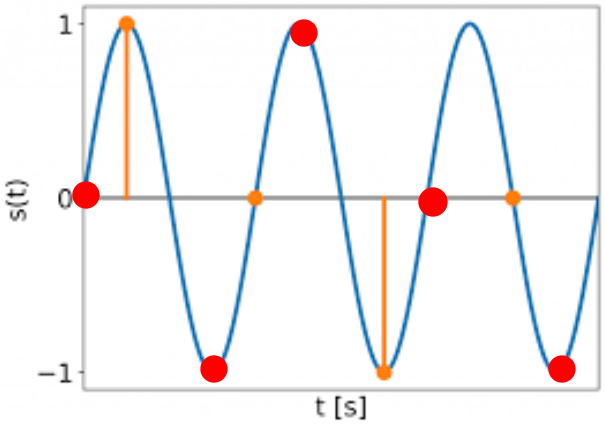
OFDM: Sampling Offset

$$x(t-\Delta t) = \sum_{k=0}^{N-1} a_k e^{2\pi i f_k (t-\Delta t)/N}$$

$$x(t-\Delta t) = \sum_{k=0}^{N-1} a_k e^{2\pi i f_k t/N - 2\pi i f_k \Delta t/N}$$

$$\phi = 2\pi f_k \Delta t/N$$





Tx Digital Signal

Rx Digital Signal

Continuous Time Signal

Antenna/Spatial Cancellation

$$y_1(t) = h_{e1} * e(t) + h_{t1} * x(t)$$ Rx signal @ antenna 1

$$y_2(t) = h_{e2} * e(t) + h_{t2} * x(t)$$ Rx signal @ antenna 2

Fourier Transform:

$$Y_1(f) = H_{e1}E(f) + H_{t1}X(f)$$

$$Y_2(f) = H_{e2}E(f) + H_{t2}X(f)$$

In Vector Form:

$$\mathbf{Y} = \mathbf{H_e}E(f) + \mathbf{H_t}X(f)$$

Dot product with vector orthogonal to H_t :

$$\mathbf{Y} \cdot \mathbf{H}^{\perp} = \mathbf{H_e} \cdot \mathbf{H}^{\perp}E(f)$$

Antenna/Spatial Cancellation

$$\mathbf{Y} \cdot \mathbf{H}^{\perp} = \mathbf{H_e} \cdot \mathbf{H}^{\perp} E(f)$$

$$\mathbf{H}^{\perp} = \begin{bmatrix} 1 \\ \frac{-Ht_1}{Ht_2} \end{bmatrix}$$

$$Y_1(f) + Y_2(f) - \frac{H_{t1}}{H_{t2}} = \left[H_{e1} - H_{e2} \frac{H_{t1}}{H_{t2}} \right] E(f)$$

$$Y_1(f) - Y_2(f) \frac{H_{t1}}{H_{t2}} = CE(f)$$

Antenna/Spatial Cancellation

$$\mathbf{Y} \cdot \mathbf{H}^{\perp} = \mathbf{H_e} \cdot \mathbf{H}^{\perp} E(f)$$

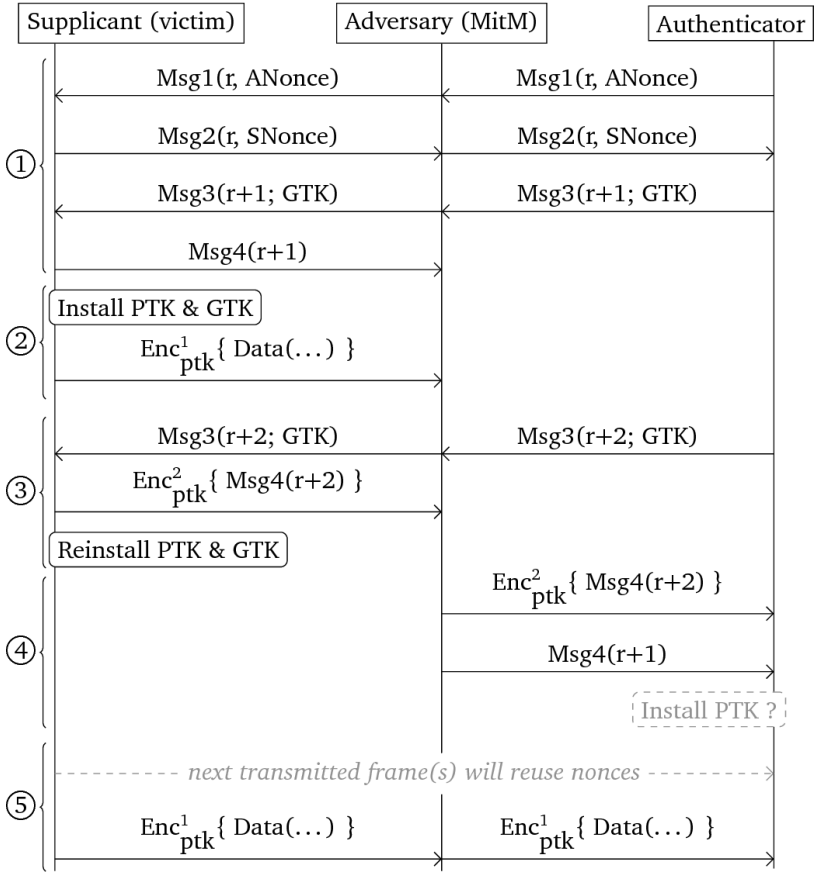
For 3-MIMO:

$$\mathbf{H}^{\perp} = \begin{bmatrix} 1 \\ 1 \\ -\frac{H_{t_1} + H_{t2}}{H_{t3}} \end{bmatrix}$$

$$Y_1(f) + Y_2(f) - Y_3(f)\left(\frac{H_{t1}}{H_{t3}} + \frac{H_{t2}}{H_{t3}}\right) = \left[H_{e1} + H_{e2} - H_{e3}\frac{H_{t1} + H_{t2}}{H_{t3}}\right] E(f)$$

$$Y_1(f) + Y_2(f) - Y_3(f)\left(\frac{H_{t1}}{H_{t3}} + \frac{H_{t2}}{H_{t3}}\right) = CE(f)$$

Key Reinstallation Attack



Side Channel Cryptographic Key Extraction

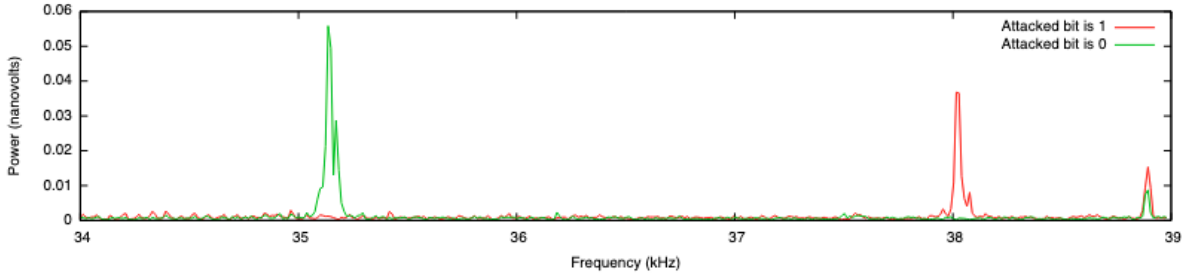
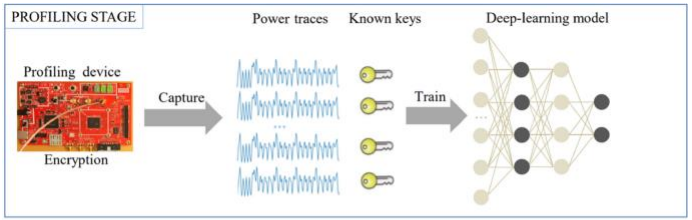
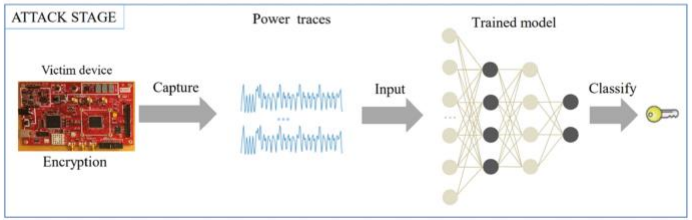


Figure 32: Power measurement frequency spectra of the second modular exponentiation.

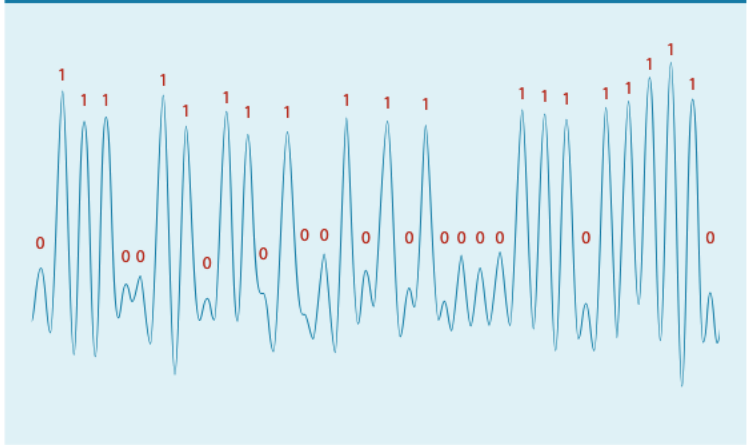


(a) The profiling stage of a deep-learning based side-channel attack.



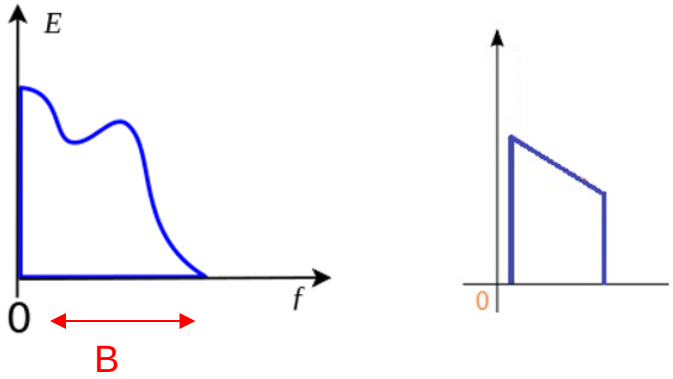
(b) The attack stage of a deep-learning based side-channel attack.

Figure 8. A signal segment from an electric attack, after demodulating and combining measurements of several decryptions. Note the correlation between the signal (blue) and the correct key bits (red).

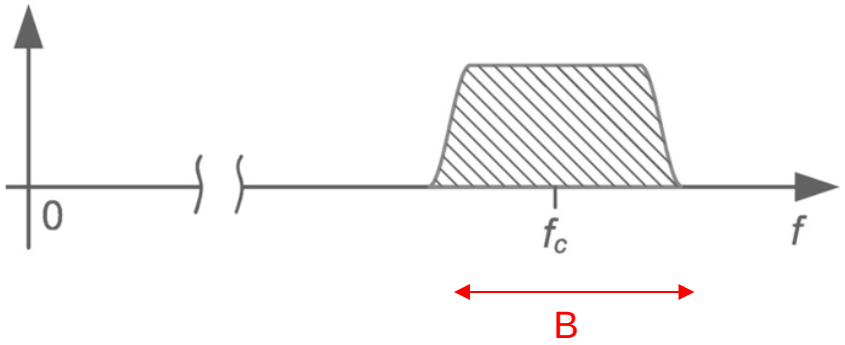


Baseband

Example **baseband** signals



Example **bandpass** (not baseband) signal



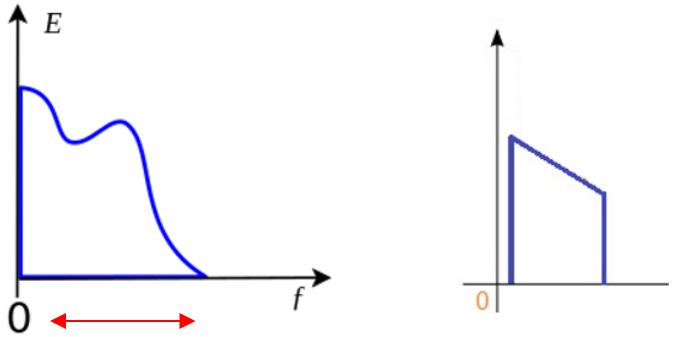
We want to transmit a bandlimited signal

In a more convenient region of the spectrum

Source: [PySDR]

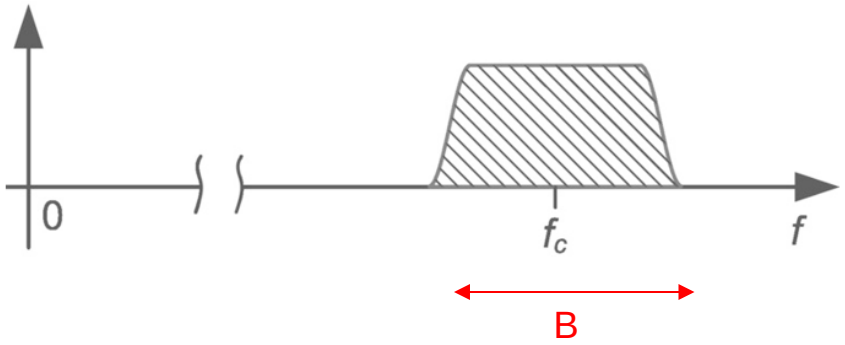
The importance of LO in RX

Example **baseband** signals



We want to transmit a bandlimited signal

Example **bandpass** (not baseband) signal



In a more convenient region of the spectrum

WHY do we need to downconverter?

- We can only capture baseband (i.e., without downconvertion).
- Capturing the full spectrum is too expensive (i.e., how much of the spectrum we capture is given by 1/Ts.
- A radio with 160 MHz MHz sample rate is USD$17,000.

Error Function Convexity

Reminder:

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

$$E(\tilde{\mathbf{a}}, \tilde{\mathbf{f}}) = \sum_{t=0}^{N-1} |x(t) - \tilde{x}(t)|^2$$

Assume fixed f tilde:

$$E = \sum_{t=0}^{N-1} < x(t) - \tilde{x}(t) | x(t) - \tilde{x}(t) >$$

$$E = \sum_{t=0}^{N-1} < x(t) | x(t) - \tilde{x}(t) > - < \tilde{x}(t) | x(t) - \tilde{x}(t) >$$

$$E = \sum_{t=0}^{N-1} < x(t) | x(t) > - < x(t) | \tilde{x}(t) > - < \tilde{x}(t) | x(t) > + < \tilde{x}(t) | \tilde{x}(t) >$$

$$E = \sum_{t=0}^{N-1} \left(|x(t)|^2 - x(t)\tilde{x}(t)^* - \tilde{x}(t)x(t)^* + |\tilde{x}(t)|^2 \right)$$

Error Function Convexity

Reminder:

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

$$E = \sum_{t=0}^{N-1} \left(|x(t)|^2 - x(t)\tilde{x}(t)^* - \tilde{x}(t)x(t)^* + |\tilde{x}(t)|^2 \right)$$

$$\frac{\delta E}{\delta \tilde{a}^*} = -\sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N} + \sum_{t=0}^{N-1}\sum_{m=0}^{N-1} \tilde{a}_m e^{2\pi i \tilde{f}_m t/N} e^{-2\pi i \tilde{f}_k t/N}$$

$$\frac{\delta E}{\delta \tilde{a}^*} = -\sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N} + \sum_{t=0}^{N-1} \tilde{a}_k$$

$$\frac{\delta E}{\delta \tilde{a}^*} = -\sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N} + N\tilde{a}_k$$

$$\sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N} = N\tilde{a}_k$$

(We know this is a min. because, for fixed f tilde we have an ordinary least-squares problem)

$$\tilde{a}_k = \frac{1}{N} \sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N}$$

Error Function Convexity

$$E(\tilde{\mathbf{a}}, \tilde{\mathbf{f}}) = \sum_{t=0}^{N-1} |x(t) - \tilde{x}(t)|^2$$

Reminder:

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

$$x(t) = \sum_{k=0}^{N-1} a_k e^{2\pi i f_k t/N}$$

$$s_{geo-series} = \frac{a(r^n - 1)}{r - 1}$$

Assume fixed a:

$$E = \sum_{t=0}^{N-1} \left(|x(t)|^2 - x(t)\tilde{x}(t)^* - \tilde{x}(t)x(t)^* + |\tilde{x}(t)|^2 \right)$$

Assuming f and f tilde are orthogonal*

$$E = \sum_{t=0}^{N-1}\sum_{k=0}^{N-1} |a_k|^2 - \sum_{t=0}^{N-1}\sum_{k=0}^{N-1} a_k \tilde{a}_k^* e^{2\pi i (f_k - \tilde{f}_k) t/N} - \sum_{t=0}^{N-1}\sum_{k=0}^{N-1} a_k^* \tilde{a}_k e^{-2\pi i (f_k - \tilde{f}_k) t/N} + \sum_{t=0}^{N-1}\sum_{k=0}^{N-1} |\tilde{a}_k|^2$$

Using sum of geometric series

$$E = \sum_{k=0}^{N-1} N|a_k|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i (f_k - \tilde{f}_k)} - 1}{e^{2\pi i (f_k - \tilde{f}_k)/N} - 1} \right|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i (f_k - \tilde{f}_k)} - 1}{e^{2\pi i (f_k - \tilde{f}_k)/N} - 1} \right|^2 + \sum_{k=0}^{N-1} N|\tilde{a}_k|^2$$

* This is only true if f= f tilde. But will be close to orthogonal if values are not too far apart

Error Function Convexity

Reminder:

$$\tilde{x}(t) = \sum_{k=0}^{N-1} \tilde{a}_k e^{2\pi i \tilde{f}_k t/N}$$

$$x(t) = \sum_{k=0}^{N-1} a_k e^{2\pi i f_k t/N}$$

From solution at fixed a we know:

$$\tilde{a}_k = \frac{1}{N} \sum_{t=0}^{N-1} x(t) e^{-2\pi i \tilde{f}_k t/N}$$

$$\tilde{a}_k = \sum_{t=0}^{N-1} a_k e^{2\pi i f_k t/N} e^{-2\pi i \tilde{f}_k t/N} = \frac{a_k}{N} \frac{e^{2\pi i (f_k - \tilde{f}_k)} - 1}{e^{2\pi i (f_k - \tilde{f}_k)/N} - 1}$$

Plug into this expression:

$$E = \sum_{k=0}^{N-1} N|a_k|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i (f_k - \tilde{f}_k)} - 1}{e^{2\pi i (f_k - \tilde{f}_k)/N} - 1} \right|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i (f_k - \tilde{f}_k)} - 1}{e^{2\pi i (f_k - \tilde{f}_k)/N} - 1} \right|^2 + \sum_{k=0}^{N-1} N|\tilde{a}_k|^2$$

To get:

$$E = \sum_{k=0}^{N-1} N|a_k|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i (f_k - \tilde{f}_k)} - 1}{e^{2\pi i (f_k - \tilde{f}_k)/N} - 1} \right|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i (f_k - \tilde{f}_k)} - 1}{e^{2\pi i (f_k - \tilde{f}_k)/N} - 1} \right|^2 + \sum_{k=0}^{N-1} N \frac{|a_k|^2}{N^2} \left| \frac{e^{2\pi i (f_k - \tilde{f}_k)} - 1}{e^{2\pi i (f_k - \tilde{f}_k)/N} - 1} \right|^2$$

Error Function Convexity

$$E = \sum_{k=0}^{N-1} N|a_k|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i(f_k - \tilde{f}_k)} - 1}{e^{2\pi i(f_k - \tilde{f}_k)/N} - 1} \right|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i(f_k - \tilde{f}_k)} - 1}{e^{2\pi i(f_k - \tilde{f}_k)/N} - 1} \right|^2 + \sum_{k=0}^{N-1} N\frac{|a_k|^2}{N^2} \left| \frac{e^{2\pi i(f_k - \tilde{f}_k)} - 1}{e^{2\pi i(f_k - \tilde{f}_k)/N} - 1} \right|^2$$

$$E = \sum_{k=0}^{N-1} N|a_k|^2 - \sum_{k=0}^{N-1} \frac{|a_k|^2}{N} \left| \frac{e^{2\pi i(f_k - \tilde{f}_k)} - 1}{e^{2\pi i(f_k - \tilde{f}_k)/N} - 1} \right|^2$$

$$E = \sum_{k=0}^{N-1} N|a_k|^2 - \sum_{k=0}^{N-1} \left(\frac{\sin(\pi(f_k - \tilde{f}_k))}{\sin(\pi(f_k - \tilde{f}_k/N)} \right)^2$$

Using symbolic solver:

$$\frac{\delta E}{\delta \tilde{f}_k} = \frac{2\pi \sin(\pi x) \csc^2(\frac{\pi x}{N}) \left(\sin(\pi x) \cot(\frac{\pi x}{N} - N\cos(\pi x)) \right)}{N}$$

Where:

$$x = f_k - \tilde{f}_k$$

Error Function Convexity

Using symbolic solver:

$$\frac{\delta E}{\delta \tilde{f}_k} = \frac{2\pi \sin(\pi x) \csc^2(\frac{\pi x}{N}) \left(\sin(\pi x) \cot(\frac{\pi x}{N} - N\cos(\pi x))\right)}{N}$$

$$\frac{\delta^2 E}{\delta \tilde{f}_k^2} = \frac{1}{N} 2\pi^2 \csc^2(\pi x/N) \left(N^2 \cos^2(\pi x) + \sin^2(\pi x) \left(2\cot^2(\pi x/N + \csc^2(\pi x/N) - N^2\right) - 4N \sin(\pi x)\cos(\pi x)\cot(\pi x/N)\right)$$

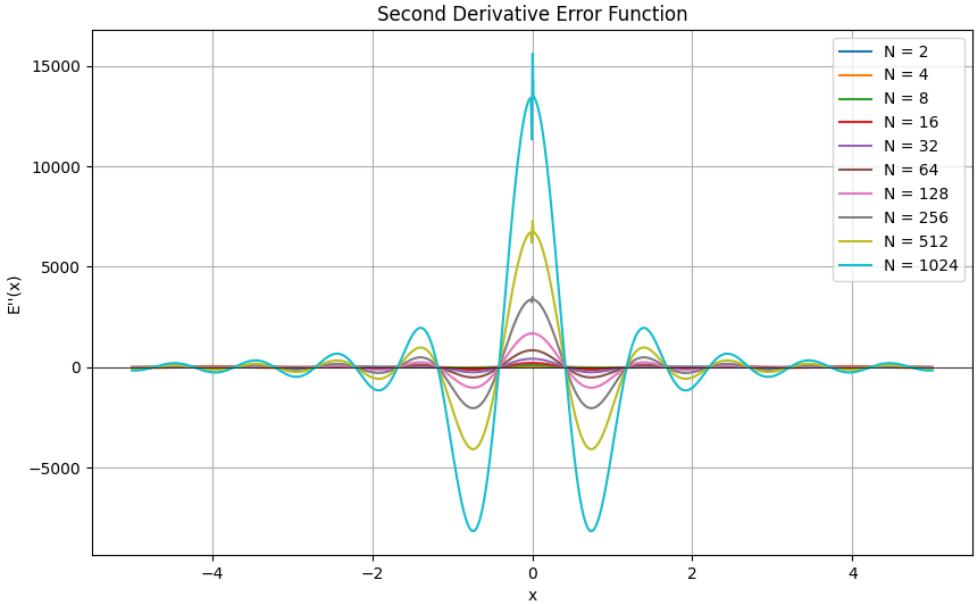
Where:

$$x = f_k - \tilde{f}_k$$

Showing Convexity is HARD:
Manually, I **failed**
Symbolic Solvers also **failed**

Error Function Convexity

NUMERICAL SOLUTION



Zeros of Error Function Second Derivative:

```
Root for N:2 = 0.500000000157555
Root for N:4 = 0.431938788005115
Root for N:8 = 0.418878806105801
Root for N:16 = 0.415796186508688
Root for N:32 = 0.415036193725720
Root for N:64 = 0.414846853932895
Root for N:128 = 0.414799565498124
Root for N:256 = 0.414787757349532
Root for N:512 = 0.414784828295256
Root for N:1024 = 0.414784141685676
```

Where:

$$x = f_k - \tilde{f}_k$$

Does the assumption f and f tilde are orthogonal remains on this range? From some rough experiments NO, it seems to be good in the range ± 0.16

$$\frac{\delta^2 E}{\delta \tilde{f}_k^2} > 0 \; \forall \tilde{f}_k \, \epsilon [f_k - 0.4, f_k + 0.4]$$

Discrete Fourier Transform (DFT)

Forward Transform (Fourier Decomposition):

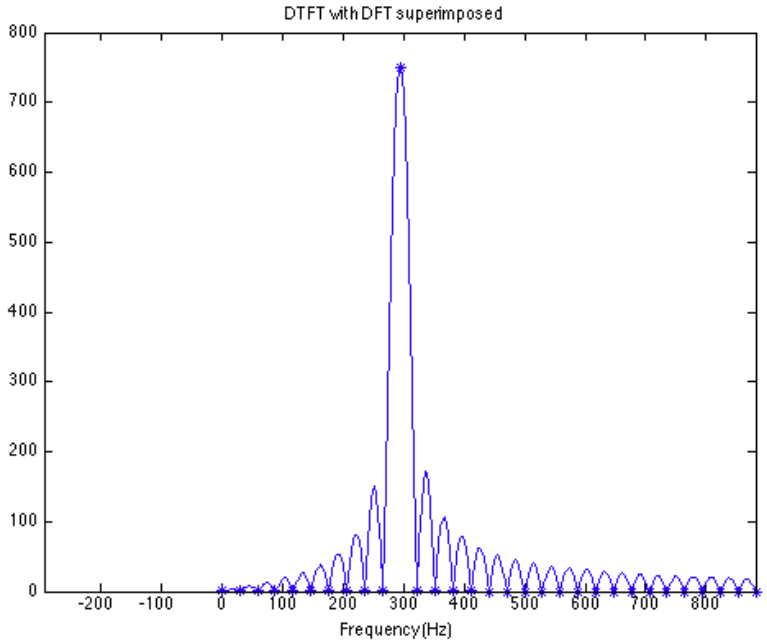
$$F[m] =< f[n], \phi_m[n] >= \frac{1}{N} \sum_{n=0}^{N-1} f[n] e^{-2i\pi f_k n/N}$$

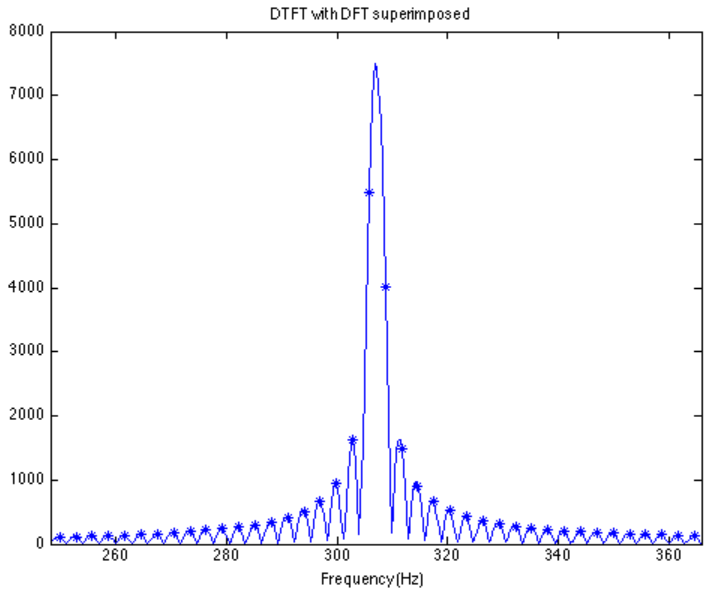
Linear Orthogonal Decomposition with Sinusoidal Basis

Inverse Transform (Fourier Reconstruction):

$$f[n] = \sum_{n=0}^{N-1} F[m] e^{2\pi f_k n/N}$$

DFT Interpretation





Related Work

Detecting passive eavesdroppers in the MIMO wiretap channel
Receiver LO leakage detection when there is a clear channel (i.e., other RX/Tx pause operations).

Securing Inductively-Coupled Communication
Detection of near-field communication eavesdropper such as in RFID systems. Near-Filed channel is greatly affected by eavesdropper presence.

Multiple studies regarding detection of radios through LO leakage
This body of work focus on the detection of receivers' leakage when there are no transmissions.