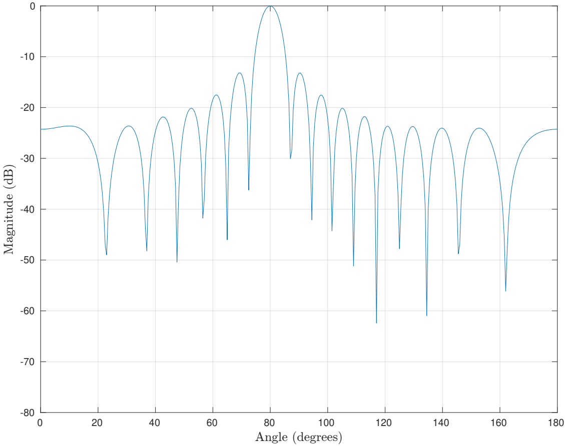
# Power-Efficient Deceptive Wireless Beamforming Against Eavesdroppers

Georgios Chrysanidis, **Antonios Argyriou** (Univ. of Thessaly)
Le-Nam Tran (UCD), Yanming Zhang (CUHK), Yanwei Liu (CAS).

March 25th, 2025, IEEE WCNC, Milan

# Beamforming: Array Response

When we have an array of anntennas (Tx/Rx) we may steer the signal to a preferred direction




Relative power of the transmitted signal for different spatial directions.

# Eavesdropping & Beamforming

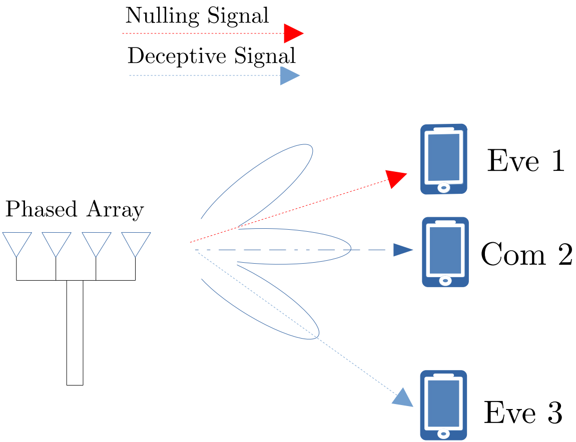
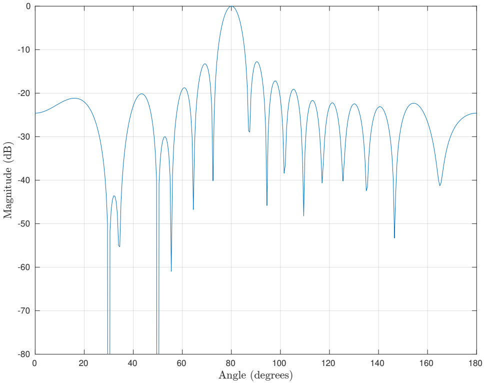



Figure: A transmitter has to face two receivers that eavesdrop (Eve 1 & 3) besides the legitimate receiver (Com 2).

# How do we tackle eavesdroppers with Beamforming (1)

## Array Response with Transmit Beamforming & Nulling

Array response when doing transmit beamforming with an optimization method. Nulling with $\theta_c$=$80^o$, $\theta_{\text{eav}}$=$\{30^o,50^o\}$.



# How do we tackle eavesdroppers with Beamforming (2)

## More Techniques

- More advanced techniques like injecting artificial noise towards the direction of the eavesdroppers have been explored in [LCMC11].

# How do we tackle eavesdroppers with Beamforming (2)

## More Techniques

- More advanced techniques like injecting artificial noise towards the direction of the eavesdroppers have been explored in [LCMC11].
- A similar idea is Directional Modulation (DM) which enables secure communication with phased arrays and beamforming [DB09].

# How do we tackle eavesdroppers with Beamforming (2)

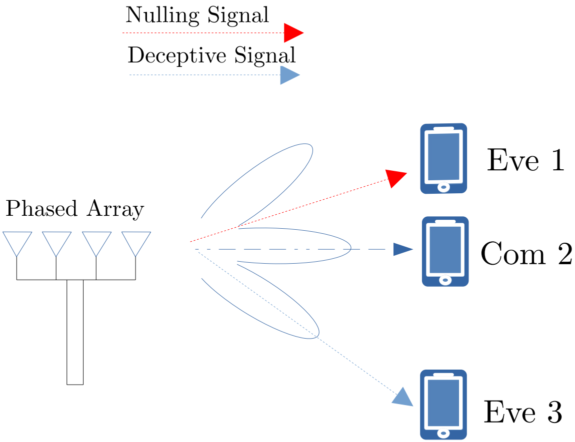
## More Techniques

- More advanced techniques like injecting artificial noise towards the direction of the eavesdroppers have been explored in [LCMC11].
- A similar idea is Directional Modulation (DM) which enables secure communication with phased arrays and beamforming [DB09].
- Multi-Function RF (MFRF) systems have proposed the joint design of a signal for communications, RADAR, and electronic RF jamming but without considering eavesdropping [TS22].

# How do we tackle eavesdroppers with Beamforming (2)

## More Techniques

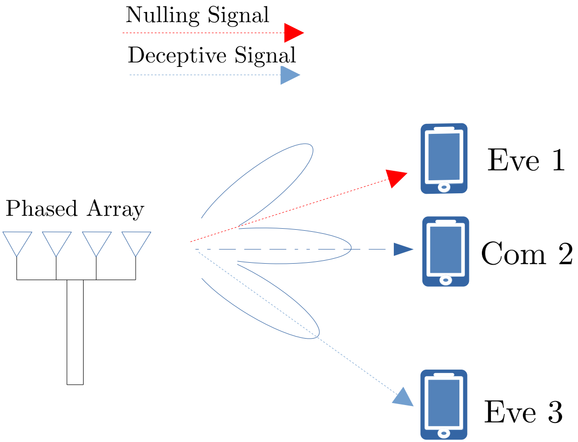
- More advanced techniques like injecting artificial noise towards the direction of the eavesdroppers have been explored in [LCMC11].
- A similar idea is Directional Modulation (DM) which enables secure communication with phased arrays and beamforming [DB09].
- Multi-Function RF (MFRF) systems have proposed the joint design of a signal for communications, RADAR, and electronic RF jamming but without considering eavesdropping [TS22].
- Al alternative is to inject deceptive signals that spoof some parameters of the signal emiitted in the direction of the eavesdroppers [Arg23].




- A transmitter has to face two receivers that eavesdrop (Eve 1 & 3): *We propose to send a deceptive signal with our method (Eve 3) instead of nulling.*

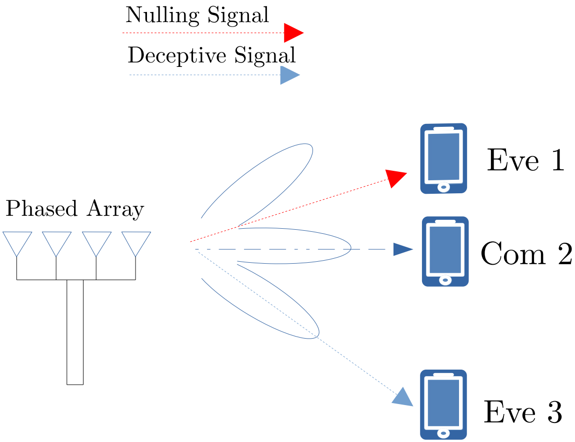
# Eavesdropping & Beamforming

## Deception




- A transmitter has to face two receivers that eavesdrop (Eve 1 & 3): *We propose to send a deceptive signal with our method (Eve 3) instead of nulling.*
- Deception of what?

# Eavesdropping & Beamforming
## Deception




- A transmitter has to face two receivers that eavesdrop (Eve 1 & 3): *We propose to send a deceptive signal with our method (Eve 3) instead of nulling.*
- Deception of what?
- Spoofed relative distance and velocity

# Communication Model

- We consider the OFDM is used for the nominal communication: $\mathbf{x}_i$ are the QAM symbols, $\mathbf{F}^H$ the IDFT matrix.

# Communication Model

- We consider the OFDM is used for the nominal communication: $\mathbf{x}_i$ are the QAM symbols, $\mathbf{F}^H$ the IDFT matrix.
- Consider the $i$-th eavesdropper.

$$\mathbf{y}_i = \mathbf{H}_i^{\text{circ}} \mathbf{F}^H \mathbf{x}_i + \mathbf{n}. \tag{1}$$

$\mathbf{H}_i^{\text{circ}}$ is the circulant channel matrix that includes the effects of the OFDM cyclic prefix.

# Communication Model

- We consider the OFDM is used for the nominal communication: $\mathbf{x}_i$ are the QAM symbols, $\mathbf{F}^H$ the IDFT matrix.
- Consider the $i$-th eavesdropper.

$$\mathbf{y}_i = \mathbf{H}_i^{\text{circ}} \mathbf{F}^H \mathbf{x}_i + \mathbf{n}. \tag{1}$$

  $\mathbf{H}_i^{\text{circ}}$ is the circulant channel matrix that includes the effects of the OFDM cyclic prefix.
- For each OFDM symbol, the OFDM receiver at the $i$-th eavesdropper first performs the typical OFDM processing. That is it applies a DFT to the $L$ samples of the OFDM symbol in $\mathbf{y}_i$ to obtain the frequency-domain (FD) signal:

$$\tilde{\mathbf{y}}_i = \mathbf{F}\mathbf{y}_i = \mathbf{F}\mathbf{H}_i^{\text{circ}} \mathbf{F}^{\mathrm{H}} \mathbf{x}_i + \tilde{\mathbf{n}} = \tilde{\mathbf{H}}_i \mathbf{x}_i + \tilde{\mathbf{n}}. \tag{2}$$

# Signal Pre-Coding for Eavedropper Deception

- We send $\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i}$ instead of $\mathbf{x}_{e,i}$.

## Signal Pre-Coding for Eavedropper Deception

- We send $\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i}$ instead of $\mathbf{x}_{e,i}$.
- Repeating the derivation in (2) now for the eavesdropper we have:

$$\tilde{\mathbf{y}}_{e,i} = \mathbf{F}\mathbf{y} = \mathbf{F}\mathbf{H}_i\mathbf{F}^{\mathbf{H}}\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i} + \tilde{\mathbf{n}} = \tilde{\mathbf{H}}_i\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i} + \tilde{\mathbf{n}}. \tag{3}$$

# Signal Pre-Coding for Eavedropper Deception

- We send $\tilde{\mathbf{H}}_{\mathrm{sp}}\mathbf{x}_{e,i}$ instead of $\mathbf{x}_{e,i}$.
- Repeating the derivation in (2) now for the eavesdropper we have:

$$\tilde{\mathbf{y}}_{e,i} = \mathbf{F}\mathbf{y} = \mathbf{F}\mathbf{H}_i\mathbf{F}^{\mathbf{H}}\tilde{\mathbf{H}}_{\mathrm{sp}}\mathbf{x}_{e,i} + \tilde{\mathbf{n}} = \tilde{\mathbf{H}}_i\tilde{\mathbf{H}}_{\mathrm{sp}}\mathbf{x}_{e,i} + \tilde{\mathbf{n}}. \tag{3}$$

- The above expression allows us to understand how $\tilde{\mathbf{H}}_{\mathrm{sp}}$ should be created: The collective impact of the perceived channel is now $\tilde{\mathbf{H}}_i\tilde{\mathbf{H}}_{\mathrm{sp}}$ for the $i$-th user.

# Signal Pre-Coding for Eavedropper Deception

- We send $\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i}$ instead of $\mathbf{x}_{e,i}$.
- Repeating the derivation in (2) now for the eavesdropper we have:

$$\tilde{\mathbf{y}}_{e,i} = \mathbf{F}\mathbf{y} = \mathbf{F}\mathbf{H}_i\mathbf{F}^{\mathrm{H}}\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i} + \tilde{\mathbf{n}} = \tilde{\mathbf{H}}_i\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i} + \tilde{\mathbf{n}}. \tag{3}$$

- The above expression allows us to understand how $\tilde{\mathbf{H}}_{\text{sp}}$ should be created: The collective impact of the perceived channel is now $\tilde{\mathbf{H}}_i\tilde{\mathbf{H}}_{\text{sp}}$ for the $i$-th user.
- The $\ell$-th entry in the vector $\mathbf{x}_{e,i}$ indicates the symbol that is transmitted in the $\ell$-th subcarrier.

# Signal Pre-Coding for Eavedropper Deception

- We send $\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i}$ instead of $\mathbf{x}_{e,i}$.
- Repeating the derivation in (2) now for the eavesdropper we have:

$$\tilde{\mathbf{y}}_{e,i} = \mathbf{F}\mathbf{y} = \mathbf{F}\mathbf{H}_i\mathbf{F}^{\mathrm{H}}\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i} + \tilde{\mathbf{n}} = \tilde{\mathbf{H}}_i\tilde{\mathbf{H}}_{\text{sp}}\mathbf{x}_{e,i} + \tilde{\mathbf{n}}. \tag{3}$$

- The above expression allows us to understand how $\tilde{\mathbf{H}}_{\text{sp}}$ should be created: The collective impact of the perceived channel is now $\tilde{\mathbf{H}}_i\tilde{\mathbf{H}}_{\text{sp}}$ for the $i$-th user.
- The $\ell$-th entry in the vector $\mathbf{x}_{e,i}$ indicates the symbol that is transmitted in the $\ell$-th subcarrier.
- If $f_\ell$ is the frequency of the $\ell$-th subcarrier we populate this matrix as:

$$[\tilde{\mathbf{H}}_{\text{sp}}]_{\ell,\ell} = \exp(-j2\pi f_\ell \frac{R_{\text{sp}}}{c}) \exp(j2\pi f_{\text{sp}} m T_L). \tag{4}$$

## Optimization Problem

- $\mathbf{A}(\boldsymbol{\theta}_{\mathrm{e}}), \mathbf{A}(\boldsymbol{\theta}_{\mathrm{c}})$ contain the steering vectors towards the eavesdroppers and comms receivers respectively.
- The deceptive wireless beamforming (DWB) problem is:

$$\min_{\mathbf{s},\mathbf{X}_e} \mathbf{s}^{\mathrm{H}}\mathbf{s} \quad \text{s.t. } \mathbf{A}(\boldsymbol{\theta}_{\mathrm{e}})\mathbf{S} = \mathbf{F}^{\mathbf{H}}\tilde{\mathbf{H}}_{\mathrm{sp}}\mathbf{X}_e \qquad (5)$$
$$\mathbf{A}(\boldsymbol{\theta}_{\mathrm{c}})\mathbf{S} = \mathbf{D}_{\mathrm{c}}.$$

- The first constraint states that the OFDM signal can consist of any combination of valid QAM symbols $\mathbf{X}_e$ that will be spoofed with $\tilde{\mathbf{H}}_{\mathrm{sp}}$ and fed into the IDFT $\mathbf{F}^{\mathbf{H}}$ to produce a deceiving OFDM symbol.
- The second constraint corresponds is an under-determined system of linear equations (when $N_T > N_c$).

# Simulations

- Uniform Linear Array of $N_T$ elements
- We consider the Tx and various combinations of wireless receivers (eavedropping and com- munication) that were uniformly distributed at random spatial directions in the range [0,180] degrees, and random distances in the range of [1,100] meters.
- We present average power consumption results at the Tx for 1000 random topology configurations using 64-QAM

# Results - Beampattern

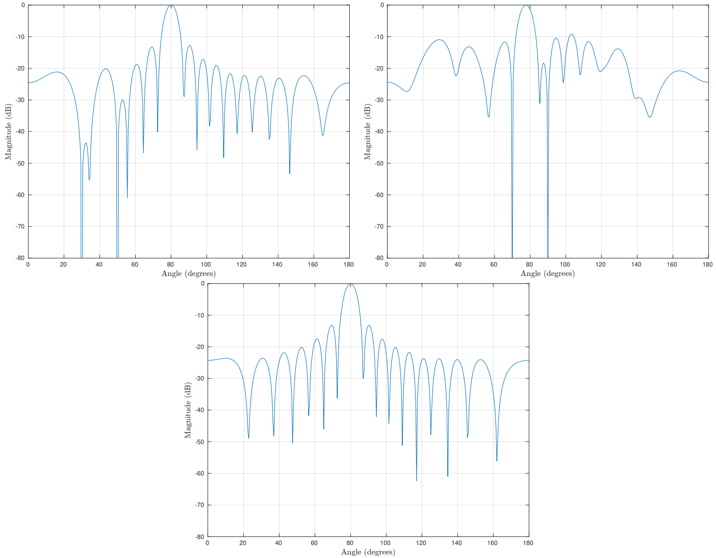
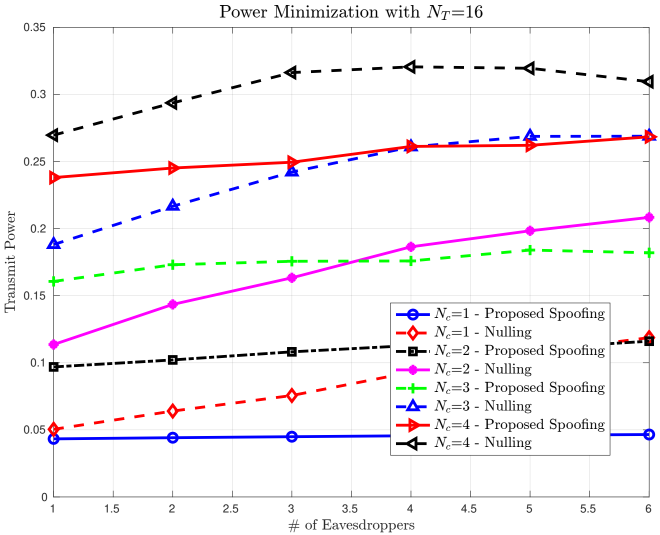


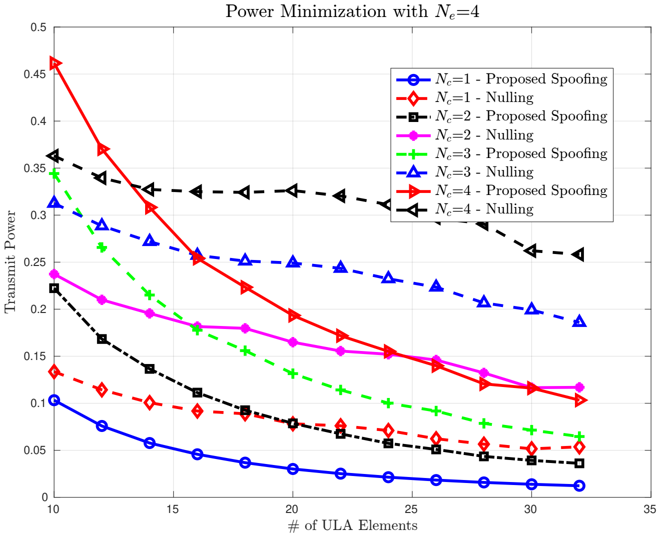

Figure: Array responses for the nulling techniques in (a), (b), and DWB (c).

# Results - Transmit Power (1)

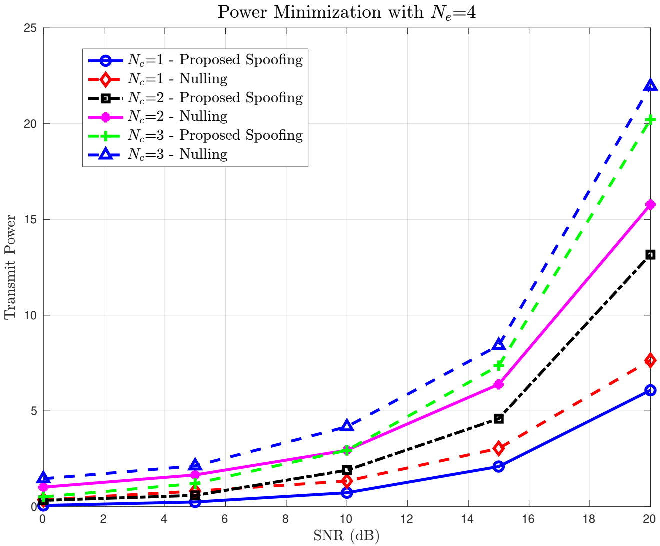



(a) Tx SNR of 10 dB, $N_T = 16$.

# Results - Transmit Power (2)




(b) Tx SNR of 10 dB, $N_e = 4$.




(c) $N_e = 4$ and different $N_c$ and SNR.

## Conclusions

- In this paper we proposed the concept of deceptive wireless beamforming (DWB) to tackle eavesdroppers in OFDM wireless communication systems.

# Conclusions

- In this paper we proposed the concept of deceptive wireless beamforming (DWB) to tackle eavesdroppers in OFDM wireless communication systems.
- DWB deceives the eavesdroppers in terms of range and Doppler (velocity) instead of nulling the signal towards them.

# Conclusions

- In this paper we proposed the concept of deceptive wireless beamforming (DWB) to tackle eavesdroppers in OFDM wireless communication systems.
- DWB deceives the eavesdroppers in terms of range and Doppler (velocity) instead of nulling the signal towards them.
- The beamformer is designed by solving a relaxed QP.

# Conclusions

- In this paper we proposed the concept of deceptive wireless beamforming (DWB) to tackle eavesdroppers in OFDM wireless communication systems.
- DWB deceives the eavesdroppers in terms of range and Doppler (velocity) instead of nulling the signal towards them.
- The beamformer is designed by solving a relaxed QP.
- Simulation results indicate that DWB can lead to a beamformer design that achieves very low transmission power, preserves the beam shape, and ensures the privacy of two location parameters of the Tx.

# References


Antonios Argyriou.
Range-Doppler Spoofing in OFDM Signals for Preventing Wireless Passive Emitter Tracking.
In *IEEE Radar Conference (RadarConf23)*, San Antonio, Texas, 2023.

Michael P. Daly and Jennifer T. Bernhard.
Directional Modulation Technique for Phased Arrays.
*IEEE Transactions on Antennas and Propagation*, 57(9):2633–2640, 2009.

Wei-Cheng Liao, Tsung-Hui Chang, Wing-Kin Ma, and Chong-Yung Chi.
QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach.
*IEEE Transactions on Signal Processing*, 59(3):1202–1216, 2011.

Bo Tang and Petre Stoica.
MIMO Multifunction RF Systems: Detection Performance and Waveform Design.
*IEEE Transactions on Signal Processing*, 70:4381–4394, 2022.