How Secure Is the Time-Modulated Array-Enabled OFDM Directional Modulation?

Zhihao Tao, Zhaoyi Xu, Athina Petropulu

Rutgers The State University of New Jersey

Work supported by ARO grant W911NF2320103 and NSF grants ECCS-2033433, ECCS-2320568

ICASSP 2024 KOREA

Outline

Outline

Introduction

- Physical Layer Security (PLS) can ensure wireless communication security when cryptographic methods fail to provide low latency and scalability.

- Physical Layer Security (PLS) can ensure wireless communication security when cryptographic methods fail to provide low latency and scalability.
- Directional modulation (DM) is a PLS approach, that modulates the antenna transmissions so that the communication information is distorted in all directions except in the directions of the legitimate receivers[1].
- Thus, DM makes it difficult for an eavesdropper who is located in a different direction than the legitimate users to intercept the communication signals it receives.

[1] Daly and Bernhard 2009; Su et al. 2021.

- Physical Layer Security (PLS) can ensure wireless communication security when cryptographic methods fail to provide low latency and scalability.
- Directional modulation (DM) is a PLS approach, that modulates the antenna transmissions so that the communication information is distorted in all directions except in the directions of the legitimate receivers[1].
- Thus, DM makes it difficult for an eavesdropper who is located in a different direction than the legitimate users to intercept the communication signals it receives.
- DM can be achieved by appropriately designing the antenna weights, or via symbol level precoding, that creates interference between the transmitted data symbols.

[1] Daly and Bernhard 2009; Su et al. 2021.

Time-Modulated Arrays (TMA)

- Recently, time-modulated arrays (TMAs) were proposed to construct the DM transmitter[2].

[2] Ding et al. 2019.

Time-Modulated Arrays (TMA)

- Recently, time-modulated arrays (TMAs) were proposed to construct the DM transmitter[2].
- In **TMAs** the antennas connect and disconnect to the RF chain in a *periodic* manner. The connect/disconnect patterns can be designed so that symbols are received intact along a desirable spatial direction and scrambled in all other directions[3].

[2] Ding et al. 2019.
[3] Shan et al. 2018; Huang et al. 2022.

Time-Modulated Arrays (TMA)

- Recently, time-modulated arrays (TMAs) were proposed to construct the DM transmitter[2].

- In **TMAs** the antennas connect and disconnect to the RF chain in a *periodic* manner. The connect/disconnect patterns can be designed so that symbols are received intact along a desirable spatial direction and scrambled in all other directions[3].

- When an OFDM transmit waveform is used, a periodic connect/disconnect pattern over multiple OFDM symbols gives rise to harmonics around the carrier frequency $\rightarrow$ intercarrier interference (scrambling of data symbols)

[2] Ding et al. 2019.

[3] Shan et al. 2018; Huang et al. 2022.

Time-Modulated Arrays (TMA)

- Recently, time-modulated arrays (TMAs) were proposed to construct the DM transmitter[2].
- In **TMAs** the antennas connect and disconnect to the RF chain in a *periodic* manner. The connect/disconnect patterns can be designed so that symbols are received intact along a desirable spatial direction and scrambled in all other directions[3].
- When an OFDM transmit waveform is used, a periodic connect/disconnect pattern over multiple OFDM symbols gives rise to harmonics around the carrier frequency $\rightarrow$ intercarrier interference (scrambling of data symbols)
- TMA is a hardware-based approach and does not require location info on the eavesdroppers or the complex design on the transmitted signals. Its drawback is reduced energy efficiency.

[2] Ding et al. 2019.

[3] Shan et al. 2018; Huang et al. 2022.

Our Contribution

- Previous studies on the TMA DM technique have mainly focused on hardware implementation, energy efficiency improvement, ON-OFF pattern design, and applications, but have not looked into how secure the TMA DM system is.[4]
- In this paper, we investigate the level of security provided by the TMA achieved scrambling.

[4] Nooraiepour et al. 2022; Purushothama et al. 2023; Li et al. 2022; Xu and Petropulu 2023.

Our Contribution

- Previous studies on the TMA DM technique have mainly focused on hardware implementation, energy efficiency improvement, ON-OFF pattern design, and applications, but have not looked into how secure the TMA DM system is.[4]
- In this paper, we investigate the level of security provided by the TMA achieved scrambling.
- We show for the first time that
  - Unless certain action is taken, the TMA OFDM system is actually not secure enough.
  - An eavesdropper could use an Independent Component Analysis (ICA)-based approach and exploit prior knowledge of TMA to defy the TMA scrambling.

[4] Nooraiepour et al. 2022; Purushothama et al. 2023; Li et al. 2022; Xu and Petropulu 2023.

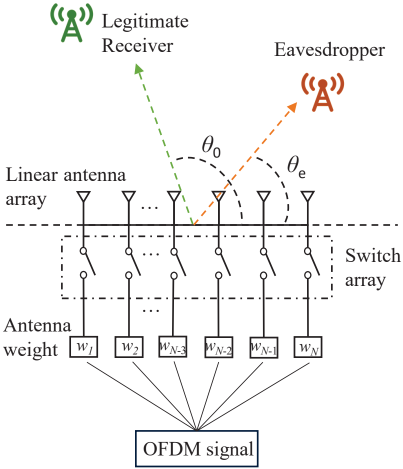
Our Contribution

- Previous studies on the TMA DM technique have mainly focused on hardware implementation, energy efficiency improvement, ON-OFF pattern design, and applications, but have not looked into how secure the TMA DM system is.[4]
- In this paper, we investigate the level of security provided by the TMA achieved scrambling.
- We show for the first time that
  - Unless certain action is taken, the TMA OFDM system is actually not secure enough.
  - An eavesdropper could use an Independent Component Analysis (ICA)-based approach and exploit prior knowledge of TMA to defy the TMA scrambling.
- We also propose a novel TMA implementation mechanism to make the eavesdropper's job harder.

[4] Nooraiepour et al. 2022; Purushothama et al. 2023; Li et al. 2022; Xu and Petropulu 2023.

Outline

- Consider a TMA using a uniform linear array with N elements.
- The array transmits an OFDM waveform with K subcarriers spaced by f_s.



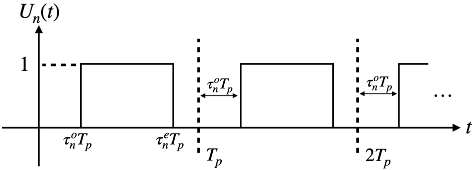
System Model

- Let s_k be the digitally modulated data symbol assigned to the k-th subcarrier. The OFDM symbol equals

$$x(t) = \frac{1}{\sqrt{K}} \sum_{l=1}^{K} s_k e^{j2\pi[f_0+(l-1)f_s]t}. \quad (1)$$

- The OFDM symbol radiated towards direction $\theta \in [0, \pi]$ can be expressed as

$$y(t,\theta) = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} x(t) w_n U_n(t) e^{j(n-1)\pi\cos\theta}, \quad (2)$$



- We set $w_n = e^{-j(n-1)\pi\cos\theta_0}$ to focus the beam towards θ_0.

System Model

- Let the normalized switch ON time instant and the normalized ON time duration be denoted by τ_n^o and $\Delta\tau_n$, respectively, we can expand $U_n(t)$ in the form of Fourier series as

$$U_n(t) = \sum_{-\infty}^{\infty} a_{mn} e^{j2m\pi f_s t}, \tag{3}$$

where

$$a_{mn} = \Delta\tau_n \operatorname{sinc}(m\pi\Delta\tau_n) e^{-jm\pi(2\tau_n^o + \Delta\tau_n)}. \tag{4}$$

- By combining the above equations, we rewrite $y(t,\theta)$ as

$$y(t,\theta) = \frac{1}{\sqrt{NK}} \sum_{l=1}^{K} s_k e^{j2\pi[f_0+(l-1)f_s]t} \sum_{m=-\infty}^{\infty} e^{j2m\pi f_s t} V_m, \tag{5}$$

where

$$V_m = \sum_{n=1}^{N} a_{mn} e^{j(n-1)\pi(\cos\theta - \cos\theta_0)}. \tag{6}$$

- In order to implement DM functionality, τ_n^o and $\Delta\tau_n$ are chosen to satisfy

$$V_{m\neq 0}(\tau_n^o, \Delta\tau_n, \theta = \theta_0) = 0,$$
$$V_{m=0}(\tau_n^o, \Delta\tau_n, \theta = \theta_0) \neq 0. \quad (7)$$

- This can be achieved by the following three conditions:
  - (C1) $\Delta\tau_n, \tau_n^o \in \{\frac{h-1}{N}\}_{h=1,2,\ldots,N}$ (note that the subscript n is not necessarily equal to h)
  - (C2) $\tau_p^o \neq \tau_q^o, \Delta\tau_p = \Delta\tau_q = \Delta\tau$ for $p \neq q$
  - (C3) $\sum_{n=1}^{N} \Delta\tau_n \neq 0$

- For simplicity, we skip noise and assume that same power is assigned to each antenna in each subcarrier.

Outline

The Proposed Formulation at the Eavesdropper

- After OFDM demodulation, the received data symbol on the i-th subcarrier can be expressed as $y_i(\theta) = 1/\sqrt{NK}\sum_{l=1}^{K} s_k V_{i-l}$.

- Based on the signals received on all subcarriers, $\boldsymbol{y}$, the eavesdropper can formulate the problem

$$\boldsymbol{y} = \boldsymbol{V}\boldsymbol{s}, \tag{8}$$

where $\boldsymbol{V} \in \mathbb{C}^{K\times K}$ is a Toeplitz matrix as follows

$$\boldsymbol{V} = \frac{1}{\sqrt{NK}} \begin{bmatrix} V_0 & V_{-1} & \cdots & V_{-(K-2)} & V_{-(K-1)} \\ V_1 & V_0 & \cdots & V_{-(K-3)} & V_{-(K-2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ V_{K-2} & V_{K-3} & \cdots & V_0 & V_{-1} \\ V_{K-1} & V_{K-2} & \cdots & V_1 & V_0 \end{bmatrix}, \tag{9}$$

and $\boldsymbol{s} = [s_1, s_2, \cdots, s_K]^T$.

The Proposed Formulation at the Eavesdropper

- Due to (C1)-(C3), along θ_0, $\boldsymbol{V}$ is diagonal and the received signal equals $\boldsymbol{y}(\theta_0) = \Delta\tau\sqrt{N/K}\boldsymbol{s}$.

The Proposed Formulation at the Eavesdropper

- Due to (C1)-(C3), along θ_0, $\boldsymbol{V}$ is diagonal and the received signal equals $\boldsymbol{y}(\theta_0) = \Delta\tau\sqrt{N/K}\boldsymbol{s}$.
- In all other directions, the signal of each subcarrier contains the harmonic signals from all other subcarriers, which gives rise to **symbol scrambling**.

The Proposed Formulation at the Eavesdropper

- Due to (C1)-(C3), along θ_0, $\boldsymbol{V}$ is diagonal and the received signal equals $\boldsymbol{y}(\theta_0) = \Delta\tau\sqrt{N/K}\boldsymbol{s}$.
- In all other directions, the signal of each subcarrier contains the harmonic signals from all other subcarriers, which gives rise to **symbol scrambling**.
- In $\boldsymbol{y} = \boldsymbol{V}\boldsymbol{s}$, the elements of $\boldsymbol{s}$ are statistically independent and non-Gaussian. Although $\boldsymbol{V}$ is unknown to the eavesdropper, $\boldsymbol{s}$ can be estimated from $\boldsymbol{y}$ with **ambiguities** via an ICA approach.

[5] Hyvärinen 1999.

The Proposed Formulation at the Eavesdropper

- Due to (C1)-(C3), along θ_0, $\boldsymbol{V}$ is diagonal and the received signal equals $\boldsymbol{y}(\theta_0) = \Delta\tau\sqrt{N/K}\boldsymbol{s}$.
- In all other directions, the signal of each subcarrier contains the harmonic signals from all other subcarriers, which gives rise to **symbol scrambling**.
- In $\boldsymbol{y} = \boldsymbol{V}\boldsymbol{s}$, the elements of $\boldsymbol{s}$ are statistically independent and non-Gaussian. Although $\boldsymbol{V}$ is unknown to the eavesdropper, $\boldsymbol{s}$ can be estimated from $\boldsymbol{y}$ with **ambiguities** via an ICA approach.
- ICA tries to find $\boldsymbol{W}$ such that $\boldsymbol{W}\boldsymbol{y}$ is maximally non-Gaussian.

[5] Hyvärinen 1999.

The Proposed Formulation at the Eavesdropper

- Due to (C1)-(C3), along θ_0, $\boldsymbol{V}$ is diagonal and the received signal equals $\boldsymbol{y}(\theta_0) = \Delta\tau\sqrt{N/K}\boldsymbol{s}$.
- In all other directions, the signal of each subcarrier contains the harmonic signals from all other subcarriers, which gives rise to **symbol scrambling**.
- In $\boldsymbol{y} = \boldsymbol{V}\boldsymbol{s}$, the elements of $\boldsymbol{s}$ are statistically independent and non-Gaussian. Although $\boldsymbol{V}$ is unknown to the eavesdropper, $\boldsymbol{s}$ can be estimated from $\boldsymbol{y}$ with **ambiguities** via an ICA approach.
- ICA tries to find $\boldsymbol{W}$ such that $\boldsymbol{W}\boldsymbol{y}$ is maximally non-Gaussian.
- In this work, we adopt negentropy to measure non-Gaussianity and implement FastICA[5] to find $\boldsymbol{W}$.

[5] Hyvärinen 1999.

Addressing Scaling and Permutation Ambiguities in $\boldsymbol{W}$

- The inverse of $\boldsymbol{W}$, produced by ICA, may not be equal to the actual mixing matrix, $\boldsymbol{V}$, since there exist scaling and permutation ambiguities in $\boldsymbol{W}$. Those ambiguities would prevent the correct recovery of source symbols.

Addressing Scaling and Permutation Ambiguities in $\boldsymbol{W}$

- The inverse of $\boldsymbol{W}$, produced by ICA, may not be equal to the actual mixing matrix, $\boldsymbol{V}$, since there exist scaling and permutation ambiguities in $\boldsymbol{W}$. Those ambiguities would prevent the correct recovery of source symbols.

- **Assumptions:** The eavesdropper knows
  - The OFDM specifics of the transmitted signals, e.g., the number of subcarriers, K, and spacing f_s
  - The data modulation scheme
  - The rules (C1)-(C3) which the transmitter used to select the TMA parameters.

Addressing Scaling and Permutation Ambiguities in $\boldsymbol{W}$

- The inverse of $\boldsymbol{W}$, produced by ICA, may not be equal to the actual mixing matrix, $\boldsymbol{V}$, since there exist scaling and permutation ambiguities in $\boldsymbol{W}$. Those ambiguities would prevent the correct recovery of source symbols.

- **Assumptions:** The eavesdropper knows
  - The OFDM specifics of the transmitted signals, e.g., the number of subcarriers, K, and spacing f_s
  - The data modulation scheme
  - The rules (C1)-(C3) which the transmitter used to select the TMA parameters.

- The scaling ambiguity can be divided into amplitude and phase ambiguity. Knowledge of the transmit constellation can be used to resolve the amplitude scaling ambiguity.

Resolving the Permutation Ambiguity

- To solve the permutation ambiguity we leverage the fact that $\boldsymbol{V}$ is a Toeplitz matrix.

Resolving the Permutation Ambiguity

- To solve the permutation ambiguity we leverage the fact that $\boldsymbol{V}$ is a Toeplitz matrix.

- Let $\boldsymbol{F} \stackrel{\triangle}{=} \boldsymbol{W}^{-1}$.
  In the absence of ambiguities, it would hold that $\boldsymbol{F} = \boldsymbol{V}$ and thus $\boldsymbol{F}$ would have a Toeplitz structure.

Resolving the Permutation Ambiguity

- To solve the permutation ambiguity we leverage the fact that $\boldsymbol{V}$ is a Toeplitz matrix.

- Let $\boldsymbol{F} \stackrel{\triangle}{=} \boldsymbol{W}^{-1}$.
  In the absence of ambiguities, it would hold that $\boldsymbol{F} = \boldsymbol{V}$ and thus $\boldsymbol{F}$ would have a Toeplitz structure.

- We reorder $\boldsymbol{F}$, checking whether the reordering creates a Toeplitz matrix.
  - There are $K!$ possible orderings
  - Considering the fact that the main diagonal elements can determine the Toeplitz structure of $\boldsymbol{F}$, we focus on the main diagonal elements
  - We use standard deviation, σ, to measure the similarity of the main diagonal elements

Resolving the Permutation Ambiguity

Algorithm 1 Reordering Algorithm

1: Calculate the amplitude of each elements in $\boldsymbol{F}$ and get a new matrix $\boldsymbol{Q}$, the ith column of which is denoted by $\boldsymbol{q}_i$;
2: **for each** $i = 1, 2, ..., K$ **do**
3: Take $\boldsymbol{q}_i(1)$ as the first diagonal element in the first row of $\boldsymbol{Q}$;
4: Find the closest elements to $\boldsymbol{q}_i(1)$ in the remaining rows of $\boldsymbol{Q}$ and put them in the corresponding diagonal placements;
5: Obtain a diagonal vector $\boldsymbol{d}$ after step 4 and normalize it by $\boldsymbol{d}/\|\boldsymbol{d}\|$;
6: Compute the standard deviation σ_i of normalized $\boldsymbol{d}$;
7: **end for**
8: Let $\boldsymbol{\sigma} = [\sigma_1, ..., \sigma_K]$ and find the index of the minimum element in $\boldsymbol{\sigma}$ as I;
9: Let $i = I$ and execute steps 3 and 4, we can obtain a reordered $\boldsymbol{Q}$ and accordingly reordered $\boldsymbol{F}$.

- The complexity of the process is $O(K^3)$.

Resolving the Scaling Phase Ambiguity

- Regarding the **phase scaling ambiguity**, we exploit the knowledge of the Toeplitz structure first.
  - For M-PSK modulation, there will be M^K phase possibilities for $\boldsymbol{F}$
  - The Toeplitz constraint can reduce it to M since the phases of diagonal elements of $\boldsymbol{F}$ must be the same, and each source signal can have up to M phase transformations. Denote these possibilities as $\boldsymbol{F}_1, \boldsymbol{F}_2, ..., \boldsymbol{F}_M$.

Resolving the Scaling Phase Ambiguity

- Regarding the **phase scaling ambiguity**, we exploit the knowledge of the Toeplitz structure first.
  - For M-PSK modulation, there will be M^K phase possibilities for $\boldsymbol{F}$
  - The Toeplitz constraint can reduce it to M since the phases of diagonal elements of $\boldsymbol{F}$ must be the same, and each source signal can have up to M phase transformations. Denote these possibilities as $\boldsymbol{F}_1, \boldsymbol{F}_2, ..., \boldsymbol{F}_M$.

- Let $\phi = \cos\theta_e - \cos\theta_0$. It holds that

$$V_0 = \Delta\tau \sum_{n=1}^{N} e^{j(n-1)\pi\phi} = \Delta\tau \frac{\sin(\frac{N}{2}\pi\phi)}{\sin(\frac{1}{2}\pi\phi)} e^{j\frac{(N-1)}{2}\pi\phi}. \tag{10}$$

- Then we obtain

$$\gamma \triangleq \frac{Re(V_0)}{Im(V_0)} = \frac{1}{\tan \frac{N-1}{2}\pi\phi} = \frac{Re(\mathbf{V}(1,1))}{Im(\mathbf{V}(1,1))}, \tag{11}$$

Resolving the Scaling Phase Ambiguity

- Then we obtain

$$\gamma \triangleq \frac{Re(V_0)}{Im(V_0)} = \frac{1}{\tan \frac{N-1}{2}\pi\phi} = \frac{Re(\mathbf{V}(1,1))}{Im(\mathbf{V}(1,1))}, \tag{11}$$

- To resolve the remaining phase ambiguity, we check whether there exist solutions of N, $\Delta\tau$, $\{\tau_n^o\}_{n=1,2,\ldots,N}$ according with (C1)-(C3) and φ that correspond to exactly one of the elements in $\{\boldsymbol{F}_u\}_{u=1,2,\ldots,M}$.

Resolving the Scaling Phase Ambiguity

- Then we obtain

$$\gamma \triangleq \frac{Re(V_0)}{Im(V_0)} = \frac{1}{\tan \frac{N-1}{2}\pi\phi} = \frac{Re(\mathbf{V}(1,1))}{Im(\mathbf{V}(1,1))}, \tag{11}$$

- To resolve the remaining phase ambiguity, we check whether there exist solutions of N, $\Delta\tau$, $\{\tau_n^o\}_{n=1,2,\ldots,N}$ according with (C1)-(C3) and φ that correspond to exactly one of the elements in $\{\boldsymbol{F}_u\}_{u=1,2,\ldots,M}$.

- The steps of resolving the phase ambiguity are exhibited in the following algorithm.

Resolving the Scaling Phase Ambiguity

Algorithm 2 Phase Ambiguity Resolving Algorithm

```
Obtain {F_u}_{u=1,2,...,M} according to the transmission constellation and the Toeplitz structure;
Calculate the ratio of the real part and the imaginary part of each F_u, denoted as {λ_u}_{u=1,2,...,M}, respectively;
for each λ_u do
    Compute N_u and Δτ_u according to (6) and λ = 1/tan((N−1)/2 πφ);
    Check if N_u ∈ G_N and if Δτ_u ∈ [0,1]: if both are yes, keep this group of solutions; otherwise, discard them;
end for
if Only one group of N_u and Δτ_u found then
    Return F_u corresponding to this group of solutions;
else
    for each group of N_u and Δτ_u do
        Check if {τ_n^o}_{n=1,2,...,N} can be found by (C1)-(C3) and (5): if yes, keep this group of solutions and return the corresponding F_u; otherwise, discard them.
    end for
end if
```

Defending the TMA Scrambling

- Since the above ICA can work only in stationary environments and necessitates long data for estimating the required higher-order statistics, we can disturb the applicability of ICA by changing the mixing matrix of TMA over time.

Defending the TMA Scrambling

- Since the above ICA can work only in stationary environments and necessitates long data for estimating the required higher-order statistics, we can disturb the applicability of ICA by changing the mixing matrix of TMA over time.

- This can be done by selecting randomly $\{\tau_n^o\}_{n=1,2,\ldots,N}$ in each OFDM symbol period according to $\tau_n^o \in \{\frac{h-1}{N}\}_{h=1,2,\ldots,N}$ and $\tau_p^o \neq \tau_q^o$.

Defending the TMA Scrambling

- Since the above ICA can work only in stationary environments and necessitates long data for estimating the required higher-order statistics, we can disturb the applicability of ICA by changing the mixing matrix of TMA over time.
- This can be done by selecting randomly $\{\tau_n^o\}_{n=1,2,\ldots,N}$ in each OFDM symbol period according to $\tau_n^o \in \{\frac{h-1}{N}\}_{h=1,2,\ldots,N}$ and $\tau_p^o \neq \tau_q^o$.
- Also, this mechanism is able to maintain the DM functionality as it still satisfies the above scrambling scheme.

Outline

Numerical Results

- We simulated a TMA OFDM scenario with $N = 7$ antennas, $K = 16$ subcarriers, and BPSK data modulation. The eavesdropper collects $H = 1\text{e}5$ OFDM symbols.

Numerical Results

- We simulated a TMA OFDM scenario with $N = 7$ antennas, $K = 16$ subcarriers, and BPSK data modulation. The eavesdropper collects $H = 1\text{e}5$ OFDM symbols.

- We conducted 6 experiments: in each one, the legitimate user is at θ_0, and the eavesdropper at θ_e.

Table: Average BER of the TMA system

No.	$\theta_0(^\circ)$	$\theta_e(^\circ)$	φ	BER1	BER2	BER3
1	50	90	-0.6428	0.3080	0	0.4504
2	60	30	0.3660	0.2640	0	0.5218
3	80	40	0.5924	0.4474	0	0.5004
4	30	70	/	0.5487	0	0.4168
5	40	90	/	0.3754	0	0.4824
6	50	130	/	0.2744	0	0.4789

Numerical Results

- Next, we set $\theta_0 = 60^\circ$, $\theta_e = 30^\circ$, $N = 7$, $\Delta\tau = 1/N$, $\{\tau_n^o\}_{n=1,2,\ldots,N} = (n-1)/N$, φ is assumed to be known.

- Next, we set $\theta_0 = 60°$, $\theta_e = 30°$, $N = 7$, $\Delta\tau = 1/N$, $\{\tau_n^o\}_{n=1,2,\ldots,N} = (n-1)/N$, φ is assumed to be known.

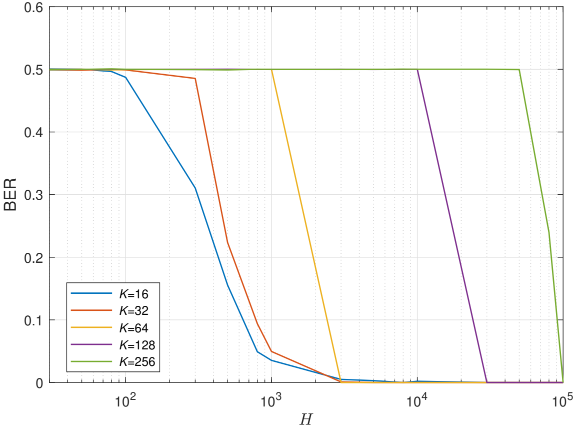


Figure: Scrambling defying performance comparison.

Outline

Conclusions

- We have shown, for the first time, that the data scrambling of TMA OFDM DM systems can be defied by an eavesdropper.

Conclusions

- We have shown, for the first time, that the data scrambling of TMA OFDM DM systems can be defied by an eavesdropper.
- We have shown that based on the scrambled symbols, the eavesdropper can formulate a blind source separation problem, and introduced a novel ICA-based scheme that can infer the mixing matrix with no ambiguities and recover the transmitted symbols.

Conclusions

- We have shown, for the first time, that the data scrambling of TMA OFDM DM systems can be defied by an eavesdropper.

- We have shown that based on the scrambled symbols, the eavesdropper can formulate a blind source separation problem, and introduced a novel ICA-based scheme that can infer the mixing matrix with no ambiguities and recover the transmitted symbols.

- We have also proposed a simple TMA implementation mechanism to make the job of the eavesdropper harder.

Conclusions

- We have shown, for the first time, that the data scrambling of TMA OFDM DM systems can be defied by an eavesdropper.
- We have shown that based on the scrambled symbols, the eavesdropper can formulate a blind source separation problem, and introduced a novel ICA-based scheme that can infer the mixing matrix with no ambiguities and recover the transmitted symbols.
- We have also proposed a simple TMA implementation mechanism to make the job of the eavesdropper harder.
- Numerical results have demonstrated the effectiveness and efficiency of proposed defying and defending approaches.

- Daly, Michael P. and Jennifer T. Bernhard (2009). "Directional Modulation Technique for Phased Arrays". In: *IEEE Transactions on Antennas and Propagation*. DOI: 10.1109/TAP.2009.2027047.
- Ding, Yuan et al. (2019). "Time-Modulated OFDM Directional Modulation Transmitters". In: *IEEE Transactions on Vehicular Technology*. DOI: 10.1109/TVT.2019.2924543.
- Huang, Gaojian et al. (2022). "Target Localization Using Time-modulated Directional Modulated Transmitters". In: *IEEE Sensors Journal*, pp. 1–1. DOI: 10.1109/JSEN.2022.3178699.
- Hyvärinen, A. (1999). "Fast and robust fixed-point algorithms for independent component analysis". In: *IEEE Transactions on Neural Networks*. DOI: 10.1109/72.761722.

Li, Haotian, Yikai Chen, and Shiwen Yang (2022). "Chaotic-Enabled Phase Modulation in Time-Modulated Arrays for Secure Transmission". In: *IEEE Transactions on Antennas and Propagation* 70.11, pp. 10454–10464. DOI: 10.1109/TAP.2022.3191162.

Nooraiepour, Alireza et al. (2022). "Time-varying metamaterial-enabled directional modulation schemes for physical layer security in wireless communication links". In: *ACM Journal on Emerging Technologies in Computing Systems* 18.4, pp. 1–20.

Purushothama, Jayakrishnan Methapettyparambu et al. (2023). "Synthesis of Energy Efficiency-Enhanced Directional Modulation Transmitters". In: *IEEE Transactions on Green Communications and Networking*. DOI: 10.1109/TGCN.2022.3208023.

- Shan, Chengzhao et al. (2018). "Joint radar-communications design based on time modulated array". In: *Digital Signal Processing* 82, pp. 43–53. ISSN: 1051-2004. DOI: https://doi.org/10.1016/j.dsp.2018.07.013. URL: https://www.sciencedirect.com/science/article/pii/S1051200418305505.
- Su, Nanchi, Fan Liu, and Christos Masouros (2021). "Secure Radar-Communication Systems With Malicious Targets: Integrating Radar, Communications and Jamming Functionalities". In: *IEEE Transactions on Wireless Communications* 20.1, pp. 83–95. DOI: 10.1109/TWC.2020.3023164.
- Xu, Zhaoyi and Athina P. Petropulu (2023). "A Secure Dual-Function Radar Communication System via Time-Modulated Arrays". In: *2023 IEEE Radar Conference (RadarConf23)*. DOI: 10.1109/RadarConf2351548.2023.10149569.