

A Novel Physical Layer Design for Addressing the Trade-off between Security and Energy Efficiency

Jules Burgat^{*†}, Jean-Baptiste Doré^{*}, Joumana Farah[†], Matthieu Crussière[†]

^{*}CEA-Leti, Univ. Grenoble Alpes, Grenoble, France,

[†]Univ Rennes, INSA Rennes, CNRS, IETR-UMR 6164, F-35000 Rennes, France.

Abstract—Security remains a key challenge in wireless communications, especially with the rise of critical applications such as remote healthcare, autonomous vehicles, industrial control systems, and satellite communications. Physical layer security (PLS) offers an attractive alternative or complement to cryptographic methods by leveraging the physical properties of the transmission channel, eliminating the need for key distribution. Building on Wyner’s wiretap model, PLS has inspired schemes such as artificial noise (AN) and out-phased array linearized signaling (OPALS), each offering different trade-offs between energy efficiency, security, and complexity. In this work, we propose two novel PLS schemes that bridge the gap between AN and OPALS. We introduce the beamforming loss (BL) as a metric to evaluate the energy overhead of securing transmissions. Our methods are evaluated based on several criteria: BL, peak-to-average power ratio (PAPR), and resilience to eavesdroppers, under various attacks. Results demonstrate that the proposed schemes balance the high security of AN and the energy efficiency of OPALS.

Index Terms— Physical layer security, energy efficiency, artificial noise, OPALS, beamforming loss, PAPR

I. INTRODUCTION

Security is a cornerstone of modern communication systems, especially as wireless technologies continue to evolve and proliferate across critical applications. Traditional cryptographic solutions provide robust protection against eavesdropping but rely heavily on key distribution and computational assumptions, which may be vulnerable to advances in computing power, such as quantum technologies. In this context, PLS has emerged as a promising alternative or complement to classical encryption, especially for satellite communications as presented in [1]. Unlike cryptographic approaches, PLS mechanisms exploit the physical characteristics of the communication channel to secure information, inherently avoiding the need for key sharing. This makes PLS particularly attractive for low-latency, low-complexity, or resource-constrained environments. The foundation of PLS was established in Wyner’s seminal work on the wiretap channel [2], which introduced a theoretical framework showing that secure and reliable communication is achievable over a degraded channel without the use of secret keys, by maximizing both the transmission rate and the equivocation at the eavesdropper.

Beamforming [3] represents the most basic and least secure form of PLS, relying solely on directing signal energy toward the legitimate receiver to reduce signal leakage. However, its security is highly limited, especially in the presence of multiple and/or well-positioned eavesdroppers. To overcome these limitations, more advanced PLS techniques have been proposed, such as directional modulation (DM) [4] and symbol-level precoding [5]. Among them, AN [6] and OPALS [7] have garnered significant attention due to their complementary strengths in enhancing secrecy and improving energy efficiency, respectively.

AN enhances secrecy by injecting structured interference into the transmitted signal, degrading the eavesdropper’s channel while having minimal impact on the legitimate receiver. This approach is particularly effective in multi-antenna scenarios, where the spatial degrees of freedom can be exploited to align the artificial noise in directions orthogonal to the intended user. However, the price to pay is the allocation of additional resources to AN, both in terms of spatial dimensions and transmit power. On the other hand, OPALS, introduced in [7], focuses on achieving a balance between secrecy and energy efficiency. It leverages waveform-level signal design and Linear amplification with nonlinear components (LINC) techniques [8] to significantly reduce the PAPR, which is a common limitation in power-constrained systems like satellite or Internet of Things (IoT) networks. By shaping the transmitted symbols to lie on concentric rings with controlled phases, OPALS achieves both low envelope variation and an inherent level of security, albeit at the cost of increased power to preserve the low envelope variation.

The two schemes, although effective individually, present different trade-offs. While AN generally provides stronger secrecy guarantees, it often comes at the cost of higher energy consumption and PAPR. Conversely, OPALS offers better energy efficiency and hardware friendliness, but may be less robust to sophisticated eavesdropping strategies. Understanding and optimizing these trade-offs is a central theme of this work. We propose a hybrid physical-layer security scheme that combines the strengths of AN and OPALS, aiming to achieve a balance between the high secrecy performance of AN and the energy efficiency and low PAPR of OPALS. To ensure a fair and comprehensive comparison, we introduce the notion of BL, which quantifies the energy overhead induced by securing the transmission compared to a naive multi-antenna beamforming system. The methods are evaluated according to multiple criteria, including BL, PAPR robustness against both naive and sophisticated eavesdroppers, and resistance to brute-force attacks. Our analysis shows that the proposed methods provide a balanced compromise between the low PAPR of OPALS and the high security of AN.

The remainder of the paper is structured as follows. In Section II, we present the system model, including the definition of beamforming loss and the mathematical formulation of the proposed schemes. Section III provides a theoretical analysis of the new schemes’ BL as well as a theoretical comparison of their security performance. Simulation results are presented in Section IV, where the different methods are compared under realistic settings. Finally, Section V concludes the paper and discusses future research directions.

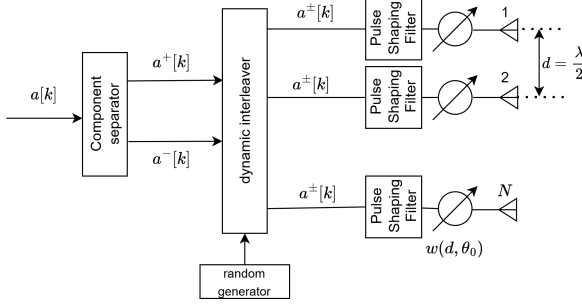


Fig. 1: Dynamic Directional Modulation System.

II. SYSTEM MODEL

A. Overview

We consider a general dynamic Directional Modulation (DM) system, illustrated in Figure 1. The transmitter aims to deliver a message to a single-antenna receiver located at direction $\theta_0 \in [-\frac{\pi}{2}, \frac{\pi}{2}]$.

The transmitter is equipped with N antennas uniformly spaced along the vertical axis, with inter-antenna spacing d , typically set to $\frac{\lambda}{2}$, where λ is the signal wavelength. At each time instant k , the data symbol $a[k]$ —drawn from an M -ary quadrature amplitude modulation (QAM) or any other modulation—is split by the component separator into two sub-signals $a^+[k]$ and $a^-[k]$, satisfying $a^+[k] + a^-[k] = 2a[k]$. The sequence $(a[k])_k$ is supposed to be i.i.d. and normalized, i.e., $\mathbb{E}[|a[k]|^2] = 1$, where $\mathbb{E}[\cdot]$ is the expectation of a random variable. A dynamic interleaver then distributes these sub-signals across the antenna array, assuming an even number of antennas for balanced processing.

The line-of-sight (LoS) channel model considered in this work is representative of practical scenarios such as satellite communications and is consistent with the assumptions adopted in the literature, including OPALS and the recent works [9], section II-A. Under the far-field assumption, a phase shift of $2\pi\alpha \sin \theta$ occurs between adjacent antennas in the direction θ , where $\alpha = d/\lambda$. Let $\mathbf{w}_\theta = [1, \dots, e^{-2j\pi(N-1)\alpha \sin \theta}]$ be the spatial channel response in direction θ . Beamforming weights $\bar{\mathbf{w}}_{\theta_0}$ are applied at the transmitter to focus energy towards direction θ_0 . Therefore, the received signal at angle θ and time k is:

$$r_\theta[k] = h[k] \sum_{n=0}^{N-1} e^{jn\tilde{\theta}} a^\pm[k] + \eta[k], \quad (1)$$

where:

- $a^\pm[k]$ denotes either $a^+[k]$ or $a^-[k]$ depending of which antenna proceed $a^+[k]$ and $a^-[k]$,
- $h[k] \in \mathbb{C}$ is an attenuation constant whose amplitude is proportional to the emitter-receiver distance,
- $\eta[k]$ is the additive white Gaussian noise (AWGN) of power σ_n^2 ,
- $\tilde{\theta} = 2\pi\alpha(\sin \theta_0 - \sin \theta)$.

For $\theta = \theta_0$ (i.e., the intended direction), we have $\tilde{\theta} = 0$. In this case, as as many antenna proceed $a^+[k]$ than $a^-[k]$, we have $r_{\theta_0}[k] = h[k] N a[k]$ and thus the legitimate receiver obtains the desired signal $a[k]$ without distortion and without the knowledge of the random source generation. Notably, this method does not require any secret sharing, which makes it particularly attractive compared to conventional secure transmission schemes.

When the per-antenna transmitted power is normalized to 1, and the attenuation constant $h[k]$ is supposed to be 1, the desired signal at $\theta = \theta_0$ is scaled by a factor of $N/\sqrt{\mathbb{E}[|a^\pm|^2]}$. By contrast, in a conventional beamforming system without security constraints, the scaling factor is N . We define the BL, denoted by B_{loss} , as the ratio between the gain of the conventional beamforming system and that of the proposed framework for the same per-antenna emitted power:

$$B_{\text{loss}} = \frac{N^2}{N^2/\mathbb{E}[|a^\pm|^2]} = \mathbb{E}[|a^\pm|^2]. \quad (2)$$

This definition highlights the inherent trade-off between security and power efficiency. In unintended directions ($\theta \neq \theta_0$), the signal undergoes distortion due to the dynamic mapping and phase misalignment.

Next, we present our method which focuses on the construction of the sub-signals $a^\pm$.

B. Mathematical description of the proposed method

The proposed approach falls within the class of dynamic directional modulation (DDM) systems. The symbol $a[k]$ is decomposed into the superposition of two phase-shifted components whose amplitudes are jointly controlled by a time-varying scaling parameter. The sub-signals $a^\pm[k]$ are defined as:

$$a_{\text{dyn}}^+[k] := a[k] \left(1 + j \sqrt{\frac{R[k]^2}{|a[k]|^2} - 1} \right), \quad (3)$$

$$a_{\text{dyn}}^-[k] := a[k] \left(1 - j \sqrt{\frac{R[k]^2}{|a[k]|^2} - 1} \right). \quad (4)$$

where $R[k]$ denotes a real-valued, time-varying scaling parameter. It can be verified that $a_{\text{dyn}}^+[k] + a_{\text{dyn}}^-[k] = 2a[k]$.

(a) **Deterministic scheme:** The auxiliary signal is defined as

$$R[k] = R_{\text{det},a[k]} = |a[k]| + \epsilon, \quad (5)$$

and $\epsilon > 0$ is a fixed margin parameter.

(b) **Randomized scheme:** The auxiliary signal is given by

$$R[k] = R_{\text{rand},a[k]} = |a[k]| + X, \quad (6)$$

where $X \sim \mathcal{U}([0, \epsilon])$ is a uniformly distributed random variable over the interval $[0, \epsilon]$. The probability density function (PDF) of X is

$$f_X(x) = \frac{1}{\epsilon} \mathbb{1}_{[0, \epsilon]}(x), \quad (7)$$

where $\mathbb{1}_{[0, \epsilon]}(\cdot)$ denotes the indicator function.

This randomized model introduces controlled fluctuations in the signal modulus, thereby increasing the uncertainty experienced by the eavesdropper. The expected value and variance of X are given by $\mathbb{E}[X] = \epsilon/2$ and $\text{Var}[X] = \epsilon^2/12$, respectively. Consequently, the parameter ϵ governs the average amount of additional energy injected into the signal: larger values of ϵ yield greater expected deviations and potentially enhanced security, at the cost of reduced energy efficiency.

Note that using a decomposition $\tilde{R}_{a[k]} = |a[k]| + \tilde{X}$ with $\tilde{X} \sim \mathcal{U}([0, \epsilon_{a[k]}])$ is also a conceivable approach, but it does not yield significant improvement compared to the randomized strategy within the scope of our analysis.

These decompositions can also be interpreted through the lens of AN, as the emitted signal is a sum of the signal of interest superimposed with an auto-generated noise. The four decomposition methods are exemplified in Figure 2. The received constellation in direction $\theta = 0.2$ with $\theta_0 = 0$ is also shown in each case. As shown in the figure, the number of possible transmitted symbols for OPALS and the deterministic decomposition is finite, in contrast to AN and the randomized method, which exhibit an infinite symbol set. From a security perspective, infinite cardinality is a desirable property, as it increases the difficulty of message recovery at eavesdroppers. Conversely, a finite candidate set could enable a sophisticated eavesdropper to perform a brute-force search to recover $a[k]$, as highlighted in [5]. The constant-envelope property of the OPALS decomposition is evident, as all sub-signals lie on circles of equal radius. The following section presents the theoretical security performance of each method, regarding the attacks presented in [10] and [11]. More specifically, we provide theoretical insights into the energy efficiency of our proposed techniques and evaluate the robustness of the different schemes against an eavesdropper equipped with multiple sensors.

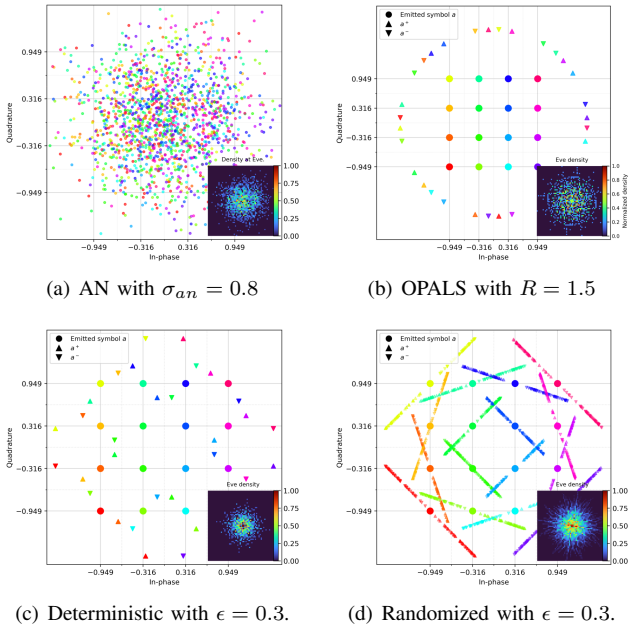


Fig. 2: Transmitter-side signal decomposition of the original message using different methods. The 2D-density of the received constellation observed by an eavesdropper located at $\theta = 0.2$ is shown in the bottom-right corner of each subfigure.

III. THEORETICAL COMPARISON

A. Energy efficiency

The aim of this section is to evaluate the security of each method with respect to its energy efficiency. We compare the robustness of two baseline approaches—AN and OPALS—under various eavesdropping scenarios, using the BL as a metric. The proposed strategies from Section II-B are also included in this analysis. The first lemma is introduced to derive the BL of the two novel strategies.

Lemma 1. Let $\{a[k]\}_{k \in \mathbb{N}}$ be a normalized symbol sequence from any modulation scheme. For the deterministic and randomized decompositions defined in Section II-B and parameterized by $\epsilon > 0$, the expected power of each sub-signal $a_{dyn}^\pm[k]$ is:

$$\mathbb{E}[|a_{dyn}^\pm[k]|^2] = \begin{cases} 1 + 2\epsilon \mathbb{E}[|a[k]|] + \epsilon^2, & (\text{deterministic}), \\ 1 + \epsilon \mathbb{E}[|a[k]|] + \frac{\epsilon^2}{3}, & (\text{randomized}). \end{cases} \quad (8)$$

Accordingly, the corresponding BL for both schemes is given by

$$B_{loss} = \mathbb{E}[|a_{dyn}^\pm[k]|^2]. \quad (9)$$

Proof. First, using the structure of sub-signals $a^\pm[k]$ from Section II-B, one can show that $|a[k]^+| = |a[k]^-|$ for both methods. Then, after squaring (3) and (4), the results follow from the constellation normalization $\mathbb{E}[|a[k]|^2] = 1$ and the fact that $\mathbb{E}[|U|] = \epsilon/2$ and $\mathbb{E}[|U|^2] = \epsilon^2/12$, if X is a uniform random variable over $[0, \epsilon]$. $\square$

The principle of AN is recalled in Appendix A. Its BL is given by

$$B_{loss}(\text{AN}) = \frac{1}{1 - \sigma_{an}^2},$$

where σ_{an}^2 is the power allocated to the artificial noise, leaving $(1 - \sigma_{an}^2)$ for the useful signal. We can now proceed to compare the different methods in terms of security while also accounting for energy efficiency.

B. Robustness against a multi-sensor eavesdropper

A widely studied eavesdropping scenario, explored in [10] and [11], involves a sophisticated eavesdropper deploying multiple sensors. Although [10] and [11] focus on the AN and OPALS schemes, respectively, both attacks rely on using multiple antennas in different directions to estimate the transmitted message by solving a noisy linear system, and can be applied to the two novel strategies proposed in this paper. After retrieving the emitted vector, the eavesdropper can estimate the message of interest. Specifically, if $\mathbf{W} \in \mathbb{C}^{M,N}$ is the eavesdropper channel matrix, where M is the number of eavesdropper antennas, and $\mathbf{x}[k]$ is the processed vector, the received message is:

$$\mathbf{r}[k] = \mathbf{W}\mathbf{x}[k] + \boldsymbol{\eta}[k], \quad (10)$$

where $\boldsymbol{\eta}[k] \in \mathbb{C}^M$ represents the AWGN at the eavesdropper with power σ_n^2 . The attack estimates $\mathbf{x}[k]$ as $\hat{\mathbf{x}}[k] := (\mathbf{W}^H \mathbf{W})^{-1} \mathbf{W}^H \mathbf{r}[k]$, and the transmitted symbol is then estimated. We denote by $\hat{a}_{an}[k]$ and $\hat{a}_{opals}[k]$ the least squares (LS) estimates obtained from the attacks in [10] and [11], respectively. The following property is key to understanding the robustness of these schemes against such attacks at a fixed BL.

Property 1. Suppose an eavesdropper deploys M antennas in directions $\theta_1, \dots, \theta_M$. Then, for a fixed BL B_{loss} and a fixed noise level σ_n , there exists a constant $C'(\theta_1, \dots, \theta_M)$ such that for any method (namely AN, OPALS, Deterministic, and

Randomized), the mean Square error (MSE) for the estimation of the message $a[k]$ is given by:

$$MSE(a[k], \hat{a}[k]) = \frac{B_{loss}}{N^2} \sigma_n^2 C(\theta_1, \dots, \theta_M), \quad (11)$$

where $C(\theta_1, \dots, \theta_M)$ is a constant that only depends on the wiretapping directions.

From a BL perspective, all methods exhibit similar robustness against the multi-sensor eavesdropping attack. A comparable result was shown in [7] for a single-antenna eavesdropper, where different methods were shown to achieve equivalent performance, albeit without theoretical assessment. The following proof supports this conclusion.

Proof. See Appendix B $\square$

In the case of the randomized scheme, the pseudo-random generation in Eq. (6) introduces additional complexity for producing the pseudo-random variable X . Nevertheless, the overall order of complexity remains unchanged. An important additional metric for evaluating energy efficiency is the PAPR. Although a closed-form expression of the PAPR as a function of the BL is not available, we will assess its behavior through simulation results.

IV. SIMULATION RESULTS

Numerical evaluations are conducted for a 16-QAM modulation, $\theta_0 = 0$, a channel attenuation $h[k]$ equals to 1, and a root-raised cosine filter used for the pulse shaping filter with a roll-off factor of 0.25.

We compare the performance of AN, OPALS, and our proposed methods (deterministic and randomized) under a common BL, ensuring a fair and consistent evaluation. Unlike conventional comparisons that independently fix parameters such as $R[k]$ or σ_{an} , our analysis adopts the BL of a non-secure beamforming system as a baseline reference for comparison. Secrecy capacity is not used as a performance metric in this work, since the expression $\log_2(1 + \text{SNR}_{\text{legit.}}) - \log_2(1 + \text{SINR}_{\text{Eve}})$, where $\text{SNR}_{\text{legit.}}$ denotes the signal-to-noise ratio at the legitimate receiver and SINR_{Eve} the signal-to-interference-plus-noise ratio at the eavesdropper, is valid only for Gaussian inputs, whereas the signaling induced by a^+ and a^- in Section II-B is explicitly non-Gaussian (see [12]).

A. Energy efficiency comparison

Figure 3 depicts the BL as the normalized received power in terms of the eavesdropper direction θ , for the different methods and parameter configurations. The normalization therefore make this Figure indenpendant of N the number of emitted antennas. A baseline system without security, such as conventional beamforming, delivers a signal power scaled by N^2 for the legitimate receiver. In contrast, the secure schemes yield a lower power scaling due to the added security overhead. The BL quantifies this degradation as the ratio between the received power with and without security in the legitimate direction θ_0 . For instance, setting $R[k] = 5$ for all k results in a BL of 14 dB for OPALS, while AN achieves a BL of 3 dB with $\sigma_{an} = 0.70$. When $\epsilon = 0.40$, our proposed method balances AN and OPALS, yielding a BL of 12 dB. It is also important to note that the received power in certain directions—such as 30° —is null for the beamforming system. In contrast, for secure transmission schemes, the received power remains approximately constant outside the main lobe: around -20 dB

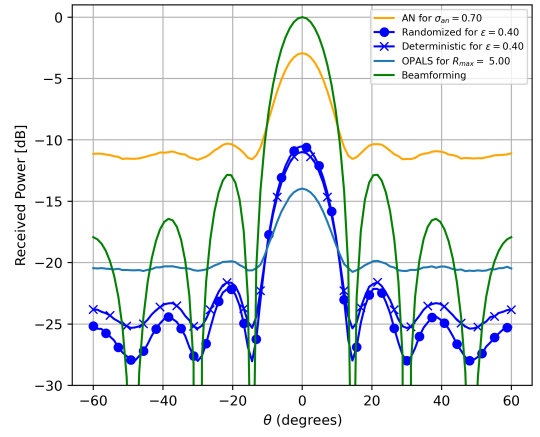


Fig. 3: Normalized received power for the different methods, using a normalized emitted power per antenna.

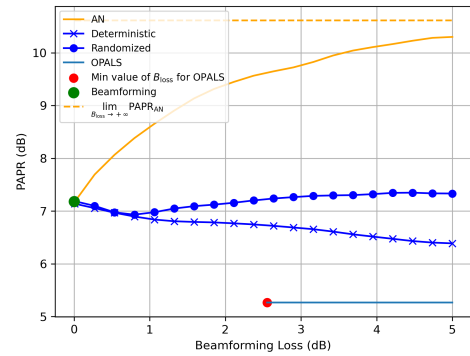


Fig. 4: PAPR vs. BL.

for OPALS, and about -25 dB for our proposed method. A lower received power outside the main lobe is desirable from a security perspective. This figure highlights the inherent trade-off between security and performance, showing the cost of incorporating security into wireless transmission systems.

Figure 4 illustrates the trade-off between PAPR (which only depends on the decomposition scheme, not the number of antennas N) and BL under a per-antenna power constraint. OPALS exhibits a sharp increase in B_{loss} , which remains above a minimum threshold due to the peak constraint $R_{\max} > \max_k |a[k]|$. For 16-QAM symbols, this imposes a BL of at least 2.6 dB. While this method ensures a low PAPR, the required power overhead limits its energy efficiency. Both AN and our proposed randomized scheme result in an infinite constellation at the eavesdropper, even in a noiseless scenario, thereby improving security by eliminating the implementation of brute force attacks. This property comes at the cost of a high PAPR for AN schemes compared to OPALS and our proposed deterministic method that shares the feature of producing finite constellations for the eavesdropper. Indeed, for $B_{loss} = 2.6$ dB, OPALS and our deterministic scheme have a PAPR smaller than 7 dB, while AN has a PAPR greater than 9.5 dB.

While both the AN and randomized methods offer an effectively infinite constellation at the eavesdropper, their PAPR behavior differs. Indeed, the randomized scheme provides the best trade-off, as its PAPR increases only slightly—from 7 dB to 7.5 dB—over the studied BL range. In contrast, the AN

scheme's PAPR rises rapidly, reaching 10 dB for a BL of 3 dB.

Although the deterministic scheme results in a PAPR almost 1 dB higher than OPALS, it does not suffer from the same strict BL constraint ($B_{\text{loss}} \geq 2.6$ dB for 16-QAM) and can thus offer a better spectral efficiency at similar power budgets. For the deterministic scheme, PAPR is a decreasing function of BL and appears to approach the PAPR of OPALS. In fact, for a normalized 16-QAM constellation, and according to Lemma 1, we have:

$$\text{PAPR}_{\text{det.}}(\epsilon) = \frac{\max |a^{\pm}[k]|}{1 + 2\epsilon \mathbb{E}[|a[k]|] + \epsilon^2} = \frac{\max (|a[k]| + \epsilon)^2}{1 + 2\epsilon \mathbb{E}[|a[k]|] + \epsilon^2},$$

which is a decreasing function of ϵ , independent of N , and tends to 1 as $\epsilon \rightarrow \infty$.

Overall, our proposed schemes—randomized and deterministic—bridge the gap between AN and OPALS, offering flexible trade-offs on energy efficiency depending on system security requirements.

B. Security comparison

In this section, we focus on the case of a multi-antenna eavesdropper, as described in Section III-B. Such an adversary can exploit its multiple observations to jointly process the received signals. In particular, if the eavesdropper has at least as many antennas as the transmitter, it can suppress the masking signal for AN (the auxiliary signal in our case, see Equations (3), (4)) by solving a linear system, which significantly reduces its effective noise level. This situation illustrates a critical limitation of secrecy capacity as a performance metric: the eavesdropper, being over-equipped with more antennas than the legitimate receiver, can achieve reception quality that surpasses that of the intended user. Consequently, secrecy capacity may even become null, which makes it unsuitable for a fair comparison of security levels across different methods and BL. For this reason, we instead adopt the MSE as the security performance metric.

Property 1 is illustrated in Table I. The beamforming system corresponds to the AN method without artificial noise injection, i.e., a BL of 0 dB. Therefore, when $\text{BL} > 0$ dB, the beamforming method does not exist. Conversely, when $\text{BL} = 0$ dB, the AN, OPALS, deterministic, and randomized methods are considered as undefined, as they reduce to a beamforming framework without security features. For fixed levels of AWGN power and BL, each method demonstrates consistent robustness against an eavesdropper deploying the attacks presented in [10] and [11], using $M = N = 8$ receivers uniformly distributed in $[-\pi/3, \pi/3] \setminus [\theta_0 - 0.2, \theta_0 + 0.2]$. Note that a higher MSE indicates greater security. As expected, increasing the BL results in enhanced security.

We now turn to analyze the robustness of each method with respect to the PAPR criterion, as shown in Figure 5.

TABLE I: MSE between the estimated and original message for $M = N = 8$, with $\sigma_n = 0.25$ and 0.5. Values obtained via Monte-Carlo simulation (1000 independent runs); the 95% confidence-interval half-width is ≤ 0.1 dB for every entry.

Method \ BL	0 dB		2 dB		4 dB	
	0.25	0.5	0.25	0.5	0.25	0.5
AN [6]	Undef.	Undef.	-19.67	-13.61	-17.61	-11.62
OPALS [7]	Undef.	Undef.	Undef.	Undef.	-17.59	-11.68
Randomized	Undef.	Undef.	-19.74	-13.59	-17.68	-11.62
Deterministic	Undef.	Undef.	-19.72	-13.58	-17.70	-11.67
Beamforming	-21.67	-15.57	-	-	-	-

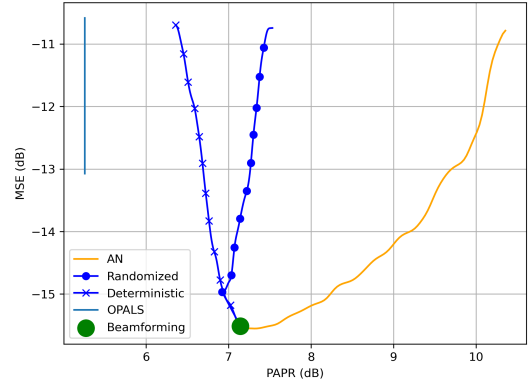


Fig. 5: Illustration of Property 1: MSE vs. PAPR for $N = 8$, $\sigma_n = 0.5$, and an eavesdropper having $M = N = 8$ receivers equally distributed outside $[\theta_0 - 0.2, \theta_0 + 0.2]$.

The vertical behaviour of the MSE curve for OPALS is due to the fact that the PAPR is constant for this method. Also, since the PAPR as a function of the BL is not bijective for the randomized method (see Figure 4), its inverse function does not exist. This explains why the same PAPR of 7.1 dB can correspond to two different values of the MSE, depending on the chosen BL. As previously shown by the results of Figure 4, the randomized method outperforms AN whatever the PAPR is. For the deterministic scheme, the MSE reaches high values at a much lower PAPR compared to both AN and the randomized scheme, while offering a finite constellation at the eavesdropper, thereby reducing robustness against brute-force attacks.

V. CONCLUSION AND PERSPECTIVES

In this work, we introduced two novel secure transmission methods that bridge the gap between AN and OPALS schemes. Depending on the use case, each proposed approach provides a better trade-off in terms of performance security and energy efficiency. A comprehensive evaluation was carried out using multiple criteria including PAPR, BL, and MSE. Importantly, our methods preserve the advantageous features of AN and OPALS while mitigating their limitations. For instance, our randomized scheme achieves a better PAPR compared to classical AN, while offering infinite constellations at the eavesdropper side, a desirable property for security analysis.

While several works in the literature have proposed PAPR reduction techniques for AN-based systems (e.g., [13]), these methods could be directly applied or adapted to our security schemes, which is left for future work. However, such techniques tend to reduce the constellation cardinality observed by the eavesdropper, which is misaligned with the intended security goals. The computational resources required to implement these solutions are also significantly larger than those of the studied framework. This is why we chose to compare our proposed methods primarily against the classical AN and OPALS schemes. As a future perspective, we plan to extend OPALS to Non-Line-of-Sight (NLoS) channels and perform a similar comparative study of all methods under more realistic propagation conditions.

APPENDIX A ARTIFICIAL NOISE DESCRIPTION

In the AN scheme [6], confidentiality is ensured by injecting artificial noise that lies in the null space of the legitimate receiver's channel, preventing any interference at the intended user. The AN vector $\boldsymbol{\mu}[k] \in \mathbb{C}^{N \times 1}$ is constructed such that:

$$\mathbf{w}_{\theta_0} \boldsymbol{\mu}[k] = 0.$$

To do so, an orthonormal basis of the null space of $\mathbf{w}_{\theta_0}$ is computed, yielding a matrix $\mathbf{V} \in \mathbb{C}^{N \times (N-1)}$ that satisfies $\mathbf{w}_{\theta_0} \mathbf{V} = \mathbf{0}$ and $\mathbf{V}^H \mathbf{V} = \mathbf{I}_{N-1}$. The AN is then defined as:

$$\boldsymbol{\mu}[k] := \mathbf{V} \mathbf{n}[k],$$

where $\mathbf{n}[k] \sim \mathcal{N}(\mathbf{0}, \sigma_{an}^2 \mathbf{I}_{N-1})$, and $\sigma_{an}^2 \in [0, 1]$ denotes the power allocated to AN.

Assuming unit average power per antenna and $\mathbb{E}[|a[k]|^2] = 1$, the transmitted signal becomes:

$$\mathbf{x}[k] := \sqrt{1 - \sigma_{an}^2} a[k] \mathbf{w}_{\theta_0}^H + \sqrt{\frac{N}{N-1}} \boldsymbol{\mu}[k], \quad (12)$$

where $(\cdot)^H$ denotes the conjugate transpose.

The received message in direction θ is therefore:

$$\begin{aligned} r_\theta[k] &= h[k] \mathbf{w}_\theta \mathbf{x}[k] + \eta[k] \\ &= \sqrt{1 - \sigma_{an}^2} a[k] h[k] \mathbf{w}_\theta \mathbf{w}_{\theta_0}^H \\ &\quad + \sqrt{\frac{N}{N-1}} \mathbf{w}_\theta \boldsymbol{\mu}[k] + \eta[k]. \end{aligned}$$

APPENDIX B PROOF OF PROPERTY 1

The following development is made using the notation $\hat{a}_{\text{opals}}[k]$. However, it is exactly the same for any of the novel strategies by using the notations of II-B. For these schemes, the transmitted vector is given by

$$\mathbf{x}_{\text{opals}}[k] = \frac{1}{\sqrt{\mathbb{E}[|a^\pm[k]|^2]}} [a^\pm[k], \dots, a^\pm[k]]^T.$$

Using an LS estimation of $\mathbf{x}_{\text{opals}}$ in the linear system (10) and then estimating $a[k]$ gives

$$\begin{aligned} \hat{a}_{\text{opals}}[k] &= \frac{\sqrt{\mathbb{E}[|a^\pm[k]|^2]}}{N} \sum_{n=1}^N \hat{\mathbf{x}}_{\text{opals}}[k] \\ &= a[k] + \frac{\sqrt{\mathbb{E}[|a^\pm[k]|^2]}}{N} \sum_{n=1}^N (\mathbf{L} \boldsymbol{\eta})_n, \end{aligned}$$

where $\mathbf{L} := (\mathbf{W}^H \mathbf{W})^{-1} \mathbf{W}^H \in \mathcal{M}_{N \times M}(\mathbb{C})$, $\boldsymbol{\eta} \in \mathbb{C}^M$ is the noise vector, and $(\cdot)_{p,q}$ denotes the coefficient in position (p, q) of a matrix. Then,

$$\begin{aligned} \text{MSE}(a[k], \hat{a}_{\text{opals}}[k]) &= \frac{\mathbb{E}[|a^\pm[k]|^2]}{N^2} \mathbb{E} \left[\left| \sum_{n=1}^N (\mathbf{L} \boldsymbol{\eta})_n \right|^2 \right] \\ &= \frac{B_{\text{loss}}}{N^2} \sigma_n^2 \sum_{1 \leq p, q \leq N} (\mathbf{L} \mathbf{L}^H)_{p,q}. \end{aligned}$$

The last equality was obtained by using the fact that the covariance matrix of the noise vector, $\boldsymbol{\Gamma}_{\mathbf{L} \boldsymbol{\eta}}$, is given by

$$\boldsymbol{\Gamma}_{\mathbf{L} \boldsymbol{\eta}} = \sigma_n^2 \mathbf{L} \mathbf{L}^H,$$

with the covariance matrix of a random vector $\mathbf{y} \in \mathbb{C}^N$, $\boldsymbol{\Gamma}_{\mathbf{y}} \in \mathcal{M}_N(\mathbb{C})$, being defined as

$$(\boldsymbol{\Gamma}_{\mathbf{y}})_{i,j} = \text{cov}(x_i, x_j) = \mathbb{E}[(x_i - \mathbb{E}[x_i])(x_j - \mathbb{E}[x_j])].$$

By following the same reasoning for AN, and using equations (10) and (12), the estimation of the emitted vector $\mathbf{x}[k]$ is

$$\begin{aligned} \hat{\mathbf{x}}_{\text{an}}[k] &= \mathbf{L} \mathbf{r}[k] \\ &= \sqrt{1 - \sigma_{an}^2} a[k] \mathbf{w}_{\theta_0}^H + \sqrt{\frac{N}{N-1}} \boldsymbol{\mu}[k] + \mathbf{L} \boldsymbol{\eta}[k]. \end{aligned}$$

Then, to recover $a[k]$, the eavesdropper must reconstruct the legitimate channel to suppress the effect of artificial noise—typically by applying the beamforming vector $\mathbf{w}_{\theta_0}$, as was done in [10]. Consequently, we obtain:

$$\begin{aligned} \hat{a}_{\text{an}}[k] &= \frac{1}{N \sqrt{1 - \sigma_{an}^2}} \mathbf{w}_{\theta_0} \hat{\mathbf{x}}_{\text{an}}[k] \\ &= a[k] + \frac{1}{N \sqrt{1 - \sigma_{an}^2}} \mathbf{w}_{\theta_0} \mathbf{L} \boldsymbol{\eta}[k]. \end{aligned}$$

Therefore,

$$\begin{aligned} \text{MSE}(a[k], \hat{a}_{\text{an}}[k]) &= \frac{1}{N^2 (1 - \sigma_{an}^2)} \mathbb{E} \left[\left| \sum_{n=1}^N (\mathbf{L} \boldsymbol{\eta})_n \right|^2 \right] \\ &= \frac{B_{\text{loss}}}{N^2} \sigma_n^2 \sum_{1 \leq p, q \leq N} (\mathbf{L} \mathbf{L}^H)_{p,q} \\ &= \text{MSE}(a[k], \hat{a}_{\text{opals}}[k]). \end{aligned}$$

REFERENCES

- [1] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2020.
- [2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [3] B. Van Veen and K. Buckley, "Beamforming: a versatile approach to spatial filtering," *IEEE ASSP Magazine*, vol. 5, no. 2, pp. 4–24, 1988.
- [4] O. Ansari and M. G. Amin, "Directional modulation techniques for secure wireless communication: a comprehensive survey," *Journal of Wireless Communications and Networking*, vol. 2022, no. 1, p. 93, 2022. [Online]. Available: <https://doi.org/10.1186/s13638-022-02175-7>
- [5] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional Modulation Via Symbol-Level Precoding: A Way to Enhance Security," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1478–1493, 2016.
- [6] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.
- [7] E. Tollefson, B. R. Jordan, and J. D. Gaedert, "Out-phased array linearized signaling (OPALS): A practical approach to physical layer encryption," in *IEEE Military Communications Conference (MILCOM)*, Tampa, FL, USA, 2015, pp. 294–299.
- [8] D. Cox, "Linear Amplification with Nonlinear Components," *IEEE Trans. on Commun.*, vol. 22, no. 12, pp. 1942–1945, Dec. 1974.
- [9] J. Chen, Y. Xiao, X. Lei, Y. Ding, H. Niu, K. Liu, Y. Zhong, S. Yang, V. Fusco, and W. Xiang, "A survey on directional modulation: opportunities, challenges, recent advances, implementations, and future trends," *IEEE Internet of Things Journal*, vol. 12, no. 16, pp. 32 581–32 615, 2025.
- [10] H. Niu, Y. Xiao, X. Lei, and M. Xiao, "Artificial Noise Elimination: From the Perspective of Eavesdroppers," *IEEE Transactions on Communications*, vol. 70, no. 7, pp. 4745–4754, 2022.
- [11] J. Burgat, J.-B. Doré, J. Farah, and M. Crussière, "Vulnerability Analysis of Dynamic Directional Modulations: a Multi-Sensor Receiver Attack," in *IEEE Military Communications Conference (MILCOM)*, 2024, pp. 1–6.
- [12] E. Telatar, "Capacity of Multi-antenna Gaussian Channels," *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 585–595, 1999. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4460100604>
- [13] Y. He, Y. Liu, N. Du, and N. Xie, "Directional modulation for QAM signals with PAPR reduction," in *2016 46th European Microwave Conference (EuMC)*, 2016, pp. 1307–1310.