PAPR-Aware Artificial Noise for Secure Massive MIMO Downlink

Idowu Ajayi, Yahia Medjahdi, Rafik Zayani, Lina Mroueh, Fatima Kaddour

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 7 June 2022, accepted 18 June 2022, date of publication 27 June 2022, date of current version 1 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3186695

PAPR-Aware Artificial Noise for Secure Massive MIMO Downlink

IDOWU AJAYI[1], (Graduate Student Member, IEEE), YAHIA MEDJAHDI[2], (Member, IEEE), RAFIK ZAYANI[3], (Member, IEEE), LINA MROUEH[1], AND FATIMA ZOHRA KADDOUR[4]

[1]Institut Supérieur d'Électronique de Paris (ISEP), 75006 Paris, France
[2]Centre for Digital Systems, IMT Nord Europe, Institut Mines-Télécom, Université de Lille, 59000 Lille, France
[3]CEA-Leti, Université Grenoble Alpes, 38000 Grenoble, France
[4]L'Agence Nationale des Fréquences, 94704 Maisons-Alfort, France

Corresponding author: Idowu Ajayi (idowu.ajayi@isep.fr)

This work was supported in part by the Institut Supérieur d'Électronique de Paris (ISEP), and in part by the Agence Nationale des Fréquences (ANFR).

ABSTRACT This paper introduces a new approach to providing secure physical-layer massive multiple-input multiple-output (MIMO) based communications that can improve the energy efficiency of the system. This is achieved by synthesizing orthogonal artificial noise (AN) that has to be constrained to lie in the null space of the legitimate users' channels while it should lie in the range space of the eavesdropper's channel. In addition, this AN reduces the peak-to-average power ratio (PAPR) of the transmit signal. Indeed, low PAPR signals are preferable and more efficient for low-cost hardware, thus improving the energy consumption of massive MIMO systems. In this paper, we propose a new PAPR-aware precoding scheme based on the use of AN to enhance the secrecy performance of massive MIMO while reducing the PAPR of the transmit signal and guaranteeing excellent transmission quality for legitimate users. The scheme is formulated as a convex optimization problem that can be resolved via steepest gradient descent (GD). Accordingly, we developed a new iterative algorithm, referred to as PAPR-Aware-Secure-mMIMO, that makes use of instantaneous information to solve the optimization problem. Simulation results show the efficiency of our proposed algorithm in terms of PAPR reduction and secrecy, which is also studied with respect to power distribution between useful signal and AN, PAPR targets and the number of BS antennas.

INDEX TERMS Artificial noise (AN), massive multiple-input multiple-output (MIMO), peak-to-average power ratio (PAPR), physical layer security (PLS), power allocation, steepest gradient descent (GD), zero-forcing (ZF) precoding.

I. INTRODUCTION

The concept of physical layer security (PLS) builds on the pivotal idea of turning wireless channel's imperfections, such as noise and fading, into a source of security. It is considered a promising technique that exploits the channel properties to send confidential messages to the legitimate receiver (Bob) even in the presence of a powerful eavesdropper (Eve). It is a field that is gaining more attention in recent times because it offers the advantages of lower computational complexity and lower resource requirement compared to legacy cryptography and it is potentially quantum secure [1]. These attributes will make PLS an interesting choice for 5G-and-Beyond services such as massive machine type communication (mMTC) and ultra-reliable and low latency communication (URLLC).

Massive multiple-input multiple-output (MIMO) systems, where the base station (BS) is equipped with a very large number of antennas, have recently received a lot of attention [2]. Some of the advantages of massive MIMO include improvement in throughput, better radiated energy efficiency, reduced latency, simplification of the media access control (MAC) layer, and robustness to intentional jamming. It is a key technology for the next generation wireless systems and supports 5G and Beyond services [3].

The use of artificial noise (AN) injection to provide security is a well-established concept. It is classified as a channel enhancing technique [4]. The concept was introduced in [5] and the main idea is that when a transmitter (Alice) has a

The associate editor coordinating the review of this manuscript and approving it for publication was Walid Al-Hussaibi.

higher spatial degree of freedom than an eavesdropper, it can exploit it by using the available power to transmit AN in the null space of the legitimate receiver but the range space of the eavesdropper. This AN will be transparent to Bob but it will degrade the channel of Eve, hence secrecy is provided. However, a major challenge that is yet to receive enough attention in the literature is the high peak-to-average power ratio (PAPR) of the transmit signals in emerging massive MIMO systems, which are caused by the use of high dimensional precoding matrix. Moreover, this high PAPR can be accentuated by in-phase superposition between the information signal and the AN sub-spaces [1]. High PAPR of transmit signal is associated with hardware impairments, especially power amplifiers (PA) non-linearity problems leading to signal distortion, phase rotation, and adjacent channel interference. The optimal transmit signals require that the power amplifiers are backed-off and operated in their linear region [6]. Operating at such a large backoff degrades the efficiency of that PA, which is the most power-consuming unit at the BS. This leads to a decrease in the global system energy efficiency [7].

The authors in [8] showed that the famous AN-based technique proposed in [5] causes high PAPR in the antenna domain for a multiple-input single-output (MISO) model due to the accidental in-phase addition (superposition) of AN subspaces and the signal subspace. This was compared with traditional orthogonal frequency division multiplexing (OFDM) signal in the time domain. To solve this problem, an angle rotation based technique was proposed to reduce the PAPR, while maintaining the secrecy capacity performance as that of the original AN-aided method. In [9], the authors proposed to either change the distribution of the added AN from Gaussian to uniform in flat fading environments or use an optimized AN. This does not only avoids PAPR increase but also helps reduce the PAPR of OFDM signal transmission in a single-input single-output (SISO) model. In [10], the authors proposed a power allocation algorithm for AN subspaces to solve the non-convex optimization problem of PAPR. It is based on fractional programming, the difference between convex functions programming and non-convex quadratic equality constraint relaxation.

In our work, we study and propose a scheme referred to as PAPR-Aware-Secure-mMIMO. It has the advantage of providing security due to AN injection while reducing the PAPR of the transmit signal. The main contributions of this article can be summarized as follows:

- We propose, as a convex optimization problem, a method to design a PAPR-aware AN signal.
- We showed that this convex optimization problem can be easily solved by an iterative algorithm that makes use of instantaneous information via the gradient descent (GD) approach. The proposed AN achieves the same secrecy rate as legacy AN aided schemes employing random AN [5] but with the additional advantage of a reduced PAPR. Using numerical simulation, we validate the performance of our proposed scheme in a downlink massive MIMO transmission exposed to passive eavesdropping.
- We analyze the PAPR performance of the transmission scheme with respect to (w.r.t.) the number of transmit antennas at the base station (BS) and target PAPRs.
- We study the impact of the ratio of the power distribution between the useful signal and the AN on the secrecy capacity, PAPR and symbol error rate (SER) in our proposed transmission scheme.

TABLE 1. Abbreviations.

AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BS	Base Station
CCDF	Complementary Cumulative Density Function
CSI	Channel State Information
GD	Gradient Descent
LSA	Least Squares Approximation
MAC	Media Access Control
MIMO	Multiple Input Multiple Output
MISO	Multiple Input Single Output
mMTC	Massive Machine Type Communication
MUI	Multi User Interference
OFDM	Orthogonal Frequency Division Multiplexing
PA	Power Amplifiers
PAPR	Peak to Average Power Ratio
PLS	Physical Layer Security
QAM	Quadrature Amplitude Modulation
SER	Symbol Error Rate
SISO	Single Input Single Output
SNR	Signal to Noise Ratio
TDD	Time Division Duplexing
URLLC	Ultra-Reliable and Low Latency Communication
ZF	Zero Forcing

The rest of this paper is organized as follows. Section II is devoted to describing the system model of the AN precoded secure massive MIMO downlink transmission. In Section III, the proposed PAPR-aware AN injected transmission scheme is presented. We then describe, in Section IV, the algorithm for the generation of the PAPR-aware AN. Simulation results are presented and discussed in Section V. Section VI concludes the paper. For the sake of clarity, we show all abbreviations in Table 1.

Notations: Vectors are denoted by lowercase boldface letters (e.g. $\boldsymbol{x}$), matrices are denoted by uppercase boldface letters (e.g. $\mathbf{X}$) and individual vector elements are denoted by normal letters (e.g. x). Absolute value, l_2-norm and l_∞-norm are denoted by $|\boldsymbol{x}|$, $\|\boldsymbol{x}\|_2$ and $\|\boldsymbol{x}\|_\infty$ respectively. The $N \times N$ identity matrix is denoted by $\mathbf{I_N}$. Tr($\mathbf{X}$) is the trace of $\mathbf{X}$ and det($\mathbf{X}$) is the determinant of $\mathbf{X}$. Transpose, Conjugate

transpose and Frobenius norm are symbolized by $\mathbf{X}^T$, $\mathbf{X}^\dagger$ and $\|\mathbf{X}\|_F^2$ respectively. $\mathbb{E}\{.\}$ stands for the expectation operator and $\{.\}^\ell$ represents the ℓ^{th} iteration step.

II. SYSTEM MODEL

We consider a single-cell massive MIMO downlink transmission between a BS (Alice) with N_t antennas and N_r legitimate single-antenna receiver terminals in the presence of passive eavesdropper (Eve) equipped with $N_{r,e}$ receive antennas as shown in Fig. 1. Eve can be perceived either as an eavesdropper with multiple antennas or several single antenna eavesdroppers that can collaborate and carry out cooperative detection. In our study, we consider the situation in which all eavesdroppers collaborate to eavesdrop on the information transmitted to only one legitimate terminal. In essence, in this paper, Bob signifies one terminal out of the available N_r terminals. Note that N_t is significantly larger than N_r and $N_{r,e}$ ($N_t \gg N_r, N_{r,e}$).

We assume a non-line-of-sight rich scattering environment and, as such, model all channels as uncorrelated flat-fading Rayleigh channels. It is assumed that the main channel, $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$, can be perfectly estimated and is available at the BS using channel reciprocity in time division duplexing (TDD) mode. Reciprocity implies that the channel responses in the uplink are identical to the channel responses in the downlink. This property holds as long as the uplink and downlink transmissions happen within the channel coherence interval. The property is commonly used in the literature related to massive MIMO with TDD mode [11]–[14]. We assume that Alice is unaware of Eve's channel state information (CSI), $\mathbf{H}_e \in \mathbb{C}^{N_{r,e} \times N_t}$. The entries of $\mathbf{H}$ and $\mathbf{H}_e$ are independent and identically distributed (i.i.d.) zero-mean complex Gaussian variables with unit variance.

We calculate the null space matrix, $\mathbf{V} \in \mathbb{C}^{N_t \times N_t}$, for $\mathbf{H}$ using the Moore–Penrose Pseudoinverse [15]:

$$\mathbf{V} = \mathbf{I}_{N_t} - \mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{H}. \tag{1}$$

Zero-forcing (ZF) precoding scheme is considered in this paper. It aims to cancel out multi-user interference (MUI) between the legitimate receivers. The computational complexity of ZF precoding is discussed in [16], [17]. The adopted ZF precoding vector, $\mathbf{F} \in \mathbb{C}^{N_t \times N_r}$, is can be written as

$$\mathbf{F} = \mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}. \tag{2}$$

For an AN-precoded system with a total available power, P, the power budget is respected by distributing the power between the information signal and AN. The power allocated to the information signal is represented as θP while the rest of the power budget, $(1-\theta)P$, is dedicated to the AN, where $0 < \theta \leq 1$.

We adopt equal power allocation across all transmit antennas. Thus, when a random AN is injected into the null space of the main channel, the transmit signal, $\boldsymbol{x} \in \mathbb{C}^{N_t \times 1}$ for a data vector, $\boldsymbol{s} \in \mathbb{C}^{N_r \times 1}$ with N_r complex values, can be

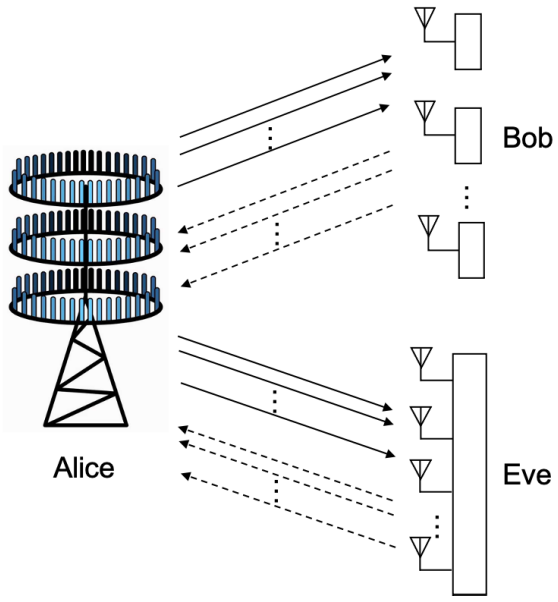

FIGURE 1. System model of the AN precoded single-carrier massive MIMO downlink transmission with N_t antennas at the BS, N_r single antenna legitimate receivers and $N_{r,e}$ antennas at the eavesdropper where $N_t \gg N_r, N_{r,e}$.

expressed as

$$\boldsymbol{x} = \sqrt{\frac{\theta}{\psi}}\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{V}\boldsymbol{k}, \tag{3}$$

where $\boldsymbol{k} \in \mathbb{C}^{N_t \times 1}$ is the randomly generated AN with a covariance matrix $\sigma_k^2\mathbf{I}_{N_t}$, while ψ and ξ stand respectively for the Frobenius norms of $\mathbf{F}$ and $\mathbf{V}$ that are included for normalization and derived as

$$\psi = \frac{N_t - N_r}{N_r}, \tag{4}$$

$$\xi = N_t - N_r. \tag{5}$$

The details of these derivations (4) and (5) are given in the Appendix.

For the m-th legitimate terminal, the received symbol is as

$$y_{b_m} = \sqrt{\frac{\theta}{\psi}}s_m + n_b, \tag{6}$$

where s_m is the m-th element in the transmit data vector $\boldsymbol{s}$ and n_b is the complex Additive White Gaussian Noise (AWGN) component at the legitimate terminal with variance σ_b^2 which is uncorrelated with s_m.

The received signal at the eavesdropper, $\boldsymbol{y}_{e_1} \in \mathbb{C}^{N_{r,e} \times 1}$, is

$$\boldsymbol{y}_{e_1} = \sqrt{\frac{\theta}{\psi}}\mathbf{H}_e\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{H}_e\mathbf{V}\boldsymbol{k} + \boldsymbol{n}_e, \tag{7}$$

where $\boldsymbol{n}_e \in \mathbb{C}^{N_{r,e} \times 1}$ is the i.i.d. AWGN sample with covariance matrix $\sigma_e^2\mathbf{I}_{N_{r,e}}$.

Secrecy capacity is the maximum transmission rate at which the eavesdropper is unable to decode any information [18]. It is equal to the positive difference between the

main channel capacity and the capacity of the wiretap channel. A positive value means secrecy is achievable and a zero implies there is no secrecy guarantee. We measure secrecy capacity in b/s/Hz (or bits/channel use).

From (6), the channel capacity when we consider only one legitimate receiver is written as

$$C_b = \log_2(1 + \frac{\theta}{\psi}\overline{\gamma}), \tag{8}$$

where $\overline{\gamma}$ is the average signal-to-noise ratio (SNR) at the legitimate receiver given as

$$\overline{\gamma} = \frac{\mathbb{E}\{|\, s\,|^2\}}{\sigma_b^2} = \frac{\sigma_s^2}{\sigma_b^2}, \tag{9}$$

and σ_s^2 is the variance of the transmit data symbol, s_m.

Inspired by [19], we show the channel capacity for Eve when a Gaussian random AN is injected in the null space of the main channel with equal power allocation,

$$\psi\sigma_s^2 + \xi\sigma_k^2 = P. \tag{10}$$

For notational convenience, we represent

$$\mathbf{A} = \mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger, \text{ and } \mathbf{B} = \mathbf{H}_e\mathbf{V}\mathbf{V}^\dagger\mathbf{H}_e^\dagger. \tag{11}$$

By letting $\sigma_s^2 = \theta P/\psi$ and $\sigma_k^2 = (1-\theta)P/\xi$, the wiretap channel capacity for a cooperative eavesdropper attempting to intercept a single symbol out of all the transmitted symbols can be written as

$$C_e = \frac{1}{N_{r,e}}\Bigg(\log_2\det\left(\mathbf{I}_{N_{r,e}} + \frac{\theta\overline{\gamma}}{\psi}\mathbf{A} + \frac{(1-\theta)\overline{\gamma}}{\xi}\mathbf{B}\right) - \log_2\det\left(\mathbf{I}_{N_{r,e}} + \frac{(1-\theta)\overline{\gamma}}{\xi}\mathbf{B}\right)\Bigg). \tag{12}$$

From (8) and (12), considering a model in which the symbol sent to a single terminal is intercepted by collaborating eavesdroppers, the secrecy capacity when a Gaussian random AN is injected is given as

$$C_{s_1} = C_b - C_e. \tag{13}$$

III. PAPR-AWARE AN

Massive MIMO offers a high-dimensional null space thanks to a large number of transmit antennas. The precoders currently used in massive MIMO exhibit transmit signals with high PAPR, regardless of whether it is a single-carrier or OFDM transmission [4]. Also, high PAPR is a known challenge in the literature for schemes considering AN injection for security. The PAPR is defined as the ratio of the highest (peak) signal power to its average power value. For a transmit signal injected with random AN as seen in (3), the PAPR is expected to be high and can be written as

$$\text{PAPR}_1 = \frac{\max_{n=1,2,\ldots,N_t}\left[\,||\, x_n\,||^2\,\right]}{\mathbb{E}[|\,|\boldsymbol{x}\,||^2]} = \frac{\|\boldsymbol{x}\|_\infty^2}{\|\boldsymbol{x}\|_2^2}, \tag{14}$$

where x_n is the signal transmitted over the n-th antenna out of the N_t transmit antennas. To jointly minimize the PAPRs associated with all antennas in (14) results in a non-convex problem that is complicated to solve and, to the best of our knowledge, there is no efficient solution for such a non-convex problem. Inspired by the work in [20], our proposed transmission scheme transforms the PAPR reduction problem into a convex optimization problem which can be solved by an algorithm using real-time data via the GD approach. The clipping signals in the algorithm are used to design a PAPR-aware AN signal, thereby achieving both PAPR reduction and security enhancement.

Our goal is to exploit the null space provided by massive MIMO in the design of the PAPR-aware AN. Similar to other AN injection schemes, this PAPR-aware noise is injected into the null space of the main channel, $\mathbf{H}$. This means that the AN will remain transparent to Bob but will degrade the wiretap channel, $\mathbf{H}_e$, since it is in its range space. Indeed, the majority of the literature with passive eavesdroppers considered that Bob's channel is independent of Eve in wireless environments, which can be satisfied when they are separated apart by at least half a wavelength [21], [22]. Note that this is only true in rich scattering environments.

In the proposed transmission scheme, we commence by computing ZF-precoded signal that gives high transmission quality in terms of MUI. We then apply an iterative algorithm to evaluate the peak-canceling signals. This reduces the PAPR of the transmit signal and enhances security. To begin the scheme, the ZF precoded signal, $\boldsymbol{\upsilon} \in \mathbb{C}^{N_t\times 1}$, is represented as

$$\boldsymbol{\upsilon} = \sqrt{\frac{1}{\psi}}\mathbf{F}\boldsymbol{s}. \tag{15}$$

To obtain the optimal PAPR, the high amplitudes of the transmit signal is iteratively clipped to an optimal threshold before transmission. The clipping threshold, λ^ℓ, for every iteration is approximately the square root of the mean power of the signal across all transmit antennas at that iteration step. The clipped signal whose difference is used to calculate the PAPR reducing AN for an ℓ-th iteration is given as

$$\upsilon_n^\ell = \begin{cases} \upsilon_n^\ell, & \text{if } |\,\upsilon_n^\ell\,| < \lambda, \\ \lambda^\ell \exp^{j\phi_n^\ell}, & \text{if } |\,\upsilon_n^\ell\,| > \lambda. \end{cases} \tag{16}$$

For every channel realization, the optimal clipping signal at each iteration step on the algorithm, $\boldsymbol{z}^\ell \in \mathbb{C}^{N_t\times 1}$, and is expressed as

$$\boldsymbol{z}^\ell = \mathbf{V}\boldsymbol{\omega}^\ell. \tag{17}$$

However the peak canceling signal hardly equals $\boldsymbol{z}$. To address this challenge, we employ the convex optimization problem (18) below. The proposed iterative algorithm is then used to search for $\ddot{\boldsymbol{\omega}}$, the optimal solution to (18).

$$\begin{aligned} &\underset{\{\ddot{\boldsymbol{\omega}}\}}{\text{minimize}}\ \boldsymbol{G}(\boldsymbol{\omega}) = \|\mathbf{V}\boldsymbol{\omega} - \boldsymbol{z}\|_2^2, \\ &\text{subject to} \begin{cases} \boldsymbol{s} = \mathbf{H}(\sqrt{\frac{\theta}{\psi}}\mathbf{F}\mathbf{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{V}\ddot{\boldsymbol{\omega}}), \\ \mathbb{E}\{|\,\ddot{\boldsymbol{\omega}}\,|^2\} = \mathbb{E}\{|\,\mathbf{V}\boldsymbol{k}\,|^2\}. \end{cases} \end{aligned} \tag{18}$$

The first constraint is intended to ensure that the added PAPR reducing AN remains transparent to the legitimate receiver while keeping zero MUI. The second constraint ensures that this added PAPR reducing AN is of equal variance and comparable with the randomly generated AN. This guarantees that the security is maintained and allows for a fair comparison of the schemes.

The optimization problem above can be solved using the steepest GD method [23], [24]. The search directions of the steepest gradient at every iteration step in the algorithm is given by the negative gradient of $\boldsymbol{G}$ at $\boldsymbol{\omega}^{\ell}$ denoted as

$$\nabla_{\omega}^{\ell+1}\boldsymbol{G}(\boldsymbol{\omega}^{\ell+1}) = \frac{2}{\mathcal{L}_{\omega}}\mathbf{V}^{\dagger}(\mathbf{V}\boldsymbol{\omega}^{\ell} - \boldsymbol{z}^{\ell+1}), \tag{19}$$

where $\mathcal{L}_e = 2\sigma_{max}^2(\mathbf{V})$ is the Lipschitz constant [25] for $\|\mathbf{V}\boldsymbol{\omega} - \boldsymbol{z}\|_2^2$. At each iteration step in the proposed algorithm, the signal to be clipped, $\boldsymbol{\upsilon}$, is given as

$$\boldsymbol{\upsilon}^{\ell+1} = \boldsymbol{\upsilon}^{\ell} + p\mathbf{V}\boldsymbol{\omega}^{\ell+1}, \tag{20}$$

where p is a regularization factor calculated using Least Squares Approximation (LSA) [26]. By using this regularization factor, the amplitude of peak canceling signals generated by LSA is almost equal to those of the original clipping noise. It can be expressed as

$$p^{\ell} = \frac{|\ \mathbf{V}\boldsymbol{\omega}^{\ell}\ |^{T}|\ \boldsymbol{z}^{\ell}\ |}{\|\mathbf{V}\boldsymbol{\omega}^{\ell}\|^2}. \tag{21}$$

As earlier described, the final PAPR-aware AN for every channel realization is the summation of the $p^{\ell}\mathbf{V}\boldsymbol{\omega}^{\ell}$ for every step of the iteration. For a total number of iterations, L, the final injected AN, $\ddot{\boldsymbol{\omega}}$, is given by

$$\ddot{\boldsymbol{\omega}} = \frac{\ddot{\boldsymbol{\omega}}^{L}}{\sigma_{\ddot{\boldsymbol{\omega}}^{L}}}, \tag{22}$$

where $\sigma_{\ddot{\boldsymbol{\omega}}^{L}}$ is the standard deviation of the total injected AN $\ddot{\boldsymbol{\omega}}^{L}$ and

$$\ddot{\boldsymbol{\omega}}^{L} = \sum_{\ell=0}^{L-1} p^{\ell}\mathbf{V}\boldsymbol{\omega}^{\ell}.$$

At the final step of the algorithm, we obtain the PAPR-aware AN precoded signal, $\ddot{\boldsymbol{x}} \in \mathbb{C}^{N_t \times 1}$, written as

$$\ddot{\boldsymbol{x}} = \sqrt{\frac{\theta}{\psi}}\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\ddot{\boldsymbol{\omega}}. \tag{23}$$

IV. PAPR-AWARE-SECURE-mMIMO ALGORITHM

In this section, we sequentially itemize the steps employed in the proposed -Secure-mMIMO algorithm. As stated, the algorithm achieves both security and PAPR reduction simultaneously. The algorithm steps are shown in Tab. **Algorithm 1**.

The received signal for Bob, a single terminal, remains identical to (6). This is because, similar to the random AN, the AN is also constrained to the null space of the main channel and is therefore transparent to Bob. The received signal at the eavesdropper is expressed as follows:

$$\boldsymbol{y}_{e_2} = \sqrt{\frac{\theta}{\psi}}\mathbf{H}_e\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\mathbf{H}_e\ddot{\boldsymbol{\omega}} + \boldsymbol{n}_e, \tag{24}$$

where $\ddot{\boldsymbol{\omega}}$ is the PAPR-aware AN designed by the algorithm. Now the PAPR of the signal when the PAPR-aware AN is injected will be significantly lower than the PAPR when random AN is injected. The PAPR expression is seen below and the results are validated through simulations in the next section,

$$\text{PAPR}_2 = \frac{\max_{n=1,2,\ldots,N_t}\left[|\ \ddot{x}\ |_n^2\right]}{\mathbb{E}[|\ |\ddot{\boldsymbol{x}}|\ |^2]} = \frac{\|\ddot{\boldsymbol{x}}\|_{\infty}^2}{\|\ddot{\boldsymbol{x}}\|_2^2}. \tag{25}$$

The main channel capacity remains the same as (8) since this AN remains transparent to Bob and has no impact on the main channel. Also, by normalization of the PAPR-aware AN, $\ddot{\boldsymbol{\omega}}$, and respecting the equal power allocation condition described in (10), the wiretap channel capacity will remain the same as when we inject a random AN. Hence, the equal power allocation condition is fulfilled for the PAPR reducing AN when

$$\psi\sigma_s^2 + \sigma_{\ddot{\omega}}^2 = P. \tag{26}$$

Intuitively, we expect the secrecy capacities to be the same since the covariances of the random AN and PAPR-aware AN are the same. In essence, the secrecy gain due to AN injection remains the same,

$$C_{s_2} = C_{s_1}. \tag{27}$$

Algorithm 1 PAPR-Aware-Secure-mMIMO

Initialization: $\boldsymbol{\omega} = 0, z = 0, \ddot{\boldsymbol{\omega}} = 0, \boldsymbol{\upsilon} = \sqrt{\frac{1}{\psi}}\mathbf{F}\boldsymbol{s}$, $\mathcal{L}_{\omega} = 2\sigma_{max}^2(\mathbf{V})$
for ℓ = 0,...,L−1 **do**
  $\lambda^{\ell} = \sqrt{\mathbb{E}[|\boldsymbol{\upsilon}^{\ell}|^2]}$
  $\boldsymbol{d}^{\ell} = \boldsymbol{\upsilon}^{\ell}$
  $d_n^{\ell+1} = \lambda^{\ell}\exp^{\theta_n^{\ell}}$ ▷ $\forall\ |\ \upsilon_n^{\ell}\ | > \lambda^{\ell}$
  $\boldsymbol{z}^{\ell+1} = \boldsymbol{d}^{\ell+1} - \boldsymbol{\upsilon}^{\ell}$
  $\boldsymbol{\omega}^{\ell+1} = \boldsymbol{\omega}^{\ell} - \frac{2}{\mathcal{L}_{\omega}}\mathbf{V}^{\dagger}(\mathbf{V}\boldsymbol{\omega}^{\ell} - \boldsymbol{z}^{\ell+1})$
  $p^{\ell} = \frac{\sum|\mathbf{V}\boldsymbol{\omega}^{\ell+1}||\boldsymbol{z}^{\ell+1}|}{\sum|\mathbf{V}\boldsymbol{\omega}^{\ell+1}|^2}$
  $\boldsymbol{\upsilon}^{\ell+1} = \boldsymbol{\upsilon}^{\ell} + p^{\ell}\mathbf{V}\boldsymbol{\omega}^{\ell+1}$
  $\ddot{\boldsymbol{\omega}}^{\ell+1} = \ddot{\boldsymbol{\omega}}^{\ell} + p^{\ell}\mathbf{V}\boldsymbol{\omega}^{\ell+1}$
  if ℓ == L-1 **then**
    $\ddot{\boldsymbol{\omega}} = \ddot{\boldsymbol{\omega}}^{\ell+1}/\sigma_{\ddot{\boldsymbol{\omega}}^{\ell+1}}$
    $\ddot{\boldsymbol{x}} = \sqrt{\frac{\theta}{\psi}}\mathbf{F}\boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}}\ddot{\boldsymbol{\omega}}$
  end if
end for
return $\ddot{\boldsymbol{x}}$

V. SIMULATION RESULTS AND DISCUSSIONS

In this section, we present the simulation results for the proposed PAPR-Aware-Secure-mMIMO scheme for security

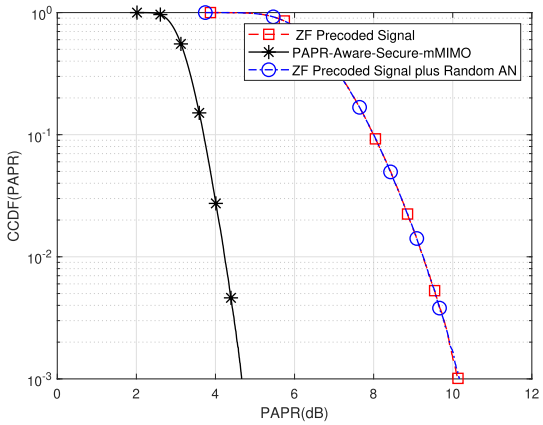

FIGURE 2. CCDFs of the PAPR of the proposed AN-aided scheme compared with signal with random AN and signal without added AN.

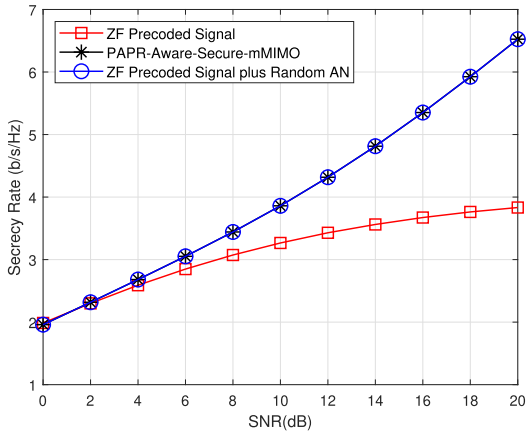

FIGURE 3. Secrecy capacity performance of the proposed AN-aided scheme compared to the capacity with Random AN injection and no AN injection when $\theta = 0.9$.

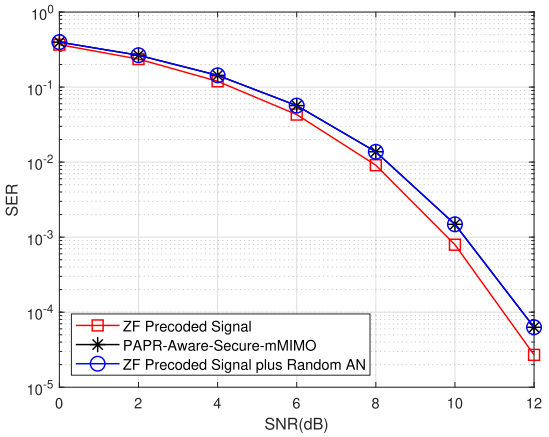

FIGURE 4. Symbol error rate performance for 16 QAM constellation size with power allocation ratio, $\theta = 0.9$.

enhancement and PAPR reduction. We use the complementary cumulative distribution function (CCDF) to evaluate the PAPR reduction performance, which denotes the probability that the PAPR of the estimated signal exceeds a given threshold. The secrecy rate is used to measure the secrecy performance of the system. For all simulations, 40 iterations ($\mathtt{L} = 40$) of the algorithm are carried out for every channel realization.

In Fig. 2, we compare the PAPR of the transmit signal using our algorithm to the PAPR of the transmit signal when a random AN is employed. The simulation was carried out considering a BS with $N_t = 70$ antennas, $N_r = 10$ legitimate terminals and $\theta = 0.9$. It can be seen that our algorithm provides a substantial PAPR reduction (shown by the solid line) compared to the PAPR for the signal with ZF precoding only and the signal with random AN injection, shown by the dash and dash-dot lines respectively in Fig. 2. At CCDF of 0.1%, we observe a gain of 5.5 dB. Another point to note is that even without AN injection, massive MIMO has a high PAPR due to the precoding schemes. We observe that with these simulation parameters, the random AN, which is also known for its high PAPR challenges, does not accentuate the PAPR in the massive MIMO scheme. This is evident from the fact that the PAPR for both the ZF precoding scheme without any AN injection and the scheme with random AN injection is 10.1 dB at a CCDF of 0.1%. This implies that the high PAPR is due to the massive MIMO precoding and is not accentuated by the AN injection.

In Fig. 3, the secrecy rate performance of the AN-aided scheme is plotted against the average SNR. We assume the same SNR for Bob and Eve. With 70 BS antennas and a power allocation ratio $\theta = 0.9$, we consider the capacity of a single legitimate terminal out of 10 legitimate users and the capacity of a cooperative Eve consisting of 10 receive antennas. For Eve, we look at the capacity in relation to a single transmitted symbol received. We can observe that when we transmit the ZF-precoded signal without any AN injection, the secrecy rate is 2 b/s/Hz at SNR = 0 dB. With the increase in SNR, this rate slightly grows to reach a limit of 4 b/s/Hz. This is in agreement with the work done in [27] where the authors showed that considering a single terminal, the secure transmission may be limited in massive MIMO with passive eavesdropping if the number of eavesdropper antennas is too large. However, with the injection of AN, the transmission scheme provides a continuous enhancement of the achievable secrecy rate as the SNR increases. In essence, the secrecy capacity C_s becomes larger since C_e is limited by the variance of the AN in a high SNR regime while C_b keeps rising. Note that the plots have been simulated with the assumption of the same SNR at Bob and Eve, a condition that is not necessarily always true in practical scenarios. It is possible that Eve has a positional advantage over Bob and therefore a better SNR. In essence, the injection of the AN technique remains a useful security technique for massive MIMO. However, this secrecy rate is the same for both cases when we inject random AN as in legacy AN works and when we inject our proposed PAPR reducing AN. This is the benefit of our proposed scheme, as we obtain the secrecy offered by legacy AN schemes but with a reduced PAPR, thereby making this less expensive and more feasible for practical deployments.

In Fig. 4, we analyze the SER performance of the proposed scheme in comparison to the cases when random AN

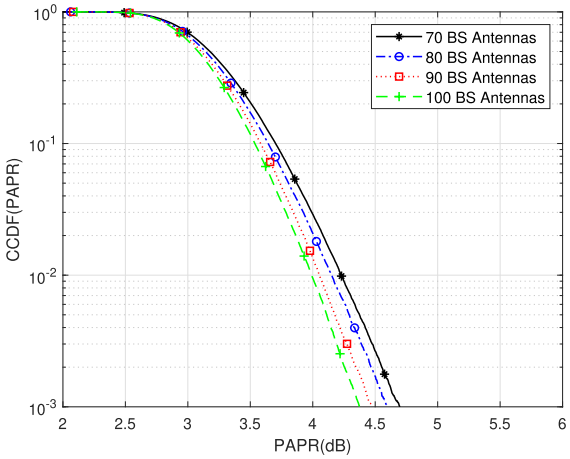

FIGURE 5. PAPR gain performance of the proposed AN-aided scheme w.r.t. the number of BS antennas.

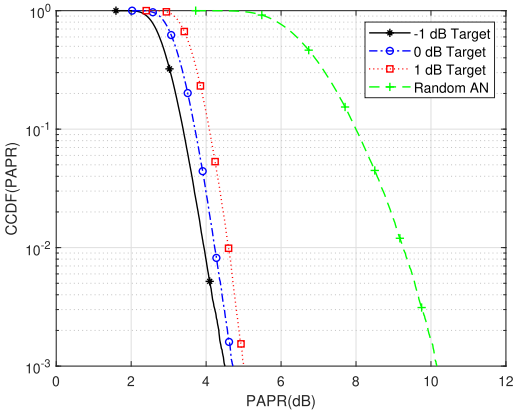

FIGURE 6. Comparison of the CCDF of the PAPR of proposed AN-aided scheme for different PAPR targets at power allocation ratio, θ, of 0.9.

is injected and when no AN is injected using the 16-QAM constellation size and the power allocation ratio of $\theta = 0.9$. It can be observed that with an SER value of 10^{-4}, there is about 0.5 dB of SNR loss for our scheme, compared to the ZF precoding without any AN injection scheme. Expectedly, the SER performance is the same in our scheme and for the scheme with random AN injection. It is obvious that the added signal related to PAPR reduction and secrecy does not affect the quality of transmission.

The impact of the number of transmit antennas N_t on the PAPR reduction gain is analyzed in Fig. 5. We consider the range of $N_t \in [70, 100]$, $N_r = 10$ and $\theta = 0.9$. We observe that for a fixed number of legitimate users, the PAPR gain shows marginal improvement (less than 0.3 dB) when the number of BS antennas goes from 70 to 100. However, it is worth using more BS antennas if the number of legitimate terminals becomes higher.

Fig. 6 shows the performance of the proposed algorithm w.r.t. various target PAPR levels. We see that for a target PAPR of -1 dB, we achieve a PAPR of 4.5 dB that is 5.5 dB higher than the target PAPR. When the target is 1 dB, the achieved PAPR is 5 dB which is 4 dB above the target. Consequently, we can conclude that the algorithm is more effective when the target PAPR is less strict.

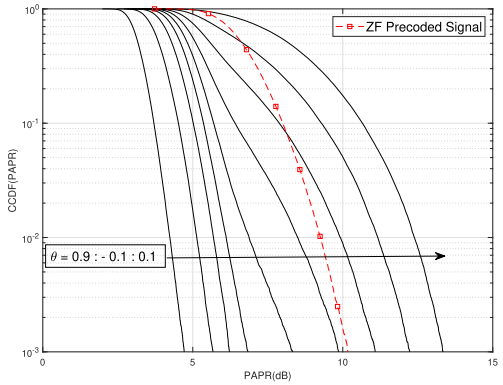

FIGURE 7. PAPR performance w.r.t. power allocation ratio: $\theta = 0.9$ corresponds to the leftmost curve and $\theta = 0.1$ corresponds to the rightmost curve.

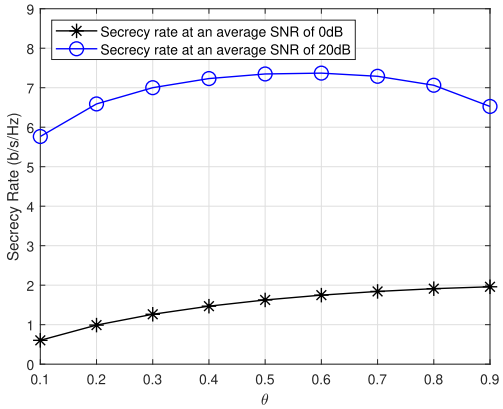

FIGURE 8. Secrecy rate performance w.r.t. power allocation ratio, θ, at high and low SNR regimes.

In Fig 7, we see the impact of θ on the PAPR performance of the proposed PAPR-Aware-Secure-mMIMO scheme. There is a trade-off between the attained PAPR and the percentage of the power allocated to AN. Note that $\theta \in]0, 1]$ where $\theta = 1$ corresponds to ZF precoding case without AN injection. When $\theta = 0$, the useful signal is null and there is no need to design a PAPR-aware AN. As more power is allocated to the AN (i.e., with θ decrease), the PAPR significantly increases. We observe that when more power is allocated to the AN, the algorithm is no longer effective, resulting in a PAPR equal to or greater than the PAPR without AN injection (ZF precoding only). In fact, we observe a very high PAPR of up to 13.3 dB when $\theta = 0.1$ and it can be deduced that the high PAPR is the combined effect of the PAPR increase due to both massive MIMO precoding and AN injection. As less power is allocated to the PAPR-aware AN, we observe a constant decrease in the attained PAPR and we obtain a 4.70 dB PAPR when $\theta = 0.9$. As earlier discussed, the secrecy capacity at this point (6.5 b/s/Hz) is also significantly higher than the secrecy capacity without any AN injection (3.8 b/s/Hz when $\theta = 1$). Hence, $\theta = 0.9$ is the optimal point providing maximum PAPR reduction and at the same time significant enhancement in secrecy capacity with a marginal SNR loss in terms of SER.

In Fig. 8, we analyze the secrecy capacity performance in relation to the ratio between the useful signal power θP and

the PAPR-aware AN one $(1-\theta)P$. Low and high SNR regimes stand respectively for SNRs of 0 and 20 dB. In the low SNR case, we can observe that with higher θ, the secrecy capacity increases to about 2 b/s/Hz. We can conclude that there is no need for AN injection in this regime since the secrecy capacity is limited by the thermal noise. Hence, allocating some of the power to AN will have a detrimental effect on the capacity of Bob. However, in the high SNR regime, the secrecy capacity becomes higher reaching its maximum value $C_s = 7.4$ b/s/Hz when θ is between 0.5 and 0.6. This approximately corresponds to equal power allocation between the useful signal and the AN.

VI. CONCLUSION

In this paper, we proposed, as a convex optimization problem, a method to design a PAPR-aware AN that significantly reduces PAPR and enhances security in a massive MIMO downlink transmission. This optimization was solved by an online iterative algorithm, referred to as PAPR-Aware-Secure-mMIMO, that makes use of instantaneous information using the GD approach. The proposed transmission scheme is easy to implement and offers a solution to the high PAPR challenge in massive MIMO. By using the high dimensional null space provided by massive MIMO, the algorithm iteratively clips a ZF-precoded signal to a threshold and uses the difference between the input signal and the clipped signal to generate AN. This AN is constrained to lie in the null space of the main channel between the BS (Alice) and Bob but the range space of the wiretap channel due to the uncorrelation between the main channel and the wiretap channel. We have shown the expressions for the PAPR and the secrecy rate for this scheme and confirmed the result using numerical simulations. Simulation results for the secrecy capacity and PAPR show that our proposed algorithm achieves the same secrecy as legacy AN injection schemes but with a significantly reduced PAPR. We also studied the PAPR gain vs. the number of BS antennas and observed that for a fixed number of terminals, increasing the number of BS antennas does not improve the PAPR gain. We studied the ability of the proposed algorithm w.r.t. PAPR targets and observed that the algorithm performs better when the target is less strict. A study of the secrecy, PAPR, and error rate performances of the scheme in relation to the power allocation ratio (θ) showed that an optimal point is achieved when $\theta = 0.9$ which implies allocating 90% of the available power to the useful signal and the remaining 10% to the artificial noise. In future work, we intend to study advanced machine learning methods to enhance the time-complexity of our iterative algorithm.

APPENDIX A
FROBENIUS NORM OF F

The proof that the normalization of the ZF precoder (2) is as given in (4)

$$\begin{aligned}\mathbf{F} &= \mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}\\ \mathbf{F}^\dagger &= (\mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{H}\end{aligned}$$

$$\begin{aligned}\|\mathbf{F}\|_F^2 &= \mathrm{Tr}(\mathbf{F}^\dagger\mathbf{F})\\ \|\mathbf{F}\|_F^2 &= \mathrm{Tr}\left[(\mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{H}\mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}\right]\\ \|\mathbf{F}\|_F^2 &= \mathrm{Tr}\left[(\mathbf{H}\mathbf{H}^\dagger)^{-1}\right]\end{aligned}$$

Using the derivations of the expectation of trace of complex inverse Wishart matrices as shown in [28], [29]

$$\|\mathbf{F}\|_F^2 = \frac{N_r}{N_t - N_r}.$$

APPENDIX B
FROBENIUS NORM OF V

The proof that the normalization of the null space matrix (1) is as given in (5)

$$\begin{aligned}\mathbf{V} &= \mathbf{I}_{N_t} - \mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{H}\\ \|\mathbf{V}\|_F^2 &= \mathrm{Tr}(\mathbf{V}\mathbf{V}^\dagger)\\ \|\mathbf{V}\|_F^2 &= \mathrm{Tr}(\mathbf{I}_{N_t} - \mathbf{H}^\dagger(\mathbf{H}\mathbf{H}^\dagger)^{-1}\mathbf{H})\\ \|\mathbf{V}\|_F^2 &= \mathrm{Tr}(\mathbf{I}_{N_t} - (\mathbf{H}\mathbf{H}^\dagger)(\mathbf{H}\mathbf{H}^\dagger)^{-1})\\ \|\mathbf{V}\|_F^2 &= \mathrm{Tr}(\mathbf{I}_{N_t}) - \mathrm{Tr}(\mathbf{I}_{N_r})\\ \|\mathbf{V}\|_F^2 &= N_t - N_r.\end{aligned}$$

REFERENCES

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Feb. 2019.

[2] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[3] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Feb. 2013.

[4] P. Angueira, I. Val, J. Montalban, O. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 810–838, 2022.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[6] S. P. Yadav and S. C. Bera, "Nonlinearity effect of power amplifiers in wireless communication systems," in *Proc. Int. Conf. Electron., Commun. Comput. Eng. (ICECCE)*, Nov. 2014, pp. 12–17.

[7] K. N. R. S. V. Prasad, E. Hossain, and V. K. Bhargava, "Energy efficiency in massive MIMO-based 5G networks: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 86–94, Jun. 2017.

[8] T. Hong and Z.-P. Li, "Peak-to-average power ratio reduction for an artificial noise aided secure communication system," in *Proc. 3rd Int. Conf. Inf. Sci. Control Eng. (ICISCE)*, Jul. 2016, pp. 1370–1374.

[9] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6190–6204, Sep. 2018.

[10] T. Hong and G.-X. Zhang, "Power allocation for reducing PAPR of artificial-noise-aided secure communication system," *Mobile Inf. Syst.*, vol. 2020, pp. 1–15, Jul. 2020.

[11] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[12] J. Tan and L. Dai, "Channel feedback in TDD massive MIMO systems with partial reciprocity," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12960–12974, Dec. 2021.

[13] Q. Qin, L. Gui, B. Gong, and S. Luo, "Sparse channel estimation for massive MIMO-OFDM systems over time-varying channels," *IEEE Access*, vol. 6, pp. 33740–33751, 2018.

[14] X. Jiang and F. Kaltenberger, "Channel reciprocity calibration in TDD hybrid beamforming massive MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 3, pp. 422–431, Jun. 2018.
[15] J. C. A. Barata and M. S. Hussein, "The Moore–Penrose pseudoinverse: A tutorial review of the theory," *Brazilian J. Phys.*, vol. 42, nos. 1–2, pp. 146–165, Apr. 2012.
[16] G. Chen, Q. Zeng, X. Xue, and Z. Li, "A low complexity precoding algorithm based on parallel conjugate gradient for massive MIMO systems," *IEEE Access*, vol. 6, pp. 54010–54017, 2018.
[17] C. Zhang, Z. Li, L. Shen, F. Yan, M. Wu, and X. Wang, "A low-complexity massive MIMO precoding algorithm based on Chebyshev iteration," *IEEE Access*, vol. 5, pp. 22545–22551, 2017.
[18] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.
[19] S.-H. Tsai and H. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.
[20] R. Zayani, H. Shaiek, and D. Roviras, "PAPR-aware massive MIMO-OFDM downlink," *IEEE Access*, vol. 7, pp. 25474–25484, 2019.
[21] F. Pan, Z. Pang, M. Luvisotto, M. Xiao, and H. Wen, "Physical-layer security for industrial wireless control systems: Basics and future directions," *IEEE Ind. Electron. Mag.*, vol. 12, no. 4, pp. 18–27, Dec. 2018.
[22] W. C. Jakes, *Microwave Mobile Communications*. New York, NY, USA: Wiley, 1974.
[23] X. Qin, Z. Yan, and G. He, "A near-optimal detection scheme based on joint steepest descent and Jacobi method for uplink massive MIMO systems," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 276–279, Feb. 2016.
[24] W. Wan, "Implementing online natural gradient learning: Problems and solutions," *IEEE Trans. Neural Netw.*, vol. 17, no. 2, pp. 317–329, Mar. 2006.
[25] G. Golub and C. van Loan, *Matrix Computations*, 3rd ed. Stockholm, Sweden: Johns Hopkins Univ, 2012.
[26] H. Li, T. Jiang, and Y. Zhou, "An improved tone reservation scheme with fast convergence for PAPR reduction in OFDM systems," *IEEE Trans. Broadcast.*, vol. 57, no. 4, pp. 902–906, Dec. 2011.
[27] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.
[28] P. Jolanta and H. Thomas, "Mixtures of traces of Wishart and inverse Wishart matrices," *Commun. Statist. Theory Methods*, vol. 50, no. 21, pp. 1–17, 2021.
[29] J. M. Robb, *Aspects of Multivariate Statistical Theory*. Hoboken, NJ, USA: Wiley, 2005, ch. 3.

IDOWU AJAYI (Graduate Student Member, IEEE) received the bachelor's degree in electronics and computer engineering from Lagos State University, in 2013, and the master's degree in wireless telecommunications and the Internet of Things from the Institut Supérieur d'Électronique de Paris (ISEP), in 2019, where he is currently pursuing the doctoral degree in telecommunications security with the LISITE Laboratory. His research interests include physical layer security (PLS), application of deep learning in PLS, massive MIMO, PAPR reduction, and channel estimation.

YAHIA MEDJAHDI (Member, IEEE) received the engineering degree from the National Polytechnic School, Algiers, the M.Sc. degree in signal processing for communications from the Galilee Institute, Sorbonne Paris Nord University, in 2008, and the Ph.D. degree from the Conservatoire National des Arts et Métiers (CNAM), in July 2012. He is currently an Associate Professor with the Centre for Digital Systems of IMT Nord Europe, Lille. Prior to that, he worked as an Associate Professor with the Institut Supérieur d'Électronique de Paris (ISEP); a Researcher with the CEDRIC Laboratory of CNAM; and an Assistant Professor with the Djilali Bounaama University of Khemis Miliana, Algeria. He served as a Postdoctoral Researcher with the ICTEAM Laboratory, Université Catholique de Louvain (UCL), Belgium. He has been involved in several ICT-European and French projects (PHYDYAS, EMPHATIC, and WONG5) dealing with waveform design for 5G and PMR systems. He has published more than 30 papers in peer-reviewed journals and international conferences, and one book chapter. His research interests include waveform design for beyond-5G, channel estimation, PAPR reduction, and non-linearity of power amplifiers.

RAFIK ZAYANI (Member, IEEE) received the Engineering, M.Sc., and Ph.D. degrees from the Ecole Nationale d'Ingénieurs de Tunis (ENIT), in 2003, 2004, and 2009, respectively, and the Habilitation à Diriger des Recherches (HDR) degree from the CNAM-Paris, in 2020. Since 2005, he has been with the Innov'COM Laboratory, Sup'Com School, Tunisia. Since 2009, he has been an Assistant Professor (tenure position) with the ISI/Université de Tunis El Manar, Tunisia. Since 2010, he has also been an Associate Researcher with the CEDRIC Laboratory, Conservatoire National des Arts et Métiers, France. Recently, he joined the Commissariat à l'Energie Atomique et aux Energies Alternatives, CEA-Leti, Grenoble, France. He is currently an Established Researcher with long experience in multicarrier communications and energy efficiency enhancement by transmitter linearization techniques (baseband DPD) and PAPR reduction, high power amplifier characterization, neural networks, identification modeling and equalization, and MIMO technologies. He was involved in developing enhanced multicarrier waveforms, such as FBMCOQAM, UFMC, GFDM, BF-OFDM, and WOLA-OFDM. He has contributed to several European (EMPHATIC) and French (WONG5) projects that aim at designing flexible air-interfaces for future wireless communications (5G and Beyond). He was awarded the H2020 Marie Sklodowska-Curie Actions (MSCA) Individual Fellowship Grant for his ADMA5 Project proposal (2018–2020).

LINA MROUEH received the Engineering degree from Télécom Paris, in 2006, the M.Sc. degree from the University of Pierre and Marie Curie, in 2006, the Ph.D. degree from Télécom Paris, in 2010, and the Habilitation degree from Sorbonne University, in 2019. From 2006 to 2009, she worked as a Research Engineer with the Seamless Radio Laboratory of Motorola Labs. In 2009, she was a visiting student with the Communication Theory Group, ETH Zürich; and then a postdoctoral student, in 2010. She is currently a Professor with the Institut Supérieur d'Électronique de Paris (ISEP) and the Head of the Research Group in Electronics and Communications. Her research interests include the MIMO communications systems, the radio resource allocation, and the dimensioning in wireless networks.

FATIMA ZOHRA KADDOUR received the master's and Ph.D. degrees from the Institut Mines-Télécom, Télécom ParisTech, in 2010 and 2014, respectively. She works as a Research Engineer with CEA-Leti, where she developed 2D channel estimation on SF-FDMA networks. She is currently the Head of the Frequency Assignation Department, Agence Nationale des Fréquences (ANFR). Her main research interests include radio resource allocation, power control, interference mitigation, and channel estimation.