Secrecy Energy Efficiency in PAPR-Aware Artificial Noise Scheme for Secure Massive MIMO

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

Secrecy Energy Efficiency in PAPR-Aware Artificial Noise Scheme for Secure Massive MIMO

Idowu Ajayi*, Yahia Medjahdi¶, Lina Mroueh*, Rafik Zayani‡ and Fatima Kaddour†

*Institut Supérieur d'Électronique de Paris (ISEP), Paris, France
¶IMT Nord Europe, Institut Mines-Télécom, Univ. Lille, Centre for Digital Systems, F-59000 Lille, France
‡CEA-Leti, Université Grenoble Alpes, 38000 Grenoble, France
†Agence Nationale des Fréquences (ANFR), Maisons-Alfort, France
Corresponding author: Idowu Ajayi (idowu.ajayi@isep.fr)

***Abstract*—In this paper, we study the secrecy energy efficiency (SEE) in an artificial noise (AN)-aided secure massive multiple-input multiple-output (MIMO) scheme. The scheme uses instantaneous information to design a peak-to-average power (PAPR)-aware AN that simultaneously improves secrecy and reduces PAPR. High PAPR leads to non-linear in-band signal distortion and out-of-band radiation causing adjacent channel interference. To ensure optimal secrecy performance, high power amplifiers (HPAs) at the base station (BS) are backed off to operate in the linear region only. The amount of back-off needed to ensure linearity of the HPA has a direct impact on the energy efficiency of the system and by extension the SEE. For our scheme, the magnitude of this back-off is determined by the power allocation ratio between the data and AN. Hence, we propose an optimal power allocation ratio for the scheme. This is to ensure a good trade-off between the energy efficiency, security, and reliability of the system. Simulation results show a better SEE performance for our scheme compared to legacy massive MIMO schemes with or without random AN injection. Finally, we study the impact of spatially correlated Rayleigh fading on the proposed scheme.**

***Index Terms*—Artificial noise (AN), massive multiple-input multiple-output (MIMO), matched filter (MF) precoding, peak-to-average power ratio (PAPR), high power amplifier (HPA), physical layer security (PLS), secrecy energy efficiency (SEE).**

I. Introduction and Motivations

Physical layer security (PLS) is a paradigm that uses wireless channel characteristics such as noise, fading, diversity, and interference as a source of security [1]. Injection of artificial noise (AN) to provide security is a well-established concept in PLS [2]. This technique has the challenge of high peak-to-average power ratio (PAPR) transmit signals. The increase in PAPR is caused by the in-phase superposition of the useful signal and the AN. To address this high PAPR challenge, the authors in [3]–[5] proposed AN signal angle rotation, change in the distribution of AN signal, and power allocation techniques respectively. In contrast to the aforementioned works that addressed PAPR reduction in multiple-input single-output and single-input single-output contexts, we focus on massive multiple-input multiple-output (MIMO) in this work.

Massive MIMO has great potential for 5G and Beyond services. It is a system in which the base station (BS) is equipped with a large number of antennas. The advantages include improvement in throughput, reduced latency, better spectral and radiated energy efficiencies, etc. [6]. It uses simple linear precoding methods such as matched filter (MF), zero-forcing (ZF), etc. However, one of its major challenges is also the high PAPR of its transmit signals due to the high dimensional precoding matrix [7].

High power amplifiers (HPAs) are the highest power-consuming unit at the BS. They are used to increase the power of the signal before transmission. A high PAPR forces the HPA to operate in the non-linear region. Consequently, there will be problems such as non-linear in-band signal distortion, out-of-band radiation leading to adjacent channel interference, etc. [8]. To mitigate against these challenges, input back-off (IBO) is introduced. The implication is that the HPA's operating point is reduced to accommodate the high signal peaks in the linear region of the HPA. The disadvantage of doing this is that the HPAs will have low energy efficiency. Most of the power supplied to the HPA will be wasted as heat. This is highly undesirable, especially in massive MIMO systems where improved energy efficiency is an important goal. Considering all the aforementioned, in [9], we proposed a novel algorithm to generate a PAPR-aware AN, referred to as PAPR-Aware-Secure-mMIMO. In a massive MIMO downlink, the scheme provides security due to AN injection while simultaneously reducing the PAPR of the transmit signal.

Further to this, in this paper, we study the energy efficiency of PAPR-Aware-Secure-mMIMO (with MF precoding adopted). Most PLS schemes demonstrate secrecy improvement in terms of secrecy capacity. However, since power availability is a very important factor in practical systems, it is worth studying secrecy gains w.r.t. the energy efficiency of the system. Some of our contributions are as follows:

- In this scheme, the power allocation ratio (θ) between the useful signal and AN has a direct impact on energy efficiency. Therefore, we propose an optimal θ based on the PAPR, secrecy capacity, and symbol error rate (SER) performance when MF precoding is adopted.
- Using numerical simulation, we show the significant energy efficiency gain for our proposed scheme compared to the legacy schemes in terms of secrecy energy efficiency (SEE) and HPA efficiency. In addition, of major significance is the impact of spatial correlation on the

This work was funded by Institut Supérieur d'Électronique de Paris (ISEP) and Agence Nationale des Fréquences (ANFR).

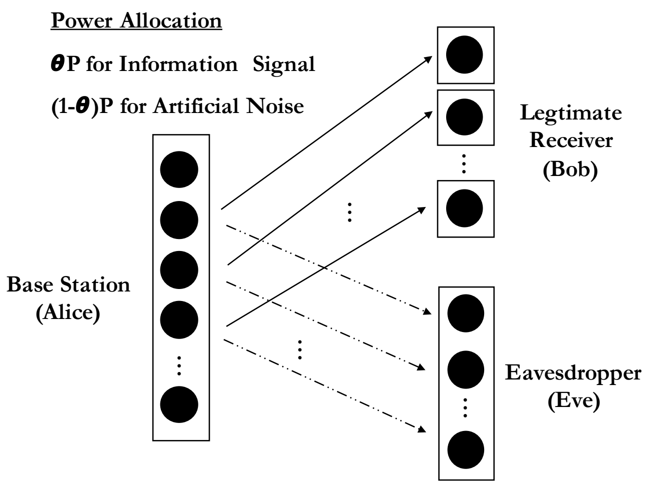


Fig. 1: System model of the AN precoded single-carrier massive MIMO downlink transmission with N_t antennas at the BS, N_r single antenna legitimate receivers and $N_{r,e}$ antennas at the eavesdropper where $N_t \gg N_r, N_{r,e}$.

performance of massive MIMO systems. In practice, channels are usually spatially correlated (space-selective fading). Hence, we study the impact of correlation on the SEE and SER performance of the scheme.

The rest of this paper is organized as follows: Sub-section II(A) is devoted to the system model of the PLS scheme and in sub-section II(B), we describe the PAPR-Aware-Secure-mMIMO algorithm. In Section III, we present the performance metrics that quantify the PAPR, HPA efficiency, secrecy capacity and SEE gains provided by the proposed scheme. Simulation results are discussed in Section IV. Finally, Section V concludes the paper.

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 $\mathbf{I_N}$. det$(\mathbf{X})$ is the determinant of $\mathbf{X}$ and conjugate transpose is symbolized by $\mathbf{X}^\dagger$. $\mathbb{E}\{.\}$ stands for the expectation operator.

II. System Model

A. System Model

As seen in Fig. 1, we consider a massive MIMO downlink transmission in which the BS (Alice) is equipped with N_t antennas. The legitimate receivers are N_r single antenna receivers and the eavesdropper consists of $N_{r,e}$ single antennas that can carry out cooperative detection. Note that N_t is significantly larger than N_r and $N_{r,e}$ ($N_t \gg N_r, N_{r,e}$). For the security performance of the scheme, Alice is represented by all N_t antennas, Bob is one out of the N_r single antenna receivers, and Eve is represented by all $N_{r,e}$ antennas.

In our scheme, we assume that the channel reciprocity property in the time division duplexing (TDD) mode holds. The concept is that the uplink and downlink channel responses are the same during the coherence time of the channel [10]. The main channel, $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$, is modeled as a Rayleigh flat fading channel and the perfect estimate is available at Alice and Bob thanks to channel reciprocity. It is assumed that the wiretap channel, $\mathbf{H}_e \in \mathbb{C}^{N_{r,e} \times N_t}$, is unknown to Alice. 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. Using Moore-Penrose pseudoinverse [11], the null space of the main channel, $\mathbf{V} \in \mathbb{C}^{N_t \times N_t}$, is written as:

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

B. PAPR-Aware-Secure-mMIMO

In PAPR-Aware-Secure-mMIMO, instantaneous information is used to generate a PAPR-Aware AN, $\boldsymbol{\omega} \in \mathbb{C}^{N_t \times 1}$, that simultaneously provides security while significantly reducing the PAPR of the transmit signal. Ideally, when $\boldsymbol{\omega}$ is projected into the null-space, $\mathbf{V}$, it should be equal to the peak-canceling signal, $\boldsymbol{z} \in \mathbb{C}^{N_t \times 1}$. However, the peak-canceling signal hardly equals $\boldsymbol{z}$, and the convex optimization statement below is used to solve this challenge. The proposed iterative algorithm is then used to search for $\ddot{\boldsymbol{\omega}} \in \mathbb{C}^{N_t \times 1}$, the optimal solution to (2). It is solved using the steepest gradient descent (SGD).

$$\begin{aligned} &\underset{\{\ddot{\boldsymbol{\omega}}\}}{\text{minimize}} \; \boldsymbol{G}(\boldsymbol{\omega}) = \|\mathbf{V}\boldsymbol{\omega} - \boldsymbol{z}\|_2^2, \\ &\text{subject to } \begin{cases} \boldsymbol{s} = \mathbf{H}\ddot{\boldsymbol{x}}, \\ \mathbb{E}\{|\ \ddot{\boldsymbol{\omega}}\ |^2\} = \mathbb{E}\{|\ \mathbf{V}\boldsymbol{k}\ |^2\}. \end{cases} \end{aligned} \tag{2}$$

The first constraint ensures that the added PAPR-Aware AN remains transparent to the legitimate receiver while mitigating the multi-user interference (MUI). The transmit signal when the PAPR-Aware AN is added is $\ddot{\boldsymbol{x}} \in \mathbb{C}^{N_t \times 1}$, and $\boldsymbol{s} \in \mathbb{C}^{N_r \times 1}$ is the data vector. The second constraint ensures that this added PAPR-Aware AN is of equal variance and comparable with the randomly generated AN, $\boldsymbol{k} \in \mathbb{C}^{N_t \times 1}$. This guarantees that security is maintained and allows for a fair comparison with legacy schemes. A summary of the major algorithm steps is given below:

- Precode the transmit symbols using MF precoding.
- Based on a pre-determined PAPR target, evaluate the optimal clipping threshold for the transmit signal.
- Iteratively clip the transmit signal to this clipping threshold for all iteration steps.
- Subtract the transmit signal from the clipped signal to get the peak-canceling signal, $\boldsymbol{z}$.
- At every iteration step, the goal is to transform this excess signal (peak-canceling signal) into AN that is projected into the null space of the main channel.
- Search using SGD for the steepest gradient at every iteration step for the optimal $\boldsymbol{\omega}$ for which $\mathbf{V}\boldsymbol{\omega} = \boldsymbol{z}$.
- At the final iteration, sum up all the PAPR-Aware ANs generated during all the iterations of the algorithm.
- The transmitter then allocates the available power (P) between the useful signal and the PAPR-Aware AN. θP is allocated to the useful signal and $(1-\theta)P$ to the AN, where $0 < \theta \leq 1$.

A detailed description of the proposed scheme and obtained results can be seen in [9]. The PAPR-aware AN that is added at the final step of the algorithm, $\ddot{\boldsymbol{\omega}}$, is the summation of all ANs generated at every step of the algorithm, $\boldsymbol{\omega}^{\ell} \in \mathbb{C}^{N_t \times 1}$.

$$\ddot{\boldsymbol{\omega}} = \sum_{\ell=0}^{L-1} p^{\ell} \mathbf{V} \boldsymbol{\omega}^{\ell}, \tag{3}$$

where p is a regularization factor which is computed using least squares approximation (LSA). The resulting transmit signal is written as:

$$\ddot{\boldsymbol{x}} = \sqrt{\frac{\theta}{\psi}} \mathbf{F} \boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}} \ddot{\boldsymbol{\omega}}. \tag{4}$$

$\mathbf{F} \in \mathbb{C}^{N_t \times N_r}$, is the precoding matrix and is given by:

$$\mathbf{F} = \left[\frac{\mathbf{h}_1^{\dagger}}{\|\mathbf{h}_1\|}, \ldots, \frac{\mathbf{h}_{N_r}^{\dagger}}{\|\mathbf{h}_{N_r}\|} \right]. \tag{5}$$

The Frobenius norms of $\mathbf{F}$ ($\psi = N_r$) and $\mathbf{V}$ ($\xi = N_t - N_r$) are included for the normalization of the data and AN precoding. For the m-th legitimate receiver out of all the N_r single antenna receivers, the received symbol is given as:

$$y_{b_m} = \sqrt{\frac{\theta}{\psi}} \mathbf{h}_m \mathbf{f}_m s_m + \sum_{\substack{n=1 \\ n \neq m}}^{N_r} \sqrt{\frac{\theta}{\psi}} \mathbf{h}_m \mathbf{f}_n s_n + z_m, \tag{6}$$

where s_m is the m-th element in the transmit data vector $\boldsymbol{s}$, s_n is the n-th element in the data vector transmitted to other receivers in the same cell, and z_m is the complex additive white gaussian noise (AWGN) component at the legitimate terminal with variance ${\sigma_m}^2$ which is uncorrelated with s_m. The first term in (6) is the desired signal whose signal-to-noise ratio (SNR) is maximized due to the MF precoding, and the second term shows the intra-cell MUI.

The signal received at the eavesdropper is

$$\boldsymbol{y}_e = \sqrt{\frac{\theta}{\psi}} \mathbf{H}_e \mathbf{F} \boldsymbol{s} + \sqrt{\frac{1-\theta}{\xi}} \mathbf{H}_e \mathbf{V} \ddot{\boldsymbol{\omega}} + \boldsymbol{z}_e, \tag{7}$$

where $\boldsymbol{z}_e$ is i.i.d AWGN with covariance matrix $\sigma_e^2 \mathbf{I}_{N_{r,e}}$.

III. Performance Metrics

In this section, we present the performance metrics used to study the PAPR-Aware-Secure-mMIMO algorithm with MF precoding. With these metrics, we can propose an optimal power allocation ratio for the scheme and highlight the energy efficiency gains.

A. Peak-to-Average Power Ratio (PAPR)

The PAPR is defined as the ratio of the highest (peak) signal power to its average power value. For the transmit signal (4), it can be written as:

$$\text{PAPR} = \frac{\max_{a=1,2,\ldots,N_t} \left[| \ddot{x}_a |^2 \right]}{\mathbb{E}[| \ddot{\boldsymbol{x}} |^2]} = \frac{\|\ddot{\boldsymbol{x}}\|_{\infty}^2}{\|\ddot{\boldsymbol{x}}\|_2^2}, \tag{8}$$

B. High Power Amplifier Efficiency

For the a-th transmit antenna, the HPA efficiency denoted η_a, is modeled according to [12] as,

$$\eta_a = \left(\frac{P_a^{out}}{P_{a,max}^{out}} \right)^{\beta} \eta_{max}, \tag{9}$$

where P_a^{out} is the operating point of the antenna HPA and $P_{a,max}^{out}$ is the maximum HPA output power. This ratio represents, on a linear scale, the output back-off (OBO) of the HPA. The maximal HPA efficiency is η_{max} and $\beta \in [0, 1]$ is the efficiency exponent depending on the type of HPA. The value of β is 0.5 and 1 for non-ideal class B and A HPAs, respectively. In this paper, we consider class B HPAs because they are more efficient and do not have the heating problems associated with class A HPAs. Class B HPAs use two complementary transistors for each half of the waveform so that each transistor device amplifies only half of the output waveform. Hence, they have significantly better efficiency than class A HPAs. Due to their zero bias, the OBO is equal to the IBO [13]. Hence, the HPA efficiency can be rewritten in terms of IBO as:

$$\eta_a = \left(\frac{P_a^{in}}{P_{a,max}^{in}} \right)^{\beta} \eta_{max}, \tag{10}$$

where P_a^{in} is the input operating point of the antenna HPA and $P_{a,max}^{in}$ is the maximum HPA input power. For the proposed scheme and the legacy schemes to achieve complete linearity, we introduce an IBO that is equal to the magnitude of the PAPR. This guarantees that the peak signal points still fall within the linear region of the HPA. On a linear scale, the IBO will be the inverse of the PAPR. The HPA efficiency is then,

$$\eta_a = \left(\frac{1}{\text{PAPR}} \right)^{\beta} \eta_{max}. \tag{11}$$

C. Secrecy Capacity

Secrecy capacity is the maximum rate of confidential information that can be transmitted between legitimate devices without benefiting the eavesdropper [14]. It is evaluated as the positive difference between the main channel capacity and the wiretap channel capacity. For a single antenna terminal, the main channel capacity can be expressed as:

$$C_{b_m} = \log_2 \left(1 + \frac{\dfrac{\theta \overline{\gamma} \|\mathbf{h}_m\|^2}{\psi}}{\dfrac{\theta \overline{\gamma}}{\psi} \displaystyle\sum_{\substack{n=1 \\ n \neq m}}^{N_r} \dfrac{| \mathbf{h}_m \mathbf{h}_n^{\dagger} |^2}{\|\mathbf{h}_n\|^2} + 1} \right), \tag{12}$$

where $\overline{\gamma}$ is the average SNR at the legitimate receiver and is given as

$$\overline{\gamma} = \frac{\mathbb{E}\{| s |^2\}}{\sigma_m^2} = \frac{\sigma_s^2}{\sigma_m^2}, \tag{13}$$

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

Inspired by [15], the channel capacity for the eavesdropper is given as:

$$C_e = \frac{1}{N_{r,e}}\Bigg(\log_2 \det\left(\mathbf{I}_{N_{r,e}} + \frac{\theta\overline{\gamma}}{\psi}\mathbf{A} + \frac{(1-\theta)\overline{\gamma}}{\xi}\mathbf{B}\right) - \log_2 \det\left(\mathbf{I}_{N_{r,e}} + \frac{(1-\theta)\overline{\gamma}}{\xi}\mathbf{B}\right)\Bigg), \tag{14}$$

where $\mathbf{A} = \mathbf{H}_e\mathbf{F}\mathbf{F}^{\dagger}\mathbf{H}_e^{\dagger}$, and $\mathbf{B} = \mathbf{H}_e\mathbf{V}\mathbf{V}^{\dagger}\mathbf{H}_e^{\dagger}$ are adopted for notational convenience.

From (12) and (14), the secrecy capacity is evaluated by:

$$C_s = [C_{b_m} - C_e]^{+}. \tag{15}$$

D. Secrecy Energy Efficiency (SEE)

Energy efficiency refers to the total number of bits successfully transmitted by consuming a Joule of energy [16]. Similarly, SEE is the total number of confidential information bits transmitted by consuming a Joule of energy. The total power consumption at the BS is the combined HPA power across all antennas and the circuit power consumption which is also proportional to the number of active antennas, N_t [16]. It can be written as:

$$P_{\text{total}} = \sum_{a\in N_t} \frac{P_a^{out}}{\eta_a} + N_t P_{cir}, \tag{16}$$

where P_{cir} denotes the circuit power consumption. From (15) and (16), the SEE is evaluated as:

$$\text{SEE} = \frac{C_s}{P_{\text{total}}}. \tag{17}$$

IV. Numerical results

In this section, we present the simulation results for the proposed PAPR-Aware-Secure-mMIMO scheme. In all simulations, 40 iterations of the algorithm are carried out for every channel realization. We consider N_t = 70 antennas at the BS (Alice), N_r = 10 single antenna legitimate receivers while Bob is 1 out of the 10, and $N_{r,e}$ = 10 cooperative eavesdropper antennas.

A. Optimal Power Allocation

In Fig. 2, we study the effect of the power allocation on the PAPR performance of the PAPR-Aware-Secure-mMIMO algorithm when MF precoding is used. Note that $\theta \in]0, 1]$ where θ = 1 corresponds to MF precoding case without AN injection. When θ = 0, the useful signal is null and there is no need to design a PAPR-aware AN. The result shows that the PAPR is lowest when 90% of the power is allocated to the data and the remaining 10% is given to the AN. As more power is allocated to the AN (θ decrease), the PAPR increases. The algorithm becomes ineffective when more power is allocated to the AN than the useful signal ($\theta < 0.5$). At this point, the PAPR performance is not better than the schemes with or without random AN. The PAPR is as high as 13.3 dB when $\theta = 0.1$. This can be explained by the fact that the performance at that point is a combined effect of the PAPR challenges due to the large size of the massive MIMO precoding matrix and the in-phase superposition effect of the AN injection scheme.

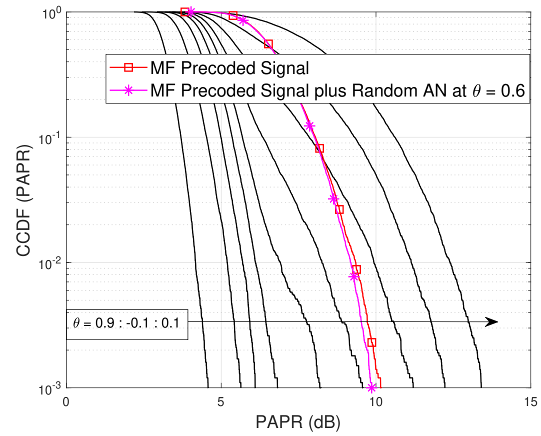


Fig. 2: PAPR performance w.r.t. power allocation ratio: θ=0.9 corresponds to the leftmost curve and θ = 0.1 corresponds to the rightmost curve.

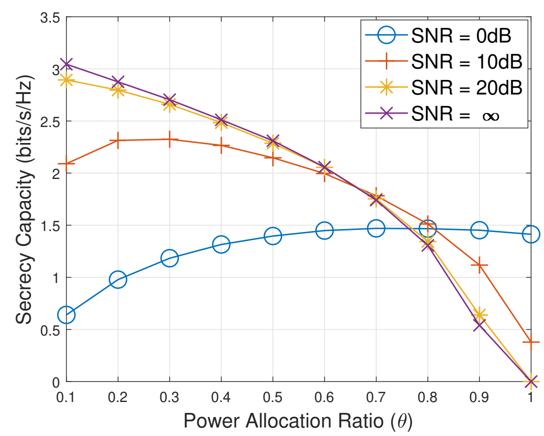
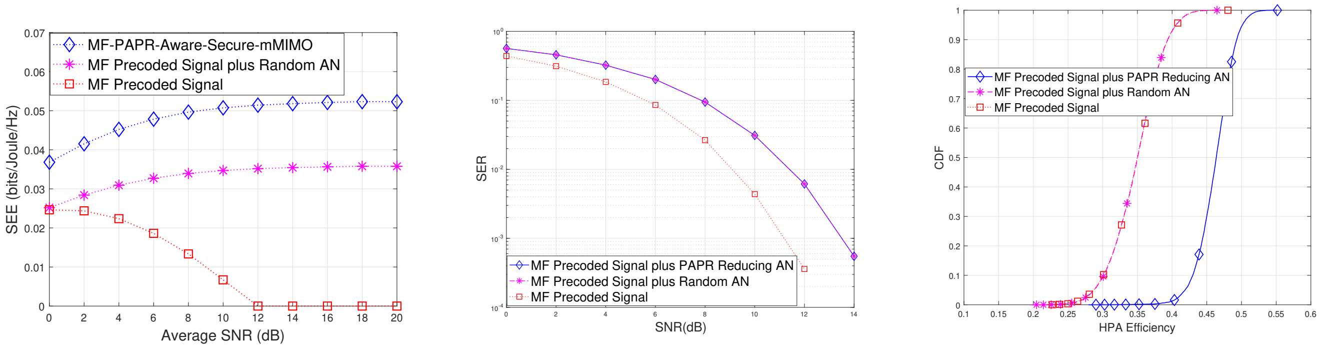


Fig. 3: Secrecy capacity performance of the proposed PAPR-Aware AN-aided scheme compared to the power allocation ratio (θ) at different SNR regimes.

To know the optimal PAPR when MF precoding is adopted, we will go further to study the effect of θ on the secrecy capacity of the system. Different SNR regimes are considered: low SNR ($\overline{\gamma}$ = 0 dB), medium SNR ($\overline{\gamma}$ = 10 dB), high SNR ($\overline{\gamma}$ = 20 dB), and very high SNR ($\overline{\gamma} = \infty$) regimes. In the low SNR regime, the secrecy capacity increases as more power is allocated to the useful signal. This is evident from the fact that the secrecy capacity is significantly affected by the thermal noise in this region. We can conclude that there is no need for AN injection in this region. For the three higher SNR regions, we observe negative slopes for all three. As more power is allocated to the useful signal, the secrecy capacity decreases. This indicates that AN injection is necessary for the higher SNR regimes because without AN, the capacity of the single antenna Bob will be more affected by the MUI than the capacity of the cooperative eavesdropper. However, an increase in the AN power leads to an increase in PAPR as already shown in Fig. 2. Therefore, we can observe that a choice of θ = 0.6 is an optimal allocation ratio for the PAPR-Aware-Secure-mMIMO scheme with MF precoding. At a CCDF of 0.1%, we obtain a PAPR of 6.5 dB and a secrecy



(a) SEE performance of the proposed scheme vs legacy schemes at θ = 0.6.

(b) SER performance for 16 QAM constellation size at θ = 0.6.

(c) CDFs of the HPA Efficiency of the proposed scheme.

Fig. 4: Performance evaluation of the energy efficiency gain of PAPR-Aware-Secure-mMIMO in terms of SEE, SER, and CDF of HPA.

capacity greater than 2 bps/Hz in higher SNR regimes ($\overline{\gamma}$ = 10, 20, and ∞).

B. Energy Efficiency Gain

Our proposed scheme with a PAPR of 6.5 dB will have HPAs with better efficiency than legacy schemes with a PAPR of 10.1 dB. Thus, for our proposed scheme and the legacy schemes to achieve complete linearity, we introduce IBOs of -6.5 dB and -10.1dB respectively[1]. This is based on the PAPR values at a CCDF of 0.1% as shown in Fig. 2. The choice of a level of 0.1% implies that after introducing the IBO, 99.9% of the signal will lie in the linear region of the HPA. It has been shown in [16] that 200 mW/antenna is an optimal transmit power in massive MIMO downlink using MF precoding. It is evident from (10) and (16) that as the IBO increases, the HPA efficiency decreases leading to higher total power consumption. Consuming higher power for the same secrecy capacity leads to lower SEE. Hence, we observe in Fig. 4a, that our proposed scheme shows the highest SEE performance and increases to the highest steady value as the average SNR increases. Next, the scheme with random AN injection outperforms the scheme without any AN injection. For the latter, the SEE goes to zero from 12 dB. This indicates that the secrecy capacity in the higher SNR regimes for this scheme is zero because the MUI limits the single antenna Bob more than the cooperative eavesdropper. Massive MIMO schemes combat this by increasing the number of transmit antennas but the scope of this work is limited to a massive MIMO system with 70 BS antennas only.

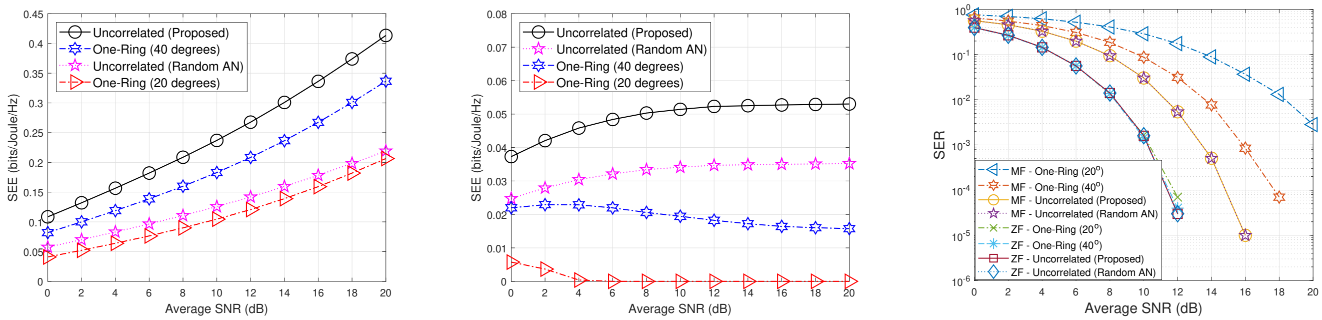
In Fig. 4b, we show the SER performance of the proposed algorithm compared to the cases when random AN is injected and when no AN is injected. 16-QAM constellation size is considered and θ = 0.6. At the SER value of 10^{-3}, there is about 2 dB of SNR loss for our scheme, compared to the MF precoding without any AN injection scheme. The SER performance is the same for our scheme and the scheme with random AN injection. This is expected since the variance of the ANs is the same for both. We can conclude that the 2 dB loss in SNR is acceptable in transmission quality for the gains in energy efficiency and secrecy.

In Fig. 4c, we compare the cumulative distribution function (CDF) of the HPA efficiencies for PAPR-Aware-Secure-mMIMO with the legacy schemes. In this simulation we adopted class B HPAs with efficiency exponent, β = 0.5 and maximal HPA efficiency, η_{max} = 0.78. The HPA efficiency is inversely proportional to PAPR which means that they are related by a decreasing function. Our proposed scheme with a PAPR of 6.5 dB will have HPAs with better efficiency than legacy schemes with a PAPR of 10.1 dB. The range of HPA efficiencies goes from 0.3 when the PAPR is 6.5 dB at a CCDF of 0.1% to values as high as 0.57 when the CCDF is 1. In contrast, the HPA efficiency is much lower for the scheme with random AN and the scheme without any AN injection. The efficiency is 0.2 when the PAPR is 10.1 dB at CCDF of 0.1% and has peak values of 0.45 at CCDF of 1. Evidently, by adopting our proposed scheme, we can improve the energy consumption efficiency of our HPA.

C. Impact of Spatial Correlation

Finally, we study the impact of spatial correlated Rayleigh fading on the performance of PAPR-Aware-Secure-mMIMO. For this, the main channel, $\mathbf{H}$, is modeled as a correlated Rayleigh flat fading channel. We suppose that the BS is elevated such that there is no scattering in its near field but there is a localized scattering around the receivers. In essence, all multipath components are due to this scattering and $\bar{\varphi}$ represents the angle of an arbitrary multipath component. Note that $\bar{\varphi} = \varphi + \delta$, where φ is the deterministic nominal angle and δ is the random deviation from the nominal angle with angular standard deviation (ASD) represented as σ_φ. The level of correlation increases as σ_φ decreases. We assume that the deviations are uniformly distributed $\delta \sim \mathcal{U}[-\sqrt{3}\sigma_\varphi, \sqrt{3}\sigma_\varphi]$. This is referred to in the literature as one-ring local scattering model [17]. All scatterers are assumed to lie on a circle centered at the receiver terminal. A nominal angle, $\varphi = 30°$, and angular standard deviation $\sigma_\varphi = [20°, 40°]$ are considered in this study. Correlation is only considered for PAPR-Aware-Secure-mMIMO and not for the legacy random AN scheme.

[1]It is important to note that equations (12), (14) and (15) are only valid when the transmit signal is linearly amplified by the HPA



(a) SEE performance for ZF Precoding (b) SEE performance for MF Precoding (c) SER performance

Fig. 5: Impact of spatial correlation on PAPR-Aware-Secure-mMIMO.

We consider both ZF and MF precoding schemes. Note that the optimal θ for ZF precoding was proposed in [9], as 0.9.

An increase in spatial correlation has a negative impact on the secrecy capacity and PAPR (the two determining components of the SEE). It leads to a decrease in secrecy capacity and an increase in PAPR. In other words, HPA efficiency will decrease and this will result in a SEE decrease. From both Fig. 5a and 5b, the SEE performance is lowest when $\sigma_\varphi = 20°$. However, ZF precoding is less sensitive to spatial correlation than MF precoding. In Fig. 5c, for MF precoding, at SER value of 10^{-3}, there is about 2 dB of SNR loss for our scheme without correlation compared to when there is a correlation of $\sigma_\varphi = 40°$. This SER loss increases as the correlation increases. The SER for ZF precoding is not impacted by the correlation, this is explained by the MUI cancellation obtained with ZF precoding.

V. Conclusion

In this paper, we studied the SEE performance in a scheme that uses instantaneous information to design a PAPR-aware AN for a secure massive MIMO downlink. Our proposed scheme achieved a PAPR of 6.5 dB at a CCDF of 0.1% compared to the 10.1 dB achieved by legacy schemes. This meant that the back-off needed to achieve HPA linearity in our proposed scheme was less than that needed in legacy schemes. We showed that the HPAs in our proposed scheme had a better efficiency range (0.3 - 0.57) than the HPAs in the legacy schemes (0.2 - 0.45). In essence, our scheme consumed the least amount of power and as a result, had the best performance in terms of SEE. The power allocation ratio (θ) between the useful signal and the AN has a direct link to the energy efficiency in our scheme. We also studied the optimal θ considering the PAPR, secrecy capacity, and SER performances of the scheme. We concluded that $\theta = 0.6$ (i.e. 60% of the power budget is dedicated to the useful signal and 40% to the AN) is an optimal choice for the PAPR-Aware-Secure-mMIMO algorithm when MF precoding is used. Finally, the scheme is very sensitive to spatial correlation. Suggested future work is a modification of the transmission scheme to deal with the spatial correlation.

References

[1] P. Angueira et al, “A survey of physical layer techniques for secure wireless communications in industry,” *IEEE Communications Surveys Tutorials*, vol. 24, no. 2, pp. 810–838, 2022.

[2] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[3] T. Hong and Z.-P. Li, “Peak-to-average power ratio reduction for an artificial noise aided secure communication system,” in *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, 2016, pp. 1370–1374.

[4] 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. on Wireless Comm.*, vol. 17, no. 9, pp. 6190–6204, 2018.

[5] T. Hong and G. Zhang, “Power allocation for reducing PAPR of artificial-noise-aided secure communication system,” in *Hindawi Mobile Information Systems*, 2020, pp. 1–15.

[6] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, “Energy and spectral efficiency of very large multiuser MIMO systems,” *IEEE Transactions on Communications*, vol. 61, no. 4, pp. 1436–1449, 2013.

[7] C. Mollén, E. G. Larsson, and T. Eriksson, “Waveforms for the massive MIMO downlink: Amplifier efficiency, distortion, and performance,” *IEEE Transactions on Communications*, vol. 64, no. 12, 2016.

[8] S. P. Yadav and S. C. Bera, “Nonlinearity effect of power amplifiers in wireless communication systems,” in *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, 2014, pp. 12–17.

[9] I. Ajayi, Y. Medjahdi, R. Zayani, L. Mroueh, and F. Z. Kaddour, “PAPR-aware artificial noise for secure massive MIMO downlink,” *IEEE Access*, vol. 10, pp. 68 482–68 490, 2022.

[10] J. Tan and L. Dai, “Channel feedback in TDD massive MIMO systems with partial reciprocity,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12 960–12 974, 2021.

[11] J. C. A. Barata and M. S. Hussein, “The moore–penrose pseudoinverse: A tutorial review of the theory,” in *Brazilian Journal of Physics*, vol. 42, no. 1-2, 2012, pp. 146–165.

[12] T. Jiang, C. Li, and C. Ni, “Effect of PAPR reduction on spectrum and energy efficiencies in OFDM systems with class-A HPA over AWGN channel,” *IEEE Transactions on Broadcasting*, vol. 59, no. 3, pp. 513–519, 2013.

[13] P. Colantonio, F. Giannini, R. Giofre, and L. Piazzon, “The doherty power amplifier”, in advanced microwave circuits and systems,” *Advanced Microwave Circuits and Systems. London*, 2010.

[14] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 356–360.

[15] S.-H. Tsai and H. V. Poor, “Power allocation for artificial-noise secure MIMO precoding systems,” *IEEE Transactions on Signal Processing*, vol. 62, no. 13, pp. 3479–3493, 2014.

[16] M. A. Rao, A. Jehangir, S. Mustafa, M. N. Sohail, and U. R. Ateeq, “Energy efficiency augmentation in massive MIMO systems through linear precoding schemes and power consumption modeling,” *Wireless Communications and Mobile Computing*, pp. 1–13, 2020.

[17] E. Björnson, J. Hoydis, and L. Sanguinetti, “Massive MIMO networks: Spectral, energy, and hardware efficiency,” *Foundations and Trends in Signal Processing*, vol. 11, no. 3-4, pp. 154–655, 2017.