Secure Communication for Spatially Correlated Massive MIMO with Low-Resolution DACs

Dan Yang, *Student Member, IEEE,* Jindan Xu, *Member, IEEE,* Wei Xu, *Senior Member, IEEE,* Ning Wang, *Member, IEEE,* Bin Sheng, *Member, IEEE,* and A. Lee Swindlehurst, *Fellow, IEEE*

***Abstract*—In this paper, the performance of a secure massive multiple-input multiple-output (MIMO) system adopting low-resolution digital-to-analog converters (DACs) is analyzed over spatially correlated wireless channels. A tight lower bound for the achievable secrecy rate is derived with artificial noise (AN) transmitted in the null space of the user channels. Using the analytical results, the impact of spatial correlation on the secrecy rate is explicitly evaluated in the presence of low-resolution DACs. The analytical observations reveal that using low-resolution DACs can be beneficial to the secrecy performance compared with ideal DACs, when the channels are strongly correlated and optimal power allocation is not employed.**

***Index Terms*—Physical layer security, massive MIMO, spatial correlation, digital-to-analog converters (DACs)**

I. Introduction

PHYSICAL layer security (PLS) has become an emerging technology for securing wireless communication without relying upon traditional cryptographic mechanisms. Compared to conventional upper-layer cryptographic schemes, PLS has the advantages of low computational complexity and low resource consumption [1]. Massive multiple-input multiple-output (MIMO) systems provide another disruptive technology for fifth generation (5G) cellular communications, and have shown great potential in improving spectral and energy efficiency. The use of large-scale antenna arrays in massive MIMO provides a large excess of redundant spatial degrees of freedom (DoF), which can be exploited to achieve secure physical layer transmission. This idea has been attracting increasing research interest in the past few years [2], [3].

Massive MIMO transmission requires a very high power consumption if high-resolution digital-to-analog converters (DACs) are employed in the RF chains for each antenna. At the transmitter, power expenditure is dominated by power amplifiers (PAs), which are usually required to operate within a high linearity regime to avoid distortion. A practical solution to the above challenge is to use low-resolution DACs, which relaxes the requirement of linearity and allows the amplifiers to operate closer to saturation, thus increasing the efficiency of PAs [4], [5]. In [6], both finite-bit DACs at base station (BS) and finite-bit analog-to-digital converters (ADCs) at user side were analyzed in the massive MIMO downlink. The work was then extended in [7] by considering spatially correlated channels. Further in [8], a constant envelope precoding technique was devised for the multiuser MIMO with one-bit DACs.

The effect of hardware impairments (HWIs) on spectral efficiency of massive MIMO systems has been studied in [9]. Regarding the secrecy performance, the authors in [10] analyzed the effects of HWIs on secrecy rate, where ideal converters with infinite resolution were considered. Secure communication in a massive MIMO system with low-resolution DACs was investigated in [11], which revealed that low-resolution DACs can achieve superior secrecy rate under certain conditions, e.g., at low SNR or with a large power allocation factor.

Most of the existing works on low-resolution DACs transmissions have focused on the assumption of independent identically distributed (i.i.d.) channels for massive MIMO. However, in practice, the limited space between the BS antennas as well as the rich scattering propagation environment can result in spatial correlation. The impact of correlated Rayleigh fading channels on optimal multiuser loading was analyzed in [6] by applying asymptotic random matrix theory. How spatial correlation impacts secure massive MIMO communication with low-resolution DACs is still an open problem.

In this paper, we focus on secure transmission in the massive MIMO downlink when low-resolution DACs are employed. A tight lower bound for the ergodic secrecy rate is derived that explicitly characterizes the impact of channel correlation on the secrecy rate for typical correlated channels. An optimal power allocation strategy is proposed, which suggests that more power should be allocated to AN when strong channel correlation is present. It is revealed that using low-resolution DACs can improve the secrecy performance for a fixed power allocation factor under strong spatially correlated channels.

Notation: $\mathbf{X}^*$, $\mathbf{X}^T$, $\mathbf{X}^H$ and $\mathrm{tr}(\mathbf{X})$ represent the conjugate, transpose, conjugate transpose and trace of matrix $\mathbf{X}$, respectively. $\mathbb{E}\{\cdot\}$ is the expectation operator. $\mathrm{diag}(\cdot)$ denotes a diagonal matrix that retains only the diagonal elements of the input matrix, and $\widetilde{\mathrm{diag}}(\cdot)$ represents a diagonal matrix with the input vector as its diagonal entries.

Manuscript received March 5, 2021; accepted June 28, 2021. This work was supported by the NSFC under grants 61941115 and 62022026, and the Natural Science Foundation of Jiangsu Province for Distinguished Young Scholars under Grant BK20190012. *(Corresponding author: Wei Xu, Bin Sheng.)*

D. Yang, J. Xu, and B. Sheng are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (email: dyang@seu.edu.cn, jdxu@seu.edu.cn, sbdtt@seu.edu.cn).

W. Xu is with the National Mobile Communications Research Lab, Southeast University, Nanjing 210096, China, and also with Henan Joint International Research Laboratory of Intelligent Networking and Data Analysis, Zhengzhou University, Zhengzhou, 450001 China (wxu@seu.edu.cn).

N. Wang is with the School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China.

A. Lee Swindlehurst is with the Center for Pervasive Communications and Computing, University of California at Irvine, Irvine, CA 92697 USA (e-mail: swindle@uci.edu).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2021.3094204, IEEE Wireless Communications Letters

II. System Model

The secure massive MIMO system under investigation comprises one N-antenna BS, K single-antenna legitimate users, and one M-antenna passive eavesdropper. The channel matrices are modeled based on the Kronecker channel model as shown in [12]. To make the problem more tractable, we consider the system with a common correlation matrix at the BS. Specifically, the channel between the BS and the users is modeled as $\mathbf{H} = \mathbf{D}^{\frac{1}{2}}\widetilde{\mathbf{H}}\mathbf{R}^{\frac{1}{2}}$, where the elements of $\widetilde{\mathbf{H}} \in \mathbb{C}^{K\times N}$ are i.i.d. Gaussian random variables with zero mean and unit variance, the diagonal matrix $\mathbf{D} \in \mathbb{C}^{K\times K}$ characterizes the large-scale fading with its kth diagonal element given by β_k, and $\mathbf{R} \in \mathbb{C}^{N\times N}$ is the transmit covariance matrix satisfying $\mathrm{tr}(\mathbf{R}) = N$. Similarly, the channel matrix between the BS and the eavesdropper is $\mathbf{H}_\mathrm{e} = \mathbf{D}_\mathrm{e}^{\frac{1}{2}}\widetilde{\mathbf{H}}_\mathrm{e}\mathbf{R}^{\frac{1}{2}}$, where $\widetilde{\mathbf{H}}_\mathrm{e} \in \mathbb{C}^{M\times N}$ contains i.i.d. Rayleigh fading channel coefficients following $\mathcal{CN}(0,1)$. The diagonal matrix $\mathbf{D}_\mathrm{e}$ represents the large-scale fading at the eavesdropper with identical diagonal entries β^e.

The BS desires to transmit the symbols $\mathbf{s} = [s_1, s_2, ..., s_K] \in \mathbb{C}^{K\times 1}$ to the legitimate users with $\mathbb{E}\{\mathbf{s}\mathbf{s}^H\} = \mathbf{I}_K$ using a linear precoding matrix $\mathbf{W} \in \mathbb{C}^{N\times K}$. The eavesdropper's channel state information (CSI) is assumed unknown to the BS, and AN is injected to ensure confidential communication. The AN vector $\mathbf{t} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N-K})$ is precoded by an AN shaping matrix $\mathbf{V} \in \mathbb{C}^{N\times(N-K)}$. Denote by P the total transmit power. The power allocation factor $\xi \in (0,1]$ aims to strike a balance between the transmit signal and the AN. The unquantized downlink transmit signal vector $\mathbf{x}$ is then expressed as

$$\mathbf{x} = \sqrt{\mu}\mathbf{W}\mathbf{s} + \sqrt{\nu}\mathbf{V}\mathbf{t}, \tag{1}$$

where $\mu \triangleq \frac{\xi P}{K}$ and $\nu \triangleq \frac{(1-\xi)P}{N-K}$.

The precoded signal is transmitted after DAC quantization, which is denoted by $\mathcal{Q}(\mathbf{x})$. Establishing the non-linear quantization model of a finite-bit DAC is challenging. We follow a popular way of charactering the quantizer by a linear function applying the simple additive quantization noise model. The quantized signal vector can accordingly be decomposed as

$$\mathbf{z} = \mathcal{Q}(\mathbf{x}) = \sqrt{1-\rho}\mathbf{x} + \mathbf{q}, \tag{2}$$

where the quantization noise $\mathbf{q}$ is assumed to be uncorrelated with the input signal $\mathbf{x}$, and

$$\mathbf{C}_\mathbf{q} = \mathbb{E}\{\mathbf{q}\mathbf{q}^H\} = \rho\mathbb{E}\big\{\mathrm{diag}(\mathbf{x}\mathbf{x}^H)\big\}. \tag{3}$$

The value of the distortion factor ρ depends on the DAC resolution; for example, it can be chosen as in [5] for DAC resolutions of less than 5 bits, or as $\rho = \frac{\sqrt{3}\pi}{2}\cdot 2^{-2b}$ for scenarios with higher precision, where b represents the number of quantization bits. From (1) and (3), the covariance matrix of the quantization noise equals

$$\mathbf{C}_\mathbf{q} = \rho\big[\mu\mathrm{diag}(\mathbf{W}\mathbf{W}^H) + \nu\mathrm{diag}(\mathbf{V}\mathbf{V}^H)\big]. \tag{4}$$

Given the CSI of the legitimate channels, the matrix $\mathbf{V}$ is designed to lie in the null space of the channel matrix $\mathbf{H}$, i.e., $\mathbf{H}\mathbf{V} = \mathbf{0}$, which (ideally) makes the AN "invisible" to the legitimate users [13]. Using (1) and (2), the signals received at the users and the eavesdropper are expressed as

$$\mathbf{y} = \sqrt{1-\rho}(\sqrt{\mu}\mathbf{H}\mathbf{W}\mathbf{s} + \sqrt{\nu}\mathbf{H}\mathbf{V}\mathbf{t}) + \mathbf{H}\mathbf{q} + \mathbf{n} \tag{5}$$

$$\mathbf{y}_\mathrm{e} = \sqrt{1-\rho}(\sqrt{\mu}\mathbf{H}_\mathrm{e}\mathbf{W}\mathbf{s} + \sqrt{\nu}\mathbf{H}_\mathrm{e}\mathbf{V}\mathbf{t}) + \mathbf{H}_\mathrm{e}\mathbf{q} + \mathbf{n}_\mathrm{e}, \tag{6}$$

where $\mathbf{n} \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2\mathbf{I}_K)$ and $\mathbf{n}_\mathrm{e} \sim \mathcal{CN}(\mathbf{0}, \sigma_\mathrm{e}^2\mathbf{I}_M)$ respectively represent the additive noise terms at the users and at the eavesdropper.

III. Achievable Ergodic Secrecy Rate Analysis

In this section, we derive a tight lower bound for the ergodic secrecy rate of the secure multiuser massive MIMO downlink and analyze the impact of spatial correlation on the secrecy rate in the presence of low-resolution DACs.

A. Lower Bound on the Achievable Ergodic Secrecy Rate

We adopt linear matched filter (MF) precoding for data transmission, i.e., $\mathbf{W} = \mathbf{H}/\|\mathbf{H}\|$. The received signal at the kth user according to (5) is expressed as

$$y_k = \sqrt{1-\rho}\big(\sqrt{\mu}\mathbf{h}_k^T\mathbf{W}\mathbf{s} + \sqrt{\nu}\mathbf{h}_k^T\mathbf{V}\mathbf{t}\big) + \mathbf{h}_k^T\mathbf{q} + n_k. \tag{7}$$

Then, under the assumption of Gaussian distributed interference, a lower bound on the ergodic rate for the kth user can be calculated as

$$R_k = \mathbb{E}\big\{\log_2(1+\gamma_k)\big\}, \tag{8}$$

$$\gamma_k = \frac{(1-\rho)\mu\big|\mathbf{h}_k^T\mathbf{w}_k\big|^2}{\varrho + \mathbf{h}_k^T\mathbf{C}_\mathbf{q}\mathbf{h}_k^* + (1-\rho)\nu\mathbf{h}_k^T\mathbf{V}\mathbf{V}^H\mathbf{h}_k^* + \sigma_n^2}, \tag{9}$$

where $\varrho = (1-\rho)\mu\sum\limits_{j\neq k}\big|\mathbf{h}_k^T\mathbf{w}_j\big|^2$, $\mathbf{h}_k^T$ denotes the kth row of $\mathbf{H}$, and $\mathbf{w}_k$ is the kth column of $\mathbf{W}$. Note that the numerator of γ_k is the power of the desired signal component for the kth user, and the denominator represents the power from inter-user interference, quantization noise from the low-resolution DACs, AN leakage, and thermal noise.

Lemma 1: A lower bound on the achievable rate (8) of user k is given by

$$\underline{R}_k = \log_2\bigg(1 + \frac{(1-\rho)\beta_k^2\gamma_0\xi N/\sum_{i=1}^K\beta_i}{\varrho' + \rho\beta_k\gamma_0 + 1}\bigg), \tag{10}$$

where $\varrho' = (1-\rho)\xi\gamma_0\beta_k\mathrm{tr}(\mathbf{R}^2)\sum\limits_{j\neq k}\beta_j/(N\sum_{i=1}^K\beta_i)$, and $\gamma_0 = \frac{P}{\sigma_n^2}$ is the average SNR.

Proof: Please refer to Appendix A. ■

To guarantee secure communication in the worst case, we assume that the eavesdropper has perfect CSI of all legitimate users and can remove all the interference from the legitimate users [2], [3], [10], [11]. According to (6), the ergodic rate of the eavesdropper is expressed as

$$C = \mathbb{E}\bigg\{\log_2\big(1 + (1-\rho)\mu\mathbf{w}_k^H\mathbf{H}_\mathrm{e}^H\mathbf{X}^{-1}\mathbf{H}_\mathrm{e}\mathbf{w}_k\big)\bigg\}, \tag{11}$$

where $\mathbf{X}$ is defined as

$$\mathbf{X} = (1-\rho)\nu\mathbf{H}_\mathrm{e}\mathbf{V}\mathbf{V}^H\mathbf{H}_\mathrm{e}^H + \mathbf{H}_\mathrm{e}\mathbf{C}_\mathbf{q}\mathbf{H}_\mathrm{e}^H. \tag{12}$$

Furthermore, we assume that σ_e^2 is negligibly small corresponding to the worst case, and consequently, C is independent of the path-loss of the eavesdropper β^e [2], [3], [10], [11]. A tight upper bound for C is derived in the following lemma.

Lemma 2: For $N\to\infty$, an upper bound on the eavesdropping rate is given by

$$\overline{C} = \log_2\bigg(1 + \frac{\phi M\xi\kappa\beta_k/\sum_{i=1}^K\beta_i}{\phi\kappa^2\big(\frac{N}{\mathrm{tr}(\mathbf{R}^2)} - a\big) - \varpi}\bigg), \tag{13}$$

where $a = \frac{M}{N}$, $b = \frac{K}{N}$, $\rho' = \frac{\rho}{1-\rho}$, $\phi = 1-b$, $\kappa = 1-\xi+\rho'$, and $\varpi = ab(1-\xi)^2$.

Proof: Please refer to Appendix B. ■

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2021.3094204, IEEE Wireless Communications Letters

Applying *Lemma 1* and *Lemma 2*, a lower bound on the ergodic secrecy rate of the kth user is obtained in *Theorem 1*.

Theorem 1: For $N \to \infty$, the achievable ergodic secrecy rate for the kth user is lower bounded by

$$\underline{R}_{\text{sec}} \triangleq [\underline{R}_k - \overline{C}]^+, \tag{14}$$

where $[x]^+ = \max\{0, x\}$, and $\underline{R}_k$ and $\overline{C}$ are given in (10) and (13), respectively.

If no spatial correlation is present, i.e., $\mathbf{R} = \mathbf{I}$, then (14) reduces to

$$\underline{R}_{\text{sec}} = \left[\log_2\left(1 + \frac{(1-\rho)\beta_k^2\gamma_0\xi N/\sum_{i=1}^K \beta_i}{(1-\rho)\gamma_0\beta_k\xi \sum\limits_{j\neq k} \beta_j/\sum_{i=1}^K \beta_i + \rho\beta_k\gamma_0 + 1}\right) - \log_2\left(1 + \frac{\phi M\xi\kappa\beta_k/\sum_{i=1}^K \beta_i}{\phi\kappa^2(1-a) - \varpi}\right)\right]^+. \tag{15}$$

As expected, $\underline{R}_{\text{sec}}$ increases with N and γ_0.

B. Optimal Power Allocation Strategy for AN

Here we investigate the impact of the power allocation factor on the ergodic secrecy rate in (14) under spatially correlated channels. Assume $ab \ll 1$ in (13), which is reasonable in massive MIMO equipped with a large number of antennas. The derivative of $\underline{R}_{\text{sec}}$ w.r.t. ξ is calculated as

$$\frac{\partial \underline{R}_{\text{sec}}}{\partial \xi} = \frac{L_1 L_2}{\ln 2(L_3\xi + L_2)[L_2 + \xi(L_1 + L_3)]} - \frac{M\text{tr}(\mathbf{R}^2)(1+\rho')\beta_k}{\ln 2\big[\sum_{i=1}^K \beta_i\big(N - \text{tr}(\mathbf{R}^2)a\big)\kappa^2 + M\xi\beta_k\text{tr}(\mathbf{R}^2)\kappa\big]}, \tag{16}$$

where $L_1 = (1-\rho)\beta_k^2\gamma_0 N/\sum_{i=1}^K \beta_i$, $L_2 = \rho\beta_k\gamma_0 + 1$, and $L_3 = (1-\rho)\gamma_0\beta_k\text{tr}(\mathbf{R}^2)\sum\limits_{j\neq k}\beta_j/(N\sum_{i=1}^K \beta_i)$. Since $\frac{\partial \underline{R}_{\text{sec}}}{\partial \xi} > 0$ for small ξ and $\frac{\partial \underline{R}_{\text{sec}}}{\partial \xi} < 0$ for large ξ, the optimal power allocation factor ξ^* that achieves the highest secrecy rate is obtained by setting $\frac{\partial \underline{R}_{\text{sec}}}{\partial \xi} = 0$. A closed-form expression for ξ^* can be founded as follows:

$$\xi^* = \frac{-B - \sqrt{B^2 - 4AC}}{2A}, \tag{17}$$

where the parameters A, B, and C are given by

$$A = L_1L_2G_2 - L_1L_2G_3 - G_1L_3(L_1 + L_3), \tag{18}$$

$$B = (1+\rho')L_1L_2(G_3 - 2G_2) - G_1L_2(L_1 + 2L_3), \tag{19}$$

$$C = G_2L_1L_2(1+\rho')^2 - G_1L_2^2, \tag{20}$$

and $G_1 = M\text{tr}(\mathbf{R}^2)(1+\rho')\beta_k$, $G_2 = \sum_{i=1}^K \beta_i\big(N - \text{tr}(\mathbf{R}^2)a\big)$, and $G_3 = M\beta_k\text{tr}(\mathbf{R}^2)$.

Assuming $\beta_k = 1, 1 \le k \le K$, we can simplify the above expressions to evaluate the impact of spatial correlation on ξ^* for different DAC resolutions. Comparing the value of ξ^* for the special case of an i.i.d. channel, i.e.,$\text{tr}(\mathbf{R}^2) = N$ with a fully correlated channel, i.e., $\text{tr}(\mathbf{R}^2) = N^2$ for a Hermitian Toeplitz correlation matrix, we can easily observe that ξ^* decreases when $\text{tr}(\mathbf{R}^2)$ increases from N to N^2. The relationship between ξ^* and the design parameters, including the DAC resolution and channel correlation coefficient, is verified in Section IV through numerical results.

C. Impact of Spatial Correlation

We first analyze the impact of the antenna ratio a under the correlated channel condition when AN is injected. In (14), $\underline{R}_{\text{sec}}$ decreases with respect to a. Considering the special case of $\beta_k = \beta, 1 \le k \le K$, and $\xi \to 0$, by setting $R_{\text{sec}} = 0$, the maximum number of eavesdropper antennas that still allows for a positive secrecy rate can be obtained from the following proposition.

Proposition 1: If a positive secrecy rate can be achieved, then the maximum antenna ratio a is obtained as

$$a_{\text{sec}} = \frac{(1-b)N\gamma_0}{\text{tr}(\mathbf{R}^2)\big[\gamma_0\rho b(\rho - \beta - 2) + \gamma_0(1+\beta\rho) + 1 - b\big]}. \tag{21}$$

Remark 1: By direct inspection of (21), the maximum number of eavesdropper antennas that can be tolerated for secure transmission decreases with ρ and the spatial correlation level because Eve can wiretap more information under strongly correlated channels. For the special case of $\rho \to 0$ and $\text{tr}(\mathbf{R}^2) = N^2$, we have $a_{\text{sec}} = \frac{(1-b)\gamma_0}{N(1-b+\gamma_0)}$, which indicates that a_{sec} is independent of the large-scale fading factor with infinite-resolution DACs.

To extract clear insights, we further consider a representative exponential correlation model [14]

$$\mathbf{R}_{ij} = \zeta^{|i-j|}, \tag{22}$$

where ζ denotes the correlation coefficient. The exponential model is widely adopted in literature and is applicable to analysis for a massive MIMO system with uniform planar array (UPA) scenarios [15].

Proposition 2: The secrecy rate gap for different DAC resolutions decreases with the correlation coefficient ζ.

Proof: $\lim\limits_{N\to\infty} \frac{\text{tr}(\mathbf{R}^2)}{N} = \frac{1+\zeta^2}{1-\zeta^2}$ exists under the exponential correlation model in (22). From (14), we have $\frac{\partial \underline{R}_{\text{sec}}}{\partial \rho} = \frac{\partial \underline{R}_k}{\partial \rho} - \frac{\partial \overline{C}}{\partial \rho}$. The first term $\frac{\partial \underline{R}_k}{\partial \rho}$ is given by

$$\frac{\partial \underline{R}_k}{\partial \rho} = -\frac{\beta_k^2\gamma_0\xi N(1+\beta_k\gamma_0)\sum_{i=1}^K \beta_i}{\ln 2(\Upsilon\beta_k\gamma_0 + \sum_{i=1}^K \beta_i)(\Psi\beta_k\gamma_0 + \sum_{i=1}^K \beta_i)}, \tag{23}$$

where $\Upsilon = (1-\rho)(N\beta_k + \widetilde{\zeta}\sum_{j\neq k}\beta_j)\xi + \rho\sum_{i=1}^K \beta_i$, $\Psi = \rho\sum_{i=1}^K \beta_i + (1-\rho)\xi\widetilde{\zeta}\sum_{j\neq k}\beta_j$, and $\widetilde{\zeta} = \frac{1+\zeta^2}{1-\zeta^2}$. The expression of $\frac{\partial \overline{C}}{\partial \rho}$ is shown in (24), on the top of the next page. Assuming $ab \ll 1$ for typical massive MIMO systems, (24) can be simplified as

$$\frac{\partial \overline{C}}{\partial \rho} = -\frac{M\xi\phi\beta_k\widetilde{\zeta}/\sum_{i=1}^K \beta_i}{\ln 2(1-\rho)^2\big\{\big[\kappa - (M\xi\beta_k/\sum_{i=1}^K \beta_i - a\kappa)\widetilde{\zeta}\big]\kappa\phi\big\}}. \tag{25}$$

Focusing on the impact of ζ, we observe that $\frac{\partial \overline{C}}{\partial \rho} < 0$ and decreases with ζ, while $\frac{\partial \underline{R}_k}{\partial \rho} < 0$ and increases with ζ. Therefore, $\frac{\partial \underline{R}_{\text{sec}}}{\partial \rho}$ is an increasing function of ζ, which completes the proof. ■

Remark 2: From (23) and (25), it shows that $\frac{\partial \underline{R}_{\text{sec}}}{\partial \rho} < 0$ and $\frac{\partial \underline{R}_{\text{sec}}}{\partial \rho}$ is a monotonically increasing function in terms of the level of spatial correlation ζ. It implies that the eavesdropper's capacity $\overline{C}$ degrades faster than $\underline{R}_k$ does at large ζ. Thus, we conclude that there exists a threshold of correlation coefficient, i.e., $\overline{\zeta}$, where lower-resolution DACs achieve a higher secrecy rate for $\zeta \in (\overline{\zeta}, 1)$. The value of $\overline{\zeta}$ is obtained from the solution of $\frac{\partial \underline{R}_{\text{sec}}}{\partial \rho} = 0$ by focusing on the impact of spatial correlation. Note that the higher the correlation the lower the effective dimension (d.o.f.), in the extreme case of $\zeta = 1$, the users and Eve are separated only in the angle of arrival domain, which only has dimension 1 instead of N. Therefore, quantization noise from lower-resolution DACs could compensate for AN to improve secrecy rate under spatially correlated channel.

IV. Numerical Results

In this section, the analytical results are validated through Monte-Carlo simulation. We consider a system with $N = 256$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2021.3094204, IEEE Wireless Communications Letters

$$\frac{\partial \overline{C}}{\partial \rho} = -\frac{M\xi\phi\beta_k\widetilde{\zeta}[(1-a\widetilde{\zeta})\phi\kappa^2 + \varpi\widetilde{\zeta}]/\sum_{i=1}^{K}\beta_i}{\ln 2(1-\rho)^2\left[(a\widetilde{\zeta}-1)\phi\kappa^2 + \varpi\widetilde{\zeta}\right]\left\{\left[(a\kappa^2 - M\xi\kappa\beta_k/\sum_{i=1}^{K}\beta_i)\widetilde{\zeta} - \kappa^2\right]\phi + \varpi\widetilde{\zeta}\right\}} \tag{24}$$

$K = 16$, and $M = 4$ in all simulations. The large-scale fading is modeled as $\beta_k = (d_{\text{ref}}/d_k)^{\eta}$, where $\eta = 3.8$ denotes the path loss exponent, $d_{\text{ref}} = 300$ (m) and $d_k \leq 500$ (m) are, respectively, the reference distance and the distance between the BS and the kth user. The expected values in (14) were evaluated by averaging over 1000 random channel realizations.

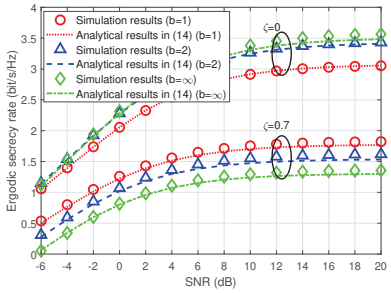


Fig. 1. Ergodic secrecy rate and analytical lower bound versus SNR for different spatial correlation coefficient ζ ($\xi = 0.7$)

Fig. 1 shows the ergodic secrecy rate versus the average SNR γ_0 under different DAC resolutions and spatial correlations. The derived lower bound on the secrecy rate is fairly accurate and tight for the entire range of SNR. In addition, it is observed that the secrecy rate is decreasing as ζ increases.

Fig. 2 plots the ergodic secrecy rate as a function of the power allocation factor ξ. The optimal power allocation factor ξ^* largely depends on ζ. Specifically, It is observed that ξ^* decreases with ζ. The information signal leakage grows when the spatial correlation is strong. Thus, more power should be allocated for AN to ensure secure communication.

In Fig. 3 (a) we show the ergodic secrecy rate versus ζ with different DAC resolutions for γ_0 = 10 dB. We choose a fixed power allocation factor ξ due to the difficulties in optimizing ξ theoretically. The secrecy rate loss due to low-resolution DACs decreases with ζ as predicted in *Remark 2*. Interestingly, although the channel correlation has a detrimental effect on the secrecy rate, the use of 1-bit DACs can improve the secrecy rate when the spatial correlation coefficient is large. This is because the additional quantization noise serves to increase the level of AN, which is beneficial for spatially colored channels if the AN level has not already been optimized. Finally, Fig. 3 (b) presents the secrecy rate versus ζ assuming the optimal power allocation ξ^* in (17) is chosen. The secrecy rate gaps are $\Delta R_{\text{sec}} = 0.697$ bit/s/Hz at $\zeta = 0$ and $\Delta R_{\text{sec}} = 0.434$ bit/s/Hz at $\zeta = 0.8$, respectively. If optimal power allocation is adopted, then using infinite-resolution DACs can always achieve a higher secrecy rate. In this case, quantization noise from lower-resolution DACs does not compensate for the AN anymore. However, we observe that the secrecy rate loss due to low-resolution DACs decreases with channel correlation coefficient, regardless of the value of ξ.

For comparison, Fig. 4 plots the Monte-Carlo simulation by using the spatial correlation model in [9], denoted by $[\mathbf{R}]_{s,m} = \frac{\beta}{L}\sum_{l=1}^{L} e^{j\pi(s-m)\sin(\varphi_l)} e^{-\frac{\Delta^2}{2}\left(\pi(s-m)\cos(\varphi_l)\right)^2}$, where β is the large scale fading coefficient, φ is the actual angle-of-arrival and Δ is the azimuth angular spread. We consider $L = 10$ scattering clusters and $\varphi \sim [\frac{-\Delta}{2}, \frac{\Delta}{2}]$. It is observed that transitioning from larger to smaller angular spread ($\Delta = 50^{\text{o}}$ to $\Delta = 12^{\text{o}}$) significantly reduces the secrecy rate of the kth user for different DAC resolutions. However, the lower resolution DAC is always beneficial for secrecy rate with a fixed ξ under highly correlated channels as expected.

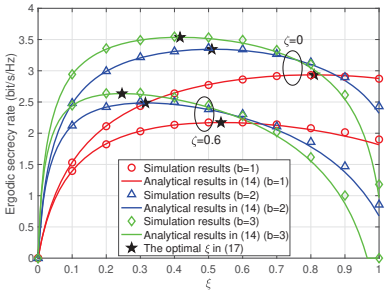
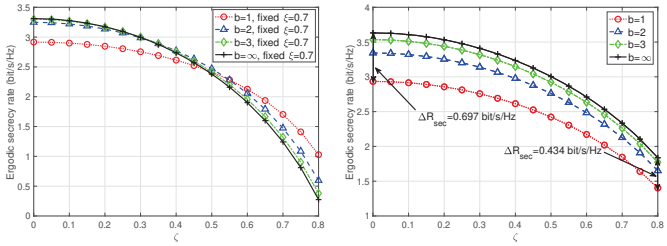


Fig. 2. Achievable ergodic secrecy rate versus the power allocation factor ξ for different DAC resolutions ($\gamma_0 = 10$ dB)



(a) with fixed ξ=0.7 (b) with optimal ξ^* in (17)

Fig. 3. Achievable ergodic secrecy rate versus ζ for different DAC resolutions

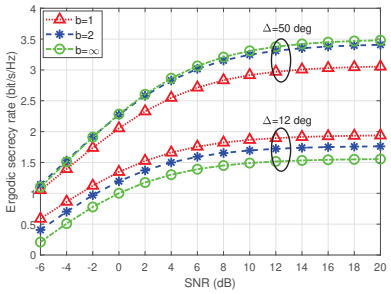


Fig. 4. Ergodic secrecy rate versus SNR ($\xi = 0.7$)

V. Conclusion

This paper has characterized the performance of AN-based secure transmission in a massive MIMO downlink system with low-resolution DACs under spatially correlated channels. In particular, it is shown that optimal secrecy performance can be obtained by increasing the amount of power dedicated to artificial noise when the channel correlation increases. Furthermore, the use of low-resolution DACs has been shown to be beneficial to the secrecy performance for a fixed power allocation factor when the channels possess strong spatial correlation. Interesting future extension of this paper includes

studying the impact of different spatial correlation matrices at both transmitter and the eavesdropper.

APPENDIX A

Consider MF precoding satisfying $\mathrm{tr}(\mathbf{W}\mathbf{W}^H)=K$, which leads to $\mathbf{W}=\sqrt{\frac{K}{N\sum_{i=1}^{K}\beta_i}}\mathbf{H}$. First, we directly obtain

$$\begin{aligned}\left|\mathbf{h}_k^T\mathbf{w}_k\right|^2&=\frac{K}{N\sum_{i=1}^{K}\beta_i}\left|\mathbf{h}_k^T\mathbf{h}_k\right|^2\\&=\frac{K\beta_k^2}{N\sum_{i=1}^{K}\beta_i}\left[\mathrm{tr}(\mathbf{R})\right]^2\xrightarrow{\text{a.s.}}\frac{KN\beta_k^2}{\sum_{i=1}^{K}\beta_i},\end{aligned}\tag{26}$$

where we have used $\frac{1}{\sqrt{N}}\widetilde{\mathbf{h}}_k^T\mathbf{R}\frac{1}{\sqrt{N}}\widetilde{\mathbf{h}}_k^*-\frac{1}{N}\mathrm{tr}(\mathbf{R})\xrightarrow{\text{a.s.}}0$ in [16, Lemma 4]. Then, the inter-user interference is calculated as

$$\begin{aligned}\varrho&=(1-\rho)\mu\sum_{j\neq k}\frac{K}{N\sum_{i=1}^{K}\beta_i}\left|\mathbf{h}_k^T\mathbf{h}_j\right|^2\\&\xrightarrow{a.s.}(1-\rho)\mu K\beta_k\mathrm{tr}(\mathbf{R}^2)\sum_{j\neq k}\beta_j\Big/\left(N\sum_{i=1}^{K}\beta_i\right).\end{aligned}\tag{27}$$

For large N and K, $\mathbf{C_q}$ converges to

$$\mathbf{C_q}\xrightarrow{a.s.}\rho\frac{P}{N}\mathbf{I}_N,\tag{28}$$

where we use the definition of μ and ν, and the fact that $\mathrm{diag}(\mathbf{W}\mathbf{W}^H)\xrightarrow{a.s.}\frac{K}{N}\mathbf{I}_N$ and $\mathrm{diag}(\mathbf{V}\mathbf{V}^H)\xrightarrow{a.s.}\frac{N-K}{N}\mathbf{I}_N$ due to the strong law of large numbers. Further, we obtain the component of the quantization noise as

$$\mathbf{h}_k^T\mathbf{C_q}\mathbf{h}_k^*\xrightarrow{a.s.}\rho\frac{P}{N}\beta_k\mathrm{tr}(\mathbf{R})=\rho P\beta_k.\tag{29}$$

Regarding the AN power, it follows that

$$\mathbf{h}_k^T\mathbf{V}\mathbf{V}^H\mathbf{h}_k^*=0,\tag{30}$$

since $\mathbf{H}\mathbf{V}=\mathbf{0}$. Finally, by substituting (26), (27), (29), (30) and the definition of μ and ν into (8), and according to the Continuous Mapping Theorem, we complete the proof.

APPENDIX B

By applying Jensen's inequality, the capacity of the eavesdropper can be upper bounded as

$$C\leq\log_2\left[1+(1-\rho)\mu\mathbb{E}\left\{\mathbf{w}_k^H\mathbf{H}_\mathrm{e}^H\mathbf{X}^{-1}\mathbf{H}_\mathrm{e}\mathbf{w}_k\right\}\right].\tag{31}$$

Let us first focus on the term $\mathbf{X}$ and by substituting (28) into (12) yields

$$\mathbf{X}\xrightarrow{a.s.}\left[(1-\rho)\nu+\rho\frac{P}{N}\right]\mathbf{X}_1+\rho\frac{P}{N}\mathbf{X}_2,\tag{32}$$

where $\mathbf{X}_1=\mathbf{H}_\mathrm{e}\mathbf{V}\mathbf{V}^H\mathbf{H}_\mathrm{e}^H$ and $\mathbf{X}_2=\mathbf{H}_\mathrm{e}\mathbf{V}_0\mathbf{V}_0^H\mathbf{H}_\mathrm{e}^H$. It is obvious that $[\mathbf{V}\ \mathbf{V}_0][\mathbf{V}\ \mathbf{V}_0]^H=\mathbf{I}_M$, because $[\mathbf{V}\ \mathbf{V}_0]$ forms a complete orthogonal basis. Eigendecompose $\mathbf{R}$ such that $\mathbf{R}=\mathbf{U}\mathbf{\Lambda}\mathbf{U}^H$ to decorrelate matrix $\mathbf{H}_\mathrm{e}$ as $\mathbf{Z}=\mathbf{H}_\mathrm{e}\mathbf{\Lambda}^{-\frac{1}{2}}\mathbf{U}^H$, where $\mathbf{\Lambda}=\mathrm{diag}(\lambda_1,...,\lambda_N)$ is the diagonal matrix of the eigenvalues of $\mathbf{R}$ and the columns of $\mathbf{U}$ consist of the corresponding eigenvectors. Since $\mathbf{U}$ is unitary, the statistics of $\mathbf{Z}\mathbf{U}$ are identical to those of $\mathbf{Z}$. Thereby, the distributions of $\mathbf{X}_1$ and $\mathbf{X}_2$ are the same as

$$\sum_{i=1}^{N}\sum_{j=1}^{N}\lambda_i^{\frac{1}{2}}\lambda_j^{\frac{1}{2}}\mathbf{z}_i\mathbf{v}_i\mathbf{v}_j^H\mathbf{z}_j^H\tag{33}$$

and

$$\sum_{i=1}^{N}\sum_{j=1}^{N}\lambda_i^{\frac{1}{2}}\lambda_j^{\frac{1}{2}}\mathbf{z}_i\mathbf{v}_{0,i}\mathbf{v}_{0,j}^H\mathbf{z}_j^H,\tag{34}$$

where $\mathbf{z}_i$ is the ith row of $\mathbf{Z}$, $\mathbf{v}_i$ and $\mathbf{v}_{0,i}$ are ith column of $\mathbf{V}$ and $\mathbf{V}_0$, respectively. Following the same approach in [17], $\mathbf{Y}=\left[(1-\rho)\nu+\rho\frac{P}{N}\right]\mathbf{Y}_1+\rho\frac{P}{N}\mathbf{Y}_2$ may be accurately approximated as a single scaled Wishart matrix $\mathbf{Y}\sim\mathcal{W}_M(\eta,\varphi\mathbf{I}_M)$, where we define $\mathbf{Y}_1=\sum_{m=1}^{N}\lambda_m\mathbf{z}_m\mathbf{v}_m\mathbf{v}_m^H\mathbf{z}_m^H$ and $\mathbf{Y}_2=\sum_{n=1}^{N}\lambda_n\mathbf{z}_n\mathbf{v}_{0,n}\mathbf{v}_{0,n}^H\mathbf{z}_n^H$. Equating the first two moments of those matrices with $\mathbf{Y}_1\sim\sum_{m=1}^{N}\lambda_m\mathcal{W}_M(N-K,\frac{1}{N}\mathbf{I}_M)$ and $\mathbf{Y}_2\sim\sum_{n=1}^{N}\lambda_n\mathcal{W}_M(K,\frac{1}{N}\mathbf{I}_M)$ leads to

$$\eta\varphi=\left[(1-\rho)\nu+\rho\frac{P}{N}\right](N-K)+\rho\frac{P}{N}K\tag{35}$$

and

$$\eta\varphi^2=\frac{\mathrm{tr}(\mathbf{R}^2)}{N}\left\{\left[(1-\rho)\nu+\rho\frac{P}{N}\right]^2(N-K)+\left(\rho\frac{P}{N}\right)^2K\right\},\tag{36}$$

where we use $\sum_{i=1}^{N}\lambda_i=\mathrm{tr}(\mathbf{R})$ and $\sum_{i=1}^{N}\lambda_i^2=\mathrm{tr}(\mathbf{R}^2)$. By exploiting the independence of the elements in $\widetilde{\mathbf{H}}_\mathrm{e}$, we can further obtain $\mathbf{X}^{-1}\xrightarrow{\text{a.s.}}1/(\varphi(\eta-M))\mathbf{I}_M$ with $\eta>M$, where we use the property $\mathbf{A}^{-1}\xrightarrow{\text{a.s.}}1/(n-m)\mathbf{I}_m$ for a Wishart matrix $\mathbf{A}\sim\mathcal{W}_m(n,\mathbf{I}_m)$ with $n>m$ [4]. Substituting this result and $\mathbb{E}\left[\mathbf{w}_k^H\mathbf{H}_\mathrm{e}^H\mathbf{H}_\mathrm{e}\mathbf{w}_k\right]=\frac{MK\beta_k}{N\sum_{i=1}^{K}\beta_i}\mathrm{tr}(\mathbf{R}^2)$ into (31) completes the proof.

REFERENCES

[1] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Jul. 2011.

[2] 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.

[3] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[4] A. K. Saxena, I. Fijalkow, and A. L. Swindlehurst, "Analysis of one-bit quantized precoding for the multiuser massive MIMO downlink," *IEEE Trans. Signal Process.*, vol. 65, no. 17, pp. 4624–4634, Sep. 2017.

[5] Y. Li, C. Tao, A. Lee Swindlehurst, A. Mezghani, and L. Liu, "Downlink achievable rate analysis in massive MIMO systems with one-bit DACs," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1669–1672, Jul. 2017.

[6] J. Xu, W. Xu, and F. Gong, "On performance of quantized transceiver in multiuser massive MIMO downlinks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 562–565, Jun. 2017.

[7] J. Xu, W. Xu, F. Gong, H. Zhang, and X. You, "Optimal multiuser loading in quantized massive MIMO under spatially correlated channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1459–1471, Feb. 2019.

[8] H. Jedda, A. Mezghani, A. L. Swindlehurst, and J. A. Nossek, "Quantized constant envelope precoding with PSK and QAM signaling," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8022–8034, Dec. 2018.

[9] E. Björnson, J. Hoydis, and L. Sanguinetti, "Massive MIMO networks: Spectral, energy, and hardware efficiency," *Found. Trends Signal Process.*, vol. 11, nos. 3–4, pp. 154–655, 2017.

[10] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 2001–2016, Mar. 2017.

[11] J. Xu, W. Xu, J. Zhu, D. W. K. Ng, and A. Lee Swindlehurst, "Secure massive MIMO communication with low-resolution DACs," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3265–3278, May 2019.

[12] D.-S. Shiu, G. J. Foschini, M. J. Gans, and J. M. Kahn, "Fading correlation and its effect on the capacity of multielement antenna systems," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 502–513, Mar. 2000.

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

[14] S. L. Loyka, "Channel capacity of MIMO architecture using the exponential correlation matrix," *IEEE Commun. Lett.*, vol. 5, no. 9, pp. 369–371, Sep. 2001.

[15] H. Lim, Y. Jang, and D. Yoon, "Bounds for eigenvalues of spatial correlation matrices with the exponential model in MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1196–1204, Feb. 2017.

[16] J. Hoydis, S. ten Brink, and M. Debbah, "Massive MIMO in the UL/DL of cellular networks: How many antennas do we need?" *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 160–171, Feb. 2013.

[17] Q. T. Zhang and D. P. Liu, "A simple capacity formula for correlated diversity Rician channels," *IEEE Commun. Lett.*, vol. 6, no. 11, pp. 481–483, Nov. 2002.