KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 9 (2023) 608–613

www.elsevier.com/locate/icte

New look at secure performance of massive MIMO with low-resolution DACs

Anh-Tu Le[a], Dinh-Thuan Do[b], Nhu-Ngoc Dao[c], Nhan Duc Nguyen[d,*], Adão Silva[e]

[a] *Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City, Viet Nam*
[b] *Department of Computer Science and Information Engineering, College of Information and Electrical Engineering, Asia University, Taichung 41354, Taiwan*
[c] *Department of Computer Science and Engineering, Sejong University, Seoul 05006, Republic of Korea*
[d] *Faculty of Mechanical-Electrical and Computer Engineering, School of Engineering and Technology, Van Lang University, 69/68 Dang Thuy Tram Street, Ward 13, Binh Thanh Dis-trict, Ho Chi Minh City, 70000, Viet Nam*
[e] *Instituto de Telecomunicações (IT), Departamento de Eletrónica, Telecomunicações e Informática (DETI), University of Aveiro, 3810-193, Aveiro, Portugal*

Received 19 January 2022; received in revised form 2 August 2022; accepted 4 September 2022
Available online 15 September 2022

Abstract

Since the requirement of secure transmission for massive multiple-input–multiple-output (mIMO) is high, we consider a secure massive MIMO system in presence of multiple digital to analog converters (DACs). We deal with complicated performance analysis of the proposed system including a base station, a legitimate user, and an eavesdropper while these nodes are equipped with multiple antennas. In particular, we intend to present the closed-form expression for the ergodic secrecy rate of the system and also calculate the optimal power allocation for better performance gain. The simulation analysis shows that quantization bits, transmit signal to noise ratio at the base station, and power allocation plays a major role in enhancing the performance of the system.

Keywords: Multiple-input–multiple-output (MIMO); Digital to analog converters (DACs); Ergodic secrecy rate; Optimal power allocation

1. Introduction

Over the years, the evolution of wireless communications has been to such an extent that users can communicate with high speed data rate and robust security [1]. In particular, to enhance the utilization of time–frequency resources and physical layer security, massive multiple-input multiple-output (MIMO) network allows simultaneous information transmissions of the destinations and transmitters which are regarded as same-frequency interference against interception by eavesdroppers [2]. There has been a lot of research on-going to analyze the performance of MIMO in various emerging technologies such as reconfigurable intelligent surfaces (RIS), unmanned aerial vehicles (UAVs), non-orthogonal multiple access (NOMA), etc.

In [3] a hybrid analog–digital architecture has been proposed for multi-user MIMO transmission in the millimeter-wave spectrum using reflect-arrays. The architecture exhibits scalability and high energy efficiency while keeping the transmitter cost-efficient. Inspired by this architecture, we design a secure multi-user hybrid analog–digital precoding scheme. In [4], the authors have proposed a massive MIMO system equipped with one-bit analog-to-digital (ADC)/ digital-to-analog (DAC). The proposed system with the proposed achievable rate expression has shown efficient power usage. The performance of the system can be enhanced compared to traditional systems by increasing the number of antennas at the sender equipment. Similarly in [5], the authors have proposed a massive MIMO with low-resolution one bit DAC in the presence of an eavesdropper. The artificial noise (AN) technique is used to improve the achievable secrecy rate of the system. A closed-form SNR-threshold expression is derived to understand whether low-res or high-res DACs are required for the efficient secrecy performance of the system. Meanwhile, in [6], the authors have suggested that usage of low-resolution DACs has shown better secrecy performance under the fixed power allocation strategy. Similarly in [7], multi-cell MIMO was considered in presence of an eavesdropper to analyze the secrecy performance of the system. AN was generated to increase the secrecy rate, but after the mathematical analysis,

* Corresponding author.
E-mail addresses: leanhtu@iuh.edu.vn (A.-T. Le), dodinhthuan@ieee.org (D.-T. Do), nndao@sejong.ac.kr (N.-N. Dao), nhan.nd@vlu.edu.vn (N.D. Nguyen), asilva@av.it.pt (A. Silva).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2022.09.004

few conditions are observed that even with AN, if there are enough antennas at the eavesdropper and enough power allocation is not given, the secure transmission may not be possible. In [8], the authors proposed a massive MIMO system that employs one-bit DAC at the base station for complexity reduction and efficient power consumption. Also, zero-forcing (ZF) precoders are utilized and asymptotic expressions for symbol error rate at each terminal are derived. It is determined that the performance of the ZF precoder mainly depends on the ratio of antennas to users.

The authors in [9] studied a precoder design in case of the imperfect location information of the unmanned aerial vehicles (UAVs) and eavesdropper. They presented the closed-form expressions of the ergodic achievable rate for two cases of conventional and the proposed precoder designs where a large number of antennas is enabled. Since it is crucial task to determine how the system satisfy the balance between the transmitted power of data and AN, the study demonstrated the optimal power splitting factor. However, it is still missing the complete analysis that how DACs affect to the system performance. In similar work, power allocation of massive MIMO is well investigated in [10] by exploiting a joint antenna selection and power allocation (JASPA) scheme. The authors presented expressions of optimization functions based on JASPA for security improvement by studying the trade-off between secrecy performance and system communications quality and recommend a quantum-inspired backtracking search algorithm (QBSA) to obtain the optimal JASPA scheme. Although a few papers developed optimal power allocation scheme [9,10], we still need to examine simpler solution and relevant approach to achieve low cost design of massive MIMO for dedicated applications, such as Internet of Things.

Since evaluating secure transmission from massive antennas at the base station to multiple antennas users is still missing, we consider a secure MIMO system that employs low-resolution DACs with the presence of a BS, legitimate user, and an eavesdropper, all consisting of multiple antennas. We first compute the expressions to identify the secrecy performance of the proposed system. Later we propose a power allocation optimization algorithm to identify its effects on the secrecy performance. The primary contributions are summarized as follows:

- We propose a massive MIMO employing multiple low-res DACs in presence of legitimate users and eavesdroppers.
- We derive the closed-form expressions for the ergodic capacity of the legitimate user and eavesdropper and then calculate the secrecy rate of each system. We compute a closed-form expression for optimal power allocation and investigate its effect on the ergodic secrecy rate.
- Finally, we perform the simulation analysis for the obtained expression in support of Monte-Carlo simulations.

The rest of the paper is organized as follows: Section 2 explains the system design and the received signals of the users present in the network. Section 3 performs the mathematical computation for obtaining the closed-form expression of ergodic secrecy rate. Section 4 performs the computation for optimal power allocation. Section 5 shows the numerical and simulation results with Section 6 proving the conclusion for the paper.

2. System model

In this paper, the system model of a secure massive MIMO employing low-resolution DACs is considered, shown in Fig. 1. The system model includes one base station (BS) with N_T antennas, one legitimate user (U) with N_R antennas and one eavesdropper (E) with N_E antennas. Further, each transmit antenna employs a pair of low-resolution DACs for processing the in-phase and quadrature signals. Specifically, the channel matrix between the BS and U is denoted as $\mathbf{H} \in \mathbb{C}^{N_R \times N_T}$, the channel matrix between the BS and E is denoted as $\mathbf{H}_E \in \mathbb{C}^{N_E \times N_T}$, the entries $\mathbf{H}$ and $\mathbf{H}_E$ are modeled as independent and identically distributed (i.i.d.) complex Gaussian random variables with zero mean and unit variance. In order to protect the confidential data from eavesdropping, the BS injects the AN into the information-bearing signals. The BS desires to transmit the symbols $\mathbf{s} \in \mathbb{C}^{N_R \times 1}$ with $\mathbb{E}\{\mathbf{s}\mathbf{s}^H\} = \mathbf{I}_{N_R}$ is precoded by a matrix $\mathbf{W} \in \mathbb{C}^{N_T \times N_R}$ with $\mathrm{tr}\{\mathbf{W}\mathbf{W}^H\} = N_R$, the AN shaping matrix $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_T - N_R})$ is multiplied by an AN shaping matrix $\mathbf{V} \in \mathbb{C}^{N_T \times (N_T - N_R)}$ with $\mathrm{tr}\{\mathbf{V}\mathbf{V}^H\} = N_T - N_R$. Then, the weighted data vector at the BS before transmission is expressed as

$$\begin{aligned}\mathbf{x} &= \sqrt{\frac{\alpha P}{N_R}}\mathbf{W}\mathbf{s} + \sqrt{\frac{(1-\alpha)\,P}{(N_T - N_R)}}\mathbf{V}\mathbf{z} \\ &= \sqrt{\beta}\mathbf{W}\mathbf{s} + \sqrt{\vartheta}\mathbf{V}\mathbf{z},\end{aligned} \tag{1}$$

where P denotes the total transmit power, $\alpha \in (0, 1]$ is a power allocation factor, $\beta = \frac{\alpha P}{N_R}$ and $\vartheta = \frac{(1-\alpha)P}{(N_T - N_R)}$. In this model, the quantized signal vector can accordingly be decomposed as

$$\mathbf{t} = \mathcal{Q}_{DA}(x) = \sqrt{1-\rho}\mathbf{x} + \mathbf{n}_{DA}, \tag{2}$$

where $\mathcal{Q}_{DA}$ is the quantization operation, $\mathbf{x}$ is the input signal, $\mathbf{n}_{DA} \sim \mathcal{CN}(\mathbf{0}, \mathbf{C}_{DA})$ is the Gaussian quantization noise, ρ is a distortion factor that depends on the DAC resolution b as [4] and

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

By substituting (1) into (3), the covariance matrix of the quantization noise is expressed as

$$\mathbf{C}_{DA} = \rho\left[\beta\mathrm{diag}\left(\mathbf{W}\mathbf{W}^H\right) + \vartheta\,\mathrm{diag}\left(\mathbf{V}\mathbf{V}^H\right)\right]. \tag{4}$$

In this paper, we consider the perfect CSI for all channels consist of user, eavesdropper and base station [7,11,12]. In addition, we consider $N_T > N_E$ and design the matrix $\mathbf{V}$ to lie in the null space of the channel matrix $\mathbf{H}$ i.e., $\mathbf{H}\mathbf{V} = \mathbf{0}$ which, in theory, renders the AN "invisible" to legitimate users [13]. Then, from (1) and (2) the signals received at the user and the eavesdropper are expressed as

$$\begin{aligned}\mathbf{y} &= \mathbf{H}\mathbf{t} + \mathbf{n} \\ &= (1-\alpha)\left(\sqrt{\beta}\mathbf{H}\mathbf{W}\mathbf{s} + \sqrt{\vartheta}\mathbf{H}\mathbf{V}\mathbf{z}\right) + \mathbf{H}\mathbf{q} + \mathbf{n},\end{aligned} \tag{5}$$

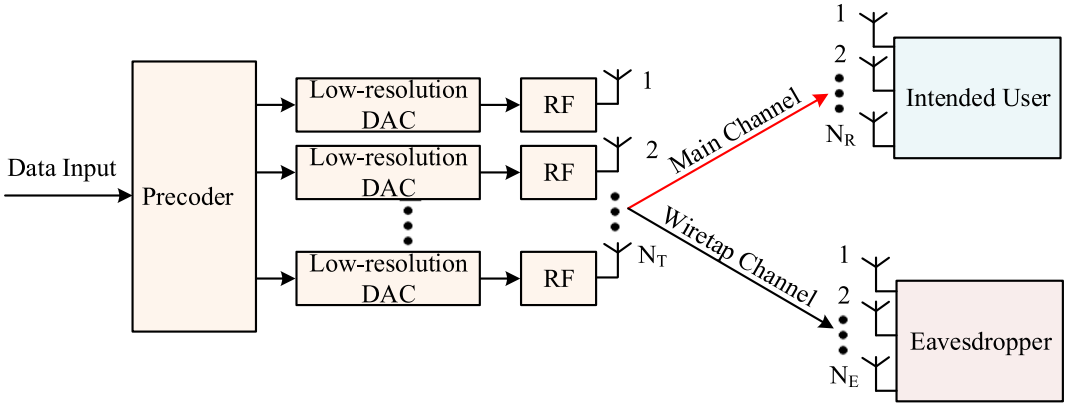

Fig. 1. System model.

and

$$\begin{aligned}\mathbf{y}_E &= \mathbf{H}_E\mathbf{t} + \mathbf{n}_E \\ &= (1-\alpha)\left(\sqrt{\beta}\mathbf{H}_E\mathbf{W}\mathbf{s} + \sqrt{\vartheta}\mathbf{H}_E\mathbf{V}\mathbf{z}\right) + \mathbf{H}_E\mathbf{q} + \mathbf{n}_E,\end{aligned} \tag{6}$$

where $\mathbf{n} \sim \mathcal{CN}(0, N_0\mathbf{I}_{N_R})$ and $\mathbf{n}_E \sim \mathcal{CN}(0, N_0\mathbf{I}_{N_E})$ are the thermal additive white Gaussian noise (AWGN) at the user and the eavesdropper respectively.

3. Achievable ergodic secrecy analysis

The achievable ergodic secrecy rate for user is given by

$$R_{\text{sec}} = \left[\bar{C}_U - \bar{C}_E\right]^+. \tag{7}$$

where $[x]^+ = \max\{0, x\}$, $\bar{C}_j (j \in \{U, E\})$ the ergodic rates of user and eavesdropper.

The lower bound on the ergodic rate for user can be written as

$$\begin{aligned}\bar{C}_U &= \mathbb{E}\left\{\log_2(1+\gamma_U)\right\} \\ &\leqslant \log_2\left(1+\mathbb{E}\{\gamma_U\}\right).\end{aligned} \tag{8}$$

From (5), the signal-to-interference-quantization-and-noise ratio (SIQNR) is given by

$$\gamma_U = \frac{(1-\rho)\,\beta\mathbf{H}\mathbf{W}\mathbf{W}^H\mathbf{H}^H}{(1-\rho)\,\vartheta\mathbf{H}\mathbf{V}\mathbf{V}^H\mathbf{H}^H + \mathbf{H}\mathbf{C}_{DA}\mathbf{H}^H + N_0\mathbf{I}_{N_R}}. \tag{9}$$

Proposition 1. *First, we denote $\eta = \frac{P}{N_0}$. Then, the asymptotic computation of the ergodic rate for user can be given by*

$$\bar{C}_U \leqslant \log_2\left(1 + \frac{(1-\rho)\,\alpha\eta\left(\frac{1}{\delta}-1\right)}{\rho\eta+1}\right). \tag{10}$$

Proof. See Appendix A.

From (6), the ergodic capacity of the eavesdropper can be evaluated as [5,6,14]

$$\bar{C}_E = E\left\{\log_2\left(1+(1-\rho)\,\beta\mathbf{W}^H\mathbf{H}_E^H\mathbf{X}^{-1}\mathbf{H}_E\mathbf{W}\right)\right\}, \tag{11}$$

where $\mathbf{X}$ is expressed by

$$\mathbf{X} = (1-\rho)\,\vartheta\mathbf{H}_E\mathbf{V}\mathbf{V}^H\mathbf{H}_E^H + \mathbf{H}\mathbf{C}_{DA}\mathbf{H}_E^H. \tag{12}$$

Proposition 2. *The ergordic capacity of the eavesdropper is given by*

$$\bar{C}_E \leqslant \log_2\left(1 + \frac{\mu\alpha\theta_1}{\delta\,(\theta_2+\theta_3)}\right), \tag{13}$$

where $\mu = \frac{N_E}{N_T}$, $\hat{\rho} = \frac{\rho}{1-\rho}$, $\theta_1 = \left(1-\alpha+\hat{\rho}\right)$, $\theta_2 = \hat{\rho}\,(1-\mu)\left(2\,(1-\alpha)+\hat{\rho}\right)$ *and* $\theta_3 = (1-\alpha)^2\left(1-\frac{\mu}{1-\delta}\right)$.

Proof. See Appendix B.

Finally, putting (10) and (13) in (7) the lower bound for the secrecy rate of the considered system is obtained as follows

$$\begin{aligned}R_{\text{sec}} &\leqslant \log_2\left(1 + \frac{(1-\rho)\,\alpha\eta\left(\frac{1}{\delta}-1\right)}{\rho\eta+1}\right) \\ &- \log_2\left(1 + \frac{\mu\alpha\theta_1}{\delta\,(\theta_2+\theta_3)}\right).\end{aligned} \tag{14}$$

4. Optimal power allocation

In this section, we investigate the impact of the power allocation factor on the ergodic secrecy rate. The derivative of R_{sec} w.r.t α can be calculated as (15) which is given in Box I, shown at the top of the next page.

Then, with small α we have $\frac{\partial R_{\text{sec}}}{\partial\alpha} > 0$ and with large α we have $\frac{\partial R_{\text{sec}}}{\partial\alpha} < 0$. Moreover, the optimal power allocation factor α^* can be achieved when we set $\frac{\partial R_{\text{sec}}}{\partial\alpha} = 0$. In addition, we assume $\mu\delta \ll 1$, which generally holds in massive MIMO networks with large antenna arrays at the BS. Then, we can rewrite (15) as

$$\begin{aligned}\frac{\partial R_{\text{sec}}}{\partial\alpha} &= \frac{\left((1-\rho)\,\eta\left(\frac{1}{\delta}-1\right)\right)}{\ln 2\left((1-\rho)\,\alpha\eta\left(\frac{1}{\delta}-1\right)+(\rho\eta+1)\right)} \\ &- \frac{\mu\,(1-\delta)}{\delta}\,\frac{\left(1+\hat{\rho}\right)}{\ln 2\left[\theta_4\theta_1^2 + \frac{\mu(1-\delta)\theta_1\alpha}{\delta}\right]}\end{aligned} \tag{16}$$

Furthermore, the closed-form expression of α^* can be calculated as follows

$$\alpha^* = \frac{\theta_4 - \sqrt{\theta_4^2 - \left(\theta_4 - \mu\left(\frac{1}{\delta}-1\right)\right)\left(\theta_4 - \frac{\mu(\rho\eta+1)}{\eta}\right)}}{(1-\rho)\left(\theta_4 - \mu\left(\frac{1}{\delta}-1\right)\right)} \tag{17}$$

$$\frac{\partial R_{\text{sec}}}{\partial \alpha} = \frac{\left((1-\rho)\,\eta\left(\frac{1}{\delta}-1\right)\right)}{\ln 2\left((1-\rho)\,\eta\left(\frac{1}{\delta}-1\right)\alpha+(\rho\eta+1)\right)} - \mu\left(\frac{1}{\delta}-1\right)\frac{(\theta_4+\delta\mu)\left(1+\hat{\rho}\right)(\theta_1)^2-\delta\mu\,(1-\alpha)^2\left(1-2\alpha+\hat{\rho}\right)-2\delta\mu\,(1-\alpha)\,\alpha\theta_1}{\ln 2\left[(\theta_4+\delta\mu)\,(\theta_1)^2-\delta\mu\,(1-\alpha)^2\right]\left[(\theta_4+\delta\mu)\,(\theta_1)^2-\delta\mu\,(1-\alpha)^2+\frac{\mu(1-\delta)}{\delta}\alpha\theta_1\right]} \tag{15}$$

Box I.

Table 1
The parameter for different quantization bits.

b	1	2	3	4	5
ρ	0.3634	0.1175	0.03454	0.009479	0.002499

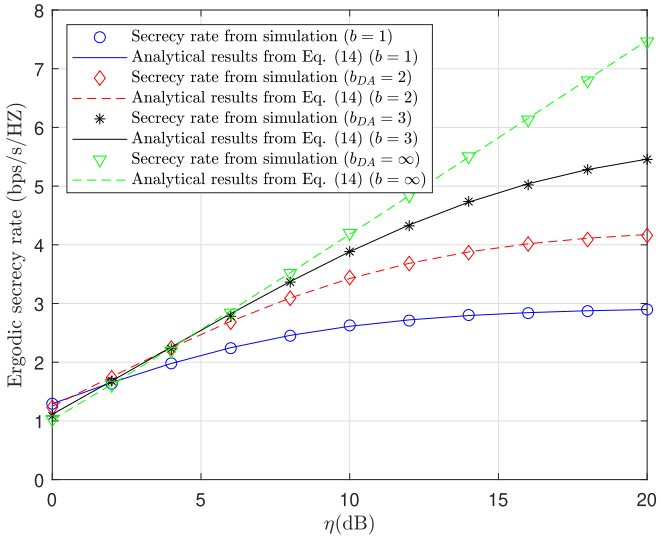

Fig. 2. Ergodic secrecy rate and analytical lower bound versus SNR.

5. Numerical results and discussions

In this section, we verify the tightness of the derived bounds and the obtained insights via numerical simulation. The parameter ρ is shown in Table 1 as [15]. We set $N_T = 100$, $N_R = 10$ and $N_E = 7$, the power allocation $\alpha = 0.8$ except for specific cases.

Fig. 2 demonstrates the simulation between ergodic secrecy rate vs transmit SNR with different quantization bits for Eq. (14). As we can observe the secrecy performance of the system is exponentially increasing for each bit increase. Also, as the transmit SNR increases, the performance gap between the curves increases. It means that for a higher number of bits, the secrecy performance of the system is rapidly increasing.

Fig. 3 shows the simulation between ergodic secrecy rate vs α for fixed transmit SNR at the BS and varying quantization bits. As we can observe, for an increase in the power level, the performance of the system increases till the point of optimal power allocation. After the optimal point, the performance curves seem to reduce, converging at a single point for the highest power allocation.

Fig. 4 illustrates the simulation between ergodic secrecy rate vs transmits SNR with optimal power allocation α^*. Comparing Fig. 2 with Fig. 4, with the introduction of α^*, there is a noticeable performance gain in the system. This

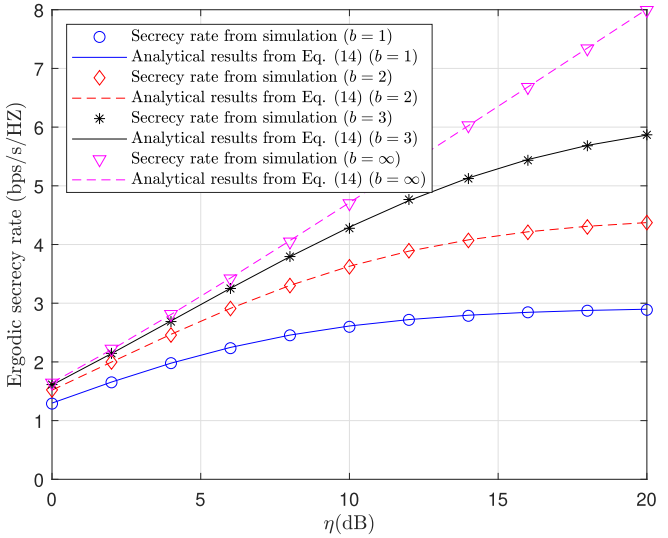

Fig. 3. Ergodic secrecy rate and analytical lower bound versus α with $\eta = 20$ dB.

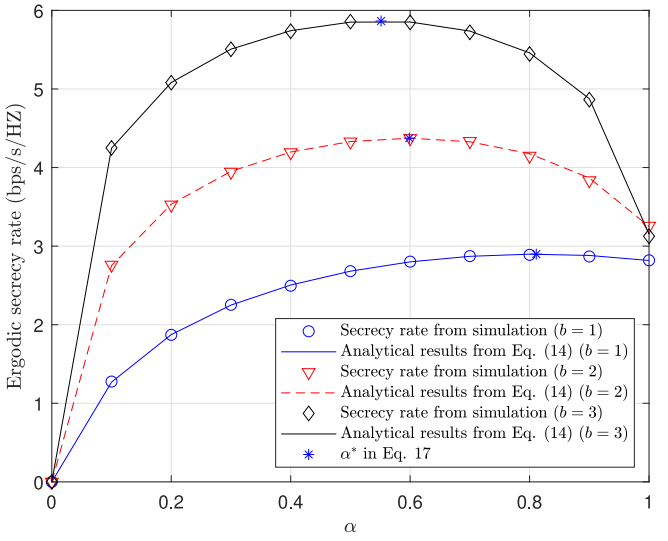

Fig. 4. Ergodic secrecy rate and analytical lower bound versus SNR with the optimal power allocation α^*.

proves that the proposed optimal power allocation strategy is efficient in enhancing the secrecy of the performance of the system.

6. Conclusion

In this paper, we have proposed a secure massive MIMO employing low-resolution DACs to characterize transmission from a BS to legitimate user and an eavesdropper, each in

presence of multiple antennas. We mainly focused on improving the secrecy performance of the proposed system by obtaining optimal power allocation for the users. We derived the closed-form expressions for achievable ergodic secrecy rate and optimal power allocation. The numerical and analytical simulations are conducted in presence of Monte-Carlo simulations, to verify the correctness of obtained expressions, for ergodic secrecy rate expressions. The simulation results show that with the increase in quantization bits, the performance of the system increases rapidly. Meanwhile, optimal power allocation plays a major role in enhancing the obtained performance as it helps in achieving approximate 0.2 times better performance than the traditional systems when the SNR at the BS is 20 dB.

CRediT authorship contribution statement

Anh-Tu Le: Methodology, Formal analysis, Writing – original draft. **Dinh-Thuan Do:** Conceptualization, Writing – review & editing, Supervision. **Nhu-Ngoc Dao:** Methodology, Supervision, Writing – original draft, Supervision. **Nhan Duc Nguyen:** Conceptualization, Writing – review & editing, Funding acquisition. **Adão Silva:** Writing – review & editing, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by the FCT/MCTES through National Funds and when applicable co-funded European Union (EU) funds under Project UIDB/50008/2020-UIDP/50008/2020. The work of Nhu-Ngoc Dao was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1G1A1008105). The work of N.D.N. was financially supported by Van Lang University, Ho Chi Minh City, Vietnam under Project 1000.

Appendix A

First, we consider a typical ZF-precoder under the constraint with $\text{tr}\{\mathbf{W}\mathbf{W}^H\}$ and we can write $\mathbf{W}$ as [5]

$$\mathbf{W} = \sqrt{\frac{N_R}{\text{tr}\left\{\left(\mathbf{H}\mathbf{H}^H\right)^{-1}\right\}}}\mathbf{H}^H\left(\mathbf{H}\mathbf{H}^H\right)^{-1}, \tag{A.1}$$

where $\mathbf{H}\mathbf{H}^H \sim W_{N_R}(N_T, \mathbf{I}_{N_R})$, where $\sim W_a(b, \Sigma)$ denotes the Wishart matrix. For, N_T and N_R go to infinity, we have [16]

$$\text{tr}\left\{\left(HH^H\right)^{-1}\right\} \overset{a.s.}{\to} \frac{\delta}{1-\delta}, \tag{A.2}$$

where $\delta = \frac{N_R}{N_T}$ and putting (A.2) into (A.1) we have

$$\mathbf{H}\mathbf{W} \overset{a.s.}{\to} \sqrt{N_R\left(\frac{1}{\delta}-1\right)}\mathbf{I}_{N_R}. \tag{A.3}$$

Next, we use the fact

$$\text{diag}\left(\mathbf{W}\mathbf{W}^H\right) \overset{a.s.}{\to} \frac{N_R}{N_T}\mathbf{I}_{N_T}, \tag{A.4}$$

and

$$\text{diag}\left(\mathbf{V}\mathbf{V}^H\right) \overset{a.s.}{\to} \frac{N_T - N_R}{N_T}\mathbf{I}_{N_T}. \tag{A.5}$$

For large N_T and N_R, with help (A.4) and (A.5), the covariance matrix $\mathbf{C}_{DA}$ converges to a scaled identity matrix as follows

$$\mathbf{C}_{DA} \to \rho\frac{P}{N_T}\mathbf{I}_{N_T}. \tag{A.6}$$

Further, we obtain the component of the quantization noise as

$$\mathbf{H}\mathbf{C}_{DA}\mathbf{H}^H \overset{a.s.}{\to} \rho P. \tag{A.7}$$

Due to the null-space AN method i.e $\mathbf{H}\mathbf{V} = \mathbf{0}$, it is obvious that

$$\mathbf{H}\mathbf{V}\mathbf{V}^H\mathbf{H}^H = 0. \tag{A.8}$$

Finally, substituting (A.3), (A.7), (A.8) into (9), the expected result can obtained. It completes the proof.

Appendix B

Putting (4) into (12), the term $\mathbf{X}$ can be expressed as

$$\mathbf{X} \overset{a.s.}{\to} \left((1-\rho)\beta + \frac{\vartheta P}{N_T}\right)\mathbf{Z}_1 + \frac{\rho P}{N_T}\mathbf{Z}_2, \tag{B.1}$$

where $\mathbf{Z}_1 = \mathbf{H}\mathbf{V}\mathbf{V}^H\mathbf{H}^H$ and $\mathbf{Z}_2 = \mathbf{H}\begin{bmatrix}\mathbf{V} & \mathbf{V}_0\end{bmatrix}\begin{bmatrix}\mathbf{V} & \mathbf{V}_0\end{bmatrix}^H\mathbf{H}^H$. It is obvious that $\begin{bmatrix}\mathbf{V} & \mathbf{V}_0\end{bmatrix}\begin{bmatrix}\mathbf{V} & \mathbf{V}_0\end{bmatrix}^H = \mathbf{I}_{N_E}$, where $\begin{bmatrix}\mathbf{V} & \mathbf{V}_0\end{bmatrix}$ is a complete orthogonal basis. Moreover, $\mathbf{X}$ is statistically equivalent to a weighted sum of two scaled Wishart matrices, i.e, $\mathbf{Z}_1 \sim W_{N_E}(N_T - N_R, \mathbf{I}_{N_E})$ and $\mathbf{Z}_2 \sim W_{N_E}(N_R, \mathbf{I}_{N_E})$. Strictly speaking, X is not a Wishart matrix and the exact distribution of X is intractable. However, X may be accurately approximated as a single scaled Wishart matrix, $\mathbf{X} \sim \mathbf{W}_{N_E}\left(\kappa, \varpi\mathbf{I}_{N_E}\right)$ where κ and ϖ are chosen such that the first two moments of $\mathbf{X}$ and $[(1-\rho)\beta + \frac{\rho P}{N_T}]\mathbf{Z}_1 + \frac{\rho P}{N_T}\mathbf{Z}_2$ are identical [7], which yields

$$\kappa\varpi = (N_T - N_E)\left[(1-\rho)\beta + \frac{\rho P}{N_T}\right] + \frac{N_E\rho P}{N_T}, \tag{B.2}$$

and

$$\kappa\varpi^2 = (N_T - N_E)\left[(1-\rho)\beta + \frac{\rho P}{N_T}\right]^2 + N_E\left(\frac{\rho P}{N_T}\right)^2. \tag{B.3}$$

After some variable substitutions and manipulations, we can obtain κ and ϖ as

$$\kappa = \frac{N_T\left\{(1-\rho)(1-\alpha)+\rho\right\}^2}{\left\{(1-\rho)(1-\alpha)+\rho\right\}^2 + (1-\rho)^2(1-\alpha)^2\frac{N_E}{N_T-N_E}}, \tag{B.4}$$

and

$$\varpi = \frac{P}{N_T}\frac{\left\{(1-\rho)(1-\alpha)+\rho\right\}^2 + (1-\rho)^2(1-\alpha)^2\frac{N_E}{N_T-N_E}}{(1-\rho)(1-\alpha)+\rho}. \tag{B.5}$$

Then, we can further obtain as $\mathbf{X}^{-} \overset{a.s.}{\to} 1/(\varpi(\kappa - N_E))\mathbf{I}_{N_E}$ with $\kappa > N_E$ for a Wishart matrix $\mathbf{A} \sim W_m(n, \mathbf{I}_m)$ with $m > n$ [8]. Then, due to central limit Theorem we have the fact $\frac{1}{N_E}\mathbf{H}_E^H\mathbf{H}_E - \mathbf{I}_{N_T} \overset{a.s.}{\to} 0_{N_T}$. In addition, applies the weak law of large numbers we have $\mathbb{E}\{\mathbf{W}^H\mathbf{W}\} = 1$. Substituting (B.4) and (B.5) into (11), we obtain expected result.

The proof is completed.

References

[1] B. Ji, Y. Li, D. Cao, C. Li, S. Mumtaz, D. Wang, Secrecy performance analysis of UAV assisted relay transmission for cognitive network with energy harvesting, IEEE Trans. Veh. Technol. 69 (7) (2020) 7404–7415.

[2] H. Gao, Y. Su, S. Zhang, Y. Hou, M. Jo, Joint antenna selection and power allocation for secure co-time co-frequency full-duplex massive MIMO systems, IEEE Trans. Veh. Technol. 70 (1) (2021)) 655–665.

[3] S. Asaad, R.F. Schaefer, H. Vincent Poor, Hybrid precoding for secure transmission in reflect-array-assisted massive MIMO systems, in: ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, 2020, pp. 8693–8697.

[4] Y. Li, C. Tao, A. Lee Swindlehurst, A. Mezghani, L. Liu, Downlink achievable rate analysis in massive MIMO systems with one-bit DACs, IEEE Commun. Lett. 21 (7) (2017) 1669–1672.

[5] J. Xu, W. Xu, J. Zhu, D.W.K. Ng, A. Lee Swindlehurst, Secure massive MIMO communication with low-resolution DACs, IEEE Trans. Commun. 67 (5) (2019) 3265–3278.

[6] D. Yang, J. Xu, W. Xu, N. Wang, B. Sheng, A.L. Swindlehurst, Secure communication for spatially correlated massive MIMO with low-resolution DACs, IEEE Wirel. Commun. Lett. 10 (10) (2021) 2120–2124.

[7] J. Zhu, R. Schober, V.K. Bhargava, Secure transmission in multicell massive MIMO systems, IEEE Trans. Wireless Commun. 13 (9) (2014) 4766–4781.

[8] A.K. Saxena, I. Fijalkow, A.L. Swindlehurst, Analysis of one-bit quantized precoding for the multiuser massive MIMO downlink, IEEE Trans. Signal Process. 65 (17) (2017) 4624–4634.

[9] S.J. Maeng, Y. Yapıcı, İ. Güvenç, A. Bhuyan, H. Dai, Precoder design for physical-layer security and authentication in massive MIMO UAV communications, IEEE Trans. Veh. Technol. 71 (3) (2022) 2949–2964.

[10] H. Gao, Y. Su, S. Zhang, Y. Hou, M. Jo, Joint antenna selection and power allocation for secure co-time co-frequency full-duplex massive MIMO systems, IEEE Trans. Veh. Technol. 70 (1) (2021) 655–665.

[11] C. Lu, W. Xu, H. Shen, J. Zhu, K. Wang, MIMO channel information feedback using deep recurrent network, IEEE Commun. Lett. 23 (1) (2019) 188–191.

[12] H. Xie, F. Gao, S. Jin, An overview of low-rank channel estimation for massive MIMO systems, IEEE Access 4 (2016) 7313–7321.

[13] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun. 7 (6) (2008) 2180–2189.

[14] A. Goldsmith, S. Jafar, N. Jindal, S. Vishwanath, Capacity limits of MIMO channels, IEEE J. Sel. Areas Commun. 21 (5) (2003) 684–702.

[15] J. Max, Quantizing for minimum distortion, IRE Trans. Inf. Theory 6 (1) (1960) 7–12.

[16] A.M. Tulino, S. Verdú, et al., Random matrix theory and wireless communications, Found. Trends® Commun. Inf. Theory 1 (1) (2004) 1–182.