Downlink Secrecy Rate of One-Bit Massive MIMO System with Active Eavesdropping

M. A. Teeti

***Abstract*—In this study, we consider the physical-layer security in the downlink of a Massive MIMO system employing one-bit quantization at the base station. We assume an active eavesdropper that attempts to spoiling the channel estimation acquisition at the BS for a legitimate user, whereas overhearing on downlink transmission. We consider the two most widespread methods for degrading the eavesdropper's channel, the nullspace artificial noise (NS-AN) and random artificial noise (R-AN). Then, we present a lowerbound on the secrecy rate and asymptotic performance, considering zero-forcing beamforming (ZF-BF) and maximum-ratio transmission beamforming (MRT-BF). Our results reveal that even when the eavesdropper is close enough to the intercepted user, a positive secrecy rate is possible–which increases as the number of BS antennas N is increased until it saturates–as long as the transmit power of eavesdropper is less than that of the legitimate user during channel training. We show that ZF-BF with NS-AN provides the best performance. Interestingly, it is shown that when the BS's power is fixed, MRT-BF and ZF-BF are asymptotically equivalent and hence the artificial noise technique is the performance indicator. In contrast, in an energy-efficient Massive MIMO system with the total BS's power is reduced proportional to $1/N$, the performance is independent of artificial noise asymptotically and hence the beamforming technique is the performance indicator. In addition, when BS's power is reduced proportional to $1/\sqrt{N}$, all combinations of beamforming and artificial noise schemes are equally likely asymptotically, independent of quantization noise. We present various numerical results to corroborate our analysis.**

***Index Terms*—Massive MIMO, physical layer security, active eavesdropping, ergodic information leakage, one-bit quantization**

I. Introduction

Information secrecy in Massive multiple-input multiple-output (MIMO) system—as a key technology for fifth-generation networks—has been a critical issue that spurred widespread interest [1], [2], [3], [4], [5], [6]. One challenge in Massive MIMO lies in the increase in hardware complexity and energy consumption [7] due to the large number of antennas at the base station (BS). In recent years, there has been a growing interest in replacing the high-resolution analog-to-digital converters (ADCs) and digital-to-analog converters (DACs) with low-resolution ADCs and DACs. The extreme case of 1-bit ADC/DAC has been gaining much attention [8], [9], [10], [11] because of the considerable design simplicity offered to the physical layer and negligible energy consumption. With this in mind, it is of interest to understand the secrecy capability of Massive MIMO employing one-bit quantization, which is the aim of this work.

M. Teeti is with School of Information Engineering, East China University of Technology, Nanchang, 330013, China (e-mail: teeti.moh@gmail.com)

In a major advance in 1949, Claude Shannon [12] established the information-theoretic basis of communication secrecy of cryptographic systems. In classical security, the transmitter often shields the private message by a means of shared-key cryptographic techniques carried out at the logical layers of the network. Typically, the encryption key is very long and computationally demanding. In addition, it is susceptible to interception by powerful adversaries, especially in a wireless environment. Consequently, key sharing becomes infeasible in dynamic wireless networks with nodes of limited resources. To tackle this problem, physical-layer security provides an alternative or a complement to classical cryptography, which exploits the statistical differences between the channel of the legitimate receiver and that of the eavesdropper to guarantee secrecy.

The first information-theoretic approach to physical-layer security dates back to Wyner's work [13] on the degraded Gaussian wiretap channel. Later, Csiszar and Korner [14] generalized Wyner's work to the non-degraded wiretap channel. In the preceding works of Wyner, Csiszar, and Korner, it was shown that when the channel of the legitimate receiver is more capable (less noisy) than that of the eavesdropper, secure communication is possible with no need for classical cryptography. The maximal rate at which the transmitter and legitimate receiver can communicate securely is limited by the *secrecy capacity*, defined as the maximal of the difference between the channel mutual information of the legitimate receiver and that of the eavesdropper.

In the literature, *passive attack* refers to the situation where an eavesdropper is concealing himself and thus only eavesdropping on the confidential transmission. On the other hand, *active attack* refers to the situation where an eavesdropper is not only eavesdropping on the confidential transmission but also jamming the transmission. In the literature, many attempts have been made [1], [15], [16], [6], [17] to study the impact of passive attack in Massive MIMO systems under different scenarios. One common thing among most of the above works and others in the literature is the use of *artificial noise* to degrade the eavesdropper channel [5] and hence improve security. Most of the above works focus on a careful design of data beamforming (or precoding) and artificial noise. In the literature, two artificial noise techniques are widely used, the nullspace artificial noise (NS-AN) and random artificial noise (R-AN) [5]. With NS-AN, the artificial noise is made aligned with the nullspace of the channel of the intended user while with the R-AN, the artificial noise is generated randomly.

Stemming from the fact that meeting physical-layer security in the information-theoretic sense gives rise to a significant loss in data rate, Bin Chen et al., [3] consider a cryptographic-

like scheme to achieve security in Massive MIMO system in the presence of a powerful eavesdropper. In [3], the message symbols are randomly phase rotated while this phase rotation is only available at the legitimate receiver through downlink training with a small amount of overhead. There, it is shown that when the BS is equipped with a sufficiently large number of antennas; we guarantee secure communication with high probability.

It is well-known that the promising gains of Massive MIMO systems [18], [19], [20] are affected by *pilot contamination* [21], whether resulting from pilot reuse [21] in multi-cellular networks or *pilot attack* [22], [23], [4] created intentionally by an active eavesdropper. In fact, the pilot attack can cause serious degradation of the secrecy rate since the beam-formed signal in the downlink will be partly aligned with the direction of eavesdropper's channel, thus increasing the information leakage. This situation becomes more pronounced when the pilot attack is severe, under which no positive secrecy rate is possible. Many attempts [24], [25], [26], [27], [28] with the purpose of detecting and combating pilot attack in Massive MIMO have been done. Yuksel et al., [24] showed that pilot attack can be eliminated asymptotically as the size of the pilot set (which is assumed known to everyone) is increased as long as users select their pilots randomly. Q. Xiong et al., [25] propose an efficient energy-based detector to identify a pilot attack without the knowledge of the channel state information (CSI). T. T. Do et al., [26] consider a single-user uplink Massive MIMO and study two anti-jamming strategies based on pilot re-transmission and pilot adaptation technique. R. F. Schaefer et al., [28] consider a single-cell Massive MIMO with a single-antenna eavesdropper and use artificial noise technique. Hence, the achievable secrecy rate is investigated and power-ratio based pilot attack detection is suggested. There, it is shown that secrecy rate can drop to zero as the power of eavesdropper is increased. Tan et al., [27] consider pilot jamming in the uplink and propose jamming-resistant approach using unused pilot and pilot hopping to estimate the jamming channel. With zero-forcing type receiver, it is shown in [27] that we can greatly enhance the robustness of the massive MIMO uplink against jamming attacks.

In multicell multiuser Massive MIMO systems, Wu et al., [23] consider an active eavesdropper armed with multiple antennas, and present signal design using beamforming based on maximum-ratio transmission and NS-AN technique under correlated channel. They show that the NS-AN can enjoy the highly correlated channels, enabling secure communication; however, this is not the case when the channel is weakly correlated or independent and identically distributed (i.i.d.). To overcome the limitation in [23], the authors in [29] consider pilot-data exploitation for CSI acquisition. They show that decreasing the legitimate user's power render its received signal lie in a different eigenspace as that of the eavesdropper in the asymptotic limit of data length, thus mitigating the effect of a strong pilot attack. We refer the interested readers to [30] and relevant references thereof for a recent review of the literature on physical layer security in 5G networks.

Using low-resolution ADCs/DACs at the BS in Massive MIMO can substantially simplify the physical layer and reduce energy consumption, particularly when the one-bit quantization is considered. A related challenge is the design of the channel estimator and the precoder [31], [32] which turns to be not trivial as the quantization can break the structure of the beamforming matrix. This challenge can exacerbate when a pilot attack is present in the system. In [33] the design of artificial noise is investigated in a simple scenario of a multiple-antenna system under the constraint of a few RF chains at the BS, considering a passive eavesdropper and perfect CSI at the BS. The impact of hardware impairment (such as phase noise and amplified receiver noise) on secrecy in massive MIMO is studied in [34] and hence both the uplink training and the design of artificial noise are optimized to enhance secrecy under a passive eavesdropper. More recently, a low-resolution Massive MIMO system with multiple-antenna passive eavesdropper is studied in [35]. With perfect CSI assumed available at the BS, it is shown that quantization noise gives rise to the increase in secrecy rate.

The main limitation of the previous studies on the secrecy of Massive MIMO system with quantization or limited RF chains at the BS is the focus on passive attack scenarios with the assumption of perfect CSI at the BS. As far as quantization is concerned, the assumption of perfect CSI becomes inaccurate even in the absence of pilot contamination. Particularly, the perfect CSI is unjustified when the extreme 1-bit quantization case is considered. Even greater importance is the impact of active eavesdropping on secrecy in quantized Massive MIMO systems, which is not well understood in the literature. In this work, we will particularly study the one-bit quantized Massive MIMO system with an active eavesdropper, and investigate its secrecy performance under various beamforming and artificial noise techniques.

A. Contributions

We summarize the main contributions of this work as follows:

1) We derive a lower bound on secrecy rate under various beamforming and artificial noise scheme, and asymptotic performance analysis (when the number of BS antennas $N \to \infty$) is given.
2) We show analytically (as $N \to \infty$) a threshold on the transmit power ratio between the eavesdropper and intercepted user below which a positive secrecy rate is possible. As a result, when the eavesdropper is near enough to the intercepted user, secure communication turns to be difficult (if not impossible) when the transmit ratio is close to 1. This result is confirmed by simulation of a practical scenario.
3) We show that when the power at the BS is fixed, the NS-AN technique outperforms R-AN technique, regardless of beamforming technique as $N \to \infty$.
4) We show that in an energy-efficient Massive MIMO system with power reduced proportional to $1/N$, the zero-forcing beamforming (ZF-BF) outperforms maximum-ratio transmission beamforming (MRT-BF), regardless of artificial noise. Further, when the power is reduced proportional to $1/\sqrt{N}$ all schemes are asymptotically equivalent and quantization noise is irrelevant.

B. Paper outline

We organize the rest of the paper as follows. Section II introduces signal models in uplink and downlink and we discuss channel estimation. Section III presents the design of downlink beamforming and artificial noise. Also, we show the analysis of information rates and main results. In Section IV we present the asymptotic performance comparison and the condition under which secure communication is possible is given. In Section V we present some numerical examples to verify our analytical results and Section VI concludes this work.

II. Signal Model and Channel Estimation

We consider the downlink of a single-cell Massive MIMO system with 1-bit ADCs/DACs employed at the BS. The BS is assumed equipped with N antennas which serves $K \ll N$ single-antenna users in the same time-frequency resource block. We assume the communication system operates in the time-division duplex (TDD). A single-antenna active eavesdropper is assumed that attacks only one legitimate user by contaminating its CSI acquisition at the BS during channel training and overhearing on the downlink transmission.

We consider Rayleigh block-fading for both BS-users and BS-eavesdropper channels with coherence time T_c. Within each block the channel remains constant over T_c symbol intervals and changes independently from one block to another. The composite BS-users' small-scale fading channel is denoted by $H = [\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_K] \in \mathcal{C}^{N\times K}$ and $\boldsymbol{g} \in \mathcal{C}^{N\times 1}$ denotes the BS-eavesdropper's small-scale fading channel. Both H and $\boldsymbol{g}$ comprise i.i.d. complex Gaussian random variables, each with zero-mean and unit variance. The (n, j)-th element of H, denoted h_{nj}, represents the channel between the n-th BS antenna and user j, whereas g_n denotes the n-th component of $\boldsymbol{g}$. Further, we denote by β_j & β_e the large-scale fading coefficients associated with legitimate user j and eavesdropper, respectively. We assume all large-scale fading coefficients changes slowly in order of several T_c intervals and hence assumed available to everyone. Since we are interested in downlink rate, we divide the coherence time into two parts for training (over τ symbol intervals) and downlink transmission (over $T_c - \tau$ symbol intervals).

A. Uplink signal model

At the start of communication, all legitimate users in the system send mutually orthogonal pilot sequences, each of length τ, in the uplink for channel estimation at the BS, whereas the eavesdropper concurrently transmits the same pilot sequence of user k (intercepted user) to impair its channel acquisition at the BS. We denote by $\Psi = [\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \cdots, \boldsymbol{\psi}_K]^T \in \mathcal{CN}^{K\times\tau}$ the pilot matrix satisfying $\Psi\Psi^H = \tau I_K$, where $\boldsymbol{\psi}_j = [\psi_j(1), \psi_j(2), \cdots, \psi_j(\tau)]^T$ is the pilot sequence of user j. For simplicity of analysis, there is no loss of generality in assuming unit-modulus pilot symbols, i.e., $|\psi_j(t)|^2 = 1$.

Thus, the discrete-time received signal at the BS during τ symbol intervals can be written as

$$Y = \sum_{j=1}^{K} \sqrt{p'_j}\boldsymbol{h}_j\boldsymbol{\psi}_j^T + \sqrt{p'_e}\boldsymbol{g}\boldsymbol{\psi}_k^T + Z \tag{1}$$

where p'_j and p'_e are the average received power at the BS from user j and eavesdropper, respectively, i.e.,

$$p'_j = \beta_j p_j \tag{2a}$$

$$p'_e = \beta_e p_e \tag{2b}$$

where p_j and p_e are the average transmit powers of user j and eavesdropper, respectively. The matrix $Z \in \mathcal{CN}^{N\times\tau}$ denotes a complex additive white Gaussian noise (AWGN) with i.i.d. $\mathcal{CN}(0, 1)$ components. Since the rows of Y (corresponding to BS antenna n) are i.i.d., hence we focus on an arbitrary row n. Hence, the (n, t)-th entry of Y is

$$y_n(t) = \sum_{j=1}^{K} \sqrt{p'_j}h_{nj}\psi_j(t) + \sqrt{p'_e}g_n\psi_k(t) + z_n(t). \tag{3}$$

Then, the signal after the one-bit quantizer (1-bit ADC) attached to the n-th BS antenna is expressed as

$$v_n(t) = \text{sign}(y_n(t)) \tag{4}$$

where $\text{sign}(\cdot)$ is the sign function which yields the sign of the real and imaginary parts of $y_n(t)$ independently. Here we assume a zero-threshold quantizer. Accordingly, the constellation of the quantized signal corresponds to the quadrature phase-shift keying constellation, i.e., $\mathcal{A} = \frac{1}{\sqrt{2}}\{1 + j, 1 - j, -1 + j, -1 - j\}$.

Since $y_n(t)$ is complex Gaussian random variable, it holds from the Bussgang theorem [36] that we can express $v_n(t)$ as a sum of a scaled version of $y_n(t)$ and an uncorrelated term (quantization noise), i.e.,

$$\begin{aligned} v_n(t) &= \gamma y_n(t) + q_n(t) \\ &= \sum_{j=1}^{K} \sqrt{\gamma^2 p'_j}h_{nj}\psi_j(t) + \sqrt{\gamma^2 p'_e}g_n\psi_k(t) \\ &\quad + \gamma z_n(t) + q_n(t) \end{aligned} \tag{5}$$

where γ is a scaling factor and $q_n(t)$ is the quantization noise. From (5), γ is obtained by the linear minimum mean squared error (LMMSE) solution, i.e., $\gamma = E[y_n^*(t)v_n(t)]/\sigma_y^2$. From [36], $E[y_n^*(t)v_n(t)] = \sqrt{2\sigma_y^2/\pi}$, where σ_y^2 is the variance of $y_n(t)$. Hence,

$$\gamma := \sqrt{\frac{2/\pi}{\sigma_y^2}} = \sqrt{\frac{2/\pi}{\sum_{j=1}^{K} p'_j + p'_e + 1}} \tag{6}$$

and the variance of quantization noise is thus given by

$$\begin{aligned} \sigma_q^2 &= E[|v_n(t)|^2] - \gamma^2 E[|y_n(t)|] \\ &= 1 - 2/\pi \approx 0.3634. \end{aligned} \tag{7}$$

At two time instants t and t', the covariance between $y_n(t)$ and $y_n(t')$ can be generally expressed as

$$\begin{aligned} C(t, t') &= \sum_{j=1}^{K} p'_j\psi_j^*(t)\psi_j(t') + p'_e\psi_k^*(t)\psi_k(t') \\ &\quad + E[z_n^*(t)z_n(t')]. \end{aligned} \tag{8}$$

When $t \neq t'$, we have $C(t, t') = \sum_{j=1}^{K} p'_j\psi_j^*(t)\psi_j(t') + p'_e\psi_k^*(t)\psi_k(t')$, i.e., the signal is generally correlated in the

time domain. When $t' = t$, we have $C(t,t) = \sigma_y^2 = \sum_{j=1}^{K} p_j' + p_e' + 1$. However, when K is sufficiently large—which is the case in Massive MIMO systems—the condition $\sigma_y^2 \gg C(t,t')$, $t \neq t'$, is satisfied due to the sum of a large number of cross terms in (8). Therefore, signals received at different time instants can be approximately assumed uncorrelated. As a result, given the number of users is sufficiently large we can safely assume the quantization noise uncorrelated (with zero-mean and variance σ_q^2). We point out here that this assumption will have a negligible effect on the results in this paper. Finally, without loss of generality, in this work we assume $\tau = K \gg 1$.

B. Channel estimation

The BS correlates (5) with the pilot symbols of user l to estimate h_{nl}. Hence,

$$\begin{aligned}\tilde{v}_l &:= \frac{1}{\sqrt{\tau}} \sum_{t=1}^{\tau} \psi_k^*(t) v_n(t) \\ &= \sqrt{\gamma^2 \tau p_l'} h_{nl} + \sqrt{\gamma^2 \tau p_e'} g_n \delta(l-k) + \gamma \tilde{z}_l + \tilde{q}_l \end{aligned} \quad (9)$$

where $\tilde{z}_l$ and $\tilde{q}_l$ are zero-mean scalar random variables with variances 1 and σ_q^2, respectively.

Using (9) the LMMSE estimate of h_{nl} reads

$$\hat{h}_{nl} = \frac{\gamma \sqrt{p_l' \tau}}{\gamma^2 p_l' \tau + \gamma^2 p_e' \tau \delta(l-k) + \gamma^2 + \sigma_q^2} \tilde{v}_l := \lambda_l \tilde{v}_l \quad (10)$$

and therefore the variance of $\hat{h}_l$ is

$$\sigma_{\hat{h}_l}^2 = \frac{\gamma^2 p_l' \tau}{\gamma^2 p_l' \tau + \gamma^2 p_e' \tau \delta(l-k) + \gamma^2 + \sigma_q^2}. \quad (11)$$

Stacking all channel estimates in a matrix form, the composite channel estimate, denoted $\hat{H}$, can be written as

$$\hat{H} = V \Psi^H \Lambda / \sqrt{\tau} \quad (12)$$

where $\Lambda = \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_K) \in \mathcal{R}^{K \times K}$ is a diagonal matrix and $V \in \mathcal{CN}^{N \times \tau}$ is the quantized signal corresponding to Y, where the (n,t)-th entry of V is defined in (4). Finally, we remark that the channel estimates $\hat{h}_{nl}$ are treated as i.i.d. $\mathcal{CN}(0, \sigma_{\hat{h}_l}^2)$, thanks to the law of large numbers. This follows from the fact that $\tilde{v}_l$ is typically comprised of a sum of a large number of random variables.

C. Downlink signal model

Over one symbol interval, the BS synthesizes the following signal vector (precoded signal):

$$\tilde{\boldsymbol{x}} = \sqrt{\frac{\theta}{\eta}} W \boldsymbol{s} + \sqrt{\frac{\bar{\theta}}{\zeta}} r. \quad (13)$$

After the one-bit quantizers (1-bit DACs) at the BS, the discrete-time transmitted signal is

$$\boldsymbol{x} = \sqrt{\frac{p_d}{N}} \, \mathrm{sign}(\tilde{\boldsymbol{x}}) \quad (14)$$

where $\boldsymbol{s} = [s_1, s_2, \cdots, s_K]^T$ comprises K independent complex Gaussian symbols (normalized), $W = [\boldsymbol{w}_1, \boldsymbol{w}_2, \cdots, \boldsymbol{w}_K] \in \mathbb{C}^{N \times K}$ is the precoding (or beamforming) matrix with $\boldsymbol{w}_i$ being the i-th column of W, and $r = [r_1, r_2, \cdots, r_N]^T \in \mathbb{C}^N$ is a zero-mean artificial noise vector generated deliberately to weaken the eavesdropper's channel. We assume $\eta E[\mathrm{tr}(WW^H)] = \zeta E[\|r\|^2] = 1$ where η, ζ are long-term normalization constants. Further, $\theta \in (0,1)$ and $\bar{\theta} = 1 - \theta$ are power fractions allocated to the beamformed signal and artificial noise, respectively. Consequently, we have $E[\|\tilde{\boldsymbol{x}}\|^2] = 1$. From (13), the scaling factor $\sqrt{p_d/N}$ is introduced to restrict the average power at the BS to p_d.

Since $\tilde{\boldsymbol{x}}$ is a unit norm vector and we consider the channel matrix H drawn from random Gaussian matrix ensembles, the variance of each component of $\tilde{\boldsymbol{x}}$, (13) turns to be $\sigma_{\tilde{x}}^2 = 1/N$. From [36], we can express (14) as

$$\begin{aligned}\boldsymbol{x} &= \sqrt{\frac{p_d}{N}} (\bar{\gamma} \tilde{\boldsymbol{x}} + \bar{\boldsymbol{q}}) = \sqrt{\frac{\theta \bar{\gamma}^2 p_d}{N \eta}} W \boldsymbol{s} + \sqrt{\frac{\bar{\theta} \bar{\gamma}^2 p_d}{N \zeta}} r + \sqrt{\frac{p_d}{N}} \bar{\boldsymbol{q}} \\ &= \sqrt{\frac{2\theta p_d}{\pi \eta}} W \boldsymbol{s} + \sqrt{\frac{2\bar{\theta} p_d}{\pi \zeta}} r + \sqrt{\frac{p_d}{N}} \bar{\boldsymbol{q}} \end{aligned} \quad (15)$$

where $\bar{\gamma}$ is a scaling factor follows from the Bussgang theorem as discussed previously, which is given by

$$\bar{\gamma} := \sqrt{2/\pi/\sigma_{\tilde{x}}^2} = \sqrt{2N/\pi}. \quad (16)$$

For simplicity of notation, we express (15) as

$$\boldsymbol{x} = c_1 W \boldsymbol{s} + c_2 r + c_3 \bar{\boldsymbol{q}} \quad (17)$$

where c_1, c_2 and c_3 are, respectively defined by

$$c_1 = \sqrt{2\theta p_d / \pi \eta} \quad (18a)$$

$$c_2 = \sqrt{2\bar{\theta} p_d / \pi \zeta} \quad (18b)$$

$$c_3 = \sqrt{p_d / N}. \quad (18c)$$

III. Secrecy capacity analysis

In this section, we establish the achievable rate $\underline{R}_k$ of the intercepted user k, and an upper-bound on the eavesdropper's rate $\overline{R}_e$. We use the underline and overline notation to distinguish between a lowerbound and upperbound, respectively. Then the secrecy rate $\underline{R}_s$ is given by [14]

$$\underline{R}_s = \left[\underline{R}_k - \overline{R}_e\right]^+ \quad (19)$$

where $[A]^+ = A$ when $A > 0$ and $[A]^+ = 0$ when $A < 0$.

A. Data beamforming and artificial noise

In this work, we intend no effort to optimize the structure of the beamforming matrix, thus we will consider two classical beamforming techniques; the maximum ratio transmission beamforming (MRT-BF) and zero-forcing beamforming (ZF-BF). Using the channel estimate at the BS, W is thus given by

$$W := \begin{cases} \hat{H}^* & \text{if MRT-BF,} \\ \hat{H}^* (\hat{H}^T \hat{H}^*)^{-1} & \text{if ZF-BF.} \end{cases} \quad (20)$$

The normalization constant η can be evaluated as follows. Let $\hat{H} = \tilde{H} \Sigma^{1/2}$ where $\tilde{H}$ is a random Gaussian matrix with

i.i.d. $\mathcal{CN}(0,1)$ components, and Σ is a diagonal matrix whose diagonal elements comprise the vector $[\sigma^2_{\hat{h}_1}, \sigma^2_{\hat{h}_2}, \cdots, \sigma^2_{\hat{h}_K}]$. Thus, when MRT-BF is used we have that

$$\begin{aligned}\eta_{\text{mrt}} &= E[\text{tr}(W_{\text{mrt}}W_{\text{mrt}}^H)] = E[\text{tr}(\Sigma^{1/2}\tilde{H}^T\tilde{H}^*\Sigma^{1/2})] \\ &= \text{tr}(\Sigma^{1/2}E[\tilde{H}^T\tilde{H}^*]\Sigma^{1/2}) = N\,\text{tr}(\Sigma) \end{aligned} \tag{21}$$

and when ZF is used, we can write

$$\begin{aligned}\eta_{\text{zf}} &= E[\text{tr}(W_{\text{zf}}^H W_{\text{zf}})] = E[\text{tr}(\Sigma^{-1/2}(\tilde{H}^T\tilde{H}^*)^{-1}\Sigma^{-1/2})] \\ &= \text{tr}(\Sigma^{-1/2}E[(\tilde{H}^T\tilde{H}^*)^{-1}]\Sigma^{-1/2}) = \frac{\text{tr}(\Sigma^{-1})}{N-K} \end{aligned} \tag{22}$$

where in (22) we have used $E[(\tilde{H}^T\tilde{H}^*)^{-1}] = (N-K)^{-1}I_K$, which follows from the property of the inverse of central Wishart matrix $\tilde{H}^T\tilde{H}^*$ [37].

The artificial noise vector r in (13) is defined by

$$\boldsymbol{n} = S\tilde{\boldsymbol{n}} \tag{23}$$

where S is a shaping matrix and $\tilde{\boldsymbol{n}}$ is an $N \times 1$ Gaussian vector with i.i.d. $\mathcal{CN}(0,1)$ components. We study R-AN and NS-AN in which $\boldsymbol{n} \in \text{nullspace}(\hat{H}^T)$. In the R-AN approach, we let $S = I_N$, thus $\boldsymbol{n} = \tilde{\boldsymbol{n}}$. When NS-AN is used, we let S be the orthogonal complement matrix of $\hat{H}^T$, given by $S = I_N - \hat{H}^*(\hat{H}^T\hat{H}^*)^{-1}\hat{H}^T$. Thus we can summarize:

$$S \coloneqq \begin{cases} I_N & \text{if R-AN,} \\ I_N - \hat{H}^*(\hat{H}^T\hat{H}^*)^{-1}\hat{H}^T & \text{if NS-AN.} \end{cases} \tag{24}$$

From (23) and (24), it follows easily that the respective normalization constants corresponding to R-AN and NS-AN are given by

$$\zeta_{\text{r-an}} = N \tag{25}$$

$$\zeta_{\text{ns-an}} = N - K. \tag{26}$$

B. Data rates analysis

The received signal at the intercepted user k is

$$\begin{aligned} r_k = &\sqrt{\beta_k c_1^2}\boldsymbol{h}_k^T\boldsymbol{w}_k s_k + \sum_{j=1, j\neq k}^{K}\sqrt{\beta_k c_1^2}\boldsymbol{h}_k^T\boldsymbol{w}_j s_j \\ &+ \sqrt{\beta_k c_2^2}\boldsymbol{h}_k^T S\tilde{\boldsymbol{n}} + \sqrt{\beta_k c_3^2}\boldsymbol{h}_k^T\bar{\boldsymbol{q}} + \nu_k \end{aligned} \tag{27}$$

and the eavesdropper receives

$$\begin{aligned} r_e = &\sqrt{\beta_e c_1^2}\boldsymbol{g}^T\boldsymbol{w}_k s_k + \sum_{j=1, j\neq k}^{K}\sqrt{\beta_e c_1^2}\boldsymbol{g}^T\boldsymbol{w}_j s_j \\ &+ \sqrt{\beta_e c_2^2}\boldsymbol{g}^T S\tilde{\boldsymbol{n}} + \sqrt{\beta_e c_3^2}\boldsymbol{g}^T\bar{\boldsymbol{q}} + \nu_e \end{aligned} \tag{28}$$

where both $\nu_k, \nu_e \sim \mathcal{CN}(0,1)$, denoting the Gaussian noises at the intercepted user and eavesdropper, respectively.

To obtain a lower bound on secrecy rate, we shall make two main assumptions that have been considered in the literature, serving as a worst-case scenario. First, to obtain a lowerbound on rate achievable by the legitimate use we assume the legitimate user has no access to its channel realization and its beamforming vector, and thus the user utilizes only its knowledge of the long-term statistics of the channel for decoding. Second, to obtain an upperbound on information leakage we assume the eavesdropper has access to its channel realizations and the beamforming vector of intercepted user. Further, we assume that the eavesdropper can cancel out all inter-user interference, which is conceivable through a collusion of other users with the eavesdropper.

Therefore, after ignoring the second term in (28), we rewrite (28) as

$$r_e = \sqrt{\beta_e c_1^2}\boldsymbol{g}^T\boldsymbol{w}_k s_k + \sqrt{\beta_e c_2^2}\boldsymbol{g}^T S\tilde{\boldsymbol{n}} + \sqrt{\beta_e c_3^2}\boldsymbol{g}^T\bar{\boldsymbol{q}} + \nu_e \tag{29}$$

and hence the information rate leaked to the eavesdropper is given by[1]

$$\overline{R}_e = E\left[\log\left(1 + c_1^2\beta_e\boldsymbol{w}_k^H\boldsymbol{g}^* C_e^{-1}\boldsymbol{g}^T\boldsymbol{w}_k\right)\right] \tag{30}$$

where C_e is the covariance matrix of the effective noise seen by the eavesdropper, given by

$$C_e = c_2^2\beta_e\boldsymbol{g}^T S\boldsymbol{g}^* + c_3^2\beta_e\sigma_q^2\boldsymbol{g}^T\boldsymbol{g}^* + 1. \tag{31}$$

Since (30) is hard to compute, we resort to a simple upper bound, which proves to be a very good approximation as shown by numerical results in Sec. V.

Next, we express (27) as

$$r_k = a s_k + n_{\text{eff}} \tag{32}$$

where a is a constant which depends on the statistics of the channel and n_{eff} is an effective noise which is uncorrelated with s_k. It follows easily that a is given by

$$a \coloneqq E[s_k^* r_k] = c_1\sqrt{\beta_k}E[\boldsymbol{h}_k^T\boldsymbol{w}_k] \tag{33}$$

where we have used the fact that all four terms in (27) are mutually uncorrelated. The variance of n_{eff} is thus

$$\begin{aligned} \sigma^2_{n_{\text{eff}}} &= E[|r_k|^2] - |a|^2 \\ &= c_1^2\beta_k\,\text{Var}(\boldsymbol{h}_k^T\boldsymbol{w}_k) + \sum_{j=1, j\neq k}^{K} c_1^2\beta_k E[|\boldsymbol{h}_k^T\boldsymbol{w}_j|^2] \\ &\quad + c_2^2\beta_k E[\boldsymbol{h}_k^T S\boldsymbol{h}_k^*] + \beta_k\sigma_q^2 p_d + 1. \end{aligned} \tag{34}$$

where $\text{Var}(\cdot)$ is the variance operator. In (34) we have used the fact that $SS^H = S$ for both R-AN and NS-AN schemes.

By treating the non-Gaussian noise n_{eff} as Gaussian noise with the same variance (i.e., information-theoretic worst case), therefore the achievable rate of the intercepted user k is

$$\underline{R}_k = \log\left(1 + |a|^2/\sigma^2_{n_{\text{eff}}}\right). \tag{35}$$

C. Mutual information between intercepted user's channel and eavesdropper's channel

Because of pilot attack, the estimated channel of legitimate user k will contain information about the channel of eavesdropper. Here, we characterize this information which turns to be useful in our analysis of the main results.

[1] In (30) we have treated the quantization noise in the downlink as Gaussian, which is a technical assumption. By the law of large numbers, $\boldsymbol{g}^T\bar{\boldsymbol{q}}$ (third term in (29)) can be very well approximated as a Gaussian random variable for a sufficiently large N.

Lemma 1. *The eavesdropper's channel vector can be expressed as*

$$\boldsymbol{g} = \sqrt{\kappa_R}\hat{\boldsymbol{h}}_k + \boldsymbol{\epsilon} \tag{36}$$

where κ_R is the received power ratio between the eavesdropper and intercepted user k, i.e.,

$$\kappa_R = \frac{p'_e}{p'_k} = \frac{\beta_e p_e}{\beta_k p_k} := \frac{\beta_e}{\beta_k}\kappa_T \tag{37}$$

and $\boldsymbol{\epsilon}$ is uncorrelated Gaussian (approximately) error vector with covariance matrix given by

$$C_{\boldsymbol{\epsilon}} = (1 - \kappa_R \sigma^2_{\hat{h}_k}) I_N \tag{38}$$

Proof. The proof is straightforward which follows from the classical work on MMSE solution. Appendix A presents the details. □

Although Lemma 1 is a straightforward result, however, it is noteworthy. It can tell us how much information about the eavesdropper's channel $\boldsymbol{g}$ is contained in the channel estimate $\hat{\boldsymbol{h}}_k$. From (38), one can show that the mutual information $I(\boldsymbol{g}; \hat{\boldsymbol{h}}_k) = h(\boldsymbol{g}) - h(\boldsymbol{g}|\hat{\boldsymbol{h}}_k)$ is given by

$$I(\boldsymbol{g}; \hat{\boldsymbol{h}}_k) = N \log\left(\frac{1}{1 - \kappa_R \sigma^2_{\hat{h}_k}}\right) \geq 0. \tag{39}$$

Equation (39) indicates that $I(\boldsymbol{g}; \hat{\boldsymbol{h}}_k)$ can grow large and will be limited only by AWGN and quantization noise when $\kappa_R \gg 1$. Note that $\kappa_R \sigma^2_{\hat{h}_k} < 1$. Since in particular the nullspace noise is a function of $\hat{\boldsymbol{h}}_k$(which is correlated with $\boldsymbol{g}$), it follows that part of this noise resides in the nullspace of the eavesdropper's channel. Thus part of the nullspace noise will be annihilated at the eavesdropper, giving rise to an increase in his information rate which leads to a significant reduction of the secrecy rate.

D. Main results

Here, we give a lowerboud on the achievable secrecy rate under different beamforming and artifical noise techniques. In the following, all derived information rates are given in their normalized form[2].

We state our findings in the following two theorems.

Theorem 1. *Consider a one-bit quantized Massive MIMO system with N antennas at the BS and K single-antenna users in the presence of a single-antenna active eavesdropper. If the BS uses MRT-BF, then the achievable downlink rate $\underline{R}_k$ of the intercepted user k, is given by*

$$\underline{R}_k^{\text{MRT}} \geq \log\left(1 + \frac{2\theta\pi^{-1}\,\text{tr}^{-1}(\Sigma)\beta_k \sigma^4_{\hat{h}_k} p_d N}{2\theta\beta_k p_d/\pi + P_k^{AN} + \beta_k \sigma_q^2 p_d + 1}\right). \tag{40}$$

Further, if the BS uses ZF-BF, then $\underline{R}_k$ is given by

$$\underline{R}_k^{\text{ZF}} \geq \log\left(1 + \frac{2\theta\pi^{-1}\,\text{tr}^{-1}(\Sigma^{-1})\beta_k p_d (N-K)}{2\theta\beta_k p_d(1-\sigma^2_{\hat{h}_k})/\pi + P_k^{AN} + \beta_k \sigma_q^2 p_d + 1}\right) \tag{41}$$

[2]The normalization factor is $(1 - \tau/T_c)$, i.e., the fraction of time over which downlink transmission is considered in this work.

where P^{AN} is the effective artificial noise power given by

$$P_k^{\text{AN}} = \begin{cases} 2\bar{\theta}\beta_k p_d/\pi & \textit{if R-AN} \\ 2\bar{\theta}\beta_k p_d(1-\sigma^2_{\hat{h}_k})/\pi & \textit{if NS-AN.} \end{cases} \tag{42}$$

Proof. See Appendix B. □

Theorem 2. *Consider the system model in Theorem 1. When N is sufficiently large, the average information leaked to the eavesdropper is upper-bounded (equal or approximate) by*

$$\overline{R}_e^{\text{MRT}} \lesssim \log\left(1 + \frac{2\theta\beta_e p_d \sigma^2_{\hat{h}_k}\left(\kappa_R \sigma^2_{\hat{h}_k} N + 1\right)}{\pi\,\text{tr}(\Sigma)(P_e^{\text{AN}} + \beta_e p_d \sigma_q^2 + 1)}\right) \tag{43}$$

when the BS uses MRT-BF, and when the BS uses ZF-BF,

$$\overline{R}_e^{\text{ZF}} \lesssim \log\left(1 + \frac{2\theta\beta_e p_d\left(\kappa_R(N-K-1) + \sigma^{-2}_{\hat{h}_k}\right)}{\pi\,\text{tr}(\Sigma^{-1})(P_e^{\text{AN}} + \beta_e p_d \sigma_q^2 + 1)}\right) \tag{44}$$

where κ_R is defined in (37) *and P_e^{AN} is the power of artificial noise seen at the eavesdropper defined by*

$$P_e^{\text{AN}} = \begin{cases} 2\bar{\theta}\beta_e p_d/\pi & \text{if R-AN} \\ 2\bar{\theta}\beta_e p_d(1-\kappa_R\sigma^2_{\hat{h}_k})/\pi & \text{if NS-AN.} \end{cases} \tag{45}$$

Proof. See Appendix C □

It is clear from Theorem 1 and Theorem 2 that the rate of intercepted user and information rate of eavesdropper are always greater when the BS uses the NS-AN than R-AN, which is clear from (42) and (45), respectively.

From the preceding results, the achievable secrecy rate is

$$\underline{R}_s^{\text{MRT}} = \left[\underline{R}_k^{\text{MRT}} - \overline{R}_e^{\text{MRT}}\right]^+ \tag{46}$$

$$\underline{R}_s^{\text{ZF}} = \left[\underline{R}_k^{\text{ZF}} - \overline{R}_e^{\text{ZF}}\right]^+ \tag{47}$$

The expressions in (46) and (47) can be further maximized with respect to the power fraction θ by setting the first derivative of the rate difference to zero and solving the resulting equation for $\theta \in (0, 1)$. Due to the long expressions of θ in terms of all other system parameters, we omit them and hence computed numerically instead. We leave it to the reader to verify that when all parameters are fixed, the optimal policy is to allocate almost all power to artificial noise in the asymptotic limit of N.

We remark that the results in Theorems 1 & 2 can be specialized for the no-quantization case (infinite-resolution ADCs/DACs) by replacing p_d with $p_d\pi/2$ and setting $\sigma_q^2 = 0$ in (40)- (45), setting $\gamma = 1, \sigma_q^2 = 0$ in (11) and redefining Σ accordingly.

IV. Asymptotic Performance comparison

Inspecting Theorems 1 & 2 provides no clear clue of how the performance of MRT-BF and ZF-BF can be compared. Therefore, a better understanding of the performance gap can be gained through asymptotic performance. Our focus here will be on the asymptotic behavior of the beamforming/artificial noise schemes as the number of BS antennas

increases with no limit. As shown next, the asymptotic performance renders it easy to capture the important parameters for a specific scheme to guarantee a positive secrecy rate, which turns to be even very useful for the non-asymptotic case.

In the following, we assume $N \to \infty$. Since energy-efficient (EE) Massive MIMO system is of great importance, hence we study the asymptotic behavior of the secrecy rate under such a system.

A. Non-energy-efficient Massive MIMO system

Here, we assume that the total power at the BS is fixed, irrelevant to the number of BS antennas. In the following, we state our results in the following corollary to Theorems 1 &2.

Corollary 1. *Assume the BS uses MRT-BF or ZF-BF. Then when R-AN is used, the maximum secrecy rate converges to*

$$R_{s,\text{R-AN}}^{\text{no-EE}} \to \log\left[\left(\frac{\beta_k\left(p_d\beta_e\left(\pi\sigma_q^2+2\right)+\pi\right)}{\kappa_R\beta_e(p_d\beta_k\left(\pi\sigma_q^2+2\right)+\pi)}\right)\right]^+ \tag{48}$$

and when NS-AN is used, the maximum secrecy rate converges to

$$R_{s,\text{NS-AN}}^{\text{no-EE}} \to \left[\log\left(\frac{\beta_k\left(p_d\beta_e\left(\pi\sigma_q^2+2-2\kappa_R\sigma_{\hat{h}_k}^2\right)+\pi\right)}{\kappa_R\beta_e\left(p_d\beta_k\left(\pi\sigma_q^2+2-2\sigma_{\hat{h}_k}^2\right)+\pi\right)}\right)\right]^+ \tag{49}$$

asymptotically as $N \to \infty$.

The expressions (48) and (49) unfold by maximizing the asymptotic limit of $\underline{R}_k^{\text{MRT}} - \overline{R}_e^{\text{MRT}}$ regarding θ as $N \to \infty$. It turns out that the optimal θ converges to 0 asymptotically, i.e., almost all power is allocated to artificial noise asymptotically. From 48 and 49, a positive secrecy rate is possible if the transmit power ratio (during channel training) between the eavesdropper and intercepted user satisfies

$$\kappa_T = \frac{p_e}{p_k} < 1 + \underbrace{\frac{\pi\beta_k\left(\beta_k-\beta_e\right)}{\left(p_d\beta_k\left(\pi\sigma_q^2+2\right)+\pi\right)\beta_e^2}}_{\Delta\beta}. \tag{50}$$

Further, since (48) and (49) are positive under the same condition (50), we have that

$$\Delta^{\text{no-EE}} = R_{s,\text{NS-AN}}^{\text{no-EE}} - R_{s,\text{R-AN}}^{\text{no-EE}} > 0 \tag{51}$$

We summarize our conclusions from Corollary 1 as follows:

1) The NS-AN outperforms R-AN asymptotically, independent of the beamforming technique.
2) Using R-AN entails more BS antennas to achieve the same performance of NS-AN.
3) Both NS-AN and R-AN are useless when (50) is violated.

B. Energy-efficient Massive MIMO system

Here, we assume an energy-efficient (EE) massive MIMO system, where the total power at the BS can be reduced proportional to $1/\sqrt{N}$ or $1/N$. In the sequel, we use EE1 and EE2 for a Massive MIMO system with power reduced proportional to $1/\sqrt{N}$ or $1/N$, respectively. Hence,

$$p_d = \begin{cases} \rho/\sqrt{N} & \text{if EE1,} \\ \rho/N & \text{if EE2} \end{cases} \tag{52}$$

where ρ is a fixed value (predetermined at the BS).

We state our results in the following two corollaries.

Corollary 2. *Consider an energy-efficient one-bit Massive MIMO with active eavesdropper with power at the BS is proportional to* $1/\sqrt{N}$. *If the BS uses MRT-BF or ZF-BF, then the maximum secrecy rate converges to*

$$R_s^{\text{EE1}} \to \left[\log\left(\frac{\beta_k}{\kappa_R\beta_e}\right)\right]^+. \tag{53}$$

irrespective of the artificial noise scheme.

Corollary 3. *Consider an energy-efficient one-bit Massive MIMO with active eavesdropper with power at the BS is proportional to* $1/N$. *If the BS uses MRT-BF with R-AN or NS-AN, then the maximum secrecy rate converges to*

$$R_s^{\text{EE2, MRT}} \to \left[\log\left(\frac{\pi\,\text{tr}(\Sigma)+2\beta_k\sigma_{\hat{h}_k}^4\rho}{\pi\,\text{tr}(\Sigma)+2\beta_e\sigma_{\hat{h}_k}^4\kappa_R\rho}\right)\right]^+ \tag{54}$$

and when ZF-BF with R-AN or NS-AN is used, then the maximum secrecy rate converges to

$$R_s^{\text{EE2, ZF}} \to \left[\log\left(\frac{\pi\,\text{tr}(\Sigma^{-1})+2\beta_k\rho}{\pi\,\text{tr}(\Sigma^{-1})+2\beta_e\kappa_R\rho}\right)\right]^+ \tag{55}$$

By inspection of Corollaries 2 & 3 we can observe that a positive secrecy rate is possible if the transmit power ratio satisfies

$$\kappa_T < \left(\frac{\beta_k}{\beta_e}\right)^2. \tag{56}$$

This means that the transmit power ratio during the pilot attack plays a central role in impacting the secrecy rate. Since (54) and (55) are both positive under the same condition (56), thus it is easy to show that

$$\Delta^{\text{EE2}} = R_s^{\text{EE2, ZF}} - R_s^{\text{EE2, MRT}} > 0 \tag{57}$$

asymptotically.

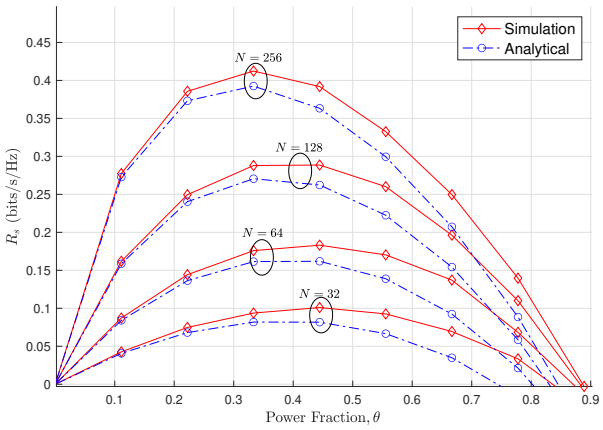
We summarize our conclusions from Corollaries 2 & 3 as follows:

1) When EE regime is considered, the performance is independent of artificial noise, contrary to no-EE regime.
2) Under EE1, MRT-BF and ZF-BF are equivalent while under EE2 regime, ZF-BF outperforms MRT-BF, asymptotically.
3) With EE regime, the asymptotic secrecy rate drops to zero when (56) is violated.

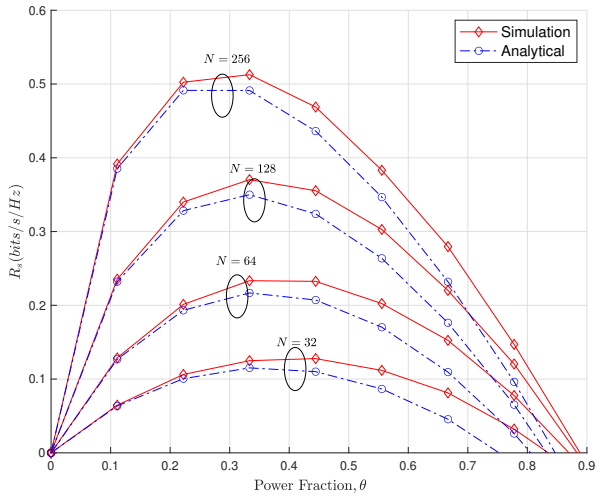
Finally, we remark again that the results in Corollaries 1–3 can be specialized for the no-quantization case (infinite-resolution ADCs/DACs) by replacing p_d with $p_d\pi/2$ and setting $\sigma_q^2 = 0$ in (40)- (45), setting $\gamma = 1, \sigma_q^2 = 0$ in (11) and redefining Σ accordingly.

V. Numerical Results and Discussion

In this section, we present some numerical results to verify the analytical results in this work. We consider a single-cell Massive MIMO system with K single-antenna users and an active eavesdropper. Without loss of generality, we assume $\beta_1 = \cdots \beta_K = \beta_e = 1$ and all legitimate users transmit at the same power, i.e., $p_1 = p_2 = \cdots = p_k = p_u$. Unless otherwise stated, analytical results refer to the achievable secrecy rate using Theorems 1 & 2 and Corollaries 1-3 whereas simulation results refer to simulated achievable secrecy rate evaluated by Monte Carlo simulation with quantization-noise correlation and exact ergodic information rate leakage (30) are accounted.



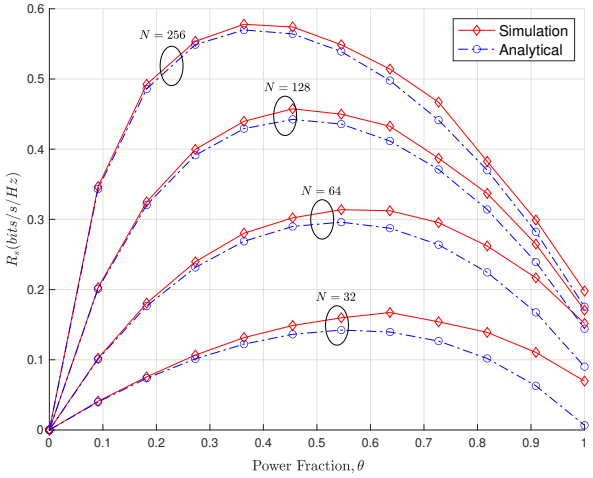
(a) MRT-BF with R-AN



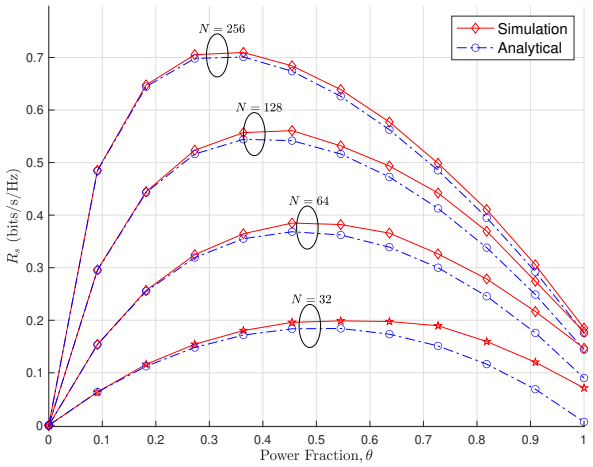
(b) MRT-BF with NS-AN

Fig. 1: Achievable secrecy rate under MRT-BF with (a) R-AN and (b) NS-AN, $K = 10, \tau = K, p_u = p_d = 10$dB and $p_e = 5$dB.

Fig. 1 shows the performance of MRT-BF for different number of BS antennas. The eavesdropper's power is set to $p_e = p_u/2 = 5$dB. We can observe that the analytical results serve as a good lowerbound on secrecy rate compared with the simulated lowerbound. We can observe that the NS-AN (Fig. 1(b)) always outperforms R-AN (Fig. 1(a)). For example, when $N = 256$, the performance gap between NS-AN and R-AN is about 0.1 bits/s/Hz.



(a) ZF-BF with R-AN



(b) ZF-BF with NS-AN

Fig. 2: Achievable secrecy rate under ZF-BF with (a) R-AN and (b) NS-AN, $K = 10, \tau = K, p_u = p_d = 10$dB and $p_e = 5$dB.

The performance of ZF-BF is shown in Fig. 2. As seen, a relatively smaller gap (compared with MRT-BF) between the simulated and analytical results. This is partly because the user rate improves under ZF-BF and hence this improvement will render the gap, resulting from our approximation error and the use of Jensen's inequality, smaller, i.e., see Appendix C. Similar to the case of MRT-BF, the NS-AN provides higher rates compared wit R-AN. Further, it is clear that ZF-BF with NS-AN achieves the highest secrecy while MRT-BF with R-AN provides the lowest secrecy rate, where the gap between them is about 0.3 bits/s/Hz when $N = 256$.

Also, we observe that in all simulated cases in Figs 1 & 2, the secrecy rate increases as the number of BS antennas N increases, while the power fraction allocated to signal is monotonically decreasing. As N increases, both the inter-

cepted user's rate and information leakage increase, thus in order to maintain a positive secrecy rate, more power should be allocated to artificial noise to degrade the eavesdropper channel.

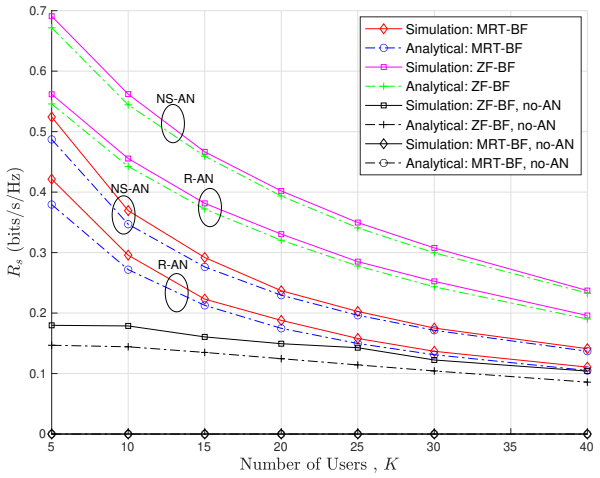


Fig. 3: The impact of number of users on secrecy rate under ZF-BF and MRT-BF, $N = 128$, $\tau = K$, $p_u = p_d = 10$dB and $p_e = 5$dB.

Fig. 3 depicts the impact of increasing the number of users on the secrecy rate. As seen, the secrecy rate decreases steadily as the number of users increases. This, in particular, follows from the increases of inter-user interference (in case of MRT-BF) and the reduction in the array gain (in case of ZF-BF), thus reducing the rate of the intercepted user. As observed previously, ZF-BF with NS-AN provides a higher secrecy rate, albeit at the price of high computational burden when compared with MRT-BF combined with R-AN.

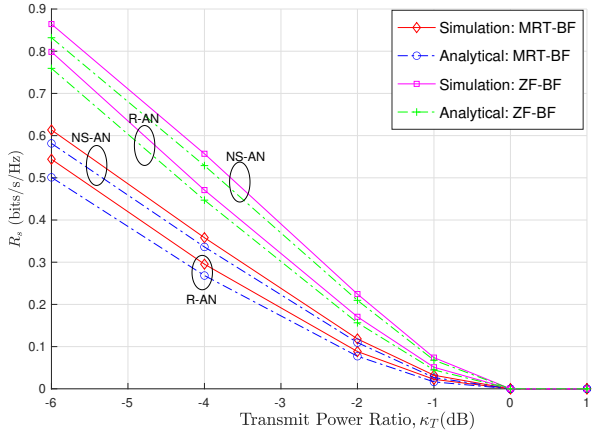


Fig. 4: The impact of transmit power ratio $\kappa_T = p_e/p_u$, during pilot attack, on secrecy rate, $N = 64$, $K = 10, \tau = K$, and $p_u = p_d = 10$dB.

The effect of transmit power ratio $\kappa_T = p_e/p_u$ during pilot attack is illustrated in Fig. 4. In all beamforming and artificial noise schemes we observe that the secrecy rate is steadily reduced as κ_T increases. In general, ZF-BF with NS-AN outperforms other schemes as observed previously. However, secrecy rate drops to zero for all schemes when κ_T approaches 1 (0dB). This is in line with the asymptotic condition derived in (50). From (50), $\kappa_T < 1$ due to $\beta_k = \beta_e = 1$ in our simulation. Thus without an advanced communication secrecy protocol, active eavesdropping can be deleterious to the secrecy rate.

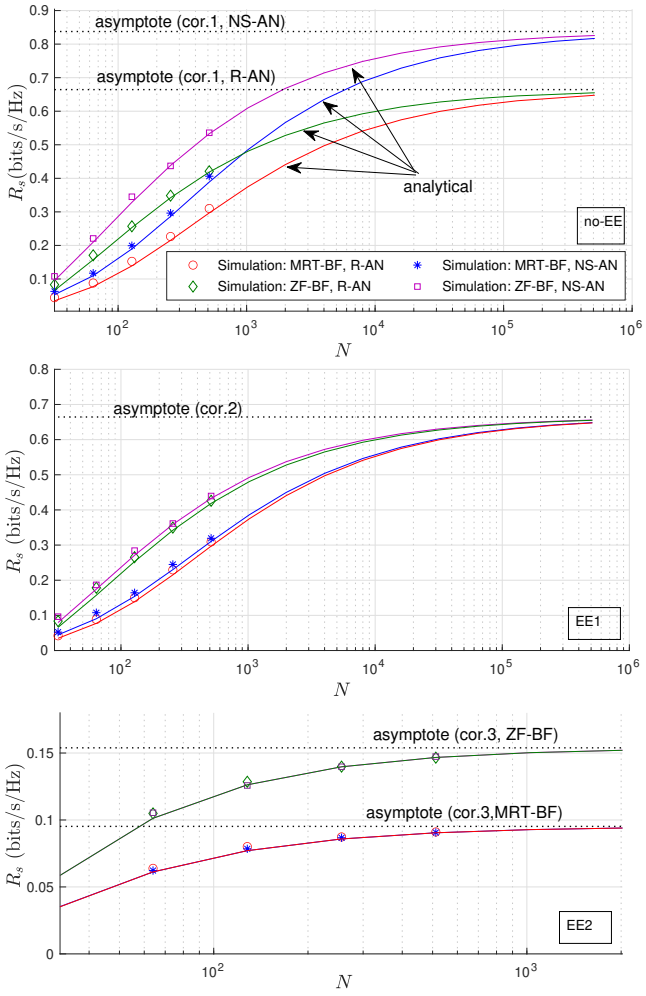


Fig. 5: Asymptotic secrecy rate under no-EE (top figure), EE1 (middle figure) and EE2 (bottom figure). The number of user is $K = 10, \tau = K$, and $p_u = 10$dB, $\rho = 10$ dB and $\kappa_T = -2$dB. ($p_d = \rho/\sqrt{N}$). Markers, solid lines and dotted lines represent simulated, analytical and asymptotic results, respectively.

Fig. 5 illustrates the asymptotic behavior of the secrecy rate as $N \to \infty$. As seen, when the power at the BS is kept fixed regardless of the number of BS antennas (Fig. 5(top), no-EE), both MRT-BF and ZF-BF are asymptotically equivalent. As N gets larger and larger, almost all power is allocated to artificial noise asymptotically, thus the artificial noise dominates (determines) the performance asymptotically. We can observe that under no-EE case, NS-AN outperforms R-AN. When the BS's power is scaled down by N (Fig. 5(bottom), EE2), almost all power should be allocated to data to maintain a positive secrecy rate as $N \to \infty$, rendering both R-AN and NS-AN

equivalent asymptotically, and hence the beamforming scheme determines the performance. When the power scales down with $\sqrt{N}$ (Fig. 5(middle), EE1), any combinations of beamforming and artificial noise schemes are asymptotically equivalent. The reader will observe the very large number of BS antennas for the no-EE and EE1 cases to converges to the corresponding asymptotic values, compared with EE2 case which converges at much faster pace.

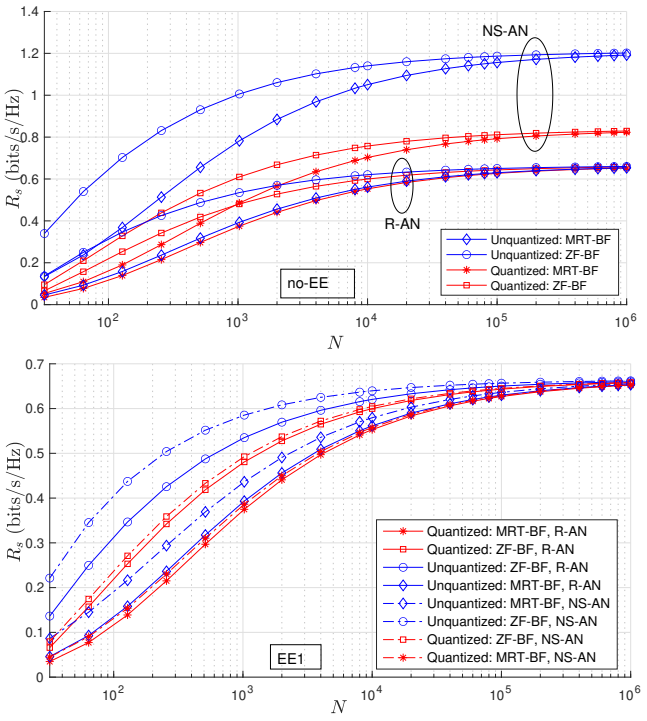


Fig. 6: Secrecy gap between quantized and unquantized systems under no-EE ($p_d = \rho$) and EE1 ($p_d = \rho/\sqrt{N}$) regimes, $K = 10$ users, $\tau = K$, and $p_u = \rho = 10$dB, and $\kappa_T = -2$dB.

Fig. 6 shows the performance gap between the quantized system and its unquantized (i.e., infinite-resolution ADCs/DACs) version under no-EE and EE1 regimes. The analytical results for the no-quantization case are obtained from our analysis as a special case as discussed previously. For the no-EE case, we observe a comparably larger gap when NS-AN is used whereas it is smaller when R-AN is used, especially under MRT-BF. Thus when the combination of MRT-BF and R-AN is considered, there is not much loss in secrecy rate because of quantization noise. We also observe that both quantized and unquantized systems are asymptotically equivalent under R-AN. This implies that the R-AN dominates the quantization noise, whereas the quantization noise dominates the NS-AN in the asymptotic limit. For EE1 regime, the gap diminishes asymptotically under all schemes and hence quantization noise is irrelevant. For the case of EE2 which is not shown here, one can verify that the secrecy rate for the unquantized case converges to different asymptotic limits for ZF-BF and MRT-BF where the artificial noise scheme is asymptotically irrelevant.

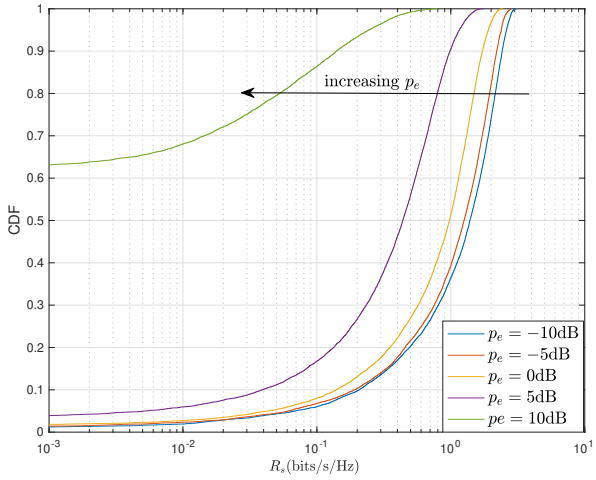


Fig. 7: CDF of secrecy rate for (ZF-BF, NS-AN)-scheme. The BS is assumed in a center of a circle of radius 1km and the eavesdropper in a circle of radius 100m around the intercepted user and all users' positions are uniformly distributed. The number of BS antennas $N = 128$, $K = 10$ users, $\tau = K$ and $p_d = p_u = 10$dB .

Fig. 7 depicts the cumulative distribution function (CDF) of the secrecy rate when the BS employs ZF-BF and NS-AN, where this scheme is chosen due to its high performance as we have shown before. We assume the BS is positioned in the center of a circle of radius 1km while the active eavesdropper in a circle of radius 100m around the intercepted user, i.e., this captures the situation when the eavesdropper is very close to the intercepted user. The positions of users are assumed random and uniformly distributed inside the circular cell. As seen in Fig. 7 the average secrecy rate decreases with increasing the power of eavesdropper. When the eavesdropper transmits at the same power level of the legitimate user the average secrecy drops to zero. This again confirms our analysis and the transmit power-ratio threshold given in (50) even in this non asymptotic case.

VI. Conclusion

This paper has investigated the secrecy in the downlink of a Massive MIMO system under the presence of an active eavesdropper and when the signal at the BS undergoes 1-bit quantization. We investigated the efficacy of two artificial noise techniques; NS-AN and R-AN. Thus, we have derived the achievable secrecy rate when the BS uses MRT-BF and ZF-BF. Although the very coarse quantization and pilot attack, secure communication is possible, where the best performance is achieved when ZF-BF is combined with NS-AN. In fact, we showed analytically that when the eavesdropper is sufficiently close to the intercepted user, the average secrecy rate drops to zero as the transmit power ratio between the eavesdropper and intercepted user approaches 1. The practical scenario examined in the paper has further corroborated our analysis.

It was shown that when the number of BS antennas N grows large, the performance is independent of the beamforming

technique and hence the NS-AN should be exploited to maximize the performance. This observation has an implication for research into other possible schemes of artificial noise to degrade the channel of eavesdropper. Further, it was shown that the total power at the BS can be reduced proportional to $1/N$ or $1/\sqrt{N}$ while a positive secrecy rate is maintained, given the ratio between the eavesdropper's power and intercepted use's power is less than $(\beta_k/\beta_e)^2$. This observation suggests considering other approaches other than artificial noise to enhance secrecy.

Due to the scope limitation of this work, a number of potential issues needs to be considered in the future, such as power control and optimal design of beamforming. We believe our findings add to the understanding of the impact of active eavesdropping in quantized Massive MIMO systems.

APPENDIX A
PROOF OF LEMMA 1

From (12), we can write

$$\hat{\boldsymbol{h}}_k = \lambda_k \left(\sqrt{\gamma^2 p'_k \tau} \boldsymbol{h}_k + \sqrt{\gamma^2 p'_e \tau} \boldsymbol{g} + \gamma \tilde{\boldsymbol{z}} + \tilde{\boldsymbol{q}} \right). \tag{58}$$

where $\tilde{\boldsymbol{z}}$ and $\tilde{\boldsymbol{q}}$ are the AWGN and quantization noise vector. Thus, given $\hat{\boldsymbol{h}}_k$, the LMMSE solution for $\boldsymbol{g}$ is

$$\hat{\boldsymbol{g}} = E\left[\boldsymbol{g}\hat{\boldsymbol{h}}_k^H\right] \left(E[\hat{\boldsymbol{h}}_k \hat{\boldsymbol{h}}_k^H]\right)^{-1} \hat{\boldsymbol{h}}_k \tag{59}$$

From (58) we have

$$E[\boldsymbol{g}\hat{\boldsymbol{h}}_k^H] = \sqrt{\lambda_k^2 \gamma^2 p'_e \tau} I_N \tag{60a}$$

$$E[\hat{\boldsymbol{h}}_k \hat{\boldsymbol{h}}_k^H] = \lambda_k^2 (\gamma^2 p'_k \tau + \gamma^2 p'_e \tau + \gamma^2 + \sigma_q^2) I_N \tag{60b}$$

Substituting (60a), (60b) with the definition of λ_k (10) in (59) we get the first term of (36). Define $\boldsymbol{\epsilon} := \boldsymbol{g} - \hat{\boldsymbol{g}}$ as the estimation error vector. From (59) and the i.i.d. assumption on channels and quantization noise, it follows easily that $C_{\boldsymbol{\epsilon}} = E[\boldsymbol{\epsilon}\boldsymbol{\epsilon}^H]$ is give by (38). This completes the proof.

APPENDIX B
PROOF OF THEOREM 1

From (35), to calculate the achievable rate of the intercepted use, we need to calculate a and $\sigma^2_{n_{\text{eff}}}$. Throughout the proof steps we will make use of $\boldsymbol{h}_k = \hat{\boldsymbol{h}}_k + \boldsymbol{e}_k$ where $\boldsymbol{e}_k$ is the estimation error vector with covariance matrix given by $(1 - \sigma^2_{\hat{h}_k}) I_N$.

A. MRT-BF

For MRT-BF, we have $\boldsymbol{w}_k = \hat{\boldsymbol{h}}_k^*$. Substituting this in (33) yields

$$a_{\text{MRT}} = c_1 \sqrt{\beta_k} \underbrace{E[\boldsymbol{h}_k^T \hat{\boldsymbol{h}}_k^*]}_{I_0} = c_1 \sqrt{\beta_k} N \sigma^2_{\hat{h}_k} \tag{61}$$

and hence

$$|a_{\text{MRT}}|^2 = \frac{2\theta \beta_k p_d}{\pi \operatorname{tr}(\Sigma)} \sigma^4_{\hat{h}_k} N \tag{62}$$

Using (34) we rewrite

$$\sigma^2_{n_{\text{eff}},\text{MRT}} = c_1^2 \beta_k \underbrace{\operatorname{Var}(\boldsymbol{h}_k^T \hat{\boldsymbol{h}}_k^*)}_{I_1} + \sum_{j=1, j\neq k}^{K} c_1^2 \beta_k \underbrace{E[|\boldsymbol{h}_k^T \hat{\boldsymbol{h}}_j^*|^2]}_{I_2} + c_2^2 \beta_k \underbrace{E[\boldsymbol{h}_k^T S \boldsymbol{h}_k^*]}_{I_3} + \beta_k \sigma_q^2 p_d + 1. \tag{63}$$

We can obtain the terms denoted by I_1, I_2 as follows:

$$\begin{aligned} I_1 &= E[|\boldsymbol{h}_k^T \hat{\boldsymbol{h}}_k^*|^2] - |I_0|^2 \\ &= E[\|\hat{\boldsymbol{h}}_k\|^4 + E[|\boldsymbol{e}_k^T \hat{\boldsymbol{h}}_k^*|^2]] - N^2 \sigma^4_{\hat{h}_j} = N \sigma^2_{\hat{h}_k} \end{aligned} \tag{64}$$

$$\begin{aligned} I_2 &= E[\boldsymbol{h}_k^T \hat{\boldsymbol{h}}_j^* \hat{\boldsymbol{h}}_j^T \boldsymbol{h}_k^*] = E[|\hat{\boldsymbol{h}}_k^T \hat{\boldsymbol{h}}_j^*|^2] + E[|\boldsymbol{e}_k^T \hat{\boldsymbol{h}}_k^*|^2] \\ &= N \sigma^2_{\hat{h}_j}. \end{aligned} \tag{65}$$

Regarding I_3, we have $S = I_N$ when R-AN scheme is used, and $S = I_N - P_{\text{proj}}$ when NS-AN scheme is used, where $P_{\text{proj}} = \hat{H}^* (\hat{H}^T \hat{H}^*)^{-1} \hat{H}^T$ is the projection matrix. Hence,

$$I_3 = \begin{cases} N & \text{if R-AN} \\ (N-K)(1 - \sigma^2_{\hat{h}_k}) & \text{if NS-AN.} \end{cases} \tag{66}$$

Substituting (64)- (66) with definitions of c_1 and c_2 in (63) yields

$$\begin{aligned} \sigma^2_{n_{\text{eff}},\text{MRT}} = & \underbrace{\frac{2\theta \beta_k p_d}{\pi \operatorname{tr}(\Sigma)} \sigma^2_{\hat{h}_k}}_{\text{beamforing uncertainity}} + \underbrace{\frac{2\theta \beta_k p_d}{\pi \operatorname{tr}(\Sigma)} \sum_{j=1, j\neq k}^{K} \sigma^2_{\hat{h}_j}}_{\text{inter-user interference}} \\ & + \underbrace{P_{\text{AN}}}_{\text{artificial noise}} + \underbrace{\beta_k \sigma_q^2 p_d + 1}_{\text{quantization noise plus AWGN}} \\ = & \frac{2\theta \beta_k p_d}{\pi} + P_{\text{AN}} + \beta_k \sigma_q^2 p_d + 1. \end{aligned} \tag{67}$$

where

$$P_{\text{AN}} = \begin{cases} 2\bar{\theta} \beta_k p_d / \pi & \text{if R-AN} \\ 2\bar{\theta} \beta_k p_d (1 - \sigma^2_{\hat{h}_k}) / \pi & \text{if NS-AN.} \end{cases} \tag{68}$$

Substituting (62), (67) with (68) in (35), the first part of Theorem 1 follows.

B. ZF-BF

For ZF-BF, we have

$$a_{\text{ZF}} = c_1 \sqrt{\beta_k} \underbrace{E[\boldsymbol{h}_k^T \boldsymbol{w}_k]}_{I_0} \tag{69}$$

$$\sigma^2_{n_{\text{eff}},\text{ZF}} = c_1^2 \beta_k \underbrace{\operatorname{Var}(\boldsymbol{h}_k^T \boldsymbol{w}_k^*)}_{I_1} + \sum_{j=1, j\neq k}^{K} c_1^2 \beta_k \underbrace{E[|\boldsymbol{h}_k^T \boldsymbol{w}_j^*|^2]}_{I_2} + c_2^2 \beta_k \underbrace{E[\boldsymbol{h}_k^T S \boldsymbol{h}_k^*]}_{I_3} + \beta_k \sigma_q^2 p_d + 1. \tag{70}$$

where $\boldsymbol{w}_k$ denotes the k-th column of $W = \hat{H}^* (\hat{H}^T \hat{H}^*)^{-1}$. Note that we need to evaluate I_0, I_1 and I_2, while I_3 is given in (66). It is easy to show that $I_0 = 1$

and hence

$$|a_{\text{ZF}}|^2 = \frac{2\theta \beta_k p_d}{\pi \operatorname{tr}(\Sigma^{-1})} (N - K) \tag{71}$$

For I_1 and I_2, we proceed as follows.

$$\begin{aligned} I_1 &= E[|\boldsymbol{h}_k^T\boldsymbol{w}_k|^2] - |E[\boldsymbol{h}_k^T\boldsymbol{w}_k]|^2 = E[|\boldsymbol{h}_k^T\boldsymbol{w}_k|^2] - 1 \\ &= E[|\boldsymbol{e}_k^T\boldsymbol{w}_k|^2] = (1-\sigma^2_{\hat{h}_k})E[\|\boldsymbol{w}_k\|^2] \\ &= \frac{(1-\sigma^2_{\hat{h}_k})\sigma^{-2}_{\hat{h}_k}}{N-K} \end{aligned} \tag{72}$$

$$\begin{aligned} I_2 &= E[|\boldsymbol{h}_k^T\boldsymbol{w}_j|^2] = E[|\boldsymbol{e}_k^T\boldsymbol{w}_k|^2] = (1-\sigma^2_{\hat{h}_k})E[\|\boldsymbol{w}_j\|^2] \\ &= \frac{(1-\sigma^2_{\hat{h}_k})\sigma^{-2}_{\hat{h}_j}}{N-K} \end{aligned} \tag{73}$$

Substituting (72), (73) (66) with the definitions of c_1 and c_2 in (70), the effective noise can be expressed by

$$\begin{aligned} \sigma^2_{n_{\text{eff}},\text{ZF}} &= \underbrace{\frac{2\theta\beta_k p_d(1-\sigma^2_{\hat{h}_k})}{\pi\sigma^2_{\hat{h}_k}\operatorname{tr}(\Sigma^{-1})}}_{\text{beamforing uncertainity}} + \underbrace{\frac{2\theta\beta_k p_d}{\pi\operatorname{tr}(\Sigma^{-1})}\sum_{j=1,j\neq k}^{K}\frac{1-\sigma^2_{\hat{h}_k}}{\sigma^2_{\hat{h}_j}}}_{\text{inter-user interference}} \\ &+ \underbrace{P_{\text{AN}}}_{\text{artificial noise}} + \underbrace{\beta_k\sigma_q^2 p_d + 1}_{\text{quantization noise plus AWGN}} \\ &= \frac{2\theta\beta_k p_d}{\pi}(1-\sigma^2_{\hat{h}_k}) + P_{\text{AN}} + \beta_k\sigma_q^2 p_d + 1. \end{aligned} \tag{74}$$

Finally, substituting (71), (74) combined with (68) in (35), the second part of Theorem 1 follows. This completes the proof.

Appendix C
Proof of Theorem 2

Here we derive a simple upper-bound on $\overline{R}_e$ (30). By the concavity of $\log(\cdot)$, applying Jensen's inequality to (30) yields

$$\overline{R}_e \leq \log\left(1 + c_1^2\beta_e E\left[\boldsymbol{w}_k^H\boldsymbol{g}^* C_e^{-1}\boldsymbol{g}^T\boldsymbol{w}_k\right]\right). \tag{75}$$

where C_e is the covariance matrix of effective noise given by (31), which is rewritten again here:

$$C_e = c_2^2\beta_e\boldsymbol{g}^T S\boldsymbol{g}^* + c_3^2\beta_e\sigma_q^2\boldsymbol{g}^T\boldsymbol{g}^* + 1. \tag{76}$$

.

When R-AN approach is used, $S = I_N$. Hence,

$$\begin{aligned} C_e^{\text{R-AN}} &= (c_2^2\beta_e + c_3^2\beta_e\sigma_q^2)\|\boldsymbol{g}\|^2 + 1 \\ &\xrightarrow{\text{a.s.}} (c_2^2\beta_e + c_3^2\beta_e\sigma_q^2)N + 1 \\ &= 2\bar{\theta}\beta_e p_d/\pi + \beta_e p_d\sigma_q^2 + 1 \end{aligned} \tag{77}$$

as N grows large which follows from the strong law of large numbers.

When NS-AN approach is used, we have $S = I_N - P_{\text{proj}}$. Using Lemma 1, we can write

$$\begin{aligned} \boldsymbol{g}^T S\boldsymbol{g}^* &= (\sqrt{\kappa_R}\hat{\boldsymbol{h}}_k + \boldsymbol{\epsilon})^T S(\sqrt{\kappa_R}\hat{\boldsymbol{h}}_k + \boldsymbol{\epsilon})^* \\ &= \boldsymbol{\epsilon}^T S\boldsymbol{\epsilon}^* = \boldsymbol{\epsilon}^T\tilde{U}\tilde{U}^H\boldsymbol{\epsilon}^* \end{aligned} \tag{78}$$

where $\tilde{U} \in \mathcal{C}^{N\times(N-K)}$ comprise $(N-K)$ eigenvectors (each has norm 1) corresponding to the $N-K$ repeated unity eigenvalues of S. Since $N \gg K$ (i.e., Massive MIMO setting), $\tilde{U}\tilde{U}^H$ can be very well approximated by a scaled identity matrix, where the off-diagonal entries of $\tilde{U}\tilde{U}^H$ are, in fact, are much smaller than the diagonal entries. Thus,

$$\tilde{U}\tilde{U}^H \approx \frac{\operatorname{tr}(\tilde{U}\tilde{U}^H)}{N} = (1-K/N)I_N \tag{79}$$

Substituting (79) in (78) yields

$$\boldsymbol{g}^T S\boldsymbol{g}^* \approx (1-K/N)\|\boldsymbol{\epsilon}\|^2 \xrightarrow{\text{a.s.}} (N-K)(1-\kappa_R\sigma^2_{\hat{h}_k}) \tag{80}$$

Therefore,

$$C_e^{\text{NS-AN}} \approx 2\bar{\theta}\beta_e p_d(1-\kappa_R\sigma^2_{\hat{h}_k})/\pi + \beta_e p_d\sigma_q^2 + 1. \tag{81}$$

We summarize,

$$C_e \approx (P_e^{\text{AN}} + \beta_e p_d\sigma_q^2 + 1)I_M \tag{82}$$

where

$$P_e^{\text{AN}} = \begin{cases} 2\bar{\theta}\beta_e p_d/\pi & \text{if R-AN} \\ 2\bar{\theta}\beta_e p_d(1-\kappa_R\sigma^2_{\hat{h}_k})/\pi & \text{if NS-AN.} \end{cases} \tag{83}$$

Substituting (82) in (75) yields

$$\overline{R}_e \lesssim \log\left(1 + \frac{c_1^2\beta_e E[\boldsymbol{w}_k^H\boldsymbol{g}^*\boldsymbol{g}^T\boldsymbol{w}]}{P_e^{\text{AN}} + \beta_e p_d\sigma_q^2 + 1}\right). \tag{84}$$

The expectation $\mu := E[\boldsymbol{w}_k^H\boldsymbol{g}^*\boldsymbol{g}^T\boldsymbol{w}]$ for both the MRT-BF and ZF-BF cases is evaluated as follows. For MRT-BF, setting $\boldsymbol{w}_k = \hat{\boldsymbol{h}}_k^*$ and using Lemma 1, we write

$$\begin{aligned} \mu_{\text{MRT}} &:= E\left[\hat{\boldsymbol{h}}_k^T\boldsymbol{g}^*\boldsymbol{g}^T\hat{\boldsymbol{h}}_k^*\right] \\ &= \kappa_R E[\|\hat{\boldsymbol{h}}_k\|^4] + 2\sqrt{\kappa_R}\Re(E[\hat{\boldsymbol{h}}_k^T\hat{\boldsymbol{h}}_k^*\boldsymbol{\epsilon}^T\hat{\boldsymbol{h}}_k^*]) + E[\hat{\boldsymbol{h}}_k^T\boldsymbol{\epsilon}^*\boldsymbol{\epsilon}^T\hat{\boldsymbol{h}}_k^*] \\ &= \kappa_R\sigma^4_{\hat{h}_k}N(N+1) + (1-\kappa_R\sigma^2_{\hat{h}_k})\sigma^2_{\hat{h}_k}N \\ &= \sigma^2_{\hat{h}_k}(\kappa_R\sigma^2_{\hat{h}_k}N + 1)N. \end{aligned} \tag{85}$$

where we make use of the fact that $\boldsymbol{\epsilon}$ is independent of $\hat{\boldsymbol{h}}$.

For ZF-BF, Lemma 1 allows us to write

$$\begin{aligned} \mu_{\text{ZF}} &:= E\left[\boldsymbol{w}_k^H\boldsymbol{g}^*\boldsymbol{g}^T\boldsymbol{w}_k\right] \\ &= E\left[\boldsymbol{w}_k^H(\sqrt{\kappa_R}\hat{\boldsymbol{h}}_k^* + \boldsymbol{\epsilon}^*)(\sqrt{\kappa_R}\hat{\boldsymbol{h}}_k^T + \boldsymbol{\epsilon}^T)\boldsymbol{w}_k\right] \\ &= \left(\kappa_R + E[\boldsymbol{w}_k^H\boldsymbol{\epsilon}^*\boldsymbol{\epsilon}^T\boldsymbol{w}_k]\right) = \kappa_R + \frac{\sigma^{-2}_{\hat{h}_k}(1-\kappa_R\sigma^2_{\hat{h}_k})}{N-K} \end{aligned} \tag{86}$$

where we make use of the fact that $\boldsymbol{\epsilon}$ is independent of $\boldsymbol{w}_k$. Substituting (85) and (86) combined with (83) and the definition of c_1, in (84), (43) and (44) follow, respectively. This completes the proof.

References

[1] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, 2014.

[2] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: Af or df?" *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.

[3] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful Massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[4] D. Kapetanović, G. Zheng, and F. Rusek, "Physical layer security for Massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27r, 2015.

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

[6] K. Guo, Y. Guo, and G. Ascheid, "Security-constrained power allocation in MU-Massive-MIMO with distributed antennas," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8139–8153, Dec 2016.

[7] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Key elements to enable millimeter wave communications for 5G wireless systems," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 136–143, December 2014.

[8] J. Zhu, W. Xu, and N. Wang, "Secure massive MIMO systems with limited RF chains," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5455–5460, June 2017.

[9] J. Mo and R. W. Heath, "High SNR capacity of millimeter wave MIMO systems with one-bit quantization," in *2014 Information Theory and Applications Workshop (ITA)*, Feb 2014, pp. 1–5.

[10] J. Mo, P. Schniter, N. G. Prelcic, and R. W. Heath, "Channel estimation in millimeter wave MIMO systems with one-bit quantization," in *2014 48th Asilomar Conference on Signals, Systems and Computers*, Nov 2014, pp. 957–961.

[11] M. A. Teeti, R. Wang, and R. Abdolee, "On the Uplink achievable rate for Massive MIMO with 1-Bit ADC and superimposed pilots," *IEEE Access*, vol. 6, pp. 37 627–37 643, 2018.

[12] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

[13] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[14] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[15] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6854–6868, Dec 2015.

[16] J. Zhu, R. Schober, and V. K. Bhargava, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, 2016.

[17] Y. Wu, J. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Transactions on Communications*, vol. 65, no. 8, pp. 3614–3628, Aug 2017.

[18] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of Massive MIMO: Benefits and challenges," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 742–758, Oct 2014.

[19] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 40–60, Jan 2013.

[20] 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, April 2013.

[21] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, November 2010.

[28] R. F. Schaefer, G. Amarasuriya, and H. V. Poor, "Physical layer security in Massive MIMO systems," in *2017 51st Asilomar Conference on Signals, Systems, and Computers*, Oct 2017, pp. 3–8.

[22] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, March 2012.

[23] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure Massive MIMO Transmission with an Active Eavesdropper," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3880–3900, 2016.

[24] Y. O. Basciftci, C. E. Koksal, and A. E. Ashikhmin, "Securing massive MIMO at the physical layer," *CoRR*, vol. abs/1505.00396, 2015. [Online]. Available: http://arxiv.org/abs/1505.00396

[25] Q. Xiong, Y. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[26] T. T. Do, H. Q. Ngo, T. Q. Duong, T. J. Oechtering, and M. Skoglund, "Massive MIMO pilot retransmission strategies for robustification against jamming," *IEEE Wireless Communications Letters*, vol. 6, no. 1, pp. 58–61, Feb 2017.

[27] T. T. Do, E. G. Larsson, and S. M. Razavizadeh, "Jamming-Resistant Receivers for the Massive MIMO Uplink," vol. 13, no. 1, pp. 210–223, 2018.

[29] Y. Wu, C. Wen, W. Chen, S. Jin, R. Schober, and G. Caire, "Data-aided secure Massive MIMO transmission with active eavesdropping," *IEEE International Conference on Communications*, vol. 2018-May, pp. 1–6, 2018.

[30] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong, X. Gao, S. Member, A. Khisti, S. Member, C. Xiao, G. Caire, K. K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[31] S. Jacobsson, G. Durisi, M. Coldrey, T. Goldstein, and C. Studer, "Quantized Precoding for Massive MU-MIMO," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 4670–4684, 2017.

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

[33] W. Zhao, S. H. Lee, and A. Khisti, "Phase-Only Zero Forcing for Secure Communication with Multiple Antennas," *IEEE Journal on Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1334–1345, 2016.

[34] 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 Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2001–2016, 2017.

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

[36] J. J. Bussgang, "Crosscorrelation functions of amplitude-distorted gaussian signals," *Research Laboratory of Electronics, Massachusetts Institute of Technology*, vol. 216, no. 216, pp. 1–14, 1952.

[37] A. M. Tulino and S. Verdú, "Random matrix theory and wireless communications," *Foundations and Trends® in Communications and Information Theory*, vol. 1, no. 1, pp. 1–182, 2004. [Online]. Available: http://dx.doi.org/10.1561/0100000001