The MISO Wiretap Channel with Channel Uncertainty: Asymptotic Perspectives

Anas Chaaban, Zouheir Rezki, Basel Alomair, and Mohamed-Slim Alouini

(Invited)

***Abstract*—The N-antenna MISO Gaussian wiretap channel with imperfect channel-state information at the transmitter (CSIT) is studied in terms of secrecy rate scaling versus the signal-to-noise ratio (SNR) and N. Two schemes are considered, beamforming (BF) and artificial noise injection (AN). It is shown that if the CSIT error is independent of SNR, then both schemes do not achieve scaling versus SNR. However, if this error vanishes as SNR increases, then AN achieves the optimal scaling versus SNR, contrary to BF. Scaling can be achieved in BF by increasing N. In fact, BF achieves the optimal scaling versus N. In the AN scheme however, injecting noise in multiple direction deteriorates its scaling versus N. Nevertheless, AN can achieve the optimal scaling if noise is sent in only one direction. This leads to better performance than BF if the CSIT error is smaller than a threshold which is also derived.**

I. Introduction

In many communication scenarios, it is required to conceal the transmitted information from a third party (eavesdropper). This concealment can be achieved using physical-layer security, which has attracted lots of research attention since [1]. In this context, we are interested in the transmission rate under which this security is guaranteed, known as the secrecy rate.

The channel model of this secure communication is known as the wiretap channel, studied in [2]–[4], to name a few. Extensions to multi-antenna Gaussian wiretap channels have been considered in [5]–[7].

In this paper, we focus on the Gaussian multiple-input single output (MISO) fading wiretap channel. With fading comes the natural question of the availability of channel-state information at the transmitter (CSIT). It is practical to assume that, using some feedback mechanism, the state of the main channel (from the transmitter to the legitimate receiver) is known with some accuracy at the transmitter. Perfect main CSIT was studied in [4], [8], [9]. Imperfect main CSIT can lead to performance degradation, which can be mild such as a reduction in secrecy rate, or severe such as a reduction in its scaling behavior. We focus on the latter case due to its practical nature, and study the scaling behavior of the secrecy rate as a function of the signal-to-noise ratio (SNR) and the number of antennas N.

A. Chaaban and M.-S. Alouini are with King Abdullah University of Science and Technology (KAUST), Computer, Electrical, and Mathematical Sciences and Engineering (CEMSE) Division, Thuwal, Saudi Arabia. Email:{anas.chaaban,slim.alouini}@kaust.edu.sa

Z. Rezki is with the Department of Electrical and Computer Engineering, University of Idaho, Moscow, ID, USA. Email:zrezki@uidaho.edu

B. Alomair is with King Abdulaziz City for Science and Technology, The National Center for Cybersecurity Technology (C4C), Riyadh, Saudi Arabia. Email: alomair@kacst.edu.sa

We consider two schemes: beamforming (BF) and artificial noise injection (AN) under two scenarios: (i) fixed precision CSIT, and (ii) CSIT whose quality improves with SNR. For the latter case, the secrecy rate scales with SNR, contrary to the former, and the optimal scaling is achieved using the AN scheme. Since no scaling versus SNR can be achieved in the former by both schemes, one could increase the secrecy rate by increasing N (which advocates massive MIMO). This improves the rate of the BF scheme, which achieves the optimal scaling versus N. On the other hand, the AN scheme, in its classical form where noise is sent in all directions orthogonal to the main channel-estimate, does not achieve any scaling versus N. This is counter-intuitive, since one would expect that when the CSIT error is small enough, sending artificial noise orthogonal to the main channel-estimate should degrade the eavesdropper observation [6] and improve upon BF.

It turns out that this behavior is due to noise-leakage [10] to the legitimate receiver. We show that this noise-leakage can be significantly reduced if we send artificial noise along *only* one direction orthogonal to the main channel-estimate, instead of sending along all $N-1$ orthogonal directions as in [10], [11]. Consequently, the AN scheme recovers a scaling behavior versus N similar to BF, and achieves higher secrecy rates than BF if the CSIT error is small enough. We derive a threshold on the quality of CSIT, below which the performance of AN becomes better than BF, and vice versa.

II. System Model

We consider a discrete-time memoryless wiretap channel consisting of an N-antenna transmitter, a single-antenna legitimate receiver, and a single-antenna eavesdropper. The outputs at both receivers at time period i, $i = 1, \cdots, n \in \mathbb{N}$ are expressed, respectively, as

$$y_i = \boldsymbol{h}_i^t \boldsymbol{x}_i + n_{yi}, \quad z_i = \boldsymbol{g}_i^t \boldsymbol{x}_i + n_{zi}, \tag{1}$$

where $\boldsymbol{x}_i \in \mathbb{R}^N$ is the transmitted signal, $\boldsymbol{h}_i, \boldsymbol{g}_i \in \mathbb{R}^N$ are the channels vectors from the transmitter to the legitimate and the eavesdropper receivers, respectively, and n_{yi} and n_{zi} are Gaussian noises with zero mean and unit variance $n_{yi}, n_{zi} \sim \mathcal{N}(0,1)$. The transmit signal $\boldsymbol{x}_i$ is constrained by an average power constraint given by

$$\frac{1}{n}\sum_{i=1}^{n} \mathrm{tr}\left(\mathbb{E}\left[\boldsymbol{x}_i \boldsymbol{x}_i^t\right]\right) \leq P. \tag{2}$$

The channel gains $\boldsymbol{h}$ and $\boldsymbol{g}$ are assumed to be independent of each other, both independent and identically distributed

(i.i.d.) in time with distribution $\mathcal{N}(\mathbf{0}, \boldsymbol{I})$. The transmitter is only provided a noisy version $\hat{\boldsymbol{h}}_i$ of $\boldsymbol{h}_i$ produced using MMSE estimation, such that

$$\boldsymbol{h}_i = \sqrt{\bar{\alpha}}\hat{\boldsymbol{h}}_i + \sqrt{\alpha}\tilde{\boldsymbol{h}}_i, \tag{3}$$

where $\tilde{\boldsymbol{h}}_i \sim \mathcal{N}(\mathbf{0}, \boldsymbol{I})$ is the estimation error which is uncorrelated and hence independent of $\boldsymbol{h}_i$, $\alpha \in (0,1)$ is the error variance, and $\bar{\alpha} = 1 - \alpha$. We note that α can be either a fixed constant which we write as $\alpha = O(1)$, or a decreasing function of P which we write as $\alpha = \theta(P^{-\beta})$ for $\beta \in (0,1)$.[1] The first case models scenarios where the channel estimation accuracy is limited due to discretization resolution e.g., while the second models scenarios where such a limitation does not constitute a bottleneck for system performance. The legitimate receiver has perfect knowledge of $\boldsymbol{h}_i$ and $\hat{\boldsymbol{h}}_i$ and the eavesdropper has knowledge of $\boldsymbol{g}_i$, $\hat{\boldsymbol{h}}_i$, and $\boldsymbol{h}_i$.

We are interested in the secrecy capacity of this channel, which is the highest achievable secrecy rate. We focus on the analysis of two transmission schemes: (i) beamforming (BF) and (ii) artificial noise (AN) injection. We study the scaling of their achievable secrecy rates versus P and N.

III. Behavior versus P

A. Beamforming

In BF, the desired signal is beamformed along $\hat{\boldsymbol{h}}$, which is combined with a wiretap code to achieve the secrecy rate [12]

$$R_{\mathsf{BF}} = \max_{\hat{P}} \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}},g}\left[\frac{1}{2}\log\left(\frac{\|\hat{\boldsymbol{h}}\|^2 + (\hat{\boldsymbol{h}}^t\boldsymbol{h})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(1+g^2\hat{P})}\right)\right], \tag{4}$$

where $\hat{P}$ is a function of $\hat{\boldsymbol{h}}$ satisfying $\mathbb{E}_{\hat{\boldsymbol{h}}}[\hat{P}] \le P$, and $g \sim \mathcal{N}(0,1)$. This achievable rate does not scale with P, i.e., it approaches a constant as P grows. To prove this, we write

$$R_{\mathsf{BF}} = \max_{\hat{P}} \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}},g}\left[\frac{1}{2}\log\left(\frac{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\|\hat{\boldsymbol{h}}\|^2}\hat{P}}{1+g^2\hat{P}}\right)\right] \tag{5}$$

$$\le \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}},g}\left[\frac{1}{2}\log\left(\max\left\{1, \frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\|\hat{\boldsymbol{h}}\|^2 g^2}\right\}\right)\right]. \tag{6}$$

This upper bound is independent of P if $\alpha = O(1)$, and behaves as $O(1)$ in P if $\alpha = \theta(P^{-\beta})$. Thus, R_{BF} achieves the optimal secrecy degrees-of-freedom (SDoF) of the channel if $\alpha = O(1)$, since the SDoF is zero in this case [13]. However, R_{BF} fails to achieve the optimal SDoF if $\alpha = \theta(P^{-\beta})$, where the SDoF becomes β [13]. The AN scheme solves this issue.

B. Artificial Noise Injection

In the AN scheme, we send the desired signal along $\hat{\boldsymbol{h}}$ while we send artificial noise orthogonal to $\hat{\boldsymbol{h}}$. Commonly, artificial noise is sent in all $N-1$ dimensions of the null-space of $\hat{\boldsymbol{h}}$ [10], [11]. This leads to the following achievable secrecy rate [14]

$$R_{\mathsf{AN}} = \max_{\hat{P}} \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}},\boldsymbol{g}}\left[\frac{1}{2}\log\left(\frac{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(N+\alpha\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2\hat{P})}}{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(N+\|\hat{\boldsymbol{F}}^t\boldsymbol{g}\|^2\hat{P})}}\right)\right], \tag{7}$$

subject to $\mathbb{E}_{\hat{\boldsymbol{h}}}[\hat{P}] \le P$, where $\hat{\boldsymbol{F}} \in \mathbb{R}^{N\times(N-1)}$ is an orthogonal matrix with $\hat{\boldsymbol{F}}^t\hat{\boldsymbol{h}} = \mathbf{0}$. Here, the power $\hat{P}$ is allocated equally between the N transmit directions. Note that we can encompass R_{BF} in R_{AN} by allowing unequal power allocation between noise and desired signal. For simplicity, we stick to equal power allocation in this paper.

The rate R_{AN} does not scale with P if $\alpha = O(1)$. Namely,

$$\frac{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(N+\alpha\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2\hat{P})}}{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(N+\|\hat{\boldsymbol{F}}^t\boldsymbol{g}\|^2\hat{P})}} \le 1 + \frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(N+\alpha\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2\hat{P})} \tag{8}$$

$$\le 1 + \frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\alpha\|\hat{\boldsymbol{h}}\|^2\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2}. \tag{9}$$

Thus,

$$R_{\mathsf{AN}} \le \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\alpha\|\hat{\boldsymbol{h}}\|^2\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2}\right)\right], \tag{10}$$

which does not scale with P if $\alpha = O(1)$. However, if $\alpha = \theta(P^{-\beta})$, then it can be shown that it scales as $\frac{\beta}{2}\log(P)$ since

$$1 + \frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(N+\|\hat{\boldsymbol{F}}^t\boldsymbol{g}\|^2\hat{P})} = \frac{1+(\|\hat{\boldsymbol{F}}^t\boldsymbol{g}\|^2 + \frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2}{\|\hat{\boldsymbol{h}}\|^2})\frac{\hat{P}}{N}}{1+\|\hat{\boldsymbol{F}}^t\boldsymbol{g}\|^2\frac{\hat{P}}{N}}$$

$$\le 1 + \frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2}{\|\hat{\boldsymbol{h}}\|^2\|\hat{\boldsymbol{F}}^t\boldsymbol{g}\|^2}, \tag{11}$$

leading to

$$R_{\mathsf{AN}} \ge \max_{\hat{P}} \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}},\boldsymbol{g}}\left[\frac{1}{2}\log\left(1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(N+\alpha\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2\hat{P})}\right) - \frac{1}{2}\log\left(1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2}{\|\hat{\boldsymbol{h}}\|^2\|\hat{\boldsymbol{F}}^t\boldsymbol{g}\|^2}\right)\right] \tag{12}$$

$$\ge \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}},\boldsymbol{g}}\left[\frac{1}{2}\log\left(\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2 P}{\|\hat{\boldsymbol{h}}\|^2(N+\alpha\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2 P)}\right) - \frac{1}{2}\log\left(1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2}{\|\hat{\boldsymbol{h}}\|^2\|\hat{\boldsymbol{F}}^t\boldsymbol{g}\|^2}\right)\right] \tag{13}$$

$$= \frac{1}{2}\log(\alpha^{-1}) + o(\log(P)), \tag{14}$$

where $o(\log(P))$ vanishes relative to $\log(P)$ as $P \to \infty$. This lower bound scales as $\frac{\beta}{2}\log(P)$ leading to the optimal scaling.

While the secrecy rate scaling for $\alpha = \theta(P^{-\beta})$ is known to be $\frac{\beta}{2}\log(P)$, only the SDoF is known for $\alpha = O(1)$. Results in [13] upper bounds this scaling by $\frac{1}{2}\log\log(P)$. Nevertheless, we believe that *the correct scaling behavior in this case is* $O(1)$ as conjectured in [13]. Fig. 1 shows the achievable rates R_{BF} and R_{AN} with $\hat{P} = P$, which will be denoted R'_{BF} and

[1] $f(x) = \theta(g(x))$ implies that $\exists M, x_0 > 0$ such that $\frac{1}{M}g(x) \le f(x) \le Mg(x)$, for all $x \ge x_0$.

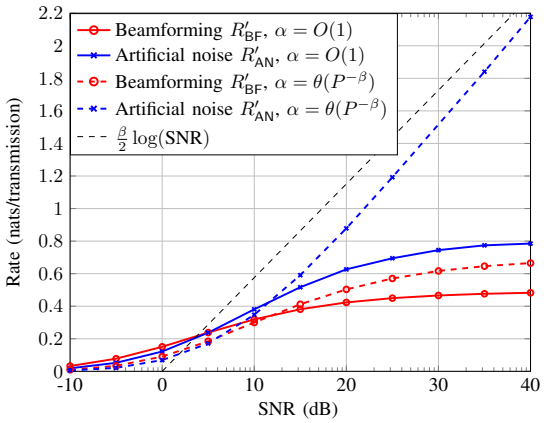

Figure 1: Secrecy rates for a setup with $N = 2$. We use $\alpha = 1/5 = O(1)$ and $\alpha = \frac{1}{1+\sqrt{P}} = \theta(P^{-\beta})$ with $\beta = \frac{1}{2}$.

R'_{AN}. Note the lack of scaling for $\alpha = O(1)$ and the scaling of R'_{AN} for $\alpha = \theta(P^{-\beta})$.

This result is rather negative for $\alpha = O(1)$, since the secrecy rate can not be increased effectively by increasing P. The good news is that it can be increased by increasing N as shown next.

IV. Behavior versus N

Here, we will focus on the scaling versus N for large P.

A. Beamforming

The rate R_{BF} can be written as

$$R_{\mathsf{BF}} \geq \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2P}{\|\hat{\boldsymbol{h}}\|^2}\right)\right]-\mathbb{E}_g\left[\frac{1}{2}\log\left(1+g^2P\right)\right]$$
$$\geq \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2P}{\|\hat{\boldsymbol{h}}\|^2}\right)\right]-\mathbb{E}_g\left[\frac{1}{2}\log\left(1+g^2P\right)\right].$$

The second term does not depend on N, so we focus on the first. From [12, Lemma 2], we have that

$$\mathbb{E}_{\tilde{\boldsymbol{h}}|\hat{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\|\hat{\boldsymbol{h}}\|^2}\right)\right]=\frac{1}{2}\log\left(\mathbb{E}_{\tilde{\boldsymbol{h}}|\hat{\boldsymbol{h}}}\left[\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\|\hat{\boldsymbol{h}}\|^2}\right]\right)+\epsilon_N$$
$$=\frac{1}{2}\log\left(\alpha+\bar{\alpha}\|\hat{\boldsymbol{h}}\|^2\right)+\epsilon_N, \tag{15}$$

since $\frac{\hat{\boldsymbol{h}}^t\boldsymbol{h}}{\|\hat{\boldsymbol{h}}\|} \sim \mathcal{N}(\sqrt{\bar{\alpha}}\|\hat{\boldsymbol{h}}\|,\alpha)$ given $\hat{\boldsymbol{h}}$, where $\epsilon_N \to 0$ as $N \to \infty$. Thus,

$$\mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\|\hat{\boldsymbol{h}}\|^2}\right)\right]=\mathbb{E}_{\hat{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\alpha+\bar{\alpha}\|\hat{\boldsymbol{h}}\|^2\right)\right]+\epsilon_N$$
$$\geq \mathbb{E}_{\hat{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\bar{\alpha}\|\hat{\boldsymbol{h}}\|^2\right)\right]+\epsilon_N$$
$$=\frac{1}{2}\log(2\bar{\alpha})+\frac{1}{2}\psi\left(\frac{N}{2}\right)+\epsilon_N,$$

where $\psi(\cdot)$ is the Digamma function. But $\psi\left(\frac{N}{2}\right) = \log\left(\frac{N}{2}\right) + \epsilon_N$. This leads to

$$R_{\mathsf{BF}} \geq \frac{1}{2}\log(\bar{\alpha}N)-\mathbb{E}_g\left[\frac{1}{2}\log\left(\frac{1}{P}+g^2\right)\right]+\epsilon_N. \tag{16}$$

By dominated convergence, this can be written as

$$R_{\mathsf{BF}} \geq \frac{1}{2}\log(\bar{\alpha}N)-\mathbb{E}_g\left[\frac{1}{2}\log\left(g^2\right)\right]+\epsilon_N+\epsilon_P \tag{17}$$
$$=\frac{1}{2}\log(2\bar{\alpha}N)+\frac{\gamma_E}{2}+\epsilon_N+\epsilon_P, \tag{18}$$

where $\epsilon_P \to 0$ as $P \to \infty$, and $\gamma_E \approx 0.577$ is Euler's constant. Thus R_{BF} scales as $\frac{1}{2}\log(N)$, which is the optimal scaling. Optimality follows since the capacity of the MISO channel without secrecy and with perfect CSIT, which serves as an upper bound for our scenario, scales as $\frac{1}{2}\log(N)$.

B. Artificial Noise Injection

On the other hand, AN provides a secrecy rate that does not scale with N, which makes the AN scheme worse than the BF scheme from this perspective. To show this, we start with (10) which, after simple manipulations, can be written as

$$R_{\mathsf{AN}} \leq \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\frac{\alpha\|\tilde{\boldsymbol{h}}\|^2+2\sqrt{\alpha\bar{\alpha}}\hat{\boldsymbol{h}}^t\tilde{\boldsymbol{h}}+\bar{\alpha}\|\hat{\boldsymbol{h}}\|^2}{\alpha\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2}\right)\right]. \tag{19}$$

Using Jensen's inequality, we obtain

$$R_{\mathsf{AN}} \leq \frac{1}{2}\log(N)-\mathbb{E}_{\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\alpha\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2\right)\right]. \tag{20}$$

But $\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}} \sim \mathcal{N}(\boldsymbol{0},\hat{\boldsymbol{F}}^t\hat{\boldsymbol{F}})$ and $\hat{\boldsymbol{F}}^t\hat{\boldsymbol{F}} = \boldsymbol{I}_{N-1}$ by definition ($\boldsymbol{I}_{N-1}$ is the identity matrix of size $(N-1)$). Thus, $\mathbb{E}_{\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\alpha\|\hat{\boldsymbol{F}}^t\tilde{\boldsymbol{h}}\|^2\right)\right] = \frac{1}{2}\log(2\alpha)+\frac{1}{2}\psi\left(\frac{N-1}{2}\right)$. Since $\psi\left(\frac{N-1}{2}\right) = \log\left(\frac{N-1}{2}\right)+\epsilon_N$, then $R_{\mathsf{AN}} \leq \frac{1}{2}\log\left(\frac{N}{N-1}\right) - \frac{1}{2}\log(\alpha)+\epsilon_N$ which does not scale with N.

This contradicts with intuition, since one would expect that if α is small, then AN is better than BF. This intuition is indeed true, and the above reduced scaling of AN owes to sending artificial noise along all $N-1$ directions orthogonal to $\hat{\boldsymbol{h}}$. To remedy this loss, we propose to send artificial noise in only one direction instead. The achievable rate then becomes

$$\hat{R}_{\mathsf{AN}} = \max_{\hat{P}} \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}},\boldsymbol{g}}\left[\frac{1}{2}\log\left(\frac{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(2+\alpha\|\hat{\boldsymbol{f}}^t\tilde{\boldsymbol{h}}\|^2\hat{P})}}{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2\hat{P}}{\|\hat{\boldsymbol{h}}\|^2(2+\|\hat{\boldsymbol{f}}^t\boldsymbol{g}\|^2\hat{P})}}\right)\right],$$

subject to $\mathbb{E}_{\hat{\boldsymbol{h}}}[\hat{P}] \leq P$, where $\hat{\boldsymbol{f}} \in \mathbb{R}^{N\times 1}$ is orthogonal to $\hat{\boldsymbol{h}}$. This achievable rate can be larger than R_{AN} and has the same scaling versus P. More importantly, it scales with N. This suggests that sending artificial noise in more than one direction harms the legitimate receiver (due to noise leakage [10]) more than the eavesdropper (see Fig. 2). This is interestingly contrary to the perfect CSIT case ($\alpha = 0$) where sending noise in all $N-1$ achieves the best scaling.

The rate $\hat{R}_{\mathsf{AN}}$ satisfies

$$\hat{R}_{\mathsf{AN}} \geq \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}},\boldsymbol{g}}\left[\frac{1}{2}\log\left(\frac{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2 P}{\|\hat{\boldsymbol{h}}\|^2(2+\alpha\|\hat{\boldsymbol{f}}^t\tilde{\boldsymbol{h}}\|^2 P)}}{1+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2 P}{\|\hat{\boldsymbol{h}}\|^2(2+\|\hat{\boldsymbol{f}}^t\boldsymbol{g}\|^2 P)}}\right)\right] \tag{21}$$

$$= \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\|\hat{\boldsymbol{f}}^t\tilde{\boldsymbol{h}}\|^2+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\alpha\|\hat{\boldsymbol{h}}\|^2}\right)\right] - \mathbb{E}_{\hat{\boldsymbol{h}},\boldsymbol{g}}\left[\frac{1}{2}\log\left(\|\hat{\boldsymbol{f}}^t\boldsymbol{g}\|^2+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2}{\|\hat{\boldsymbol{h}}\|^2}\right)\right]+\epsilon_P. \tag{22}$$

Since $\|\hat{\boldsymbol{f}}^t\boldsymbol{g}\|^2+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{g})^2}{\|\hat{\boldsymbol{h}}\|^2} = \|[\hat{\boldsymbol{f}},\ \frac{\hat{\boldsymbol{h}}}{\|\hat{\boldsymbol{h}}\|}]^t\boldsymbol{g}\|^2$, and since $[\hat{\boldsymbol{f}},\ \frac{\hat{\boldsymbol{h}}}{\|\hat{\boldsymbol{h}}\|}]^t\boldsymbol{g}$ is Gaussian with zero mean and covariance $\boldsymbol{I}_2$, then the second term above can written as $\mathbb{E}_{\boldsymbol{g}_2}\left[\frac{1}{2}\log\left(\|\boldsymbol{g}_2\|^2\right)\right]$ where $\boldsymbol{g}_2 = [g_1,\ g_2]^t$. The first term satisfies

$$\mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\|\hat{\boldsymbol{f}}^t\tilde{\boldsymbol{h}}\|^2+\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\alpha\|\hat{\boldsymbol{h}}\|^2}\right)\right] \geq \mathbb{E}_{\hat{\boldsymbol{h}},\tilde{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\frac{(\hat{\boldsymbol{h}}^t\boldsymbol{h})^2}{\alpha\|\hat{\boldsymbol{h}}\|^2}\right)\right] \tag{23}$$

$$= \mathbb{E}_{\hat{\boldsymbol{h}}}\left[\frac{1}{2}\log\left(\frac{\bar{\alpha}\|\hat{\boldsymbol{h}}\|^2}{\alpha}\right)\right]+\epsilon_N, \tag{24}$$

since $\|\hat{\boldsymbol{h}}\| \to \infty$ as $N \to \infty$. Hence,

$$\hat{R}_{\mathsf{AN}} \geq \frac{1}{2}\mathbb{E}_{\hat{\boldsymbol{h}},\boldsymbol{g}_2}\left[\log\left(\frac{\bar{\alpha}\|\hat{\boldsymbol{h}}\|^2}{\alpha\|\boldsymbol{g}_2\|^2}\right)\right]+\epsilon_P+\epsilon_N \tag{25}$$

$$= \frac{1}{2}\log\left(\frac{\bar{\alpha}}{\alpha}N\right)-\frac{1}{2}\log(2)+\frac{\gamma_E}{2}+\epsilon_P+\epsilon_N. \tag{26}$$

This is clearly better than R_{AN}; it scales as $\frac{1}{2}\log(N)$. Fig. 2 shows the rates achievable by AN when noise is injected in 1, 2, and 3 directions orthogonal to $\hat{\boldsymbol{h}}$, with $\hat{P} = P$, along with (26) for comparison. It can be seen that sending artificial noise in less directions orthogonal to $\hat{\boldsymbol{h}}$ is better.

C. Comparison

It is interesting to find the threshold value of α beyond which AN becomes better than BF and vice versa. An approximate value of this threshold can be obtained by comparing (18) and (26). This comparison leads to the following statement: *For large N and P,* BF *outperforms* AN *if* $\alpha \geq \frac{1}{4}$, *and* AN *outperforms* BF *otherwise*. Fig. 3 plots this behavior.

V. Conclusions

Secrecy rates of beamforming (BF) and artificial noise injection (AN) in a MISO wiretap channels with imperfect CSIT, do not scale with SNR if the CSIT error is independent of SNR. If this error vanishes as SNR increases, then AN achieves scaling versus SNR, contrary to BF. Since the rate does not scale with SNR if CSIT error is constant versus SNR, one can resort to increasing the number of transmit antennas. In this case, BF achieves the optimal scaling versus N, while classical AN, in which noise is sent in multiple directions, does not achieve any scaling versus N. This can be resolved by sending noise in only one direction instead, which can lead to better performance than BF especially if the CSIT error is small.

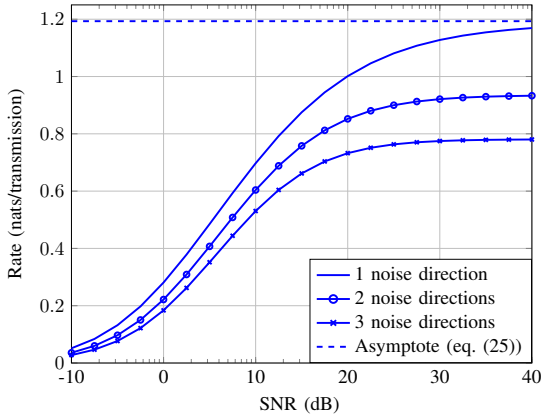

Figure 2: The achievable secrecy rate by AN under different numbers of artificial noise directions, for $N = 4$ and $\alpha = 1/5$.

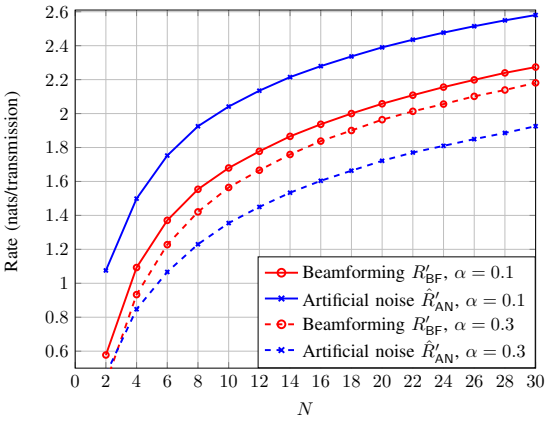

Figure 3: Secrecy rates versus N for an SNR of 50dB.

References

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

[2] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Info. Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[3] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," *IEEE Trans. on Info. Forensics and Security*, vol. 9, no. 11, pp. 1765–1779, Nov 2014.

[4] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. on Info. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. on Info. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

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

[7] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. on Info. Theory*, vol. 55, no. 9, pp. 4033–4039, Sept 2009.

[8] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. on Info. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct 2008.

[9] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. on Info. Forensics and Security*, vol. 7, no. 2, pp. 704–716, April 2012.

[10] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. on Wireless Communications*, vol. 10, no. 3, pp. 901–915, March 2011.

[11] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. on Signal Processing*, vol. 59, no. 1, pp. 351–361, Jan 2011.

[12] X. Zhou, Z. Rezki, B. Alomair, and M.-S. Alouini, "Achievable rates of secure transmission in gaussian miso channel with imperfect main channel estimation," *IEEE Trans. on Wireless Communications*, vol. 15, no. 6, pp. 4470–4485, June 2016.

[13] Z. Rezki, A. Chaaban, B. Alomair, and M.-S. Alouini, "The MISO wiretap channel with noisy main channel estimation in the high power regime," *IEEE Global Communications Conference (GLOBECOM)*, Dec. 2016 (to appear).

[14] Z. Rezki, B. Alomair, and M.-S. Alouini, "On the secrecy capacity of the MISO wiretap channel under imperfect channel estimation," in *IEEE Global Communications Conference (GLOBECOM)*, Austin, TX, Dec. 2014, pp. 1602–1607.