On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise

Ya-Lan Liang, Yung-Shun Wang, Tsung-Hui Chang, Y.-W. Peter Hong, and Chong-Yung Chi
Institute of Communications Engineering
National Tsing Hua University, Hsinchu, Taiwan
Email: {ylliang, yswang}@erdos.ee.nthu.edu.tw; changth@mx.nthu.edu.tw;
{ywhong, cychi}@ee.nthu.edu.tw

Abstract— **Physical-layer secrecy in wireless fading channels has been studied extensively in recent years to ensure reliable communication between the transmitter and the receiver subject to constraints on the information attainable by the eavesdropper. With multiple antennas at the transmitter, Goel and Negi proposed the use of artificial noise (AN) in the null space of the receiver's channel to corrupt the eavesdropper's reception, which helps guarantee secrecy without knowledge of the eavesdropper's channel. It has been shown that the secrecy capacity can be made arbitrarily large by increasing the transmission power, when perfect knowledge of the receiver's channel direction information (CDI) is available. However, in practice, this is not possible due to rate-limitations on the feedback channel. This paper studies the impact of quantized channel feedback on the secrecy capacity achievable with artificial noise. We show that, with imperfect CDI at the transmitter, the AN that was originally intended only for the eavesdropper may leak into the receiver's channel and limit the achievable secrecy rate. To maintain a constant performance degradation, the number of feedback bits must increase at least logarithmically with the transmission power. Moreover, we observe that the portion of power allocated to the transmission of AN should decrease as the number of quantization bits decreases to alleviate the degradation due to noise leakage.**

I. Introduction

Wireless networks have gained much popularity in recent years due to its ease of accessibility and mobility. However, owing to the broadcast nature of wireless media, wireless transmissions are often susceptible to eavesdropping and, therefore, the task of guaranteeing secrecy between legitimate transmitters and receivers are quite important, but difficult. In the past, these issues have mostly been addressed with application-layer cryptography which faces challenges in designing reliable encryption and key distribution algorithms.

Physical-layer secrecy was first introduced by Wyner [1] in the so called wiretap channels which consist of a transmitter, a legitimate receiver, and an eavesdropper. The notion of secrecy capacity is defined as the maximum achievable rate that the transmitter can reliably communicate with the legitimate receiver without allowing the eavesdropper to retrieve any information from the communication. It has been shown that, under perfect secrecy constraints, a non-zero secrecy capacity can be achieved in wireless environments thanks to the channel fading characteristics. With advances in multiple-input multiple-output (MIMO) technologies, the secrecy capacity achievable in wireless channels have been further enhanced with multiple antennas at the transmitters and/or at the receivers, e.g., in [2]–[5].

In [5], Goel and Negi proposed the use of artificial noise (AN) in the null space of the legitimate receiver's channel to disrupt the eavesdropper's reception. It has been shown that secrecy capacity can be made arbitrarily large by increasing the transmission power, even without knowledge of the eavesdropper's channel at the transmitter. Yet, perfect knowledge of the receiver's channel direction information (CDI) is required at the transmitter, although this is typically not attainable in practice. Our main contribution in this paper is then on the study of the impact of quantized CDI feedback on guaranteeing secrecy when using AN. The intuition is that, with only quantized CDI, the AN that was originally intended against the eavesdropper may leak into the legitimate receiver's channel and degrade the achievable secrecy capacity.

The impact of quantized channel feedback on transceiver design has been studied extensively in the literature for both single user and multi-user MIMO systems (without the presence of eavesdroppers). See [6]–[8] and [9], [10], respectively. Aiming at studying the effect of quantized channel feedback on secrecy capacity, we consider the case where the CDI at the transmitter is provided through a rate-limited feedback channel from the legitimate receiver. The CDI is first quantized into one of 2^B vectors in a quantization code book, and the corresponding index in the code book is sent back to the transmitter. We assume that the transmitter has multiple antennas but both the receiver and the eavesdropper have only a single antenna. The secrecy message is beamformed to the legitimate receiver according to the feedback quantized CDI, and AN is generated in the associated null space. We see that a significant decrease in secrecy capacity is observed due to the leakage of AN into the legitimate receiver's channel. To maintain a constant signal-to-interference-plus-noise ratio (SINR) degradation at the legitimate receiver, we show that the number of feedback bits B must increase logarithmically with the transmit power or linearly with the number of transmitter antennas. Moreover, to achieve the optimal performance, the power allocated to the transmission of AN should decrease as

This work was supported in part by the National Science Council, Taiwan, under Grants NSC-96-2628-E-007-012-MY2, NSC-97-3114-E-007-002, NSC-97-2219-E-007-001, NSC-97-2221-E-007-037, and NSC-97-2221-E-007-073-MY3.

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

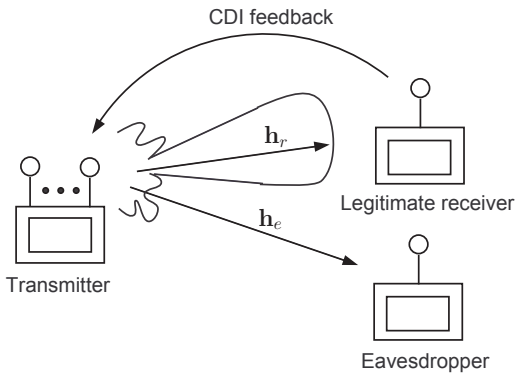

Figure 1. A network diagram consisting of a multi-antenna transmitter, a single-antenna legitimate receiver and eavesdropper. With the feedback CDI of the legitimate receiver, the transmitter transmits the secrecy message along this channel direction together with some artificial noise in its null space.

B decreases.

II. System Model and Background

Consider a network that consists of a multiple-antenna transmitter and a single-antenna legitimate receiver and eavesdropper, as shown in Figure 1. We assume that there are n_t antennas at the transmitter which transmits a data vector $\mathbf{x}[m] \in \mathbb{C}^{n_t}$ at time m. The signals observed at the receiver and the eavesdropper are respectively given by

$$y_r[m] = \mathbf{h}_r^T \mathbf{x}[m] + z_r[m], \quad (1)$$
$$y_e[m] = \mathbf{h}_e^T \mathbf{x}[m] + z_e[m], \quad (2)$$

where $\mathbf{h}_r, \mathbf{h}_e \in \mathbb{C}^{n_t}$ denote the channel vectors at the receiver and eavesdropper, respectively, and $z_r[m]$ and $z_e[m]$ are independent and identically distributed (i.i.d.) complex Gaussian noise with zero mean and unit variance, i.e., $z_r[m], z_e[m] \sim \mathcal{C}N(0,1)$. The transmitted signal $\mathbf{x}[m]$ satisfies the average power constraint

$$\mathbf{E}\left[||\mathbf{x}[m]||^2\right] \le P, \quad (3)$$

where $\mathbf{E}[\cdot]$ stands for the statistical expectation.

Suppose that the transmitter transmits a secret message w with rate R using a length-n codeword. The transmitted message w is assumed to be uniformly distributed within the index set $\mathcal{W}_n = \{1, 2, \ldots, 2^{nR}\}$. Each message is encoded into a length-n codeword $\{\mathbf{x}[m]\}_{m=1}^n$ and decoded at the legitimate receiver based on the observed sequence $\{y_r[m]\}_{m=1}^n$. With $\hat{w} \in \mathcal{W}_n$ being the decoded message, the error event can be defined as $\mathcal{E}_n = \{\hat{w} \neq w\}$. The information obtained by the eavesdropper is measured by the equivocation $I(w; \{y_e[m]\}_{m=1}^n)$.

Definition 1 (Secrecy Capacity [3], [11]) A secrecy rate, R, is achievable if there exists a sequence of $(2^{nR}, n)$ codes such that $\Pr(\mathcal{E}_n) \to 0$ and $I(w; \{y_e[m]\}_{m=1}^n)/n \to 0$ as $n \to \infty$. The *secrecy capacity*, denoted by $C_{\sec}$, is the supremum of all achievable secrecy rates, and is lower bounded by

$$\mathrm{C}_{\sec} \ge \mathrm{C}_{\sec,\mathrm{L}} \triangleq I(w; \{y_r[m]\}_{m=1}^n) - I(w; \{y_e[m]\}_{m=1}^n). \quad (4)$$

In [5], Goel and Negi proposed the use of artificial noise (AN) as a method to guarantee secrecy without knowledge of the eavesdropper's channel $\mathbf{h}_e$ at the transmitter. Specifically, this scheme proposes to transmit the signal along the direction of the legitimate receiver's channel $\mathbf{h}_r$ while imposing AN in the associated null space in order to corrupt the eavesdropper's reception. To illustrate this method, let us define

$$\mathbf{g}_r = \mathbf{h}_r / \|\mathbf{h}_r\| \quad (5)$$

as the channel direction information (CDI) of the legitimate receiver. Suppose that the transmitter has perfect knowledge of $\mathbf{g}_r$. In [5], the transmitted signal $\mathbf{x}[m]$ is proposed to be

$$\mathbf{x}[m] = \mathbf{g}_r^* u[m] + \mathbf{w}[m], \quad (6)$$

where $\{u[m]\}_{m=1}^n$ is the transmitted codeword with $u[m] \sim \mathcal{C}N(0, \sigma_u^2)$, and $\mathbf{w}[m]$ is the imposed AN. Let column vectors of $\mathbf{N}_g \in \mathbb{C}^{n_t \times (n_t - 1)}$ be an orthonormal basis of the null space of $\mathbf{g}_r^*$, i.e., $\mathbf{g}_r^T \mathbf{N}_g = \mathbf{0}^T$. The AN is generated by taking

$$\mathbf{w}[m] = \mathbf{N}_g \mathbf{v}[m], \quad (7)$$

where $\mathbf{v}[m]$ is an $(n_t - 1)$ vector of i.i.d. complex Gaussian random variables with distribution $\mathcal{C}N(0, \sigma_v^2)$. As a result, the signals observed at the legitimate receiver and the eavesdropper can be expressed respectively as

$$y_r[m] = \mathbf{h}_r^T \mathbf{g}_r^* u[m] + z_r[m], \quad (8)$$
$$y_e[m] = \mathbf{h}_e^T \mathbf{g}_r^* u[m] + \mathbf{h}_e^T \mathbf{w}[m] + z_e[m]. \quad (9)$$

According to (4), the secrecy capacity lower bound of (8) and (9) can be obtained as

$$\begin{aligned} \mathrm{C}_{\sec,\mathrm{L}} &= I(u; y_r) - I(u; y_e) \\ &= \log(1 + \mathbf{E}[\left|\mathbf{h}_r^T \mathbf{g}_r^* u[m]\right|^2]) - \log\left(1 + \frac{\mathbf{E}[\left|\mathbf{h}_e^T \mathbf{g}_r^* u[m]\right|^2]}{\mathbf{E}[\left|\mathbf{h}_e^T \mathbf{w}[m]\right|^2] + 1}\right) \\ &= \log(1 + \|\mathbf{h}_r\|^2 \sigma_u^2) - \log\left(1 + \frac{|\mathbf{h}_e^T \mathbf{g}_r^*|^2 \sigma_u^2}{\|\mathbf{h}_e^T \mathbf{N}_g\|^2 \sigma_v^2 + 1}\right). \end{aligned} \quad (10)$$

Notice that, since

$$\begin{aligned} \mathbf{E}[\|\mathbf{x}[m]\|^2] &= \mathbf{E}[\|\mathbf{g}_r^* u[m] + \mathbf{w}[m]\|^2] \\ &= \sigma_u^2 + (n_t - 1)\sigma_v^2 \le P, \end{aligned} \quad (11)$$

one can set $\sigma_u^2 = \alpha P$, and $\sigma_v^2 = \frac{(1-\alpha)P}{n_t - 1}$. By maximizing (10) over the value of $0 < \alpha \le 1$, the average secrecy capacity can be lower bounded as

$$\begin{aligned} (\mathbf{E}[\mathrm{C}_{\sec}])^+ \ge \max_{0<\alpha\le 1} \Bigg(\mathbf{E}\Bigg[&\log(1 + \|\mathbf{h}_r\|^2 \alpha P) \\ &- \log\left(1 + \frac{|\mathbf{h}_e^T \mathbf{g}_r^*|^2 \alpha P}{\|\mathbf{h}_e^T \mathbf{N}_g\|^2 (1-\alpha)/(n_t - 1) P + 1}\right) \Bigg] \Bigg)^+. \end{aligned} \quad (12)$$

Taking $P \to \infty$, one can see that

$$\lim_{P \to \infty} (\mathbf{E}[\mathrm{C}_{\sec}])^+ = \infty, \quad (13)$$

implying that high secrecy capacity can be achieved if the transmit power P is large.

III. Secrecy Capacity with Imperfect CDI

In [5], the use of AN was proposed by assuming that perfect knowledge of the legitimate receiver's CDI is available at the transmitter. However, this is not achievable in practice due to limitations in the feedback channel. In particular, the receiver is limited to a finite number of feedback bits, say B, to the transmitter, and thereby only the quantized version of CDI is available at the transmitter. This section studies the impact of limited channel feedback on the secrecy capacity. In the first subsection, the secrecy capacity lower bound under quantized CDI at the transmitter is derived. In the second subsection, the performance degradation due to imperfect CDI is analyzed.

A. Secrecy Capacity with Quantized CDI

Following the studies on quantized channel feedback given in [9] and [10] , we assume that the legitimate receiver knows perfectly its own CDI but sends back only the quantization of it to the transmitter. Specifically, suppose that the CDI $\mathbf{g}_r$ is quantized into one of 2^B unit-norm channel vectors in the code book $\mathcal{C} \triangleq \{\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_{2^B}\}$, and the corresponding index is sent back to the transmitter. The quantization vector is chosen according to the minimum distance criterion [9] so that the feedback index is given by

$$\ell^\star = \arg \max_{\ell=1,...,2^B} |\mathbf{g}_r^H \mathbf{c}_\ell|. \tag{14}$$

We define the quantized CDI vector as $\hat{\mathbf{g}}_r \triangleq \mathbf{c}_{\ell^\star}$ and rewrite the actual CDI vector as

$$\mathbf{g}_r = (\hat{\mathbf{g}}_r^H \mathbf{g}_r)\hat{\mathbf{g}}_r + \hat{\mathbf{g}}_r^\perp, \tag{15}$$

where $\hat{\mathbf{g}}_r^\perp$ is the projection of $\mathbf{g}_r$ onto the orthogonal complement subspace of $\hat{\mathbf{g}}_r$ (thus $(\hat{\mathbf{g}}_r^\perp)^H \hat{\mathbf{g}}_r = 0$). Notice that $\mathbf{g}_r$ can also be expressed as

$$\mathbf{g}_r = \hat{\mathbf{g}}_r \cos\theta + \tilde{\mathbf{g}}_r \sin\theta, \tag{16}$$

where $\cos\theta = |\hat{\mathbf{g}}_r^H \mathbf{g}_r|$ (which basically approaches one as B increases) and $\tilde{\mathbf{g}}_r = (\mathbf{g}_r - \hat{\mathbf{g}}_r \cos\theta)/\sin\theta$.

With the quantized CDI at the transmitter, it follows from (6) and (7) and that the transmitted signal vector becomes

$$\mathbf{x}[m] = \hat{\mathbf{g}}_r^* u[m] + \hat{\mathbf{N}}_g \mathbf{v}[m], \tag{17}$$

where $\hat{\mathbf{N}}_g \in \mathbb{C}^{n_t \times n_t - 1}$ contains an orthonormal basis of the null space of $\hat{\mathbf{g}}_r^*$ (i.e., $\hat{\mathbf{g}}_r^T \hat{\mathbf{N}}_g = \mathbf{0}^T$). Hence, the signal observed by the legitimate receiver is given by

$$\begin{aligned} y_r[m] &= (\mathbf{h}_r^T \hat{\mathbf{g}}_r^*) u[m] + \mathbf{h}_r^T \hat{\mathbf{N}}_g \mathbf{v}[m] + z_r[m] \\ &= \|\mathbf{h}_r\| (\hat{\mathbf{g}}_r^H \mathbf{g}_r) \cdot u[m] \\ &\qquad + \|\mathbf{h}_r\| \sin\theta \cdot \left(\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g \mathbf{v}[m]\right) + z_r[m], \end{aligned} \tag{18}$$

where in the second equality we have applied (15) and (16) to the first and second terms, respectively. We observe from (18) that the AN is leaked into the legitimate receiver's channel, thus degrading the achievable secrecy capacity. For this case, the secrecy capacity lower bound can be shown to be

$$\begin{aligned} \widehat{\mathrm{C}}_{\mathrm{sec,L}} \triangleq \log &\left(1 + \frac{\|\mathbf{h}_r\|^2 (\cos\theta)^2 \cdot \alpha P}{\|\mathbf{h}_r\|^2 \cdot (\sin\theta)^2 \|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\|^2 \left(\frac{1-\alpha}{n_t - 1}\right) P + 1}\right) \\ &- \log \left(1 + \frac{\left|\mathbf{h}_e^T \hat{\mathbf{g}}_r\right|^2 \cdot \alpha P}{\|\mathbf{h}_e^T \hat{\mathbf{N}}_g\|^2 \left(\frac{1-\alpha}{n_t - 1}\right) P + 1}\right). \end{aligned} \tag{19}$$

It is interesting to observe from (19) that, as $P \to \infty$, $\widehat{\mathrm{C}}_{\mathrm{sec,L}}$ converges to a finite value given by

$$\begin{aligned} \lim_{P \to \infty} \widehat{\mathrm{C}}_{\mathrm{sec,L}} = \log &\left(1 + \frac{\alpha (\cos\theta)^2}{\|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\|^2 (\sin\theta)^2 (1-\alpha)/(n_t - 1)}\right) \\ &- \log \left(1 + \frac{|\mathbf{h}_e^T \hat{\mathbf{g}}_r|^2 \alpha}{\|\mathbf{h}_e^T \hat{\mathbf{N}}_g\|^2 (1-\alpha)/(n_t - 1)}\right) \end{aligned} \tag{20}$$

because the amount of noise leakage also increases with P. This is in strong contrast to the result in (13) and [5] where, with perfect CDI, the secrecy capacity can be made arbitrarily large by increasing P. Two remarks regarding the above analysis are given as follows.

Remark 1 One can see from (19) and (20) that the optimal value of α varies with the accuracy of the channel quantization (i.e., the value of $\cos\theta$). In fact, as the number of feedback bits B decreases, less power should be allocated to transmitting AN since the noise leakage would be more severe. This will be illustrated through computer simulations in Section IV.

Remark 2 From (10) and (19), one can see that, for a fixed quantization accuracy, the difference between $\mathrm{C}_{\mathrm{sec,L}}$ and $\widehat{\mathrm{C}}_{\mathrm{sec,L}}$ goes to infinity as $P \to \infty$. To keep this difference a finite constant, intuitively the number of feedback bits B should be increased along with the transmit power P. Indeed, we will show in the next subsection that B has to be scaled up at least logarithmically with P in order to maintain a constant performance degradation.

B. Analysis of Performance Degradation

In the subsection, we first show that the average secrecy capacity loss due to imperfect CDI

$$\Delta \mathrm{C}_{\mathrm{sec,L}} \triangleq \left(\mathbf{E}[\mathrm{C}_{\mathrm{sec,L}}]\right)^+ - \left(\mathbf{E}[\widehat{\mathrm{C}}_{\mathrm{sec,L}}]\right)^+ \tag{21}$$

is upper bounded by a function which depends only on the SINR at the legitimate receiver. Second, we show that B has to be increased at least logarithmically with P or linearly with n_t in order to maintain a constant average SINR degradation.

To this end, it is noted from [9] that, for any two independent and isotropically distributed unit-norm vectors $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{C}^{n_t}$, the inner product $|\mathbf{w}_1^T \mathbf{w}_2|^2$ is a Beta-distributed random variable with parameters $(1, n_t - 1)$, which is denoted by $\beta(1, n_t - 1)$. The mean of the Beta random variable is $\mathbf{E}[\beta(1, n_t - 1)] = 1/n_t$. Since $\hat{\mathbf{g}}_r$ and $\mathbf{h}_e$ are independent

and isotropically distributed in $\mathbb{C}^{n_t}$, we have in the second term in (10) that

$$|\mathbf{h}_e^T \hat{\mathbf{g}}_r^*|^2 = \|\mathbf{h}_e\|^2 \beta(1, n_t - 1). \quad (22)$$

Similarly, with $\mathbf{h}_e$ being independent of each column of $\hat{\mathbf{N}}_g$, we can write that

$$\left\|\mathbf{h}_e^T \hat{\mathbf{N}}_g\right\|^2 = \|\mathbf{h}_e\|^2 \sum_{j=1}^{n_t-1} \beta(1, n_t - 1). \quad (23)$$

The above arguments hold also for the second term in (19). Therefore, we observe that the second term in (10) and that in (19) are identically distributed. Besides, one can easily see that the first term in (10) is always greater and equal to that in (19). Thus we can upper bound (21) as

$$\Delta \mathrm{C}_{\mathrm{sec,L}} \leq \mathbf{E}[\log(1 + \|\mathbf{h}_r\|^2 \cdot \alpha P)] - \mathbf{E}\left[\log\left(1 + \frac{\|\mathbf{h}_r\|^2 (\cos\theta)^2 \cdot \alpha P}{\|\mathbf{h}_r\|^2 \left\|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\right\|^2 (\sin\theta)^2 \left(\frac{P(1-\alpha)}{n_t - 1}\right) + 1}\right)\right],$$

which implies that the worst secrecy capacity degradation is caused only by the SINR decrease at the legitimate receiver. It is worthwhile to remark that the above upper bound is tight when $(\mathbf{E}[\widehat{\mathrm{C}}_{\mathrm{sec,L}}])^+ > 0$, which typically happens when P or B is large. From the above analysis, we therefore investigate the average ratio between the legitimate receiver's SINR under perfect CDI and that under quantized CDI, i.e.,

$$\Delta\mathrm{SINR} = \mathbf{E}\left[\frac{\|\mathbf{h}_r\|^2 \left\|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\right\|^2 (\sin\theta)^2 \left(\frac{1-\alpha}{n_t-1}\right) P + 1}{(\cos\theta)^2}\right] \geq \mathbf{E}\left[\frac{\|\mathbf{h}_r\|^2 \left\|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\right\|^2 \left(\frac{1-\alpha}{n_t-1}\right) P}{(\cot\theta)^2}\right]. \quad (24)$$

To further analyze (24), let us consider the quantization cell approximation model used in [8]–[10], where it is assumed that each quantization cell is a Voronoi region of a spherical cap with surface area approximately equal to 2^{-B} of the total surface area of the n_t-dimensional unit sphere. For a given codebook $\mathcal{C} \triangleq \{\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_{2^B}\}$, the quantization cell for each vector, say $\mathbf{c}_i$, is given by

$$\mathcal{R}_i = \{\mathbf{g}_r : |\mathbf{g}_r^H \mathbf{c}_i|^2 \geq |\mathbf{g}_r^H \mathbf{c}_j|^2, \forall j \neq i\}. \quad (25)$$

In the quantization cell approximation model, $\mathcal{R}_i$ is instead approximated with

$$\mathcal{R}_i \approx \{\mathbf{g}_r : |\mathbf{g}_r^H \mathbf{c}_i|^2 \geq 1 - \delta\}, \quad (26)$$

where $\delta = 2^{-\frac{B}{n_t-1}}$ so that $\Pr(\mathcal{R}_i) = 2^{-B}$. With this approximation model, the $\|\mathbf{h}_r\|^2$, $\|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\|^2$ and $\cot\theta$ in (24) are statistically independent [9], and thus the SINR degradation $\Delta\mathrm{SINR}$ can be lower bounded as

$$\Delta\mathrm{SINR} \geq \mathbf{E}\left[\|\mathbf{h}_r\|^2\right] \cdot \mathbf{E}\left[\left\|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\right\|^2\right] \cdot \frac{1}{\mathbf{E}\left[(\cot\theta)^2\right]} \cdot \left(\frac{(1-\alpha)P}{n_t - 1}\right), \quad (27)$$

where we have applied Jensen's inequality to the third term. In addition, the probability density function of $\cot^2\theta$ can be shown to be [9]

$$f_{\cot^2\theta}(x) = \begin{cases} \frac{2^B(n_t-1)}{(x+1)^{n_t}}, & x > \delta^{-1} - 1, \\ 0, & 0 < x < \delta^{-1} - 1, \end{cases} \quad (28)$$

and, for $n_t > 2$, its expectation can be computed as

$$\mathbf{E}[\cot^2\theta] = \left[\left(\frac{3 - n_t}{2 - n_t}\right) \cdot 2^{\frac{B}{n_t-1}}\right] - 1. \quad (29)$$

Since both $\tilde{\mathbf{g}}_r$ and each column of $\hat{\mathbf{N}}_g$ are isotropically distributed in the $(n_t - 1)$-dimensional null space of $\hat{\mathbf{g}}_r$, we have as in [10] that

$$\left\|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\right\|^2 = \sum_{j=1}^{n_t-1} \beta(1, n_t - 2) \quad (30)$$

(i.e., sum of Beta-distribution random variables each with parameters $(1, n_t - 2)$), and hence

$$\mathbf{E}\left[\left\|\tilde{\mathbf{g}}_r^T \hat{\mathbf{N}}_g\right\|^2\right] = 1. \quad (31)$$

Substituting (29) and (31) into (27) gives rise to

$$\Delta\mathrm{SINR} \geq \frac{\mathbf{E}\left[\|\mathbf{h}_r\|^2\right] \left(\frac{1-\alpha}{n_t-1}\right) P}{\left[\left(\frac{3-n_t}{2-n_t}\right) \cdot 2^{\frac{B}{n_t-1}}\right] - 1}. \quad (32)$$

By reordering the terms, we obtain for $n_t > 2$,

$$B \geq (n_t - 1)\left[\log_2\left(\frac{(1-\alpha)P}{n_t - 1} \cdot \frac{\mathbf{E}\left[\|\mathbf{h}_r\|^2\right]}{\Delta\mathrm{SINR}} + 1\right) - \log_2\left(\frac{3-n_t}{2-n_t}\right)\right]. \quad (33)$$

Remark 3 Equation (33) shows that the number of feedback bits B must increase with the order of $O(\log_2 P)$ in order to maintian a constant SINR degradation. Moreover, since $\mathbf{E}\left[\|\mathbf{h}_r\|^2\right]$ is proportional to n_t, with fixed P and $\Delta\mathrm{SINR}$, B must scale linearly with n_t.

IV. Simulation Results and Discussions

In this section, we present simulation results to illustrate the impact of quantized CDI feedback on the secrecy capacity. We set the number of transmit antennas n_t to 4, and the channel vectors $\mathbf{h}_r$ and $\mathbf{h}_e$ as i.i.d. complex Gaussian random variables with zero mean and unit variance. The secrecy capacity lower bound with perfect CDI and that with quantized CDI were evaluated by (10) and (19), respectively. Given a number of feedback bits B, the quantization code book proposed in [12] was used in our simulation. The SNR was defined as the transmit power P ($\mathrm{SNR} = P$), and each simulation result was obtained by averaging over 1500 channel realizations.

Figures 2 and 3 present the simulation results of average secrecy capacity lower bound (bits/pcu) versus α for SNR= 20 dB, and versus SNR for $\alpha = 0.9$, respectively. The average secrecy capacity loss due to imperfect CDI can be

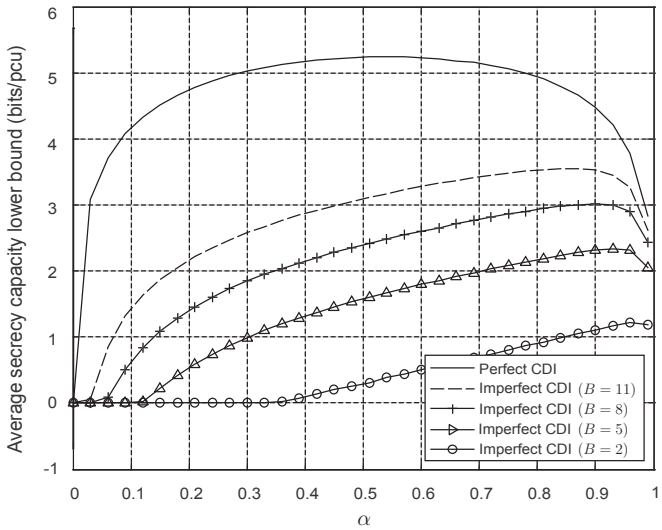

Figure 2. Simulation results of secrecy capacity lower bound versus α with AN for SNR$=$ 20 dB.

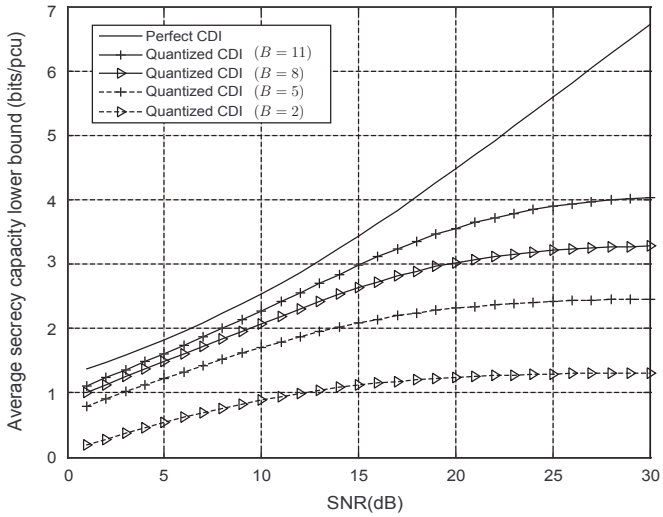

Figure 3. Simulation results of secrecy capacity lower bound versus SNR with AN for $\alpha = 0.9$.

observed from these figures. From Figure 2, it is noticed that the optimal α (which maximizes the secrecy capacity lower bound) increases with decreased B. Moreover, we observe that the performance is more sensitive to the value of α under quantized CDI. From Figure 3, we can see that the secrecy capacity lower bound with imperfect CDI is upper limited to a ceiling with respective to SNR, in sharp contrast to that with perfect CDI. To verify our analysis in Section III-B, simulation results of average secrecy capacity lower bound versus SNR for $\alpha = 0.9$ is presented in Figure 4. Instead of being fixed, B was increased with SNR according to (33) for both ΔSINR equal to 1.5 and 3. The results without using AN ($\alpha = 1$) were also presented. As seen from this figure, the average secrecy capacity loss due to imperfect CDI remains almost constant for different SNR values. We can also observe from this figure that the advantages of using AN for physical-layer secrecy is still significant even with quantized CDI.

In summary, we have presented the effect of quantized channel feedback on the secrecy capacity achievable using AN. We have shown that the average secrecy capacity loss depends only on the SINR at the legitimate receiver. Moreover, to maintain a constant SINR degradation, we have also shown that the number of feedback bits must increase at least logarithmically with the transmit power.

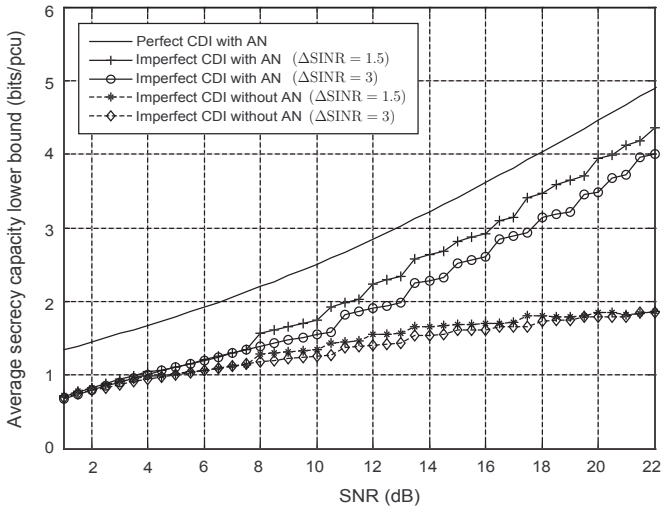

Figure 4. Simulation results of secrecy capacity lower bound versus SNR with AN for $\alpha = 0.9$ and without AN ($\alpha = 1$). The number of feedback bits was increased with SNR according to (33).

REFERENCES

[1] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[2] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," *Proc. IEEE ISIT*, Nice, France, June 24-29, 2007, pp. 2471–2475.

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *submitted to IEEE Trans. Inf. Theory*, 2008.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Proc. IEEE ISIT*, Toronto, ON, Canada, July 6-11, 2008, pp. 524–528.

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

[6] A. Narula, M. J. Lopez, M. D. Trott, and G. W. Wornell, "Efficient use of side information in multiple-antenna data transmission over fading channels," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1423–1436, Oct. 1998.

[7] D. Love, R. H. Jr., and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[8] K. Mukkavilli, A. Sabharwal, E. Erkip, and B. Aazhang, "On beamforming with finite rate feedback in multiple-antenna systems," *IEEE Trans. Inf. Theory*, vol. 49, pp. 2562–2579, Oct. 2003.

[9] T. Yoo, N. Jindal, and A. Goldsmith, "Multi-antenna downlink channels with limited feedback and user selection," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 7, pp. 1478–1491, Sep. 2007.

[10] N. Jindal, "MIMO broadcast channels with finite-rate feedback," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5045–5060, Nov. 2006.

[11] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Rur. Trans. Telecomm.*, vol. 10, no. 6, pp. 585–596, Nov. 1999.

[12] Y. Linde, A. Buzo, and R. M.Gary, "An algorithm for vector quantizer design," *IEEE Trans. Commun.*, vol. 28, no. 1, pp. 84–95, Jan. 1980.