This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceedings

On the Impact of Quantized Channel Direction Feedback in Multiple-Antenna Wiretap Channels

Shih-Chun Lin, Tsung-Hui Chang, Y.-W. Peter Hong, and Chong-Yung Chi
Institute of Communications Engineering and Department of Electrical Engineering,
National Tsing Hua University, Hsinchu, Taiwan 30013, R.O.C.
{linsc, changth}@mx.nthu.edu.tw, {ywhong, cychi}@ee.nthu.edu.tw

***Abstract*—In this work, we examine the impact of quantized channel direction feedback on the achievable secrecy rate of multiple-antenna wiretap channels. To guarantee secrecy without knowledge of the eavesdropper's channel, we consider the transmission scheme proposed by Goel and Negi where artificial noise (AN) is imposed in the null space of the legitimate receiver's channel to disrupt the eavesdropper's reception. When perfect knowledge of the legitimate receiver's channel direction information (CDI) is available at the transmitter, the secrecy rate can be made arbitrarily large by increasing the transmission power. However, perfect CDI is difficult to achieve in practice due to rate-limitations on the feedback channel. When only quantized CDI is available at the transmitter, the AN that is only intended to disrupt the eavesdropper's reception may leak into the legitimate receiver's channel, causing significant loss in secrecy rate. In fact, we show that the achievable secrecy rate under quantized CDI is bounded by a constant even as the transmission power increases. To guarantee a constant rate loss compared to the perfect CDI case, we show that the number of feedback bits must scale at least logarithmically with the transmission power. These theoretical claims are verified by computer simulations.**

I. Introduction

Physical-layer secrecy was first introduced by Wyner under the notion of wiretap channels in [1]. Here, the secrecy rate between a source and a legitimate receiver has been examined under constraints on the information attainable by the eavesdropper. Recent studies of physical-layer secrecy in the wireless channel have shown that, under perfect secrecy constraints, a non-zero secrecy capacity can always be achieved in fading environments [2] [3]. Even when knowledge of the eavesdropper's channel is not available at the transmitter, Goel and Negi [4] showed that perfect secrecy can still be guaranteed by imposing artificial noise (AN) in the null space of the legitimate receiver's channel to disrupt the eavesdropper's reception. It has been shown that the secrecy rate achievable in this case can be made arbitrarily large by increasing the transmission power. However, this result relies on perfect knowledge of the legitimate receiver's channel direction information (CDI) at the transmitter, which is generally not attainable in practice.

The main contribution of this paper is to study the impact of quantized CDI on the achievable secrecy rate under AN-assisted beamforming. Although the optimal signaling scheme is unknown for cases where knowledge of the eavesdropper's channel is unavailable, AN-assisted beamforming is asymptotically optimal at high SNR for systems with large number of transmit antennas [5]. Thus, it serves as a promising technique for practical implementation. However, to utilize AN effectively without causing interference to the legitimate receiver, AN must be placed perfectly in the null space of the legitimate receiver's channel. When only quantized CDI is available at the transmitter, AN that was originally intended to disrupt the eavesdropper's reception may leak into the legitimate receiver's channel, causing significant loss in the achievable secrecy rate. In this paper, we characterize the secrecy rate loss due to noise leakage and determine the number of feedback bits needed to achieve a constant rate loss. We first focus our studies on the multiple-input single-output single-eavesdropper (MISOSE) channel, where the transmitter has multiple antennas but both the receiver and the eavesdropper have only a single antenna. Our results are then extended to the multiple-input multiple-output multiple-eavesdropper (MIMOME) channel where the receiver and eavesdropper are equipped with multiple antennas as well.

Specifically, due to the effect of noise leakage, we first show that the secrecy rate achievable under quantized CDI is upper-bounded by a constant when the number of feedback bits B is fixed. This property differs from that of the perfect CDI case, where the secrecy rate can increase without bound by increasing the transmission power [4]. To maintain a constant rate loss compared to the perfect CDI case, we show that the number of feedback bits B must scale logarithmically with the transmission power P and linearly with the number of transmitter antennas for the MISOSE case. This result is extended to the MIMOME case, where the number of feedback bits B is also shown to scale logarithmically with P. Our results for the MISOSE case improves the bit scaling law in [10] by removing non-necessary approximation steps. The effect of quantized channel feedback on transceiver design has been studied extensively in the literature for conventional single user and multi-user multiple-input, multiple-output (MIMO) downlink systems (without eavesdroppers), e.g., in [7]–[9] and references within. However, these issues have not been addressed before in the context of physical layer secrecy.

In the following, we introduce the notations used throughout this paper. Specifically, $\mathcal{CN}(0, \sigma^2)$ denotes the distribution of a complex Gaussian random variable with mean 0 and variance σ^2 and $\beta(a, b)$ denotes a beta-distributed random variable

This work was supported by the National Science Council, Taiwan, R.O.C., under grant NSC-98-2219-E-007-004, NSC-98-2218-E-009-008-MY3, NSC-98-2219-E-007-005 and NSC-98-2219-E-007-003.

978-1-4244-6404-3/10/$26.00 ©2010 IEEE

with parameters (a, b). Moreover, $\mathbf{E}[\cdot]$ stands for the statistical expectation of a random variable and $I(;)$ represents the mutual information between two random variables (vectors). Almost-sure convergence is denoted by $\overset{a.s.}{\rightarrow}$. The function $[x]^+$ is equal to x when $x \geq 0$ and is equal to 0, otherwise. The Euclidean norm of a vector $\mathbf{x}$ is denoted by $\|\mathbf{x}\|$ and the determinant of a square matrix $\mathbf{A}$ is denoted by $|\mathbf{A}|$.

II. System Model and Background

A. Channel and signaling method

Consider a network that consists of a transmitter, a legitimate receiver and an eavesdropper. Suppose that there are n_t antennas at the transmitter, n_r antennas at the legitimate receiver and n_e antennas at the eavesdropper, where $n_t > n_r$ and $n_t \geq n_e$. In this section, we first consider the MISOSE case where $n_e = n_r = 1$ and later extend the results to the MIMOME case, where $n_e \geq 1$ and $n_r \geq 1$, in Section IV. At time i, the transmitter sends a data vector $\mathbf{x}[i] \in \mathbb{C}^{n_t}$, where $\mathbf{E}\left[\|\mathbf{x}[i]\|^2\right] \leq P$. The signals received at the receiver and the eavesdropper are given by

$$y_r[i] = \mathbf{h}_r^H \mathbf{x}[i] + z_r[i], \quad (1)$$

$$y_e[i] = \mathbf{h}_e^H \mathbf{x}[i] + z_e[i], \quad (2)$$

respectively, where $\mathbf{h}_r, \mathbf{h}_e \sim \mathcal{CN}(\mathbf{0}_{n_t \times 1}, \mathbf{I}_{n_t \times n_t})$ are the ergodic fading channel vectors at the receiver and eavesdropper, respectively, and $z_r[i]$, $z_e[i]$ are independent and identically distributed (i.i.d.) complex Gaussian noise. The channel vectors are assumed to remain constant for a sufficient amount of time for feedback, but only a quantized version of $\mathbf{h}_r$ is assumed to be available at the transmitter whereas perfect knowledge is available for both the legitimate receiver and the eavesdropper. Moreover, we assume that the distribution of $z_r[i]$, given by $\mathcal{CN}(0, 1)$, is known at the transmitter, but the variance of $z_e[i]$ is assumed to be unknown. To guarantee secrecy under these assumptions, we consider the worst case scenario where the variance of $z_e[i]$ is set to zero [4].

Suppose that the transmitter sends a secret message W using a length-n codeword $\mathbf{x}^n \triangleq \{\mathbf{x}[i]\}_{i=1}^n$ with rate R. A perfect secrecy rate R is achievable if the average error probability at the legitimate receiver approaches zero as $n \rightarrow \infty$, while no information regarding W is attainable at the eavesdropper. The message is coded across multiple coherence intervals and the number of channel usage within each coherence interval is assumed to be large enough to invoke random coding arguments (c.f. [2]). Due to the lack of knowledge on $\mathbf{h}_e$, the optimal signaling for the described MISOSE channel is unknown except for very limited cases [2] [5]. Hence, we focus our studies on the AN-assisted beamforming scheme [4], which is asymptotically optimal at high SNR for systems with large number of transmit antennas [5].

Specifically, under AN-assisted beamforming, the transmitted signal can be written as

$$\mathbf{x}[i] = \mathbf{p}s[i] + \mathbf{Q}\mathbf{a}[i], \quad (3)$$

where $s[i]$ is the message-bearing signal with power $\mathbf{E}[|s[i]|^2] = P_s$, $\mathbf{p} \in \mathbb{C}^{n_t \times 1}$ is normalized beamforming vector for sending $s[i]$, and $\mathbf{Q}\mathbf{a}[i]$ is the imposed AN. Here, $\mathbf{Q} \in \mathbb{C}^{n_t \times (n_t - 1)}$ is the AN beamformer with orthonormal columns that form the AN subspace and $\mathbf{a}[i] = [a_0[i], \ldots, a_{n_t-2}[i]]^T$ is an $(n_t - 1) \times 1$ vector with $i.i.d.$ components, where each component is distributed as $\mathcal{CN}(0, P_a)$. The AN $\mathbf{a}[i]$ is independent of $s[i]$. Beamformers $\mathbf{p}$ and $\mathbf{Q}$ are determined by available channel feedback. By considering the worst case scenario where the eavesdropper is not subject to additive noise, the signals received at the legitimate receiver and the eavesdropper are respectively given by

$$\begin{aligned} y_r[i] &= \mathbf{h}_r^H \mathbf{p}s[i] + \mathbf{h}_r^H \mathbf{Q}\mathbf{a}[i] + z_r[i] \\ y_e[i] &= \mathbf{h}_e^H \mathbf{p}s[i] + \mathbf{h}_e^H \mathbf{Q}\mathbf{a}[i]. \end{aligned} \quad (4)$$

Since the vector $\mathbf{p}$ and each column of $\mathbf{Q}$ are of unit norm, the transmit power constraint can be written as

$$\mathbf{E}[\|\mathbf{x}[i]\|^2] = P_s + (n_t - 1)P_a \leq P.$$

Thus, we set the powers of $s[i]$ and $a_\ell[i]$, for $\ell = 0, \ldots, n_t - 2$, as $P_s = \alpha P$ and $P_a = \frac{1-\alpha}{n_t - 1} P$, respectively. That is, α portion of power is allocated to the signal and $(1 - \alpha)$ to the AN. By [1], [2], the following perfect secrecy rate is achievable under the ergodic block-fading channel

$$(\mathbf{E}[I(s; y_r|\mathbf{h}_r) - I(s; y_e|\mathbf{h}_r, \mathbf{h}_e)])^+. \quad (5)$$

Moreover, it is worthwhile to remark that, when the signal received by the eavesdropper is noiseless, a non-zero secrecy rate cannot be achieved without imposing AN since y_r will always be "noisier" than y_e, regardless of the channel state.

B. Review of secrecy rate with perfect CDI

In this section, we briefly review the results of AN-assisted beamforming that is obtained with perfect knowledge of the CDI of $\mathbf{h}_r$ [4]. Specifically, the CDI of $\mathbf{h}_r$ is defined as

$$\mathbf{g}_r = \mathbf{h}_r / \|\mathbf{h}_r\|. \quad (6)$$

In this case, the beamformers in (3) are chosen as $\mathbf{p} = \mathbf{g}_r$ and $\mathbf{Q} = \mathbf{N}_g$, where the columns of $\mathbf{N}_g$ form an orthonormal basis for the left null space of $\mathbf{g}_r$. Thus, the transmitted signal is given by

$$\mathbf{x}[i] = \mathbf{g}_r s[i] + \mathbf{N}_g \mathbf{a}[i]. \quad (7)$$

Since $\mathbf{g}_r^H \mathbf{N}_g = \mathbf{0}_{1 \times (n_t - 1)}$, the received signal at the legitimate user can be expressed as

$$\tilde{y}_r[i] = \mathbf{h}_r^H \mathbf{g}_r s[i] + z_r[i]. \quad (8)$$

With Gaussian input distribution, i.e., $s[i] \sim \mathcal{CN}(0, \alpha P)$, the achievable secrecy rate given in (5) becomes

$$R_s(\alpha) = \left(\mathbf{E}\left[\log(1 + \|\mathbf{h}_r\|^2 \alpha P) - \log\left(1 + \frac{|\mathbf{h}_e^H \mathbf{g}_r|^2 \alpha}{\|\mathbf{h}_e^H \mathbf{N}_g\|^2 \frac{1-\alpha}{n_t - 1}}\right)\right]\right)^+. \quad (9)$$

Since the second term is a constant with respect to P, one can observe that the secrecy rate obtained under perfect CDI increases without bound as P goes to infinity.

III. MISOSE Secrecy Rate with Quantized CDI

In this section, we consider the case where the transmitter has multiple antennas $n_t > 1$, but the legitimate receiver and eavesdropper have only one receive antenna, i.e., $n_r = n_e = 1$.

A. Feedback model

Following the studies on quantized channel feedback given in [7] and [8], we assume that the legitimate receiver feeds back a quantized version of the CDI to the transmitter in each coherence interval whereas the channel quality information (CQI) is assumed to be unknown. Suppose that the CDI $\mathbf{g}_r$ is quantized into one of 2^B unit-norm channel vectors in the codebook $\mathcal{C} \triangleq \{\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_{2^B}\}$, and the corresponding index is sent back to the transmitter. The quantization vector is chosen according to the minimum distance criterion [7] (or equivalently the maximum correlation criterion), in which case, the feedback index and quantized CDI vector are respectively given by

$$\ell^\star = \arg \max_{\ell=1,...,2^B} \|\mathbf{g}_r^H \mathbf{c}_\ell\|, \text{ and } \hat{\mathbf{g}}_\mathrm{r} \triangleq \mathbf{c}_{\ell^\star}.$$

To gain analytical insights on the problem, we shall conduct our studies based on the random vector quantization (RVQ) codebook [7], [8], where each codeword is randomly and independently generated as an n_t-dimensional unit-norm complex Gaussian vector. Moreover, we will also resort to quantization cell approximation model used in [7] [8] [11]. Each quantization cell is approximated by 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. This model has been shown to closely approximate the behavior of RVQ in [7], [8]. The details can be found in [7] [8] [11].

B. Achievable secrecy rate under quantized CDI

In this section, we study the effect of quantized feedback on the achievable secrecy rate under AN-assisted beamforming, as given in (3) [1]. Unlike the perfect CDI case presented in (9), this secrecy rate will be bounded by a constant, even at high SNR, due to the effects of noise leakage.

Specifically, when only quantized CDI $\hat{\mathbf{g}}_r$ is available at the transmitter, the beamformers are instead chosen as $\mathbf{p} = \hat{\mathbf{g}}_r$ and $\mathbf{Q} = \hat{\mathbf{N}}_g$, where the columns of $\hat{\mathbf{N}}_g$ form an orthonormal basis for the left null space of $\hat{\mathbf{g}}_r$. The transmitted signal is

$$\mathbf{x}[i] = \hat{\mathbf{g}}_r s[i] + \hat{\mathbf{N}}_g \mathbf{a}[i]. \tag{10}$$

By (4) and the fact that $\hat{\mathbf{g}}_r^H \hat{\mathbf{N}}_g = \mathbf{0}$, the signals at the legitimate receiver and eavesdropper can be written as

$$\begin{aligned} \bar{y}_r[i] &= \|\mathbf{h}_r\|(\mathbf{g}_r^H \hat{\mathbf{g}}_r) \cdot s[i] + \|\mathbf{h}_r\|(\mathbf{g}_r^H \hat{\mathbf{N}}_g)\mathbf{a}[i] + z_r[i], \quad (11) \\ \bar{y}_e[i] &= \mathbf{h}_e^H \hat{\mathbf{g}}_r s[i] + \mathbf{h}_e^H \hat{\mathbf{N}}_g \mathbf{a}[i]. \end{aligned}$$

We observe from (11) that an additional interference occurs at the legitimate receiver due to noise leakage, causing a loss in the achievable secrecy rate. Similar to (9), the achievable secrecy rate is given by

$$R_{s,q}(\alpha) = \left(\mathbf{E}\Big[\log\left(1 + \frac{\|\mathbf{h}_r\|^2 (\cos\theta)^2 \cdot \alpha P}{\|\mathbf{h}_r\|^2 \cdot (\sin\theta)^2 \frac{1-\alpha}{n_t - 1} P + 1}\right) - \log\left(1 + \frac{\left|\mathbf{h}_e^H \hat{\mathbf{g}}_r\right|^2 \cdot \alpha}{\|\mathbf{h}_e^H \hat{\mathbf{N}}_g\|^2 \frac{1-\alpha}{n_t - 1}}\right)\Big]\right)^+, \tag{12}$$

where $\cos\theta = |\mathbf{g}_r^H \hat{\mathbf{g}}_r|$. Note that $\sin\theta = \|\mathbf{g}_r^H \hat{\mathbf{N}}_g\|$ since $\|\mathbf{g}_r^H \hat{\mathbf{g}}_r\|^2 + \|\mathbf{g}_r^H \hat{\mathbf{N}}_g\|^2 = 1$. In this case, the rate converges to a constant as P goes to infinity, which is in strong contrast to that of the perfect CDI case (c.f. (9)). Therefore, to maintain a constant secrecy rate loss compared to the perfect CDI case, one must increase the number of feedback bits as P increases.

C. Number of feedback bits scaling law

In this section, we derive the number of feedback bits B needed to achieve a constant secrecy rate loss compared the perfect CDI case. The results are summarized later in Theorem 1 and Corollary 1. A sketch proof is given below.

Let us define the the secrecy rate loss as

$$\begin{aligned} \Delta \mathrm{C}_{\mathrm{sec}} &\triangleq \max_{\alpha} R_s(\alpha) - \max_{\alpha'} R_{s,q}(\alpha') \\ &\le R_s(\alpha_p^\star) - R_{s,q}(\alpha_p^\star), \end{aligned} \tag{13}$$

where $\alpha_p^\star$ is the optimal power allocation in the perfect CDI case, i.e., $\alpha_p^\star = \arg\max_\alpha R_s(\alpha)$.

First of all, one can show that the second term in $R_s(\alpha_p^\star)$ and $R_{s,q}(\alpha_p^\star)$ are both equal to the constant

$$\mathbf{E}\left[1 + \frac{\beta(1, n_t - 1)\alpha_p^\star (n_t - 1)}{(1 - \beta(1, n_t - 1))(1 - \alpha_p^\star)}\right]. \tag{14}$$

This follows from the fact that $|\mathbf{h}_e^H \mathbf{g}_r|^2 = |\mathbf{h}_e^H \hat{\mathbf{g}}_r|^2 = \|\mathbf{h}_e\|^2 \beta(1, n_t - 1)$ since $\mathbf{g}_r$, $\hat{\mathbf{g}}_r$ and $\mathbf{h}_e$ are independent and isotropically distributed in $\mathbb{C}^{n_t}$ and that $\|\mathbf{h}_e^H \mathbf{N}_g\|^2 = \|\mathbf{h}_e\|^2 - \|\mathbf{h}_e^H \mathbf{g}_r\|^2$ and $\|\mathbf{h}_e^H \hat{\mathbf{N}}_g\|^2 = \|\mathbf{h}_e\|^2 - \|\mathbf{h}_e^H \hat{\mathbf{g}}_r\|^2$. Then, by (14) and the fact that the first term of $R_s(\alpha_p^\star)$ is greater than the first term of $R_{s,q}(\alpha_p^\star)$, it follows that the secrecy rate loss in (13) can be further upper bounded as

$$\begin{aligned} \Delta \mathrm{C}_{\mathrm{sec}} \le & \mathbf{E}\left[\log(1 + \|\mathbf{h}_r\|^2 \alpha P)\right] \\ & - \mathbf{E}\left[\log\left(1 + \frac{\|\mathbf{h}_r\|^2 (\cos\theta)^2 \cdot \alpha P}{\|\mathbf{h}_r\|^2 \cdot (\sin\theta)^2 \frac{1-\alpha}{n_t - 1} P + 1}\right)\right]. \end{aligned} \tag{15}$$

Note that this upper-bound depends only on the legitimate receiver's channel $\mathbf{h}_r$. By further utilizing properties of the RVQ codebook and the quantization cell approximation, we can obtain the following results. Detailed proofs are provided in [12].

Theorem 1: The secrecy rate loss $\Delta \mathrm{C}_{\mathrm{sec}}$ between quanitzed and perfect CDI is upper-bounded by

$$\Delta \mathrm{C}_{\mathrm{sec}} \le \log\Big[\Big(\frac{n_t(1 - \alpha_p^\star)P}{(n_t - 1)(2^{\frac{B}{n_t - 1}} - 1)} + \frac{1}{1 - 2^{\frac{-B}{n_t - 1}}}\Big) \times \Big(1 + \frac{1}{(n_t - 1)\alpha_p^\star P}\Big)\Big]. \tag{16}$$

[1] Note that, without CQI, the variable-rate coding in [2] can not be applied and, thus, the result in (5) is derived based on the constant-rate coding scheme also given in [2].

Corollary 1: To maintain a constant secrecy rate loss Δ_r, the number of feedback bits B must satisfy

$$B \geq (n_t - 1) \log \left[\frac{n_t}{n_t - 1} \frac{(1 - \alpha_p^\star)P}{\Delta_r'} + \frac{\Delta_r'}{\Delta_r' - 1} \right], \quad (17)$$

where $\Delta_r' = (2^{\Delta_r})/(1 + 1/((n_t - 1)\alpha_p^\star P))$.

By the results in (17), one can see that, to guarantee a constant secrecy rate loss, the number of feedback bits B must scale linearly with n_t and logarithmically with P, i.e., $B = \Omega(n_t \log P)$, where Ω is the big-Omega notation.

IV. Extensions to the MIMOME Case

In the section, we investigate the effect of quantized CDI feedback on the MIMOME secrecy rate, and analyze the number of feedback bits B that is needed to maintain a constant secrecy rate loss.

A. MIMOME signal model and secrecy rate

Consider the MIMOME signal model where $n_r, n_e \geq 1$. The received signal models within a certain coherence interval are given by

$$\mathbf{y}_r[i] = \mathbf{H}_r \mathbf{x}[i] + \mathbf{z}_r[i], \quad (18a)$$

$$\mathbf{y}_e[i] = \mathbf{H}_e \mathbf{x}[i], \quad (18b)$$

where $\mathbf{H}_r \in \mathbb{C}^{n_r \times n_t}$ and $\mathbf{H}_e \in \mathbb{C}^{n_e \times n_t}$ are the MIMO channel matrices corresponding to the legitimate receiver and the eavesdropper, respectively. Similar to the MISOSE case in Section II, we assume that the channels are ergodic and the elements of $\mathbf{H}_r$ and $\mathbf{H}_e$ are i.i.d. complex Gaussian distributed with zero mean and unit variance.

Assume that $n_t \geq n_r + n_e$. It follows from [4] that the transmitted signal vector $\mathbf{x}$ is given by

$$\mathbf{x}[i] = \mathbf{P}\mathbf{s}[i] + \mathbf{Q}\mathbf{a}[i], \quad (19)$$

where $\mathbf{s}[i]$ is the message-bearing signal with distribution $\mathcal{CN}(0, P_s \mathbf{I}_{n_r})$, $\mathbf{a}[i]$ is the imposed artificial noise with distribution $\mathcal{CN}(0, P_a \mathbf{I}_{n_t - n_r})$, and $\mathbf{P} \in \mathbb{C}^{n_t \times n_r}$ and $\mathbf{Q} \in \mathbb{C}^{n_t \times (n_t - n_r)}$ are the precoding matrices for $\mathbf{s}[i]$ and $\mathbf{a}[i]$, respectively. Let the SVD of $\mathbf{H}_r$ be $\mathbf{H}_r = \mathbf{V}\mathbf{\Sigma}\mathbf{U}^H$, where $\mathbf{V} \in \mathbb{C}^{n_r \times n_r}$ is a unitary matrix, $\Sigma \in \mathbb{C}^{n_r \times n_r}$ is a diagonal matrix with the singular values of $\mathbf{H}_r$ being the diagonal elements, and $\mathbf{U} \in \mathbb{C}^{n_t \times n_r}$ is a semi-unitary matrix. Denote by $\mathbf{Z} \in \mathbb{C}^{n_t \times (n_t - n_r)}$ whose column vectors form an orthonormal basis for the orthogonal complement of $\mathbf{U}$. Then the transmitter employs the "matched" precoder by choosing $\mathbf{P} = \mathbf{U}$ and $\mathbf{Q} = \mathbf{Z}$ (therefore $\mathbf{U}^H\mathbf{Q} = \mathbf{0}$). Under this setting, the received signal models in (18) become

$$\begin{aligned} \mathbf{y}_r[i] &= \mathbf{H}_r \left(\mathbf{U}\mathbf{s}[i] + \mathbf{Z}\mathbf{a}[i] \right) + \mathbf{z}_r[i] = \left(\mathbf{V}\mathbf{\Sigma} \right) \mathbf{s}[i] + \mathbf{z}_r[i] \\ \mathbf{y}_e[i] &= \mathbf{H}_e \mathbf{U}\mathbf{s}[i] + \mathbf{H}_e[i]\mathbf{Z}\mathbf{a}[i], \end{aligned} \quad (20)$$

and the associated achievable MIMOME perfect secrecy rate [4] is given by

$$\begin{aligned} R_{s,p,M}(\alpha) = \big(\mathbf{E}\big[\log \left| \mathbf{I} + \mathbf{\Sigma}^2 P_s \right| - \\ \log \left| P_s \mathbf{U}^H \mathbf{H}_e^H \left(P_a \mathbf{H}_e \mathbf{Z}\mathbf{Z}^H \mathbf{H}_e^H \right)^{-1} \mathbf{H}_e \mathbf{U} + \mathbf{I} \right| \big] \big)^+, \end{aligned} \quad (21)$$

where $P_s = \left(\frac{\alpha}{n_r} \right) P$ and $P_a = \frac{(1-\alpha)}{n_t - n_r} P$. Similar to the MISOSE case, the MIMOME secrecy rate under perfect CDI, given in (21), can be made arbitrarily large by increasing P.

Suppose that the transmitter has a quantized CDI feedback $\hat{\mathbf{U}} \in \mathbb{C}^{n_t \times n_r}$. In this case, the beamformers will be chosen as $\mathbf{P} = \hat{\mathbf{U}}$ and $\mathbf{Q} = \hat{\mathbf{Z}}$, where the columns of $\hat{\mathbf{Z}}$ form an orthonormal basis for the orthogonal complement of $\hat{\mathbf{U}}$. Since $\mathbf{U}^H\hat{\mathbf{Z}} \neq \mathbf{0}$, we instead have an undesired AN leakage term $\mathbf{V}\mathbf{\Sigma}\mathbf{U}^H\hat{\mathbf{Z}}\mathbf{a}[i]$ in $\mathbf{y}_r[i]$ from (20), and therefore the achievable secrecy rate under quantized CDI feedback becomes

$$\begin{aligned} R_{s,q,M}(\alpha) = \\ \Bigg(\mathbf{E}\Bigg[\log \Bigg| \mathbf{I} + P_s \hat{\mathbf{U}}^H \mathbf{U}\mathbf{\Sigma} \left(\mathbf{I} + P_a \mathbf{\Sigma}\mathbf{U}^H \hat{\mathbf{Z}}\hat{\mathbf{Z}}^H \mathbf{U}\mathbf{\Sigma} \right)^{-1} \mathbf{\Sigma}\mathbf{U}^H \hat{\mathbf{U}} \Bigg| \\ - \log \left| P_s \hat{\mathbf{U}}^H \mathbf{H}_e^H \left(P_a \mathbf{H}_e \hat{\mathbf{Z}}\hat{\mathbf{Z}}^H \mathbf{H}_e^H \right)^{-1} \mathbf{H}_e \hat{\mathbf{U}} + \mathbf{I} \right| \Bigg] \Bigg)^+. \end{aligned} \quad (22)$$

B. Scaling law of number of feedback bits

In this section, we examine the number of feedback bits needed to maintain a constant MIMOME secrecy rate loss. In the MIMOME case, the quantization codebook is a set of 2^B $n_t \times n_r$ semi-unitary matrices $\mathbf{C}_1, \ldots, \mathbf{C}_{2^B}$. With perfect knowledge of $\mathbf{H}_r[i]$ at the legitimate receiver, the quantized CDI $\hat{\mathbf{U}}$ is obtained by

$$\hat{\mathbf{U}} = \arg \min_{\mathbf{C} \in \{\mathbf{C}_1, \ldots, \mathbf{C}_{2^B}\}} d^2(\mathbf{U}, \mathbf{C}), \quad (23)$$

where $d(\mathbf{U}, \mathbf{C}) = n_r - \mathrm{tr}(\mathbf{U}^H\mathbf{C}\mathbf{C}^H\mathbf{U})$ is the chordal distance which measures the distortion between $\mathbf{U}$ and $\mathbf{C}$ [13]. For ease of analysis, we consider the random quantization codebook model [13] where the 2^B semi-unitary codewords are chosen independently and are uniformly (isotropically) over the n_t by n_r Grassmann manifold (which is the set of all n_r-dimensional subspaces in an n_t-dimensional space). With this codebook model, the average distortion between the quantized CDI $\hat{\mathbf{U}}$ and the true CDI $\mathbf{U}$ can be upper bounded as [13]

$$D \triangleq \mathbf{E}[d^2(\mathbf{U}, \hat{\mathbf{U}})] \leq \frac{\Gamma(\frac{1}{T})}{T} \Phi^{\frac{-1}{T}} 2^{\frac{-B}{T}} \quad (24)$$

where $\Gamma(\cdot)$ is the Gamma function, and the detailed definitions of T and Φ can be found in [13].

Following the analysis of the MISOSE case, we can show that the number of feedback bits B needed to maintain a constant rate loss Δ_r is lower bounded as

$$\begin{aligned} B \gtrapprox (n_t - n_r) n_r \Bigg[\log \left(1 + \frac{P n_t \left(\frac{1 - \alpha_P^\star}{n_t - n_r} \right) + 1}{2^{(\Delta_r - \gamma(P_s^{-1}))/n_r} - 1} \right) \\ + \log \left(\frac{\Gamma(\frac{1}{n_r(n_t - n_r)}) \Phi^{-1/(n_r(n_t - n_r))}}{n_r^2 (n_t - n_r)} \right), \Bigg]. \end{aligned} \quad (25)$$

where $\gamma(P_s^{-1}) = n_r \log \left(1 + \frac{P_s^{-1}}{n_t - n_r} \right)$. A detailed proof is given in [12]. Hence, we see that B must also scale logarithmically with P in order to maintain a rate loss below Δ_r.

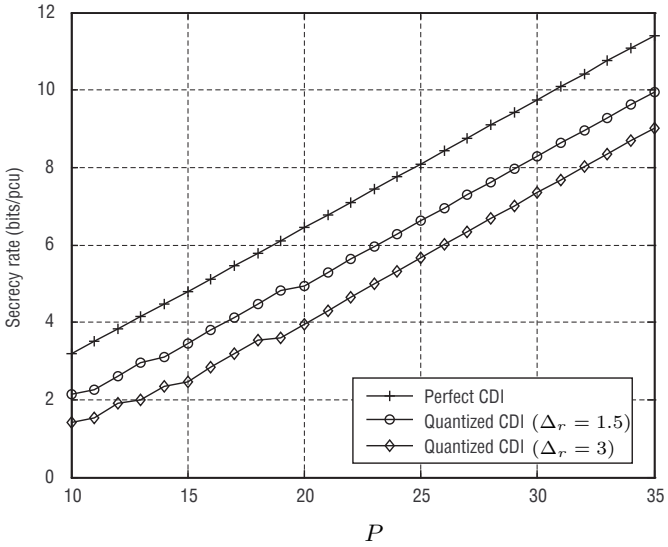

Fig. 1. Secrecy rate versus SNR when $n_r = n_e = 1$.

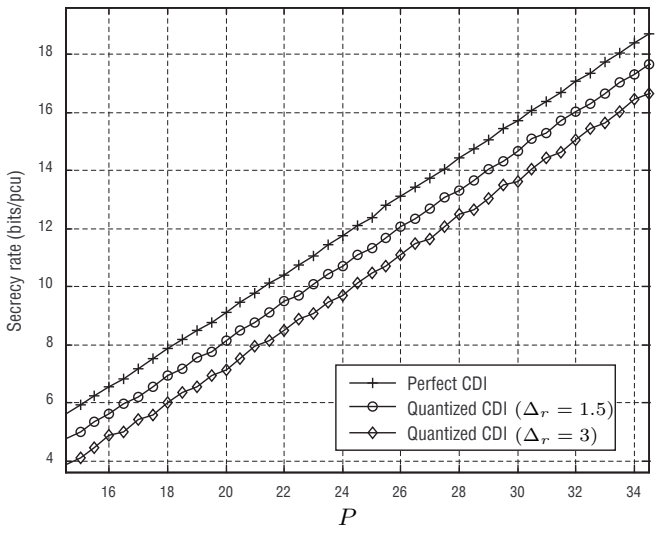

Fig. 2. Secrecy rate versus SNR when $n_r = n_e = 2$.

V. Simulation Results and Discussions

In this section, we present simulation results to illustrate the impact of quantized CDI feedback on the secrecy rate. We set the number of transmit antennas n_t to 4, and each element of the channel vectors (matrices) $\mathbf{h}_r$ ($\mathbf{H}_r$) and $\mathbf{h}_e$ ($\mathbf{H}_e$) being i.i.d. complex Gaussian random variables with zero mean and unit variance. To verify our results, we used the method in [9] to generate the quantized CDI for each channel realization of the legitimate receiver. Each simulation result was obtained by averaging over 10000 channel realizations.

In Fig. 1, the simulation results of the MISOSE feedback bit scaling is shown to verify the analytical results presented in Section III-C. Here, the number of feedback bits B is increased according to (17) for a given constant secrecy rate loss Δ_r. The secrecy rate losses Δ_r are set to 1.5 and 3, respectively. For the MIMOME case, we set the antennas at the legitimate receiver and the eavesdropper to $n_r = n_e = 2$. The results for MIMOME feedback bit scaling law are shown in Fig. 2. Although we only provide an approximation to the required number of feedback bits in the MIMOME case, one can see from this figure that the predictions are still fairly accurate.

VI. Conclusions

In this work, we have examined the effect of quantized CDI on the secrecy rate achievable with AN-assisted beamforming. We have identified the noise leakage problem due to quantized CDI and have shown how the achievable secrecy rate may be limited when the number of feedback bits is fixed. To maintain a constant secrecy rate loss compared to the perfect CDI case, we have shown that the number of bits B must scale logarithmically with respect to the transmit power P. This result has been shown for both the MISOSE and the MIMOME cases.

Acknowledgements

The authors would like to thank Mr. Meng-Hsi Chen and Mr. Chun-Yao Chen their help on the numerical simulations.

References

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

[2] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

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

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

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *submitted to IEEE Trans. Inform. Theory*, 2007.

[6] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *submitted to IEEE Trans. Inform. Theory*, March, 2009.

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

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

[9] N. Ravindran and N. Jindal, "Limited feedback-based block diagonalization for the MIMO broadcast channel," *IEEE J. Select. Areas Commun.*, vol. 26, no. 8, pp. 1473–1482, 2008.

[10] Y.-L. Liang, Y.-S. Wang, T.-H. Chang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, June 28 - July 3 2009, pp. 2351 – 2355.

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

[12] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise – the noise leakage problem," *in preparation for submission to IEEE Trans. Wireless Commun.*, 2010.

[13] W. Dai, Y. Liu, and B. Rider, "Quantization bounds on Grassmann manifolds and applications to MIMO communications," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 1108–1123, 2008.