Adaptive Limited Feedback for MISO Wiretap Channels With Cooperative Jamming

Minyan Pei, A. Lee Swindlehurst, *Fellow, IEEE*, Dongtang Ma, and Jibo Wei

***Abstract*—This paper studies a multi-antenna wiretap channel with a passive eavesdropper and an external helper, where only quantized channel information regarding the legitimate receiver is available at the transmitter and helper due to finite-rate feedback. Given a fixed total bandwidth for the two feedback channels, the receiver must determine how to allocate its feedback bits to the transmitter and helper. Assuming zero-forcing transmission at the helper and random vector quantization of the channels, an analytic expression for the achievable ergodic secrecy rate due to the resulting quantization errors is derived. While direct optimization of the secrecy rate is difficult, an approximate upper bound for the mean loss in secrecy rate is derived and a feedback bit allocation method that minimizes the average upper bound on the secrecy rate loss is studied. A closed-form solution is shown to be possible if the integer constraint on the bit allocation is relaxed. Numerical simulations indicate the significant advantage that can be achieved by adaptively allocating the available feedback bits.**

***Index Terms*—Cooperative jamming, feedback bits allocation, limited feedback, MISO wiretap channel.**

I. Introduction

PHYSICAL layer security has attracted considerable attention recently as an alternative to or an augmentation of traditional cryptography-based security. The goal of such methods is to exploit the physical characteristics of the wireless channel to enhance the security of wireless communication systems. The pioneering work of Wyner introduced the concept of the wiretap channel and secrecy capacity, and laid the basis for information-theoretic approaches for secure communication [1]. More recently, a significant effort has been invested in the study of secrecy capacity in wiretap channels with multiple antennas [2]–[8]. More detailed results are possible for multiple-input single-output (MISO) wiretap channels, which have been studied in [2]–[5] under different assumptions on channel state information and fading. In particular, for the MISO case where the channel to the legitimate receiver is known but only trivial statistical information about the eavesdropper's channel is available, it was shown in [2] that the optimal communication strategy that achieves the highest secrecy rate, is based on beamforming. With the additional degrees of freedom available in multi-antenna systems, the use of artificial noise (AN) has been proposed for selectively degrading the eavesdropper's channel, particularly in situations where no information or only statistical information is available about the eavesdropper [9], [10].

Recent work has also considered the use of friendly helpers to provide jamming signals to confuse the eavesdropper [11]–[19]. The idea of a terminal helping another improve its secrecy rate first appeared in 2006 [11], and later in [12], [13] the term *cooperative jamming* was introduced for this idea. It should be noted that although in this paper we will study cooperative jamming with Gaussian noise, cooperative jammers can also improve secrecy using Gaussian or lattice codewords, as in [14], [16]. The MISO wiretap scenario was first considered in [18], where it was shown that zero-forcing (ZF) beamforming at the helper is nearly optimal in the high signal-to-noise ratio (SNR) regime. The work of [19] showed how to obtain optimal transmit beamformers at the transmitter and helper, and also demonstrated that using a ZF beamformer at the helper is a near-optimal choice for obtaining the secrecy capacity in this scenario, assuming that the transmitter and helper have perfect channel state information (CSI) for the channels to the receiver. In practice however, knowledge of the CSI at the transmitter and helper (referred to as CSIT here) is destined to be in error. This is particularly true in frequency-division duplex (FDD) systems, where the legitimate user quantizes the CSI using a finite-sized codebook that is known to both the transmitter and receiver, and then feeds the quantized information back to the transmitter.

The effects of quantized channel feedback on transceiver design have been studied extensively for both single and multiuser downlink systems without secrecy considerations [20]–[24]. Only the recent work of [25]–[27] has considered the impact of limited feedback on secrecy for the simple wiretap channel without a helper. In [25], the degradation in secrecy rate for AN-assisted beamforming due to quantized channel direction information was studied, and the optimal power allocation between the message-bearing signal and the AN for a given number of feedback bits was examined. A lower bound on the ergodic secrecy capacity was obtained using numerical integration in [26] for AN-assisted wiretap channels. In [27], the secrecy outage probability was charac-

Manuscript received May 30, 2013; revised September 11, 2013; accepted November 27, 2013. Date of publication December 13, 2013; date of current version January 21, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Rong-Rong Chen. This work was supported by the National Nature Science Foundation of China under Grant 61002032 and by the U.S. National Science Foundation under Grant CCF-1117983. This paper was presented in part at IEEE Workshop on Signal Processing Advances in Wireless Communications, Darmstadt, Germany, June 2013.

M. Pei, D. Ma, and J. Wei are with the College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China (e-mail: mypei86@nudt.edu.cn; dongtangma@nudt.edu.cn; wjbhw@nudt.edu.cn).

A. L. Swindlehurst is with the Center for Pervasive Communications and Computing (CPCC), University of California, Irvine, CA 92664 USA (e-mail: swindle@uci.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2013.2295059

terized for codebook-based transmit beamforming. However, none of the prior work has addressed the impact of finite-rate feedback in the context of multiple-antenna wiretap channels with an external helper. This problem is interesting since each receiver must feedback CSI to both the transmitter and the helper. Errors in the CSI at the transmitter, which reduce the gain available to the receiver, must be balanced against errors in the helper CSI, which will lead to increased interference due to imperfectly nulled AN transmissions. When the total bandwidth of the two feedback channels is fixed, the optimal feedback bit allocation must address this trade-off given the available feedback throughput, SNR, number of antennas and the channel conditions.

Feedback bit allocation strategies have been proposed for other applications where both desired and interfering transmitters are present [28]–[30], although again not for the physical layer security problem. The two-user MIMO interference channel was considered in [28], and cooperative feedback to the interfering transmitter was proposed in addition to standard feedback to the desired transmitter. Under a constraint on the throughput loss caused by precoder quantization, the required number of cooperative feedback bits was derived. Cooperative multi-cell systems with limited feedback are another relevant application. The authors of [29] proposed an approach where the available bits assigned to the desired and interfering transmitters were chosen to reduce the mean loss in sum-rate due to quantization for a soft hand-off model. In their scheme, beamforming vectors were designed using a generalized eigenvector approach to maximize the sum-rate assuming a single interferer scenario, which leads to an objective different from the one considered here. In [30], a multicell MISO system with joint processing was considered, where the base stations exchange both CSI and data, and a feedback bit allocation scheme was proposed to maximize the quantization accuracy.

In this paper, we consider cooperative jamming for the MISO wiretap channel with finite-rate feedback, where the transmitter uses a maximum ratio transmission (MRT) strategy, and the helper enhances the secrecy of the legitimate channels via a ZF approach intended to produce AN that is ideally invisible to the legitimate user. Assuming a fixed total number of feedback bits available at the legitimate user, we study how to optimize allocation of the bits for the two feedback channels assuming random vector quantization (RVQ) codebooks, where the quantization vectors are independently chosen from an isotropic distribution on the unit hypersphere [21]. We first consider the general problem of maximizing the ergodic secrecy rate. While we show how to obtain an analytic expression for the ergodic secrecy rate that can be used for performance optimization, it is cumbersome and requires numerical integration. As an alternative, we then derive an upper-bound on the mean *loss* in secrecy rate assuming a fixed power allocation at the transmitter and helper. We show that for the general scenario with a global constraint on the feedback bandwidth, a closed-form solution can be found by standard convex optimization techniques if the integer constraint on the bits is relaxed. Our simulation results show that proper allocation of the feedback bits to the transmitter and helper can have a significant impact on the secrecy of the wiretap channel.

In the next section, the system model is presented together with the proposed transmission strategy. An analytical expression for the ergodic secrecy rate is developed in Section III, and then an approximate upper bound for the secrecy rate loss is derived in Section IV, together with the algorithm for adaptive limited feedback that minimizes the upper bound under a constraint on the total number of feedback bits. Numerical results are provided in Section V and we conclude in Section VI.

Notations: We use uppercase boldface for matrices and lowercase boldface for vectors. The superscripts $(\cdot)^H$ and $(\cdot)^{-1}$ denote conjugate transposition and matrix inversion, respectively. $\mathrm{Tr}(\cdot)$, $\mathrm{vec}(\cdot)$ and $\det(\cdot)$ denote the trace, column vectorization and determinant operations, respectively. $\mathbb{E}_a[\cdot]$ denotes expectation with respect to a, $\|\mathbf{a}\|$ denotes the Euclidean norm of vector $\mathbf{a}$, and the function $\{a\}^+$ represents $\max\{a,0\}$. The notation $\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ means that $\mathbf{x}$ is a vector of circularly symmetric complex Gaussian random variables with mean vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$. $\mathbf{I}_N$ denotes an $N \times N$ identity matrix (the subscript is dropped when the dimension is obvious).

II. System Model and Assumptions

A. System Model

We consider a MISO wiretap channel that includes a transmitter (Alice), a legitimate receiver (Bob), a friendly jammer (Helper) and an eavesdropper (Eve). We assume N_a antennas at Alice, N_h antennas at Helper, N_e antennas at Eve, and a single antenna at Bob. In this model, the transmitter Alice wishes to send a confidential message to Bob in the presence of Eve, with the aid of the Helper. We assume that the Helper does not know the confidential message and assists Alice by producing artificial Gaussian noise (jamming) to confuse Eve.

We assume the vector $\mathbf{x} \in \mathbb{C}^{N_a \times 1}$ is the confidential information-bearing signal transmitted by Alice, $\mathbf{z} \in \mathbb{C}^{N_h \times 1}$ is the Gaussian jamming signal generated by the Helper, and the signals $\mathbf{x}, \mathbf{z}$ satisfy the power constraints $\mathbb{E}[\|\mathbf{x}\|^2] \leq P_a$, $\mathbb{E}[\|\mathbf{z}\|^2] \leq P_h$. The received signal at Bob and Eve are respectively given by

$$y_b = \mathbf{h}_b^H \mathbf{x} + \mathbf{g}_b^H \mathbf{z} + n_b \tag{1}$$

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x} + \mathbf{G}_e \mathbf{z} + \mathbf{n}_e, \tag{2}$$

where $\{\mathbf{h}_b \in \mathbb{C}^{N_a \times 1}, \mathbf{g}_b \in \mathbb{C}^{N_h \times 1}\}$ are the channel vectors to Bob from Alice and the Helper respectively, and $\{\mathbf{H}_e \in \mathbb{C}^{N_e \times N_a}, \mathbf{G}_e \in \mathbb{C}^{N_e \times N_h}\}$ are the corresponding channels for Eve. The terms n_b and $\mathbf{n}_e$ represent circularly symmetric unit-variance Gaussian noise at Bob and Eve, respectively; their distributions are denoted by $n_b \sim \mathcal{CN}(0,1)$ and $\mathbf{n}_e \sim \mathcal{CN}(0, \mathbf{I})$. All channels are assumed to be mutually independent and each composed of circularly symmetric complex Gaussian entries, i.e., $\mathbf{h}_b \sim \mathcal{CN}(\mathbf{0}, \sigma_h^2 \mathbf{I})$ and $\mathbf{g}_b \sim \mathcal{CN}(\mathbf{0}, \sigma_g^2 \mathbf{I})$. The instantaneous realizations of both $\mathbf{h}_b$ and $\mathbf{g}_b$ are known perfectly to Bob, but Alice and the Helper only have quantized information about them obtained via distinct finite-rate feedback channels from the legitimate receiver. We also assume that $\mathrm{vec}(\mathbf{H}_e) \sim \mathcal{CN}(\mathbf{0}, \sigma_{he}^2 \mathbf{I})$ and $\mathrm{vec}(\mathbf{G}_e) \sim \mathcal{CN}(\mathbf{0}, \sigma_{ge}^2 \mathbf{I})$, and that these distributions are known to all legitimate parties (although we will see that this assumption can be relaxed when dealing with secrecy rate loss). All channels are assumed to remain constant during the time required for channel estimation and feedback.

In the finite-rate feedback model, the legitimate receiver first quantizes the channel direction information (CDI), $\tilde{\mathbf{h}}_b = \mathbf{h}_b/\|\mathbf{h}_b\|$ and $\tilde{\mathbf{g}}_b = \mathbf{g}_b/\|\mathbf{g}_b\|$, by exploiting two distinct quantization codebooks, $\mathcal{C}_1 = \{\mathbf{c}_{1,1}, \mathbf{c}_{1,2}, \ldots, \mathbf{c}_{1,2^{B_1}}\}$ and $\mathcal{C}_2 = \{\mathbf{c}_{2,1}, \mathbf{c}_{2,2}, \ldots, \mathbf{c}_{2,2^{B_2}}\}$, which consist of N_a- and N_h-dimensional unit norm vectors and are of size 2^{B_1} and 2^{B_2}, respectively ($\mathcal{C}_1$ is the codebook at Alice, $\mathcal{C}_2$ is the codebook at the Helper). The codebooks are designed off-line and known to all parties. Using the minimum chordal distance metric [20], [23], the CDI indices are computed by Bob as

$$n_1 = \arg \max_{1 \le i \le 2^{B_1}} |\tilde{\mathbf{h}}_b^H \mathbf{c}_{1,i}| \qquad \hat{\mathbf{h}}_b = \mathbf{c}_{1,n_1} \tag{3}$$

$$n_2 = \arg \max_{1 \le j \le 2^{B_2}} |\tilde{\mathbf{g}}_b^H \mathbf{c}_{2,j}| \qquad \hat{\mathbf{g}}_b = \mathbf{c}_{2,n_2}, \tag{4}$$

where $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{g}}_b$ are the quantized CDI of the two links for Bob. After quantization, Bob informs Alice and the Helper of their respective codebook indices n_1 and n_2 through distinct error- and delay-free feedback channels. Note that only the CDI is quantized, since the transmission strategies discussed below do not require knowledge of the channel gain.

B. Transmission Strategies

We focus on MRT beamforming at Alice and a ZF transmission scheme at the Helper, which is a reasonable approach for the MISO case considered here. Thus, the unit-norm beamforming vector for Bob at Alice is chosen as $\mathbf{t} = \hat{\mathbf{h}}_b$. The ZF constraint imposed on the jamming noise generated by the Helper can be expressed as $\mathbf{z} = \mathbf{\Gamma v}$, where $\mathbf{\Gamma} \in \mathbb{C}^{N_h \times (N_h - 1)}$ is an orthonormal basis for the null-space of $\hat{\mathbf{g}}_b^H$, and $\mathbf{v}$ is a vector of independent and identically distributed (i.i.d) Gaussian random variables of variance σ_v^2. Due to the power constraint at the Helper, we have $\mathbb{E}[\|\mathbf{z}\|^2] = \mathbb{E}[\mathbf{v}^H \mathbf{\Gamma}^H \mathbf{\Gamma v}] = (N_h - 1)\sigma_v^2 \le P_h$. The received signal at Bob and Eve are thus

$$y_b = \mathbf{h}_b^H \mathbf{t} s + \mathbf{g}_b^H \mathbf{\Gamma} \boldsymbol{v} + n_b \tag{5}$$

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{t} s + \mathbf{G}_e \mathbf{\Gamma} \boldsymbol{v} + \mathbf{n}_e. \tag{6}$$

The fundamental problem we are addressing is the following: if the total number of feedback bits B_b from the legitimate receiver is fixed, how should B_1 and B_2 be allocated among the transmitter and helper for optimal secrecy? Besides optimization of the feedback bit allocation, there is also an optimal power level for P_h; if too much power is allocated to the Helper when there are insufficient bits available for good CSI, the AN provided by the Helper does more harm than good due to interference leakage. The choice of transmit power to use at Alice could in principle also be optimized in order to maximize secrecy performance, although our simulations indicate that the best performance is achieved when Alice transmits with full power P_a. In the absence of a formal proof of this observation, we will assume that Alice transmits with full power P_a, recognizing that this may not be optimal in all cases. In the next section, we attempt a direct analysis using the ergodic secrecy rate. While our resulting analytic expression can be used to solve the desired optimization problem, a complicated process involving numerical integration is required. Thus, in Section IV, we consider a simpler approach based on secrecy rate loss, and we optimize the bit allocation to minimize an upper bound on the loss for fixed P_a and P_h.

III. Ergodic Secrecy Rate Analysis With Limited Feedback

A. Achievable Secrecy Rate With Quantized CDI

To quantify the secrecy performance of the scenario described above, we assume that the channels are ergodic block-fading that remain constant over a sufficient amount of time for signal transmission and feedback, and that the messages are coded across multiple fading blocks (a similar model was used in the related study of [25]). We further assume a scenario with delay-tolerant traffic, and use ergodic secrecy rate as our performance metric rather than secrecy outage rate [31]. For Gaussian signaling with $s \sim \mathcal{CN}(0, P_a)$, the achievable ergodic secrecy rate at Bob for the above ZF-based transmission strategy is given by [25]

$$R_s^{LFB} = \left\{\mathbb{E}_{\mathbf{h}_b, \mathbf{g}_b}\left[R_b^{LFB}\right] - \mathbb{E}_{\mathbf{H}_e, \mathbf{G}_e}\left[R_e^{LFB}\right]\right\}^+, \tag{7}$$

where

$$R_b^{LFB} = \log_2\left(1 + \frac{P_a |\mathbf{h}_b^H \hat{\mathbf{h}}_b|^2}{\|\mathbf{g}_b^H \mathbf{\Gamma}\|^2 \sigma_v^2 + 1}\right)$$

$$R_e^{LFB} = \log_2\left(1 + P_a \hat{\mathbf{h}}_b^H \mathbf{H}_e^H \left(\mathbf{I} + \sigma_v^2 \mathbf{G}_e \mathbf{\Gamma} \mathbf{\Gamma}^H \mathbf{G}_e^H\right)^{-1} \mathbf{H}_e \hat{\mathbf{h}}_b\right).$$

To represent the effect of quantized CDI on the achievable secrecy rate, we rewrite the actual channel direction vectors as

$$\tilde{\mathbf{h}}_b = \hat{\mathbf{h}}_b \cos\theta_1 + \mathbf{e} \sin\theta_1 \tag{8}$$

$$\tilde{\mathbf{g}}_b = \hat{\mathbf{g}}_b \cos\theta_2 + \mathbf{r} \sin\theta_2, \tag{9}$$

where $\cos\theta_1 = |\tilde{\mathbf{h}}_b^H \hat{\mathbf{h}}_b|$, $\cos\theta_2 = |\tilde{\mathbf{g}}_b^H \hat{\mathbf{g}}_b|$, and $\mathbf{e}$ and $\mathbf{r}$ are unit-norm vectors orthogonal to $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{g}}_b$, respectively. Thus, we have

$$\begin{aligned} R_b^{LFB} &= \log_2\left(1 + \frac{P_a \|\mathbf{h}_b\|^2 \cos^2\theta_1}{\sigma_v^2 \|\mathbf{g}_b\|^2 \|\mathbf{r}^H \mathbf{\Gamma}\|^2 \sin^2\theta_2 + 1}\right) \\ &= \log_2\left(1 + \frac{P_a \|\mathbf{h}_b\|^2 \cos^2\theta_1}{I_H + 1}\right). \end{aligned} \tag{10}$$

The interference I_H from the jammer is implicitly defined by the first term in the denominator of (10).

B. Auxiliary Results

In this subsection, we provide three lemmas that will be used in the ergodic secrecy rate analysis. The quantization cell approximation used in the proofs is based on the assumption that each quantization cell is a Voronoi region with surface area equal to 2^{-B} of the total area of the unit sphere for a B-bit codebook. Details for this model can be found in [20], [24]. As shown in [24], analysis based on the quantization cell approximation is close to the performance of random vector quantization, and so we use this approach to analyze the achievable rate.

Lemma 1 (Signal Power Distribution): Define $X = \|\mathbf{h}_b\|^2 \cos^2\theta_1$, where θ_1 is defined in (8). Then under the quantization cell approximation model, the cumulative distribution function (CDF) of X is given by

$$F_X(x) = 1 - 2^{B_1} e^{-x/\sigma_h^2} + e^{-\frac{x}{\sigma_h^2(1-\delta_1)}} \sum_{i=0}^{N_a-1} \frac{(\delta_1^{i-N_a+1}-1)x^i}{i!\sigma_h^{2i}(1-\delta_1)^i}, \tag{11}$$

where $\delta_1 = 2^{-\frac{B_1}{N_a-1}}$.

Proof: See Appendix A. ■

Lemma 2 (Interference Power Distribution): Under the quantization cell approximation model, the interference term I_H is an exponential random variable with probability distribution function (PDF) given by

$$f_{I_H}(y) = \frac{1}{P_h\sigma_g^2\delta_2} e^{-\frac{y}{P_h\sigma_g^2\delta_2}} \qquad y \ge 0, \tag{12}$$

where $\delta_2 = 2^{-\frac{B_2}{N_h-1}}$.

Proof: See Appendix B. ■

Lemma 3 (Distribution of SINR for Eve): Define $Z = \mathbf{u}_0^H\mathbf{J}^{-1}\mathbf{u}_0$, where $\mathbf{J} = \sum_{n=1}^N \mathbf{u}_n\mathbf{u}_n^H + \sigma^2\mathbf{I}$, and $\{\mathbf{u}_n, n = 0, 1, \cdots, N\}$ are $M \times 1$ independent zero-mean complex Gaussian variables with $\mathbb{E}[\mathbf{u}_n\mathbf{u}_n^H] = P_n\mathbf{I}$. Then the complementary CDF of Z is

$$R_Z(z) = e^{-\frac{z}{\gamma}} \sum_{m=1}^{M} \frac{A_m(z)}{(m-1)!}\left(\frac{z}{\gamma}\right)^{m-1}, \tag{13}$$

where $\gamma \equiv P_0/\sigma^2$, $\Gamma_n \equiv P_n/P_0$,

$$A_m(z) = \begin{cases} 1, & M \ge N+m \\ \frac{1+\sum_{i=1}^{M-m} D_i z^i}{\prod_{n=1}^{N}(1+\Gamma_n z)}, & M < N+m \end{cases}$$

and D_i is the coefficient of z^i in $\prod_{n=1}^N(1+\Gamma_n z)$.

Proof: This result is provided by eq. (11) in [32]. ■

C. Ergodic Secrecy Rate

Using Lemma 1 and Lemma 2, we can derive an analytic expression for the ergodic rate of the channel between Alice and Bob averaged over the parameters of the quantization, which we denote by $\mathbb{E}_{\theta_1,\theta_2,\mathbf{e},\mathbf{r}}[R_b^{LFB}]$, where $\mathbb{E}_{\theta_1,\theta_2,\mathbf{e},\mathbf{r}}[\cdot]$ denotes expectation with respect to $\theta_1, \theta_2, \mathbf{e}, \mathbf{r}$. Next we define $\mathbf{H}_e\mathbf{t} = \mathbf{u}_0$ and $\mathbf{G}_e\mathbf{\Gamma} = [\mathbf{u}_1, \ldots, \mathbf{u}_{N_h-1}]$, and note that $\{\mathbf{u}_n, n = 0, 1, \cdots, N_h-1\}$ are $N_e \times 1$ independent zero-mean complex Gaussian variables. The SINR at Eve becomes

$$\gamma_e = P_a\mathbf{u}_0^H\left(\mathbf{I} + \sum_{j=1}^{N_h-1} \sigma_v^2\mathbf{u}_j\mathbf{u}_j^H\right)^{-1}\mathbf{u}_0, \tag{14}$$

and we can derive an analytic expression for the ergodic rate of the eavesdropper's channel using Lemma 3. Putting these results together, an analytic expression for the ergodic secrecy rate can be obtained, which is provided below in Theorem 1.

Theorem 1: Denote $\gamma_b \triangleq \frac{P_a\|\mathbf{h}_b\|^2\cos^2\theta_1}{1+I_H}$, $\gamma_e \triangleq P_a\mathbf{u}_0^H\left(\mathbf{I} + \sigma_v^2\sum_{n=1}^{N_h-1}\mathbf{u}_n\mathbf{u}_n^H\right)^{-1}\mathbf{u}_0$, and $\sigma_v^2 = \frac{P_h}{N_h-1}$. Then $C_s = \max\{C_1 - C_2, 0\}$, Where

$$\begin{aligned} C_1 =& \mathbb{E}_{\gamma_b}\left[\log_2(1+\gamma_b)\right] \\ =& \log_2(e)\frac{P_a\sigma_h^2}{P_h\sigma_g^2\delta_2\delta_1^{N_a-1}} \cdot I_1\left(\frac{1}{P_a\sigma_h^2}, \frac{P_a\sigma_h^2}{P_h\sigma_g^2\delta_2}, 0, 1\right) \\ &- \log_2(e) \\ &\times \sum_{i=0}^{N_a-1}\sum_{l=0}^{i} \frac{\left(P_a\sigma_h^2(1-\delta_1)\right)^{l+1-i}\left(\delta_1^{i-N_a+1}-1\right)}{P_h\sigma_g^2\delta_2(i-l)!} \\ &\cdot I_1\left(\frac{1}{P_a\sigma_h^2(1-\delta_1)}, \frac{P_a\sigma_h^2(1-\delta_1)}{P_h\sigma_g^2\delta_2}, i, l+1\right) \end{aligned} \tag{15}$$

$$\begin{aligned} C_2 =& \mathbb{E}_{\gamma_e}\left[\log_2(1+\gamma_e)\right] \\ =& \log_2(e)\sum_{m=1}^{N_e-N_h+1} \frac{1}{(m-1)!\left(P_a\sigma_{he}^2\right)^{m-1}} \\ &\times I_2\left(\frac{1}{P_a\sigma_{he}^2}, 1, m-1, 1\right) + \log_2(e) \\ &\times \sum_{m=\max\{1,N_e-N_h+2\}}^{N_e} \frac{\left(P_a\sigma_{he}^2\right)^{N_h-m}}{(m-1)!\left(\sigma_v^2\sigma_{ge}^2\right)^{N_h-1}} \\ &\cdot I_1\left(\frac{1}{P_a\sigma_{he}^2}, \frac{P_a\sigma_{he}^2}{\sigma_v^2}, m-1, N_h-1\right) + \log_2(e) \\ &\times \sum_{m=\max\{1,N_e-N_h+2\}}^{N_e} \sum_{i=1}^{N_e-m} \frac{\left(P_a\sigma_{he}^2\right)^{N_h-m-i}\binom{N_h-1}{i}}{(m-1)!\left(\sigma_v^2\sigma_{ge}^2\right)^{N_h-1-i}} \\ &\cdot I_1\left(\frac{1}{P_a\sigma_{he}^2}, \frac{P_a\sigma_{he}^2}{\sigma_v^2\sigma_{ge}^2}, m+i-1, N_h-1\right), \end{aligned} \tag{16}$$

and $I_1(\cdot,\cdot,\cdot,\cdot)$ is the integral

$$I_1(a,b,m,n) = \int_0^\infty \frac{x^m e^{-ax}}{(x+b)^n(x+1)}dx, \tag{17}$$

which can be evaluated as explained in (47), $I_2(\cdot,\cdot,\cdot,\cdot)$ is the integral

$$I_2(a,b,m,n) = \int_0^\infty \frac{x^m e^{-ax}}{(x+b)^n}dx, \tag{18}$$

which can be evaluated as explained in (48).

Proof: See Appendix C. ■

The resulting expression is quite complicated in the general case. In the following, we provide simplified or approximate expressions for the ergodic secrecy rate in several special scenarios, where $\sigma_h = \sigma_g = \sigma_{he} = \sigma_{ge} = 1$. These expressions will be used to obtain analytical results and useful insights on the achievable average secrecy rate and allocation of the feedback bits. Note that the derived approximation may not be an achievable secrecy rate, although it is useful for feedback design.

1) High SNR Case: If we define $P_a = \alpha P_h$ and let P_h grow large, the noise term is negligible with respect to the interference term in the SINR expressions. In this case, the ergodic secrecy rate drops to zero when $N_e \ge N_h$, since the eavesdropper can theoretically null the interference from the Helper. For the case where $N_e < N_h$, the ergodic secrecy rate can be expressed as in Theorem 2.

Theorem 2: Denote $\tilde{\gamma}_b \triangleq \frac{P_a\|\mathbf{h}_b\|^2\cos^2\theta_1}{I_H}$, $\sigma_v^2 = \frac{P_h}{N_h-1}$, $\tilde{\gamma}_e \triangleq \frac{P_a}{\sigma_v^2}\mathbf{u}_0^H\left(\sum_{n=1}^{N_h-1}\mathbf{u}_n\mathbf{u}_n^H\right)^{-1}\mathbf{u}_0$. If $N_e < N_h$, then $\tilde{C}_s = \max\{\tilde{C}_1 - \tilde{C}_2, 0\}$, where $\tilde{C}_1$ and $\tilde{C}_2$ are derived as (19) and (20) at the bottom of the page.

Proof: See Appendix D. ■

2) Single-Antenna Eavesdropper: For the special case where $N_a = N_h = 2$, $N_e = 1$, the achievable ergodic rates C_1 and C_2 in Theorem 1 reduce to (21) and (22) at the bottom of the page. This can be substituted into $C_s^{2,2,1} = \{C_1^{2,2,1} - C_2^{2,2,1}\}^+$ to yield a simplified expression for the ergodic secrecy rate. For high SNR with $P_h \rightarrow \infty$ and $P_a = \alpha P_h$, the expressions for $C_1^{2,2,1}$ and $C_2^{2,2,1}$ in (21) and (22) can be approximated as (23) and (24) at the bottom of the page.

Fig. 1 shows the ergodic secrecy rate as a function of the transmit power P_h, with $N_a = N_b = 2$, $N_e = 1$ and $P_a = \alpha P_h$ for $\alpha = 0.4,\ 5$. The dash-dotted lines are obtained using the asymptotic expressions in (23) and (24). We see that the secrecy rate increases with α (higher relative power at the Helper) and as the total number of feedback bits for Bob B_b is increased. Also, for large P_h, the secrecy rate yielded by (21) and (22) asymptotically converges to the limiting value derived by (23) and (24). Furthermore, the simplified expression for the ergodic

$$\begin{aligned}\tilde{C}_1 &= \mathbb{E}_{\tilde{\gamma}_b}\left[\log_2(1+\tilde{\gamma}_b)\right]\\ &= \log_2(e)\left[\frac{\alpha}{\delta_2\delta_1^{N_a-1}}\cdot I_1\left(0,\frac{\alpha}{\delta_2},0,1\right) - \sum_{i=0}^{N_a-1}\frac{\alpha(1-\delta_1)\left(\delta_1^{i-N_a+1}-1\right)}{\delta_2}\cdot I_1\left(0,\frac{\alpha(1-\delta_1)}{\delta_2},i,i+1\right)\right]\end{aligned} \tag{19}$$

$$\begin{aligned}\tilde{C}_2 &= \mathbb{E}_{\tilde{\gamma}_e}\left[\log_2(1+\tilde{\gamma}_e)\right]\\ &= \log_2(e)\sum_{k=0}^{N_e-1}\binom{N_h-1}{k}\left(\alpha(N_h-1)\right)^{N_h-k-1}\cdot I_1(0,\alpha(N_h-1),k,N_h-1).\end{aligned} \tag{20}$$

$$\begin{aligned}C_1^{2,2,1} &= \log_2(e)\left[\frac{P_a}{P_h\delta_1\delta_2}\cdot I_1\left(\frac{1}{P_a},\frac{P_a}{P_h\delta_2},0,1\right) - \frac{P_a(1-\delta_1)\left(\delta_1^{-1}-1\right)}{P_h\delta_2}\cdot I_1\left(\frac{1}{P_a(1-\delta_1)},\frac{P_a(1-\delta_1)}{P_h\delta_2},0,1\right)\right]\\ &= \log_2(e)\left[\frac{P_a\left(e^{\frac{1}{P_a}}E_1\left(\frac{1}{P_a}\right)-e^{\frac{1}{P_h\delta_2}}E_1\left(\frac{1}{P_h\delta_2}\right)\right)}{\delta_1(P_a-P_h\delta_2)}\right.\\ &\qquad\left.-\frac{P_a(1-\delta_1)\left(\delta_1^{-1}-1\right)\left(e^{\frac{1}{P_a(1-\delta_1)}}E_1\left(\frac{1}{P_a(1-\delta_1)}\right)-e^{\frac{1}{P_h\delta_2}}E_1\left(\frac{1}{P_h\delta_2}\right)\right)}{P_a(1-\delta_1)-P_h\delta_2}\right]\end{aligned} \tag{21}$$

$$\begin{aligned}C_2^{2,2,1} &= \log_2(e)\left(\frac{P_a(N_h-1)}{P_h}\right)^{N_h-1}\cdot I_1\left(\frac{1}{P_a},\frac{P_a(N_h-1)}{P_h},0,N_h-1\right)\\ &= \log_2(e)\frac{P_a}{P_a-P_h}\left[e^{\frac{1}{P_a}}E_1\left(\frac{1}{P_a}\right)-e^{\frac{1}{P_h}}E_1\left(\frac{1}{P_h}\right)\right].\end{aligned} \tag{22}$$

$$\begin{aligned}\tilde{C}_1^{2,2,1} &= \log_2(e)\left[\frac{\alpha}{\delta_1\delta_2}I_1(0,\frac{\alpha}{\delta_2},0,1) - \frac{\alpha(1-\delta_1)\left(\delta_1^{-1}-1\right)}{\delta_2}I_1\left(0,\frac{\alpha(1-\delta_1)}{\delta_2},0,1\right)\right]\\ &= \log_2(e)\left[\frac{\alpha\left(\ln(\alpha)-\ln(\delta_2)\right)}{\delta_1(\alpha-\delta_2)} - \frac{\alpha(1-\delta_1)\left(\delta_1^{-1}-1\right)\left(\ln\left(\alpha(1-\delta_1)\right)-\ln(\delta_2)\right)}{\alpha(1-\delta_1)-\delta_2}\right]\end{aligned} \tag{23}$$

$$\tilde{C}_2^{2,2,1} = \log_2(e)\alpha I_1(0,\alpha,0,1) = \log_2(e)\frac{\alpha\ln\alpha}{\alpha-1}. \tag{24}$$

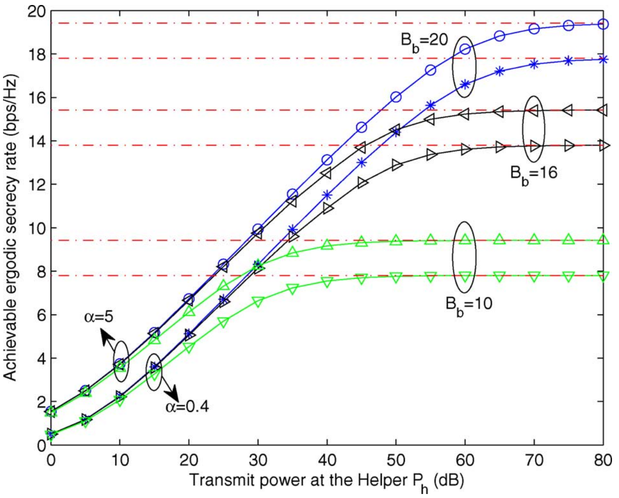


Fig. 1. Achievable ergodic secrecy rate versus transmit power at the Helper for $P_a = \alpha P_h$, when $N_a = N_b = 2, N_e = 1$.

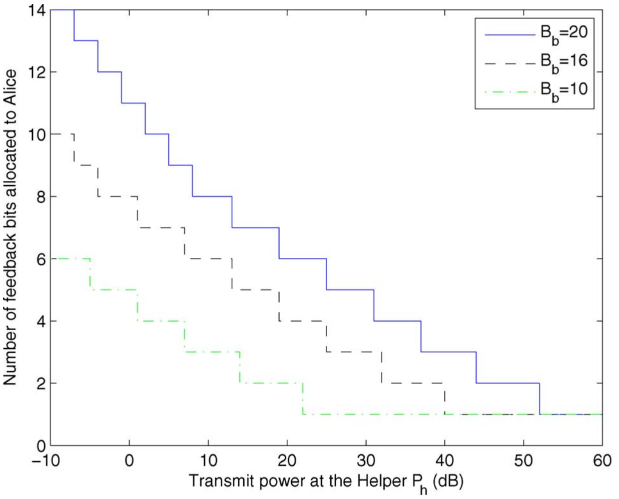


Fig. 2. Number of feedback bits allocated to Alice versus transmit power at the Helper for $P_a = \alpha P_h, \alpha \neq 0$, when $N_a = N_b = 2, N_e = 1$.

secrecy rate for $N_a = N_h = 2, N_e = 1$ in the high SNR regime yields a simple feedback bits allocation strategy, that is only one bit allocated for Alice and the other $B_b - 1$ bits allocated for the Helper.

In Fig. 2, we further show the variation in the number of feedback bits allocated to Alice as a function of P_h for several different values of B_b available to Bob. In Fig. 2, for $N_a = N_h = 2$, $N_e = 1$ and $P_a = \alpha P_h, \alpha \neq 0$, we see that as the power transmitted by the Helper increases, the number of feedback bits allocated to Alice is reduced, due to an increasing need to quantize the interfering channel with greater resolution. In the limit for very high P_h, only one bit is allocated to Alice, and the remaining $B_b - 1$ bits are used to quantize the Helper's channel. Note that this result is independent of α.

While difficult, optimization of the derived ergodic secrecy rate in the general case for arbitrary N_e, N_h, N_a, P_h and P_a over the parameters B_1, B_2 and P_h is possible, especially since the expressions depend only on the channel distributions and thus the required computation can be performed offline. As an alternative, in the next section we consider a simpler approach based on secrecy rate *loss*. We will see that an additional advantage of using secrecy rate loss as a metric is that knowledge of the eavesdropper's parameters (channel variance and number of antennas) is not necessary.

IV. Secrecy Rate Loss With Limited Feedback

Here we derive an upper bound on the secrecy rate loss due to the use of quantized CSI, and then we find the feedback bit allocation to minimize the bound for fixed P_h. The advantage of this approach is that it leads to a simpler closed-form solution, but the disadvantage is that the solution depends on a fixed value of P_h, which must be optimized separately.

A. Characterization of the Secrecy Rate Loss

The secrecy rate loss at Bob due to quantized CDI is given by

$$\Delta R_s \triangleq \mathbb{E}_{\theta_1,\theta_2,\mathbf{e},\mathbf{r}}\left[R_s^{PFB} - R_s^{LFB}\right], \tag{25}$$

where R_s^{PFB} denotes the secrecy rate achieved with perfectCSI:

$$R_s^{PFB} = \left\{R_b^{PFB} - \mathbb{E}_{\mathbf{H}_e,\mathbf{G}_e}\left[R_e^{PFB}\right]\right\}^+, \tag{26}$$

and

$$R_b^{PFB}=\log_2\left(1+P_a\|\mathbf{h}_b\|^2\right)$$
$$R_e^{PFB}=\log_2\left(1+P_a\tilde{\mathbf{h}}_b^H\mathbf{H}_e^H\left(\sigma_e^2\mathbf{I}+\sigma_v^2\mathbf{G}_e\tilde{\boldsymbol{\Gamma}}\tilde{\boldsymbol{\Gamma}}^H\mathbf{G}_e^H\right)^{-1}\mathbf{H}_e\tilde{\mathbf{h}}_b\right).$$

Similar to our previous notation, $\tilde{\boldsymbol{\Gamma}}$ is an orthonormal basis for the nullspace of $\tilde{\mathbf{g}}_b^H$.

Note that $\hat{\mathbf{h}}_b$ and $\tilde{\mathbf{h}}_b$ are isotropically distributed unit-norm vectors independent of $\mathbf{H}_e$. Thus, $\mathbf{H}_e\hat{\mathbf{h}}_b$ and $\mathbf{H}_e\tilde{\mathbf{h}}_b$ have the same distribution. Furthermore, $[\hat{\mathbf{g}}_b^H\ \boldsymbol{\Gamma}]$ and $[\tilde{\mathbf{g}}_b^H\ \tilde{\boldsymbol{\Gamma}}]$ are both unitary matrices independent of $\mathbf{G}_e$, so $\mathbf{G}_e\boldsymbol{\Gamma}$ and $\mathbf{G}_e\tilde{\boldsymbol{\Gamma}}$ have the same distribution. Therefore, the second terms inside the $(\cdot)^+$ operator in both (7) and (26) are identical, i.e.,

$$\mathbb{E}_{\mathbf{H}_e,\mathbf{G}_e}\left[R_e^{LFB}\right] = \mathbb{E}_{\mathbf{H}_e,\mathbf{G}_e}\left[R_e^{PFB}\right]. \tag{27}$$

A similar observation was made in [25], [26]. Thus, for uncorrelated Rayleigh fading at the eavesdropper, analysis of the effect of feedback quantization does not require knowledge of the variance of the eavesdropper's channel nor the number of eavesdropper antennas. Note that while we assume Eve treats the interference as noise here, our argument is still valid if Eve performs interference cancelation.

Since it is clear that $R_s^{PFB} \geq R_s^{LFB}$, the secrecy rate loss in (25) becomes

$$\Delta R_s = \begin{cases} 0 & \text{if } R_s^{PFB} = 0 \\ \mathbb{E}\left[R_s^{PFB}\right] & \text{if } R_s^{LFB} = 0, R_s^{PFB} > 0 \\ \mathbb{E}\left[R_b^{PFB} - R_b^{LFB}\right] & \text{if } R_s^{LFB} > 0. \end{cases} \tag{28}$$

For all three cases in (28), the expression $\mathbb{E}[R_b^{PFB} - R_b^{LFB}]$ serves as an upper bound for ΔR_s. For the first case, if $R_s^{PFB} =$

0, then $R_s^{LFB} = 0$ and $\mathbb{E}[R_b^{PFB} - R_b^{LFB}] = 0 = \Delta R_s$. For the second case, when $R_s^{LFB} = 0$ and $R_s^{PFB} > 0$, then $R_b^{LFB} \leq \mathbb{E}_{\mathbf{H}_e, \mathbf{G}_e}[R_e^{LFB}] = \mathbb{E}_{\mathbf{H}_e, \mathbf{G}_e}[R_e^{PFB}] < R_b^{PFB}$, and thus $\Delta R_s \leq \mathbb{E}[R_b^{PFB} - R_b^{LFB}]$. The third case is obvious. Therefore the secrecy rate loss at the legitimate receiver can be upper-bounded as

$$\begin{aligned}
\Delta R_s &\leq \mathbb{E}\left[R_b^{PFB} - R_b^{LFB}\right] \\
&= \mathbb{E}\left[\log_2\left(1 + P_a\|\mathbf{h}_b\|^2\right)\right] + \mathbb{E}\left[\log_2(1 + I_H)\right] \\
&\quad - \mathbb{E}\left[\log_2\left(1 + P_a\|\mathbf{h}_b\|^2\cos^2\theta_1 + I_H\right)\right] \\
&\overset{(a)}{\leq} \mathbb{E}\left[\log_2\left(1 + P_a\|\mathbf{h}_b\|^2\right)\right] \\
&\quad - \mathbb{E}\left[\log_2\left(1 + P_a\|\mathbf{h}_b\|^2\cos^2\theta_1\right)\right] + \mathbb{E}\left[\log_2(1 + I_H)\right] \\
&= \mathbb{E}\left[-\log_2\left(1 - \frac{P_a\|\mathbf{h}_b\|^2\sin^2\theta_1}{1 + P_a\|\mathbf{h}_b\|^2}\right)\right] + \mathbb{E}\left[\log_2(1 + I_H)\right] \\
&\overset{(b)}{\simeq} \log_2(e)\mathbb{E}\left[\left(1 - \frac{1}{1 + P_a\|\mathbf{h}_b\|^2}\right)\sin^2\theta_1\right] \\
&\quad + \mathbb{E}\left[\log_2(1 + I_H)\right] \\
&\overset{(c)}{\leq} \log_2(e)\left(1 - \frac{1}{1 + P_a\mathbb{E}\left[\|\mathbf{h}_b\|^2\right]}\right)\mathbb{E}\left[\sin^2\theta_1\right] \\
&\quad + \log_2\left(1 + \mathbb{E}[I_H]\right),
\end{aligned} \tag{29}$$

where (a) results because $I_H \geq 0$ and $\log_2$ is monotonically increasing, (b) uses $-\ln(1 - x) \simeq x$ when $x \to 0$, and (c) is obtained by applying Jensen's inequality to (b) and exploiting the independence between the channel norm and channel direction vector. Note that the inequality in (a) will typically be tight, since $I_H \ll P_a\|\mathbf{h}_b\|^2\cos^2\theta_1$ when the power received from Alice is much stronger than the interference leaked from the Helper.

Since $\mathbf{r}$ and each column of $\tilde{\mathbf{\Gamma}}$ are independent and isotropically distributed $N_h - 1$ dimensional vectors, we have as in [22, Lemma 1] that

$$\|\mathbf{r}^H\mathbf{\Gamma}\|^2 = (N_h - 1)\beta(1, N_h - 2), \tag{30}$$

where $\beta(1, N_h - 2)$ is a Beta-distributed random variable with parameters $(1, N_h - 2)$. Furthermore, using $\mathbb{E}[\beta(1, M - 2)] = 1/(M - 1)$ and [23]:

$$\begin{aligned}
\mathbb{E}\left[\|\mathbf{h}_b\|^2\right] &= N_a\sigma_h^2 \qquad \mathbb{E}\left[\|\mathbf{g}_b\|^2\right] = N_h\sigma_g^2 \\
\mathbb{E}[\sin^2\theta_1] &\leq 2^{-\frac{B_1}{N_a - 1}} \quad \mathbb{E}[\sin^2\theta_2] \leq 2^{-\frac{B_2}{N_h - 1}},
\end{aligned}$$

we have

$$\mathbb{E}[I_H] = \mathbb{E}\left[\sigma_v^2\|\mathbf{g}_b\|^2\|\mathbf{r}^H\mathbf{\Gamma}\|^2\sin^2\theta_2\right] \leq P_h\frac{N_h\sigma_g^2}{N_h - 1}2^{-\frac{B_2}{N_h - 1}}, \tag{31}$$

where we also use the fact that random variables $\|\mathbf{g}_k\|^2$, $\sin^2\theta_{k,2}$, $\|\mathbf{r}_k^H\mathbf{\Gamma}\|^2$ are mutually independent [23, Lemma 2].

Finally, we obtain the upper bound of the secrecy rate loss at the legitimate receiver as

$$\begin{aligned}
\Delta R_{s,k} &\leq \log_2(e)\alpha_0 2^{-\alpha B_1} + \log_2(1 + \beta_0 2^{-\beta B_2}) \\
&\leq -\log_2(1 - \alpha_0 2^{-\alpha B_1}) + \log_2(1 + \beta_0 2^{-\beta B_2}) \\
&= \Delta R_s^{UB}
\end{aligned} \tag{32}$$

where

$$\begin{aligned}
\alpha &= \frac{1}{N_a - 1} & \beta &= \frac{1}{N_h - 1} \\
\alpha_0 &= \frac{P_a N_a \sigma_h^2}{1 + P_a N_a \sigma_h^2} & \beta_0 &= P_h\frac{N_h\sigma_g^2}{N_h - 1}.
\end{aligned}$$

B. Feedback Bit Allocation Policy

We assume that the legitimate receiver has a fixed constraint on the total number of available feedback bits, i.e., $B_b = B_1 + B_2$. The feedback bit allocation problem that minimizes the upper bound on the secrecy rate loss can be described as

$$\begin{aligned}
&\min_{B_1, B_2 \in \{0, \mathbb{Z}^+\}} \frac{1 + \beta_0 2^{\beta B_2}}{1\alpha_0 2^{-\alpha B_1}} \\
&\text{s.t.} \qquad B_1 + B_2 = B_b
\end{aligned} \tag{33}$$

The optimization of (33) is a non-linear integer programming problem, and in general the optimal solution must be obtained by an exhaustive search over $B_1 = \{0, \cdots, B_b\}$ with $B_2 = B_b - B_1$. For the special case where $N_a = N_h$, the following closed-form solution can be found by relaxing the integer constraint on B_1, B_2 and treating them as continuous variables. Solving for the resulting unique stationary point yields:

$$\begin{aligned}
B_1^* &= -\frac{1}{\alpha}\log_2\left(-\beta_0 2^{-\alpha B_b} + \frac{\sqrt{(2\alpha_0\beta_0 2^{-\alpha B_b} + 1)^2 - 1}}{2\alpha_0}\right) \\
B_2^* &= B_b - B_1^*.
\end{aligned} \tag{34}$$

One then simply searches the integer values above and below B_1^* to determine the optimal allocation.

Note that (33) is a function of the total number of available bits B_b, the number of transmit antennas N_a, N_h, the transmit power allocations P_a, P_h, and the channel statistics σ_h^2, σ_g^2. Thus, the optimal feedback bit allocation remains fixed as long as the channel statistics and transmit power allocations are constant.

V. Numerical Results

For the simulation results presented here, we consider a flat Rayleigh fading MISO wiretap channel with $N_a = N_h = 4$ and $N_e = 2$. All the channel coefficients were assumed to be i.i.d. complex Gaussian random variables with zero mean and unit variance. Each simulation result was obtained by averaging over 10000 independent channel realizations. Note that, since $N_a = N_h$ in the following examples, taking the integer values closest to the result in (34) can be used to find the bit allocation for minimizing secrecy rate loss. The performance obtained using this approach was found to be identical to that obtained by an exhaustive search.

In the left side of Fig. 3, we plot the actual average achievable secrecy rate assuming RVQ and the analytic ergodic secrecy rate expression in Theorem 1 versus the number of feedback bits allocated to Alice for two different Helper power allocations, where the total number of feedback bits available to Bob is constrained as $B_b = 20$. The right side of the figure shows the mean secrecy rate loss and the upper bound obtained using

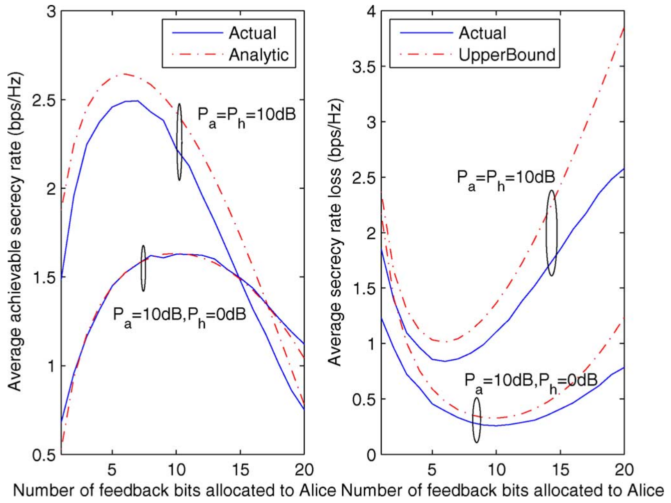


Fig. 3. Average secrecy rate and secrecy rate loss versus number of feedback bits allocated to Alice with $B_b = 20$.

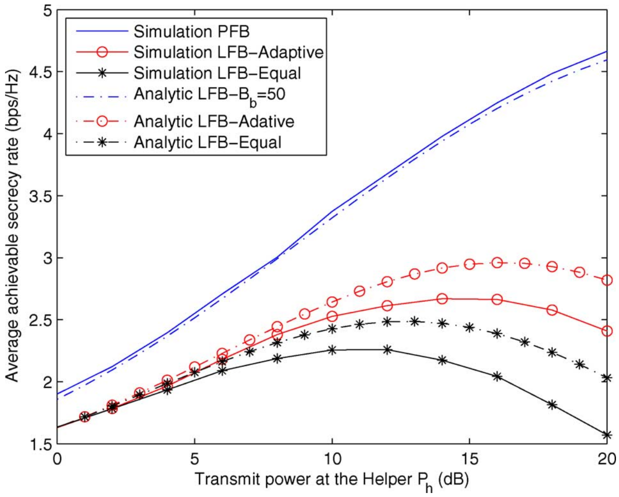


Fig. 4. Average achievable secrecy rate versus transmit power at the Helper for $B_b = 20$, $P_a = 10$ dB.

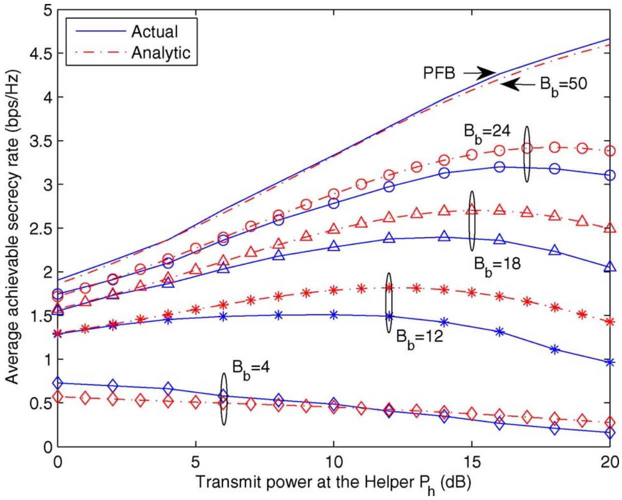


Fig. 5. Average achievable secrecy rate versus transmit power at the Helper with different values of B_b, for $P_a = 10$ dB.

(32). In both cases, we see that optimizing the analytic expression provides essentially the same result as optimizing the actual rate or rate loss. The closed-form solution for the feedback bit allocation in (34) yields $B_1^* = 5.8585$ and hence $B_1 = 6$ when $P_a = P_h = 10$ dB, and $B_1^* = 9.8127$ or $B_1 = 10$ when $P_a = 10$ dB, $P_h = 0$ dB. More bits are allocated to the Helper when its available power increases since the interference leakage from Helper more severely impacts Bob than the loss of gain from Alice.

Fig. 4 compares the average secrecy rate achieved by the ZF-based transmission scheme using RVQ codebooks versus the transmit power at the Helper with different feedback bit allocation strategies. The total number of feedback bits for Bob is $B_b = 20$ and $P_a = 10$ dB. The adaptive feedback bit allocation strategy is obtained by solving the optimization problem (33) using an exhaustive search. While there is a significant gap between the performance obtained with perfect and limited feedback, the adaptive bit allocation policy provides a substantial gain over simply allocating the bits equally between Alice and the Helper. For comparison, we also show the corresponding analytic ergodic secrecy rate obtained in Theorem 1. Although there is a gap in the secrecy rate between these curves as P_h increases, we see the same behavior as a function of P_h. Note there is clearly an optimal power level for P_h. Use of the proposed adaptive feedback bit allocation allows the Helper to be useful for a wider range of P_h; for equal bit allocation, the secrecy rate decreases for values of P_h greater than 12 dB, while for the optimal allocation this only occurs when $P_h > 16$ dB.

The secrecy rate as a function of P_h for several different values of B_b available to Bob are compared in Fig. 5. Not surprisingly, the secrecy rate increases with higher-quality quantization of the CDI. Again, we also see that the optimal transmit power at the Helper decreases as the total number of feedback bits decreases. For example, we see that if B_b is only four, the presence of the Helper actually makes the secrecy performance worse at any power level. This implies that the presence of a Helper providing cooperative jamming is only useful if a sufficient number of bits are available to accurately characterize the CSI. As more bits are added and the ZF-jamming constraint can be more accurately achieved, the benefit of the Helper becomes clear.

VI. Conclusions

In this paper, we have investigated the effect of quantized channel state information on the secrecy rate achievable with a ZF-based transmission strategy in the MISO channel with cooperative jamming. We derived an analytic expression for the ergodic secrecy rate and an upper bound for the secrecy rate loss as a function of the feedback bit allocations to the transmitter and cooperative jammer assuming random vector codebooks. We then studied the problem of optimizing the ergodic secrecy rate and the bound on secrecy rate loss as a function of the feedback allocation, assuming a fixed feedback bandwidth for the legitimate user. Direct maximization of the ergodic secrecy rate is difficult and requires cumbersome numerical methods, but allows one to find the optimal power assignment at the Helper in addition to the optimal feedback bit allocation. On the other hand, minimizing the bound on secrecy rate loss requires a fixed Helper power allocation, but leads to a closed-form solution. Simulations demonstrate that optimally allocating the feedback bits between the transmitter and Helper can lead to a significant improvement in secrecy.

Appendix A

Proof of Lemma 1: Based on the quantization cell approximation [24], the CDF of $\cos^2\theta_1$ is obtained as

$$\begin{aligned} F_{\cos^2\theta_1}(x) &= 1 - F_{\sin^2\theta_1}(1-x) \\ &= \begin{cases} 0, & 0 \le x \le 1-\delta_1 \\ 1 - 2^{B_1}(1-x)^{N_a-1}, & 1-\delta_1 < x \le 1 \\ 1, & x > 1 \end{cases} \end{aligned} \tag{35}$$

where $\delta_1 = 2^{-\frac{B_1}{N_a-1}}$. Thus, the CDF of X is given by

$$\begin{aligned} F_X(x) &= P\left(\|\mathbf{h}_b\|^2 \cos^2\theta_1 \le x\right) \\ &= \int_0^{\frac{x}{1-\delta_1}} f_{\|\mathbf{h}_b\|^2}(y)dy \\ &\quad - \int_x^{\frac{x}{1-\delta_1}} 2^{B_1}\left(1-\frac{x}{y}\right)^{N_a-1} f_{\|\mathbf{h}_b\|^2}(y)dy. \end{aligned} \tag{36}$$

Noting that $\|\mathbf{h}_b\|^2$ has a $\Gamma(N_a, \sigma_h^2)$ distribution, the first term in (36) is given by

$$\begin{aligned} \int_0^{\frac{x}{1-\delta_1}} f_{\|\mathbf{h}_b\|^2}(y)dy &= F_{\|\mathbf{h}_b\|^2}\left(\frac{x}{1-\delta_1}\right) \\ &= 1 - e^{-\frac{x}{\sigma_h^2(1-\delta_1)}} \sum_{i=0}^{N_a-1} \frac{x^i}{i!\sigma_h^{2i}(1-\delta_1)^i}, \end{aligned} \tag{37}$$

and the second term in (36) can be written as

$$\begin{aligned} &\int_x^{\frac{x}{1-\delta_1}} 2^{B_1}\left(1-\frac{x}{y}\right)^{N_a-1} f_{\|\mathbf{h}_b\|^2}(y)dy \\ &\qquad = 2^{B_1} e^{-x/\sigma_h^2} F_{\|\mathbf{h}_b\|^2}\left(\frac{\delta_1}{1-\delta_1}x\right). \end{aligned} \tag{38}$$

Thus,

$$F_X(x) = 1 - 2^{B_1} e^{-x/\sigma_h^2} + e^{-\frac{x}{\sigma_h^2(1-\delta_1)}} \sum_{i=0}^{N_a-1} \frac{(\delta_1^{i-N_a+1}-1)x^i}{i!\sigma_h^{2i}(1-\delta_1)^i}. \tag{39}$$

Appendix B

Proof of Lemma 2: Let $X = \|\mathbf{g}_b\|^2 \sin^2\theta_2$, $Z \sim \beta(1, N_h - 2)$, and suppose X is independent of Z. Then the interference term I_H due to quantization is $I_H = P_h Y$, where $Y = XZ$. Noting that $\|\mathbf{g}_b\|^2$ has a Gamma distribution with parameters (N_h, σ_g^2), we have $X \sim \Gamma(N_h - 1, \sigma_g^2\delta_2)$ with $\delta_2 = 2^{-\frac{B_2}{N_h-1}}$ [24, Lemma 1]. Thus the CDF of Y is

$$\begin{aligned} &F_Y(y) \\ &= P(XZ \le y) = \int_0^\infty F_Z\left(\frac{y}{x}\right) f_X(x)dx \\ &= \int_0^y f_X(x)dx + \int_y^\infty \left(1 - \left(1-\frac{y}{x}\right)^{N_h-2}\right) f_X(x)dx \\ &= 1 - e^{-y/(\sigma_g^2\delta_2)}, \end{aligned} \tag{40}$$

which is the CDF of an exponential random variable with mean $\sigma_g^2\delta_2$. From this, it is easy to show that I_H is an exponential random variable with mean $P_h\sigma_g^2\delta_2$.

Appendix C

Proof of Theorem 1: First denote $X = P_a\|\mathbf{h}_b\|^2\cos^2\theta_1$, $Y = I_H$, then $\gamma_b = \frac{X}{1+Y}$. Using Lemma 1 and Lemma 2, the CDF of the random variable γ_b can be derived as

$$\begin{aligned} &F_{\gamma_b}(x) \\ &= \int_0^\infty F_X\left((1+y)x\right) f_Y(y)dy \\ &= 1 - \frac{P_a\sigma_h^2 2^{B_1}}{P_h\sigma_g^2\delta_2} \frac{e^{-\frac{x}{P_a\sigma_h^2}}}{x + \frac{P_a\sigma_h^2}{P_h\sigma_g^2\delta_2}} \\ &\quad + \sum_{i=0}^{N_a-1}\sum_{l=0}^{i} \frac{\left(P_a\sigma_h^2(1-\delta_1)\right)^{l+1-i}\left(\delta_1^{i-N_a+1}-1\right)}{P_h\sigma_g^2\delta_2(i-l)!} \\ &\quad \cdot \frac{e^{-\frac{x}{P_a\sigma_h^2(1-\delta_1)}} x^i}{\left(x + \frac{P_a\sigma_h^2(1-\delta_1)}{P_h\sigma_g^2\delta_2}\right)^{l+1}}. \end{aligned} \tag{41}$$

Then

$$\begin{aligned} &\mathbb{E}_{\gamma_b}\left[\log_2(1+\gamma_b)\right] \\ &= \log_2(e)\int_0^\infty \ln(1+x) f_{\gamma_b}(x)dx \\ &\overset{(a)}{=} \log_2(e)\int_0^\infty \frac{1-F_{\gamma_b}(x)}{x+1}dx \\ &= \log_2(e)\frac{P_a\sigma_h^2}{P_h\sigma_g^2\delta_2\delta_1^{N_a-1}} \cdot I_1\left(\frac{1}{P_a\sigma_h^2}, \frac{P_a\sigma_h^2}{P_h\sigma_g^2\delta_2}, 0, 1\right) \\ &\quad - \log_2(e)\sum_{i=0}^{N_a-1}\sum_{l=0}^{i} \frac{\left(P_a\sigma_h^2(1-\delta_1)\right)^{l+1-i}\left(\delta_1^{i-N_a+1}-1\right)}{P_h\sigma_g^2\delta_2(i-l)!} \\ &\quad \cdot I_1\left(\frac{1}{P_a\sigma_h^2(1-\delta_1)}, \frac{P_a\sigma_h^2(1-\delta_1)}{P_h\sigma_g^2\delta_2}, i, l+1\right), \end{aligned} \tag{42}$$

where (a) follows from integration by parts, and

$$I_1(a,b,m,n) = \int_0^\infty \frac{x^m e^{-ax}}{(x+b)^n(x+1)}dx. \tag{43}$$

From Lemma 3, we have the complementary CDF of γ_e as follows:

$$\begin{aligned}R_{\gamma_e}(y) &= \begin{cases} e^{-\frac{y}{\gamma}}\sum_{m=1}^{N_e}\frac{A'_m(y)}{(m-1)!}\left(\frac{y}{\gamma}\right)^{m-1} & \text{if } N_e < N_h \\ e^{-\frac{y}{\gamma}}\sum_{m=1}^{N_e-N_h+1}\frac{\left(\frac{y}{\gamma}\right)^{m-1}}{(m-1)!} & \\ \quad +e^{-\frac{y}{\gamma}}\sum_{m=N_e-N_h+2}^{N_e}\frac{A'_m(y)}{(m-1)!}\left(\frac{y}{\gamma}\right)^{m-1} & \text{if } N_e \geq N_h, \end{cases}\end{aligned} \tag{44}$$

where $\gamma = P_a\sigma_{he}^2$,

$$A'_m(y) = \frac{1+\sum_{i=1}^{N_e-m}D_i y^i}{\left(1+\frac{\sigma_v^2\sigma_{ge}^2}{P_a\sigma_{he}^2}y\right)^{N_h-1}},$$

and D_i is the coefficient of y^i in $\left(1+\frac{\sigma_v^2\sigma_{ge}^2}{P_a\sigma_{he}^2}y\right)^{N_h-1}$. In order to obtain a unified expression for $R_{\gamma_e}(y)$, we rewrite it as follows:

$$\begin{aligned}R_{\gamma_e}(y) &= e^{-\frac{y}{P_a\sigma_{he}^2}}\sum_{m=1}^{N_e-N_h+1}\frac{1}{(m-1)!}\left(\frac{y}{P_a\sigma_{he}^2}\right)^{m-1} \\ &+e^{-\frac{y}{P_a\sigma_{he}^2}}\sum_{m=\max\{1,N_e-N_h+2\}}^{N_e}\frac{A'_m(y)}{(m-1)!}\left(\frac{y}{P_a\sigma_{he}^2}\right)^{m-1}.\end{aligned} \tag{45}$$

Thus

$$\begin{aligned}&\mathbb{E}_{\gamma_e}\left[\log_2(1+\gamma_e)\right] \\ &= \log_2(e)\int_0^\infty \frac{R_{\gamma_e}(y)}{y+1}dy \\ &= \log_2(e)\sum_{m=1}^{N_e-N_h+1}\frac{1}{(m-1)!\left(P_a\sigma_{he}^2\right)^{m-1}} \\ &\quad\times I_2\left(\frac{1}{P_a\sigma_{he}^2},1,m-1,1\right) \\ &\quad+\log_2(e)\sum_{m=\max\{1,N_e-N_h+2\}}^{N_e}\frac{\left(P_a\sigma_{he}^2\right)^{N_h-m}}{(m-1)!(\sigma_v^2\sigma_{ge}^2)^{N_h-1}} \\ &\quad\times\left[I_1\left(\frac{1}{P_a\sigma_{he}^2},\frac{P_a\sigma_{he}^2}{\sigma_v^2\sigma_{ge}^2},m-1,N_h-1\right)\right. \\ &\quad+\sum_{i=1}^{N_e-m}\binom{N_h-1}{i}\left(\frac{\sigma_v^2\sigma_{ge}^2}{P_a\sigma_{he}^2}\right)^i \\ &\quad\left.\cdot I_1\left(\frac{1}{P_a\sigma_{he}^2},\frac{P_a\sigma_{he}^2}{\sigma_v^2\sigma_{ge}^2},m+i-1,N_h-1\right)\right]\end{aligned} \tag{46}$$

A closed-form expression for the integral I_1 can be found as follows:

$$\begin{aligned}&I_1(a,b,m,n) \\ &= \sum_{i=1}^{n}\frac{(-1)^{i-1}}{(1-b)^i}\cdot I_2(a,b,m,n-i+1)+\frac{I_2(a,1,m,1)}{(b-1)^n},\end{aligned} \tag{47}$$

where

$$\begin{aligned}I_2(a,b,m,n) &= \int_0^\infty \frac{x^m e^{-ax}}{(x+b)^n}dx \\ &= e^{ab}\sum_{i=0}^{m}\binom{m}{i}(-b)^{m-i}I_0(a,b,i-n)\end{aligned} \tag{48}$$

and $I_0(\cdot,\cdot,\cdot)$ is the integral

$$I_0(a,b,m) = \int_b^\infty x^m e^{-ax}dx \tag{49}$$

with closed-form expression

$$\begin{aligned}I_0(a,b,m) &= \int_b^\infty x^m e^{-ax}dx = a^{-(m+1)}\Gamma(m+1,ab) \\ &= \begin{cases} m!e^{-ab}\sum_{i=0}^{m}\frac{b^i}{i!a^{m-i+1}}, & m\geq 0 \\ E_1(ab), & m=-1 \\ \frac{(-a)^{-m-1}}{(-m-1)!}\left(E_1(ab)-e^{-ab}\sum_{i=0}^{-m-2}\frac{(-1)^i i!}{(ab)^{i+1}}\right), & m\leq -2\end{cases}\end{aligned} \tag{50}$$

where $E_1(x)$ is the exponential integral function of the first order [33].

Appendix D

Proof of Theorem 2: The proof is similar to the one in Appendix C for Theorem 1. For simplicity, we only provide some key steps of the proof. First, let $P_a = \alpha P_h$, $\sigma_h = \sigma_g = \sigma_{he} = \sigma_{ge} = 1$, using Lemma 1 and Lemma 2, the CDF of the random variable $\tilde{\gamma}_b$ can be derived as

$$\begin{aligned}F_{\tilde{\gamma}_b}(x) &= 1-\frac{\alpha 2_1^B}{\delta_2}\frac{1}{x+\frac{\alpha}{\delta_2}} \\ &\quad+\sum_{i=0}^{N_a-1}\frac{\alpha(1-\delta_1)(\delta_1^{i-N_a+1}-1)}{\delta_2}\frac{x^i}{\left(x+\frac{\alpha(1-\delta_1)}{\delta_2}\right)^{i+1}}.\end{aligned} \tag{51}$$

Then

$$\begin{aligned}\tilde{C}_1 &= \mathbb{E}_{\tilde{\gamma}_b}\left[\log_2(1+\tilde{\gamma}_b)\right] \\ &= \log_2(e)g\left[\frac{\alpha}{\delta_2\delta_1^{N_a-1}}\cdot I_1(0,\frac{\alpha}{\delta_2},0,1)\right. \\ &\quad-\sum_{i=0}^{N_a-1}\frac{\alpha(1-\delta_1)\left(\delta_1^{i-N_a+1}-1\right)}{\delta_2} \\ &\quad\left.\times I_1\left(0,\frac{\alpha(1-\delta_1)}{\delta_2},i,i+1\right)\right].\end{aligned} \tag{52}$$

The quantity $\mathbf{u}_0^H\left(\sum_{n=1}^{N_h-1}\mathbf{u}_n\mathbf{u}_n^H\right)^{-1}\mathbf{u}_0$ is equivalent to the signal-to-interference ratio of an N_e-branch MMSE diversity combiner with $N_h - 1$ interferers. The CDF of $Z = \mathbf{u}_0^H(\sum_{n=1}^{N_h-1}\mathbf{u}_n\mathbf{u}_n^H)^{-1}\mathbf{u}_0$ is given in [32, eq. (18)] as

$$R_Z(z) = \begin{cases} 1, & N_e \geq N_h \\ \frac{\sum_{k=0}^{N_e-1}\binom{N_h-1}{k}z^k}{(1+z)^{N_h-1}}, & N_e < N_h \end{cases} \tag{53}$$

Thus,

$$\begin{aligned}\tilde{C}_2 &= \mathbb{E}_{\tilde{\gamma}_e}\left[\log_2(1+\tilde{\gamma}_e)\right] \\ &= \begin{cases} \infty, & N_e \geq N_h \\ \log_2(e)\sum_{k=0}^{N_e-1}\binom{N_h-1}{k}\left(\alpha(N_h-1)\right)^{N_h-k-1} & \\ \quad\cdot I_1\left(0, \alpha(N_h-1), k, N_h-1\right), & N_e < N_h \end{cases}\end{aligned} \tag{54}$$

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 2466–2470.

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

[4] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[5] S.-C. Lin and P.-H. Lin, "On secrecy capacity of fast fading multiple-input wiretap channels with statistical CSIT," *IEEE Trans. Inf. Forens. Secur.*, vol. 8, no. 2, pp. 414–419, Feb. 2013.

[6] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wiretap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

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

[10] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, Apr. 2009, pp. 2437–2440.

[11] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access Wiretap channel with collective secrecy," in *Proc. 44th Annu. Allerton Conf. Commun., Contr., Comput.*, Sep. 2006, pp. 809–816.

[12] E. Tekin and A. Yener, "The Gaussian multiple access wiretap channel: Wireless secrecy and cooperative jamming," in *Proc. Inf. Theory and Appl. Workshop, ITA'07*, San Diego, CA, Jan. 2007, pp. 404–413.

[13] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[14] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[15] J. Wang and A. Swindlehurst, "Cooperative jamming in MIMO *ad-hoc* networks," in *Proc. 43rd Asilomar Conf. Signals, Syst. Comput.*, 2009, pp. 1719–1723.

[16] X. He and A. Yener, "Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels," *IEEE Trans. Inf. Theory*, Jul. 2009, available at arXiv:0907.5388, submitted for publication.

[17] S. A. A. Fakoorian and A. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[18] A. Wolf and E. A. Jorswieck, "On the zero forcing optimality for friendly jamming in MISO wiretap channels," in *Proc. IEEE 11th Int. Workshop on Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2010, pp. 1–5.

[19] S. A. A. Fakoorian and A. L. Swindlehurst, "Secrecy capacity of MISO Gaussian wiretap channel with a cooperative jammer," in *Proc. IEEE 12th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, June 2011, pp. 416–420.

[20] 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, no. 10, pp. 2562–2579, Oct. 2003.

[21] W. Santipach and M. Honig, "Asymptotic capacity of beamforming with limited feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2004, pp. 290–295.

[22] J. C. Roh and B. D. Rao, "Transmit beamforming in multiple-antenna systems with finite rate feedback: A VQ-based approach," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1101–1112, Mar. 2006.

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

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

[25] 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," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[26] L. Sun and S. Jin, "On the ergodic secrecy rate of multiple-antenna wiretap channels using artificial noise and finite-rate feedback," in *Proc. IEEE Int. Symp. Pers. Indoor and Mobile Radio Commun. (PIMRC)*, Sep. 2011, pp. 1264–1268.

[27] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.

[28] K. Huang and R. Zhang, "Cooperative precoding with limited feedback for MIMO interference channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1012–1021, Mar. 2012.

[29] R. Bhagavatula and R. W. Heath, "Adaptive limited feedback for sum-rate maximizing beamforming in cooperative multicell systems," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 800–811, Feb. 2011.

[30] S. Yu, H. Kong, Y. Kim, S. Park, and I. Lee, "Novel feedback bit allocation methods for multi-cell joint processing systems," *IEEE Trans. Wireless Commun.*, vol. PP, no. 99, pp. 1–7, 2012.

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

[32] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.

[33] I. S. Gradshteyn and I. M. Ryzhik, , A. Jeffrey and D. Zwillinger, Eds., *Table of Integrals, Series, Products*, 7th ed. New York, NY, USA: Academic, 2007.

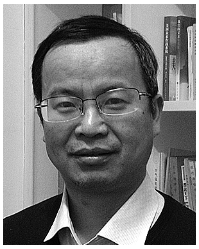
Minyan Pei received the B.Sc. degree in applied mathematics from Peking University, Beijing, China, in 2007, and the Ph.D. degree in information and communication engineering from the National University of Defense Technology (NUDT), Changsha, China, in 2013.

From November 2011 to November 2012, she was a Visiting Student at the Center for Pervasive Communications and Computing (CPCC), University of California Irvine, CA, under the supervision of Professor A. Lee Swindlehurst. She is currently with the College of Electronic Science and Engineering at NUDT. Her research interests are in signal processing for wireless communications, including multiple-input-multiple-output systems, cooperative communication, and physical-layer security.

A. Lee Swindlehurst received the B.S. (*summa cum laude*) and M.S. degrees in electrical engineering from Brigham Young University, Provo, UT, in 1985 and 1986, respectively, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, in 1991.

From 1986 to 1990, he was with ESL, Inc., Sunnyvale, CA, where he was involved in the design of algorithms and architectures for several radar and sonar signal processing systems. He was on the faculty of the Department of Electrical and Computer Engineering at Brigham Young University from 1990–2007, where he was a Full Professor and served as Department Chair from 2003–2006. During 1996–1997, he held a joint appointment as a visiting scholar at both Uppsala University, Uppsala, Sweden, and at the Royal Institute of Technology, Stockholm, Sweden. From 2006–2007, he was on leave working as Vice President of Research for ArrayComm LLC, San Jose, CA. He is currently the Associate Dean for Research and Graduate Studies in the Henry Samueli School of Engineering and a Professor of the Electrical Engineering and Computer Science Department at the University of California, Irvine. His research interests include sensor array signal processing for radar and wireless communications, detection and estimation theory, and system identification, and he has over 230 publications in these areas.

Prof. Swindlehurst is a past Secretary of the IEEE Signal Processing Society, past Editor-in-Chief of the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, and past member of the Editorial Boards for the EURASIP *Journal on Wireless Communications and Networking* and the IEEE SIGNAL PROCESSING MAGAZINE the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He is a recipient of several paper awards: the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 and 2010 IEEE Signal Processing Society's Best Paper Awards, the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory, and is coauthor of a paper that received the IEEE Signal Processing Society Young Author Best Paper Award in 2001.



Dongtang Ma received the B.S. degree in applied physics and the M.S. and Ph.D. degrees in information and communication engineering from the National University of Defense Technology (NUDT), Changsha, P. R. China, in 1990, 1997, and 2004, respectively.

From 2004 to 2009, he was an Associate Professor with the College of Electronic Science and Engineering, NUDT. Since 2009, he is a Professor in the Department of Communication Engineering, College of Electronic Science and Engineering, NUDT. From August 2012 to February 2013, he was a Visiting Professor at CCSR, University of Surrey, UK. His research interests include physical layer security, cooperative communication and networks, multiple-input-multiple-output (MIMO), and space communication.

Prof. Ma is an IEEE member and one of the Executive Directors of Hunan Electronic Institute.

Jibo Wei received the B.S. and M.S. degrees in Electronic Engineering from the National University of Defense Technology (NUDT), Changsha, China, in 1989 and 1992, and the Ph.D. degree in electronic engineering from Southeast University, Nanjing, China, in 1998.

He is currently the Director and a Professor of the Department of Communication Engineering at NUDT. His research interests include wireless network protocol and signal processing in communications, more specially, the areas of multiple-input-multiple-output (MIMO), multicarrier transmission, cooperative communication, and cognitive network.

Prof. Wei is the member of the IEEE Communication and Vehicular Technology Societies. He is also an editor for the *Journal on Communications* and the Senior Member of China Institute of Communications and Electronics.