Artificial-Noise-Aided Secure Multi-Antenna Transmission With Limited Feedback

Xi Zhang, *Member, IEEE*, Matthew R. McKay, *Senior Member, IEEE*,
Xiangyun Zhou, *Member, IEEE*, and Robert W. Heath, Jr., *Fellow, IEEE*

***Abstract*—We present an optimized secure multi-antenna transmission approach based on artificial-noise-aided beamforming, with limited feedback from a desired single-antenna receiver. To deal with beamformer quantization errors as well as unknown eavesdropper channel characteristics, our approach is aimed at maximizing throughput under dual performance constraints—a connection outage constraint on the desired communication channel and a secrecy outage constraint to guard against eavesdropping. We propose an adaptive transmission strategy that judiciously selects the wiretap coding parameters, as well as the power allocation between the artificial noise and the information signal. This optimized solution reveals several important differences with respect to solutions designed previously under the assumption of perfect feedback. We also investigate the problem of how to most efficiently utilize the feedback bits. The simulation results indicate that a good design strategy is to use approximately 20% of these bits to quantize the channel gain information, with the remainder to quantize the channel direction, and this allocation is largely insensitive to the secrecy outage constraint imposed. In addition, we find that 8 feedback bits per transmit antenna is sufficient to achieve approximately 90% of the throughput attainable with perfect feedback.**

***Index Terms*—Artificial noise, adaptive transmission, limited feedback, physical-layer security, power allocation.**

I. Introduction

As a means of providing enhanced security to wireless networks, physical-layer methods have been receiving considerable attention from the research community [2]–[5]. In this context, secure techniques for various contemporary architectures have now been considered, including multi-input multi-output systems, relaying systems, cognitive-radio systems, and large-scale networks (see [6]–[11] and references therein). A common assumption in work on wireless physical-layer security is that the transmitter has accurate knowledge of the channel to its desired communicating receiver, and in some cases also perfect knowledge of the channel to the eavesdroppers. In general, knowing the eavesdropper channels appears questionable in practice, particularly if such eavesdroppers are "passive" and remain quiet. In addition, typically only an approximation for the desired communication channel may be assumed at the transmitter; due, for example, to practical finite-rate constraints on feedback links (which may be insecure) from the desired receiver to the transmitter.

If multiple antennas are available at the transmitter, intelligent signal processing may be used to provide security against unknown passive eavesdroppers. This idea has been exploited in [12]–[18], where artificial noise is generated in a controlled manner to degrade the eavesdropper's signal reception, while, in theory, not causing additional noise at the desired receiver. The solutions in [12]–[18] all assume perfect knowledge of the desired receiver's channel at the transmitter (utilized for appropriate beamformer design). Recently, various contributions have attempted to relax this requirement, allowing for certain channel imperfections at the transmitter. In particular, the study in [19]–[24] focused on the transmission design and analysis when the channel of the desired receiver is assumed to be known at the transmitter but with unbounded Gaussian errors. This modeling is most appropriate for specifying errors caused by imperfect channel estimation, but it does not model nor address the problem of practical limited-feedback constraints.

Limited feedback channels are important in practice, particularly in widely-used frequency division duplex (FDD) systems, for which the channel knowledge is typically obtained at the receiver through the use of pilot training, and conveyed to the transmitter through the use of digital feedback. Hence, it is important to study secure transmission design under such conditions with limited feedback constraints. Along this line, only a limited amount of work has been done [25]–[28]. To be specific, [25] characterized the ergodic secrecy rate performance for single-antenna systems. With multiple transmit antennas, [26] analyzed the secrecy outage probability in slow fading channels without using artificial noise. For fast fading channels, considering beamforming with artificial noise, [27] provided optimal power allocation that maximizes the ergodic secrecy rate in two asymptotic regions, while [28] derived a lower bound to the ergodic secrecy capacity in integral form and studied the optimal power allocation numerically.

Manuscript received April 25, 2014; revised September 6, 2014 and December 21, 2014; accepted December 29, 2014. Date of publication January 13, 2015; date of current version May 7, 2015. The work of X. Zhang and M. R. McKay was supported by the Hong Kong Research Grants Council under Grant No. 616312. The work of R. W. Heath was supported by the National Science Foundation under Grant No. NSF-CCF-1218338. This work was presented in part at the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Florence, Italy, May 2014. The associate editor coordinating the review of this paper and approving it for publication was H. Wymeersch.

X. Zhang was with the Department of Electronic and Computer Engineering, the Hong Kong University of Science and Technology, Kowloon, Hong Kong. He is now with the Communication Technology Laboratory, Huawei Technologies Co., Ltd., People's Republic of China (e-mail: panda.zhang@huawei.com).

M. R. McKay is with the Department of Electronic and Computer Engineering, the Hong Kong University of Science and Technology, Kowloon, Hong Kong (e-mail: eemckay@ust.hk).

X. Zhou is with the Research School of Engineering, the Australian National University, Canberra, ACT 0200, Australia (e-mail: xiangyun.zhou@anu.edu.au).

R. W. Heath, Jr. is with the Department of Electrical and Computer Engineering, the University of Texas at Austin, Austin, TX 78712 USA (e-mail: rheath@utexas.edu).

Digital Object Identifier 10.1109/TWC.2015.2391261

In this paper, we consider a scenario where a multi-antenna transmitter communicates with a desired single-antenna receiver in the presence of a passive eavesdropper, assuming that there exists a limited-rate feedback channel from the desired receiver to the transmitter. Different from the single-antenna system in [25], our transmitter is equipped with multiple transmit antennas, thus providing more flexibility in signal processing. Instead of the traditional beamforming approach in [26], artificial-noise-aided beamforming is adopted in this work to provide enhanced security performance. In contrast to the fast fading channels in [27], [28], we consider a slow fading scenario, and seek to design optimized artificial-noise-aided transmission under suitably chosen outage performance measures (as opposed to ergodic rate). Due to the limited feedback constraint, a key challenge faced in the design of artificial-noise-aided beamforming systems is the artificial noise leakage into the desired communication channel, caused by beamformer quantization errors. To deal with this issue, while also accounting for the lack of eavesdropper channel knowledge, we present a novel optimized rate-adaptive transmission approach aimed to maximize throughput under dual performance constraints. The first is a *connection outage* constraint, which specifies a maximal outage level on the desired communication channel; the second is a *secrecy outage* constraint, which governs the level of security against eavesdropping for a "worst-case" scenario with zero thermal noise at the eavesdropper. We develop an adaptive transmission strategy that judiciously selects the wiretap coding parameters (i.e., the coding rate and the rate redundancy for achieving secrecy), as well as the optimal power allocation between the artificial noise and the information signal. Our optimized solution reveals several important differences with respect to solutions designed previously under the assumption of perfect feedback [17], as well as providing practical engineering design insights and guidelines. These are summarized as follows.

1) In terms of maximizing the secrecy throughput, the relative amount of available transmit power to allocate to the information signal and the artificial noise depends on the number of feedback bits and the total power available. With additional feedback bits, the transmitter gains confidence in regards to the desired communication channel, and the optimal strategy is to allocate less power to the information signal and give more to the artificial noise. If the total available power is increased, with limited feedback, the optimal power allocation strategy is to give a larger fraction of this power to the information signal and less to the artificial noise. This is in contrast to the optimal power allocation strategy with perfect knowledge of the desired communication channel (i.e., with unlimited feedback), for which the optimal power split between the information signal and artificial noise tends to be fixed as the transmit power grows large.
2) In our previous work [17], we showed that with perfect knowledge of the desired communication channel (i.e., unlimited feedback), the secrecy throughput grows unbounded with increasing transmit power. Here in this paper, we point out that with only limited feedback from the desired receiver, even with an arbitrarily large transmit power, the secrecy throughput remains bounded.
3) Simulation results indicate that for a given total number of feedback bits, a good "rule of thumb" is to allocate roughly 80% of the bits for specifying the channel direction information (CDI), and the remainder for specifying the channel gain information (CGI). This allocation strategy gives near-optimal secrecy throughput performance for a wide range of system parameters, and in particular, its optimality is insensitive to the secrecy outage constraint.
4) In terms of the number of feedback bits required, for practical finite transmission powers, roughly 8 feedback bits *per antenna* is sufficient to achieve 90% of the secrecy throughput achievable with perfect knowledge of the desired communication channel (i.e., unlimited feedback).

II. System Model

To model a slow-varying rich-scattering environment, we consider Rayleigh fading channels that remain constant for each message transmission and change independently from one transmission block to the next. The transmitter is equipped with $N \geq 2$ antennas, while the desired receiver and the eavesdropper each has only a single antenna. The received signal at the desired receiver can be written as

$$y_d = \mathbf{h}^H \mathbf{x} + n_d \tag{1}$$

where $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$ is the desired communication channel, $\mathbf{x}$ is the transmitted vector, and $n_d \sim \mathcal{CN}(0, \sigma_d^2)$ is the thermal noise. The received signal at the eavesdropper is

$$y_e = \mathbf{g}^H \mathbf{x} + n_e \tag{2}$$

where $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \sigma_g^2 \mathbf{I}_N)$ is the channel to the eavesdropper. Note that here we did not specify a value for σ_g^2. Also, the thermal noise level at the eavesdropper is typically unknown. To facilitate a robust secure transmission design, we consider a "worst-case" scenario with $n_e = 0$.

A. Limited Feedback and Quantization

In this paper, we consider the situation with limited feedback [29]–[39] from the desired receiver and no feedback from the eavesdropper. For each channel realization, the transmitter first sends a sequence of training symbols. After receiving these, the desired receiver and the eavesdropper both perform channel estimation to obtain knowledge of their own channel, which is assumed to be perfect. While the eavesdropper does not disclose its channel information, the desired receiver decomposes the obtained channel information $\mathbf{h}$ into the CDI $\mathbf{h}/\|\mathbf{h}\|$ and the CGI $\|\mathbf{h}\|$, which are important for beamforming and rate-adaptation, respectively. This information is conveyed to the transmitter via B feedback bits: B_1 bits to quantize the CDI and $B_2 = B - B_1$ bits to quantize the CGI. Note that the CGI is real and positive, thus it can be quantized efficiently using a small number of bits [37]. Meanwhile, the CDI is a N-dimensional unit-norm complex vector. To quantize the CDI, we choose 2^{B_1} unit-norm vectors to form a codebook $\mathcal{C} = \{\mathbf{c}_1, \ldots, \mathbf{c}_{2^{B_1}}\}$, known at both the transmitter and receiver. An index $\hat{\ell} = \arg\max_{\ell \in \{1,\ldots,2^{B_1}\}} |\mathbf{c}_\ell^H \mathbf{h}|$ is computed by the receiver and fed back to the transmitter. Therefore, $\mathbf{c}_{\hat{\ell}}$ is the quantized CDI available at the transmitter.

A common method for generating the quantization codebook $\mathcal{C}$ (though, used mainly for performance analysis purposes) is to employ random vector quantization (RVQ), which independently selects the codebook entries from a uniform distribution on the unit complex hypersphere [31], [34], [35]. One can typically achieve better performance, however, with properly designed *deterministic* quantization codebooks, and these have been thoroughly investigated [32], [33]. In [32], for example, the codebook design was addressed by relating to the problem of Grassmannian line packing, and the resulting design criterion for a good quantization codebook was to minimize the maximum correlation between any pair of quantization vectors. The quantization codebooks used in this paper are generated following this criterion.

For a codebook $\mathcal{C}$, the quantization cell associated with $\mathbf{c}_\ell \in \mathcal{C}$ is given by $\mathcal{V}_\ell = \{\mathbf{z} | \|\mathbf{z}\| = 1, |\mathbf{z}^H \mathbf{c}_\ell| \geq |\mathbf{z}^H \mathbf{c}_j|, \forall j \neq \ell\}$. To facilitate our later analysis, as done in [32]–[37], we approximate $\mathcal{V}_\ell$ by:

$$\tilde{\mathcal{V}}_\ell = \left\{ \mathbf{z} | \|\mathbf{z}\| = 1, \left|\mathbf{z}^H \mathbf{c}_\ell\right|^2 \geq 1 - 2^{-\frac{B_1}{N-1}} \right\} \tag{3}$$

where the quantity $2^{-B_1/(N-1)}$ reflects the maximum quantization error in the CDI. This approximation was first introduced in [32], [33] and then used in [34]. The approximated quantization cell can be viewed as a spherical cap on the unit complex hypersphere. As will be seen later, this quantization cell approximation not only allows one to characterize the distribution of quantization error (see Lemma 6 in [35]), but also provides an accurate performance indication for any well-designed quantization codebook [32]–[37].

B. Artificial-Noise-Aided Beamforming

Denote the information signal by $u \sim \mathcal{CN}(0, \sigma_u^2)$. Define a power allocation ratio ϕ as the ratio of the information signal power σ_u^2 to the total transmit power P. Thus, $\sigma_u^2 = P\phi$. To confuse the eavesdropper, the transmitter performs artificial-noise-aided beamforming [12] by aligning the information signal along the informed channel direction and injecting artificial noise in orthogonal directions. To be specific, given $\hat{\ell}$, the transmitted vector $\mathbf{x}$ in (1) admits:

$$\mathbf{x} = \mathbf{c}_{\hat{\ell}} u + \mathbf{W}\mathbf{v} \tag{4}$$

where $\mathbf{W}$ is a $N \times (N-1)$ complex matrix with $[\mathbf{c}_{\hat{\ell}}, \mathbf{W}]$ being an orthonormal basis, and $\mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \sigma_v^2 \mathbf{I}_{N-1})$ is the artificial noise vector with $\sigma_v^2 = P(1-\phi)/(N-1)$. Note that this beamforming strategy does not require knowledge of the CGI.

C. Wiretap Coding and Outages

Before transmission, the data is encoded using Wyner's well-known wiretap coding scheme [2]. The codeword rate and the confidential information rate are denoted by R_b and R_s, respectively. The codeword rate R_b is the actual transmission rate of the codewords, while the confidential information rate R_s is the rate of the embedded secret message, to be sent to the desired receiver. The rate redundancy $R_e := R_b - R_s$ provides secrecy against eavesdropping. More discussion on code construction can be found in [40].

Without the eavesdropper's instantaneous channel information, the maximum confidential information rate with perfect secrecy (i.e., the difference between the channel capacities to the desired receiver and the eavesdropper) is unknown and thereby unachievable. Furthermore, with only quantized channel information of the desired receiver, the widely used performance metric—*outage probability of secrecy capacity* [4]—is no longer a suitable performance measure, as it does not lead to any directly applicable wiretap coding scheme. In this case, we appeal to a revised secrecy outage formulation proposed in [41], [42] to exploit the statistical knowledge of the quantization error and the eavesdropper's channel. That is, we choose the largest possible codeword rate R_b while keeping the required decoding reliability at the desired receiver, and choose the smallest possible rate redundancy R_e while providing the required security performance against eavesdropping, both from a probabilistic sense. By doing so, we maximize the achievable confidential information rate $R_s = R_b - R_e$, which is delivered to the desired receiver while the risks of decoding error and being eavesdropped are both under control. More specifically, if the channel from the transmitter to the desired receiver cannot support R_b, the transmitted message cannot be decoded correctly and we consider this a *connection outage* event. If the channel from the transmitter to the eavesdropper can support a data rate larger than R_e, perfect secrecy cannot be achieved and a *secrecy outage* event is deemed to occur. In the next section, we first characterize the connection and secrecy outage probabilities.

III. Outage Performance Analysis

In this section, we first analyze the connection and secrecy outage performance of the artificial-noise-aided beamforming scheme with limited feedback.

A. Connection Outage Probability

The connection outage probability is defined as the probability that the capacity of the desired communication channel falls below a preselected codeword rate R_b. Denote the instantaneous CDI by $\mathbf{d} = \mathbf{h}/\|\mathbf{h}\|$. Given a feedback index $\hat{\ell}$, the CDI available at the transmitter is $\mathbf{c}_{\hat{\ell}}$. Define

$$\cos^2 \theta := \left|\mathbf{d}^H \mathbf{c}_{\hat{\ell}}\right|^2 \tag{5}$$

to reflect how well the obtained CDI aligns with the exact channel direction.

By (1) and (4), the signal at the desired receiver is

$$y_d = \|\mathbf{h}\|\mathbf{d}^H\mathbf{c}_{\hat{\ell}}u + \|\mathbf{h}\|\mathbf{d}^H\mathbf{W}\mathbf{v} + n_d$$

with the signal-to-interference-plus-noise ratio (SINR)

$$\begin{aligned}\mathrm{SINR}_d &= \frac{\|\mathbf{h}\|^2\left|\mathbf{d}^H\mathbf{c}_{\hat{\ell}}\right|^2\sigma_u^2}{\|\mathbf{h}\|^2\|\mathbf{d}^H\mathbf{W}\|^2\sigma_v^2 + \sigma_d^2}\\ &= \frac{\|\mathbf{h}\|^2\cos^2\theta\sigma_u^2}{\|\mathbf{h}\|^2\left(1-\cos^2\theta\right)\sigma_v^2 + \sigma_d^2} \qquad (6)\end{aligned}$$

which follows (5) and the fact that $|\mathbf{d}^H\mathbf{c}_{\hat{\ell}}|^2 + \|\mathbf{d}^H\mathbf{W}\|^2 = 1$. The first term in the denominator comes from the artificial noise that leaks into the desired communication channel due to limited feedback and inaccurate beamforming.

To the transmitter, the quantization error in the obtained CDI is unknown, and the instantaneous SINR (i.e., for a given $\mathbf{h}$) at the desired receiver is random. As such, the connection outage probability can be expressed as

$$p_{\mathrm{co}}(R_b, \phi, \mathbf{h}) := \Pr\left(\log_2(1+\mathrm{SINR}_d) \le R_b\right).$$

Since the optimal quantization codebook is generally unknown, in this paper, we consider the quantization cell approximation in (3). Based on this approximation, an approximated distribution for the "quantization error" $1-\cos^2\theta$, where $\cos^2\theta$ is defined in (5), was provided in Lemma 6 of [35]. Using this result, by (6), our connection outage probability p_{co} can be approximated by

$$\begin{aligned}&\tilde{p}_{\mathrm{co}}\left(R_b, \phi, \|\mathbf{h}\|\right)\\ &= \begin{cases} 0 & \text{for } R_b \le R_1\\ 1 - 2^{B_1}\left(\frac{\|\mathbf{h}\|^2P\phi - \sigma_d^2\left(2^{R_b}-1\right)}{\|\mathbf{h}\|^2\left(P\phi + \frac{P(1-\phi)}{N-1}\left(2^{R_b}-1\right)\right)}\right)^{N-1} & \text{for } R_1 < R_b \le R_2\\ 1 & \text{for } R_b > R_2\end{cases} \qquad (7)\end{aligned}$$

where

$$\begin{aligned}R_1 &= \log_2\left(1 + \frac{\|\mathbf{h}\|^2P\phi\left(1-2^{-\frac{B_1}{N-1}}\right)}{\|\mathbf{h}\|^2\frac{P(1-\phi)}{N-1}2^{-\frac{B_1}{N-1}} + \sigma_d^2}\right)\\ R_2 &= \log_2\left(1 + \frac{\|\mathbf{h}\|^2P\phi}{\sigma_d^2}\right).\end{aligned}$$

The first boundary value R_1 is the capacity of the desired communication channel with maximum quantization error in the CDI. Therefore, R_1 is also the maximum data rate achievable without causing connection outages. The second boundary value R_2 represents the capacity of the desired communication channel with perfect channel knowledge at the transmitter side. Note that $\tilde{p}_{\mathrm{co}}$ and R_1 are both functions of the number of feedback bits used for the CDI B_1. As $B_1 \to \infty$, $R_1 \to R_2$ and $\tilde{p}_{\mathrm{co}}$ approaches a step function at $R_b = R_2$. When the number of feedback bits used for the CDI is not too small (e.g., $B_1 \ge 3N$), (7) provides an accurate approximation for the actual connection outage probability.

B. Secrecy Outage Probability

The secrecy outage probability p_{so} is defined as the probability that the channel capacity to the eavesdropper exceeds a preselected rate redundancy R_e. By (2) and (4), the received signal at the eavesdropper admits

$$y_e = \mathbf{g}^H\mathbf{c}_{\hat{\ell}}u + \mathbf{g}^H\mathbf{W}\mathbf{v}$$

with corresponding signal-to-interference ratio (SIR)

$$\mathrm{SIR}_e = \frac{\left|\mathbf{g}^H\mathbf{c}_{\hat{\ell}}\right|^2\sigma_u^2}{\|\mathbf{g}^H\mathbf{W}\|^2\sigma_v^2}.$$

Though the eavesdropper's channel is unknown to the transmitter, by [17, eq. (5)], the secrecy outage probability can be computed as

$$\begin{aligned}p_{\mathrm{so}}(R_e, \phi) &:= \Pr\left(\log_2(1+\mathrm{SIR}_e) \ge R_e\right)\\ &= \left(1 + \left(2^{R_e}-1\right)\left(\frac{\phi^{-1}-1}{N-1}\right)\right)^{1-N} \qquad (8)\end{aligned}$$

which is independent of the informed channel direction $\mathbf{c}_{\hat{\ell}}$, and thus of the desired communication channel $\mathbf{h}$. Here, as a robust design, we ignored the thermal noise at the eavesdropper. Hence, the SIR at the eavesdropper becomes distance-independent, due to the fact that both the signal and the interference come from the same point of transmission. Therefore, the derived expression for the secrecy outage probability is valid for an eavesdropper located at an arbitrary distance. In the literature [43], [44], a zero-noise assumption is also used to represent the scenario where the eavesdropper is located arbitrarily close to the transmitter. If the analysis holds true for this case, as one may expect, it is also valid when the eavesdropper is located at a certain (but unknown) distance from the transmitter, due to distance attenuation. In general, our analysis allows the eavesdropper to be located at an arbitrary distance from the transmitter, with the only constraint that the Rayleigh fading assumption still holds.

IV. Secure Transmission Design

In the last section, we analyzed the connection and secrecy outage probabilities of artificial-noise-aided beamforming scheme with limited feedback. To guarantee the reliability performance of desired communication and the secrecy performance against eavesdropping, we specify a connection and a secrecy outage constraint, respectively. For a given channel realization, the design target is to maximize the confidential information rate under the dual connection and secrecy outage constraints. By averaging the maximum confidential information rate over all channel realizations, we can then investigate the average secrecy throughout performance.

In this section, considering that the CGI is just a positive scalar, which is relatively easy to quantize, we temporarily assume that the transmitter is well-informed about the CGI. In other words, the channel gain is assumed to be accurately known at the transmitter. We then focus on the secure transmission design with quantized CDI and will consider quantization for the CGI in the next section. The main problem we study can be summarized as follows.

Problem 1: What are the optimal transmission design parameters that maximize the confidential information rate, under dual connection and secrecy outage constraints?

For a given realization of the desired communication channel $\mathbf{h}$, recalling that the confidential information rate is given by the difference between the codeword rate and the rate redundancy $R_s = R_b - R_e$, Problem Problem 1 can be expressed as

$$R_s^*(\mathbf{h}) = \max_{R_b, R_e, \phi} [R_b - R_e]^+$$
$$\text{s.t.} \quad \tilde{p}_{\text{co}}(R_b, \phi, \|\mathbf{h}\|) \le \sigma, p_{\text{so}}(R_e, \phi) \le \epsilon \quad (9)$$

where $[x]^+ = \max\{0, x\}$ and $\sigma, \epsilon \in [0, 1]$ are the enforced connection and secrecy outage constraints. Since an exact expression for p_{co} seems unavailable, here we use its approximation $\tilde{p}_{\text{co}}$, provided in (7). Meanwhile, p_{so} was derived in (8) without any approximation. Here we point out that with our design strategy, the *outage probability of secrecy capacity* [4], i.e., $\Pr\{C_s < R_s^*\}$, where C_s is the unknown secrecy capacity given by the capacity difference between the desired receiver and the eavesdropper, is also guaranteed to be smaller than $\sigma + \epsilon$. This can be proved by invoking the union bound technique and here the proof is omitted for brevity. The solution to the optimization problem in (9) is also the answer to the question we asked in Problem 1. That is, solving the optimization problem in (9) will give us the maximum confidential information rate that can be delivered to the desired receiver while the risks of decoding errors and being eavesdropped are both under control.

A. Conditions for Secure Transmission

The optimization problem in (9) may not always have a positive solution. This occurs when, under dual connection and secrecy outage constraints, the maximum confidential information rate R_s^* is strictly zero. Here, we establish the necessary and sufficient conditions on the system parameters under which a positive R_s^* can be achieved.

Define $\lceil x \rceil$ as the smallest positive integer which is larger than x. We first present a condition on the number of feedback bits used for the CDI.

Proposition 1: Under the dual outage constraints in (9), for a positive confidential information rate to be achievable, the number of feedback bits used for the CDI must satisfy:

$$B_1 \ge B_1^{\min} := \left\lceil \log_2 \left(\frac{1-\sigma}{\epsilon} \right) \right\rceil. \quad (10)$$

Proof: See Appendix A. ■

Here $B_1^{\min}$ is the minimum number of feedback bits, above which a positive confidential information rate is achievable. This minimum requirement is established under the best possible situation where the desired receiver is free of thermal noise, i.e., $n_d = 0$. As can be seen from (6), assuming zero noise for the desired receiver is equivalent to assuming that the desired communication channel has an arbitrarily large strength $\|\mathbf{h}\|$.

From (10), we make the following observations:

- For a given connection outage constraint σ, an exponential reduction in the secrecy outage constraint ϵ necessitates a linear increase in $B_1^{\min}$. Moreover, as $\epsilon \to 0$, $B_1^{\min} \to \infty$, implying that as the secrecy outage constraint becomes more and more stringent, an arbitrarily large number of feedback bits is required to achieve any non-zero confidential information rate. This is a consequence of the fact that a more stringent outage constraint ϵ translates to a larger required rate redundancy R_e, and therefore a larger codeword rate R_b, for the confidential information rate $R_s = R_b - R_e$ to be positive. With all else fixed, this can obviously be obtained by improving the quality of the desired communication channel through additional feedback bits.
- Similarly, for a given secrecy outage constraint ϵ, an exponential reduction in the connection outage constraint σ towards zero (i.e., an exponential increase in $1 - \sigma$ towards one) necessitates a linear increase in $B_1^{\min}$. Moreover, as $\sigma \to 0$, $B_1^{\min} \to \lceil \log_2(1/\epsilon) \rceil$, implying that as the connection outage constraint is made more stringent, the required number of feedback bits grows, as above, but in this case it remains bounded. That is, unlike secrecy outages, connection outages can be avoided, provided that the number of feedback bits exceeds this limiting bound. This phenomena, while not immediately obvious, is due to the fact that with a well-designed quantization codebook, the CDI errors due to limited feedback are strictly upper bounded, and these can be made arbitrarily small as the number of feedback bits increases. Indeed, there comes a point in which the codeword rate R_b, when matched to the capacity of the desired communication channel under a worst-case quantization noise assumption (thus, avoiding connection outages), can still exceed the required rate redundancy R_e, thereby leading to a positive confidential information rate R_s.
- Interestingly, the condition in (10) shows no dependence at all on the number of transmit antennas N. This result is not immediately intuitive, due to the dependence of N on different aspects of the system. To examine this, first recall that this achievability condition is established under the assumption that the desired receiver is free of thermal noise. In this case, as can be seen from (6), the SINR at the desired receiver depends on the angular mismatch between the beamformer and the channel vector, but not the channel strength. (Thus, the additional array gain available to the beamformer by increasing the number of antennas is inconsequential.) Moreover, increasing N leads to a larger quantization error in the CDI, and this in turn leads to an increased connection outage probability. Consequently, to meet the specified connection outage constraint, the transmitter must employ a reduced codeword rate. In contrast to these negative effects, increasing N allows higher dimensionality for the generated artificial noise, which in turn provides additional protection against eavesdropping and thus a reduced secrecy outage probability. In terms of rate, this implies that the transmitter can use a smaller rate redundancy to satisfy the same secrecy outage constraint. What is most curious is that, as implied by (10), the reduction of both rates (i.e., R_b due to increased connection outages and R_e due to reduced secrecy outages) as N is increased is the same, such that the difference between them R_s is unaffected.

TABLE I
REQUIRED FEEDBACK BITS FOR CDI $B_1^{\min}$

$B_1^{\min}$		ϵ			
		1	0.1	0.01	0.001
σ	1	1	1	1	1
	0.1	1	4	7	10
	0.01	1	4	7	10

Table I gives some example values for $B_1^{\min}$ in (10) for different connection and secrecy outage constraints. Here, we see that the number of feedback bits required to get a non-zero confidential information rate is generally small.

Now we consider the case where the thermal noise at the desired receiver is non-negligible (i.e., $n_d \neq 0$). In this case, to achieve a positive confidential information rate, in addition to the number of feedback bits needed to satisfy (10), the strength of the desired communication channel must also be sufficiently large, as indicated in the following.

Proposition 2: Assuming the condition in (10) is satisfied, to achieve a positive confidential information rate, the strength of the desired communication channel must also satisfy:

$$\|\mathbf{h}\|^2 > \mu_{\min} := \frac{(N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}}-1\right)}{P\left(1-\sqrt[N-1]{\frac{1-\sigma}{2^{B_1}\epsilon}}\right)}\sigma_d^2. \qquad (11)$$

Proof: See Appendix B. ■

Here $\mu_{\min}$ is the minimum strength of the desired communication channel required for a positive confidential information rate to be achievable. From a design perspective, (11) implies that one should adopt an "on-off" transmission scheme [41], with a transmit threshold $\mu_{\min}$.

Actually, the condition in (11) is closely related to that in (10). Since (10) was derived assuming zero thermal noise, it is independent of the strength of the desired communication channel. Now, this fact can also be observed from (11). That is, when $n_d = 0$ (thus $\sigma_d^2 = 0$), the requirement on the channel strength disappears (it simply needs to be greater than zero). When the thermal noise at the desired receiver becomes non-negligible (i.e., $\sigma_d^2 \neq 0$), to compensate for this effect, while the lower bound on the required number of feedback bits does not change, a requirement on the channel strength comes up, as given in (11).

One may interpret the interplay between the conditions in (10) and (11) from a stochastic point of view. To this end, first note that the CGI $\|\mathbf{h}\|$ is randomly distributed on $[0, \infty)$. As B_1 approaches the theoretical lower limit $\log_2[(1-\sigma)/\epsilon]$, the denominator in (11) approaches zero and the transmit threshold $\mu_{\min}$ becomes arbitrarily large. Thus, the probability of the event $\{\|\mathbf{h}\|^2 > \mu_{\min}\}$, and consequently the probability of achieving a positive confidential information rate, tends to zero. Clearly, the larger the number of feedback bits B_1 (i.e., as it grows beyond its lower limit $\log_2[(1-\sigma)/\epsilon]$), the smaller the threshold $\mu_{\min}$, and thus the greater the probability of achieving a positive confidential information rate.

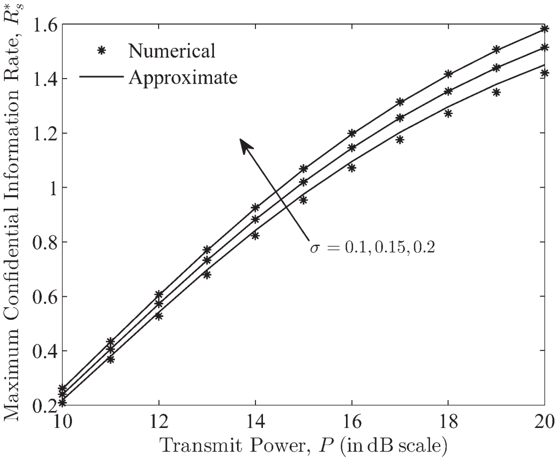


Fig. 1. Maximum confidential information rate R_s^* versus the transmit power P for different connection outage constraints σ. Results are shown for the case where $\sigma_d^2 = 1$, $N = 2$, $B_1 = 6$, $\epsilon = 0.05$ and $\|\mathbf{h}\| = 2$.

B. Optimized Transmission Design

Having discussed the conditions under which a positive confidential information rate is achievable, we now provide a closed-form solution to the optimization problem in (9).

Theorem 1: Assume that the conditions in (10) and (11) are satisfied. The optimal choices of the transmission rates (R_b and R_e) and the power allocation ratio ϕ in (9) are given by

$$\phi^* = \frac{\left(\beta+\sigma_d^2\right)(\alpha-\beta\gamma) - \sqrt{\alpha-\beta\gamma+\sigma_d^2(1-\gamma)}\sqrt{\alpha\gamma\sigma_d^2(\beta+\sigma_d^2)}}{\beta(\alpha-\beta\gamma)+\alpha\sigma_d^2(1-\gamma)}$$

$$R_b^* = \log_2\left(1+\frac{\alpha\phi^*}{\beta(1-\phi^*)+\sigma_d^2}\right)$$

$$R_e^* = \log_2\left(1+\gamma\frac{\phi^*}{1-\phi^*}\right) \qquad (12)$$

where

$$\alpha = \|\mathbf{h}\|^2 P\left(1-\sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}}\right)$$

$$\beta = \frac{\|\mathbf{h}\|^2 P}{N-1}\sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}}$$

$$\gamma = (N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}}-1\right). \qquad (13)$$

The corresponding (strictly positive) maximum confidential information rate is therefore

$$R_s^*\left(\|\mathbf{h}\|^2\right) = R_b^* - R_e^*. \qquad (14)$$

Proof: See Appendix C. ■

It turns out that for the maximum confidential information rate R_s^* in (14), the desired communication channel $\mathbf{h}$ appears only in the form of $\|\mathbf{h}\|^2$. Thus, to facilitate our later analysis, here we have slightly abused notation and written it as $R_s^*(\|\mathbf{h}\|^2)$, rather than $R_s^*(\mathbf{h})$ as in (9).

Note that for the optimization problem in (9), the approximated connection outage probability in (7) was used. Hence,

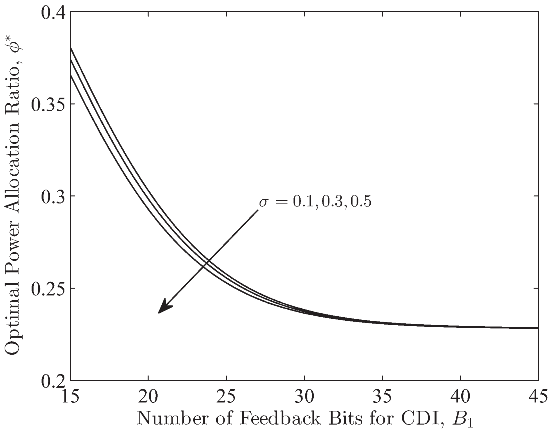


Fig. 2. Optimal power allocation ratio ϕ^* versus the number of feedback bits used for the CDI B_1 for different connection outage constraints σ. Results are shown for the case where $\sigma_d^2 = 1$, $N = 4$, $P = 100$, $\epsilon = 0.01$ and $\|\mathbf{h}\| = 2$.

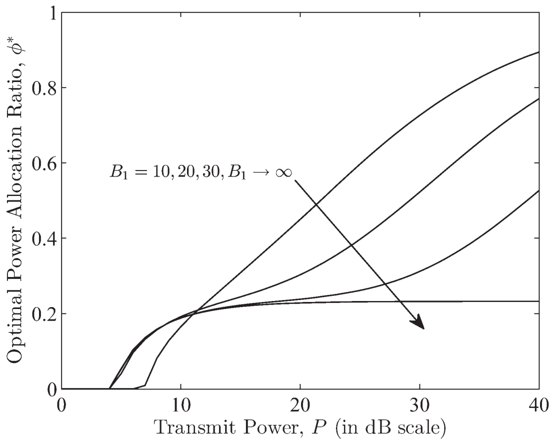


Fig. 3. Optimal power allocation ratio ϕ^* versus the transmit power P, compared with the case of accurate CDI. Results are shown for the case where $\sigma_d^2 = 1$, $N = 4$, $\sigma = 0.1$, $\epsilon = 0.01$ and $\|\mathbf{h}\| = 2$.

the maximum confidential information rate in (14) is also an approximation. In Fig. 1, we compare (14) with the exact maximum confidential information rate, found by inverting the simulated connection outage probability and optimizing the transmit power allocation numerically. The quantization codebooks are generated based on the design criterion in [32], [33]. As can be seen, the difference between the exact result and our analytical approximation is almost negligible. That is to say, the considered quantization cell approximation has only a negligible effect on the optimality of the proposed transmission design and the solution derived based on the quantization cell approximation accurately predicts the maximum achievable confidential information rate.

Based on (12), we find the following:

- As demonstrated in Fig. 2, for a given transmit power P, the optimal power allocation ratio ϕ^* decreases with increasing number of feedback bits used for the CDI B_1. This implies that, if more feedback bits are available, then one should allocate more transmit power to the artificial noise, and less power to the information signal. This may be counter-intuitive, as one could expect the transmitter to give a larger fraction of power to the information signal when it gets more confident about the desired communication channel (the idea of allocating more power to higher quality channels is the basis of conventional waterfilling algorithms, for example). However, with the secrecy constraint, it is the achievable rate *difference* that matters, not only the capacity of the desired communication channel, and the bottleneck affecting the achievable rate difference is the unknown channel of the eavesdropper. With more feedback bits, generating extra artificial noise would have reducing effect on the desired communication channel (approaching asymptotic orthogonality), but could effectively degrade the eavesdropper's signal reception, giving an improved confidential information rate. We also have $\lim_{B_1\to\infty} \phi^* = \phi^*_{\text{perfect}}$, where ϕ^*_{perfect} is the optimal power allocation ratio with perfect knowledge of the desired communication channel, derived previously in [17, eq. (29)].
- As demonstrated in Fig. 3, for a given number of feedback bits used for the CDI B_1, the optimal power allocation ratio ϕ^* increases with the transmit power P. This implies that, if extra transmit power is available, then one should allocate more transmit power to the information signal, and less power to the artificial noise. An intuitive explanation can be given as follows. With a fixed number of feedback bits, the desired communication channel has certain advantage over the eavesdropper's channel. By giving a larger fraction of the transmit power to the information signal, this advantage can be further expanded. That is, the increase in the supported codeword rate is larger than that in the required rate redundancy, leading to an improved confidential information rate. Given a finite B_1, we also have $\lim_{P\to\infty} \phi^* = 1$, implying that with limited feedback and an arbitrarily large transmit power, the confidential information rate is maximized when the transmitter gives all of its power to the information signal. This observation is quite different from the case with perfect knowledge of the desired communication channel, where $\lim_{P\to\infty} \phi^*_{\text{perfect}} < 1$ [17, eq. (31)]. With limited feedback, as $P \to \infty$, by using a larger power allocation ratio, both the supported codeword rate and the required rate redundancy increase unbounded. However, the difference between them, i.e., the confidential information rate, increases to a finite asymptote. With perfect knowledge of the desired communication channel, as $P \to \infty$, if a certain fraction of the transmit power is reserved for generating artificial noise to limit the eavesdropper's signal reception and thereby the required rate redundancy, the confidential information rate can be made arbitrarily large. This is why different power allocation strategies are observed in the asymptotic region where $P \to \infty$.

C. Secrecy Throughput Performance

In the last subsection, for a given realization of the desired communication channel, we maximized the data rate which is delivered to the desired receiver while the risks of decoding error and being eavesdropped are under control. In this subsection, we investigate the secrecy throughput performance. To be specific, the secrecy throughput is defined as the confidential information rate averaged over all channel realizations, taking into account the probability of connection outage σ, given by

$$\eta = (1-\sigma)\mathbb{E}_{\mathbf{h}}\left[R_s^*\left(\|\mathbf{h}\|^2\right)\right] \quad \text{(bits/channel use)}.$$

Assuming that the number of feedback bits used for the CDI B_1 is chosen to satisfy (10), and with the optimized transmission design provided in Theorem 1, the corresponding secrecy throughput is

$$\eta = (1-\sigma)\int_{\mu_{\min}}^{\infty} R_s^*(z) f_{\|\mathbf{h}\|^2}(z)\mathrm{d}z \tag{15}$$

where the transmit threshold $\mu_{\min}$ is defined in (11) and for $z > 0$, $f_{\|\mathbf{h}\|^2}(z) = z^{N-1}\mathrm{e}^{-z}/(N-1)!$.

In [17, eq. (35)], we showed that with perfect knowledge of the desired communication channel, the secrecy throughput grows unbounded (logarithmically) with increasing transmit power. With limited feedback, we present the following remark.

Remark 1: From (12)–(15), as the transmit power grows large, the secrecy throughput converges to a finite asymptote:

$$\lim_{P\to\infty}\eta = (1-\sigma)\log_2\left(\frac{\sqrt[N-1]{\frac{2^{B_1}}{1-\sigma}}-1}{\sqrt[N-1]{\frac{1}{\epsilon}}-1}\right). \tag{16}$$

By adding extra feedback bits (i.e., increasing B_1), the throughput limit in (16) will be increased, as one may expect. An explanation for the observed convergence is given as follows:

- With perfect knowledge of the desired communication channel, by increasing the transmit power P, the optimal power allocation ratio ϕ^*_{perfect} in [17, eq. (29)] increases to an asymptote which is strictly less than one. Therefore, the rate redundancy required to satisfy the secrecy outage constraint is limited to a constant value. Meanwhile, the supported codeword rate grows unbounded with increasing P, and this is why the secrecy throughput with perfect knowledge of the desired communication channel increases to infinity, as can be seen from [17, eq. (35)].
- With quantized CDI feedback from the desired receiver, by increasing the transmit power P, the optimal power allocation ratio ϕ^* in (12) increases towards one. Consequently, the rate redundancy required to satisfy the secrecy outage constraint increases towards infinity (which is not the case with perfect knowledge of the desired communication channel). Though the supported codeword rate also increases with increasing P, the difference between the supported codeword rate and the required rate redundancy converges to a certain value. This is why the secrecy throughput with quantized CDI feedback converges to (16) instead of growing unbounded with increasing P.

Thus far, we have considered the outage constraints, ϵ and σ, as fixed. One may also ask how the specific choice of ϵ and σ influence the throughput performance of our optimized transmission scheme in Theorem 1. This is investigated in Fig. 4, which plots the secrecy throughput versus the connection and secrecy outage constraints. As can be seen, for any given connection outage constraint, strengthening the secrecy outage constraint would reduce the achievable throughput, as one may expect. On the other hand, if the secrecy outage constraint is fixed while the connection outage constraint is varied, different behavior is observed depending on the specific value of the secrecy constraint. In particular, if the secrecy constraint is not too strong (e.g., the curve highlighted for $\epsilon = 0.033$), then the secrecy throughput is maximized with as few connection outages as possible; while if the secrecy constraint is sufficiently strong (e.g., the curve highlighted for $\epsilon = 0.009$), then allowing for connection outages (and for this example, quite a lot of outages) can indeed lead to an increased throughput. This observation suggests that a worst-case assumption (i.e., no connection outages allowed, thereby assuming maximum quantization error) does not necessarily yield the maximum secrecy throughput. That is to say, instead of simply assuming maximum quantization error, exploiting the statistical knowledge of the quantization error due to limited feedback can indeed provide a better secrecy throughput.

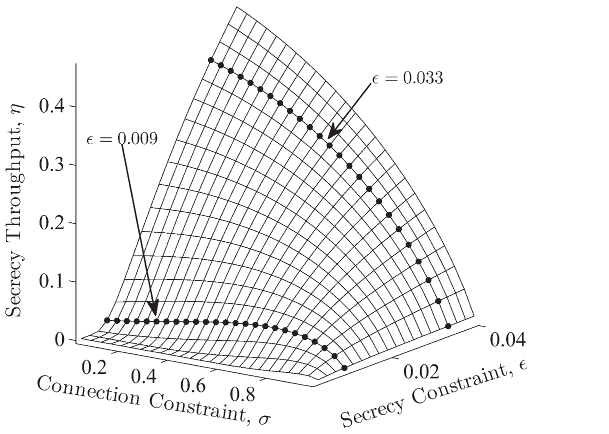


Fig. 4. Secrecy throughput η versus the connection and secrecy outage constraints σ and ϵ. Results are shown for the case where $\sigma_d^2 = 1$, $N = 4$, $P = 10$ and $B_1 = 8$.

V. Quantization of Channel Gain Information

Up to this point, as in [35], [37], we have assumed that the CGI is accurately known at the transmitter. In practice, however, this will need to be quantized, along with the CDI. Here we explicitly account for this issue. Specifically, we address the following problem.

Problem 2: How to quantize the CGI and what is the corresponding secrecy throughput, under dual connection and secrecy outage constraints?

With different numbers of feedback bits allocated to quantize the CGI, we consider different transmission/quantization schemes. Recall that we use B_2 feedback bits to quantize the CGI. When $B_2 = 1$, an on-off transmission scheme is adopted, where the rate parameters and power allocation ratio are chosen to take fixed values, and the feedback bit indicates whether to transmit or not. When $B_2 \geq 2$, we use a multi-stage quantization scheme to enable adaptive transmission, where the rate parameters and power allocation ratio are chosen based on the feedback about the strength of the desired channel. Each scheme is now discussed in turn.

A. One-Bit CGI Feedback

When $B_2 = 1$, this single bit can be used to indicate if the channel strength is above a certain threshold, and thus the transceiver can perform a fixed-rate on-off transmission. More specifically, define $m = \mathbb{1}_{\{\|\mathbf{h}\|^2 \geq \mu_T\}}$, where $\mathbb{1}_{\{\cdot\}}$ is the indicator function and μ_T is a preselected threshold. The case $m = 0$ implies that the transmission should be suspended. Alternatively, if $m = 1$, the transmitter conducts transmission using the optimized design provided in Theorem 1, and assuming that the squared amplitude of the desired communication channel is taking its smallest possible value: $\|\mathbf{h}\|^2 = \mu_T$. In this way, the connection and secrecy outage constraints in (9) are both satisfied.

From (15), the secrecy throughput with one-bit CGI feedback is given by

$$\eta = (1 - \sigma) R_s^*(\mu_T) \tilde{\Gamma}(N, \mu_T) \tag{17}$$

where $R_s^*(\cdot)$ was derived previously in (14) and $\tilde{\Gamma}(\cdot, \cdot)$ is the regularized upper incomplete gamma function, defined as $\tilde{\Gamma}(N, x) = \mathrm{e}^{-x} \sum_{k=0}^{N-1} x^k/k!$.

As mentioned previously, if $\|\mathbf{h}\|^2 \leq \mu_{\min}$, defined in (11), then $R_s^*(\|\mathbf{h}\|^2) = 0$. Hence, the transmit threshold should be chosen as $\mu_T > \mu_{\min}$. Note in addition that as $\mu_T \to \infty$, $R_s^*(\mu_T)$ increases to a finite asymptote, while $\tilde{\Gamma}(N, \mu_T)$ tends to zero; thus, the throughput in (17) also approaches zero. Based on these two observations, we numerically optimize μ_T in the range $(\mu_{\min}, \infty)$ to maximize the secrecy throughput.

B. Multiple-Bit CGI Feedback

When $B_2 \geq 2$, the transceiver can perform rate-adaptive transmission, where the rate choice belongs to a finite set, bounded by the number of quantization steps. In this case, the throughput-optimal CGI quantization scheme is difficult to characterize. Here, we consider a quantization scheme which is reasonably easy to implement and also provides a good throughput performance with a relatively small number of quantization bits.

We first define the inverse function for the regularized upper incomplete gamma function $x = \tilde{\Gamma}_{-1}(N, y)$ such that $y = \tilde{\Gamma}(N, x)$. Though there is no closed-form expression for this function, standard software packages such as Matlab provide well-developed routines for numerical evaluation.

From the conditions in (10) and (11), we know that it is unnecessary to quantize the range $\|\mathbf{h}\|^2 < \mu_{\min}$. Meanwhile, though the CGI $\|\mathbf{h}\|$ may take large values, the corresponding probabilities are typically small. Hence, we consider quantization for the CGI in a bounded interval $\mu_1 < \|\mathbf{h}\|^2 \leq \mu_2$, where $\mu_1 = \tilde{\Gamma}_{-1}(N, \tilde{\Gamma}(N, \mu_{\min}) - \delta)$, $\mu_2 = \tilde{\Gamma}_{-1}(N, \delta)$, with δ as a small positive constant. The upper limit μ_2 is introduced to truncate large CGI values appearing with only small probability, while the lower limit $\mu_1 > \mu_{\min}$ is invoked to improve the quantization efficiency. (A more detailed explanation of this second condition will be given subsequently.) The value of δ will be chosen to make sure that $\mu_1 < \mu_2$ and to cover an appropriate subset $[\mu_1, \mu_2]$ of $[\mu_{\min}, \infty)$.

The key idea of the considered quantization scheme is to divide the range between μ_1 and μ_2 into $2^{B_2} - 2$ quantization intervals, such that $\|\mathbf{h}\|^2$ has the same probability of falling into each interval. This is a quite simple scheme, analogous to the "histogram equalization" approach used in image processing [45], which we will refer to as "equalized quantization". To be precise, for any given CGI $\|\mathbf{h}\| \in (0, \infty)$, the receiver generates an index m through (18), shown on the bottom of the page, where $k \in \{1, \ldots, 2^{B_2} - 2\}$. The value of m is then fed back to the transmitter.

At the transmitter side, when $m = 0$ is received, transmission is suspended. When $m \in \{1, \ldots, 2^{B_2} - 1\}$ is received, it applies the optimized design provided in Theorem 1, by assuming that the squared amplitude of the desired communication channel is at its smallest value possible, given the quantization value m:

$$\|\mathbf{h}\|^2 = \tilde{\Gamma}_{-1}\left(N, \tilde{\Gamma}(N, \mu_1) - (m-1)\frac{\tilde{\Gamma}(N, \mu_1) - \tilde{\Gamma}(N, \mu_2)}{2^{B_2} - 2}\right). \tag{19}$$

In this way, the connection and secrecy outage constraints in (9) are both satisfied. This worst-case assumption is also the reason why we choose $\mu_1 > \mu_{\min}$: From (14), we know that $R_s^*(\mu_{\min}) = 0$. Then, if we were to set $\mu_1 = \mu_{\min}$, with the worst-case assumption above, the first quantization interval after μ_1 is wasted. Moreover, choosing μ_1 in excess of $\mu_{\min}$ allows one to impose a lower bound on the achievable confidential information rate $R_s^*(\mu_1)$ that must be satisfied, before transmission is conducted. This, in turn, results in more efficient use of the available quantization bits.

With the proposed equalized quantization scheme for the CGI, from (15), the secrecy throughput becomes

$$\begin{aligned}\eta =& (1 - \sigma)\frac{\tilde{\Gamma}(N, \mu_1) - \tilde{\Gamma}(N, \mu_2)}{2^{B_2} - 2} \\ & \times \sum_{m=1}^{2^{B_2}-2} R_s^*\left(\tilde{\Gamma}_{-1}\left(N, \tilde{\Gamma}(N, \mu_1) - (m-1)\frac{\tilde{\Gamma}(N, \mu_1) - \tilde{\Gamma}(N, \mu_2)}{2^{B_2} - 2}\right)\right) \\ & + (1 - \sigma) R_s^*(\mu_2) \tilde{\Gamma}(N, \mu_2)\end{aligned}$$

where $R_s^*(\cdot)$ is given in (14).

Fig. 5 plots the secrecy throughput achieved with the CGI quantization scheme introduced above. Here, the number of bits used for quantizing the CDI B_1 is kept fixed, while the number of bits used for quantizing the CGI B_2 is varied. We see that with only four or five bits, the equalized quantization

$$m = \begin{cases} 0 & \text{for } \|\mathbf{h}\|^2 < \mu_1 \\ k & \text{for } \tilde{\Gamma}_{-1}\left(N, \tilde{\Gamma}(N, \mu_1) - (k-1)\frac{\tilde{\Gamma}(N, \mu_1) - \tilde{\Gamma}(N, \mu_2)}{2^{B_2} - 2}\right) \leq \|\mathbf{h}\|^2 < \tilde{\Gamma}_{-1}\left(N, \tilde{\Gamma}(N, \mu_1) - k\frac{\tilde{\Gamma}(N, \mu_1) - \tilde{\Gamma}(N, \mu_2)}{2^{B_2} - 2}\right) \\ 2^{B_2} - 1 & \text{for } \|\mathbf{h}\|^2 \geq \mu_2 \end{cases} \tag{18}$$

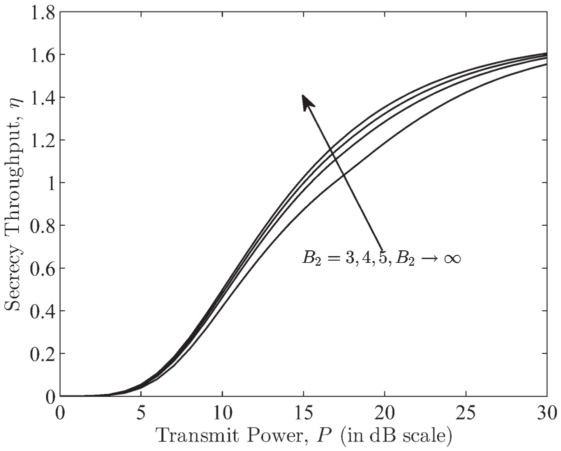


Fig. 5. Secrecy throughput η versus the transmit power P, with quantized CGI, compared with the case of accurate CGI. Results are shown for the case where $\sigma_d^2 = 1$, $N = 4$, $B_1 = 10$, $\sigma = 0.05$, $\epsilon = 0.02$ and $\delta = 0.0001$.

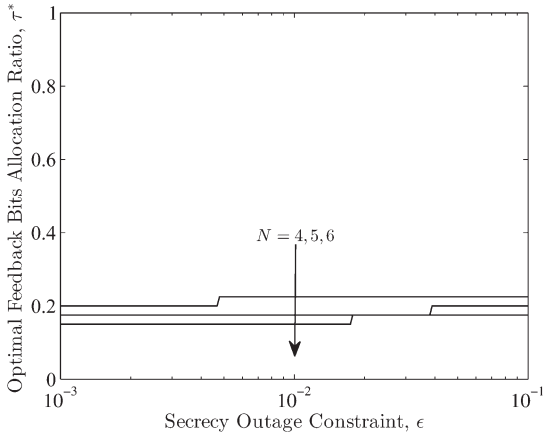


Fig. 6. Optimal feedback bits allocation ratio τ^* versus the secrecy outage constraint ϵ, for different number of transmit antennas N. Results are shown for the case where $\sigma_d^2 = 1$, $P = 10$, $B = 40$, $\sigma = 0.05$ and $\delta = 0.0001$.

scheme provides a throughput performance which is close to that achieved with perfect CGI knowledge (i.e., $B_2 \to \infty$).

C. Allocation of Feedback Bits Between CDI and CGI

In practice, a single feedback channel is used for conveying both quantized CDI and CGI. Thus, an interesting problem emerges.

Problem 3: For a given number of feedback bits, what is the most efficient allocation between the CDI and CGI to maximize the secrecy throughput?

To study this problem, we first define $\tau = B_2/B$, which we term the "feedback bits allocation ratio". Clearly, τ represents the fraction of bits allocated to the CGI, while $1 - \tau$ represents the fraction of bits allocated to the CDI. While difficult to characterize Problem 3 analytically, we will study this problem through simulations.

Intuitively, giving too few feedback bits to either the CGI or the CDI (i.e., with τ sufficiently close to zero or one respectively) will lead to a degraded secrecy throughput. Fig. 6 shows the optimal τ that maximizes the secrecy throughput, i.e., τ^*, against the secrecy outage constraint ϵ for different numbers of antennas N. We see that for the scenario considered, $\tau^* \approx 0.2$. This number is rather small, but nonetheless intuitive. The CGI is just a positive scalar, which does not require many bits to quantize; while the CDI requires quantization of a N-dimensional complex vector (under norm constraints), to accurately specify the beamforming direction. Moreover, this optimal allocation ratio is insensitive to changes in the secrecy outage constraint.

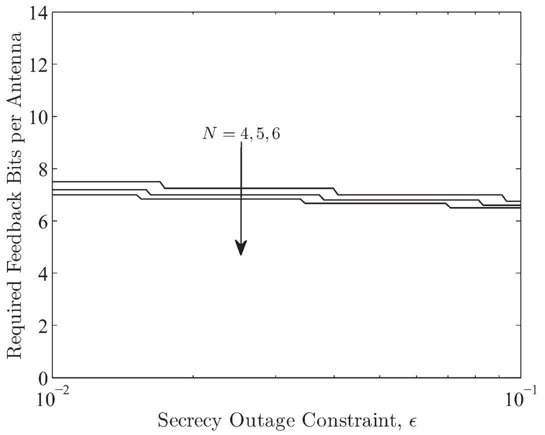


Fig. 7. Required number of feedback bits per antenna for achieving 90% of the secrecy throughput with perfect knowledge of the desired communication channel versus the secrecy outage constraint ϵ, for different number of transmit antennas N. Results are shown for the case where $\sigma_d^2 = 1$, $P = 20$, $\sigma = 0.03$ and $\delta = 0.0001$.

Based on the observations above, we claim the following: With limited feedback, to maximize the secrecy throughput, a good "rule of thumb" is to allocate roughly 20% of the feedback bits for quantizing the CGI, and the remainder for quantizing the CDI.

In addition to the specific parameterizations considered in Fig. 6, this claim was also found to be valid over a wider selection of parameters (e.g., P, B, and σ). We do not report these additional simulation results here, for conciseness.

D. Quantization Efficiency

With optimized feedback allocation between the CDI and CGI, we now analyze the quantization efficiency in terms of the number of feedback bits required for achieving a good performance. This issue is studied in Fig. 7, which plots the required number of feedback bits to achieve a high fraction (in this example, 90%) of the throughput achievable with unlimited feedback. Again, we plot the results as a function of the secrecy outage constraint ϵ, for different antenna numbers N. Based on these results, we make the following interesting observation.

For a reasonable secrecy outage constraint (e.g., $\epsilon \in [0.001, 0.1]$), roughly 8 feedback bits per antenna is sufficient for achieving 90% of the secrecy throughput that would be attainable with perfect knowledge of the desired communication channel.

Once again, although not shown, in addition to the particular parameterizations considered in Fig. 7, we also found this claim to be valid for a wider range of parameters (e.g., P and N). While Fig. 7 indicates that 8 bits of feedback per antenna is sufficient for even reasonably strong outage constraints, as the secrecy outage constraint becomes very relaxed or even removed (e.g., $\epsilon \in [0.5, 1]$), our additional numerical studies have revealed that the required number of feedback bits may indeed be reduced further to around 4 feedback bits per antenna.

VI. Conclusion and Future Work

Assuming limited feedback from the desired receiver and no feedback from the eavesdropper, we designed an artificial-noise-aided beamforming technique that enhances secrecy in slow fading channels. Our proposed method was designed to maximize the throughput by adaptively adjusting the wiretap coding rates and the power allocation between the information signal and artificial noise in response to the feedback information, such that dual connection and secrecy outage constraints were met. Our analysis provided key insights into the associated system parameters, such as the optimal power allocation, the number of feedback bits, the number of antennas, the imposed outage constraints, and so on. The proposed method also demonstrated significant differences with respect to previous designs based on perfect feedback.

In this paper, we assumed that the channel estimation at the receiver side is perfect, and focused on the design with a rate-limited feedback link. Possible future extensions include consideration of practical channel estimation schemes with optimized pilot design. In addition, scenarios where the desired receiver and the eavesdropper have multiple antennas are also of interest and will be important topics for future study.

Appendix

A. Proof of Proposition 1

First note that the connection outage probability $\tilde{p}_{\mathrm{co}}$ in (7) depends on the codeword rate R_b, the secrecy outage probability p_{so} in (8) depends on the rate redundancy R_e, while both $\tilde{p}_{\mathrm{co}}$ and p_{so} depend on the power allocation ratio ϕ. For a given ϕ, the connection outage constraint $\tilde{p}_{\mathrm{co}}(R_b, \phi, \|\mathbf{h}\|) \leq \sigma$ implies that the maximum allowable codeword rate is

$$R_b^{\max} = \log_2\left(1 + \frac{\|\mathbf{h}\|^2 P\phi\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}}\right)}{\|\mathbf{h}\|^2 \frac{P(1-\phi)}{N-1} \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}} + \sigma_d^2}\right). \tag{20}$$

Similarly, under the secrecy outage constraint $p_{\mathrm{so}}(R_e, \phi) \leq \epsilon$, the minimum required rate redundancy is given by

$$R_e^{\min} = \log_2\left(1 + \frac{\phi}{1-\phi}(N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right)\right). \tag{21}$$

The confidential information rate $R_s = R_b - R_e$ is therefore maximized when $R_b = R_b^{\max}$ and $R_e = R_e^{\min}$. Clearly, to achieve a positive R_s, we require $R_b^{\max} > R_e^{\min}$.

Under the ideal scenario where the desired receiver has zero thermal noise, i.e., $n_d = 0$ (thus $\sigma_d^2 = 0$), $R_b^{\max}$ in (20) admits

$$R_b^{\max}|_{n_d=0} = \log_2\left(1 + \frac{\phi}{1-\phi}(N-1)\left(\sqrt[N-1]{\frac{2^{B_1}}{1-\sigma}} - 1\right)\right) \tag{22}$$

which is independent of the channel strength $\|\mathbf{h}\|$ and the transmit power P. Now, from (21) and (22), for $R_b^{\max}|_{n_d=0} > R_e^{\min}$ to hold requires $2^{B_1}/(1-\sigma) > 1/\epsilon$, which is independent of ϕ and the number of transmit antennas N. Reformulating this condition in terms of the number of feedback bits B_1 and rounding it up to the nearest integer, we establish Proposition 1.

B. Proof of Proposition 2

As discussed in Appendix A, the confidential information rate $R_s = R_b - R_e$ is maximized when $R_b = R_b^{\max}$ and $R_e = R_e^{\min}$, with $R_b^{\max}$ and $R_e^{\min}$ defined in (20) and (21) respectively. These quantities depend on the power allocation ratio ϕ, which is still to be optimized. In particular, we require

$$R_s^*(\mathbf{h}) = \max_{0<\phi<1} \left[R_b^{\max} - R_e^{\min}\right]^+. \tag{23}$$

Here, in contrast to Appendix A, we consider the case where the thermal noise at the desired receiver is non-negligible, i.e., $n_d \sim \mathcal{CN}(0, \sigma_d^2)$ with $\sigma_d^2 > 0$. For R_s^* to be positive entails $R_b^{\max} > R_e^{\min}$ for some ϕ. From (20) and (21), an equivalent condition is

$$\frac{\|\mathbf{h}\|^2 P\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}}\right)}{\|\mathbf{h}\|^2 \frac{P(1-\phi)}{N-1} \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}} + \sigma_d^2} > \frac{N-1}{1-\phi}\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right)$$

for some ϕ, which can be rewritten as

$$\|\mathbf{h}\|^2 > \frac{(N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right)}{(1-\phi)P\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1\epsilon}}}\right)}\sigma_d^2 \tag{24}$$

for some ϕ. By letting $\phi = 0$ to minimize the right-hand-side, we get the minimum channel strength required for achieving a positive R_s^*, reported in Proposition 2.

C. Proof of Theorem 1

With the conditions in (10) and (11) satisfied, by (24), the range of the power allocation ratio ϕ that gives a positive confidential information rate is

$$0 < \phi < \phi_{\max} := 1 - \frac{\sigma_d^2(N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right)}{\|\mathbf{h}\|^2 P\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1\epsilon}}}\right)}.$$

Then, the optimization problem in (23) reduces to

$$\begin{aligned} R_s^*(\mathbf{h}) &= \max_{0<\phi<\phi_{\max}} R_b^{\max} - R_e^{\min} \\ &= \max_{0<\phi<\phi_{\max}} \log_2\left(\frac{1 + \frac{\|\mathbf{h}\|^2 P\phi\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}}\right)}{\|\mathbf{h}\|^2 \frac{P(1-\phi)}{N-1} \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}} + \sigma_d^2}}{1 + \frac{\phi}{1-\phi}(N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right)}\right) \end{aligned}$$

where $R_b^{\max}$ and $R_e^{\min}$ are defined in (20) and (21) respectively. Exploiting the monotonicity of the logarithm function, we solve this by setting the derivative of the quantity inside the brackets to zero, and keeping the only solution which satisfies the constraint. The results obtained are then summarized in Theorem 1.

Acknowledgment

We sincerely thank the anonymous reviewers for their valuable comments which have greatly improved the quality of this paper.

References

[1] X. Zhang, X. Zhou, M. R. McKay, and R. W. Heath, Jr., "Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Florence, Italy, May 2014, pp. 3968–3972.

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

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[5] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 524–528.

[7] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[8] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[9] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[10] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[11] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multiantenna transmission in wireless*ad hoc* networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

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

[13] S. Gerbracht, A. Wolf, and E. A. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *Proc. Int. ITG Workshop Smart Antennas*, Bremen, Germany, Feb. 2010, pp. 394–401.

[14] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers," in *Proc. IEEE Int. Conf. Commun.*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[15] Q. Li, W. K. Ma, and A. M. C. So, "Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial noise," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2011, pp. 207–211.

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

[17] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificialnoise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[18] Q. Li and W. K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[20] T. Y. Liu, S. C. Lin, T. H. Chang, and Y. W. P. Hong, "How much training is enough for secrecy beamforming with artificial noise," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, ON, Canada, Jun. 2012, pp. 4782–4787.

[21] D. W. K. Ng and R. Schober, "Resource allocation for secure OFDMA communication systems," in *Proc. Aust. Commun. Theory Workshop*, Melbourne, Australia, Feb. 2011, pp. 13–18.

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

[23] M. Pei, J. Wei, K. K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[24] Y. Yang, W. Wang, H. Zhao, and L. Zhao, "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation," *J. Commun. Networks*, vol. 14, no. 4, pp. 374–384, Aug. 2012.

[25] Z. Rezki, A. Khisti, and M. S. Alouini, "On the ergodic secret message capacity of the wiretap channel with finite-rate feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, USA, Jul. 2012, pp. 239–243.

[26] S. Bashar, Z. Ding, and 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.

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

[28] 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 Mobile Radio Commun.*, Toronto, ON, Canada, Sep. 2011, pp. 1264–1268.

[29] W. Santipach and M. L. Honig, "Signature optimization for DS-CDMA with limited feedback," in *Proc. IEEE Int. Symp. Spread-Spectrum Tech. Appl.*, Prague, Czech Republic, Sep. 2002, pp. 180–184.

[30] D. J. Love, R. W. Heath, Jr., W. Santipach, and M. L. Honig, "What is the value of limited feedback for MIMO channels?" *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 54–59, Oct. 2004.

[31] W. Santipach and M. L. Honig, "Asymptotic capacity of beamforming with limited feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, IL, USA, Jun. 2004, p. 290.

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

[33] K. 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.

[34] S. Zhou, Z. Wang, and G. B. Giannakis, "Quantifying the power loss when transmit beamforming relies on finite-rate feedback," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1948–1957, Jul. 2005.

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

[36] B. Mondal and R. W. Heath, Jr., "Performance analysis of quantized beamforming MIMO systems," *IEEE Trans. Signal Process.*, vol. 54, no. 12, pp. 4753–4766, Dec. 2006.

[37] 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, Sep. 2007.

[38] C. K. Au-Yeung and D. J. Love, "On the performance of random vector quantization limited feedback beamforming in a MISO system," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 458–462, Feb. 2007.

[39] Y. Wu, R. H. Y. Louie, M. R. McKay, and I. B. Collings, "MIMO beamforming with quantized feedback in ad hoc networks: Transmission capacity analysis," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Nov. 2010, pp. 1582–1587.

[40] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

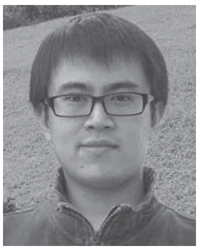
[41] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[42] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

[43] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Commun.*, vol. 8, no. 8, pp. 1248–1257, May 2014.

[44] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1617–1628, Oct. 2014.

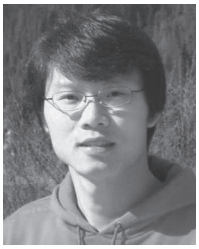
[45] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.



Xi Zhang (S'11–M'14) received the B.E. degree in communication engineering from the University of Electronic Science and Technology of China in 2010, and the Ph.D. degree in electronic and computer engineering from the Hong Kong University of Science and Technology in 2014. He is now working in the Communication Technology Laboratory, Huawei Technologies Co., Ltd. His current research interests are in the fields of wireless communication with millimeter wave and massive MIMO techniques.

Matthew R. McKay (S'03–M'07–SM'13) received the Ph.D. degree from the University of Sydney, Australia, prior to joining the Hong Kong University of Science and Technology (HKUST), where he is currently the Hari Harilela Associate Professor of Electronic and Computer Engineering. His research interests include communications, signal processing, random matrix theory, and associated applications. Most recently, he has developed a keen interest in the interdisciplinary areas of computational immunology and financial engineering.

He and his coauthors have received best paper awards at IEEE ICASSP 2006, IEEE VTC 2006, ACM IWCMC 2010, IEEE Globecom 2010, and IEEE ICC 2011. He also received a 2010 Young Author Best Paper Award by the IEEE Signal Processing Society, the 2011 Stephen O. Rice Prize in the Field of Communication Theory by the IEEE Communication Society, and the 2011 Young Investigator Research Excellence Award by the School of Engineering at HKUST. In 2013, he was the recipient the Asia-Pacific Best Young Researcher Award by the IEEE Communication Society. He is currently serving on the editorial board for the mathematics journal, *Random Matrices: Theory and Applications*, and he served on the editorial board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2012 to 2014.



Xiangyun Zhou (S'08–M'11) received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the Australian National University in 2007 and 2010, respectively. From 2010 to 2011, he worked as a Postdoctoral Fellow at UNIK—University Graduate Center, University of Oslo, Norway. He joined the Australian National University in 2011 and currently works as a Senior Lecturer. His research interests are in fields of communication theory and wireless networks.

Dr. Zhou currently serves on the editorial board of the following journals: IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, and *Security and Communication Networks* (Wiley). He also served as a guest editor for *IEEE Communications Magazine's* feature topic on wireless physical layer security and *EURASIP Journal on Wireless Communications and Networking's* special issue on energy harvesting wireless communications. He was a co-chair of the ICC workshop on wireless physical layer security at ICC'14 and ICC'15. He was the chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He is a recipient of the Best Paper Award at ICC'11.

Robert W. Heath, Jr. (S'96–M'01–SM'06–F'11) received the B.S. and M.S. degrees from the University of Virginia, Charlottesville, VA, USA, in 1996 and 1997, respectively, and the Ph.D. from Stanford University, Stanford, CA, USA, in 2002, all in electrical engineering. From 1998 to 2001, he was a Senior Member of the Technical Staff then a Senior Consultant at Iospan Wireless Inc, San Jose, CA where he worked on the design and implementation of the physical and link layers of the first commercial MIMO-OFDM communication system. Since January 2002, he has been with the Department of Electrical and Computer Engineering at The University of Texas at Austin where he is a Cullen Trust for Higher Education Endowed Professor, and is Director of the Wireless Networking and Communications Group. He is also President and CEO of MIMO Wireless Inc. and Chief Innovation Officer at Kuma Signals LLC. His research interests include several aspects of wireless communication and signal processing: limited feedback techniques, multihop networking, multiuser and multicell MIMO, interference alignment, adaptive video transmission, manifold signal processing, and millimeter wave communication techniques. He is a co-author of the book *Millimeter Wave Wireless Communications* (Prentice Hall, 2014).

He has been an Editor for the IEEE TRANSACTIONS ON COMMUNICATION, an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and lead guest editor for an IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS special issue on limited feedback communication, and lead guest editor for an IEEE JOURNAL ON SELECTED TOPICS IN SIGNAL PROCESSING special issue on Heterogenous Networks. He currently serves on the steering committee for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He was a member of the Signal Processing for Communications Technical Committee in the IEEE Signal Processing Society and is a former Chair of the IEEE COMSOC Communications Technical Theory Committee. He was a technical co-chair for the 2007 Fall Vehicular Technology Conference, general chair of the 2008 Communication Theory Workshop, general co-chair, technical co-chair and co-organizer of the 2009 IEEE Signal Processing for Wireless Communications Workshop, local co-organizer for the 2009 IEEE CAMSAP Conference, technical co-chair for the 2010 IEEE International Symposium on Information Theory, the technical chair for the 2011 Asilomar Conference on Signals, Systems, and Computers, general chair for the 2013 Asilomar Conference on Signals, Systems, and Computers, founding general co-chair for the 2013 IEEE GlobalSIP conference, and technical co-chair for the 2014 IEEE GLOBECOM conference.

Dr. Heath was a co-author of best student paper awards at IEEE VTC 2006 Spring, WPMC 2006, IEEE GLOBECOM 2006, IEEE VTC 2007 Spring, and IEEE RWS 2009, as well as co-recipient of the Grand Prize in the 2008 WinTech WinCool Demo Contest. He was co-recipient of the 2010 and 2013 EURASIP Journal on Wireless Communications and Networking best paper awards, the 2012 Signal Processing Magazine best paper award, a 2013 Signal Processing Society best paper award, the 2014 EURASIP Journal on Advances in Signal Processing best paper award, and the 2014 Journal of Communications and Networks best paper award. He was a 2003 Frontiers in Education New Faculty Fellow. He is also a licensed Amateur Radio Operator and is a registered Professional Engineer in Texas.