ARTIFICIAL-NOISE-AIDED SECURE MULTI-ANTENNA TRANSMISSION IN SLOW FADING CHANNELS WITH LIMITED FEEDBACK

Xi Zhang[⋆]*, Xiangyun Zhou*[†]*, Matthew R. McKay*[⋆]*, Robert W. Heath Jr.*[‡]

[⋆]Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, People's Republic of China

[†]Research School of Engineering, Australian National University, Australia

[‡]Department of Electrical and Computer Engineering, University of Texas at Austin, United States of America

ABSTRACT

We study secure multi-antenna transmission with limited feedback from the intended receiver and no feedback from the malicious eavesdropper. Our system uses the artificial-noise-aided beamforming approach to enhance secrecy, considering slow fading channels with outage constraints on the reliability performance of legitimate communication and the secrecy performance against eavesdropping. Our analytical results provide conditions on the minimum number of feedback bits and the minimum strength of the intended channel for making secure transmission possible. We observe that strengthening the secrecy outage constraint puts higher requirements on the number of feedback bits and the strength of the intended channel. To maximize the achievable secrecy rate, the optimal transmit power allocation between the information signal and the artificial noise is also derived in closed form.

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

1. INTRODUCTION

Much existing literature on physical-layer security assumes feedback of channel information from the eavesdropper. This is often an idealistic assumption and the designed system might be vulnerable if the eavesdropper chooses to keep silent and does not disclose its channel information to the legitimate users. Previous contributions have intentionally introduced artificial noise to degrade the eavesdropper's signal reception, which also reduced/removed the requirement for the eavesdropper's channel knowledge [1–6]. Nevertheless, most of the work in this line assumed perfect knowledge of the intended channel, which is still often too optimistic. Several previous papers have considered secure transmission design when the channel knowledge of the eavesdropper is not available, and that of the intended receiver is only imperfectly known at the transmitter [7–12]. To be specific, the studies in [7, 8] maximized the transmit power used to generate artificial noise, whilst guaranteeing a certain level of signal reception at the intended receiver. For fast fading channels, the studies in [9–11] characterized the ergodic secrecy rate performance and investigated the optimal transmit power allocation. For slow fading channels, the studies in [12] developed efficient algorithms for finding the optimal transmission rates and transmit power allocation that maximize the secrecy outage capacity.

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 X. Zhou was supported by the Australian Research Council's Discovery Projects funding scheme under Project No. DP110102548. The work of R. W. Heath was supported by the National Science Foundation under Grant No. NSF-CCF-1218338.

In this paper, we consider artificial-noise-aided secure multi-antenna transmission in slow fading channels, with limited feedback [13–18] from the intended receiver and no feedback from the eavesdropper. The channel knowledge obtained from pilot training is decomposed into two parts: the channel quality information (CQI) (i.e., the amplitude), and the channel direction information (CDI) (i.e., the direction in the unit complex hypersphere). The CQI is just a real positive number, while the CDI is a complex vector. For this reason, we assume that the CQI is accurately known at the transmitter, and focus on the quantization of the CDI [19]. We apply random vector quantization (RVQ) to quantize and feed back the CDI. Outage constraints are given to the reliability performance of legitimate communication and the secrecy performance against eavesdropping, and we carefully choose the transmission rates for wiretap coding [20] to meet these constraints. Our analytical results provide an easy-to-follow design guideline for the optimal secrecy rate performance. We first derive conditions on the number of feedback bits and the strength of the intended channel, under which a positive secrecy rate is achievable. Then, we provide a closed-form solution for the optimal transmit power allocation between the information signal and the artificial noise for achieving the maximum secrecy rate.

Prior work in [10] also considered quantized CDI, but studied the ergodic secrecy rate for fast fading channels, while we apply an outage formulation to study the secure transmission design in slow fading channels. While [12] developed numerical algorithms for finding the optimal design parameters in slow fading channels, we provide closed-form solutions, which lead to new insights. First, our analysis reveals that a minimum number of feedback bits and a minimum strength of the intended channel are required for achieving a positive secrecy rate. Secondly, we observe that imposing a more stringent secrecy outage constraint puts higher requirements on the number of feedback bits and the strength of the intended channel. Finally, we demonstrate different asymptotic behaviors of the optimal transmit power allocation with perfect channel knowledge [5] or with only limited feedback.

2. SYSTEM MODEL

Consider a system where the transmitter is equipped with $N \geq 2$ antennas, while the intended receiver and the malicious eavesdropper each has only a single antenna. We apply independent slow Rayleigh fading to model the wireless channels in a rich-scattering environment without line-of-sight transmission. The received signal at the intended receiver is given by

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

where $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$ is the intended channel, $\mathbf{x}$ is the transmitted vector, and $n_b \sim \mathcal{CN}(0,1)$ is the normalized thermal noise. The received signal at the eavesdropper is given by

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

where $\mathbf{g} \sim \mathcal{CN}\left(\mathbf{0}, \sigma_g^2 \mathbf{I}_N\right)$ is the channel to the eavesdropper, with σ_g^2 as the variance of each element of $\mathbf{g}$. As will be seen later, our analysis is valid for any value of σ_g^2, allowing the eavesdropper to be located at an arbitrary distance from the transmitter. As a robust secure transmission design, we consider a powerful eavesdropper with negligible thermal noise, i.e., $n_e \approx 0$.

2.1. Limited Feedback and Quantization

After pilot training, the obtained channel information is decomposed into the CQI $\|\mathbf{h}\|$ and the CDI $\mathbf{h}/\|\mathbf{h}\|$. Note that the CQI follows a chi distribution, which is real and positive, and it can be quantized efficiently using a small number of bits. Meanwhile, the CDI is uniformly distributed on the N-dimensional unit complex hypersphere, which is much more difficult to quantize. Hence, we assume that the CQI is accurately known at the transmitter, and use B_1 bits to quantize the CDI [19]. We choose 2^{B_1} unit-norm vectors to form a codebook $\mathcal{C} = \{\mathbf{c}_1, \ldots, \mathbf{c}_{2^{B_1}}\}$, which is known at both the transmitter and receiver. Then, an index selected from the following criterion:

$$\hat{\ell} = \underset{\ell \in \{1,\ldots,2^{B_1}\}}{\arg\max} \left|\mathbf{c}_\ell^H \mathbf{h}\right| \tag{3}$$

is fed back to the transmitter. Therefore, the corresponding unit-norm vector $\mathbf{c}_{\hat{\ell}}$ is the quantized CDI available at the transmitter. If the entries in $\mathcal{C}$ are drawn from the unit hypersphere randomly and independently, the resulting quantization scheme is RVQ. The optimal quantization scheme is generally unknown, and RVQ is adopted because it is amenable to analysis and performs close to optimal quantization [21–23].

2.2. Artificial-Noise-Aided Beamforming

Define the power allocation ratio ϕ as the ratio of the information signal power σ_u^2 to the total transmit power P. We denote the information signal by $u \sim \mathcal{CN}\left(0, \sigma_u^2\right)$ with $\sigma_u^2 = P\phi$. To confuse the malicious eavesdropper, the transmitter performs artificial-noise-aided beamforming [1]. To be specific, given a feedback index $\hat{\ell}$, the quantized CDI available at the transmitter is $\mathbf{c}_{\hat{\ell}}$; then, the transmitted vector $\mathbf{x}$ in (1) admits:

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

where $[\mathbf{c}_{\hat{\ell}}, \mathbf{W}]$ is an orthonormal basis and $\mathbf{v} \sim \mathcal{CN}\left(\mathbf{0}, \sigma_v^2 \mathbf{I}_{N-1}\right)$ is the artificial noise vector with $\sigma_v^2 = P(1-\phi)/(N-1)$.

2.3. Quantization Cell Approximation

As done in [23, 24], we approximate the quantization cell associated with $\mathbf{c}_{\hat{\ell}} \in \mathcal{C}$ as

$$\tilde{\mathcal{V}}_{\hat{\ell}} = \left\{\mathbf{z} \middle| \|\mathbf{z}\| = 1, \left|\mathbf{z}^H \mathbf{c}_{\hat{\ell}}\right|^2 \geq 1 - 2^{-\frac{B_1}{N-1}}\right\} \tag{5}$$

where the quantity $2^{-\frac{B_1}{N-1}}$ reflects the maximum quantization error in the CDI. It was shown in [23, 24] that the performance of RVQ can be closely approximated by such an approximation.

2.4. Wiretap Coding and Outage Definitions

Before transmission, the data is encoded using a wiretap code [20]. The codeword rate and the secrecy rate are denoted by R_b and R_s, respectively, with the rate redundancy $R_e := R_b - R_s$ intentionally added to provide secrecy. If the intended channel cannot support the codeword rate R_b, we consider this as a *connection outage* event. If the channel to the eavesdropper can support a data rate larger than the rate redundancy R_e, a *secrecy outage* is deemed to occur [25]. More discussions on code construction can be found in [26].

3. SECURE TRANSMISSION DESIGN

In this section, we first derive the connection and secrecy outage probabilities to measure the reliability performance of legitimate communication and the secrecy performance against eavesdropping, respectively. Then, we provide a detailed secure transmission design for the transmission rates and transmit power allocation, under given outage probability constraints.

3.1. Connection Outage Probability

For a given realization of the intended channel, the connection outage probability $p_{\text{co}}(\mathbf{h})$ is defined as the probability that the signal-to-noise ratio (SNR) at the intended receiver falls below a preselected threshold β_b.

Denote the exact CDI by $\mathbf{d} = \mathbf{h}/\|\mathbf{h}\|$. Given a feedback index $\hat{\ell}$, the exact CDI $\mathbf{d}$ will fall into $\tilde{\mathcal{V}}_{\hat{\ell}}$. By (5), we define

$$\cos^2\theta := \left|\mathbf{d}^H \mathbf{c}_{\hat{\ell}}\right|^2 \geq 1 - 2^{-\frac{B_1}{N-1}}. \tag{6}$$

The randomness in quantization error is embedded in the distribution of $\cos^2\theta$. By [23, Lemma 6], the cumulative distribution function of $\sin^2\theta = 1 - \cos^2\theta$ is given by

$$\Pr\left(\sin^2\theta \leq z\right) = \begin{cases} 0 & \text{for } z \leq 0 \\ 2^{B_1} z^{N-1} & \text{for } 0 < z \leq 2^{-\frac{B_1}{N-1}} \\ 1 & \text{for } z > 2^{-\frac{B_1}{N-1}} \end{cases}. \tag{7}$$

By (1) and (4), the received signal at the intended receiver is given by

$$y_b = \|\mathbf{h}\| \mathbf{d}^H \mathbf{c}_{\hat{\ell}} u + \|\mathbf{h}\| \mathbf{d}^H \mathbf{W}\mathbf{v} + n_b \tag{8}$$

with the corresponding SNR given by

$$\text{SNR}_b = \frac{\|\mathbf{h}\|^2 \cos^2\theta \sigma_u^2}{\|\mathbf{h}\|^2 \sin^2\theta \sigma_v^2 + 1} \tag{9}$$

which follows from (6) and the fact $\left|\mathbf{d}^H \mathbf{c}_{\hat{\ell}}\right|^2 + \|\mathbf{d}^H \mathbf{W}\|^2 = 1$.

To the transmitter, the quantization error in the obtained CDI is unknown, and the SNR at the intended receiver is actually a random variable. By (7), the connection outage probability $p_{\text{co}}(\mathbf{h})$ can be computed as

$$\begin{aligned} p_{\text{co}}(\mathbf{h}) &= \Pr\left(\text{SNR}_b \leq \beta_b\right) \\ &= \begin{cases} 0 & \text{for } \beta_b \leq \beta_1 \\ 1 - 2^{B_1}\left(\frac{\|\mathbf{h}\|^2 P\phi - \beta_b}{\|\mathbf{h}\|^2\left(P\phi + \frac{P(1-\phi)}{N-1}\beta_b\right)}\right)^{N-1} & \text{for } \beta_1 < \beta_b \leq \beta_2 \\ 1 & \text{for } \beta_b > \beta_2 \end{cases} \end{aligned} \tag{10}$$

where

$$\beta_1 = \frac{\|\mathbf{h}\|^2 P\phi\left(1-2^{-\frac{B_1}{N-1}}\right)}{\|\mathbf{h}\|^2 \frac{P(1-\phi)}{N-1} 2^{-\frac{B_1}{N-1}} + 1}$$
$$\beta_2 = \|\mathbf{h}\|^2 P\phi. \tag{11}$$

Note that the connection outage probability $p_{\text{co}}(\mathbf{h})$ and the defined boundary value β_1 are both functions of the number of feedback bits for the CDI B_1. As B_1 grows large, $\beta_1 \to \beta_2$ and $p_{\text{co}}(\mathbf{h})$ becomes a step function with transition at $\beta_b = \|\mathbf{h}\|^2 P\phi$.

3.2. Secrecy Outage Probability

For a given realization of the intended channel, the secrecy outage probability $p_{\text{so}}(\mathbf{h})$ is defined as the probability that the received SNR at the eavesdropper exceeds a preselected threshold β_e.

By (2) and (4), the received signal at the eavesdropper y_e is given by

$$y_e = \mathbf{g}^H \mathbf{c}_{\hat{\ell}} u + \mathbf{g}^H \mathbf{W}\mathbf{v} \tag{12}$$

with corresponding SNR

$$\text{SNR}_e = \frac{\left|\mathbf{g}^H \mathbf{c}_{\hat{\ell}}\right|^2 \sigma_u^2}{\|\mathbf{g}^H \mathbf{W}\|^2 \sigma_v^2}. \tag{13}$$

Since the channel to the eavesdropper is unknown to the legitimate users, by [5, eq. (5)], the secrecy outage probability $p_{\text{so}}(\mathbf{h})$ can be computed as

$$p_{\text{so}}(\mathbf{h}) = \Pr\left(\text{SNR}_e \geq \beta_e\right) = \left(1 + \beta_e \frac{\phi^{-1}-1}{N-1}\right)^{1-N} \tag{14}$$

which is independent of $\mathbf{h}$. Note that this result holds true for any value of σ_g^2, allowing the eavesdropper to be located at an arbitrary distance from the transmitter, which is very desirable.

We now provide a detailed secure transmission design under given constraints on the connection and secrecy outage probabilities.

3.3. Connection and Secrecy Outage Constraints

To ensure the reliability performance of legitimate communication and the secrecy performance against eavesdropping, we enforce the following constraints on the connection and secrecy outage probabilities:

$$p_{\text{co}}(\mathbf{h}) \leq \sigma \quad \text{and} \quad p_{\text{so}}(\mathbf{h}) \leq \epsilon \tag{15}$$

where $\sigma, \epsilon \in [0,1]$. We then carefully choose the transmission rates R_b and R_e to meet these constraints.

By (10), for a given realization of the intended channel, the connection outage constraint $p_{\text{co}}(\mathbf{h}) \leq \sigma$ implies that the maximum allowable codeword rate $R_b = \log_2(1+\beta_b)$ is

$$R_b^{\max}(\mathbf{h}, \phi) = \log_2\left(1 + \frac{\|\mathbf{h}\|^2 P\phi\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}}\right)}{\|\mathbf{h}\|^2 \frac{P(1-\phi)}{N-1} \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}} + 1}\right). \tag{16}$$

As can be seen, with a sufficient number of feedback bits for the CDI (i.e., as $B_1 \to \infty$), the transmitter adapts the codeword rate R_b to the capacity of the intended channel, regardless of the connection outage constraint σ.

From (14), under the secrecy outage constraint $p_{\text{so}}(\mathbf{h}) \leq \epsilon$, the minimum required rate redundancy $R_e = \log_2(1+\beta_e)$ is

$$R_e^{\min}(\mathbf{h}, \phi) = \log_2\left(1 + \frac{\phi}{1-\phi}(N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right)\right). \tag{17}$$

Note that the required rate redundancy R_e becomes infinitely large in the limit that $\epsilon = 0$ with $\phi \neq 0$, i.e., it is impossible to completely avoid secrecy outages. Henceforth, we focus on the case $\epsilon \in (0,1]$.

Since the achievable secrecy rate is given by $R_s = R_b - R_e$, it is desirable to choose the maximum R_b and the minimum R_e that meet the outage constraints. Note that the transmit power allocation is yet to be optimized for maximizing the secrecy rate. From (16) and (17), for a given realization of the intended channel, the maximum secrecy rate $R_s^{\max}$, under the outage constraints in (15), is given by

$$R_s^{\max}(\mathbf{h}) = \max_{\phi \in (0,1)} \left[R_b^{\max}(\mathbf{h}, \phi) - R_e^{\min}(\mathbf{h}, \phi)\right]^+ \tag{18}$$

where $[x]^+ = \max\{0, x\}$.

3.4. Conditions for Positive Secrecy Rate

We now investigate the conditions under which a positive secrecy rate is achievable. From (18), we derive two necessary conditions as follows.

First, a minimum number of feedback bits for the CDI is required:

$$B_1 \geq B_1^{\min} := \begin{cases} \left\lfloor \log_2\left(\frac{1-\sigma}{\epsilon}\right)\right\rfloor + 1 & \text{for } \sigma + \epsilon < 1 \\ 1 & \text{for } \sigma + \epsilon \geq 1 \end{cases} \tag{19}$$

where $\lfloor x \rfloor$ is the integer part of x. This condition suggests that under the connection and secrecy outage constraints, a positive secrecy rate cannot be achieved if the transmitter is not sufficiently confident about the beamforming direction. We point out that the first case is most relevant since the allowable outage probabilities are typically small, while the second case is not very relevant in practice.

From (19), we make the following observations:

- For a given connection outage constraint σ, reducing the secrecy outage constraint ϵ exponentially requires a linear increase in the minimum number of feedback bits for the CDI $B_1^{\min}$, and it grows unbounded as $\epsilon \to 0$. The underlying reason is that to reduce the quantization error in the CDI and thereby giving a chance for achieving a positive secrecy rate, a large number of feedback bits is required. This observation is illustrated in Fig. 1. With a typical secrecy outage constraint $\epsilon \in [0.001, 0.01]$, roughly $B_1^{\min} \in [7, 10]$ feedback bits are needed, and it is not very sensitive to the value of σ.
- Interestingly, this condition is independent of the number of transmit antennas N. As can be seen from (5) and (10), for a given number of feedback bits for the CDI B_1, increasing N will lead to a larger quantization error and thus a larger connection outage probability. Meanwhile, as can be seen from (14), increasing N would reduce the secrecy outage probability. These two effects canceled each other and this is why we do not see N in (19).
- For a given secrecy outage constraint ϵ, the required minimum number of feedback bits $B_1^{\min}$ increases by imposing a more stringent connection outage constraint (i.e., reducing σ), and its maximum value is given by $\left\lfloor \log_2\left(\frac{1}{\epsilon}\right)\right\rfloor + 1$. This makes sense because we assumed bounded quantization error in the CDI. When $\sigma = 0$,

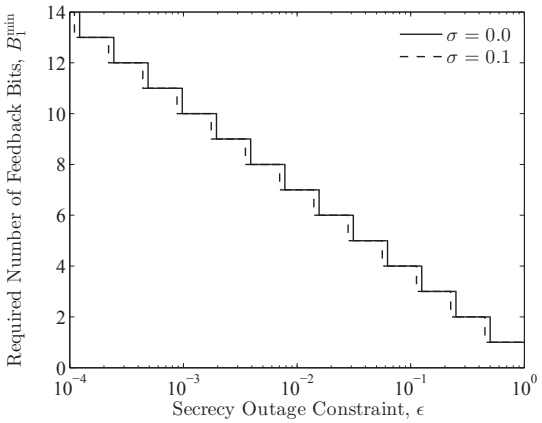

Fig. 1. Minimum required number of feedback bits for the CDI $B_1^{\min}$ versus the secrecy outage constraint ϵ.

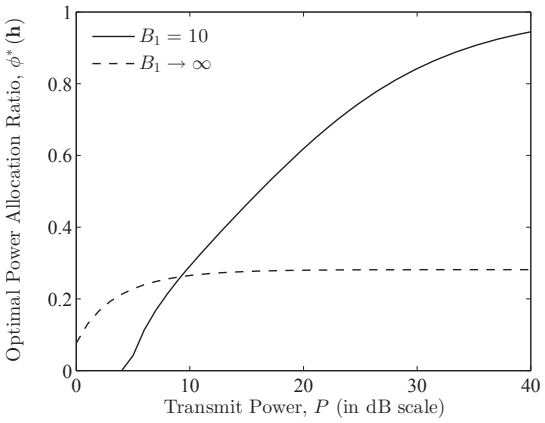

Fig. 2. Optimal power allocation ratio $\phi^*(\mathbf{h})$ versus the transmit power P, with $N = 8$, $\sigma = 0.01$, $\epsilon = 0.01$ and $\|\mathbf{h}\| = 2\sqrt{2}$.

the transmitter assumes that the angle between the obtained CDI and the exact one is at its maximum possible value, and thereby matches the codeword rate in (16) to the minimum possible capacity of the intended channel.

Second, having satisfied the condition in (19), the strength of the intended channel still must be strong enough:

$$\|\mathbf{h}\|^2 > \mu_1 := \frac{(N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right)}{P\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}\epsilon}}\right)}. \tag{20}$$

From this condition, an on-off transmission strategy [25] with a transmit threshold μ_1 is adopted. As expected, with a sufficient number of feedback bits for the CDI (i.e., as $B_1 \to \infty$), the transmit threshold μ_1 converges to the one with perfect knowledge of the intended channel, given in [5, eq. (28)].

3.5. Transmit Power Allocation Optimization

When the conditions for a positive secrecy rate in (19) and (20) are satisfied (i.e., $B_1 \geq B_1^{\min}$ and $\|\mathbf{h}\|^2 > \mu_1$), secure transmission becomes possible and we further optimize the transmit power allocation between the information signal and the artificial noise. The power allocation problem in (18) can now be rewritten as

$$R_s^{\max}(\mathbf{h}) = \max_{\phi \in (0, \phi_{\max})} R_b^{\max}(\mathbf{h}, \phi) - R_e^{\min}(\mathbf{h}, \phi) \tag{21}$$

where

$$\phi_{\max} = 1 - \frac{(N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right)}{\|\mathbf{h}\|^2 P\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}\epsilon}}\right)} > 0. \tag{22}$$

By the monotonicity of the logarithm function, we find the optimal power allocation ratio as follows:

$$\phi^*(\mathbf{h}) = \frac{(X - YZ - Z)\,Y + X - \sqrt{X - YZ - Z + 1}\sqrt{XZ\,(Y+1)}}{(X - YZ)\,Y + X - XZ} \tag{23}$$

where

$$X = \|\mathbf{h}\|^2 P\left(1 - \sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}}\right)$$
$$Y = \frac{\|\mathbf{h}\|^2 P}{N-1}\sqrt[N-1]{\frac{1-\sigma}{2^{B_1}}}$$
$$Z = (N-1)\left(\sqrt[N-1]{\frac{1}{\epsilon}} - 1\right). \tag{24}$$

From (23), we make the following observations:

- With a given transmit power P, increasing the number of feedback bits for the CDI B_1 leads to a decrease in the optimal power allocation ratio $\phi^*(\mathbf{h})$. Since we assumed that the CQI is accurately known at the transmitter, as one may expect, we have $\lim_{B_1 \to \infty} \phi^*(\mathbf{h}) = \phi^*_{\text{perfect}}(\mathbf{h})$, where $\phi^*_{\text{perfect}}(\mathbf{h})$ is the optimal power allocation ratio with perfect knowledge of the intended channel, given in [5, eq. (29)].
- With a given number of feedback bits for the CDI B_1, by increasing the transmit power P, the optimal power allocation ratio $\phi^*(\mathbf{h})$ increases towards one, i.e., $\lim_{P \to \infty} \phi^*(\mathbf{h}) = 1$. This is quite different from the case with perfect channel knowledge (i.e., $B_1 \to \infty$), where $\lim_{P \to \infty} \phi^*_{\text{perfect}}(\mathbf{h}) < 1$ [5]. With quantization error in the CDI and as the transmit power grows large, the optimal power allocation strategy is to give more transmit power to the information signal, which will in turn reduce the artificial noise that leaks into the intended channel. This observation is confirmed in Fig. 2.

4. CONCLUSION

The obtained optimal design of artificial-noise-aided secure multi-antenna transmission with limited feedback can be summarized as follows: 1) For given connection and secrecy outage constraints in (15), ensure that there are enough feedback bits for the CDI, as stated in (19); 2) When the intended channel is stronger than (20), transmit with the rates and power allocation parameters in (16), (17) and (23). The secrecy throughput can be evaluated by averaging the maximum secrecy rate over all channel realizations, and it is currently under investigation, together with the quantization of the CQI.

5. REFERENCES

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

[2] W. Shi and J. Ritcey, "Robust beamforming for MISO wiretap channel by optimizing the worst-case secrecy capacity," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, America, Nov. 2010, pp. 300–304.

[3] X. Zhang, X. Zhou, and M. R. McKay, "Benefits of multiple transmit antennas in secure communication: A secrecy outage viewpoint," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, America, Nov. 2011, pp. 212–216.

[4] 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, America, Nov. 2011, pp. 207–211.

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

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

[7] 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.

[8] 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.

[9] 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.

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

[11] 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, Canada, Jun. 2012, pp. 4782–4787.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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, America, Nov. 2010, pp. 1582–1587.

[19] D. J. Love, R. W. Heath Jr., V. K. N. Lau, D. Gesbert, B. D. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems," *IEEE J. Select. Areas Commun.*, vol. 26, no. 8, pp. 1341–1365, Oct. 2008.

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

[21] W. Santipach, Y. Sun, and M. L. Honig, "Benefits of limited feedback for wireless channels," in *Proc. Allerton Conf. Commun., Control, Comput.*, Monticello, America, Oct. 2003.

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

[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. Select. Areas Commun.*, vol. 25, no. 7, pp. 1478–1491, Sep. 2007.

[25] 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.

[26] 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.