On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels

Xi Zhang, *Student Member, IEEE,* Xiangyun Zhou, *Member, IEEE,*
and Matthew R. McKay, *Member, IEEE*

Abstract—In this paper, we investigate the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels. The primary design concerns include the transmit power allocation and the rate parameters of the wiretap code. We consider two scenarios with different complexity levels: i) the design parameters are chosen to be fixed for all transmissions, ii) they are adaptively adjusted based on the instantaneous channel feedback from the intended receiver. In both scenarios, we provide explicit design solutions for achieving the maximal throughput subject to a secrecy constraint, given by a maximum allowable secrecy outage probability. We then derive accurate approximations for the maximal throughput in both scenarios in the high signal-to-noise ratio region, and give new insights into the additional power cost for achieving a higher security level, whilst maintaining a specified target throughput. In the end, the throughput gain of adaptive transmission over non-adaptive transmission is also quantified and analyzed.

Index Terms—Physical-layer security, multi-antenna transmission, artificial noise, power allocation, secrecy outage probability, throughput optimization.

I. INTRODUCTION

WITH the rapid development of wireless technology, an ever-increasing amount of sensitive data (e.g., private conversation, credit card information) is transmitted over wireless networks. However, the broadcasting nature of the wireless medium makes it especially vulnerable to malicious interception. Currently, cryptographic algorithms, typically designed without exploiting the physical properties of the wireless medium, are used to keep broadcasted messages confidential. For such techniques, although the expenditure of interception may be very high, providing robust encryption algorithms is becoming ever more challenging, due to the continuing development of computing devices. By taking the physical properties of the wireless channels into consideration, the recently developed physical-layer security techniques can

guarantee secure transmission regardless of the eavesdropper's computational capability. As such, these techniques have drawn a lot of recent attention from the research community.

A. Background and Previous Work

The notion of perfect secrecy was first introduced by Shannon [1]. Subsequently, pioneering works on physical-layer security [2, 3] proved that there exist coding schemes which can ensure transmission reliability and perfect secrecy simultaneously. Many recent papers have expanded upon these initial contributions, considering different system configurations and assumptions. Particularly, multi-antenna techniques have been extensively studied as a means for achieving security enhancements [4–8]. However, in much of the literature on physical-layer security, the eavesdropper's channel state information (CSI) was assumed to be available at the transmitter, which is usually impractical. To relax this strong assumption, the authors in [9] proposed a multi-antenna transmission scheme that inserts artificial noise into the transmitted signal in a controlled manner, thus to confuse the malicious eavesdropper. This transmission scheme requires the instantaneous CSI feedback from the intended receiver, but not the eavesdropper, which is a major advancement toward practical secure communications.

Building on the ideas from [9], the design and analysis of artificial-noise-aided transmission has been further studied for both fast and slow fading channels [10–16]. For fast fading channels, the channel coherence time is much shorter than the codeword length and the ergodic secrecy rate is often used as the performance metric for designing beamforming and power allocation strategies [10–12]. For slow fading channels, the channel coherence time is usually longer than the codeword length, and in such scenarios outage-based formulations become more appropriate. To this end, various secrecy outage formulations were proposed first in [17, 18] and recently in [19, 20]. In particular, the first formulation developed in [17, 18] has been used for studying artificial-noise-aided multi-antenna transmission schemes in [13–16]. This secrecy outage formulation characterizes the possibility of having a secure and reliable transmission, without distinguishing secrecy from reliability. In other words, a secrecy outage event defined therein may occur due to either an insecure link to the eavesdropper or an unreliable link to the intended receiver. To better assist the secure transmission design, revised secrecy outage formulations were independently developed in [19] and [20].

X. Zhang and M. R. McKay are with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong (e-mails: xizhangx@ust.hk, eemckay@ust.hk).

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

In these revised outage formulations, a secrecy outage event arises solely due to an insecure link to the eavesdropper; thus, the secrecy and reliability performance can be measured separately. These revised secrecy outage formulations can be utilized to obtain a better understanding and more practically-oriented designs for the artificial-noise-aided secure multi-antenna transmission.

B. Our Approach and Contributions

In this paper, we provide new design guidelines for artificial-noise-aided secure multi-antenna transmission in slow fading channels, based on the recently developed secrecy outage formulation in [20]. This formulation allows us to measure the secrecy and reliability performance for any given rate parameters of the wiretap code. In turn, we are able to set the rate parameters to achieve a target secrecy level, given by a maximum allowable secrecy outage probability. To the best of the authors' knowledge, no prior work on artificial-noise-aided multi-antenna transmission has considered the rate parameters of the wiretap code as design parameters.

Our main contributions include explicit design solutions and new performance analysis results for the throughput-maximizing transmission schemes with either fixed-rate or adaptive-rate encoder, under a constraint on the level of secrecy. The design concerns include the rate parameters of the wiretap code, as well as the transmit power allocation between the information-bearing signal and the artificial noise. We consider two scenarios with different system complexities:

- In the first scenario, the design parameters are optimized off-line and remain fixed for all transmissions. We divide our design into two steps: The first step minimizes the transmission delay for a given data rate, while the second step maximizes the average throughput. In the first step, closed-form solutions are derived for the optimal system parameters and the secrecy-delay tradeoff for fixed-rate transmission is captured. In the second step, the average throughput is maximized by numerically optimizing the data rate with the optimal designs of all other system parameters already given in closed form. To obtain further analytical insights, we derive a high signal-to-noise ratio (SNR) approximation of the optimal data rate to maximize the average throughput. Focusing on the high SNR region, we further investigate the additional power cost incurred by imposing or strengthening the secrecy constraint, while guaranteeing a specified target throughput.
- In the second scenario, the design parameters are dynamically adjusted based on the instantaneous channel feedback from the intended receiver. We provide an analytical solution to the optimal system parameters that maximize the achievable data rate for each realization of the intended channel, under the secrecy constraint, such that the average throughput is also maximized. In the high SNR region, we present accurate approximations for the maximal throughput, which enable us to study the additional power cost incurred by imposing or strengthening the secrecy constraint, while achieving a specified target

throughput. Finally, we analyze the throughput gain of adaptive-rate transmission over fixed-rate transmission. Whilst doing adaptation is always beneficial in terms of increasing the throughput, our analysis shows that in the high SNR region, the throughput gain is most significant when the number of transmit antennas is small. Moreover, we show that the throughput gain brought by doing adaption is not very sensitive to the required secrecy level.

We point out that, similar to our work, a very recent contribution [21] also used a secrecy outage formulation along the lines of [19, 20] to study artificial-noise-aided multi-antenna transmission. The main focus therein was to minimize the power consumption for given levels of secrecy and quality-of-service performance, while the transmission rates were not part of the design consideration. In contrast, we consider a transmission system with a fixed transmit power, and optimize the rate parameters of the wiretap code as well as the transmit power allocation to maximize the average throughput, subject to (s.t.) a secrecy outage constraint.

II. SYSTEM MODEL AND PERFORMANCE METRIC

We consider the transmission from Alice to Bob in the presence of an eavesdropper Eve. Alice is equipped with multiple transmit antennas ($N \geq 2$) while Bob and Eve each has one receive antenna. Thus, the channel from Alice to Bob is multiple-input and single-output (MISO). We assume a non-line-of-sight rich scattering environment, and as such, model all channels as uncorrelated Rayleigh fading. It is also assumed that Bob can estimate his channel accurately and use a perfect feedback link to inform Alice about his instantaneous CSI. This feedback link is not secure and can be intercepted by Eve. We further assume that the coherence time is long enough to support the wiretap code [2] and the time used for learning the channel and feeding back the CSI is negligible. Assuming Eve is a passive eavesdropper, the instantaneous CSI of Eve is thereby unavailable to Alice.

The N dimensional symbol vector to be transmitted is defined as $\mathbf{x}$ and the received signal at Bob is given by

$$y_b = \mathbf{h}^T \mathbf{x} + n_b , \qquad (1)$$

where the $N \times 1$ vector $\mathbf{h}$ is the channel fading gain from Alice to Bob and n_b is the receiver noise at Bob. The entries of $\mathbf{h}$ and n_b are assumed to be independent and identically distributed (i.i.d.) zero-mean complex Gaussian variables with unit variance.

Similarly, the received signal at Eve is given by

$$y_e = \mathbf{g}^T \mathbf{x} + n_e , \qquad (2)$$

where the $N \times 1$ vector $\mathbf{g}$ captures the channel fading gain from Alice to Eve and n_e is the receiver noise at Eve. The entries of $\mathbf{g}$ are assumed to be i.i.d. zero-mean complex Gaussian variables each with variance σ_g^2.

A. Transmit Beamforming with Artificial Noise Generation

The authors in [9] introduced the concept of generating artificial noise to guarantee secure transmission. The key idea

is outlined as follows. Alice generates an orthonormal basis of $\mathbb{C}^N$ as $\mathbf{W} = [\mathbf{w}_1 \ \mathbf{W}_2]$, where $\mathbf{w}_1 = \mathbf{h}^*/||\mathbf{h}||$. Then she mixes some artificial noise with the message symbol u as

$$\mathbf{x} = \mathbf{w}_1 u + \mathbf{W}_2 \mathbf{v} \ ,$$

where u is complex Gaussian distributed and $\mathbf{v}$ is the artificial noise vector.

With this beamforming strategy, by (1) and (2), the received signal at Bob becomes

$$y_b = \mathbf{h}^T \mathbf{w}_1 u + \mathbf{h}^T \mathbf{W}_2 \mathbf{v} + n_b = ||\mathbf{h}|| u + n_b \ , \qquad (3)$$

while the received signal at Eve becomes

$$y_e = \mathbf{g}^T \mathbf{w}_1 u + \mathbf{g}^T \mathbf{W}_2 \mathbf{v} + n_e = g_1 u + \mathbf{g}_2^T \mathbf{v} + n_e \ , \qquad (4)$$

where $g_1 = \mathbf{g}^T \mathbf{w}_1$ and $\mathbf{g}_2^T = \mathbf{g}^T \mathbf{W}_2$.

The total transmit power available at Alice is denoted as P. The power allocation ratio Φ is defined as the fraction of the information-bearing signal power to the total transmit power. Thus, the variance of u is set to $P\Phi$. By (3), it is clear that Alice is performing maximal ratio transmission on the channel to Bob and the instantaneous effective channel gain is $||\mathbf{h}||^2$. Therefore, the instantaneous channel capacity to Bob is $C_b = \log_2\left(1 + P\Phi||\mathbf{h}||^2\right)$, where $||\mathbf{h}||^2 \sim \text{Gamma}\,(N, 1)$. The complementary cumulative distribution function (c.c.d.f.) of $||\mathbf{h}||^2$ is $\bar{F}_{||\mathbf{h}||^2}(r) = \tilde{\Gamma}\,(N, r)$, where $\tilde{\Gamma}\,(\cdot, \cdot)$ is the regularized upper incomplete gamma function. All transmit power not allocated to u is equally assigned to the $N - 1$ entries of $\mathbf{v}$, due to the absence of Eve's CSI. Therefore, the entries of $\mathbf{v}$ are set to be i.i.d. zero-mean complex Gaussian variables each with variance $\sigma_v^2 = \frac{P(1-\Phi)}{N-1}$. The power allocation ratio Φ may be dynamically adjusted based on $\mathbf{h}$.

Since the noise power at Eve is typically unknown to Alice, a robust approach, as done in [10], is to design for the worst-case scenario and assume that there is no receiver noise at Eve (i.e., $n_e = 0$). Therefore, from (4), for a given realization of the channel fading gains (i.e., $\mathbf{h}$ and $\mathbf{g}$), the instantaneous SNR at Eve is given by

$$\gamma_e = \frac{|g_1|^2 \sigma_u^2}{||\mathbf{g}_2||^2 \sigma_v^2} = \frac{N-1}{\Phi^{-1}-1} \frac{|g_1|^2}{||\mathbf{g}_2||^2} \ .$$

Since $\mathbf{g}$ has i.i.d. complex Gaussian entries each with variance σ_g^2 and $\mathbf{W}$ is unitary, $\mathbf{g}^T \mathbf{W} = [g_1 \ \mathbf{g}_2]$ also has i.i.d. complex Gaussian entries each with variance σ_g^2. Using [22, Eq. 19], the c.c.d.f. of γ_e can be characterized as

$$\bar{F}_{\gamma_e}(\gamma_e) = \left(1 + \gamma_e \left(\frac{\Phi^{-1}-1}{N-1}\right)\right)^{1-N} \ . \qquad (5)$$

As $N \to \infty$, this converges to the c.c.d.f. of an exponential distribution with mean $\frac{\Phi}{1-\Phi}$. Note that if Φ is adaptively adjusted based on $\mathbf{h}$, the distribution of the received SNR at Eve would be changed dynamically.

B. Secure Transmission and Throughput

Using the well-known wiretap code [2], data is encoded before transmission. The rates of the transmitted codeword and the secret message are denoted as R_b and R_s, respectively. In this paper, we refer to the rates R_b and R_s as the rate parameters of the wiretap code. The rate redundancy $R_e \triangleq R_b - R_s$ is intentionally added in order to provide secrecy against eavesdropping. If the instantaneous channel capacity to Eve $C_e = \log_2(1 + \gamma_e)$ is larger than R_e, perfect secrecy cannot be achieved and a secrecy outage is deemed to occur.

We consider an on-off transmission scheme [20] where Alice decides to transmit or not, based on her knowledge of Bob's channel $\mathbf{h}$. To be specific, Alice transmits only if the effective channel gain $||\mathbf{h}||^2$ exceeds a threshold μ. As will be seen, this on-off scheme is adopted to prevent undesirable transmissions which incur capacity outages (i.e., $R_b > C_b$) or unacceptably high risk of secrecy outage (which occurs when $C_e > R_e$). With the on-off transmission strategy, the transmit probability is

$$p_{\text{tx}}(\mu) = \bar{F}_{||\mathbf{h}||^2}(\mu) = \tilde{\Gamma}\,(N, \mu) \ . \qquad (6)$$

Since the channel fading gain changes from time to time, Alice would transmit once the effective channel gain exceeds the preselected threshold (i.e., $||\mathbf{h}||^2 > \mu$). In this way, the value of the transmit probability p_{tx} is directly related to the average delay, i.e., the larger p_{tx}, the shorter the expected delay.

Since the rates of the wiretap code may be adaptively adjusted based on Bob's channel feedback, the rates R_b and R_s are potentially functions of $\mathbf{h}$. The average throughput is then defined as

$$\eta = \mathbb{E}_{\mathbf{h}}\left[R_s\,(\mathbf{h})\right] \quad (\text{bits/channel use}) \ , \qquad (7)$$

where $R_s\,(\mathbf{h}) = 0$ for $||\mathbf{h}||^2 \leq \mu$, as a consequence of the on-off transmission protocol. Note that this throughput definition is meaningful only when: i) the risk of secrecy outage is under control, ii) the intended receiver can decode the messages correctly. As will be seen later, our designs can satisfy these two conditions simultaneously; thus, it is meaningful to apply this throughput definition.

C. Secrecy Performance Characterization

From (5), it is clear that changing the power allocation would effectively alter the distribution of the received SNR at Eve. With on-off transmission, for a given $\mathbf{h}$, if $||\mathbf{h}||^2 > \mu$, Alice would specify three parameters: $R_b\,(\mathbf{h})$, $R_s\,(\mathbf{h})$ and $\Phi\,(\mathbf{h})$ for transmission; otherwise, she stops transmission. Therefore, the secrecy outage probability is given by

$$p_{\text{so}}\,(R_b\,(\mathbf{h}), R_s\,(\mathbf{h}), \Phi\,(\mathbf{h}))$$
$$= \begin{cases} \Pr\,(C_e\,(\Phi\,(\mathbf{h})) > R_b\,(\mathbf{h}) - R_s\,(\mathbf{h})) & \text{if } ||\mathbf{h}||^2 > \mu \ , \\ 0 & \text{other} \ , \end{cases}$$

where

$$\Pr\,(C_e\,(\Phi\,(\mathbf{h})) > R_b\,(\mathbf{h}) - R_s\,(\mathbf{h}))$$
$$= \left(1 + \left(2^{R_b(\mathbf{h}) - R_s(\mathbf{h})} - 1\right)\left(\frac{\Phi^{-1}(\mathbf{h}) - 1}{N-1}\right)\right)^{1-N} \ , \qquad (8)$$

evaluated from (5).

Since we assumed that $n_e = 0$, the above-mentioned p_{so} is an upper bound on the actual secrecy outage probability. It

depends on the power allocation ratio Φ, but not the transmit power P.

The overall secrecy outage probability of this transmission system is given by

$$\bar{p}_{\text{so}} = \mathbb{E}\left[p_{\text{so}}\left(R_b\left(\mathbf{h}\right), R_s\left(\mathbf{h}\right), \Phi\left(\mathbf{h}\right)\right) \mid \|\mathbf{h}\|^2 > \mu \right] . \quad (9)$$

In sequel, we consider the optimization of the throughput performance, given a maximum allowable secrecy outage probability ϵ.

III. SECURE TRANSMISSION DESIGN WITH NON-ADAPTIVE ENCODER

In this section, we consider the scenario where a single codebook is used by Alice and Bob, thus R_b and R_s are carefully chosen to have fixed values which do not change with $\mathbf{h}$. In addition, the value of Φ is also optimized off-line and remains fixed. We refer to this as the non-adaptive encoding (NAE) scheme.

The primary design objective is to meet the secrecy requirement given on the secrecy outage probability. For the NAE scheme, the design parameters R_b, R_s and Φ have fixed values for all transmissions (i.e., they do not change with $\mathbf{h}$); thus, (8) becomes independent of $\mathbf{h}$. Consequently, the conditional expectation in (9) can be ignored, and the overall secrecy outage probability $\bar{p}_{\text{so}}$ in this case is described by (8). In other words, for the NAE scheme, the overall secrecy outage probability is a function of R_b, R_s and Φ, and the secrecy requirement can be written as $\bar{p}_{\text{so}}\left(R_b, R_s, \Phi\right) \leq \epsilon$.

Meanwhile, as already mentioned, on-off transmission with threshold μ is adopted to prevent undesirable transmissions which incur capacity outages at Bob. When Alice decides to transmit (i.e., $\|\mathbf{h}\|^2 > \mu$), the channel capacity to Bob is

$$C_b = \log_2\left(1 + P\Phi\|\mathbf{h}\|^2 \right) > \log_2\left(1 + P\Phi\mu \right) .$$

Thus, with R_b satisfying $R_b \leq \log_2\left(1 + P\Phi\mu \right)$, the transmitted messages can be decoded at Bob with an arbitrarily low error probability.

From (6) and (7), the throughput of the NAE scheme is given by

$$\eta_{\text{NAE}} = p_{\text{tx}}\left(\mu\right) \times R_s . \quad (10)$$

Now we consider throughput optimization of this NAE scheme under the secrecy constraint. Combining the above discussions, the throughput optimization problem is posed as follows:

$$\max_{\mu, R_b, R_s, \Phi} \quad p_{\text{tx}}\left(\mu\right) \times R_s$$
$$\text{s.t.} \quad \bar{p}_{\text{so}}\left(R_b, R_s, \Phi\right) \leq \epsilon ,$$
$$R_b \leq \log_2\left(1 + P\Phi\mu \right) ,$$
$$0 \leq R_s \leq R_b ,$$
$$0 \leq \Phi \leq 1 ,$$
$$0 \leq \mu . \quad (11)$$

We solve the problem in two steps. In the first step, we fix R_s and maximize $p_{\text{tx}}\left(\mu\right)$ with respect to (w.r.t.) μ, R_b and Φ. Since R_s is fixed, by maximizing p_{tx}, this step can be viewed as a delay-minimizing design, while satisfying the secrecy

constraint. With a minor abuse of notation, the maximal p_{tx} for a given R_s is denoted as $p_{\text{tx}}^{\max}\left(R_s\right)$, where μ is optimized already. Then, in the second step, we consider the throughput maximization, i.e., maximizing $p_{\text{tx}}^{\max}\left(R_s\right) \times R_s$ w.r.t. R_s.

A. Delay Minimization

From (11), the delay minimization problem is posed as

$$\max_{\mu, R_b, \Phi} \quad p_{\text{tx}}\left(\mu\right)$$
$$\text{s.t.} \quad \bar{p}_{\text{so}}\left(R_b, \Phi\right) \leq \epsilon ,$$
$$R_b \leq \log_2\left(1 + P\Phi\mu \right) ,$$
$$R_s \leq R_b ,$$
$$0 \leq \Phi \leq 1 ,$$
$$0 \leq \mu . \quad (12)$$

To simplify the expressions throughout the paper, we define the quantity:

$$\lambda\left(\epsilon, N\right) := \left(N - 1\right)\left(\epsilon^{\frac{1}{1-N}} - 1 \right) . \quad (13)$$

The solution to (12) is presented as follows, while the derivation is relegated to Appendix A.

Proposition 1. With a non-adaptive encoder, for a prescribed message rate R_s and under the secrecy constraint $\bar{p}_{\text{so}} \leq \epsilon$, the maximal transmit probability in (12) leading to the minimal average delay is given by:

$$p_{\text{tx}}^{\max} = \tilde{\Gamma}\left(N, \frac{1}{P}\left(\sqrt{2^{R_s}\lambda\left(\epsilon, N\right)} + \sqrt{2^{R_s} - 1} \right)^2 \right) . \quad (14)$$

This is achieved with the following choice of system parameters:

$$\Phi^* = \frac{\sqrt{2^{R_s} - 1}}{\sqrt{2^{R_s}\lambda\left(\epsilon, N\right)} + \sqrt{2^{R_s} - 1}} , \quad (15)$$

$$R_b^* = R_s + \log_2\left(\sqrt{\left(1 - 2^{-R_s}\right)\lambda\left(\epsilon, N\right)} + 1 \right) , \quad (16)$$

$$\mu^* = \frac{2^{R_b^*} - 1}{P\Phi^*} .$$

From (15) and (16), several observations can be made:
- R_b^* and Φ^* are independent of P. This is explained by noting that with the zero-noise assumption of Eve, the secrecy outage probability depends only on R_b and Φ. Therefore, for a given Φ, whether the secrecy constraint can be satisfied depends only on R_b. Since the latter optimization w.r.t. Φ also does not involve P, the independence is then observed.
- Φ^* increases with N (since $\lambda\left(\epsilon, N\right)$ decreases with N, as shown in Appendix B), approaching the constant:

$$\lim_{N \to \infty} \Phi^* = \frac{1}{1 + \sqrt{\ln\left(\frac{1}{\epsilon}\right) / \left(1 - 2^{-R_s}\right)}} .$$

This result follows the intuition that when more transmit antennas are installed, a smaller fraction of power can be used for generating artificial noise while still ensuring the required security level.
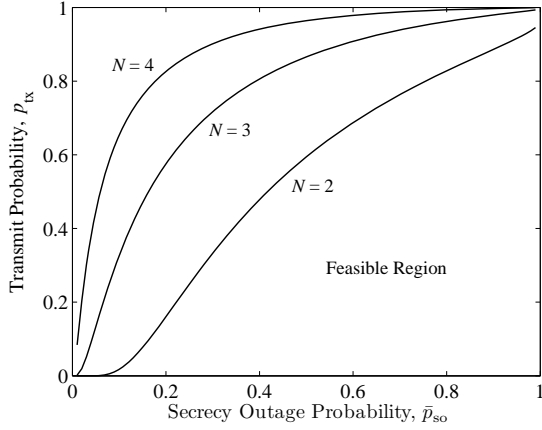
Fig. 1. Optimal tradeoff between the secrecy and delay performance of the NAE scheme for different numbers of transmit antennas, with $P = 10$ dB and $R_s = 2$ bits/channel use.
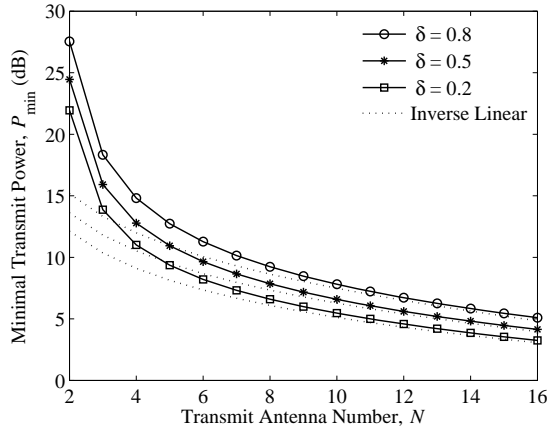

Fig. 2. Minimal power consumption of the NAE scheme under joint secrecy and delay constraint versus the number of transmit antennas for different delay constraints, with $\epsilon = 0.01$ and $R_s = 2$ bits/channel use.

The points above focus on the optimal system parameters. Some useful insights regarding the system performance and design implications may also be concluded:

- For a given transmission system (i.e., given N and P) and a prescribed message rate R_s, the optimal tradeoff curve between the secrecy and delay performance is completely specified by (14). This is observed by noting that p_{tx}^{max} is achieved when $\bar{p}_{so} = \epsilon$, while varying ϵ effectively traces the optimal tradeoff. In [23], we considered the minimization of the overall secrecy outage probability under an average delay constraint (i.e., $\min \bar{p}_{so}$ s.t. $p_{tx} \geq \delta$), which is the symmetric problem to (12). Since the tradeoff curve obtained in [23] coincides with (14), we conclude that each point on the optimal tradeoff curve is Pareto optimal [24]. As shown in Fig. 1, the area under each curve represents the feasible region of $(\bar{p}_{so}, p_{tx})$, points of which are achievable.
- If the system is designed to operate under a joint secrecy and delay constraint (i.e., $\bar{p}_{so} \leq \epsilon$ and $p_{tx} \geq \delta$), the minimum required transmit power P_{min} can be computed

by replacing p_{tx}^{max} in (14) with δ and solving the obtained equality w.r.t. P. This comes from the Pareto optimality indicated above and the fact that increasing P would effectively expand the feasible region. If extra antennas may be added, the decreasing rate of P_{min} is most significant for small N. For the special case $\delta = 0.5$, it can be proved that P_{min} decreases inverse linearly as N goes large, using [25, Eq. 6.2]. As shown in Fig. 2, this inverse linear behavior holds for a wide range of δ (here, the dotted lines are properly scaled inverse linear curves, shown for reference).

B. Throughput Optimization and Analysis

Having maximized p_{tx} for a given R_s, from (11) and (14), the optimal message rate that maximizes the throughput is given by

$$R_s^* = \arg\max_{R_s > 0} \eta_{NAE} = \arg\max_{R_s > 0} p_{tx}^{max}(R_s) \times R_s , \quad (17)$$

and the corresponding maximal throughput is given by

$$\eta_{NAE}^* = p_{tx}^{max}(R_s^*) \times R_s^* . \quad (18)$$
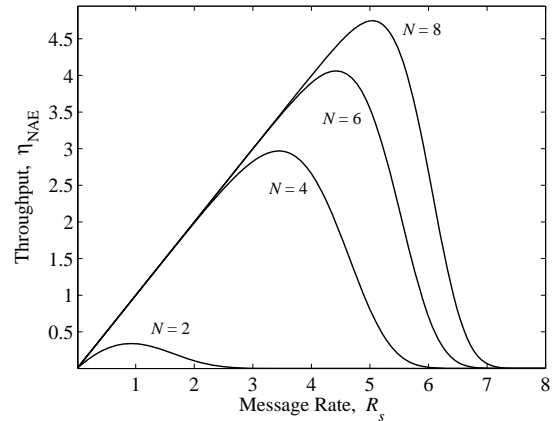

Fig. 3. Throughput of the NAE scheme versus the message rate for different numbers of transmit antennas, with $P = 20$ dB and $\epsilon = 0.01$.

From (14) and (17), it can be shown that if R_s is too small, even though p_{tx} may be high (i.e., close to one), the value of η_{NAE} is still very small; whereas, if R_s is too large, the value of p_{tx} and therefore η_{NAE} will also become very small. Moreover, by differentiating $\eta_{NAE} = p_{tx}^{max}(R_s) \times R_s$ w.r.t. R_s, one can verify that the derivative is first positive and then negative with increasing R_s; thus R_s^* is unique. As such, even if the objective function is non-concave, as shown in Fig. 3, we still can solve the derivative to find R_s^* numerically.

Though it seems difficult to find a general closed-form solution for (17), we can obtain an accurate approximation in the high SNR region. Specifically, as derived in Appendix C, when $P \to \infty$, we have

$$R_s^* \approx \frac{1}{N \ln(2)} \left(W_0 \left(\frac{\exp(1) N! P^N}{\left(\sqrt{\lambda(\epsilon, N)} + 1 \right)^{2N}} \right) - 1 \right) , \quad (19)$$

where $W_0\left(\cdot\right)$ is the principle branch of the Lambert-W function and $\lambda\left(\epsilon,N\right)$ is defined in (13).

From (19) and [26, Eq. 65], we know that R_s^* increases with P. Therefore, from (15) and (16), we can observe that for the throughput-maximizing scheme, as $P \to \infty$, the optimal power allocation ratio Φ^* and the added rate redundancy $R_e^* = R_b^* - R_s^*$ converge to

$$\lim_{P\to\infty} \Phi^* = \frac{1}{\sqrt{\lambda\left(\epsilon,N\right)+1}} \,, \tag{20}$$

$$\lim_{P\to\infty} R_e^* = \log_2\left(\sqrt{\lambda\left(\epsilon,N\right)}+1\right) \,. \tag{21}$$

Furthermore, based on (19), a high SNR throughput approximation for the NAE scheme is derived in Appendix D, and is given as follows:

$$\eta_{\mathrm{NAE}}^*\left(\epsilon\right) \approx \eta_{\mathrm{NAE}}^{\epsilon=1} - \eta_{\mathrm{NAE}}^{\mathrm{loss}}\left(\epsilon\right) \,, \tag{22}$$

where

$$\eta_{\mathrm{NAE}}^{\epsilon=1} = \log_2(P) - \frac{1}{N}\log_2(\ln(P)) + \frac{1}{N}\log_2((N-1)!), \tag{23}$$

$$\eta_{\mathrm{NAE}}^{\mathrm{loss}}(\epsilon) = 2\log_2\left(\sqrt{\lambda(\epsilon,N)}+1\right). \tag{24}$$

Here $\eta_{\mathrm{NAE}}^{\epsilon=1}$ is the high SNR throughput approximation for the NAE scheme when the system is operating without any secrecy constraint (i.e., $\epsilon = 1$), while $\eta_{\mathrm{NAE}}^{\mathrm{loss}}\left(\epsilon\right)$ reflects the throughput loss for realizing secure transmission. Interestingly, the throughput loss in (24) is independent of P and this is a direct consequence of the zero-noise assumption of Eve.

From (22)-(24), several observations can be made:

- The benefits of adding extra transmit antennas are two-fold: i) the system is more capable of achieving a larger throughput, ii) the throughput loss for securing the transmission will be reduced. However, the benefits in terms of reducing $\eta_{\mathrm{NAE}}^{\mathrm{loss}}\left(\epsilon\right)$ by adding extra antennas are limited, i.e.,

$$\lim_{N\to\infty} \eta_{\mathrm{NAE}}^{\mathrm{loss}}\left(\epsilon\right) = 2\log_2\left(\sqrt{\ln\left(\frac{1}{\epsilon}\right)}+1\right) \,,$$

  which depends only on ϵ, as we may expect.

- Even in the high SNR region, the second term in (23) is usually insignificant due to the double logarithm. Therefore, to achieve a specified target throughput, the additional power cost for imposing or strengthening the secrecy constraint can be approximated as

$$\Delta_P^{\mathrm{NAE}}\left(\epsilon_1,\epsilon_2,N\right) \ (\mathrm{dB}) \tag{25}$$

$$\approx \begin{cases} 20\log_{10}\left(\sqrt{\lambda\left(\epsilon_2,N\right)}+1\right) & \text{if } \epsilon_2 \le \epsilon_1 = 1 \,, \\ \frac{10}{N-1}\log_{10}\left(\frac{\epsilon_1}{\epsilon_2}\right) & \text{if } \epsilon_2 \le \epsilon_1 \ll 1 \,, \end{cases}$$

  which is independent of the targeted throughput. It is clear that the power cost in both cases in (25) can be effectively reduced by adding extra transmit antennas.

In Fig. 4, we show that the throughput approximation in (22) is quite accurate by comparing with the exact maximal throughput, which is obtained by numerically optimizing (17). When the secrecy constraint is strengthened, in order to maintain a specified target throughput, for $N = 4$, the first
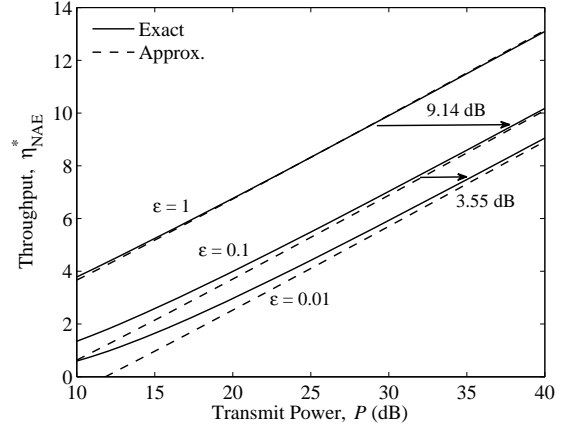

Fig. 4. Throughput of the NAE scheme and the high SNR approximation versus the transmit power for different secrecy constraints, with $N = 4$.

arrow shows that with $\epsilon_1 = 1$ and $\epsilon_2 = 0.1$, the additional power cost is 9.14 dB, while the second arrow suggests that with $\epsilon_1 = 0.1$ and $\epsilon_2 = 0.01$, the additional power cost is 3.55 dB. These two values are very close to the approximation provided in (25). Note that when N is very small (e.g., $N = 2$), the approximation in (22) becomes inaccurate due to the approximation procedure used in Appendix D and a better approximation can be obtained by plugging (19) into (18).

IV. SECURE TRANSMISSION DESIGN WITH ADAPTIVE ENCODER

In this section, we consider the scenario where Alice dynamically adjusts the system parameters: R_b, R_s and Φ for each realization of the channel to Bob $\mathbf{h}$. In other words, Alice performs adaptive encoding (AE). As before, the target is to maximize the throughput under the secrecy constraint given by a maximum allowable secrecy outage probability ϵ. In particular, the values of R_b, R_s and Φ are dynamically chosen to meet the requirement on the secrecy outage probability for each transmission, i.e., $p_{\mathrm{so}}\left(R_b\left(\mathbf{h}\right), R_s\left(\mathbf{h}\right), \Phi\left(\mathbf{h}\right)\right) \le \epsilon$. This design will in turn satisfy the requirement on the overall secrecy outage probability. With the secrecy constraint satisfied, the problem of maximizing the throughput is equivalent to maximizing $R_s\left(\mathbf{h}\right)$ for each $\mathbf{h}$. Intuitively, the AE scheme can achieve a larger throughput compared with the NAE scheme, but demands a higher complexity.

A. Message Rate Maximization

From (8), the problem of maximizing $R_s\left(\mathbf{h}\right)$ for each $\mathbf{h}$ is given by

$$\max_{R_b(\mathbf{h}),R_s(\mathbf{h}),\Phi(\mathbf{h})} R_s\left(\mathbf{h}\right)$$

$$\text{s.t. } p_{\mathrm{so}}\left(R_b\left(\mathbf{h}\right), R_s\left(\mathbf{h}\right), \Phi\left(\mathbf{h}\right)\right) \le \epsilon \,,$$

$$R_b\left(\mathbf{h}\right) \le \log_2\left(1 + P\Phi\left(\mathbf{h}\right)\|\mathbf{h}\|^2\right) \,,$$

$$0 \le R_s\left(\mathbf{h}\right) \le R_b\left(\mathbf{h}\right) \,,$$

$$0 \le \Phi\left(\mathbf{h}\right) \le 1 \,, \tag{26}$$

where the second constraint eliminates the capacity outages at the intended receiver.

The solution to (26) is presented as follows, whilst the derivation is relegated to Appendix E.

Proposition 2. With an adaptive encoder, for a given realization of the intended channel $\mathbf{h}$ and under the secrecy constraint $p_{so}\left(R_b\left(\mathbf{h}\right), R_s\left(\mathbf{h}\right), \Phi\left(\mathbf{h}\right)\right) \leq \epsilon$, the maximal message rate in (26) is given by:

$$R_s^{\max}\left(\mathbf{h}\right) \qquad (27)$$
$$= 2\log_2\left(\frac{\sqrt{P\lambda\left(\epsilon, N\right)\|\mathbf{h}\|^2} - \sqrt{P\|\mathbf{h}\|^2 - \lambda\left(\epsilon, N\right) + 1}}{\lambda\left(\epsilon, N\right) - 1}\right),$$

where $\lambda\left(\epsilon, N\right)$ is defined in (13). The corresponding optimal system parameters are given by:

$$\mu^* = \lambda\left(\epsilon, N\right)/P, \qquad (28)$$

$$\Phi^*\left(\mathbf{h}\right) = \frac{\sqrt{\lambda\left(\epsilon, N\right)\left(1 + \frac{1 - \lambda\left(\epsilon, N\right)}{P\|\mathbf{h}\|^2}\right)} - 1}{\lambda\left(\epsilon, N\right) - 1}, \qquad (29)$$

$$R_b^*\left(\mathbf{h}\right) = \log_2\left(1 + P\Phi^*\left(\mathbf{h}\right)\|\mathbf{h}\|^2\right). \qquad (30)$$

From (27)-(30), several observations can be made:

- Intuitively, we may expect that a positive message rate can always be achieved by properly adjusting the transmission system; thus, it may not be necessary to introduce the on-off transmission protocol. However, the derivation in Appendix E shows that after guaranteeing the secrecy performance, a positive $R_s\left(\mathbf{h}\right)$ can be achieved only when $\|\mathbf{h}\|^2 > \lambda\left(\epsilon, N\right)/P$. In other words, when Bob's channel is not sufficiently good, a positive $R_s\left(\mathbf{h}\right)$ and the required secrecy performance cannot be achieved simultaneously, no matter how Alice adjusts the power allocation or encoding. Therefore, to maximize the throughput whilst guaranteeing the required secrecy level, on-off transmission with $\mu = \lambda\left(\epsilon, N\right)/P$ is introduced, as stated in (28).
- The optimal power allocation ratio $\Phi^*\left(\mathbf{h}\right)$ in (29) decreases with increasing P, approaching the constant:

$$\lim_{P\to\infty}\Phi^*\left(\mathbf{h}\right) = \frac{1}{\sqrt{\lambda\left(\epsilon, N\right)} + 1}, \qquad (31)$$

which is independent of $\mathbf{h}$ and is identical to that for the NAE scheme in (20). This convergence suggests that in the high SNR region, near optimal performance can be obtained by employing a non-adaptive power allocation strategy.
- With optimized power allocation, $R_b\left(\mathbf{h}\right)$ is set to the instantaneous capacity of Bob's channel to guarantee successful decoding, as shown in (30). From (27) and (30), we can observe that as $P \to \infty$, the added rate redundancy $R_e\left(\mathbf{h}\right) = R_b\left(\mathbf{h}\right) - R_s\left(\mathbf{h}\right)$ converges to

$$\lim_{P\to\infty}R_e\left(\mathbf{h}\right) = \log_2\left(\sqrt{\lambda\left(\epsilon, N\right)} + 1\right), \qquad (32)$$

which is independent of $\mathbf{h}$ and is identical to that for the NAE scheme in (21).
- Furthermore, as shown in Appendix E, $R_s^{\max}\left(\mathbf{h}\right)$ in (27) is always achieved when $p_{so}\left(R_b\left(\mathbf{h}\right), R_s\left(\mathbf{h}\right), \Phi\left(\mathbf{h}\right)\right) = \epsilon$ and this implies that the overall secrecy outage probability in (9) is also guaranteed to be $\bar{p}_{so} = \epsilon$.
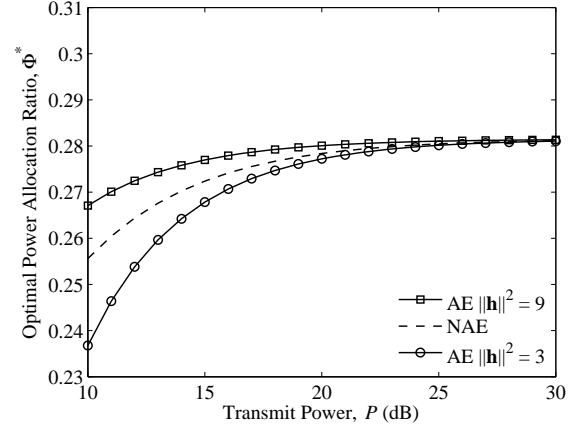

Fig. 5. Optimal power allocation ratios of the NAE and AE schemes versus the transmit power, with $N = 8$ and $\epsilon = 0.01$.

Fig. 5 illustrates our analysis, showing $\Phi^*\left(\mathbf{h}\right)$ for the AE scheme for different $\mathbf{h}$. The value of Φ^* for the NAE scheme is also shown for comparison and it is found by numerically optimizing R_s in (17), followed by plugging it into (15). As we may expect, the optimal power allocation ratios all converge to the same limit with increasing P. This observation is similar to the one in [10] where the channel gain was found to be irrelevant in finding the optimal power allocation in the high SNR region for maximizing the ergodic secrecy rate in fast fading channels. However, besides the similarity, the difference is also significant. In the high SNR region, the optimal power allocation ratio that maximizes the ergodic secrecy rate for fast fading channels [10] is around 0.5, while the limiting value of $\Phi^*\left(\mathbf{h}\right)$ in (31) that maximizes the throughput for slow fading channels depends strongly on the required security level ϵ and the number of transmit antennas N.

B. Throughput Performance Analysis

By (7) and (27), the throughput for the optimized AE scheme is given by

$$\eta_{AE}^* = \mathbb{E}_\mathbf{h}\left[R_s^{\max}\left(\mathbf{h}\right)\right]. \qquad (33)$$

Though it seems difficult to find a closed-form expression, similar to the NAE case, progress can be made by appealing to the high SNR region. Specifically, as $P \to \infty$, the following approximation is derived in Appendix F:

$$\eta_{AE}^* \approx \log_2\left(\frac{P}{\lambda\left(\epsilon, N\right)}\right) + \frac{\psi(N)}{\ln(2)} \qquad (34)$$
$$+ 2\log_2\left(\frac{\sqrt{\lambda\left(\epsilon, N\right)}}{\sqrt{\lambda\left(\epsilon, N\right)} + 1}\right)\tilde{\Gamma}\left(N, \frac{\lambda\left(\epsilon, N\right)}{P}\right)$$
$$+ \frac{\left(\lambda\left(\epsilon, N\right)/P\right)^N}{N^2(N-1)!\ln(2)}{}_2F_2\left(N, N; N+1, N+1; -\frac{\lambda\left(\epsilon, N\right)}{P}\right),$$

where $\lambda\left(\epsilon, N\right)$ is defined in (13), $\psi\left(N\right)$ is the digamma function, and ${}_2F_2\left(\cdot, \cdot; \cdot, \cdot; \cdot\right)$ is the generalized hypergeometric function [27, Eq. 9.14.1].

To gain more insights, as shown in Appendix F, when $P \to \infty$, (34) is further approximated as

$$\eta_{\text{AE}}^* (\epsilon) \approx \eta_{\text{AE}}^{\epsilon=1} - \eta_{\text{AE}}^{\text{loss}} (\epsilon) , \qquad (35)$$

where

$$\eta_{\text{AE}}^{\epsilon=1} = \log_2 (P) + \frac{\psi (N)}{\ln(2)} , \qquad (36)$$

$$\eta_{\text{AE}}^{\text{loss}} (\epsilon) = 2 \log_2 \left(\sqrt{\lambda (\epsilon, N)} + 1 \right) . \qquad (37)$$

Here $\eta_{\text{AE}}^{\epsilon=1}$ is the high SNR throughput approximation for the AE scheme without any secrecy constraint, which coincides with the high SNR approximation of the ergodic capacity of the MISO Rayleigh fading channel [28], while $\eta_{\text{AE}}^{\text{loss}} (\epsilon)$ reflects the throughput loss incurred by enforcing the secrecy constraint.

From (35)-(37), several observations can be made:

- In the high SNR region, the throughput loss for imposing the secrecy constraint in (37) is independent of P and it is identical to the throughput loss for the NAE scheme in (24). The throughput loss in (37) is actually twice the limiting value of the rate redundancy in (32). This can be explained by noting that in the high SNR region, the transmit threshold in (28) is close to zero and, in addition to the rate redundancy in (32), the transmission system also suffers a power loss since a certain fraction of power is used to generate artificial noise, as shown in (31). It is interesting that this power loss leads to a data rate loss which is identical with the rate redundancy in (32).

- In the high SNR region, to achieve a specified target throughput, the additional power cost for imposing or strengthening the secrecy constraint can be approximated from (35) and the results are identical to those for the NAE scheme in (25). However, although the NAE and AE schemes suffer the same power cost when imposing the same secrecy constraint, the AE scheme still outperforms the NAE scheme in terms of the throughput performance. This is due to the fact that when the secrecy constraint is removed, the AE scheme is designed to achieve a better throughput performance, compared with the NAE scheme. Specifically, when $\epsilon = 1$, for both schemes, all the transmit power is allocated to the information-bearing signal and the data will be transmitted without wiretap coding. In this case, the NAE scheme still chooses a constant rate to transmit and the transmit threshold is set to the minimum required effective channel gain to support the selected rate; while the AE scheme always transmits at the instantaneous capacity of Bob's channel and the transmit threshold is therefore set to zero.

In Fig. 6, we show that the throughput approximation in (35) is quite accurate by comparing with the exact maximal throughput, which is obtained by numerically evaluating (33). The additional power cost analysis is confirmed by the examples therein. Note that when N is very small (e.g., $N = 2$), (35) becomes less accurate due to the approximation procedure used in Appendix F and (34) provides a better approximation.
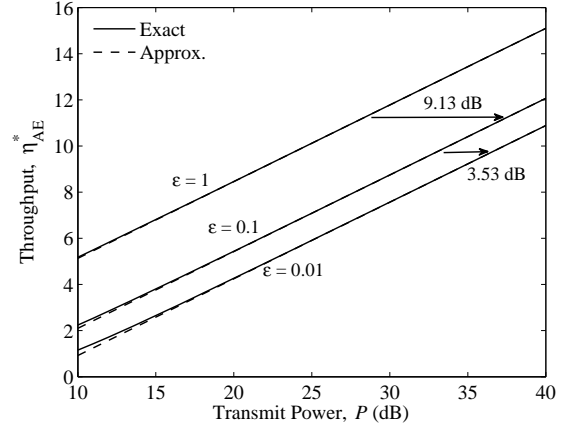

Fig. 6. Throughput of the AE scheme and the high SNR approximation versus the transmit power for different secrecy constraints, with $N = 4$.

C. Throughput Gain of Adaptation: AE over NAE

In the following, we analyze the throughput gain brought by doing adaptation. With the throughput approximations for the NAE and AE schemes in (22) and (35), in the high SNR region, the throughput gain can be approximated by

$$\eta_{\text{AE}}^* - \eta_{\text{NAE}}^* \qquad (38)$$
$$\approx \frac{1}{N} \log_2 (\ln (P)) + \left(\frac{\psi (N)}{\ln (2)} - \frac{1}{N} \log_2 ((N-1)!) \right) .$$

With this approximation, several observations can be made:

- In the high SNR region, the throughput gain increases with P, albeit very slowly, as can be seen from the double logarithm in the first term of (38).

- It turns out that as N increases, the second term in (38) (i.e., the P-independent term) increases slowly. The first term, on the other hand, decreases very fast with N (i.e., linearly), and moreover, this term becomes dominant when P is large. These observations imply that for high SNR, the throughput gap between the NAE and AE schemes shrinks when the number of antennas grows. Consequently, for systems operating at high SNRs, if the number of antennas is not small, it may be more preferable to employ the NAE scheme rather than the AE scheme, due to the complexity saving.

- The throughput gain approximation in (38) is independent of the secrecy constraint ϵ. This can be explained by noting that in the high SNR region, the NAE and AE schemes incur the same throughput loss for imposing the secrecy constraint, as shown in (22) and (35).

Fig. 7 compares the approximation in (38) with the exact throughput gain. It is clear that the exact throughput gain decreases with increasing N. Note that the variation in the throughput gain is not very significant over a wide range of ϵ, though the gain does decrease with strengthening the secrecy constraint (i.e., reducing ϵ). We note that the approximation is not very accurate, since the throughput gain is relatively small and thus the approximation error in (38) is relatively pronounced. What is important is that, as stated above, our
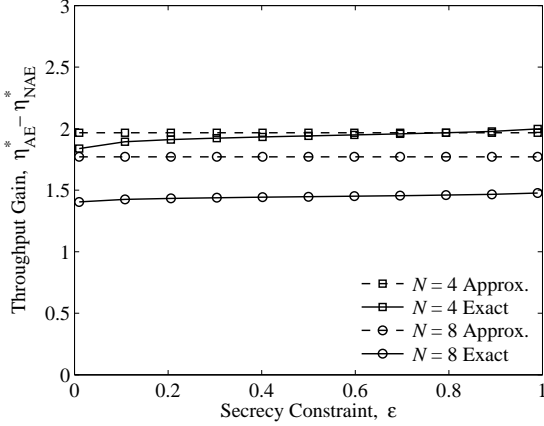
Fig. 7. Throughput gain of the AE scheme over the NAE scheme and the high SNR approximation versus the secrecy constraint for different number of transmit antennas, with $P = 40$ dB.

analysis accurately predicts the varying trends of the exact throughput gain.

V. CONCLUSION

This paper investigated the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels. We provided explicit design solutions to the secrecy-constrained throughput-maximization problem with either non-adaptive transmission (i.e., the NAE scheme) or adaptive transmission (i.e., the AE scheme). To facilitate practical system design, we examined the additional power cost for achieving a higher secrecy level for both schemes and analyzed the throughput gain of the AE scheme over the NAE scheme in the high SNR region. Our analysis obtained new insights on the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels.

APPENDIX

A. Proposition 1

In this proof, we derive the optimal values of the system parameters R_b, μ and Φ to maximize the transmit probability p_{tx} in (12) (i.e., minimize the average delay). We first optimize R_b and μ for a given Φ, and then optimize Φ. The message rate R_s is assumed to be at a prescribed value.

As we discussed at the beginning of Section III, for the NAE scheme, the overall secrecy outage probability in (9) reduces to (8). For a given Φ, from (8), it is clear that the secrecy constraint in (12) can be satisfied by choosing a large enough R_b. Substituting (8) into the secrecy constraint in (12) (i.e., $\bar{p}_{\mathrm{so}}(R_b, \Phi) \leq \epsilon$) and solving w.r.t. R_b, we have

$$R_b \geq R_s + \log_2\left(1 + \frac{\lambda\Phi}{1 - \Phi}\right) =: R_b^{\min},$$

where λ is defined in (13) and its parameters are omitted for brevity.

To minimize the average delay, the transmit probability p_{tx} in (6) needs to be maximized. From (6), it is clear that p_{tx} is maximized when the transmit threshold μ is set to its smallest

possible value. From the second constraint in (12), which eliminates capacity outages at Bob, we know that for a given Φ, μ should be set to

$$\mu_{\min} := \frac{1}{P\Phi}\left(2^{R_b^{\min}} - 1\right),$$

in order to maximize the transmit probability, whilst satisfying the secrecy constraint.

Substituting $\mu_{\min}$ into (6), the corresponding p_{tx} is given by

$$p_{\mathrm{tx}}(\Phi) = \tilde{\Gamma}(N, \omega(\Phi)), \qquad (39)$$

where

$$\omega(\Phi) = \frac{\rho}{1 - \Phi} + \frac{\varrho}{\Phi}, \quad \rho = \frac{2^{R_s}\lambda}{P}, \quad \varrho = \frac{2^{R_s} - 1}{P}. \qquad (40)$$

Since the regularized upper incomplete gamma function decreases with its second parameter, it is clear that $p_{\mathrm{tx}}(\Phi)$ in (39) achieves its maximum when $\omega(\Phi)$ takes its minimum. Note that $\omega(\Phi)$ is a convex function of Φ; thus, by solving the derivative of $\omega(\Phi)$ w.r.t. Φ, the optimal power allocation ratio can be found as

$$\Phi^* = \frac{\sqrt{\varrho}}{\sqrt{\rho} + \sqrt{\varrho}},$$

and the corresponding maximal transmit probability $p_{\mathrm{tx}}^{\max}$ is given by

$$p_{\mathrm{tx}}^{\max} := p_{\mathrm{tx}}(\Phi^*) = \tilde{\Gamma}\left(N, (\sqrt{\rho} + \sqrt{\varrho})^2\right).$$

Summarizing the obtained results, we have Proposition 1.

B. Monotonicity of Quantity in (13)

In this proof, we show that λ in (13) decreases with increasing N. To this end, we temporarily assume that N is a continuous variable. Taking the derivative of λ w.r.t. N, we have

$$\frac{\mathrm{d}\lambda}{\mathrm{d}N} = \epsilon^{\frac{1}{1-N}}\left(1 + \frac{\ln(\epsilon)}{N - 1}\right) - 1. \qquad (41)$$

To show that the above derivative is negative, we need to show that the expression in the bracket is smaller than $\epsilon^{\frac{1}{N-1}}$. Since the secrecy constraint ϵ is smaller than one, we know that $\frac{\ln(\epsilon)}{N-1} < 0$. From the inequality $1 + x < e^x$ for $x < 0$, letting $x = \frac{\ln(\epsilon)}{N-1}$, we see that the quantity in the bracket in (41) satisfies

$$1 + \frac{\ln(\epsilon)}{N - 1} < \exp\left(\frac{\ln(\epsilon)}{N - 1}\right) = \epsilon^{\frac{1}{N-1}}.$$

Thus, we know that the derivative in (41) is negative. Since the discrete N is just a sampled version of the continuous N, the monotonic properties are the same. We then know that λ in (13) decreases with increasing N.

C. Approximation of Optimal Message Rate in (19)

In this proof, we derive an approximation for the optimal message rate R_s^* in (17). From the discussions after (18), we know that one can solve the derivative of the throughput η_{NAE} w.r.t. R_s to find R_s^*. However, the equality obtained by setting the derivative to zero is quite complicated and seems not solvable. Hence, we consider first approximating the throughput and then optimizing the approximated throughput. The details can be found as follows.

Using the inequality $2^{R_s} > 2^{R_s} - 1$, a lower bound to η_{NAE} can be given by

$$\eta_{\text{NAE}} \geq \log_2(x) \times \tilde{\Gamma}(N, \varsigma x) =: \eta_{\text{NAE}}^{\text{LB}}, \qquad (42)$$

where $x = 2^{R_s}$, $\varsigma = \frac{1}{P}\left(\sqrt{\lambda} + 1\right)^2$ and λ is defined in (13).

As $P \to \infty$, it is clear that $\varsigma \to 0$. Using the series representation of the regularized upper incomplete gamma function [27, Eq. 8.352.4.*], we expand $\eta_{\text{NAE}}^{\text{LB}}$ in (42) as

$$\eta_{\text{NAE}}^{\text{LB}} = \log_2(x) \, e^{-\varsigma x} \sum_{k=0}^{N-1} \frac{(\varsigma x)^k}{k!}$$

$$= \log_2(x) \, e^{-\varsigma x} \left(e^{\varsigma x} - \sum_{k=N}^{\infty} \frac{(\varsigma x)^k}{k!} \right)$$

$$= \log_2(x) \left(1 - \sum_{l=0}^{\infty} \frac{(-\varsigma x)^l}{l!} \sum_{k=N}^{\infty} \frac{(\varsigma x)^k}{k!} \right) \qquad (43)$$

$$= \log_2(x) \left(1 - \frac{(\varsigma x)^N}{N!} + \mathcal{O}\left(\varsigma^{N+1}\right) \right), \qquad (44)$$

where in (43) we used the standard series expansion of the exponential function.

Ignoring the high order terms in the above series representation and taking the derivative w.r.t. x, we have

$$\frac{d\tilde{\eta}_{\text{NAE}}^{\text{LB}}}{dx} = \frac{\varsigma^N}{x \ln(2) N!} \left(N! \varsigma^{-N} - x^N \left(1 + \ln\left(x^N\right)\right) \right).$$

We then set the above derivative to zero and solve the obtained equality w.r.t. x. After summarizing the obtained results, we have the approximation in (19).

D. High SNR Throughput Approximation in (22)

In (19), we have obtained an approximation for the optimal message rate R_s^* in (17). Plugging an approximation for (19) into a lower bound to the throughput in (44) and ignoring the high order terms, we can get an elegant approximation for the maximal throughput η_{NAE}^*. The details can be found as follows.

In [26, Eq. 65], a series expansion is provided for the principle branch of the Lambert-W function $W_0(\cdot)$, and it states that as $x \to \infty$,

$$W_0(x) = \ln\left(\frac{x}{\ln(x)}\right) + \mathcal{O}\left(\frac{\ln(\ln(x))}{\ln(x)}\right).$$

Thus, as $P \to \infty$, by ignoring the high order terms, (19) can be further approximated as

$$\tilde{R}_s^* = \frac{1}{N} \log_2 \left(\frac{\frac{N! P^N}{\left(\sqrt{\lambda}+1\right)^{2N}}}{\ln\left(\frac{\exp(1) N! P^N}{\left(\sqrt{\lambda}+1\right)^{2N}}\right)} \right),$$

where λ is defined in (13). Note that as $P \to \infty$, $\frac{2^{\tilde{R}_s^*}}{P} \to 0$. Substituting the above approximation into the throughput lower bound in (44), we have

$$\eta_{\text{NAE}}^* \approx \tilde{R}_s^* \left(1 - \mathcal{O}\left(\left(\frac{2^{\tilde{R}_s^*}}{P}\right)^N \right) \right).$$

Taking the leading order term yields

$$\eta_{\text{NAE}}^* \approx \log_2(P) - \frac{1}{N} \log_2(\ln(P)) + \frac{1}{N} \log_2(N!)$$
$$- \frac{1}{N} \log_2\left(N + \mathcal{O}\left(\frac{1}{\ln(P)}\right) \right) - 2 \log_2\left(\sqrt{\lambda}+1\right).$$

Here $\mathcal{O}\left(\frac{1}{\ln(P)}\right) = \frac{1}{\ln(P)} \left(1 + \ln(N!) - 2N \ln\left(\sqrt{\lambda}+1\right) \right)$, which can be ignored for high P, thereby giving (22).

E. Proposition 2

In this proof, we derive the optimal values of the system parameters R_b, R_s and Φ to maximize the message rate R_s in (26) for a given realization of the intended channel $\mathbf{h}$, whilst satisfying the secrecy constraint. (Note that for the AE scheme, the design parameters R_b, R_s and Φ are intrinsically functions of $\mathbf{h}$.) We first optimize R_b and R_s for a given Φ, and then optimize Φ.

For a given Φ, to eliminate capacity outages at Bob (i.e., the second constraint in (26)), Alice sets R_b to the capacity of Bob's channel:

$$R_b(\Phi) = C_b = \log_2\left(1 + P\Phi\|\mathbf{h}\|^2\right).$$

For a given Φ, if Alice decides to transmit with $R_b(\Phi)$ above, and with $R_s < R_b(\Phi)$, the secrecy outage probability for this transmission is given by (8) as

$$p_{\text{so}}(R_b(\Phi), R_s, \Phi) = \left(1 + \left(2^{R_b(\Phi) - R_s} - 1 \right) \left(\frac{\Phi^{-1} - 1}{N - 1} \right) \right)^{1-N},$$

which simply increases with increasing R_s. Thus, the maximal R_s will be obtained when the secrecy constraint in (26) is met with equality, i.e., $p_{\text{so}}(R_b(\Phi), R_s, \Phi) = \epsilon$. Solving this equality gives

$$R_s(\Phi) = \log_2\left(\frac{1 + \tau\Phi}{1 + \frac{\lambda\Phi}{1-\Phi}} \right), \qquad (45)$$

which is a function of Φ, $\tau = P\|\mathbf{h}\|^2$ and λ is defined in (13).

From (45), we see that when $\tau \leq \lambda$ (equivalently, $\|\mathbf{h}\|^2 \leq \frac{\lambda}{P}$), it is impossible to adjust $\Phi \in (0,1)$ to achieve a positive R_s. For the alternative case, when $\tau > \lambda$ (i.e., $\|\mathbf{h}\|^2 > \frac{\lambda}{P}$), the range of Φ which can guarantee that $R_s(\Phi) > 0$ is $(0, 1 - \frac{\lambda}{\tau})$. Henceforth, we focus on the case where $\tau > \lambda$.

Since $R_s(\Phi)$ in (45) is non-concave on Φ and the logarithm function is monotonic, we then maximize an equivalent objective function $\frac{1+\tau\Phi}{1+\frac{\lambda\Phi}{1-\Phi}}$, which is concave on $\Phi \in (0,1)$ for $\tau > \lambda$. Solving the derivative of $\frac{1+\tau\Phi}{1+\frac{\lambda\Phi}{1-\Phi}}$ w.r.t. Φ leads to

$$\Phi^* = \frac{\sqrt{\tau\lambda(\tau-\lambda+1)}-\tau}{\tau\lambda-\tau},$$

while it is also confirmed that $0 < \Phi^* < 1 - \frac{\lambda}{\tau}$ when $\tau > \lambda$. Summarizing the obtained results, we have Proposition 2.

F. High SNR Throughput Approximation in (35)

Having optimized the message rate for each realization of the intended channel, the average throughput can be computed by averaging the maximum message rate in (27) over all channel realizations. Plugging (27) into (33), we have

$$\eta_{\mathrm{AE}}^* = 2\int_{\frac{\lambda}{P}}^{\infty} \log_2\left(\frac{\sqrt{P\lambda r}-\sqrt{Pr-(\lambda-1)}}{\lambda-1}\right)\mathrm{e}^{-r}\frac{r^{N-1}}{(N-1)!}\mathrm{d}r, \quad (46)$$

where λ is defined in (13) and the lower limits comes from the transmit threshold in (28).

It seems difficult to find a closed-form expression for the above integral; instead, we appeal to the high SNR region. The quantity $\lambda - 1$ is independent of P; thus, it is negligible compared with Pr when P is large. Therefore, by omitting the quantity $\lambda - 1$ under the second square root sign in (46), we have

$$\eta_{\mathrm{AE}}^* \approx 2\log_2\left(\frac{\sqrt{P}}{\sqrt{\lambda}+1}\right)\tilde{\Gamma}\left(N,\frac{\lambda}{P}\right) + \int_{\frac{\lambda}{P}}^{\infty}\log_2(r)\mathrm{e}^{-r}\frac{r^{N-1}}{(N-1)!}\mathrm{d}r$$

$$= 2\log_2\left(\frac{\sqrt{\lambda}}{\sqrt{\lambda}+1}\right)\tilde{\Gamma}\left(N,\frac{\lambda}{P}\right) + \frac{\lambda}{P}\frac{\mathrm{T}\left(3,N,\frac{\lambda}{P}\right)}{\ln(2)(N-1)!}, \quad (47)$$

where we used to the integral identities in [27, Eq. 4.358.1.6] and [29, Eq. 29], and $\mathrm{T}(3,N,x)$ is a special case for the Meijer G-function [27, Eq. 9.301] with parameters:

$$\mathrm{T}(3,N,x) = \mathrm{G}_{2,3}^{3,0}\left(x\,\middle|\,\begin{matrix}0,0\\-1,-1,N-1\end{matrix}\right).$$

By [29, Eq. 37 & 38], (47) can be equivalently expressed as

$$\eta_{\mathrm{AE}}^* \approx \log_2\left(\frac{P}{\lambda}\right) + 2\log_2\left(\frac{\sqrt{\lambda}}{\sqrt{\lambda}+1}\right)\tilde{\Gamma}\left(N,\frac{\lambda}{P}\right)$$

$$+ \frac{(\lambda/P)^N}{(N-1)!\ln(2)}\sum_{k=0}^{\infty}\frac{(-\lambda/P)^k}{k!\,(N+k)^2} + \frac{\psi(N)}{\ln(2)}.$$

We then note that $\frac{1}{(N+k)^2} = \frac{1}{N^2}\frac{(N)_k(N)_k}{(N+1)_k(N+1)_k}$, where $(N)_k = \frac{(N+k-1)!}{(N-1)!}$ for $k \geq 0$ is the Pochhammer symbol. Thus, the infinite summation can be expressed in terms of a hypergeometric function [27, Eq. 9.14.1] and we have the result in (34). By definition, with a large P, the regularized incomplete gamma function in the second term of the equation above is close to one while the third term is with order $\mathcal{O}(P^{-N})$; thus, we have the result in (35).

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Technol. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[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. 24, no. 3, pp. 339–348, May 1978.

[4] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. Ann. Conf. Inf. Scien. Syst.*, Baltimore, America, Mar. 2007, pp. 905–910.

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

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

[7] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

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

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[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, America, 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] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[18] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[19] 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.

[20] 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.

[21] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

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

[23] 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.

[24] S. P. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge Univ. Pr., 2004.

[25] N. M. Temme, "Asymptotic inversion of incomplete gamma functions," *Mathem. Comput.*, vol. 58, no. 198, pp. 755–764, Apr. 1992.

[26] R. M. Corless, D. J. Jeffrey, and D. E. Knuth, "A sequence of series for the Lambert W function," in *Proc. Int. Sympos. Symbolic Algebraic Comput.*, no. 8, Hawaii, America, 1997, pp. 197–204.

[27] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Academic Pr., 2007.

[28] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge Univ. Pr., 2005.

[29] K. O. Geddes, M. L. Glasser, R. A. Moore, and T. C. Scott, "Evaluation of classes of definite integrals involving elementary functions via differentiation of special functions," *Applic. Algebra Eng., Commun. Comput.*, vol. 1, no. 2, pp. 149–165, 1990.
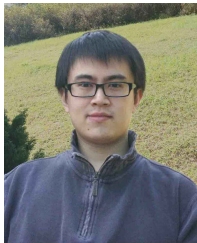
Xi Zhang (S'11) received the B.E. degree in School of Communication and Information Engineering from University of Electronic Science and Technology of China in 2010. He is currently a Ph.D. candidate at the Department of Electronic and Computer Engineering in Hong Kong University of Science and Technology. His research interests are in the fields of wireless communication and signal processing techniques, including physical-layer security, ad-hoc networking and random matrix theory.
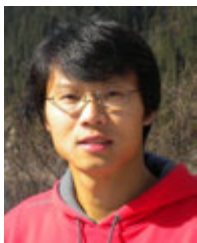
Xiangyun Zhou (S'08-M'11) is a lecturer at the Australian National University (ANU), Australia. He received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the ANU in 2007 and 2010, respectively. From June 2010 to June 2011, he worked as a postdoctoral fellow at UNIK - University Graduate Center, University of Oslo, Norway. His research interests are in the fields of communication theory and wireless networks. Dr. Zhou serves on the editorial board of Security and Communication Networks Journal (Wiley) and Ad Hoc & Sensor Wireless Networks Journal. He has also served as the TPC member of major IEEE conferences. He is a recipient of the Best Paper Award at the 2011 IEEE International Conference on Communications.

Matthew R. McKay (S'03-M'07) received the combined B.E. degree in Electrical Engineering and the B.IT. degree in Computer Science from the Queensland University of Technology, Australia, in 2002, and the Ph.D. degree in Electrical Engineering from the University of Sydney, Australia, in 2007. He then worked as a Research Scientist at the Commonwealth Science and Industrial Research Organization (CSIRO), Sydney, prior to joining the faculty at the Hong Kong University of Science and Technology (HKUST) in 2007, where he is currently the Hari Harilela Associate Professor of Electronic and Computer Engineering. He is also a member of the Center for Wireless Information Technology at HKUST, as well as an affiliated faculty member with the Division of Biomedical Engineering. His research interests include communications and signal processing; in particular the analysis and design of MIMO systems, random matrix theory, information theory, wireless ad-hoc and sensor networks, and physical-layer security.

Dr. McKay was awarded the University Medal upon graduating from the Queensland University of Technology. He and his coauthors have been awarded a Best Student Paper Award at IEEE ICASSP 2006, Best Student Paper Award at IEEE VTC 2006-Spring, Best Paper Award at ACM IWCMC 2010, Best Paper Award at IEEE Globecom 2010, Best Paper Award at IEEE ICC 2011, and was selected as a Finalist for the Best Student Paper Award at the Asilomar Conference on Signals, Systems, and Computers 2011. In addition, he received the 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. Dr. McKay serves on the editorial boards of the IEEE Transactions on Wireless Communications and the mathematics journal, Random Matrices: Theory and Applications. In 2011, he served as the Chair of the Hong Kong Chapter of the IEEE Information Theory Society, whilst previously serving as the Vice-Chair and the Secretary. He has also served on the technical program committee for numerous international conferences, as well as the Publications Chair for IEEE SPAWC 2009, Publicity Chair for IEEE SPAWC 2012, and Poster Chair for IEEE CTW 2013.