Artificial Noise Injection for Securing Single-Antenna Systems

Biao He, *Member, IEEE,* Yechao She, *Student Member, IEEE,* and Vincent K. N. Lau, *Fellow, IEEE*

***Abstract*—We propose a novel artificial noise (AN) injection scheme for wireless systems over quasi-static fading channels, in which a single-antenna transmitter sends confidential messages to a half-duplex receiver in the presence of an eavesdropper. Different from classical AN injection schemes, which rely on a multi-antenna transmitter or external helpers, our proposed scheme is applicable to the scenario where the legitimate transceivers are very simple. We analyze the performance of the proposed scheme and optimize the design of the transmission. Our results highlight that perfect secrecy is always achievable by properly designing the AN injection scheme.**

***Index Terms*—Physical layer security, artificial noise, secrecy outage probability.**

I. Introduction

The ubiquity of wireless devices in modern life has led to an unprecedented amount of private and sensitive data being transmitted over wireless channels. Consequently, security issues of wireless transmissions have become critical due to the unalterable open nature of the wireless medium. As a complement to traditional cryptographic techniques based on encryption, physical layer security (PLS) has been widely studied for ensuring secure wireless communications by exploiting the characteristics of wireless channels [1–3].

Secure transmission with artificial noise (AN) injection to confuse eavesdroppers is a key technique for PLS, and has been widely studied in the literature. The classical AN injection schemes were investigated in, e.g., [4–8]. For the scenario where the transmitter has multiple antennas, AN is designed to lie in the nullspace of the receiver's channel to degrade the eavesdropper's channel, while in the single-antenna scenario, external relays or helpers are adopted to collaboratively generate AN. In [9], an AN injection scheme was proposed for the scenario where the idealized full-duplex receiver is available. The receiver broadcasts AN and receives messages from the transmitter simultaneously. Although a multi-antenna transmitter and external helpers are not needed, however, the scheme in [9] requires the advanced full-duplex receiver with very good self-interference cancelation.

Different from the aforementioned scenarios for AN injection schemes, practical wireless systems often consist of simple legitimate transceivers. A basic system operation is that a single-antenna transmitter wants to send confidential messages to a half-duplex receiver without any helpers. The simplicity of the legitimate transmitter-receiver pair indeed makes it challenging to inject AN into such a single-antenna system. For transmission over multi-path fading channels, AN injection schemes for single-antenna systems were studied in [10–12] by exploiting the degrees of freedom from the cyclic prefix. However, these schemes rely on not only the multi-path diversity, but also the idealized assumption that keys or channel state information (CSI) can be secretly shared between the transmitter and the receiver. To the best of our knowledge, how to effectively inject AN into a basic single-antenna system (over flat fading channels) has still not been addressed in the literature.

In this paper, we propose a novel AN injection scheme for single-antenna systems with a half-duplex receiver and no helpers, which addresses the challenging problem of injecting AN in single-antenna systems. Our proposed scheme does not rely on multi-path diversity or the idealized assumption that keys or CSI are secretly shared. We highlight that perfect secrecy can always be achieved by properly designing the proposed scheme. Note that existing PLS techniques cannot ensure perfect secrecy of transmissions over quasi-static fading channels when the instantaneous CSI of eavesdroppers is unknown. Our results show that the proposed AN injection scheme significantly improves the performance of the single-antenna wiretap system.

Throughout the paper, we adopt the following notations: $\mathbb{E}\{\cdot\}$ denotes the expectation operation, $\mathbb{P}\{\cdot\}$ denotes the probability measure, $\mathcal{CN}\left(\mu,\sigma^2\right)$ denotes the circularly symmetric complex Gaussian distribution with mean μ and variance σ^2.

II. System Model

We consider a wiretap system over quasi-static Rayleigh fading channels. As illustrated in Figure 1, a transmitter, Alice, wants to send confidential messages to a half-duplex receiver, Bob, in the presence of an eavesdropper, Eve. Alice, Bob, and Eve each have a single antenna.[1] Note that the consideration of a single-antenna eavesdropper has been widely adopted in the literature, e.g., [10, 13–17].

A. Channel Model

We adopt a block fading model where the channel gains remain constant over a block of symbols and change independently from one block to the next. The instantaneous

This work was supported by Grant T21-602/15.

B. He is with the Center for Pervasive Communications and Computing, University of California at Irvine, Irvine, CA 92697. Email: biao.he@uci.edu. This work was completed when B. He was with Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong.

Y. She and V. K. N. Lau are with the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong. Emails:{yshe, eeknlau}@ust.hk.

Manuscript received xx; revised xx

[1] Although we focus on a single-antenna system in this paper, the proposed AN injection scheme is also applicable to multi-antenna systems where Alice, Bob, and/or Eve have multiple antennas.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2703159, IEEE Transactions on Vehicular Technology

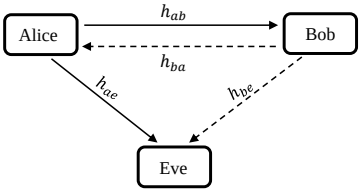


Fig. 1: A wiretap system.

channel gain from i to j ($i, j \in \{a, b, e\}$) is denoted as $h_{ij} \sim \mathcal{CN}\left(0, \mathbb{E}\left\{|h_{ij}|^2\right\}\right)$, where the subscripts a, b and e represent Alice, Bob, and Eve, respectively, and we denote the power gain of the channel from i to j as $g_{ij} = |h_{ij}|^2$. The probability density function (PDF) of g_{ij} is given by

$$f_{g_{ij}}(g_{ij}) = \frac{1}{\bar{g}_{ij}} \exp\left(-\frac{g_{ij}}{\bar{g}_{ij}}\right), \tag{1}$$

where $\bar{g}_{ij} = \mathbb{E}\{g_{ij}\}$ denotes the average power gain of the channel from i to j. We assume that the channel between the transmitter and the receiver is reciprocal, i.e., $h_{ij} = h_{ji}$, and h_{ab}, h_{ae}, and h_{be} are independent of each other. At the start of each block, Alice transmits pilot symbols to enable channel estimation at the receiver. We assume that Bob can perfectly estimate the channel to Alice, and hence, Bob knows the instantaneous CSI $h_{ab} = h_{ba}$. We further assume that the duration of a block is sufficiently long and the time spent on training is negligible.

B. Secure Encoding

We assume that Alice uses the widely adopted wiretap code for data transmissions. There are two rate parameters, namely, the codeword transmission rate, R_b, and the confidential information rate, R_s. The positive rate difference $R_b - R_s$ is the cost required to provide secrecy against the eavesdropper. A length n wiretap code is constructed by generating 2^{nR_b} codewords $x^n(w, v)$, where $w = 1, 2, \cdots, 2^{nR_s}$ and $v = 1, 2, \cdots, 2^{n(R_b - R_s)}$. For each message index w, we randomly select v from $\left\{1, 2, \cdots, 2^{n(R_b - R_s)}\right\}$ with uniform probability and transmit the codeword $x^n(w, v)$. In addition, we consider fixed-rate transmission, where the encoding rates R_b and R_s are fixed over time.

III. New Artificial Noise Injection Scheme

We propose a novel AN injection scheme to defend against eavesdropping attacks in single-antenna systems. The two-phase scheme is detailed as follows.

A. Phase 1

In the first phase, Bob broadcasts pseudo random AN. The received signal at Alice or Eve in Phase 1 is given by

$$y_{i,1} = \sqrt{P_b} h_{bi} z + n_i, \quad i \in \{a, e\}, \tag{2}$$

where the subscripts a and e denote the parameters for Alice and Eve, respectively, $z \sim \mathcal{CN}(0, 1)$ denotes the normalized complex Gaussian AN from Bob, P_b denotes the average transmit power at Bob, and $n_i \sim \mathcal{CN}(0, \sigma_i^2)$ denotes the additive white Gaussian noise (AWGN) at Alice or Eve.

During Phase 1, Bob does not send any pilot symbols for the channel estimation. Thus, Alice and Eve do not know the instantaneous CSI, i.e., h_{bi}, and cannot decode z.

B. Phase 2

In the second phase, Alice forwards the received signal $y_{a,1}$ from Phase 1 along with the information-bearing signal to Bob. We denote the normalized transmitted signal at Alice in Phase 2 as x_a with $\mathbb{E}\left\{|x_a|^2\right\} = 1$, which is given by

$$x_a = \sqrt{\alpha} s + \sqrt{1 - \alpha} \frac{y_{a,1}}{|y_{a,1}|}, \tag{3}$$

where s denotes the normalized information-bearing signal, with $\mathbb{E}\left\{|s|^2\right\} = 1$, and $0 < \alpha \leq 1$ denotes the power allocation parameter between the information-bearing signal and the AN. The received signal at Bob or Eve in Phase 2 is given by

$$y_{i,2} = \sqrt{P_a} h_{ai} x_a + n_i = \sqrt{\alpha P_a} h_{ai} s + \frac{\sqrt{(1-\alpha) P_a} h_{ai}}{\sqrt{P_b g_{ba} + \sigma_a^2}} \left(\sqrt{P_b} h_{ba} z + n_a\right) + n_i, \ i \in \{b, e\}, \tag{4}$$

where the subscripts b and e denote the parameters for Bob and Eve, respectively, P_a denotes the average transmit power at Alice, and $n_b \sim \mathcal{CN}(0, \sigma_b^2)$ denotes the AWGN at Bob. From (4), we note that Bob needs to know $P_a, P_b, \alpha, \sigma_a^2, h_{ab} = h_{ba}, g_{ba} = |h_{ba}|^2$, and z to cancel the received AN. As mentioned before, Bob knows the instantaneous CSI $h_{ab} = h_{ba}$ and $g_{ba} = |h_{ba}|^2$. He also knows z, which is generated by himself in Phase 1, and his average transmit power P_b. We further assume that Alice has publicly shared the (fixed) values of P_a, α, and σ_a^2 to Bob before the transmission. Thus, Bob can successfully cancel the received AN. Then, the received signal-to-noise ratios (SNRs) at Bob and Eve are, respectively, given by

$$\gamma_b = \frac{\alpha P_a g_{ab}}{\frac{(1-\alpha) P_a g_{ab}}{P_b g_{ba} + \sigma_a^2} \sigma_a^2 + \sigma_b^2} \tag{5}$$

$$\gamma_e = \frac{\alpha P_a g_{ae}}{(1-\alpha) P_a g_{ae} + \sigma_e^2}. \tag{6}$$

It is worth pointing out that (6) is based on the assumption that Eve has a single antenna. If Eve has multiple antennas, she can take advantage of the receiver diversity to improve the received SNR, while her received SNR is still degraded by the injected AN.

IV. Performance Analysis and Optimal Power Allocation

A. Performance Analysis

We first derive the PDFs of the received SNRs, and then characterize the security, reliability, and throughput performances of the system.

1) PDF of Received SNR:
We rewrite (5) and (6) as $\gamma_b = \Phi(g_{ab})$ and $\gamma_e = \Psi(g_{ae})$, respectively. We note that $\Phi(g_{ab})$ and $\Psi(g_{ae})$ are differentiable and monotonic for $g_{ab} > 0$ and $g_{ae} > 0$, respectively. Thus, $\gamma_b = \Phi(g_{ab})$ and $\gamma_e = \Psi(g_{ae})$ can be uniquely solved for g_{ab}

and g_{ae} to give $g_{ab} = \Phi^{-1}(\gamma_b)$ and $g_{ae} = \Psi^{-1}(\gamma_e)$, respectively. We then obtain the PDFs of γ_b and γ_e, respectively, as

$$\begin{aligned} f_{\gamma_b}(\gamma_b) &= f_{g_{ab}}\left(\Phi^{-1}(\gamma_b)\right)\frac{\partial\Phi^{-1}(\gamma_b)}{\partial\gamma_b} \\ &= \frac{1}{2\alpha\bar{g}_{ab}P_aP_b}\left(\frac{\omega_3}{\sqrt{\omega_1^2+4\alpha\omega_2\gamma_b}}+(1-\alpha)P_a\sigma_a^2+P_b\sigma_b^2\right) \\ &\quad\times\exp\left(-\frac{\omega_1+\sqrt{\omega_1^2+4\alpha\omega_2\gamma_b}}{2\alpha\bar{g}_{ab}P_aP_b}\right) \end{aligned} \tag{7}$$

$$\begin{aligned} f_{\gamma_e}(\gamma_e) &= f_{g_{ae}}\left(\Psi^{-1}(\gamma_e)\right)\frac{\partial\Phi^{-1}(\gamma_e)}{\partial\gamma_e} \\ &= \frac{\alpha\sigma_e^2}{P_a\bar{g}_{ae}\left(\alpha-(1-\alpha)\gamma_e\right)^2}\exp\left(-\frac{\gamma_e\sigma_e^2}{\bar{g}_{ae}\left(P_a\left(\alpha-(1-\alpha)\gamma_e\right)\right)}\right), \end{aligned} \tag{8}$$

where $\omega_1 = \left((1-\alpha)\gamma_b-\alpha\right)P_a\sigma_a^2 + P_b\gamma_b\sigma_b^2$, $\omega_2 = P_aP_b\sigma_a^2\sigma_b^2$, and $\omega_3 = \left(\alpha+2(1-\alpha)\gamma_b\right)\omega_2 + (1-\alpha)\left((1-\alpha)\gamma_b-\alpha\right)P_a\sigma_a^4 + P_b^2\gamma_b\sigma_b^4$.

2) Security, Reliability, and Throughput Performances: The security performance is measured by the secrecy outage probability, which is defined by [13]

$$p_{\text{so}} = \mathbb{P}\left(C_e > R_b - R_s\right), \tag{9}$$

where $C_e = \log_2(1+\gamma_e)$ denotes Eve's instantaneous channel capacity. From (8), we have

$$p_{\text{so}} = \begin{cases} 0, & \text{if } \alpha \le 1-2^{R_s-R_b}, \\ \exp\left(-\frac{(2^{R_b}-2^{R_s})\sigma_e^2}{(2^{R_s}+(\alpha-1)2^{R_b})\bar{g}_{ae}P_a}\right), & \text{otherwise.} \end{cases} \tag{10}$$

The reliability performance of the system is measured by the connection outage probability, which is defined by

$$p_{\text{co}} = \mathbb{P}\left(R_b > C_b\right), \tag{11}$$

where $C_b = \log_2(1+\gamma_b)$ denotes Bob's instantaneous channel capacity. From (7), we have

$$p_{\text{co}} = \mathbb{P}\left(\gamma_b < 2^{R_b}-1\right) = \int_0^{2^{R_b}-1} f_{\gamma_b}(\gamma_b)\,\mathrm{d}\gamma_b. \tag{12}$$

The closed-form expression for p_{co} is intractable due to the complicated expression for $f_{\gamma_b}(\gamma_b)$ in (7).

The throughput of the system is given by

$$\eta = \frac{1}{2}(1-p_{\text{co}})R_s = \frac{1}{2}\left(1-\int_0^{2^{R_b}-1} f_{\gamma_b}(\gamma_b)\,\mathrm{d}\gamma_b\right)R_s, \tag{13}$$

where the scalar factor $1/2$ is due to the fact that two time units are required in two phases.

Remark 1: From (10), we highlight that perfect secrecy, i.e., $p_{\text{so}} = 0$, can be achieved with the proposed AN injection scheme for any $R_b > R_s > 0$ by setting the power allocation parameter as

$$\alpha \le 1-2^{R_s-R_b}. \tag{14}$$

Note that existing PLS techniques cannot ensure perfect secrecy of transmissions over quasi-static fading channels; see, e.g., [4] and [13–15].

B. Optimal Power Allocation

In the following, we derive the optimal power allocation parameter that maximizes the throughput subject to the security and reliability constraints. We assume that the encoding rates have already been designed. The problem is formulated as

$$\max_{\alpha} \quad \eta(\alpha) \tag{15a}$$

$$\text{s.t.} \quad p_{\text{so}} \le \epsilon, p_{\text{co}} \le \delta, 0 < \alpha \le 1, \tag{15b}$$

where $\epsilon \in [0,1]$ and $\delta \in [0,1]$ denote the maximum allowed secrecy outage probability and the maximum allowed connection outage probability, respectively. We note that η monotonically increases as α decreases. Thus, the optimal power allocation parameter is obtained by finding the maximum α that satisfies all the constraints in (15b), which is given by

$$\alpha^o = \min\left\{\left(1-2^{R_s-R_b}\right)\left(1-\frac{\sigma_e^2}{P_a\bar{g}_{ae}\ln\epsilon}\right), 1\right\}. \tag{16}$$

V. Joint Rate and Power Allocation Design in Asymptotic Scenario

In this section, we allow more degrees of freedom, such that R_b and R_s can be optimally chosen, and investigate the joint rate and power allocation design.

A. Problem Formulation

The design problem is formulated as

$$\max_{\alpha,R_b,R_s} \quad \eta(\alpha,R_b,R_s) \tag{17a}$$

$$\text{s.t.} \quad p_{\text{so}} \le \epsilon, p_{\text{co}} \le \delta, R_b \ge R_s > 0, 0 < \alpha \le 1. \tag{17b}$$

For any given R_b and R_s, the optimal α is still given by (16). We find that the closed-form solutions of the optimal R_b and R_s are mathematically intractable due to the complicated expression for the PDF of the received SNR at Bob, i.e., (7). The optimal R_b and R_s for the design problem can be obtained only by numerically solving $\max_{R_b,R_s}\eta(\alpha=\alpha^o,R_b,R_s)$ subject to the constraints in (17b). In the following subsections, we study an asymptotic scenario where $\sigma_a^2 \to 0$, in which the closed-form solutions of R_b and R_s are tractable.

B. Asymptotic Analysis

We now resort to the asymptotic analysis of the scenario of $\sigma_a^2 \to 0$. This condition can be validated when Alice has a very sensitive receiver compared with Bob, such that $\sigma_a^2 \ll \sigma_b^2$. In such a scenario, the noise power at Bob is determined by σ_b^2 only, and the received SNR at Bob is rewritten as

$$\gamma_b = \alpha P_a g_{ab}/\sigma_b^2. \tag{18}$$

Then, the PDF of γ_b becomes

$$f_{\gamma_b}(\gamma_b) = \frac{\sigma_b^2}{\alpha P_a\bar{g}_{ab}}\exp\left(-\frac{\sigma_b^2\gamma_b}{\alpha P_a\bar{g}_{ab}}\right), \tag{19}$$

the connection outage probability becomes

$$p_{\text{co}} = \mathbb{P}\left(\gamma_b < 2^{R_b}-1\right) = 1-\exp\left(-\frac{\sigma_b^2\left(2^{R_b}-1\right)}{\alpha P_a\bar{g}_{ab}}\right), \tag{20}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2703159, IEEE Transactions on Vehicular Technology

and the throughput of the system becomes

$$\eta = \frac{1}{2}\left(1 - p_{\text{co}}\right) R_s = \frac{1}{2}\exp\left(-\frac{\sigma_b^2\left(2^{R_b}-1\right)}{\alpha P_a \bar{g}_{ab}}\right) R_s. \quad (21)$$

The expressions for γ_e, $f_{\gamma_e}(\gamma_e)$, and p_{so} are kept unchanged as (6), (8), and (10), respectively.

C. Feasible Constraint

We first determine the feasible constraints subject to which a non-zero throughput is achievable. The feasible range of ϵ and δ in the asymptotic scenario where $\sigma_a^2 \to 0$ is summarized in the following proposition.

Proposition 1: The feasible range of the security and reliability constraints is given by

$$\left\{(\epsilon, \delta) : 0 \le \epsilon \le 1, \delta_l(\epsilon) < \delta \le 1\right\}, \quad (22)$$

where

$$\delta_l(\epsilon) = 1 - \exp\left(-\frac{\sigma_b^2}{P_a \bar{g}_{ab}\left(1 - \frac{\sigma_e^2}{P_a \bar{g}_{ae} \ln \epsilon}\right)}\right). \quad (23)$$

Proof: See Appendix A. ■

D. Design Solution

The closed-form solutions of the optimal α, R_b, and R_s to the design problem in the asymptotic scenario where $\sigma_a^2 \to 0$ are summarized in the following proposition.

Proposition 2: The optimal α, R_b, and R_s that maximize the throughput subject to the security and reliability constraints are given by

$$\alpha^* = \left(1 - 2^{R_s^* - R_b^*}\right)\left(1 - \frac{\sigma_e^2}{P_a \bar{g}_{ae} \ln \epsilon}\right), \quad (24)$$

$$R_b^* = \min\left\{\log_2\left(\phi_1\right), \log_2\left(2^{\psi} + \sqrt{4^{\psi} - 2^{\psi}}\right)\right\}, \quad (25)$$

$$R_s^* = \min\left\{\log_2(\phi_2), \psi\right\}, \quad (26)$$

where

$$\phi_1 = \frac{\sigma_b^2 \bar{g}_{ae} \ln \epsilon + \bar{g}_{ab} \ln\left(1-\delta\right)\left(\sigma_e^2 - P_a \bar{g}_{ae} \ln \epsilon\right)}{2\sigma_b^2 \bar{g}_{ae} \ln \epsilon}, \quad (27)$$

$$\phi_2 = -\frac{\left(\sigma_b^2 \bar{g}_{ae} \ln \epsilon + \bar{g}_{ab} \ln\left(1-\delta\right)\left(\sigma_e^2 - P_a \bar{g}_{ae} \ln \epsilon\right)\right)^2}{4\sigma_b^2 \bar{g}_{ab} \bar{g}_{ae} \ln\left(1-\delta\right) \ln \epsilon \left(P_a \bar{g}_{ae} \ln \epsilon - \sigma_e^2\right)}, \quad (28)$$

and ψ is the solution of x to

$$\frac{\sqrt{4^x - 2^x}}{x 2^x \left(2^{x+1} + 2\sqrt{4^x - 2^x} - 1\right)} = \frac{\sigma_b^2 \bar{g}_{ae} \ln 2 \ln \epsilon}{\bar{g}_{ab}\left(P_a \bar{g}_{ae} \ln \epsilon - \sigma_e^2\right)}. \quad (29)$$

Proof: See Appendix B. ■

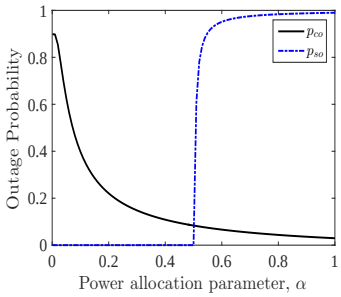
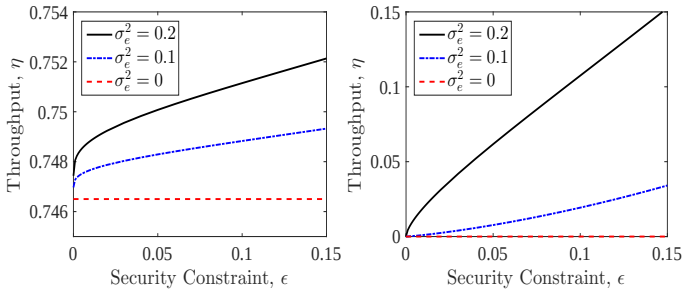


Fig. 2: The outage provability versus the power allocation parameter. The system parameters are $R_b = 2, R_s = 1$, $P_a = P_b = 10$ dB, $\bar{g}_{ab} = \bar{g}_{ae} = 1$, and $\sigma_a^2 = \sigma_b^2 = \sigma_e^2 = 0.1$.



(a) Proposed scheme. (b) Benchmark scheme.

Fig. 3: The throughput versus the security constraint. The system parameters are $P_a = P_b = 10$ dB, $\bar{g}_{ab} = \bar{g}_{ae} = 1, \sigma_a^2 = 0, \sigma_b^2 = 0.1, \sigma_e^2 = 0, 0.1, 0.2$, and $\delta = 0.1$.

VI. Numerical Results

We first show the reliability and security performances of the proposed AN injection scheme with different power allocations. Figure 2 plots the connection outage probability, p_{co}, and the secrecy outage probability, p_{so}, versus the power allocation parameter, α. The encoding rates are fixed at $R_b = 2$ and $R_s = 1$. As depicted in the figure, p_{co} decreases as α increases, while p_{so} increases as α increases. This observation indicates that there exists a tradeoff between the reliability and security performances. Allocating more power to the information-bearing signal and less power to the AN improves the reliability performance but worsens the security performance. Additionally, we find that $p_{\text{so}} = 0$ when $\alpha \le 0.5$ in the figure, which confirms that perfect secrecy is achievable by the proposed AN injection scheme with enough power allocated to the AN. Note that $p_{\text{so}} \simeq 1$ when $\alpha = 1$, which indicates that the system is very insecure without the proposed AN injection scheme.

We now compare the performances of our proposed AN injection scheme and a benchmark scheme. We adopt the secure on-off transmission scheme [13, 14], which is an existing secure transmission scheme for single-antenna systems, as the benchmark scheme. The comparison results are presented in Figure 3, which plots the throughput, η, versus the security constraint, ϵ. The performance achieved by the proposed AN injection scheme is shown in Figure 3(a), and the performance achieved by the benchmark scheme is shown in Figure 3(b). We note that our proposed scheme always significantly outperforms the benchmark scheme. In particular, the case of $\sigma_e^2 = 0$ represents the scenario where Eve has a very sensitive

receiver, which implies the worst-case consideration (from the legitimate users' point of view) when σ_e^2 is unknown, and the secrecy constraint of $\epsilon = 0$ indicates the requirement of perfect secrecy. We highlight that non-zero throughput is achievable by the proposed AN injection scheme even with the worst-case consideration $\sigma_e^2 = 0$ and the requirement of perfect secrecy $\epsilon = 0$. In contrast, non-zero throughput is not achievable by the existing benchmark scheme with either the worst-case consideration or the requirement of perfect secrecy.

VII. Conclusion and Future Work

In this paper, we have proposed a novel AN injection scheme which is applicable to a single-antenna system without any helpers. We have analyzed the scheme performance and optimized the power allocation. Furthermore, we have investigated the joint rate and power allocation design in the asymptotic scenario where $\sigma_a^2 \to 0$. Our results show that the proposed AN injection scheme effectively improves the performance of the system, and even perfect secrecy is achievable by allocating enough power to the AN. It is worth mentioning that the application of the proposed AN injection scheme is not limited to single-antenna systems, and an interesting future research direction is to evaluate the performance of the proposed scheme in multi-antenna systems.

Appendix A
Proof of Proposition 1

The feasible security constraint is $0 \leq \epsilon \leq 1$ without the consideration of the reliability constraint. The problem to find the minimum achievable p_{co} is formulated as

$$\min_{\alpha, R_b, R_s} \quad p_{\text{co}} \tag{30a}$$

$$\text{s.t.} \quad p_{\text{so}} \leq \epsilon, R_b > R_s > 0, 0 < \alpha \leq 1. \tag{30b}$$

From (20), we find that p_{co} is a decreasing function of α for any given R_b. Then, for any given R_b and R_s, it is wise to have the maximum α that satisfies $p_{\text{so}} \leq \epsilon$ and $0 < \alpha \leq 1$, which is given in (16). For R_b and R_s satisfying $\left(1 - 2^{R_s - R_b}\right)\left(1 - \sigma_e^2 / \left(\bar{g}_{ae} P_a \ln \epsilon\right)\right) \leq 1$, it is wise to choose

$$\alpha = (1 - 2^{R_s - R_b})(1 - \frac{\sigma_e^2}{\bar{g}_{ae} P_a \ln \epsilon}). \tag{31}$$

Substituting (31) into (20), we find that $p_{\text{co}}(R_b, R_s)$ is a convex function with respect to (w.r.t.) R_b for any given R_s, and it is wise to have

$$R_b = \log_2(2^{R_s} + \sqrt{4^{R_s} - 2^{R_s}}) \tag{32}$$

to minimize p_{co}. Substituting (31) and (32) into (20), we find that $p_{\text{co}}(R_s)$ is a decreasing function of R_s. We then find that the minimum achievable p_{co} for R_b and R_s that satisfy $\left(1 - 2^{R_s - R_b}\right)\left(1 - \sigma_e^2 / \left(\bar{g}_{ae} P_a \ln \epsilon\right)\right) \leq 1$ approaches (23) by calculating $\lim_{R_s \to 0} p_{\text{co}}(R_s)$. Following similar steps to those described above, we find that the minimum achievable p_{co} for R_b and R_s that satisfy $\left(1 - 2^{R_s - R_b}\right)\left(1 - \sigma_e^2 / \left(\bar{g}_{ae} P_a \ln \epsilon\right)\right) > 1$ is always larger than (23). Thus, the minimum achievable p_{co} approaches (23) for $R_b \geq R_s > 0$. This completes the proof.

Appendix B
Proof of Proposition 2

For any given R_b and R_s, the optimal α is given by (16). For R_b and R_s that satisfy $\left(1 - 2^{R_s - R_b}\right)\left(1 - \sigma_e^2 / \left(\bar{g}_{ae} P_a \ln \epsilon\right)\right) \leq 1$, it is wise to have α as (31). Substituting (31) into (21), we find that $\eta(R_b, R_s)$ is a concave function w.r.t. R_b for any given R_s, and it is wise to have R_b as (32) to maximize η. Then, substituting (31) and (32) into (21), we find that $\eta(R_s)$ is a concave function w.r.t. R_s for $R_s > 0$. With the consideration of $R_s \leq R_b$, we obtain the optimal R_s as (26) and the corresponding optimal R_b as (25). Following similar steps to those described above, we find that the maximum achievable η for R_b and R_s that satisfy $\left(1 - 2^{R_s - R_b}\right)\left(1 - \sigma_e^2 / \left(\bar{g}_{ae} P_a \ln \epsilon\right)\right) > 1$ is always smaller than the η achieved by having R_b and R_s as (25) and (26). Thus, the solutions of the optimal α, R_b, and R_s are given as (24), (25), and (26), respectively. This completes the proof.

References

[1] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[3] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

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

[5] 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.

[6] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[7] B. He, X. Zhou, and T. D. Abhayapala, "Achieving secrecy without knowing the number of eavesdropper antennas," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 7030–7043, Dec. 2015.

[8] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[9] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[10] H. Qin, Y. Sun, T. H. Chang, X. Chen, C. Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, June 2013.

[11] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085–3096, Apr. 2016.

[12] Y. Yang and B. Jiao, "Artificial-noise strategy for single-antenna systems over multi-path fading channels," in *IWCMC*, Aug. 2015, pp. 96–101.

[13] 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.

[14] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[15] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6913–6924, Oct. 2016.

[16] J. Hu, N. Yang, X. Zhou, W. Yang, and Y. Cai, "A versatile secure transmission strategy in the presence of outdated CSI," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10 084–10 090, Dec. 2016.

[17] J. Hu, Y. Cai, N. Yang, X. Zhou, and W. Yang, "Artificial-noise-aided secure transmission scheme with limited training and feedback overhead," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 193–205, Jan. 2017.