entropy

MDPI

Article

Novel Noise Injection Scheme to Guarantee Zero Secrecy Outage under Imperfect CSI

Hien Q. Ta [1,2,†], Lam Cao [1,2,†] and Hoon Oh [3,*,†]

[1] School of Electrical Engineering, International University, Ho Chi Minh City 700000, Vietnam; tqhien@hcmiu.edu.vn (H.Q.T.); lamct25@mp.hcmiu.edu.vn (L.C.)
[2] Vietnam National University, Linh Trung Ward, Thu Duc District, Ho Chi Minh City 700000, Vietnam
[3] Department of Electrical, Electronic and Computer Engineering, University of Ulsan, Ulsan 44610, Republic of Korea
* Correspondence: hoonoh@ulsan.ac.kr
† These authors contributed equally to this work.

Abstract: The paper proposes a novel artificial noise (AN) injection strategy in multiple-input single-output multiple-antenna-eavesdropper (MISOME) systems under imperfect channel estimation at the legitimate channel to achieve zero secrecy outage probability under any circumstance. The zero secrecy outage is proved to always be achievable regardless of the eavesdropper's number of antennas or location when the pair secrecy and codeword rates are chosen properly. The results show that when there is perfect channel state information, the zero-outage secrecy throughput increases with the transmit power, which is important for secrecy design. Additionally, an analysis of the secrecy throughput and secrecy energy efficiency gives further insight into the effectiveness of the proposed scheme.

Keywords: physical layer security; artificial noise; zero secrecy outage

check for updates

Citation: Ta, H.Q.; Cao, L.; Oh, H. Novel Noise Injection Scheme to Guarantee Zero Secrecy Outage under Imperfect CSI. *Entropy* **2023**, *25*, 1594. https://doi.org/10.3390/e25121594

Academic Editor: Mina Sheikhalishahi

Received: 18 October 2023
Revised: 21 November 2023
Accepted: 23 November 2023
Published: 28 November 2023

1. Introduction

Wireless communication has become an indispensable part of the modern world, enabling the connection and exchange of information between various devices and networks. As wireless communication continues to develop, the demand for more sophisticated security mechanisms grows, seeking to further protect sensitive data and ensure the privacy and integrity of communication. The demand for security in wireless communication arises from several factors. Firstly, wireless networks are by nature more vulnerable to security threats such as eavesdropping, interception, and unauthorized access compared to wired networks. This makes it essential to employ robust security mechanisms to safeguard transmitted data. Additionally, the continuous advancement and widespread adoption of wireless technologies have expanded the attack surface for potential threats. Traditionally, encryption techniques such as advanced encryption standard (AES) [1] and RSA [2] have been employed to encrypt data packets, making them unintelligible to unauthorized recipients. Encryption safeguards the confidentiality of transmitted data and prevents unauthorized tampering or modification during transmission. However, data encryption has certain disadvantages, such as requiring additional resources and associated setup and maintenance, increasing complexity, and reducing data processing speed.

In the past decades, physical layer security (PLS) has arisen as a propitious solution to improve the overall protection of wireless networks. The demand for PLS stems from the fact that cryptographic methods alone may not be sufficient to address all security challenges in wireless communications. PLS techniques take advantage of various physical properties, such as signal strength, fading effects, noise, and channel characteristics, to establish secure communication links. Wyner laid the foundation for physical layer security (PLS) through the study of the wiretap channel [3]. Building upon this concept, subsequent research focused on studying the secrecy in Gaussian wiretap channel and fading channel models. It was demonstrated in [4] that there exists a non-zero secrecy capacity even when channel conditions are more favorable for the eavesdropper.

More recently, novel approaches aimed at enhancing security have emerged. These include cooperative communication, as discussed in [5], and the introduction of artificial noise (AN) injection, as explored by [6]. Among these solutions, AN receivers have attracted significant attention, particularly in the context of comprehensive three-node systems, as shown in [7,8]. In [7], a secure half-duplex (HD) transmission scheme using AN injection is introduced. In this scheme, the receiver spends the first phase broadcasting AN, which is then processed and combined with the secret message at the transmitter during the later phase. In contrast, Ref. [8] investigates the use of a full-duplex (FD) jamming receiver, which simultaneously receives the desirable message and broadcasts AN to disrupt potential eavesdropping attempts. This approach is particularly effective when the eavesdropper and intended receiver are in close proximity, experiencing higher received AN power. The potential of FD receivers in physical layer security (PLS) has been further examined in subsequent studies, such as [9–11], showcasing improvements in secrecy outage probability at the cost of network connection reliability in hybrid FD/HD models with FD jamming receivers. Building on the concepts presented in [7,8], Ref. [12] proposed a secure FD transmission scheme, where the transmitter overlays the secret message with the AN coming from the receiver. Furthermore, additional research efforts have explored the use of FD relays broadcasting AN in decode-and-forward as well as amplify-and-forward relay systems, addressing scenarios with an unknown eavesdropper location [13,14]. Although PLS has been studied for years, it has limits in realistic applications, especially for a powerful eavesdropper which is located close to the transmitter or equipped with an infinite number of antennas. In fact, since the traditional AN is usually transmitted in the null space of the main channel, it will be easily canceled if the eavesdropper is powerful enough and has a large number of antennas [6]. As a result, there is no secrecy anymore, and a novel AN injection strategy is urgently required, in which the AN is transmitted in the same space as the main channel while still being canceled for legitimate receivers but not eavesdroppers by using the strategy of channel state information (CSI) leakage avoidance [15]. Furthermore, because security is required with probability 1 in some scenarios such as credit card number transmission, secrecy outage, or interception by an eavesdropper is required to be zero. As such, PLS or even other layers cannot support security in any circumstance when there is a powerful eavesdropper. Therefore, it is essential to revisit PLS for a novel design that can guarantee zero secrecy outage.

In this paper, we propose a secure transmission model using AN with a multi-antenna transmitter and an eavesdropper under imperfect channel estimation. The numerical results show an achievable zero secrecy outage probability by using a two-phase transmission protocol with channel inversion pre-coding at the transmitter. Furthermore, we also provide analysis for the secrecy throughput and in turn, the secrecy energy efficiency of the scheme.

The contributions of the paper are as follows:

- Different from conventional schemes, in which AN is transmitted in the null space of the secure signal, the proposed artificial noise injection scheme transmits AN in the same space as the secure signal and uses an extra time slot for only transmitting AN with aid reverse pilot training to achieve noise cancellation capability at legitimate receivers and not at an eavesdropper.
- Although the proposed strategy wastes one extra time slot, it reduces complexity at the transmitter, which requires one AN vector compared to an AN matrix as in the conventional strategy. This simple strategy can also be extended to apply to many other system networks to efficiently achieve zero secrecy outage.
- The closed-form formula of the secrecy rate subject to zero secrecy outage is determined. Then, the resulting zero-outage secrecy throughput can always be achieved regardless of how powerful the eavesdropper is, e.g., if it has an infinite number of antennas.

From here on, the paper is structured as follows: Section 2 introduces the system model of the proposed transmission scheme; Sections 3 and 4 show the formulation of secrecy and connection outage probability, respectively; Section 5 provides analysis for the secrecy throughput and secrecy energy efficiency of the system; finally, numerical results and discussion are given in Section 6.

2. System Model

As depicted in Figure 1, consider a three-node secure transmission model with a transmitter (Alice) sending confidential information to a legitimate receiver (Bob), while an eavesdropper (Eve) attempts to intercept the message. Alice, Bob, and Eve have N_A, 1, and N_E antennas, respectively. The fading channels are modeled as quasi-static Rayleigh with constant gain for each time slot that changes independently between different slots.

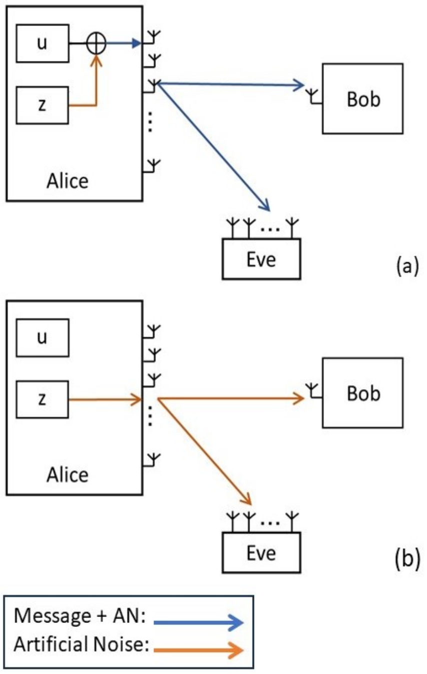

Figure 1. Two-phase transmission model: (**a**) Alice transmits noise-injected message in phase 1. (**b**) Alice transmits only AN in phase 2.

The proposed scheme is under two-phase transmission of a secret message plus artificial noise (AN) and only AN, in two different time slots. Considering the reverse training method, where Bob periodically transmits pilots for Alice to estimate the channel gain [16]. Assuming an imperfect minimum-mean-square-error (MMSE) receiver at Bob, the actual channel at Bob, denoted as $\mathbf{h}_i$ for $i \in \{1,2\}$ representing two phases of transmissions, is given by [17]

$$\mathbf{h}_i = \hat{\mathbf{h}}_i + \tilde{\mathbf{h}}_i \tag{1}$$

where $\hat{\mathbf{h}}_i \sim \mathcal{CN}(\mathbf{0}, (1-\beta)\sigma_h^2\mathbf{I}_{N_A \times N_A})$ is the estimated channel gain, and $\tilde{\mathbf{h}}_i \sim \mathcal{CN}(\mathbf{0}, \beta\sigma_h^2\mathbf{I}_{N_A \times N_A})$ is the error part with the estimation error coefficient denoted β. ($\mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}_{n\times n})$ denotes the independent and identical distributed (i.i.d) complex vector where each element has Gaussian distribution with zero-mean and variance σ^2, and $\mathbf{0}$ and $\mathbf{I}_{n\times m}$ denote the zero vector and identity matrix, respectively). We also assume that the background noise at each node has a zero-mean complex Gaussian distribution with variance σ_n^2.

The secure transmission has two phases:

2.1. Phase 1

In the first phase, Alice attempts to protect the confidential information by sending a secret message along with a superimposed AN. The secure message at Alice is transmitted with an allocated power fraction, denoted as α in the range $(0, 1)$, along with the AN as

$$\mathbf{x_1} = \frac{\hat{\mathbf{h}}_1^*}{||\hat{\mathbf{h}}_1||^2}(\sqrt{\alpha}u + \sqrt{1-\alpha}v), \tag{2}$$

where u and v denote the secret message and the AN signal, respectively, and are i.i.d zero-mean complex Gaussian with variance σ_u^2.

Due to error estimation, Bob receives

$$\begin{aligned} y_{b,1} &= \mathbf{h}_1^T \mathbf{x}_1 + n_{b,1} \\ &= (\sqrt{\alpha}u + \sqrt{1-\alpha}v) + \frac{\tilde{\mathbf{h}}_1^T \hat{\mathbf{h}}_1^*}{||\hat{\mathbf{h}}_1||^2}(\sqrt{\alpha}u + \sqrt{1-\alpha}v) + n_{b,1}, \end{aligned} \tag{3}$$

while assuming perfect CSI at Eve, it receives,

$$\begin{aligned} \mathbf{y}_{e,1} &= \mathbf{G}_1 \mathbf{x}_1 + \mathbf{n}_{e,1} \\ &= \frac{\mathbf{G}_1 \hat{\mathbf{h}}_1^*}{||\hat{\mathbf{h}}_1||^2}(\sqrt{\alpha}u + \sqrt{1-\alpha}v) + \mathbf{n}_{e,1}, \end{aligned} \tag{4}$$

respectively, where $\mathbf{G}_1$ denotes the channel gain at Eve in phase 1 with each element being i.i.d zero-mean complex Gaussian with variance σ_g^2. $n_{b,1}$ and $\mathbf{n}_{e,1}$ denote the background noise at Bob and Eve, respectively.

2.2. Phase 2

In phase 2, only artificial noise is transmitted as

$$\mathbf{x}_2 = \frac{\hat{\mathbf{h}}_2^*}{||\hat{\mathbf{h}}_2||^2}v, \tag{5}$$

which yields Bob's and Eve's received signals,

$$\begin{aligned} y_{b,2} &= \mathbf{h}_2^T \mathbf{x}_2 + n_{b,2} \\ &= v + \frac{\tilde{\mathbf{h}}_2^T \hat{\mathbf{h}}_2^*}{||\hat{\mathbf{h}}_2||^2}v + n_{b,2} \end{aligned} \tag{6}$$

and

$$\begin{aligned} \mathbf{y}_{e,2} &= \mathbf{G}_2 \mathbf{x}_2 + \mathbf{n}_{e,2} \\ &= \frac{\mathbf{G}_2 \hat{\mathbf{h}}_2^*}{||\hat{\mathbf{h}}_2||^2}v + \mathbf{n}_{e,2}, \end{aligned} \tag{7}$$

respectively, where $\mathbf{G}_2$ denotes the channel gain at Eve in phase 2, where each element is i.i.d complex Gaussian with zero-mean and variance σ_g^2. $n_{b,2}$ and $\mathbf{n}_{e,2}$ denote the background noise at Bob and Eve, respectively.

The *total transmit power* based on the channel inversion strategy can be computed from (2) and (5) as a function of $\hat{\mathbf{h}}_1$ and $\hat{\mathbf{h}}_2$ [18]:

$$\begin{aligned} P(\hat{\mathbf{h}}_1, \hat{\mathbf{h}}_2) &= E(||\mathbf{x}_1||^2) + E(||\mathbf{x}_2||^2) \\ &= \sigma_u^2(||\hat{\mathbf{h}}_1||^{-2} + ||\hat{\mathbf{h}}_2||^{-2}), \end{aligned} \tag{8}$$

which yields the average total transmit power, denoted P, of

$$\begin{aligned} P &= E_{\hat{\mathbf{h}}_1,\hat{\mathbf{h}}_2}\left[P(\hat{\mathbf{h}}_1,\hat{\mathbf{h}}_2)\right] \\ &= \frac{2\sigma_u^2}{(1-\beta)\sigma_h^2(N_A-1)}. \end{aligned} \tag{9}$$

Therefore, we obtain

$$\sigma_u^2 = (1-\beta)\sigma_h^2 P(N_A-1)/2. \tag{10}$$

3. Secrecy Outage Probability

From Eve's perspective, it is impossible to acquire $\mathbf{G}_2\hat{\mathbf{h}}_2^*/\|\hat{\mathbf{h}}_2\|^2$ phase shift in phase 2 based on the received signal in (7) as it is only noise. We see that when Eve does not experience any channel noise, the phase shift of $\mathbf{y}_{e,2}$ is determined by the phase difference between v and $\mathbf{G}_2\hat{\mathbf{h}}_2^*/\|\hat{\mathbf{h}}_2\|^2$. Since v is defined as a complex Gaussian AN vector independent of the channel phase, the signals $\mathbf{y}_{e,2}$ and $\mathbf{G}_2\hat{\mathbf{h}}_2^*/\|\hat{\mathbf{h}}_2\|^2$ are also independent. As we obtain the entropy equality,

$$H\Big(\mathbf{G}_2\hat{\mathbf{h}}_2^*/\|\hat{\mathbf{h}}_2\|^2\Big|\mathbf{y}_{e,2}) = H\Big(\mathbf{G}_2\hat{\mathbf{h}}_2^*/\|\hat{\mathbf{h}}_2\|^2\Big), \tag{11}$$

the received signal cannot give any information on the CSI, meaning that the eavesdropper can only process the secret message using (4). The SINR at Eve is given as

$$\gamma_e = \frac{\frac{|\mathbf{G}_1\hat{\mathbf{h}}_1^*|^2}{\|\hat{\mathbf{h}}_1\|^4}\alpha\sigma_u^2}{\frac{|\mathbf{G}_1\hat{\mathbf{h}}_1^*|^2}{\|\hat{\mathbf{h}}_1\|^4}(1-\alpha)\sigma_u^2+\sigma_n^2} \tag{12}$$

$$= \frac{\frac{\|\mathbf{g}\|^2}{\|\hat{\mathbf{h}}_1\|^2}\alpha\sigma_u^2}{\frac{\|\mathbf{g}\|^2}{\|\hat{\mathbf{h}}_1\|^2}(1-\alpha)\sigma_u^2+\sigma_n^2} \tag{13}$$

where $\mathbf{g} := \frac{\mathbf{G}_1\hat{\mathbf{h}}_1^*}{\|\hat{\mathbf{h}}_1\|} \sim \mathcal{CN}(0,\sigma_g^2\mathbf{I}_{N_e\times N_e})$. The capacity at Eve is given as

$$C_e = \frac{1}{2}\log_2(1+\gamma_e) \tag{14}$$

where the factor $1/2$ indicates that Eve only obtains information in the first phase.

Assume that Alice employs the wiretap code transmission scheme [3] to secure the information from Eve. The scheme uses codeword and secret rate parameters, R_b and R_s, with $R_b > R_s$. The positive difference between R_b and R_s is the cost of securing the confidential information. Since $\|\mathbf{g}\|^2 \sim \mathcal{X}_{2N_E}(0,\sigma_g^2/2)$ ($\mathcal{X}_{2N}(\sigma^2/2)$ denotes Chi-square distribution with $2N$ degrees of freedom and common variance $\sigma^2/2$), the secrecy outage probability for given transmissions is given by [19]

$$\begin{aligned} P_{so} &= Pr(C_e > R_b - R_s) \\ &= Pr\Big(\gamma_e > 2^{2(R_b-R_s)}-1\Big) \\ &= Pr\left(\|\mathbf{g}\|^2 > \frac{\|\hat{\mathbf{h}}_1\|^2(2^{2(R_b-R_s)}-1)\sigma_n^2/\sigma_u^2}{(\alpha-(1-\alpha)(2^{2(R_b-R_s)}-1))^+\sigma_u^2}\right) \\ &= \frac{\int_0^\infty x^{N_A-1}e^{-\frac{x}{(1-\beta)\sigma_h^2}}\Gamma(N_E,\Phi x)dx}{((1-\beta)\sigma_h^2)^{N_A}\Gamma(N_A)} \\ &= \frac{\Gamma(N_A+N_E)}{N_A\Gamma(N_A)}\frac{(\Phi(1-\beta)\sigma_h^2)^{N_E}}{(1+\Phi(1-\beta)\sigma_h^2)^{N_A+N_E}}{}_2F_1\left(1,N_A+N_E;N_A+1;\frac{1}{1+\Phi(1-\beta)\sigma_h^2}\right), \end{aligned} \tag{15}$$

where

$$\Phi = \frac{(2^{2(R_b-R_s)}-1)\sigma_n^2/(\sigma_u^2\sigma_g^2)}{(\alpha-(1-\alpha)(2^{2(R_b-R_s)}-1))^+}, \tag{16}$$

$(.)^+ \triangleq \max(0,.)$ and ${}_2F_1(\cdot)$ denotes the hypergeometric function [20].

Special case: When Eve has an unlimited number of antennas ($N_E \to \infty$) or is located close to Alice ($\sigma_g^2 \to \infty$), we obtain from (15) that the secrecy outage probability converges to

$$P_{so}(\hat{\mathbf{h}}_1) \to 1 \tag{17}$$

if $\alpha-(1-\alpha)(2^{2(R_b-R_s)}-1) > 0$, and, otherwise, is equal to 0 regardless of transmit power P and channel gain $||\hat{\mathbf{h}}_1||^2$. This indicates that the secrecy is guaranteed only if the pair of codeword rates (R_b, R_s) is designed such that $\alpha-(1-\alpha)(2^{2(R_b-R_s)}-1) \leq 0$, or, equivalently,

$$R_s \leq R_b - \frac{1}{2}\log_2\left(1+\frac{\alpha}{1-\alpha}\right), \tag{18}$$

which yields the zero secrecy outage probability regardless of Eve's number of antennas and location. It is also noted that the equality of (18) is called the zero-outage secrecy rate.

4. Connection Outage Probability

Since the AN is received in both phases, Bob can remove it by simply processing $y_{b,1}-\sqrt{1-\alpha}y_{b,2}$ to obtain

$$\begin{aligned} y_b &= y_{b,1}-\sqrt{1-\alpha}y_{b,2} \\ &= \sqrt{\alpha}u + \frac{\tilde{\mathbf{h}}_1^T\hat{\mathbf{h}}_1^*}{||\hat{\mathbf{h}}_1||^2}(\sqrt{\alpha}u+\sqrt{1-\alpha}v) - \frac{\tilde{\mathbf{h}}_2^T\hat{\mathbf{h}}_2^*}{||\hat{\mathbf{h}}_2||^2}\sqrt{1-\alpha}v + (n_{b,1}-\sqrt{1-\alpha}n_{b,2}). \end{aligned} \tag{19}$$

Then, the SINR at Bob, viewing the second and third terms of (19) as noise, can be obtained by [17]

$$\gamma_b = \frac{\alpha\sigma_u^2}{\left|\frac{\tilde{\mathbf{h}}_1^T\hat{\mathbf{h}}_1^*}{||\hat{\mathbf{h}}_1||}\right|^2\frac{\sigma_u^2}{||\hat{\mathbf{h}}_1||^2} + \left|\frac{\tilde{\mathbf{h}}_2^T\hat{\mathbf{h}}_2^*}{||\hat{\mathbf{h}}_2||}\right|^2\frac{(1-\alpha)\sigma_u^2}{||\hat{\mathbf{h}}_2||^2} + (2-\alpha)\sigma_n^2}, \tag{20}$$

and then, the capacity at Bob is given by

$$C_b = \frac{1}{2}\log_2(1+\gamma_b), \tag{21}$$

where the $1/2$ multiplier represents the two-phase operation. Under a fixed codeword rate R_b, an outage event happens when the channel capacity at Bob falls below the target rate R_b [18]. The probability of connection outage can be obtained from (20) and (21) as

$$\begin{aligned} P_{co} &= Pr(C_b < R_b) \\ &= Pr\left(\left|\frac{\tilde{\mathbf{h}}_1^T\hat{\mathbf{h}}_1^*}{||\hat{\mathbf{h}}_1||}\right|^2\frac{1}{||\hat{\mathbf{h}}_1||^2} > k - \left|\frac{\tilde{\mathbf{h}}_2^T\hat{\mathbf{h}}_2^*}{||\hat{\mathbf{h}}_2||}\right|^2\frac{(1-\alpha)}{||\hat{\mathbf{h}}_2||^2}\right) \end{aligned} \tag{22}$$

Since it follows from Appendix A that the cumulative density function (CDF) and probability density function (PDF) of $|\tilde{\mathbf{h}}_i^T\hat{\mathbf{h}}_i^*/||\hat{\mathbf{h}}_i||^2|^2$ is given by

$$\begin{aligned} F(x) &= 1 - \frac{1}{(1+x(1-\beta)/\beta)^{N_A}}, \\ f(x) &= \frac{N_A(1-\beta)/\beta}{(1+x(1-\beta)/\beta)^{N_A+1}}, \end{aligned} \tag{23}$$

we can obtain the connection outage probability as

$$P_{co} = 1 - \int_0^{k/(1-\alpha)} F(k - x(1-\alpha)) f(x) dx, \tag{24}$$

$$= \int_0^{\frac{k}{1-\alpha}} \frac{N_A(1-\beta)dx/\beta}{\left(1 + (k - x(1-\alpha))\frac{1-\beta}{\beta}\right)^{N_A+1}\left(1 + x\frac{1-\beta}{\beta}\right)^{N_A}} + \frac{1}{(1 + k(1-\beta)/((1-\alpha)\beta))^{N_A}}, \tag{25}$$

where

$$k = \frac{\alpha}{2^{2R_b} - 1} - \frac{(2-\alpha)\sigma_n^2}{\sigma_u^2}. \tag{26}$$

For $P_{co} \leq \delta$, where δ indicates the reliability constraint, it can be obtained from (25) that

$$R_b \leq R_b^*, \tag{27}$$

and R_b^* can be obtained by numerically searching for R_b, which results in $P_{co}(R_b) = \delta$. It should be noted that the exhaustive search is offline and the data value of R_b^* will be stored according to the system parameters. Therefore, it is not being computed online, which would yield latency in real wireless systems.

5. Zero-Outage Secrecy Throughput and Energy Efficiency

The zero-outage secrecy throughput, denoted by η, is defined as the amount of information securely received at Bob subject to zero secrecy outage and quality of service, which is

$$\begin{aligned} \eta = \max_{R_s} \quad & R_s \times (1-\delta) \\ \text{s.t.} \quad & P_{co} \leq \delta \\ & P_{so} \to 0. \end{aligned} \tag{28}$$

It follows from (18) and (27) that the zero-outage secrecy throughput can be found as

$$\eta = \left[R_b^* - \frac{1}{2}\log_2\left(1 + \frac{\alpha}{1-\alpha}\right)\right]^+ \times (1-\delta). \tag{29}$$

Then, the corresponding energy efficiency of the system is defined as the zero-outage secrecy spectral efficiency per power consumption [21], which is

$$\zeta = \frac{B \times \eta}{(N_A P_A + P_B) \times 2 + P/\mu}, \tag{30}$$

where P_A and P_B are the power consumption of each transmitter and receiver antenna, respectively, B is the bandwidth, and μ is the power amplifier coefficient. It should be noted that double circuit power in the denominator of (30) indicates two-phase transmissions.

6. Numerical Results and Discussion

In this section, we provide the numerical results of the analytical sections. Consider the GSM-1900 standard for a micro-cell model, which defines [21,22]: circuit powers with $P_A = 0.36\ W$ and $P_B = 0.24\ W$, noise power of $\sigma_n^2 = N_f N_0 B$ with $N_0 = -174$ dBm/Hz, $N_f = 3$ dB, and bandwidth $B = 200$ kHz, and channel variance $\sigma_h^2 = 10^{-(3.45+3.8\log_{10}(d_B))}$, with the distance $d_B = 1$ km between Alice and Bob.

From Figures 2 and 3, one can see that zero-outage secrecy can always be achieved when the secrecy and codeword rate, i.e., R_s and R_b, are designed properly to force the equivocate rate ($R_b - R_s$) to be larger than a threshold, as in (18). One can also see that the secrecy outage probability increases with increasing Eve's number of antennas and with a closer distance to Alice. These results show that the noise injection scheme can help to guarantee secrecy with probability 1, which is crucial in real scenarios to prevent thieves from eavesdropping on credit card numbers under any circumstance. Furthermore, the secrecy outage probability is shown to increase with an increasing number of the transmitter antennas, as illustrated in Figure 4.

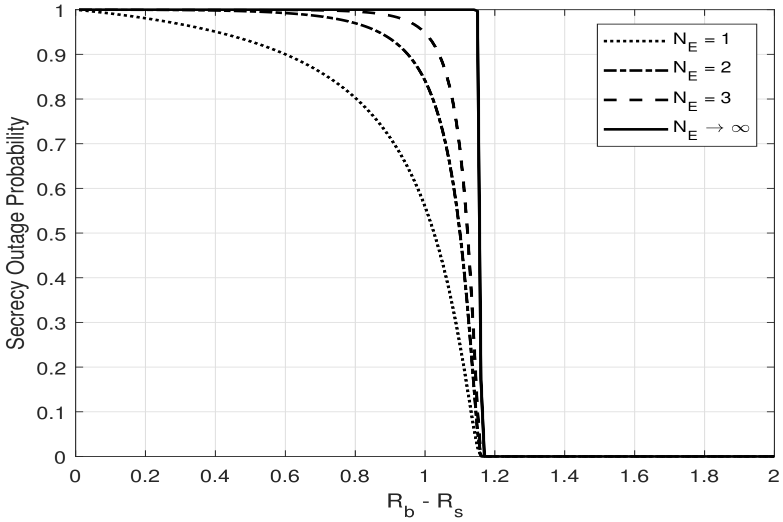

Figure 2. Secrecy outage probability, P_{SO}, versus $R_b - R_s$ for different values of N_E; $\alpha = 0.8$, $N_A = 2$, and $\sigma_g^2 = \sigma_h^2$.

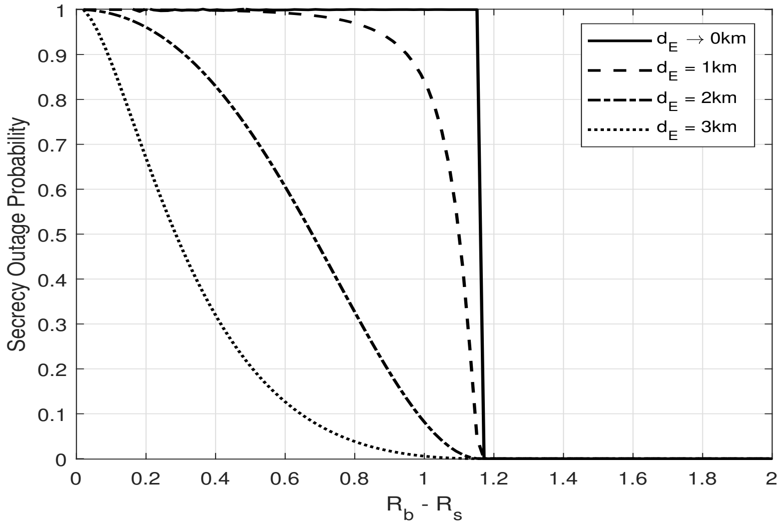

Figure 3. Secrecy outage probability, P_{SO}, versus $R_b - R_s$ for different eavesdropper distance d_E; $\alpha = 0.8$, $N_A = 2$, and $N_E = 2$.

Figures 5 and 6 depict the zero-outage secrecy throughput of the system versus α and P (dB), respectively. One can see that there exists an optimum ratio between the secret message and AN powers to maximize throughput, and the optimal power ratio increases when the transmit power increases. One can also see that when optimal α is applied, the secrecy throughput converges to a constant. This convergence of the secrecy throughput is due to the interference from estimation error.

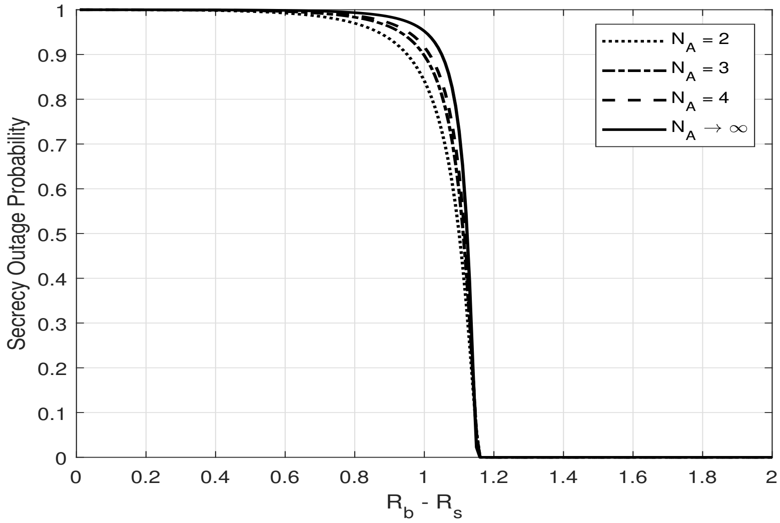

Figure 4. Secrecy outage probability, P_{SO}, versus $R_b - R_s$ for different values of N_A; $\alpha = 0.8$, $N_E = 2$, and $\sigma_g^2 = \sigma_h^2$.

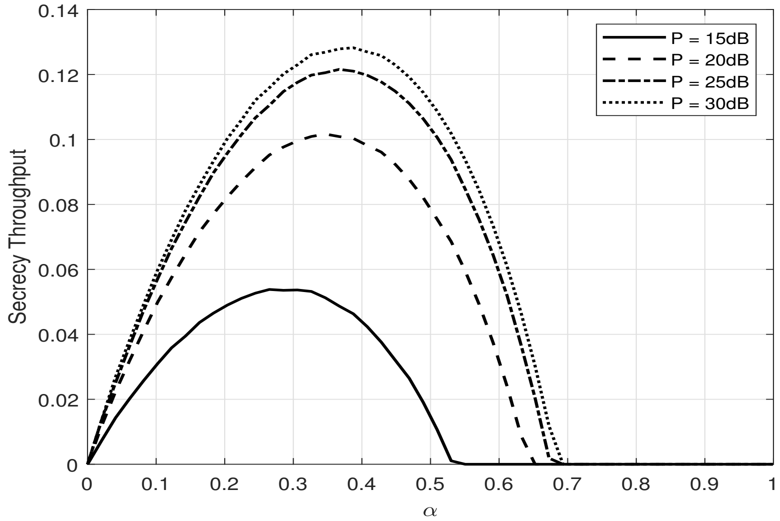

Figure 5. Secrecy throughput, η, versus α for different number of transmit power P (dB); $\beta = 0.1$, $\delta = 0.1$, and $N_A = 2$.

Figures 7 and 8 depict the SEE versus the average total transmit power P (dB) for different numbers of transmit antennas, N_A, and estimation error coefficient, β, at Alice. There exists an optimal P to maximize energy efficiency and that energy efficiency increases as the estimation error decreases. Furthermore, there also exists an optimal N_A to maximize energy efficiency, as in Figure 9, depicting the SEE versus Alice's numbers of transmit antennas for different transmit powers P (dB). This is because increasing the transmit power or number of transmit antennas significantly increases the total power consumption while the secrecy throughput stays constant (as shown in Figure 6), hence reducing the energy efficiency.

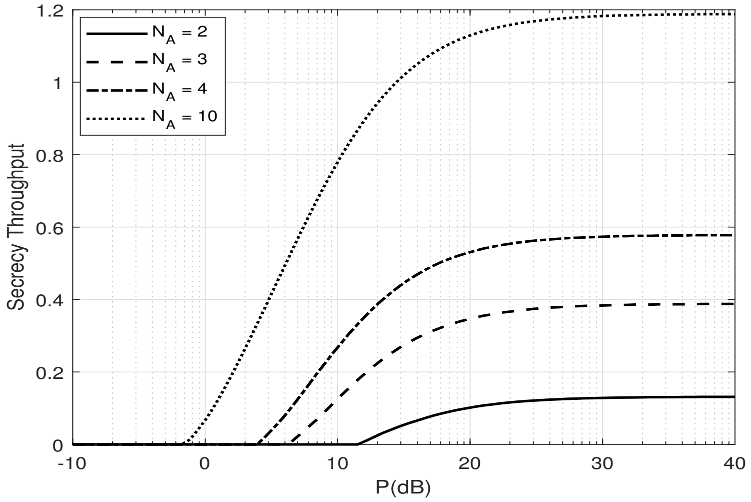

Figure 6. Secrecy throughput, η, versus P when the optimal α is applied for a different number of transmit antennas N_A; $\beta = 0.1$ and $\delta = 0.1$.

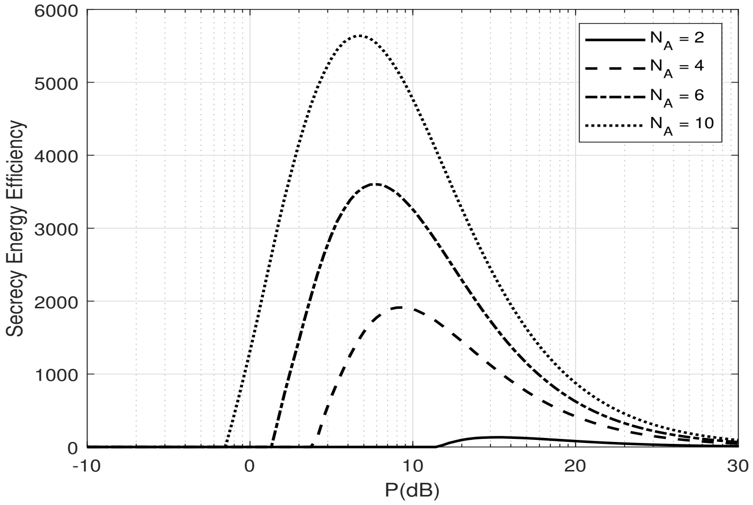

Figure 7. Secrecy energy efficiency, ζ, versus P for a different number of transmit antennas N_A when optimal α is used; $\beta = 0.1$ and $\delta = 0.1$.

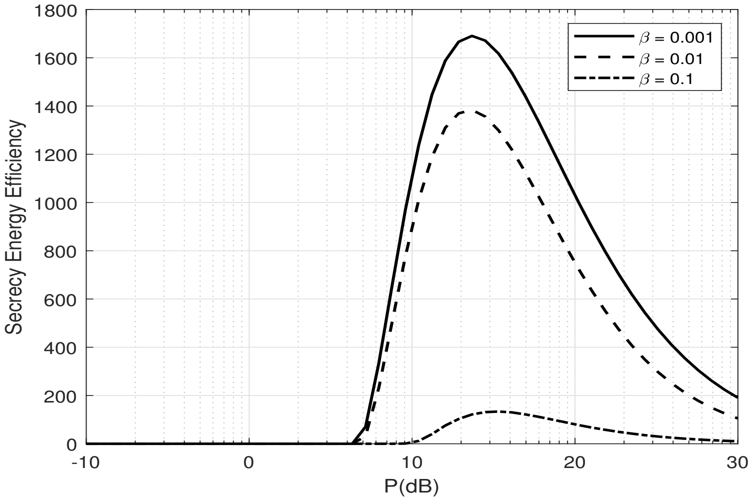

Figure 8. Secrecy energy efficiency, ζ, versus P for different number of β when the optimal α is applied; $N_A = 2$, $N_E = 2$, and $\delta = 0.1$.

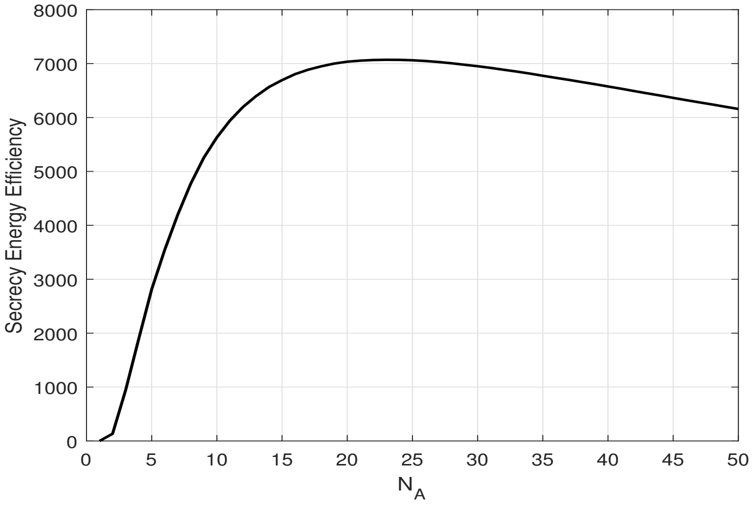

Figure 9. Secrecy energy efficiency, ζ, versus N_A when optimal α and optimal power P is used; $\beta = 0.1$ and $\delta = 0.1$.

7. Conclusions

A new artificial noise (AN) injection method for MISOME systems was proposed. We proved that zero-outage secrecy can be always achieved in any circumstance. The numerical results showed the scheme can achieve zero secrecy outage with a trade-off in the secrecy rate and half-time transmissions. The results also showed that with perfect CSI, the zero-outage secrecy throughput increases with the transmit power, which is important in secrecy design. The results also showed the existence of an optimal transmit power and the number of transmitter antennas to maximize energy efficiency. As an extension of this work, antenna selection to reduce the complexity as well as increase energy efficiency will be considered. Also, this type of transmission strategy can be applied to multi-user scenarios, providing zero secrecy outage to the whole network with one simple artificial noise injection transmission.

Author Contributions: Formal analysis, H.Q.T., L.C. and H.O.; Investigation, H.Q.T., L.C. and H.O.; software, H.Q.T., L.C. and H.O.; Writing—original draft, H.Q.T., L.C. and H.O. All authors have read and agreed to the published version of the manuscript.

Funding: This result was supported by "Regional Innovation Strategy (RIS)" through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (MOE) (2023RIS-003).

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The cumulative and probability density function (CDF and PDF) of

$$X_i = \left| \frac{\tilde{\mathbf{h}}_i^T \hat{\mathbf{h}}_i^*}{||\hat{\mathbf{h}}_i||} \right|^2 \frac{1}{||\hat{\mathbf{h}}_i||^2} \tag{A1}$$

for $i \in \{1,2\}$ is derived in this Appendix. Since $|\tilde{\mathbf{h}}_i^T \hat{\mathbf{h}}_i^* / ||\hat{\mathbf{h}}_i|||^2$ has an exponential distribution with mean of $\beta\sigma_h^2$, and $||\hat{\mathbf{h}}_i||^2$ has a chi-squared distribution with $2N_A$ degrees of freedom and common variance of $(1-\beta)\sigma_h^2/2$, we have

$$\begin{aligned}
F(x) &= Pr(X_i < x) \\
&= 1 - Pr\left(|\tilde{\mathbf{h}}_i^T \hat{\mathbf{h}}_i^* / \|\hat{\mathbf{h}}_i\||^2 > x\|\hat{\mathbf{h}}_i\|^2 \right) \\
&= 1 - \int_0^\infty e^{-\frac{xt}{\beta\sigma_h^2}} \frac{t^{N_A-1} e^{-t/((1-\beta)\sigma_h^2)}}{(N-1)!((1-\beta)\sigma_h^2)^{N_A}} dt \\
&= 1 - \frac{\int_0^\infty t^{N_A-1} e^{-t\left[\frac{x}{\beta\sigma_h^2} + \frac{1}{(1-\beta)\sigma_h^2}\right]} dt}{(N-1)!((1-\beta)\sigma_h^2)^{N_A}} \\
&= 1 - \frac{1}{(1+x(1-\beta)/\beta)^{N_A}}
\end{aligned} \tag{A2}$$

and

$$\begin{aligned}
f(x) &= dF(x)/dx \\
&= \frac{N_A(1-\beta)/\beta}{(1+x(1-\beta)/\beta)^{N_A+1}}.
\end{aligned} \tag{A3}$$

References

1. Heron, S. Advanced encryption standard (AES). *Netw. Secur.* **2009**, *2009*, 8–12. [CrossRef]
2. Milanov, E. *The RSA Algorithm*; RSA Laboratories: Bedford, MA, USA, 2009; pp. 1–11.
3. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
4. Barros, J.; Rodrigues, M.R.D. Secrecy Capacity of Wireless Channels. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; pp. 356–360. [CrossRef]
5. Wang, H.M.; Xia, X.G. Enhancing wireless secrecy via cooperation: Signal design and optimization. *IEEE Commun. Mag.* **2015**, *53*, 47–53. [CrossRef]
6. Goel, S.; Negi, R. Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
7. He, B.; She, Y.; Lau, V.K. Artificial noise injection for securing single-antenna systems. *IEEE Trans. Veh. Technol.* **2017**, *66*, 9577–9581. [CrossRef]
8. Zheng, G.; Krikidis, I.; Li, J.; Petropulu, A.P.; Ottersten, B. Improving physical layer secrecy using full-duplex jamming receivers. *IEEE Trans. Signal Process.* **2013**, *61*, 4962–4974. [CrossRef]
9. Zheng, T.X.; Wang, H.M.; Yuan, J.; Han, Z.; Lee, M.H. Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3827–3839. [CrossRef]
10. Zheng, T.X.; Wang, H.M.; Yang, Q.; Lee, M.H. Safeguarding Decentralized Wireless Networks Using Full-Duplex Jamming Receivers. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 278–292. [CrossRef]
11. Wang, H.M.; Zhao, B.Q.; Zheng, T.X. Adaptive Full-Duplex Jamming Receiver for Secure D2D Links in Random Networks. *IEEE Trans. Commun.* **2019**, *67*, 1254–1267. [CrossRef]
12. Guo, Y. Application of full duplex guarantees secure wireless communication. *J. Commun. Networks* **2017**, *19*, 105–113. [CrossRef]
13. Cao, Z.; Ji, X.; Wang, J.; Zhang, S.; Ji, Y.; Li, Y.; Wang, J. Security-Reliability Trade-Off Analysis of AN-Aided Relay Selection for Full-Duplex Relay Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 2362–2377. [CrossRef]
14. Li, B.; Zhang, M.; Rong, Y.; Han, Z. Artificial Noise-Aided Secure Relay Communication with Unknown Channel Knowledge of Eavesdropper. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 3168–3179. [CrossRef]
15. Liu, T.Y.; Lin, P.H.; Lin, S.C.; Hong, Y.W.P.; Jorswieck, E.A. To avoid or not to avoid CSI leakage in physical layer secret communication systems. *IEEE Commun. Mag.* **2015**, *53*, 19–25. [CrossRef]
16. Zhou, X.; Lamahewa, T.A.; Sadeghi, P.; Durrani, S. Two-way training: Optimal power allocation for pilot and data transmission. *IEEE Trans. Wirel. Commun.* **2010**, *9*, 564–569. [CrossRef]
17. Hassibi, B.; Hochwald, B.M. How much training is needed in multiple-antenna wireless links? *IEEE Trans. Inf. Theory* **2003**, *49*, 951–963. [CrossRef]
18. Goldsmith, A. *Wireless Communications*; Cambridge University Press: Cambridge, UK, 2005.
19. Zhou, X.; McKay, M.R.; Maham, B.; Hjorungnes, A. Rethinking the Secrecy Outage Formulation: A Secure Transmission Design Perspective. *IEEE Commun. Lett.* **2011**, *15*, 302–304. [CrossRef]
20. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Elsevier/Academic Press: Amsterdam, The Netherlands, 2007.

21. Ta, H.Q.; Kim, S.W. Adapting rate and power for maximizing secrecy energy efficiency. *IEEE Commun. Lett.* **2017**, *21*, 2049–2052. [CrossRef]
22. Wang, A.Y.; Sodini, C.G. On the energy efficiency of wireless transceivers. In Proceedings of the 2006 IEEE International Conference on Communications, Istanbul, Turkey, 25–28 June 2006; Volume 8, pp. 3783–3788.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.