electronics

MDPI

Article

Guaranteeing Zero Secrecy Outage in Relaying Systems under Eavesdropper's Arbitrary Location and Unlimited Number of Antennas

Hien Q. Ta [1,2], Nga B. T. Nguyen [1,2], Khuong Ho-Van [2,3] and Hoon Oh [4,*]

1 School of Electrical Engineering, International University, Ho Chi Minh City 700000, Vietnam; tqhien@hcmiu.edu.vn (H.Q.T.); eeeeiu19015@student.hcmiu.edu.vn (N.B.T.N.)
2 Vietnam National University Ho Chi Minh City, Linh Trung Ward, Thu Duc District, Ho Chi Minh City 700000, Vietnam
3 Department of Telecommunications Engineering, Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City 70000, Vietnam; hvkhuong@hcmut.edu.vn
4 Department of Electrical, Electronic and Computer Engineering, University of Ulsan, Ulsan 44610, Republic of Korea
* Correspondence: hoonoh@ulsan.ac.kr

Abstract: This paper proposes a three-phase transmission scheme to ensure zero secrecy outage in decode-and-forward relay systems by using the strategies of artificial noise (AN) injection and channel state information (CSI) leakage avoidance. The zero-outage secrecy spectral efficiency (ZOSSE) and energy efficiency (ZOSEE) of the scheme are then analyzed. Finally, the paper demonstrates that the scheme can always achieve zero secrecy outage even when the eavesdropper has an unlimited number of antennas or is in an arbitrary location, which shows its practical applicability. The paper also shows that the ZOSSE increases with the transmit power and that both the ZOSSE and the ZOSEE are maximized when the relay is halfway between the transmitter and the receiver. This suggests that the placement of the helper node is important in securing the communication of two distant nodes.

Keywords: physical layer security; artificial noise injection; cooperative network; zero-outage secrecy

Citation: Ta, H.Q.; Nguyen, N.B.T.; Ho-Van, K.; Oh, H. Guaranteeing Zero Secrecy Outage in Relaying Systems under Eavesdropper's Arbitrary Location and Unlimited Number of Antennas. *Electronics* **2023**, *12*, 4695. https://doi.org/10.3390/electronics12224695

Academic Editors: Kang An, Bin Li, Zhi Lin and Xiaoyan Hu

Received: 10 October 2023
Revised: 15 November 2023
Accepted: 16 November 2023
Published: 18 November 2023

1. Introduction

Wireless services have become an essential part of people's lives, for various purposes, both business and personal, thanks to their mobility, their cost saving, and their efficiency [1]. The exponential increase in users relies on wireless networks, due to their not only being reliable but also secure. The wireless channel is an open medium for intruders [2], and it is accessible to anyone, in such a way that the signal may even be modified before reaching the legitimate receivers [3], which leads to information leakage and unexpected negative impacts. Hence, security is an important aspect of designing wireless systems. Cryptosystems have been applied to the upper layer for security purposes. Despite their effectiveness, the systems may be difficult to employ in some specific architectures [3]. For that reason, the physical layer is considered as an alternative solution for security, thanks to its recent results from information theory [4]. Secret communication was introduced by Wyner in the scenario of the wiretap channel [5], which indicates that secrecy can be achieved as long as the unauthorized channel is worse than the legitimate one. However, in practice, this is not always the case. Eavesdroppers can have better channels; for example, if their locations are nearer to the transmitter compared to the intended receiver [6]. In such instances, secrecy is no longer guaranteed.

Multiple studies have focused on solutions to this problem, and injecting artificial noise (AN) to confuse eavesdroppers is one of them. The AN is sent to the null space of the authorized receiver, which does not have any effect on it but remains in the unintended ones

and, hence, degrades the wiretap channel [7]. Similar studies have been conducted, showing that the receiver is assumed to own more antennas than the eavesdropper; otherwise, secure communication is not guaranteed [8–10]. As conventional schemes cannot guarantee secrecy if the eavesdropper is powerful and also cannot achieve secrecy in some extreme scenarios requiring zero secrecy outage [11,12] (such as credit card number transmission) or extremely strict security constraints (such as the Internet of Vehicles [13,14]), this urges a novel secure transmission design. One possible design is to transmit AN in the same space as the secure message. However, to achieve the AN removal capability at the receiver, an extra timeslot for only transmitting the AN to Eve with the aid of a CSI leakage mechanism [15] is used, such that legitimate receivers—but not eavesdroppers—can cancel the AN. Therefore, a novel AN-aided design of secure transmission to guarantee zero secrecy outage is considered.

Moreover, energy efficiency is an important metric for green communication [16], and secrecy energy efficiency also has received much attention [17,18]. Secrecy energy efficiency or the secrecy throughput (bits/s) per power consumption has been considered in different fashions, such as ergodic secrecy throughput per power consumption [19] or the average of instantaneous secrecy energy efficiency [20]. While the former can be solved via fractional programming theory [17], the latter exploits the pseudo-convexity property of the objective, to convert the energy efficiency problem to the convex problem, which can be solved by the Karush–Kuhn–Tucker (KKT) conditions. Hence, energy efficiency will also be quantified in the zero-outage secret communication.

Therefore, this paper proposes an artificial-noise-aided transmission model in decode-and-forward (DF) relaying systems in three time slots subject to zero secrecy outage, and then characterizes the achievable zero-outage secrecy spectral efficiency (ZOSSE) and energy efficiency (ZOSEE). How the AN is injected was inspired by the two previously mentioned works in [21,22]. In the first time slot (first phase), the AN is transmitted by the Relay. After receiving it, the transmitter then amplifies and forwards it with the secure message in the next phase. The secure message is later decoded and forwarded with the same AN by the Relay to the receiver in the third phase. Finally, the legitimate receiver can remove the AN and successfully decode the secret message but the eavesdropper cannot, even if it has an unlimited number of antennas. This paper outlines the proposed system model in Section 2, the signal-to-noise ratio (SNR) that is received at all nodes in Section 3, the analysis of the secrecy outage probability in Section 4, and the connection outage probability in Section 5. The zero-outage secrecy spectral efficiency and the energy efficiency are determined in Sections 6 and 7, respectively. Section 8 presents numerous results for insight understanding, which are then wrapped up in Section 9.

2. System Model

Figure 1 illustrates a three-phase secure transmission scheme in a decode-and-forward (DF) relaying system to guarantee zero secrecy outage when an eavesdropper (Eve) attempts to steal the information. The transmitter (Alice) and the receiver (Bob) have one antenna each and there is no direct link between them. It is assumed that Eve and Relay have one antenna each for simplicity of notation, and we later extend the analysis to multiple-antenna cases for Eve and Relay in Sections 4 and 5, respectively. The proposed model aims to utilize a time slot to transmit only artificial noise and to prevent Eve from learning the CSI between Relay and Eve in this time slot. By this way, the legitimate receiver can use the received signal in this time slot to cancel out the artificial noise (AN) but Eve cannot. This can be achieved by allowing the reverse training phase, where Alice and Bob send pilot signals and Relay then sends the estimated CSIs via error-free feedback links, so that Eve has CSI knowledge of the channels at Alice and Bob, but not Relay.

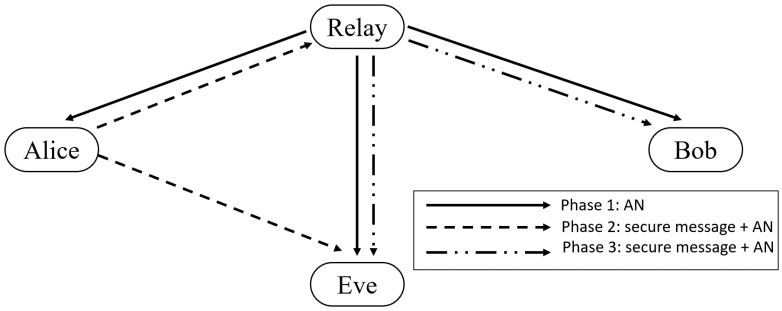

Figure 1. The proposed three-phase transmission model in decode-and-forward relaying systems.

Let $h_{ij}^{(n)}$ be the node i-j channel gain in the n-th transmission phase where $i, j \in \{A, R, B, E\}$, indicating Alice, Relay, Bob, and Eve, respectively, and $h_{ij}^{(n)}$ is a complex Gaussian distributed with zero mean and a variance of σ_{ij}^2, denoted as $h_{ij}^{(n)} \sim \mathcal{CN}(0, \sigma_{ij}^2)$. All the nodes are assumed to have perfect channel estimation, and the channels change slowly according to Rayleigh fading. We also assume that the noises at all the nodes are denoted as $n_i^{(n)} \sim \mathcal{CN}(0, \sigma_n^2)$. Our scheme has three phases: the first phase only sends the AN, while the second and third phases send the secure message with the AN. The channels are independent in each phase, and reverse pilot training is used in the first phase while forward pilot training is used in the second and third phases, as illustrated in Figure 2. The details of the pilot training and data transmission will be explained at each phase.

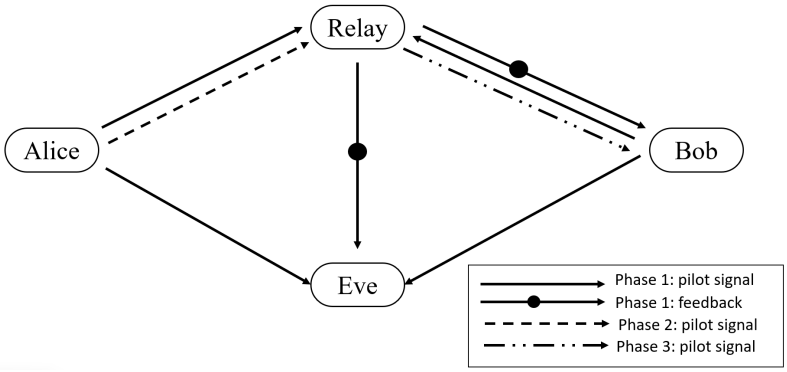

Figure 2. Pilot training in all phases.

2.1. Phase 1

In the first phase, Alice and Bob send pilot symbols to Relay for channel estimation, and the CSI between Relay and Bob is fed back to Bob in the error-free link, for the purpose of removing the AN. It is emphasized that Relay–Bob's CSI is perfectly acknowledged by Bob while Relay–Eve's CSI is unknown to Eve, and this is the key to guaranteeing secure transmissions in the next two phases.

Then, Relay generates and transmits only the artificial noise (AN), $\sqrt{P}z$, where z denotes the AN with $z \sim \mathcal{CN}(0, 1)$. Then, we obtain

$$y_i^{(1)} = \sqrt{P} h_{Ri}^{(1)} z + n_i^{(1)} \tag{1}$$

for $i \in \{A, B, E\}$.

2.2. Phase 2

In the second phase, Alice sends pilot symbols to Relay for channel estimation, and then Alice amplifies and forwards the received AN in the first phase with the superimposed secure message. Alice's transmitted signal is given by [21]:

$$x_A = \sqrt{\alpha P}s + \sqrt{(1-\alpha)P}\frac{y_A^{(1)}}{|y_A^{(1)}|}, \tag{2}$$

where s is the normalized secure information signal ($s \sim \mathcal{CN}(0,1)$), α is the portion of the power used for the signal-bearing information with $0 < \alpha < 1$, and

$$|y_A^{(1)}|^2 = P|h_{RA}^{(1)}|^2 + \sigma_n^2 \tag{3}$$

is Alice's received power. Note that the AN is amplified and forwarded in the second term of Formula (2) following [23] and is shared power with the secure message, while the total transmit power is fixed at P. Then, Relay and Eve receive

$$y_i^{(2)} = \sqrt{P}h_{Ai}^{(2)}x_A + n_i^{(2)} \tag{4}$$

for $i \in \{R, E\}$.

2.3. Phase 3

In the third phase, Relay sends pilot symbols for channel estimation at Bob, and, after receiving

$$\begin{aligned} y_R^{(2)} &= h_{AR}^{(2)}x_A + n_R^{(2)} \\ &= h_{AR}^{(2)}\left(\sqrt{\alpha P}s + \sqrt{(1-\alpha)P}\frac{y_A^{(1)}}{|y_A^{(1)}|}\right) + n_R^{(2)} \\ &= \sqrt{\alpha P}h_{AR}^{(2)}s + \sqrt{(1-\alpha)P}h_{AR}^{(2)}\frac{\sqrt{P}h_{RA}^{(1)}z + n_A^{(1)}}{\sqrt{P|h_{RA}^{(1)}|^2 + \sigma_n^2}} + n_R^{(2)} \end{aligned} \tag{5}$$

in the second phase, Relay can remove the AN, as it perfectly knows $h_{RA}^{(1)}$ and $h_{AR}^{(2)}$, and the AN emitted by itself, to obtain

$$y_R'^{(2)} = \sqrt{\alpha P}h_{AR}^{(2)}s + \frac{\sqrt{(1-\alpha)P}h_{AR}^{(2)}n_A^{(1)}}{\sqrt{P|h_{RA}^{(1)}|^2 + \sigma_n^2}} + n_R^{(2)}. \tag{6}$$

Perfect knowledge of $h_{RA}^{(1)}$ is because Relay perfectly obtains the CSI of $h_{AR}^{(1)}$ from the pilot symbols transmitted by Alice and $h_{RA}^{(1)} = h_{AR}^{(1)}$ thanks to the reciprocal property [24].

Therefore, Relay decodes the secure message s from $y_R'^{(2)}$, with an outage probability ($\mathbb{P}$ denotes the probability notation) of

$$P_{O,R} = \mathbb{P}\left(\frac{1}{3}\log_2\left(1 + \frac{\alpha P|h_{AR}^{(2)}|^2}{\sigma_n^2 + \frac{(1-\alpha)P|h_{AR}^{(2)}|^2\sigma_n^2}{P|h_{RA}^{(1)}|^2+\sigma_n^2}}\right) < R_B\right), \tag{7}$$

where the factor $\frac{1}{3}$ indicates three-phase transmission. Relay forwards it to Bob by sending

$$x_R = \sqrt{\alpha P}s + \sqrt{(1-\alpha)P}z. \tag{8}$$

Then, the received signals at Bob and Eve will be

$$\begin{aligned} y_i^{(3)} &= h_{Ri}^{(3)}x_R + n_i^{(3)} \\ &= \sqrt{\alpha P}h_{Ri}^{(3)}s + \sqrt{(1-\alpha)P}h_{Ri}^{(3)}z + n_i^{(3)} \end{aligned} \tag{9}$$

for $i \in \{B, E\}$.

3. Received SNR

In this section, we will determine the received SNR at Bob and Eve. It follows from Formulas (1) and (9) that, as Bob perfectly knows $h_{RB}^{(1)}$ and $h_{RB}^{(3)}$, he can remove the AN by subtracting $y_{RB}^{(3)}$ to $\sqrt{1-\alpha}\frac{h_{RB}^{(3)}}{h_{RB}^{(1)}}y_{RB}^{(1)}$, to obtain

$$y_B = \sqrt{\alpha P}h_{RB}^{(3)}s + n_B^{(3)} - \sqrt{1-\alpha}\frac{h_{RB}^{(3)}}{h_{RB}^{(1)}}n_B^{(1)}. \tag{10}$$

Hence, Bob's received SNR can be obtained by

$$\gamma_B = \frac{\alpha P/\sigma_n^2}{\frac{1-\alpha}{|h_{RB}^{(1)}|^2} + \frac{1}{|h_{RB}^{(3)}|^2}}. \tag{11}$$

Meanwhile, the signals received at Eve from three phases are

$$\begin{aligned} y_E^{(1)} &= \sqrt{P}h_{RE}^{(1)}z + n_E^{(1)}, \\ y_E^{(2)} &= \sqrt{P}h_{AE}^{(2)}\left(\sqrt{\alpha}s + \sqrt{1-\alpha}\frac{\sqrt{P}h_{RA}^{(1)}z + n_A^{(1)}}{\sqrt{P|h_{RA}^{(1)}|^2 + \sigma_A^2}}\right) + n_E^{(2)}, \\ y_E^{(3)} &= \sqrt{\alpha P}h_{RE}^{(3)}s + \sqrt{(1-\alpha)P}h_{RE}^{(3)}z + n_E^{(3)}. \end{aligned} \tag{12}$$

One should note that the phase shift of the channel gain $h_{RE}^{(1)}$ cannot be estimated from $y_E^{(1)}$, as the received signal $y_E^{(1)}$ is only noise. In fact, as

$$H(h_{RE}^{(1)}|y_E^{(1)}) = H\left(h_{RE}^{(1)}\right), \tag{13}$$

where $H(z)$ denotes the entropy of random variable z, this shows that the CSI cannot be obtained from the received signal. Then, decoding the secure message with the additional received signal $y_E^{(1)}$ does not help. Therefore, as Eve perfectly knows $h_{AE}^{(2)}$ and $h_{RE}^{(3)}$, it can apply the maximum–ratio combining of $y_E^{(2)}$ and $y_E^{(3)}$, to obtain its SNR of

$$\gamma_E = \frac{\alpha P|h_{AE}^{(2)}|^2}{\sigma_n^2 + (1-\alpha)P|h_{AE}^{(2)}|^2} + \frac{\alpha P|h_{RE}^{(3)}|^2}{\sigma_n^2 + (1-\alpha)P|h_{RE}^{(3)}|^2}. \tag{14}$$

4. Secrecy Outage Probability

The probability that Eve can successfully decode the secure message when the message is transmitted [25], which is also known as the secrecy outage probability (SOP), will be derived in this section. We denote the codeword rate R_B and the secrecy rate R_S. The positive difference of $R_B - R_S$ is the cost needed to transmit the message without being eavesdropping. As the channel capacity at Eve is obtained from Formula (14) as

$$C_E = \frac{1}{3}\log_2(1+\gamma_E), \tag{15}$$

where the factor $\frac{1}{3}$ indicates three-phase transmission, the SOP is derived as [25]:

$$\begin{aligned} P_{SO} &= \mathbb{P}(C_E > R_B - R_S) \\ &= \mathbb{P}\left(\gamma_E > 2^{3(R_B - R_S)} - 1\right) \\ &= \mathbb{P}(X + Y > k), \end{aligned} \tag{16}$$

where $k = 2^{3(R_B - R_S)} - 1$, and

$$X = \frac{\alpha P |h_{AE}^{(2)}|^2}{\sigma_n^2 + (1-\alpha) P |h_{AE}^{(2)}|^2}, \tag{17}$$

$$Y = \frac{\alpha P |h_{RE}^{(3)}|^2}{\sigma_n^2 + (1-\alpha) P |h_{RE}^{(3)}|^2}. \tag{18}$$

It should be noted that when Eve has M antennas, the random variable $|h_{ij}^{(n)}|^2$ changes to $||\mathbf{h}_{ij}^{(n)}||^2$, where its probability density function (PDF) and cumulative probability density function (CDF) is given by

$$\begin{aligned} p_Z(z) &= \frac{\alpha \sigma_n^2 / \sigma_{iE}^2}{(M-1)!(\alpha - (1-\alpha)z)^2 P} \left(\frac{z\sigma_n^2}{(\alpha - (1-\alpha)z) P \sigma_{iE}^2} \right)^{M-1} \exp\left(- \frac{z\sigma_n^2}{(\alpha - (1-\alpha)z) P \sigma_{iE}^2} \right), \\ F_Z(z) &= 1 - \Gamma\left(M, \frac{z\sigma_n^2}{(\alpha - z(1-\alpha)) P \sigma_{iE}^2} \right) \end{aligned} \tag{19}$$

for $z < \alpha/(1-\alpha)$ and $(Z, i) \in \{(X, A), (Y, R)\}$, respectively, where

$$\Gamma(m, x) = \int_x^\infty \frac{1}{(m-1)!} t^{m-1} e^{-t} dt \tag{20}$$

is the incomplete gamma function [26]. The result of Formula (19) is proved in Appendix A.

Therefore, it follows from Formulas (17) and (19) that the SOP is obtained by

$$\begin{aligned} P_{SO} &= 1 - \int_0^k \left(\int_0^{k-y} p_X(x) dx \right) p_Y(y) dy \\ &= 1 - \int_0^k F_X(k-y) p_Y(y) dy. \end{aligned} \tag{21}$$

For $P_{SO} \to 0$, we require from Formula (21) that

$$\int_0^k F_X(k-y) p_Y(y) dy \to 1, \tag{22}$$

or, equivalently, $k \geq 2\alpha/(1-\alpha)$. Hence, the zero-outage $P_{SO} \to 0$ can be achieved if the rate pair of (R_B, R_S) is chosen, such that

$$R_S \leq \left[R_B - \frac{1}{3} \log_2 \left(1 + \frac{2\alpha}{1-\alpha} \right) \right]^+, \tag{23}$$

where $(z)^+ = \max\{z, 0\}$.

Remark 1. *The result in Formula (23) means that secure transmission can always be guaranteed in any circumstance if we choose the pair rates properly with a constant difference of* $\frac{1}{3} \log_2 \left(1 + \frac{2\alpha}{1-\alpha}\right)$. *Here, it should be emphasized that in this paper complete security is achieved in the physical layer of relaying systems, even for single-antenna relaying systems, by the trade-off of one extra time slot for the artificial noise transmission.*

Figures 3 and 4 illustrate the SOP with respect to the rate difference $(R_B - R_S)$ for different values of Alice's transmit power P and Eve's number of antennas M, while the detail of the setup parameters is mentioned in Section 8. It is obvious that the SOP is equal to zero when $(R_B - R_S)$ is not less than the threshold, which is exactly $\frac{1}{3}\log_2\left(1 + \frac{2\alpha}{1-\alpha}\right)$, regardless of Alice's transmit power and Eve's number of antennas. It can also be seen that the SOP steeply decreases to zero at Alice's high transmit power or Eve's large number of antennas (see $P = 20$ dB in Figure 3 and $M = 1000$ in Figure 4). Thus, the zero-outage secrecy is under practical consideration of the worst scenario of Eve's unlimited number of antennas.

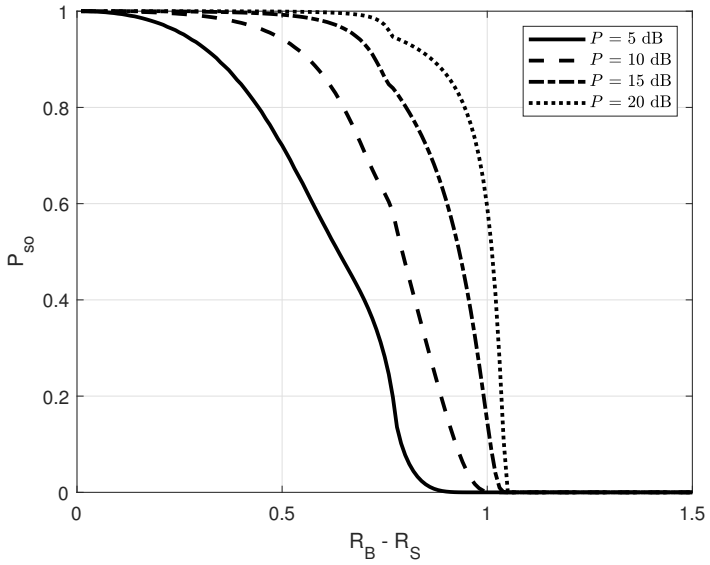

Figure 3. P_{SO} versus $(R_B - R_S)$ for different P; $M = 1$; $d_{AE} = d_{RE} = 1$ Km; $\alpha = 0.8$.

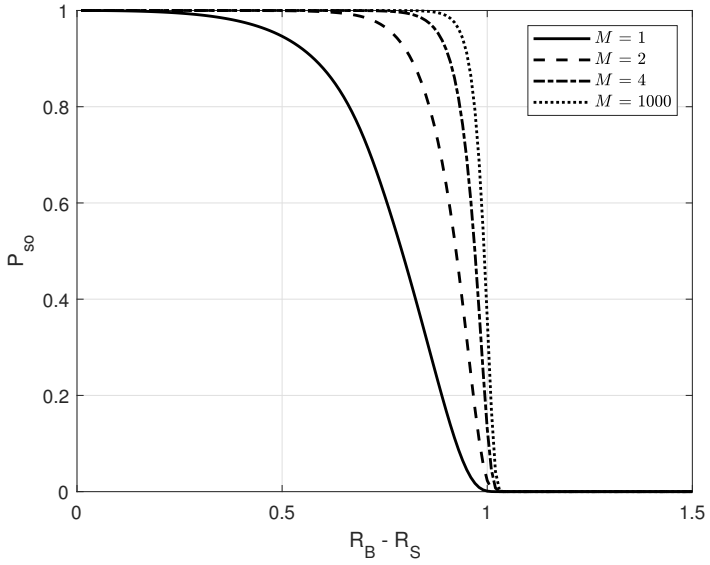

Figure 4. P_{SO} versus $(R_B - R_S)$ for different M; $P = 10$ dB, $d_{AE} = d_{RE} = 1$ Km; $\alpha = 0.8$.

5. Connection Outage Probability

In this section, the probability that a node fails to decode a message or the connection outage probability (COP) is derived. As Bob's decoding in phase 3 depends on whether Relay successfully decodes the secure message in phase 2, we need to first find the decoding

outage probability at Relay in phase 2 and then at Bob in phase 3. It follows from Formula (7) that the decoding outage probability of Relay in phase 2 is given by

$$\begin{aligned} P_{O,R} &= \mathbb{P}\left(\frac{\alpha P |h_{AR}^{(2)}|^2/\sigma_n^2}{1+\frac{(1-\alpha)P|h_{AR}^{(2)}|^2}{P|h_{RA}^{(1)}|^2+\sigma_n^2}} < 2^{3R_B}-1 \right) \\ &= \mathbb{P}\left(\frac{\alpha P/\sigma_n^2}{2^{3R_B}-1} < \frac{1}{|h_{AR}^{(2)}|^2} + \frac{(1-\alpha)P}{P|h_{AR}^{(1)}|^2+\sigma_n^2} \right) \\ &= 1-\mathbb{P}\left(|h_{AR}^{(2)}|^2 \geq \frac{1}{\left[\frac{\alpha P/\sigma_n^2}{2^{3R_B}-1} - \frac{(1-\alpha)P}{P|h_{AR}^{(1)}|^2+\sigma_n^2}\right]^+} \right) \\ &= 1-\int_r^\infty \bar{F}_{RA}\left(\frac{1}{\frac{\alpha P/\sigma_n^2}{2^{3R_B}-1} - \frac{(1-\alpha)P}{Px+\sigma_n^2}} \right) p_{RA}(x)dx, \end{aligned} \tag{24}$$

where $p_{ij}(x)$ and $\bar{F}_{ij}(x)$ indicate the PDF and the complement CDF (CCDF) of $|h_{ij}^{(n)}|^2$, respectively, with

$$\begin{aligned} p_{ij}(x) &= \exp(-x/\sigma_{ij}^2)/\sigma_{ij}^2, \\ \bar{F}_{ij}(x) &= \exp(-x/\sigma_{ij}^2) \end{aligned} \tag{25}$$

for $i, j \in \{A, R, B\}$ and $i \neq j$ being the PDF and complement CDF of $|h_{AR}^{(1)}|^2$, respectively, and

$$r = \frac{\sigma_n^2}{P}\left[\frac{(2^{3R_B}-1)(1-\alpha)}{\alpha} - 1 \right]^+. \tag{26}$$

Meanwhile, it follows from Formula (11) that the channel capacity at Bob is given by

$$C_B = \frac{1}{3}\log_2(1+\gamma_B), \tag{27}$$

and then its decoding outage probability is obtained by

$$P_{O,B} = \mathbb{P}(C_B < R_B) \tag{28}$$

$$= \mathbb{P}\Big(\gamma_B < 2^{3R_B}-1\Big), \tag{29}$$

which, from Formula (11), yields

$$\begin{aligned} P_{O,B} &= \mathbb{P}\left(\frac{\alpha P/\sigma_n^2}{\frac{1-\alpha}{|h_{RB}^{(1)}|^2} + \frac{1}{|h_{RB}^{(3)}|^2}} < 2^{3R_B}-1 \right) \\ &= 1-\mathbb{P}\left(\frac{1-\alpha}{|h_{RB}^{(1)}|^2} + \frac{1}{|h_{RB}^{(3)}|^2} \leq \frac{\alpha P/\sigma_n^2}{2^{3R_B}-1} \right) \\ &= 1-\mathbb{P}\left(|h_{RB}^{(1)}|^2 \geq \frac{1-\alpha}{\left[\frac{\alpha P/\sigma_n^2}{2^{3R_B}-1} - \frac{1}{|h_{RB}^{(3)}|^2}\right]^+} \right) \\ &= 1-\int_{\frac{(2^{3R_B}-1)\sigma_n^2}{\alpha P}}^\infty \bar{F}_{RB}\left(\frac{1-\alpha}{\frac{\alpha P/\sigma_n^2}{2^{3R_B}-1} - \frac{1}{x}} \right) p_{RB}(x)dx. \end{aligned} \tag{30}$$

Therefore, the COP of the whole relaying system can be derived as

$$\begin{aligned} P_{CO} &= 1-(1-P_{O,R})(1-P_{O,B}) \\ &= 1-\int_r^{\infty} \bar{F}_{RA}\left(\frac{1}{\frac{\alpha P/\sigma_n^2}{2^{3R_B}-1}-\frac{(1-\alpha)P}{Px+\sigma_n^2}}\right) p_{RA}(x)dx \int_{\frac{(2^{3R_B}-1)\sigma_n^2}{\alpha P}}^{\infty} \bar{F}_{RB}\left(\frac{1-\alpha}{\frac{\alpha P/\sigma_n^2}{2^{3R_B}-1}-\frac{1}{x}}\right) p_{RB}(x)dx. \end{aligned} \tag{31}$$

It is noted that when Relay has N antennas, the random variable $|h_{ij}^{(n)}|^2$ for $i,j \in \{A,R,B,E\}$ and $n \in \{1,2,3\}$ changes to $||\mathbf{h}_{ij}^{(n)}||^2$ as a random vector, which its PDF and CCDF of Formula (25) change to

$$\begin{aligned} p_{ij}(x) &= \frac{x^{N-1}\exp(-x/\sigma_{ij}^2)}{(N-1)!\sigma_{ij}^{2N}}, \\ \bar{F}_{ij}(x) &= \Gamma(N, x/\sigma_{ij}^2). \end{aligned} \tag{32}$$

Figures 5 and 6 illustrate the connection outage probability P_{CO}, with respect to R_B, for different values of Alice's transmit power P and Relay's number of antennas N, respectively, while the detail of the setup parameters is mentioned in Section 8. It can be seen that, as R_B decreases, the probability has the same behavior and the decrease is more significant for higher transmit power (higher P) or a larger number of antennas (larger N).

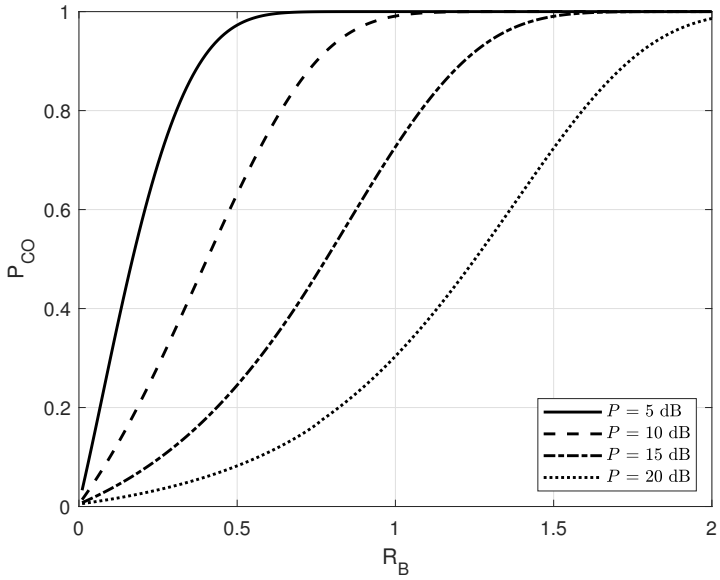

Figure 5. The connection outage probability P_{CO} versus R_B for different values of the transmit power P; $N = 1$, $d_{AR} = d_{RB} = 1$ Km; $\alpha = 0.8$.

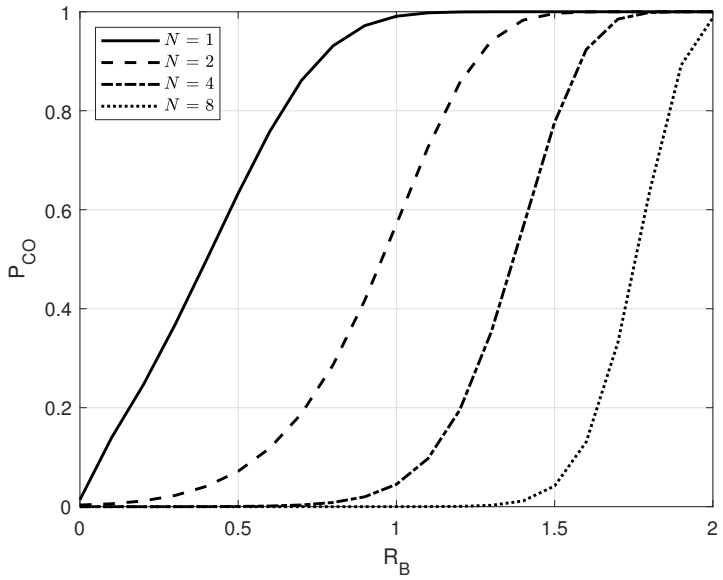

Figure 6. The connection outage probability P_{CO} versus R_B for different N; $P = 10$ dB, $d_{AR} = d_{RB} = 1$ Km; $\alpha = 0.8$.

6. Zero-Outage Secrecy Spectral Efficiency

The zero-outage secrecy spectral efficiency is defined as the amount of secure information (bits/s) reliably received by the legitimate receiver subject to zero secrecy outage ($P_{SO} \to 0$). The problem of zero-outage secrecy throughput is represented as [11,12]

$$\begin{aligned} &\max_{R_B, R_S} BW \times R_S \times (1 - P_{CO}) \\ \text{s.t.} \quad &P_{SO} \to 0, \end{aligned} \tag{33}$$

where BW indicates the signal bandwidth. As $P_{SO} \to 0$ requires the constraint on secrecy rate as in Formula (23), the zero-outage secrecy throughput denoted by $\eta(\alpha)$ is obtained by

$$\eta(\alpha) = \max_{R_B} BW \left[R_B - \frac{1}{3} \log_2 \left(1 + \frac{2\alpha}{1-\alpha} \right) \right]^+ (1 - P_{CO}) \tag{34}$$

as a function of α. Therefore, the maximum zero-outage secrecy throughput can be numerically computed via an exhausted search over α, which is

$$\eta = \max_{\alpha} \eta(\alpha). \tag{35}$$

Remark 2. *Differing from previous studies in the literature, where the constraint of $P_{SO} \to 0$ in the problem (33) yields the zero-secrecy spectral efficiency, our proposed scheme can enable positive throughput and, more than that, the zero-outage secrecy spectral efficiency increases with increasing transmitted power, as illustrated in Figure 7.*

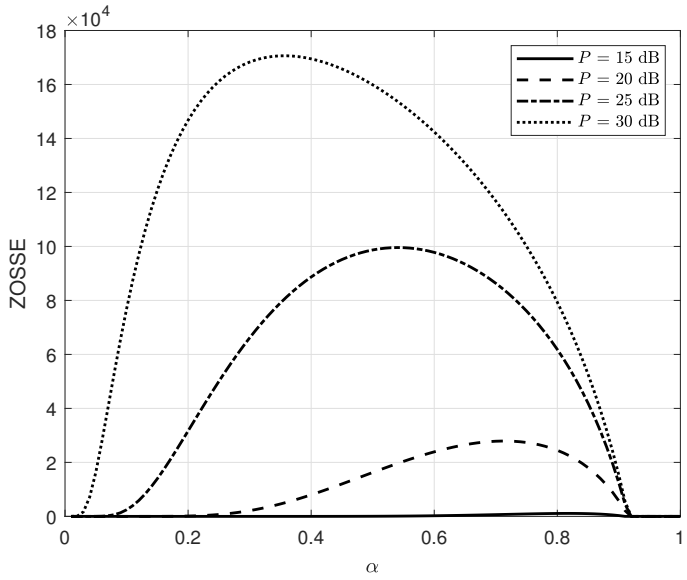

Figure 7. Zero-outage secrecy spectral efficiency, $\eta(\alpha)$, versus α for different values of the transmit power P; $d_{AR} = d_{RB} = 1$ Km.

7. Zero-Outage Secrecy Energy Efficiency

The zero-outage secrecy energy efficiency is defined as the zero-outage secrecy throughput per total transmit power. Then, it follows from Formula (35) that the zero-outage secrecy energy efficiency denoted ξ in bits/Jule is given by [20]:

$$\xi = \frac{\eta}{P_{total}}, \tag{36}$$

where P_{total} is the total transmit power used to transmit and receive the signal and is calculated over all three phases. More specifically, in the first phase, Relay transmits, while Alice and Bob receive the signal. In the second phase, Alice transmits the signal to Relay only and in the third phase, Bob receives the signal from Relay. Hence, as Relay has N antennas for both functions as transmitter and receiver, P_{total} can be computed by

$$\begin{aligned} P_{total} = &(N \times P_{R,Tx} + P_{A,Rx} + P_{B,Rx} + P/\mu) \\ &+(P_{A,Tx} + N \times P_{R,Rx} + P/\mu) \\ &+(N \times P_{R,Tx} + P_{B,Rx} + P/\mu), \end{aligned} \tag{37}$$

where μ is the amplifying coefficient, and $P_{i,Tx}$ and $P_{i,Rx}$ with $i \in \{A, R, B\}$ indicate the power of the transmitter and receiver circuit, respectively. Assuming that Alice, Bob, and Relay all use the same transceiver hardware, which means that the transceiver at either nodes shares the same power with others, it follows that $P_{i,Tx} = P_{Tx}$ and $P_{i,Rx} = P_{Rx}$ for $i \in \{A, R, B\}$. Then, from Formulas (36) and (38), the zero-outage secrecy energy efficiency can be rewritten as

$$\xi = \frac{\eta}{(2N+1)P_{Tx} + (N+3)P_{Rx} + 3P/\mu}. \tag{38}$$

8. Numerical Results

For this section, a simulation was carried out, to support what we have been discussing. MATLAB was used as the simulating tool and we used version R2019b. The simulation was run in the scenario of GSM-1900 in a cellular environment with the path loss model of $3.45 + 3.8 \times \log_{10}(d_{ij})$ [20], where d_{ij} in meters was the distance between nodes j and j, and the channel variance was then obtained by $\sigma^2_{i,j} = 10^{-(3.45+3.8\times\log_{10}(d_{ij}))}$.

The power consumption at the transmitter and at the receiver was $P_{Rx} = 240$ mW and $P_{Tx} = 360$ mW, respectively, and the amplifying coefficient $\mu = 0.4$ [27]. The noise variance was obtained from $\sigma_n^2 = N_f N_0 BW$, where the noise figure N_f had a value of 3 dB, the power density of the background noise N_0 was about -174 dBm per Hertz, and the bandwidth BW was equal to 200 KHz for GSM-1900.

The zero-outage secrecy spectral efficiency is illustrated in Figure 7, with respect to the portion of the power, α, that was used to transmit the message for distinguished values of Alice's transmit power in the case that the distances between Relay and Alice and Relay and Bob were both 1 km. One can see that the higher the transmit power was, the significantly higher ZOSSE it could obtain. In addition, there existed an optimal α, to maximize ZOSSE.

Figure 8 illustrates the maximum zero-outage secrecy spectral efficiency, with respect to the transmit power according to the location of Alice and Bob compared to Relay, in the case that the sum of d_{RA} and d_{RB} was 2 km. It can be seen that, if either Alice or Bob was placed near Relay, while the other was placed far away, the ZOSSE was nearly zero. This was because the transmission reliability of the far-distance link was low. It can also be seen that if the location of the relay was set properly in the middle of the transceiver, the ZOSSE was maximized, which was because the minimum connection outage probability was achieved.

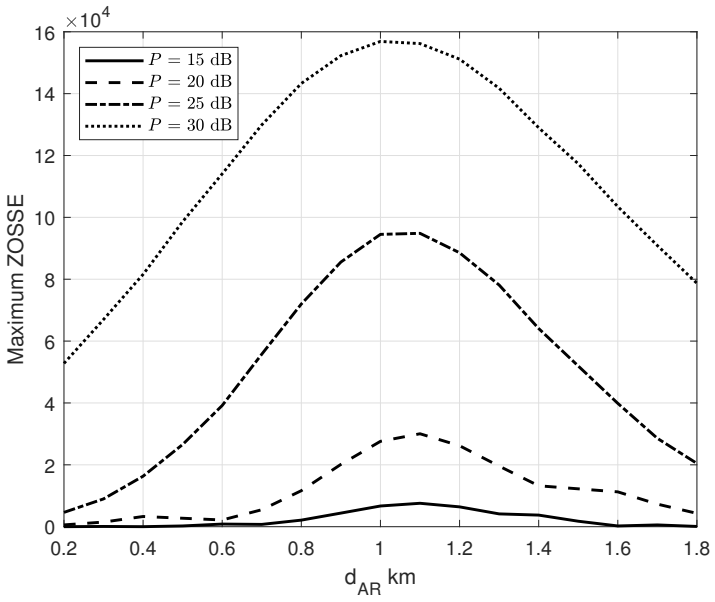

Figure 8. Maximum zero-outage secrecy spectral efficiency, η, versus d_{AR} for different P; $d_{AR} + d_{RB} =$ 2 Km.

Figures 9 and 10 illustrate the zero-outage secrecy energy efficiency with respect to Alice's transmit power P and Relay's number of antennas N when the optimum P to maximize the ZOSEE was chosen. It can be seen in Figure 9 that there existed an optimum transmit power at which the ZOSEE was maximized. When the optimum transmit power was chosen, the ZOSEE went up with the increasing number of antennas at Relay, as seen in Figure 10.

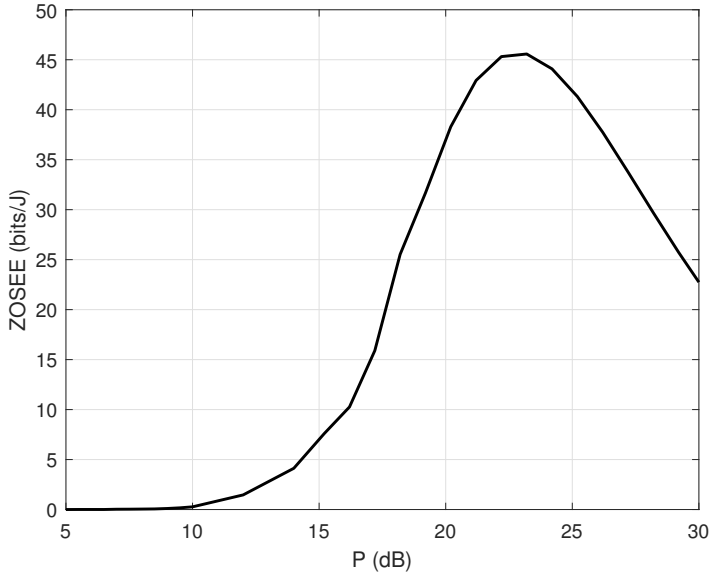

Figure 9. Zero-outage secrecy energy efficiency ξ versus the transmit power P; $N = 1$ and $d_{AR} = d_{RB} = 1$ Km.

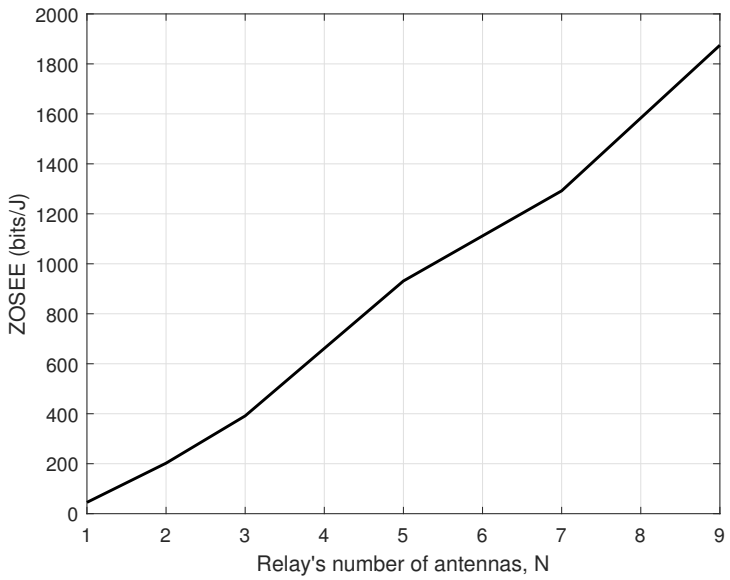

Figure 10. Zero-outage secrecy energy efficiency ξ versus Relay's number of antennas N when the optimum P is chosen; $d_{AR} = d_{RB} = 1$ Km.

9. Conclusions and Discussion

This paper used the artificial noise strategy and avoided CSI leakage, to design a three-phase decode-and-forward relaying system that ensures positive zero-outage secrecy. The paper described in detail the codeword pair design to achieve zero-outage secrecy regardless of how powerful the eavesdropper is, which is illustrated via the region of rate where the secrecy outage probability is zero. Then, the paper characterized the positive zero-outage secrecy spectral efficiency, which cannot be achieved in the literature, and the resulting energy efficiency. The numerical results showed that the secrecy outage probability can always be zero no matter where the eavesdropper is or how many antennas it has. This is because the AN is sent in the same space as the secure message, and the eavesdropper cannot cancel it out, which limits the eavesdropper's SNR and capacity to achieve zero-outage secrecy. The numerical results also showed that the zero-outage

secrecy spectral efficiency increases with increasing transmit power and that both the spectral efficiency and the energy efficiency of the zero-outage secrecy are highest when the relay is placed in the middle of the transmitter and receiver.

A physical layer of security is vital to guaranteeing secrecy, as it is the initial stage in protecting the confidentiality of information. To achieve a system that is always secure in any transmission, such as a credit card number or password transmission, the proposed system successfully guarantees security with probability 1 or zero-outage secrecy by a simple design consisting of an extra AN transmission along with a trick of pilot training, to prevent channel state information leakage to the eavesdropper. To confirm the potential application of the proposed design, our work will be extended to the finite blocklength regime. Also, this strategy of AN injection will be applied, to achieve zero-outage secrecy for multi-users in the scattered network.

Author Contributions: Formal analysis, H.Q.T. and N.B.T.N.; Investigation, H.Q.T. and N.B.T.N.; software, N.B.T.N.; Writing—original draft, H.Q.T. and K.H.-V.; Visualization, K.H.-V.; Writing—review and editing, H.O.; Supervision, H.O.; Funding acquisition, H.O. All authors have read and agreed to the published version of the manuscript.

Funding: This result was partially supported by "Regional Innovation Strategy (RIS)" through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (MOE) (2023RIS-003). It was also partially supported by Institute of Information & Communication Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (2020-0-00869, Development of 5G-based Shipbuilding & Marine Smart Communication Platform and Convergence Service).

Data Availability Statement: Data are contained within the article.

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

Appendix A

In this Appendix, we prove the PDF and CDF of the random variable Z in Formula (19). It follows from Formula (18) that

$$\begin{aligned} F_Z(z) &= \int_0^z p_Z(r)\,dr && \text{(A1)}\\ &= \mathbb{P}(Z < z) \\ &= \mathbb{P}\left(\frac{\alpha P|\mathbf{h}_{iE}|^2}{\sigma_n^2 + (1-\alpha)P|\mathbf{h}_{iE}|^2} < z\right) \\ &= \mathbb{P}\left(|\mathbf{h}_{iE}|^2 < \frac{z\sigma_n^2}{[\alpha - z(1-\alpha)]^+ P}\right) && \text{(A2)} \end{aligned}$$

for $i \in \{A, R\}$. As $|\mathbf{h}_{iE}|^2$ is chi-squared distributed with $2M$ degree of freedom and variance of $\sigma_{iE}^2/2$, we obtain the CDF of Z from (A2) as [20]

$$F_Z(z) = 1 - \Gamma\left(M, \frac{z\sigma_n^2}{(\alpha - z(1-\alpha))^+ P\sigma_{iE}^2}\right), \quad \text{(A3)}$$

which yields its PDF of

$$p_Z(z) = \frac{\alpha\sigma_n^2/\sigma_{iE}^2}{(M-1)!(\alpha-(1-\alpha)z)^2 P}\left(\frac{z\sigma_n^2}{(\alpha-(1-\alpha)z)P\sigma_{iE}^2}\right)^{M-1}\exp\left(-\frac{z\sigma_n^2}{(\alpha-(1-\alpha)z)P\sigma_{iE}^2}\right). \quad \text{(A4)}$$

References

1. Nicopolitidis, P.; Obaidat, M.S.; Papadimitriou, G.I.; Pomportsis, A.S. *Wireless Networks*; John Wiley & Sons: Hoboken, NJ, USA, 2003.
2. Karygiannis, T.; Owens, L. *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*; Technology Administration, US Department of Commerce, National Institute of Standard and Technology: Gaithersburg, MD, USA, 2002.

3. Shiu, Y.S.; Chang, S.Y.; Wu, H.C.; Huang, S.C.H.; Chen, H.H. Physical layer security in wireless networks: A tutorial. *IEEE Wirel. Commun.* **2011**, *18*, 66–74.
4. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011.
5. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
6. Liu, C.; Yang, N.; Yuan, J.; Malaney, R. Location-based secure transmission for wiretap channels. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 1458–1470. [CrossRef]
7. Goel, S.; Negi, R. Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
8. Zhou, X.; McKay, M.R. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3831–3842. [CrossRef]
9. Lv, L.; Ding, Z.; Ni, Q.; Chen, J. Secure MISO-NOMA transmission with artificial noise. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6700–6705. [CrossRef]
10. Hong, S.; Pan, C.; Ren, H.; Wang, K.; Nallanathan, A. Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. *IEEE Trans. Commun.* **2020**, *68*, 7851–7866. [CrossRef]
11. Xu, X.; Bessert, K.L.; Lin, P.H.; Jorswieck, E.A. Maximum Zero-Outage Secrecy Capacity of Fading Wiretap Channels with Finite Alphabets. In Proceedings of the 2023 57th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 22–24 March 2023 ; pp. 1–4.
12. Jorswieck, E.; Lin, P.H.; Besser, K.L. On the zero-outage secrecy-capacity of dependent fading wiretap channels. *Entropy* **2022**, *24*, 99. [CrossRef] [PubMed]
13. Aman, M.N.; Javaid, U.; Sikdar, B. A privacy-preserving and scalable authentication protocol for the internet of vehicles. *IEEE Internet Things J.* **2020**, *8*, 1123–1139. [CrossRef]
14. He, Y.; Wang, D.; Huang, F.; Zhang, R.; Gu, X.; Pan, J. A V2I and V2V collaboration framework to support emergency communications in ABS-aided Internet of Vehicles. *IEEE Trans. Green Commun. Netw.* **2023**, 1. [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. Verma, S.; Kaur, S.; Khan, M.A.; Sehdev, P.S. Toward green communication in 6G-enabled massive internet of things. *IEEE Internet Things J.* **2020**, *8*, 5408–5415. [CrossRef]
17. Zappone, A.; Jorswieck, E. Energy efficiency in wireless networks via fractional programming theory. *Found. Trends® Commun. Inf. Theory* **2015**, *11*, 185–396. [CrossRef]
18. Zappone, A.; Lin, P.H.; Jorswieck, E.A. Secrecy energy efficiency for MIMO single-and multi-cell downlink transmission with confidential messages. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2059–2073. [CrossRef]
19. Xiao, L.; Xu, Y.; Yang, D.; Zeng, Y. Secrecy energy efficiency maximization for UAV-enabled mobile relaying. *IEEE Trans. Green Commun. Netw.* **2019**, *4*, 180–193. [CrossRef]
20. Ta, H.Q.; Kim, S.W. Adapting rate and power for maximizing secrecy energy efficiency. *IEEE Commun. Lett.* **2017**, *21*, 2049–2052. [CrossRef]
21. He, B.; She, Y.; Lau, V.K. Artificial noise injection for securing single-antenna systems. *IEEE Trans. Veh. Technol.* **2017**, *66*, 9577–9581. [CrossRef]
22. Ta, H.Q.; Cao, T.L.; Ho-Van, K. Achievable Zero-Outage Secrecy Capacity Against Eavesdroppers with Unlimited Antennas and Arbitrary Location. In Proceedings of the 2022 International Conference on Advanced Technologies for Communications (ATC), Ha Noi, Vietnam, 20–22 October 2022; pp. 225–229.
23. Laneman, J.N.; Tse, D.N.; Wornell, G.W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Trans. Inf. Theory* **2004**, *50*, 3062–3080. [CrossRef]
24. Hassibi, B.; Hochwald, B.M. How much training is needed in multiple-antenna wireless links? *IEEE Trans. Inf. Theory* **2003**, *49*, 951–963. [CrossRef]
25. Zhou, X.; McKay, M.R.; Maham, B.; Hjørungnes, A. Rethinking the secrecy outage formulation: A secure transmission design perspective. *IEEE Commun. Lett.* **2011**, *15*, 302–304. [CrossRef]
26. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Elsevier: Amsterdam, The Netherlands; Academic Press: Cambridge, MA, USA, 2007.
27. 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, 11–15 June 2006; Volume 8, pp. 3783–3788.