entropy

MDPI

Article

Artificial Noise Injection and Its Power Loading Methods for Secure Space-Time Line Coded Systems

Jingon Joung [1], Jihoon Choi [2], Bang Chul Jung [3] and Sungwook Yu [1,*]

1 School of Electrical and Electronics Engineering, Chung-Ang University, Seoul 06974, Korea; jgjoung@cau.ac.kr
2 School of Electronics and Information Engineering, Korea Aerospace University, Gyeonggi-do 10540, Korea; jihoon@kau.ac.kr
3 Department of Electronics Engineering, Chungnam National University, Daejeon 34134, Korea; bcjung@cnu.ac.kr
* Correspondence: sungwook@cau.ac.kr; Tel.: +82-2-820-5740

Received: 4 May 2019; Accepted: 20 May 2019; Published: 22 May 2019

Abstract: In this paper, we consider a 2×2 space-time line coded (STLC) system having two-transmit and two-receive antennas. To improve the secrecy rate of the STLC system, in which an illegitimate receiver eavesdrops the information delivered from the STLC transmitter to the STLC receiver, we propose an artificial noise (AN) injection method. By exploiting the STLC structure, a novel AN for the STLC is designed and its optimal power loading factor is derived. Numerical results verify that the proposed secure STLC systems with the designed AN injection and the power control method can significantly improve the secrecy rate compared to the conventional STLC systems. It is observed that the proposed method is more effective if there is a significant gap between the main-channel and the eavesdropper-channel gains.

Keywords: space-time line code; physical layer security; secrecy rate; artificial noise; power control

1. Introduction

For secure wireless communications, along with cryptographic encryption on an application layer, physical-layer security (PLS) technologies [1–3] have been attracting intensive research interest from various fields with numerous successful applications, such as wireless power transmission systems [4,5], massive multi-input multi-output (MIMO) systems [6,7], millimeter wave systems [8], and unmanned aerial vehicle systems [9–12]. Contrary to an anti-jamming scheme that intends to remove the jamming signals from the received signals [13,14], i.e., the data protection from the jammer's attack, the PLS technologies are mainly focused on the data protection from being eavesdropped by the eavesdropper. Various practical PLS techniques, such as the precoding/beamforming schemes [15,16], the cooperation methods [17–20], the secrecy-achieving codes [21–23], and artificial noise (AN) injection [24–29], have been studied. Among these, the AN injection methods have been vigorously studied due to their simplicity and effectiveness. By adding AN to the transmitted signals at a transmitter (i.e., Alice), the secrecy capacity can be significantly improved as the AN affects as an interference only on an eavesdropper (i.e., Eve), not a legitimate user (i.e., Bob). In [27,28], an AN was designed for a secure space-time block coded (STBC) system to improve the secrecy rate of the STBC systems.

In this paper, we consider a two-antenna secure system, in which all devices including Alice, Bob, and Eve have two antennas. Following a vast majority of studies (see [30] and the references therein), both the main and the eavesdropper channels are assumed to be available at Alice. Nevertheless, Eve's channel cannot be nullified due to the lack of spatial degrees of freedom. Furthermore,

no nullspace of the main (Bob's) channel exists without any receive-combining technique. Thus, we employed a space-time line code (STLC) scheme in [31], which is a dual transmission scheme of space-time block code [32]. The STLC scheme has been applied to various communication systems, e.g., the multiuser systems [33,34], two-way relay systems [35,36], antenna shuffling systems [37], and blind decoding systems [38]. Here, channel state information (CSI) is assumed to be available at the transmitter under the assumption that the uplink and downlink channels are symmetric in time-division duplex (TDD) mode. Assuming the TDD mode in a two-antenna secure system considered in this paper, the channels from Bob to Alice are symmetric with the channels from Alice to Bob. Hence, the legitimate downlink channels (Bob's channel) can be obtained by estimating the uplink channels at Alice. Since STLC can achieve full spatial diversity gain with a single transmit antenna, the other transmit antenna can be utilized to generate AN. The AN is designed such that it is perfectly canceled out after decoding the STLC symbols at Bob, and its optimal power loading factor is then designed to maximize the secrecy rate, i.e., a sort of resource management scheme [34,36,39]. Furthermore, the STLC schemes can be implemented with full-blind (non-coherent) detection at the legitimate receiver [38], and the transmitter does not need to transmit long-training sequences, which also improve the secrecy rate of the network as this hinders the eavesdroppers from estimating their own channels. Numerical results verify that the designed power loading strategy maximizes the secrecy rate, and the proposed secure STLC with the power controlled AN can significantly improve PLS of the 2×2 STLC systems.

Notations: Superscripts T and $*$ denote transposition and complex conjugate, respectively, for any scalar, vector, or matrix. The notations $|x|$ and $\|\boldsymbol{x}\|$ denote the absolute value of x and the norm of a vector $\boldsymbol{x}$, respectively; null$(\boldsymbol{X})$ gives the span of the nullspace of $\boldsymbol{X}$; and $x \sim \mathcal{CN}(0, \sigma^2)$ means that a complex random variable x conforms to a normal distribution with a zero mean and variance σ^2. $\mathrm{E}[x]$ stands for the expectation of a random variable x.

2. Proposed 2×2 Secure STLC with AN

Consider an STLC system as shown in Figure 1, in which Alice sends two information symbols, x_1 and x_2, through two consecutive transmissions to Bob. Here, Eve eavesdrops the information. All devices are assumed to have two antennas, i.e., two 2×2 STLC systems, and without loss of generality, $\mathrm{E}[|x|^2] = 1$. Let $s_{m,t}$ be an STLC symbol that is transmitted through the m^{th} transmit antenna at time t, where $m, t \in \{1, 2\}$. Denote AN by $z \sim \mathcal{CN}(0, 1)$ and its complex-value weight by $a_{m,t}$ such that:

$$\mathrm{E}\left[|a_{1,1}|^2 + |a_{2,1}|^2 + |a_{1,2}|^2 + |a_{2,2}|^2\right] = 2. \tag{1}$$

The proposed secure STLC symbols with AN are then written as follows:

$$s_{1,1} = \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h_{1,1}^* x_1 + h_{2,1}^* x_2^*\right) + \sqrt{\alpha} a_{1,1} z, \tag{2a}$$

$$s_{1,2} = \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h_{2,1}^* x_1^* - h_{1,1}^* x_2\right) + \sqrt{\alpha} a_{1,2} z^*, \tag{2b}$$

$$s_{2,1} = \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h_{1,2}^* x_1 + h_{2,2}^* x_2^*\right) + \sqrt{\alpha} a_{2,1} z, \tag{2c}$$

$$s_{2,2} = \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h_{2,2}^* x_1^* - h_{1,2}^* x_2\right) + \sqrt{\alpha} a_{2,2} z^*, \tag{2d}$$

where $h_{n,m} \sim \mathcal{CN}(0, 1)$ represents the channel gain from the m^{th} transmit antenna of Alice to the n^{th} receive antenna of Bob;

$$\gamma = |h_{1,1}|^2 + |h_{2,1}|^2 + |h_{1,2}|^2 + |h_{2,2}|^2 \tag{3}$$

is for the transmit power normalization such that:

$$\mathrm{E}\left[|s_{1,1}|^2+|s_{2,1}|^2+|s_{1,2}|^2+|s_{2,2}|^2\right]=2; \tag{4}$$

and α is the power loading factor for the AN signals, where $0 \leq \alpha \leq 1$. According to the AN-power loading factor, α, three operation modes can be considered as follows:

- $\alpha = 0$: a conventional STLC mode without AN [31,33],
- $0 < \alpha < 1$: a secure STLC mode with AN,
- $\alpha = 1$: a jamming mode without data transmission.

Herein, we focus on the secure STLC mode in this letter.

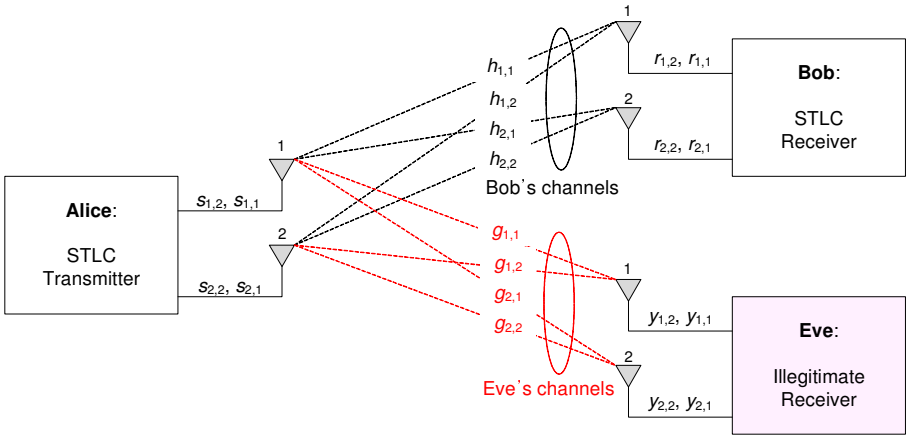

Figure 1. The 2×2 secure space-time line coded (STLC) system model, with a transmitter (Alice) and legitimate receiver (Bob). Here, one eavesdropper (Eve) eavesdrops actively.

Denoting $r_{n,t}$ as the received signal at antenna n of Bob at time t, the four received signals are then written as follows ($n, t \in \{1,2\}$):

$$r_{n,t} = h_{n,1}s_{1,t} + h_{n,2}s_{2,t} + v_{n,t}, \tag{5}$$

where $v_{n,t} \sim \mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise at $r_{n,t}$.

The received symbols $r_{1,1}$ and $r_{2,2}$ in Equation (5) are directly combined to obtain the estimate of x_1 and x_2, which are derived by using Equations (2)–(5) as follows:

$$\begin{aligned}
\tilde{x}_1 &= r_{1,1} + r_{2,2}^* && \text{(6a)}\\
&= h_{1,1}s_{1,1} + h_{1,2}s_{2,1} + v_{1,1} + h_{2,1}^*s_{1,2}^* + h_{2,2}^*s_{2,2}^* + v_{2,2}^* && \text{(6b)}\\
&= h_{1,1}\left(\sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h_{1,1}^*x_1 + h_{2,1}^*x_2^*\right) + \sqrt{\alpha}a_{1,1}z\right)\\
&\quad + h_{1,2}\left(\sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h_{1,2}^*x_1 + h_{2,2}^*x_2^*\right) + \sqrt{\alpha}a_{2,1}z\right)\\
&\quad + h_{2,1}^*\left(\sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h_{2,1}^*x_1^* - h_{1,1}^*x_2\right) + \sqrt{\alpha}a_{1,2}z^*\right)^*\\
&\quad + h_{2,2}^*\left(\sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h_{2,2}^*x_1^* - h_{1,2}^*x_2\right) + \sqrt{\alpha}a_{2,2}z^*\right)^* + v_{1,1} + v_{2,2}^* && \text{(6c)}\\
&= \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(|h_{1,1}|^2x_1 + h_{1,1}h_{2,1}^*x_2^* + |h_{1,2}|^2x_1 + h_{1,2}h_{2,2}^*x_2^*\right) + \sqrt{\alpha}\left(h_{1,1}a_{1,1} + h_{1,2}a_{2,1}\right)z\\
&\quad + \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(|h_{2,1}|^2x_1 - h_{1,1}h_{2,1}^*x_2^* + |h_{2,2}|^2x_1 - h_{1,2}h_{2,2}^*x_2^*\right) + \sqrt{\alpha}\left(h_{2,1}^*a_{1,2}^* + h_{2,2}^*a_{2,2}^*\right)z\\
&\quad + v_{1,1} + v_{2,2}^* && \text{(6d)}
\end{aligned}$$

$$= \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\gamma x_1 + \sqrt{\alpha}\left(h_{1,1}a_{1,1} + h_{1,2}a_{2,1} + h^*_{2,1}a^*_{1,2} + h^*_{2,2}a^*_{2,2}\right) z + v_1, \tag{6e}$$

$$= \sqrt{1-\alpha}\sqrt{\gamma}\, x_1 + \sqrt{\alpha}\left(h_{1,1}a_{1,1} + h_{1,2}a_{2,1} + h^*_{2,1}a^*_{1,2} + h^*_{2,2}a^*_{2,2}\right) z + v_1, \tag{6f}$$

where the first, second, and third terms of the right-hand side (RHS) of Equation (6f) are the intended signal, the interferences caused by AN, and the combined noise $v_1 = v_{1,1} + v^*_{2,2} \sim \mathcal{CN}(0, 2\sigma^2)$, respectively.

Similarly, combining $r_{1,2}$ and $r_{2,1}$ in Equation (5), the estimate of x_2 is obtained as follows:

$$\tilde{x}_2 = r^*_{2,1} - r_{1,2} \tag{7a}$$

$$= h^*_{2,1}s^*_{1,1} + h^*_{2,2}s^*_{2,1} + v^*_{2,1} - h_{1,1}s_{1,2} - h_{1,2}s_{2,2} - v_{1,2} \tag{7b}$$

$$\begin{aligned} = {} & h^*_{2,1}\left(\sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h^*_{1,1}x_1 + h^*_{2,1}x^*_2\right) + \sqrt{\alpha}a_{1,1}z\right)^* \\ & + h^*_{2,2}\left(\sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h^*_{1,2}x_1 + h^*_{2,2}x^*_2\right) + \sqrt{\alpha}a_{2,1}z\right)^* \\ & - h_{1,1}\left(\sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h^*_{2,1}x^*_1 - h^*_{1,1}x_2\right) + \sqrt{\alpha}a_{1,2}z^*\right) \\ & - h_{1,2}\left(\sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h^*_{2,2}x^*_1 - h^*_{1,2}x_2\right) + \sqrt{\alpha}a_{2,2}z^*\right) + v^*_{2,1} - v_{1,2} \end{aligned} \tag{7c}$$

$$\begin{aligned} = {} & \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(h^*_{2,1}h_{1,1}x^*_1 + |h_{2,1}|^2x_2 + h^*_{2,2}h_{1,2}x^*_1 + |h_{2,2}|^2x_2\right) + \sqrt{\alpha}\left(h^*_{2,1}a^*_{1,1} + h^*_{2,2}a^*_{2,1}\right) z^* \\ & + \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\left(-h_{1,1}h^*_{2,1}x^*_1 + |h_{1,1}|^2x_2 - h_{1,2}h^*_{2,2}x^*_1 + |h_{1,2}|^2x_2\right) - \sqrt{\alpha}\left(h_{1,1}a_{1,2} + h_{1,2}a_{2,2}\right) z^* \\ & + v_{1,1} + v^*_{2,2} \end{aligned} \tag{7d}$$

$$= \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\gamma x_2 + \sqrt{\alpha}\left(h^*_{2,1}a^*_{1,1} + h^*_{2,2}a^*_{2,1} - h_{1,1}a_{1,2} - h_{1,2}a_{2,2}\right) z^* + v_2, \tag{7e}$$

$$= \sqrt{1-\alpha}\sqrt{\gamma}\, x_2 + \sqrt{\alpha}\left(h^*_{2,1}a^*_{1,1} + h^*_{2,2}a^*_{2,1} - h_{1,1}a_{1,2} - h_{1,2}a_{2,2}\right) z^* + v_2, \tag{7f}$$

where the first, second, and third terms of the RHS of Equation (7f) are the intended signal, the interferences caused by AN, and the combined noise $v_2 = v^*_{2,1} - v_{1,2} \sim \mathcal{CN}(0, 2\sigma^2)$.

To eliminate the AN effects on Bob perfectly, the second terms in the RHS of Equations (6f) and (7f) should be a zero as follows:

$$h_{1,1}a_{1,1} + h_{1,2}a_{2,1} + h^*_{2,1}a^*_{1,2} + h^*_{2,2}a^*_{2,2} = 0 \tag{8a}$$

$$h^*_{2,1}a^*_{1,1} + h^*_{2,2}a^*_{2,1} - h_{1,1}a_{1,2} - h_{1,2}a_{2,2} = 0. \tag{8b}$$

Therefore, the AN weights, $\{a_{m,t}\}$, should fulfill the following conditions, which are a matrix and vector representation of Equation (8):

$$\begin{bmatrix} h_{1,1} & h^*_{2,1} & h_{1,2} & h^*_{2,2} \\ h_{2,1} & -h^*_{1,1} & h_{2,2} & -h^*_{1,2} \end{bmatrix} \begin{bmatrix} a_{1,1} \\ a^*_{1,2} \\ a_{2,1} \\ a^*_{2,2} \end{bmatrix} = \boldsymbol{H}\boldsymbol{a} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \tag{9}$$

From Equation (9), the AN weights are obtained as follows:

$$\boldsymbol{a} = \sqrt{2}\,\mathrm{null}(\boldsymbol{H}) \in \mathbb{C}^{4\times 1}, \tag{10}$$

where $\mathrm{null}(\boldsymbol{H})$ gives the span of the nullspace of a matrix $\boldsymbol{H}$, which is a 4×1 unit-norm vector, and thus, $|a_{1,1}|^2 + |a_{2,1}|^2 + |a_{1,2}|^2 + |a_{2,2}|^2 = 2$. Using Equations (6f), (7f) and (10), the combined STLC signals turn into the interference-free estimates as:

$$\tilde{x}_i = \sqrt{1-\alpha}\sqrt{\gamma}\, x_i + v_i,\ i \in \{1,\ 2\}. \tag{11}$$

Noting that x_1 and x_2 are not coupled with each other in Equation (11), two separate maximum-likelihood detections can be applied to detect x_1 and x_2 independently. Here, the detection signal-to-noise (SNR) is readily derived as:

$$\rho_{\text{Bob}} = \frac{(1-\alpha)\gamma}{2\sigma^2}. \tag{12}$$

From Equation (12), we verify that the secure STLC achieves performance identical to that of the conventional STLC and STBC in terms of the spatial diversity gain.

As we extend the number of transmit antennas from two to M, where M is an even number for simple derivation, which is not a necessary condition of M in practice, the AN effects on Bob Equation (8) can be generally written as follows:

$$\sum_{m=1}^{M} \left(h_{1,m} a_{1,m} + h_{2,m}^* a_{2,m}^* \right) = 0 \tag{13a}$$

$$\sum_{m=1}^{M} \left(h_{2,m}^* a_{1,m}^* - h_{1,m} a_{2,m} \right) = 0. \tag{13b}$$

Thus, the AN weights, $\{a_{m,t}\}$, should fulfill the following conditions:

$$\begin{bmatrix} h_{1,1} & h_{2,1}^* & \cdots & h_{1,m} & h_{2,m}^* & \cdots & h_{1,M} & h_{2,M}^* \\ h_{2,1} & -h_{1,1}^* & \cdots & h_{2,m} & -h_{1,m}^* & \cdots & h_{2,M} & -h_{1,M}^* \end{bmatrix} \boldsymbol{a} = \boldsymbol{H}\boldsymbol{a} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \tag{14}$$

where:

$$\boldsymbol{a} = \begin{bmatrix} a_{1,1} & a_{1,2}^* & \cdots & a_{2,m} & a_{2,m}^* & \cdots & a_{1,M} & a_{1,M}^* \end{bmatrix}^T. \tag{15}$$

From this, the AN weights are obtained as follows:

$$\boldsymbol{a} = \sqrt{M}\, \text{null}(\boldsymbol{H}) \in \mathbb{C}^{2M \times 1}. \tag{16}$$

The computational complexity to design AN for M transmit antenna STLC systems, i.e., $M \times 2$ STLC systems, is roughly $\mathcal{O}\left((2M)^3\right) = \mathcal{O}(M^3)$. Since the computational complexity to design a power control factor α, which is shown in the next section, is lower than that for the AN design, the total computational complexity of the proposed method is $\mathcal{O}(M^3)$.

3. Power Control for AN

Denote Eve's channel gain between the m^{th} transmit antenna of Alice and the n^{th} receive antenna of Eve by $g_{m,n} \sim \mathcal{CN}(0,1)$. The received signal of Eve is then written as follows ($n, t \in \{1,2\}$):

$$y_{n,t} = g_{n,1} s_{1,t} + g_{n,2} s_{2,t} + w_{n,t}, \tag{17}$$

where $w_{n,t}$ is AWGN with the same variance as $v_{n,t}$, i.e., $w_{n,t} \sim \mathcal{CN}(0, \sigma^2)$. Suppose that Eve operates optimally for the coherent detection and successive inter-symbol-interference cancellation (SIC) with full CSI (FCSI) including $\{h_{n,m}\}$ and $\{g_{n,m}\}$. In other words, we consider the worst case scenario of the secure communications. After the perfect STLC combining and SIC procedure, Eve obtains the estimate of x_i as follows:

$$\begin{bmatrix} y_{1,1} + y_{2,2}* \\ y_{2,1} - y_{1,2}^* \end{bmatrix} = \sqrt{1-\alpha}\sqrt{\frac{1}{\gamma}}\boldsymbol{G}\boldsymbol{h}x_i + \sqrt{\alpha}\boldsymbol{G}\boldsymbol{a} + \begin{bmatrix} w_{1,1} + w_{2,2}^* \\ w_{2,,1} - w_{1,2}^* \end{bmatrix}, \tag{18}$$

where:

$$\boldsymbol{G} = \begin{bmatrix} g_{1,1} & g_{2,1}^* & g_{1,2} & g_{2,2}^* \\ g_{2,1} & -g_{1,1}^* & g_{2,2} & -g_{1,2}^* \end{bmatrix}, \tag{19a}$$

$$\boldsymbol{h} = \begin{bmatrix} h_{1,1}^* & h_{2,1} & h_{1,2}^* & h_{2,2} \end{bmatrix}^T. \tag{19b}$$

Note that Eve cannot cancel AN even with FCSI. Thus, the effective signal-to-interference-plus-noise ratio (SINR) of Eve is derived from Equation (18) as follows:

$$\rho_{\text{Eve}} = \frac{(1-\alpha)\epsilon_h}{\gamma\left(4\sigma^2 + \alpha\epsilon_a\right)}, \tag{20}$$

where the effective Eve channel gain and AN are defined as:

$$\epsilon_h \triangleq \|\boldsymbol{G}\boldsymbol{h}\|^2, \tag{21}$$

$$\epsilon_a \triangleq \|\boldsymbol{G}\boldsymbol{a}\|^2. \tag{22}$$

From Equations (12) and (20), it is clear that the SNR of Bob and the SINR of Eve are the functions of a power loading factor, α. Consequently, for the given channels, the worst-case instantaneous secrecy rate is defined as a function of α as:

$$R(\alpha) \triangleq \left[\log_2\left(1+\rho_{\text{Bob}}\right) - \log_2\left(1+\rho_{\text{Eve}}\right)\right]^+, \tag{23}$$

where $[x]^+ = \max(x, 0)$.

We now design α^o, which maximizes the worst-case secrecy rate $R(\alpha)$ as follows:

$$\alpha^o = \max_{0\le\alpha\le 1} \left[\log_2 \frac{1+\rho_{\text{Bob}}}{1+\rho_{\text{Eve}}}\right]^+. \tag{24}$$

The equivalent objective function of Equation (24) can be derived as follows:

$$\begin{aligned} \left[\log_2 \frac{1+\rho_{\text{Bob}}}{1+\rho_{\text{Eve}}}\right]^+ &\overset{(a)}{\equiv} \frac{1+\rho_{\text{Bob}}}{1+\rho_{\text{Eve}}} \\ &= \frac{1+\frac{(1-\alpha)\gamma}{2\sigma^2}}{1+\frac{(1-\alpha)\epsilon_h}{\gamma(4\sigma^2+\alpha\epsilon_a)}} \\ &= \frac{\left(4\sigma^2+\epsilon_a\alpha\right)\left(2\sigma^2+\gamma^2-\gamma^2\alpha\right)}{8\sigma^4\gamma + 2\sigma^2\epsilon_h + 2\sigma^2(\epsilon_a\gamma-\epsilon_h)\alpha} \\ &\triangleq D(\alpha), \end{aligned} \tag{25}$$

where (a) comes from the facts that the secure communication is feasible, i.e., $\rho_{\text{Bob}} > \rho_{\text{Eve}}$, and $\log_2(\cdot)$ is a monotonically-increasing function.

Since the convexity of the objective function $D(\alpha)$ in Equation (25) with respect to α depends on the system parameters, namely σ^2, γ, ϵ_h, and ϵ_a, to find the optimal α^o, we have to check the critical points including two boundary points 0 and 1. To find the critical point of α' between 0 and 1, we relax the feasible reason of α to the entire real values and derive α' from the first-order optimality condition, i.e.,

$$\begin{aligned} \frac{\partial D(\alpha)}{\partial\alpha} &= \frac{(4\sigma^2+2\sigma^2\epsilon_a+\epsilon_a)\gamma^2+2\sigma^2\epsilon_a\gamma}{8\sigma^2\gamma+2\sigma^2\epsilon_h} - \frac{(\epsilon_a\gamma-\epsilon_h)(4\sigma^2+\epsilon_a\alpha)(2\sigma^2\gamma+\gamma^2-\gamma^2\alpha)}{(4\sigma^2\gamma+\epsilon_h+(\epsilon_a\gamma-\epsilon_h)\alpha)^2} \\ &= 0. \end{aligned} \tag{26}$$

By solving Equation (26) with respect to α, we can obtain the critical point α' as follows:

$$\alpha' = \begin{cases} \frac{\epsilon_a - 4\sigma^2}{2\epsilon_a} + \frac{\sigma^2}{\gamma}, & \text{if } \gamma = \frac{\epsilon_h}{\epsilon_a} \\ \frac{\sqrt{\epsilon_a \epsilon_h c(c\gamma^3 + 2\sigma^2(\epsilon_a\gamma - \epsilon_h\sigma^2)\gamma)} - \epsilon_a\gamma(4\sigma^2\gamma + \epsilon_h)}{\epsilon_a(\epsilon_a\gamma - \epsilon_a)\gamma}, & \text{else if } \gamma \geq \gamma_t \\ \text{infeasible}, & \text{otherwise}, \end{cases} \tag{27}$$

where:

$$c = \epsilon_a + 4\sigma^2 \tag{28a}$$

$$\gamma_t = \frac{\sqrt{\epsilon_a^2 + 2\epsilon_a\epsilon_h + 8\sigma^2\epsilon_h} - \sigma^2\epsilon_a}{\epsilon_a + 4\sigma^2}. \tag{28b}$$

We can then obtain the optimal α^o by considering the feasible region of α' and two boundaries of α, namely 0 and 1, as follows:

$$\alpha^o = \begin{cases} 0, & \text{if } \alpha' < 0, \\ 1, & \text{if } \alpha' > 1, \\ \alpha', & \text{otherwise} \end{cases} \tag{29}$$

From Equation (29), the interesting remarks, which can be a guideline to design the AN power loading factor, are obtained as follows:

Remark 1. *As the channel quality between Alice and Bob becomes better, i.e., γ increases, more power is allocated to the intended signals, i.e., α decreases, to further exploit the good quality of the main channels.*

Remark 2. *As the quality of the eavesdropper channel between Eve and Alice becomes better, i.e., ϵ_a and ϵ_h increase, more power is allocated to the AN signals, i.e., α increases, to hinder Eve from eavesdropping.*

The remarks are intuitively reasonable. If Eve's channel is dominant, more power is allocated to AN as it is more efficient for the secrecy rate improvement to reduce Eve's rate, i.e., the second term inside the brackets in Equation (23). On the other hand, if Bob's channel is dominant, more power is allocated to the intended signals as it is more efficient for the secrecy rate improvement to increase Bob's rate, i.e., the first term inside the brackets in Equation (23). The remarks are verified through the simulation results in Figure 2. Figure 2 shows the optimal power loading factor α^o for AN, according to γ and ϵ, where we set $\epsilon_a = \epsilon_h = \epsilon$ and $\sigma^2 = 0.1$. For varying γ, we set $\epsilon = 8$, while for varying ϵ, we set $\gamma = 4$. From these results, we clearly observe that the optimal AN power increased as ϵ increased or as γ decreased, as stated in Remarks 1 and 2.

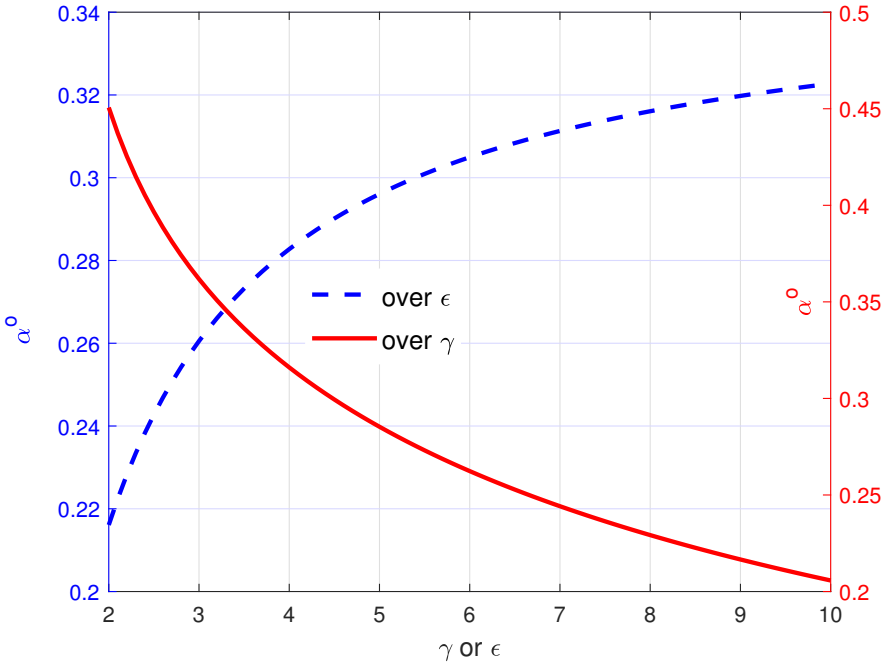

Figure 2. Optimal power loading factor α^o for artificial noise (AN) over γ when $\epsilon_a = \epsilon_h = \epsilon = 8$ and $\sigma^2 = 0.1$ and over ϵ when $\gamma = 4$ and $\sigma^2 = 0.1$.

Numerical results verifying the optimality of α^o in Equation (29) are shown in Figure 3. As observed in Figure 3, α^o achieved the maximum of the equivalent cost function $D(\alpha)$ in Equation (25) in the feasible region; as a result, the designed α^o in Equation (29) provided the maximum secrecy rate.

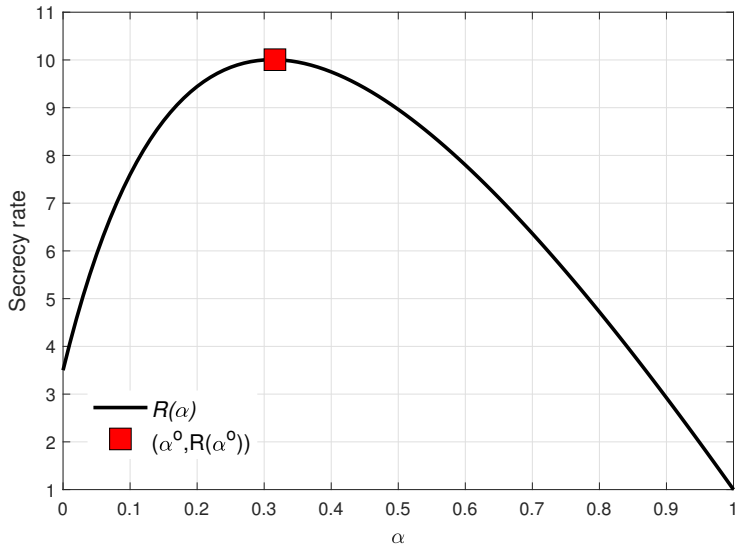

Figure 3. Secrecy rate $R(\alpha)$ over α when $\epsilon = 8$, $\gamma = 4$, and $\sigma^2 = 0.1$.

4. Numerical Results

In this section, we compare the proposed secure STLC with AN and the conventional STLC without AN. In Figure 4, the secrecy rate in Equation (23) has been evaluated over Eve's channel quality ϵ when $\gamma = 4$ and $\sigma^2 = 0.1$. Obviously, the secrecy rate decreased as ϵ increased. However, the secrecy rate's decrease of the speed of the proposed secure STLC was relatively moderate compared to that of the conventional STLC. From the results, we see that the proposed secure STLC always

outperformed the conventional STLC; especially, Eve's channel gain was relatively stronger than Bob's channel gain.

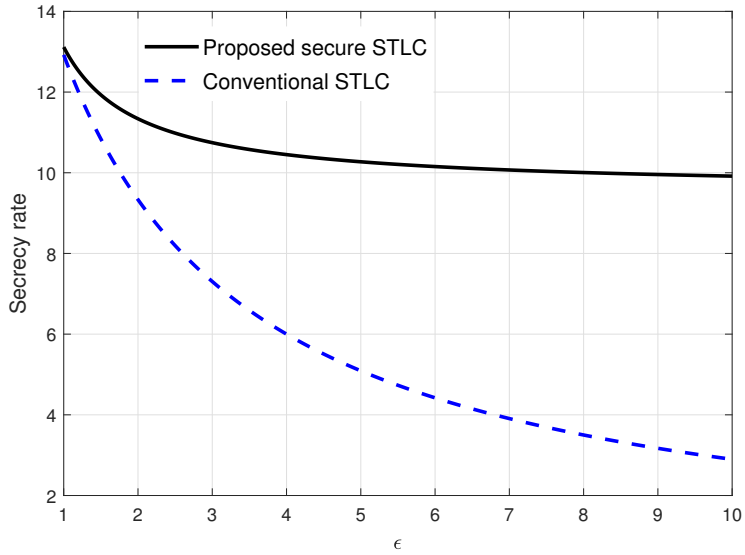

Figure 4. Secrecy rate evaluation results over Eve's channel quality ϵ when $\gamma = 4$ and $\sigma^2 = 0.1$.

In Figure 5, the secrecy rate in Equation (23) was evaluated over Bob's channel quality γ when $\epsilon = 8$ and $\sigma^2 = 0.1$. Obviously, the secrecy rate increased as γ increased. Here, the secrecy rate's increase of the speed of the proposed secure STLC was relatively faster compared to the conventional STLC. From the results, we see that the proposed secure STLC always outperformed the conventional STLC; especially, Bob's channel gain was relatively stronger than Bob's channel gain.

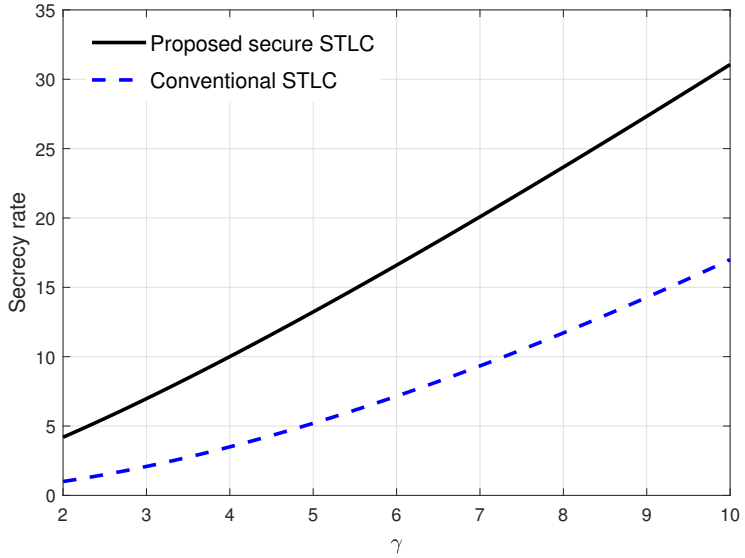

Figure 5. Secrecy rate evaluation results over Bob's channel quality γ when $\epsilon = 8$ and $\sigma^2 = 0.1$.

From the results in Figures 4 and 5, it is verified that the proposed secure STLC system with AN always outperformed the conventional STLC system, i.e., $R(\alpha^o) > R(0)$. Especially, when the main and eavesdropper channels were highly asymmetric, i.e., one channel gain was relatively stronger than the other one, the proposed secure STLC system could significantly improve the secrecy rate compared to the conventional STLC system.

In Figure 6, the secrecy rate was evaluated over noise variance σ^2. As expected, the secrecy rate decreased as σ^2 increased, and both secrecy rates of the proposed secure STLC and the conventional STLC were merged at the low secrecy rate as both Bob and Eve achieved very low rates. From the results, we see that the proposed AN with power control played a crucial role in the secure communication, especially in the high system SNR regime.

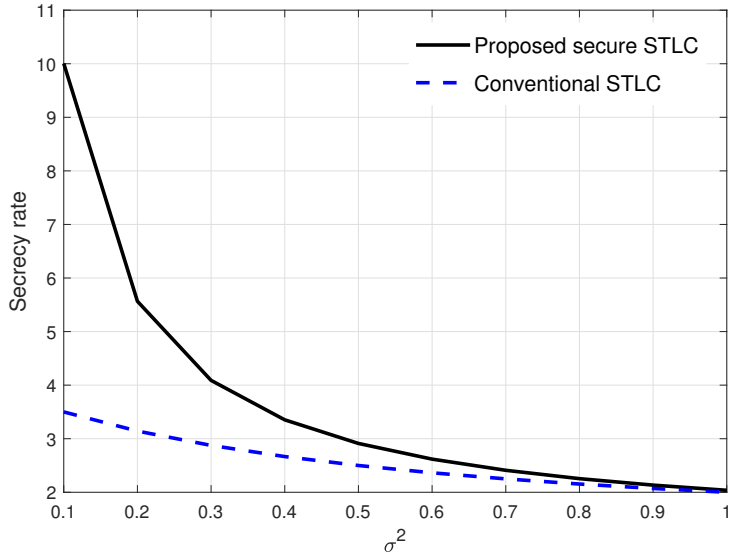

Figure 6. Secrecy rate evaluation results over noise power when $\gamma = 4$ and $\epsilon = 8$.

5. Conclusions

In this paper, we have designed artificial noise and its optimal power loading factor to improve the secrecy rate of a 2×2 space-time line code (STLC) system. The proposed secure STLC systems can significantly improve the secrecy rate of the conventional STLC system, as verified by the numerical results.

Author Contributions: Conceptualization, J.J. and J.C.; methodology, J.C.; software, J.J.; validation, J.J. and J.C.; investigation, J.C. and B.C.J.; writing, original draft preparation, J.J.; writing, review and editing, B.C.J. and S.Y.; visualization, J.J.; supervision, J.J.; project administration, J.J.; funding acquisition, J.J.

Funding: This research was supported in part by the Chung-Ang University Research Grants in 2019 and in part by the National Research Foundation of Korea (NRF) Grant 2018R1A4A1023826 funded by the Korean government (MSIT).

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

References

1. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
2. Leung-Yan-Cheong, S.K.; Hellman, M.E. The Gaussian Wire-Tap Channel. *IEEE Trans. Inf. Theory* **1978**, *IT-24*, 451–456. [CrossRef]
3. Liu, Y.; Chen, H.H.; Wang, L. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 347–376. [CrossRef]
4. Zhang, J.; Yuen, C.; Wen, C.K.; Jin, S.; Wong, K.K.; Zhu, H. Large system secrecy rate analysis for SWIPT MIMO wiretap channels. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 74–85. [CrossRef]
5. Guo, C.; Liao, B.; Feng, D.; He, C.; Ma, X. Minimum secrecy throughput maximization in wireless powered secure communications. *IEEE Trans. Veh. Technol.* **2018**, *67*, 2571–2581. [CrossRef]
6. Zhu, J.; Schober, R.; Bhargava, V.K. Linear precoding of data and artificial noise in secure massive MIMO systems. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 2245–2261. [CrossRef]
7. Wu, Y.; Schober, R.; Ng, D.W.K.; Xiao, C.; Caire, G. Secure massive MIMO transmission with an active eavesdropper. *IEEE Trans. Inf. Theory* **2016**, *62*, 3880–3900. [CrossRef]

8. Zhu, Y.; Wang, L.; Wong, K.K.; Heath, R.W. Secure communications in millimeter wave Ad Hoc networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3205–3217. [CrossRef]
9. Zhu, Y.; Zheng, G.; Fitch, M. Secrecy rate analysis of UAV-enabled mmWave networks using Matérn hardcore point processes. *IEEE J. Select. Areas Commun.* **2018**, *36*, 1397–1409. [CrossRef]
10. Li, A.; Wu, Q.; Zhang, R. UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 181–184. [CrossRef]
11. Kang, H.; Joung, J.; Ahn, J.; Kang, J. Secrecy-aware altitude optimization for quasi-static UAV base station without eavesdropper location information. *IEEE Commun. Lett.* **2019**, *23*, 851–854. [CrossRef]
12. Tang, J.; Chen, G.; Coon, J.P. Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2019**. (early access article). [CrossRef]
13. Tseng, S.; Chen, Y.; Chiu, P.; Chi, H. Jamming resilient cross-layer resource allocation in uplink HARQ-based SIMO OFDMA video transmission systems. *IEEE Access* **2017**, *5*, 24908–24919. [CrossRef]
14. Dou, Z.; Si, G.; Lin, Y.; Wang, M. An adaptive resource allocation model with anti-jamming in IoT network. *IEEE Access* **2019**, *5*, 1–9. [CrossRef]
15. Geraci, G.; Al-nahari, A.Y.; Yuan, J.; Collings, I.B. Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation. *IEEE Commun. Lett.* **2013**, *17*, 1164–1167. [CrossRef]
16. Zhang, J.; Yuen, C.; Wen, C.K.; Jin, S.; Gao, X. Ergodic secrecy sum-rate for multiuser downlink transmission via regularized channel inversion: Large system analysis. *IEEE Commun. Lett.* **2014**, *18*, 1627–1630. [CrossRef]
17. Fakoorian, S.A.A.; Swindlehurst, A.L. MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 640–649. [CrossRef]
18. Zheng, G.; Choo, L.C.; Wong, K.K. Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Trans. Signal Process.* **2011**, *59*, 1317–1322. [CrossRef]
19. Chen, X.; Zhong, C.; Yuen, C.; Chen, H.H. Multi-antenna relay aided wireless physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 40–46. [CrossRef]
20. Tran Tin, P.; The Hung, D.; Nguyen, T.N.; Duy, T.T.; Voznak, M. Secrecy performance enhancement for underlay cognitive radio networks employing cooperative multi-hop transmission with and without presence of hardware impairments. *Entropy* **2019**, *21*, 217. [CrossRef]
21. Thangaraj, A.; Dihidar, S.; Calderbank, A.; McLaughlin, S.; Merolla, J.M. Applications of LDPC codes to the wiretap channel. *IEEE Trans. Inf. Theory* **2007**, *53*, 2933–2945. [CrossRef]
22. Andersson, M.; Schaefer, R.; Oechtering, T.; Skoglund, M. Polar coding for bidirectional broadcast channels with common and confidential messages. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1901–1908. [CrossRef]
23. He, X.; Yener, A. Providing secrecy with structured codes: Two-user Gaussian channels. *IEEE Trans. Inf. Theory* **2014**, *60*, 2121–2138. [CrossRef]
24. Negi, R.; Goel, S. Secret communication using artificial noise. In Proceedings of the IEEE 62nd Vehicular Technology Conference, Dallas, TX, USA, 28 September 2005; pp. 1906–1910.
25. Goel, S.; Negi, R. Guaranteeing secrecy using artificial noise. *IEEE Trans. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
26. Mukherjee, A.; Swindlehurst, A.L. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Trans. Signal Process.* **2011**, *59*, 351–361. [CrossRef]
27. Allen, T.; Tajer, A.; Al-Dhahir, N. Secure Alamouti MAC transmissions. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3674–3687. [CrossRef]
28. Fakoorian, S.A.A.; Jafarkhani, H.; Swindlehurst, A.L. Secure space-time block coding via artificial noise alignment. In Proceedings of the Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, USA, 6–9 November 2011; pp. 651–655.
29. Wang, H.M.; Wang, C.; Ng, D.W.K. Artificial noise assisted secure transmission under training and feedback. *IEEE Trans. Signal Process.* **2015**, *63*, 6285–6298. [CrossRef]
30. Hyadi, A.; Rezki, Z.; Alouini, M. An overview of physical layer security in wireless communication systems with CSIT uncertainty. *IEEE Access* **2016**, *4*, 6121–6132. [CrossRef]
31. Joung, J. Space-Time Line Code. *IEEE Access* **2018**, *6*, 1023–1041. [CrossRef]
32. Alamouti, S.M. A simple transmitter diversity scheme for wireless communications. *IEEE J. Sel. Areas Commun.* **1998**, *16*, 1451–1458. [CrossRef]

33. Joung, J. Space-Time Line Code for Massive MIMO and Multiuser Systems with Antenna Allocation. *IEEE Access* **2018**, *6*, 962–979. [CrossRef]
34. Joung, J.; Jeong, E.R. Multiuser space-time line code with optimal and suboptimal power allocation methods. *IEEE Access* **2018**, *6*, 51766–51775. [CrossRef]
35. Joung, J. Energy efficient space-time line coded regenerative two-way relay under per-antenna power constraints. *IEEE Access* **2018**, *6*, 47026–47035. [CrossRef]
36. Joung, J.; Choi, J. Space-time line code with power allocation for regenerative two-way relay systems. *IEEE Trans. Veh. Technol.* **2019**. (early access article), doi:10.1109/TVT.2019.2905992. [CrossRef]
37. Joung, J.; Choi, J. Uneven power amplifier shuffling for space-time line code (STLC) systems. *IEEE Access* **2018**, *6*, 58491–58500. [CrossRef]
38. Joung, J.; Jung, B.C. Machine learning based blind decoding for space-time line code (STLC) systems. *IEEE Trans. Veh. Technol.* **2019**. (early access article). [CrossRef]
39. Cordeschi, N.; Amendola, D.; Shojafar, M.; Enzo, B. Distributed and adaptive resource management in cloud-assisted cognitive radio vehicular networks with hard reliability guarantees. *Veh. Commun.* **2015**, *2*, 1–12. [CrossRef]