entropy

MDPI

Article

Secrecy Enhancing Scheme for Spatial Modulation Using Antenna Selection and Artificial Noise

Pingping Shang [1,†], Weicheng Yu [2], Kai Zhang [3], Xue-Qin Jiang [3] and Sooyoung Kim [1,*]

[1] Division of Electronic Engineering, IT Convergence Research Center, Chonbuk National University, Jeonju 54896, Korea
[2] Shanghai Aerospace Electronic Technology Institute, Shanghai 201109, China
[3] Department of Communication Engineering, Donghua University, Shanghai 201620, China
* Correspondence: sookim@jbnu.ac.kr
† Current address: 567 Baekje-daero, Deokjin-gu, Jeonju, Jeollabuk-do 54896, Korea.

Received: 31 May 2019; Accepted: 23 June 2019; Published: 26 June 2019

Abstract: In this paper, we present a new secrecy-enhancing scheme for the spatial modulation (SM) system, by considering imperfect channel state information (CSI). In the proposed scheme, two antennas are activated at the same time. One of the activated antennas transmits information symbols along with artificial noise (AN) optimized under the imperfect CSI condition. On the other hand, the other activated antenna transmits another AN sequence. Because the AN are generated by exploiting the imperfect CSI of the legitimate channel, they can only be canceled at the legitimate receiver, while the passive eavesdropper will suffer from interference. We derive the secrecy rate of the proposed scheme in order to estimate the performance. The numerical results demonstrated in this paper verify that the proposed scheme can achieve a better secrecy rate compared to the conventional scheme at the same effective data rate.

Keywords: spatial modulation (SM); antenna selection; artificial noise (AN); channel state information (CSI); physical layer security (PLS); secrecy rate

1. Introduction

Spatial modulation (SM) is a spatial multiplexing multiple-input multiple-output (MIMO) scheme, and it is known that SM can overcome the drawbacks of the conventional MIMO techniques [1]. For example, SM can entirely avoid the inter-channel interference (ICI) and inter-antenna synchronization (IAS) problems by activating only a part, usually one of the transmit-antennas for data transmission at any signaling time instance. In addition, it usually needs one radio frequency (RF) chain for data transmission [2]. Due to the above-mentioned advantages, SM is expected to be one of the key technologies for future wireless networks [3].

SM is considered as a three-dimensional (3D) modulation technique, because it conveys information bits by utilizing both the antenna index and complex symbols to form a 3D constellation [4]. With this concept, efficient 3D constellation schemes were proposed in order to achieve a better spatial multiplexing gain and high data throughput [4,5]. It was emphasized that they could be easily extended to a massive MIMO system by reducing the cost of the massive numbers of RF chains at the base stations, and the security scheme could be directly adopted. On the other hand, efficient antenna selection techniques were proposed to enhance the system performance. For example, a Euclidean distance optimized antenna

selection (EDAS) method was proposed to offer a significant signal-to-noise ratio (SNR) gain [6], and later, the achievable transmit diversity order of the EDAS was analyzed [7].

Due to the inherent broadcasting nature of wireless communication systems, security and privacy protection comprise an increasingly important issue in the design and implementation of wireless networks. Recently, physical layer security (PLS) schemes combined with MIMO techniques have gained much attention, especially when SM is used [8]. Because SM changes the active antenna dynamically, it can be easily applied to a PLS scheme. For example, an antenna selection scheme for SM was proposed to achieve PLS transmission [9].

In combination with the antenna selection, the idea of injecting jamming signals, i.e., artificial noises (AN), into the transmission of SM was proposed to enhance the security [10]. It was presented that activating an extra transmit antenna to transmit AN can increase the security of SM. A similar fact was discussed in [11], where the authors proposed a secure transmission scheme for differential quadrature spatial modulation (DQSM) with AN, and it was shown that the AN technique was a meaningful idea to improve the secrecy performance. Because the AN can be also interference to the legitimate receiver, the antenna carrying AN needs to be directed to the null space, and thus, additional beamforming technique was required. One of our previous studies presented a PLS scheme with AN, which did not require a beamforming technique [12]. On the other hand, a symbol rotation-based secrecy-enhancing scheme combined with SM was proposed [13]. In this scheme, complex symbol values for transmit antenna indices and information were dynamically rotated, where the rotation values were optimized for legitimate channel state information (CSI).

However, all of the aforementioned schemes assumed perfect CSI knowledge at least for the legitimate channel. By considering that the influence of imperfect CSI due to the channel estimation error cannot be ignored, this paper proposes a new secrecy-enhancing scheme for SM under imperfect CSI. We adopt the idea of combining the antenna selection with AN for PLS and utilize the additional activation of the antenna only for transmitting AN. Especially, we propose a method to employ two AN sequences, which have the co-cancellation property, and thus, they can perfectly cancel each other only at the legitimate receiver. We assume the imperfect CSI condition by considering the practical system operation condition, and thus, the generation of AN and antenna selection are all optimized by considering imperfect CSI. In this way, the legitimate receiver can perfectly cancel the AN while the eavesdropper will suffer from the interference induced by the AN. To estimate the secrecy performance, we derive the secrecy rate of the proposed scheme.

The rest of this paper is organized as follows. In Section 2, we describe the basic concept of the conventional PLS scheme with SM by using a simple system model. Section 3 presents the proposed scheme, starting with the representation of the operational principle in brief. Afterwards, it proposes a method to generate AN, which can be perfectly canceled only at the legitimate receiver, and then presents the optimum antenna selection method by considering imperfect CSI. In Section 4, we derive the mathematical expressions of the secrecy rate of the proposed scheme. The numerical results and discussions are presented in Section 5. Finally, Section 6 draws the conclusions.

Notation: Bold lower case letters represent vectors, while bold upper case letters denote matrices. $(\cdot)^H$, $|\cdot|$, and $\|\cdot\|$ denote the Hermitian transpose, modulus operator, and Frobenius norm operations, respectively. $\binom{\cdot}{\cdot}$ is the binomial coefficient. $\mathbb{C}^{m\times n}$ stands for the complex space of $m \times n$ dimensions.

2. PLS Scheme with SM

Figure 1 shows a system model using SM for PLS. In the generic model of the PLS scheme, there is a cooperative wireless network consisting of three nodes, as shown in Figure 1. One source node, which is the legitimate transmitter node, is referred to as Alice. The corresponding destination

node is referred to as Bob, which is the legitimate receiver node. On the other hand, the third node, named Eve, is the passive eavesdropper node. In this model, Alice sends the secret data sequence and communicates confidentially with Bob. Eve attempts to intercept the ongoing communication between the legitimate link, i.e., from the transmitter Alice to the legitimate receiver Bob. In other words, Eve tries to decode and obtain the secret data content from her own observations of the received signals [9].

As shown in Figure 1, it is assumed that the transmitter Alice is equipped with N_t antennas, and M-ary amplitude and phase modulation (APM) symbols are transmitted over one of the N_t antennas at each signaling time instance. The channels from Alice to Bob and Eve are represented by the $N_{Rb} \times N_t$ matrix $\mathbf{H}$ and $N_{Re} \times N_t$ matrix $\mathbf{G}$, respectively, where N_{Rb} and N_{Re} are the numbers of receive antennas at Bob and Eve, respectively. All the channel gains for each transmitted symbol, i.e., all the elements of $\mathbf{H}$ and $\mathbf{G}$, are assumed to be independent complex Rayleigh random variables and not to have frequency selectivity. The number of transmit antennas, N_t, in the conventional SM system is usually assumed to be a power of two [1]. At the transmitter, the bit stream emitted by a binary source is divided into blocks containing n_t and ℓ bits each, where $n_t = \log_2 N_t$ is the number of bits to identify a transmit-antenna among N_t antennas, and $\ell = \log_2 M$ is the number of bits in an M-ary symbol. Therefore, the effective data rate $r_e = n_t + \ell$.

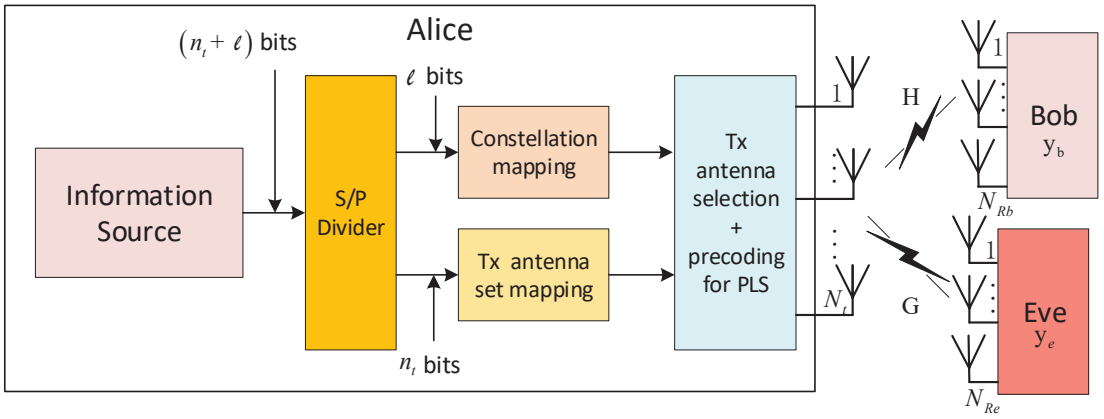

Figure 1. Physical layer security scenario for the spatial modulation systems.

When a symbol is chosen to be transmitted at the j-th antenna among N_t antennas, the transmission from Alice can be represented by the $N_t \times 1$ column vector, $\mathbf{x}$, as follows [14]:

$$\mathbf{x} = [0 \dots 0 \underbrace{x_m}_{j-th} 0 \dots 0]^T = \mathbf{e}_j \cdot x_m, \tag{1}$$

where x_m denotes a modulation symbol drawn from M-ary APM constellation whose power is normalized to one and $\mathbf{e}_j$ is a unit vector whose jth entry is non-zero for $j \in \{1, 2, \cdots, N_t\}$. Then, the received signal vector $\mathbf{y}_b \in \mathbb{C}^{N_{Rb} \times 1}$ at Bob and $\mathbf{y}_e \in \mathbb{C}^{N_{Re} \times 1}$ at Eve are represented by:

$$\mathbf{y}_b = \mathbf{H}\mathbf{x} + \mathbf{n}_b = \mathbf{h}_j x_m + \mathbf{n}_b, \tag{2}$$

and:

$$\mathbf{y}_e = \mathbf{G}\mathbf{x} + \mathbf{n}_e = \mathbf{g}_j x_m + \mathbf{n}_e, \tag{3}$$

respectively. In the above equations, $\mathbf{h}_j$ and $\mathbf{g}_j$ are the jth column vectors of $\mathbf{H}$ and $\mathbf{G}$, respectively, and $\mathbf{n}_b \in \mathbb{C}^{N_{Rb}\times 1}$ and $\mathbf{n}_e \in \mathbb{C}^{N_{Re}\times 1}$ denote the complex additive white Gaussian noise (AWGN) vectors.

3. Secrecy-Enhancing Spatial Modulation Scheme

3.1. Antenna Selection and Insertion of AN

In our proposed scheme, we consider a multiple-input single-output (MISO) system with N_a transmit antennas as shown in Figure 2. Alice is equipped with N_a antennas, while Bob and Eve are equipped with only one antenna. In the proposed system, we assume that N_a is not necessarily a power of two, N_t is a power of two, so that the antenna index can represent digital information, and $N_a > N_t$. Information symbol x_m is transmitted along with AN of $\beta_1\nu$ by one of the N_t antennas selected by matrix $\mathbf{T}_k$, and another AN of $\beta_2\nu$ is transmitted by one of the remaining $(N_a - N_t)$ antennas selected by matrix $\mathbf{T}_q$, where ν is the complex Gaussian AN with zero-mean and unit variance. In addition, β_1 and β_2 are coefficients, which are designed to cancel the AN at Bob. Accordingly, the signals received at Bob and Eve in the proposed scheme with antenna selection matrices $\mathbf{T}_k$ and $\mathbf{T}_q$ can be, respectively, presented by:

$$y_b = \mathbf{h}\mathbf{T}_k\mathbf{e}_j(x_m + \beta_1\nu) + \mathbf{h}\mathbf{T}_q\beta_2\nu + n_b, \tag{4}$$

and:

$$y_e = \mathbf{g}\mathbf{T}_k\mathbf{e}_j(x_m + \beta_1\nu) + \mathbf{g}\mathbf{T}_q\beta_2\nu + n_e, \tag{5}$$

where $\mathbf{h} \in \mathbb{C}^{1\times N_a}$ and $\mathbf{g} \in \mathbb{C}^{1\times N_a}$ are the row vectors representing the channel gains from Alice to Bob and Eve, respectively. $\mathbf{T}_k \in \mathbb{C}^{N_a\times N_t}$ is the effective transmit antenna selection matrix for $k \in \{1, 2, \cdots, P\}$, which is constructed by selecting N_t columns from identity matrix $\mathbf{I}_{N_a}$. P is the number of transmit antenna combinations, $\binom{N_a}{N_t}$, and the sample space of all possible antenna combinations is represented as $\mathbf{\Phi} = \{\Phi_1, \cdots, \Phi_k, \cdots, \Phi_P\}$, in which Φ_k denotes the k-th combination of the effective transmit antenna set. At each time slot, Alice selects one of the P combinations and shares it with Bob through a low-speed forward link, as in other conventional schemes [15]. In addition, n_b and n_e are complex AWGN with a mean value of zero and variance of σ^2. $\mathbf{T}_q \in \mathbb{C}^{N_a\times 1}$ is a single column matrix to select another antenna transmitting AN for $q \in \{1, 2, \cdots, N_a - N_t\}$. $\mathbf{T}_q$ is selected from submatrix $\mathbf{I}'_{N_a} \in \mathbb{C}^{N_a\times(N_a-N_t)}$, which is composed of the remaining column vectors in $\mathbf{I}_{N_a}$ after constructing $\mathbf{T}_k$.

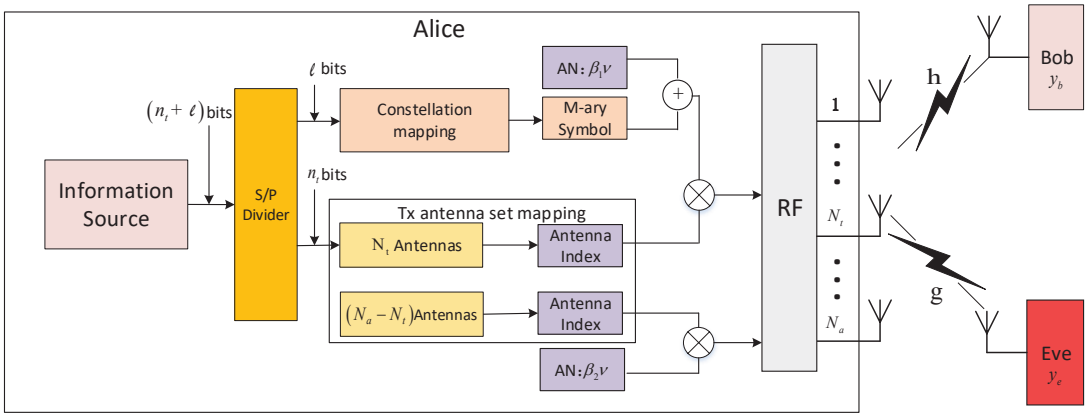

Figure 2. System model of the proposed secrecy enhancement scheme for the spatial modulation (SM) system.

3.2. Perfect Cancellation of AN

Consider the fact that perfect CSI is hard to obtain in practice due to the estimation errors. The channel gains, $\mathbf{h}$ and $\mathbf{g}$, can be expressed by:

$$\mathbf{h} = \sqrt{1-\rho^2}\hat{\mathbf{h}} + \sqrt{\rho^2}\tilde{\mathbf{h}}, \tag{6}$$

and:

$$\mathbf{g} = \sqrt{1-\rho^2}\hat{\mathbf{g}} + \sqrt{\rho^2}\tilde{\mathbf{g}}. \tag{7}$$

Here, $\hat{\mathbf{h}} \in \mathbb{C}^{1\times N_a}$ and $\tilde{\mathbf{h}} \in \mathbb{C}^{1\times N_a}$ represent the estimation and the estimation error of the main channel, i.e., from Alice to Bob, respectively. On the other hand, $\hat{\mathbf{g}} \in \mathbb{C}^{1\times N_a}$ and $\tilde{\mathbf{g}} \in \mathbb{C}^{1\times N_a}$ represent the estimation and the estimation error of the eavesdropping channel, i.e., from Alice to Eve, respectively. ρ^2 is the variance of estimation error, and it reflects the accuracy of the CSI.

Inserting (6) into (4) leads to:

$$\begin{aligned} y_b =& \sqrt{1-\rho^2}\hat{\mathbf{h}}\mathbf{T}_k\mathbf{e}_j(x_m+\beta_1\nu) + \sqrt{\rho^2}\tilde{\mathbf{h}}\mathbf{T}_k\mathbf{e}_j(x_m+\beta_1\nu) \\ &+ \sqrt{1-\rho^2}\hat{\mathbf{h}}\mathbf{T}_q\beta_2\nu + \sqrt{\rho^2}\tilde{\mathbf{h}}\mathbf{T}_q\beta_2\nu + n_b. \end{aligned} \tag{8}$$

If we let $\hat{h_j}' = \hat{\mathbf{h}}\mathbf{T}_k\mathbf{e}_j$, $\tilde{h_j}' = \tilde{\mathbf{h}}\mathbf{T}_k\mathbf{e}_j$, $\hat{h_i}' = \hat{\mathbf{h}}\mathbf{T}_q$, and $\tilde{h_i}' = \tilde{\mathbf{h}}\mathbf{T}_q$, then:

$$\begin{aligned} y_b =& \sqrt{1-\rho^2}\hat{h_j}'(x_m+\beta_1\nu) + \sqrt{\rho^2}\tilde{h_j}'(x_m+\beta_1\nu) \\ &+ \sqrt{1-\rho^2}\hat{h_i}'\beta_2\nu + \sqrt{\rho^2}\tilde{h_i}'\beta_2\nu + n_b. \end{aligned} \tag{9}$$

Similarly, if we let $\hat{g_j}' = \hat{\mathbf{g}}\mathbf{T}_k\mathbf{e}_j$, $\tilde{g_j}' = \tilde{\mathbf{g}}\mathbf{T}_k\mathbf{e}_j$, $\hat{g_i}' = \hat{\mathbf{g}}\mathbf{T}_q$, and $\tilde{g_i}' = \tilde{\mathbf{g}}\mathbf{T}_q$, then (5) can be represented by:

$$\begin{aligned} y_e =& \sqrt{1-\rho^2}\hat{g_j}'(x_m+\beta_1\nu) + \sqrt{\rho^2}\tilde{g_j}'(x_m+\beta_1\nu) \\ &+ \sqrt{1-\rho^2}\hat{g_i}'\beta_2\nu + \sqrt{\rho^2}\tilde{g_i}'\beta_2\nu + n_e. \end{aligned} \tag{10}$$

Our purpose here is to make AN cancel each other at the legitimate receiver; therefore, we need to find proper values of β_1 and β_2. According to (9), we note that $\sqrt{1-\rho^2}\hat{h_j}'\beta_1\nu + \sqrt{1-\rho^2}\hat{h_i}'\beta_2\nu$ is the interference at Bob. Therefore, we should make it equal to zero such that there is no interference at Bob. That means:

$$\sqrt{1-\rho^2}\hat{h_j}'\beta_1\nu + \sqrt{1-\rho^2}\hat{h_i}'\beta_2\nu = 0. \tag{11}$$

Then, β_1 and β_2 should be calculated by:

$$\begin{cases} \beta_1 = -\hat{h_i}' \\ \beta_2 = \hat{h_j}' \end{cases} \quad or \quad \begin{cases} \beta_1 = \hat{h_i}' \\ \beta_2 = -\hat{h_j}'. \end{cases} \tag{12}$$

Since the estimation channel vectors $\hat{\mathbf{h}}$ and $\hat{\mathbf{g}}$ are independent of each other, that is to say $\hat{h_j}' \neq \hat{g_j}'$ and $\hat{h_i}' \neq \hat{g_i}'$, β_1 and β_2 calculated in (12) will lead to:

$$\sqrt{1-\rho^2}\hat{g_j}'\beta_1\nu + \sqrt{1-\rho^2}\hat{g_i}'\beta_2\nu \neq 0. \tag{13}$$

Therefore, Eve will suffer from the interference due to the AN of $\sqrt{1-\rho^2}\hat{g}_j{}'\beta_1\nu + \sqrt{1-\rho^2}\hat{g}_i{}'\beta_2\nu$.

3.3. Optimum Selection of the Transmit Antenna Combination

Assuming that the data are transmitted by the j-th antenna, the received signal power at Eve is $\|\hat{\mathbf{g}}\mathbf{T}_k\mathbf{e}_j\|^2$, which is defined as a quantity, called leakage for Bob [16]. Generally, we can assume that the power of the received signal at Bob, i.e., $\|\hat{\mathbf{h}}\mathbf{T}_k\mathbf{e}_j\|^2$, is sufficiently large compared to the power of the AWGN, (i.e., σ^2) and that $\|\hat{\mathbf{h}}\mathbf{T}_k\mathbf{e}_j\|^2$ is sufficiently large compared to $\|\hat{\mathbf{g}}\mathbf{T}_k\mathbf{e}_j\|^2$. Based on these two assumptions, we define the signal-to-leakage noise ratio (SLNR) for the j-th channel of the k-th combination as:

$$\varphi_j(\mathbf{T}_k) = \frac{\|\hat{\mathbf{h}}\mathbf{T}_k\mathbf{e}_j\|^2}{\|\hat{\mathbf{g}}\mathbf{T}_k\mathbf{e}_j\|^2 + \sigma^2}. \tag{14}$$

Assume that the selected N_t antennas are activated with equal probability to transmit the information symbols. The optimum matrix $\mathbf{T}_k$ can be found by maximizing SLNR as follows:

$$\begin{aligned} &\max \sum_{j=1}^{N_t} \varphi_j(\mathbf{T}_k) \\ &\text{subject to } \mathbf{T}_k \in \{\mathbf{T}_1, \mathbf{T}_2, \ldots, \mathbf{T}_P\}. \end{aligned} \tag{15}$$

However, the above optimum solution of $\mathbf{T}_k$ with exhaustive search requires a high complexity. We propose the following complexity reduced method.

Assume all of the transmit antennas are independent. Then, the SLNR at the l-th, φ_l, can be represented by:

$$\varphi_l = \frac{\|\hat{h}_l\|^2}{\|\hat{g}_l\|^2 + \sigma^2}, \tag{16}$$

where $\hat{h}_l$ and $\hat{g}_l$ denote the l-th elements of the channel $\hat{\mathbf{h}}$ and $\hat{\mathbf{g}}$, respectively. In this way, we calculate the SLNR values for all transmit antennas, and the calculated SLNR values are sorted in descending order such that:

$$\underbrace{\varphi_{\pi_1} \geq \varphi_{\pi_2} \geq \cdots \geq \varphi_{\pi_{N_t}}}_{N_t \text{ selected antennas}} \geq \cdots \geq \varphi_{\pi_{N_a}}, \tag{17}$$

where $\{\pi_1, \pi_2, \cdots, \pi_{N_a}\}$ is an ordered permutation set of $\{1, 2, \cdots, N_a\}$. Therefore, the optimization problem in (15) is equivalent to selecting φ_{π_d} from (17) for $1 \leq d \leq N_t$.

4. Secrecy Rate Analysis

The received signal at the legitimate receiver Bob, y_b, can be rearranged as follows by inserting the result in (11) into (9).

$$y_b = \sqrt{1-\rho^2}\hat{h}_j{}'x_m + \sqrt{\rho^2}\tilde{h}_j{}'(x_m + \beta_1\nu) + \sqrt{\rho^2}\tilde{h}_i{}'\beta_2\nu + n_b. \tag{18}$$

If we let:

$$\tilde{n}_b = \sqrt{\rho^2}\tilde{h}_j{}'(x_m + \beta_1\nu) + \sqrt{\rho^2}\tilde{h}_i{}'\beta_2\nu + n_b, \tag{19}$$

then it can be approximated as zero-mean complex Gaussian noise with variance of $\eta_b = E[\tilde{n}_b(\tilde{n}_b)^H]$. In addition, letting $\theta = 1-\rho^2$, then the normalized value of y_b with noise variance of η_b can be approximated by:

$$\tilde{y}_b = \frac{y_b}{\sqrt{\eta_b}} \simeq \sqrt{\frac{\theta}{\eta_b}}\hat{h_j}'x_m + \hat{n}_b, \tag{20}$$

where $\hat{n}_b = \tilde{n}_b/\sqrt{\eta_b}$. After choosing the optimum matrices $\mathbf{T}_k$ and $\mathbf{T}_q$, the probability of selecting each transmit antenna and each symbol x_m is $\frac{1}{N_t}$ and $\frac{1}{M}$, respectively. Thus, the received signal at Bob follows a complex Gaussian distribution, which can be represented as:

$$P(\tilde{y}_b|\hat{h_j}', x_m) = \frac{1}{\pi}\exp\left(-|\ \tilde{y}_b - \sqrt{\frac{\theta}{\eta_b}}\hat{h_j}'x_m\ |^2\right), \tag{21}$$

and:

$$P(\tilde{y}_b) = \frac{1}{N_tM}\sum_{j=1}^{N_t}\sum_{m=1}^{M}\frac{1}{\pi}\exp\left(-|\ \tilde{y}_b - \sqrt{\frac{\theta}{\eta_b}}\hat{h_j}'x_m\ |^2\right). \tag{22}$$

Then, the ergodic rate of Bob can be written as,

$$\begin{aligned} R_b &= E_{\hat{\mathbf{h}}}\left[\int\sum_{j=1}^{N_t}\sum_{m=1}^{M} p(\tilde{y}_b, \hat{h_j}', x_m)\log_2\frac{p(\tilde{y}_b, \hat{h_j}', x_m)}{p(\tilde{y}_b)p(\hat{h_j}', x_m)}d\tilde{y}_b\right] \\ &= \log_2 N_tM - \frac{1}{N_tM}\sum_{j=1}^{N_t}\sum_{m=1}^{M}E_{\hat{\mathbf{h}}}\left[E_{\hat{n}_b}\left[\log_2\sum_{j'=1}^{N_t}\sum_{m'=1}^{M}\right.\right. \\ &\quad\left.\left.\times\ \exp\left(-\left(|\ \sqrt{\frac{\theta}{\eta_b}}\delta_{j,m}^{j',m'} + \hat{n}_b\ |^2 - |\ \hat{n}_b\ |^2\right)\right)\right]\right], \end{aligned} \tag{23}$$

in which $\delta_{j,m}^{j',m'}$ is given by:

$$\delta_{j,m}^{j',m'} = \hat{h_j}'x_m - \hat{h_{j'}}'x_{m'}. \tag{24}$$

Using Jensen's inequality, the lower bound of R_b is obtained as:

$$\begin{aligned} R_b^{low} &= \log_2 N_tM - \frac{1}{N_tM}\sum_{j=1}^{N_t}\sum_{m=1}^{M}\log_2\sum_{j'=1}^{N_t}\sum_{m'=1}^{M} \\ &\quad\times E_{\hat{\mathbf{h}}}\left[E_{\hat{n}_b}\left[\exp\left(-\left(|\ \sqrt{\frac{\theta}{\eta_b}}\delta_{j,m}^{j',m'} + \hat{n}_b\ |^2 - |\ \hat{n}_b\ |^2\right)\right)\right]\right] \\ &= \log_2 N_tM + 1 - \frac{1}{\ln 2} \\ &\quad - \frac{1}{N_tM}\sum_{j=1}^{N_t}\sum_{m=1}^{M}\log_2\sum_{j'=1}^{N_t}\sum_{m'=1}^{M}E_{\hat{\mathbf{h}}}\left[\exp\left(-\frac{\theta\ |\ \delta_{j,m}^{j',m'}\ |^2}{2\eta_b}\right)\right]. \end{aligned} \tag{25}$$

In order to derive the ergodic rate at the passive eavesdropper, we first represent (10) using θ as follows:

$$\begin{aligned} y_e = &\sqrt{\theta}\hat{g}_j{}' x_m + \\ &\sqrt{\theta}(\hat{g}_j{}'\beta_1 + \hat{g}_i{}'\beta_2)\nu + \sqrt{\rho^2}(\tilde{g}_j{}' x_m + \tilde{g}_j{}'\beta_1\nu + \tilde{g}_i{}'\beta_2\nu) + n_e. \end{aligned} \tag{26}$$

If we let:

$$\tilde{n}_e = \sqrt{\theta}(\hat{g}_j{}'\beta_1 + \hat{g}_i{}'\beta_2)\nu + \sqrt{\rho^2}(\tilde{g}_j{}' x_m + \tilde{g}_j{}'\beta_1\nu + \tilde{g}_i{}'\beta_2\nu) + n_e, \tag{27}$$

then the normalized value of y_e with $\eta_e = E[\tilde{n}_e(\tilde{n}_e)^H]$ can be approximated by:

$$\tilde{y}_e \simeq \sqrt{\frac{\theta}{\eta_e}}\hat{g}_j{}' x_m + \hat{n}_e, \tag{28}$$

where $\hat{n}_e = \tilde{n}_e / \sqrt{\eta_e}$.

Then, the ergodic rate of Eve is expressed as:

$$\begin{aligned} R_e &= E_{\hat{\mathbf{g}}}\left[\int \sum_{j=1}^{N_t}\sum_{m=1}^{M} p(\tilde{y}_e, \hat{g}_j{}', x_m)\log_2\frac{p(\tilde{y}_e, \hat{g}_j{}', x_m)}{p(\tilde{y}_e)p(\hat{g}_j{}', x_m)} d\tilde{y}_e\right] \\ &= \log_2 N_t M - \frac{1}{N_t M}\sum_{j=1}^{N_t}\sum_{m=1}^{M} E_{\hat{\mathbf{g}}}\left[E_{\hat{n}_e}\left[\log_2\sum_{j'=1}^{N_t}\sum_{m'=1}^{M}\right.\right. \\ &\quad \left.\left.\times \exp\left(-\left(\mid\sqrt{\frac{\theta}{\eta_e}}\alpha_{j,m}^{j',m'} + \hat{n}_e\mid^2 - \mid\hat{n}_e\mid^2\right)\right)\right]\right], \end{aligned} \tag{29}$$

in which $\alpha_{j,m}^{j',m'}$ is given by:

$$\alpha_{j,m}^{j',m'} = \hat{g}_j{}' x_m - \hat{g}_{j'}{}' x_{m'}. \tag{30}$$

Using Jensen's inequality, the lower bound of R_e is obtained as:

$$\begin{aligned} R_e^{low} = &\log_2 N_t M + 1 - \frac{1}{\ln 2} \\ &- \frac{1}{N_t M}\sum_{j=1}^{N_t}\sum_{m=1}^{M}\log_2\sum_{j'=1}^{N_t}\sum_{m'=1}^{M} E_{\hat{\mathbf{g}}}\left[\exp\left(-\frac{\theta\mid\alpha_{j,m}^{j',m'}\mid^2}{2\eta_e}\right)\right]. \end{aligned} \tag{31}$$

Based on (23) and (29), the ergodic secrecy rate can be written as:

$$\bar{R}_s = \max\{0, R_b - R_e\}. \tag{32}$$

5. Simulation and Numerical Results

This section presents the secrecy performance comparisons in terms of the secrecy rate. The ergodic secrecy rate, derived in (32), was numerically simulated by using several parameters including N_a, N_t, modulation order M, and SNR values. In the simulations, the power of the modulation symbol was normalized to one, and the power of the complex AWGN at both Bob and Eve was assumed to be σ^2, while the SNR was $1/\sigma^2$.

We first compared the secrecy performance of the proposed scheme according to the antenna selection method. Figure 3 shows the comparison of the secrecy performance when Alice chooses $\mathbf{T}_k$ by using the optimum selection method described in Section 3.3 and the random selection method, when $\rho^2 = 0.01$. It was assumed that $N_a = 6$ and $N_t = 4$, and different APM schemes with $M = 2$, $M = 4$, and $M = 8$ were employed. As shown in Figure 3, compared to the random selection scheme, the proposed optimum antenna selection scheme with $\mathbf{T}_k$ was able to achieve a better secrecy rate. Because the secrecy capacity of fading channels had a ceiling as the transmit SNR increased [17], $\bar{R}_s$ of the proposed scheme increased with the increasing SNR until the SNR approached about 30 dB. Furthermore, it is easy to see that a higher modulation order M yielded a higher secrecy rate.

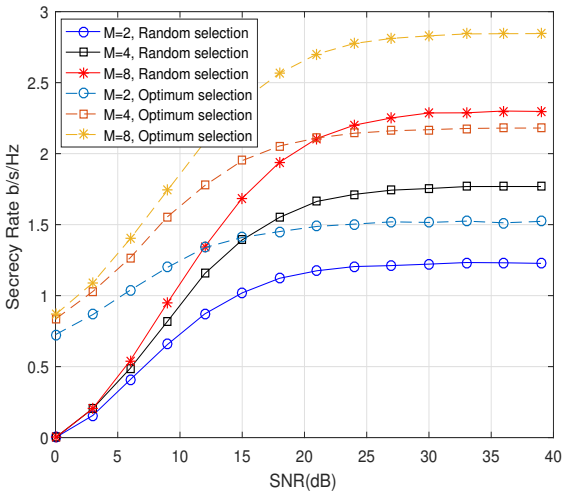

Figure 3. The secrecy rate, $\bar{R}_s$, of the proposed scheme according to the selection methods of T_k when $N_a = 6$ and $N_t = 4$.

Next, we compared the secrecy rate of the proposed scheme with the conventional scheme in [9], by applying the same effective data rate, $r_e = n_t + \ell$. Figures 4 and 5 show the comparison of $\bar{R}_s$ when r_e were four and five, respectively. When $r_e = 4$ in Figure 4, we considered the scenario that Alice employed the 8-PSK modulation, and N_a and N_t were set to three and two, respectively, in the proposed scheme. On the other hand, in the conventional scheme, Alice employed QPSK modulation, and the symbol was transmitted by one of four transmit antennas, i.e., $N_t = 4$. When $r_e = 5$ in Figure 5, N_a and N_t of the proposed scheme were set to be six and 4, respectively, and the 8-PSK modulation symbol was transmitted. On the other hand, N_t of the conventional scheme was set to be eight, and QPSK symbol was transmitted. As shown in Figures 4 and 5, we observe that the proposed scheme can achieve better secrecy performance than the conventional scheme in [9] when the perfect CSI was given, i.e., $\rho^2 = 0$. Furthermore, the proposed scheme with channel estimation error of $\rho^2 = 0.01$ produced a better performance compared to the conventional scheme with perfect CSI.

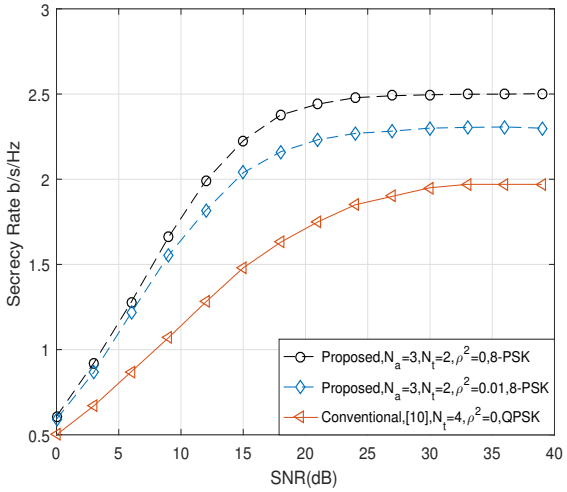

Figure 4. Comparison of $\bar{R}_s$ when r_e = 4 bits.

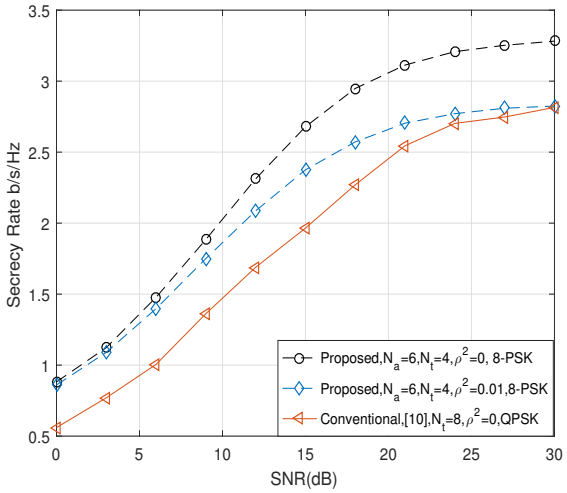

Figure 5. Comparison of $\bar{R}_s$ when r_e = 5 bits.

Figure 6 demonstrates the performance of the secrecy rate of the proposed scheme versus SNR with different numbers of transmit antennas N_a and N_t, when ρ^2 was equal to 0.01. We applied the QPSK modulation. We assumed that Alice was equipped with N_a = 3, 5, 6, 7, 10, 12, and 15 transmit antennas and utilized N_t = 2, 4, and 8 effective transmit antennas to send information. As shown in Figure 6, with the increase in the number of transmit antennas N_t, the secrecy rate was remarkably improved. When we set N_t to be a fixed value, the more antennas N_a Alice had, the higher the secrecy rate was. Simulation results also showed that the secrecy rate was growing rapidly under the low SNR. As the SNR increased, the secrecy rate tended to approach a saturation point. Because in the case of the low SNR, most of the transmit power was used to transmit the information symbols, more transmit power was used to transmit the AN in order to improve the secrecy rate as the SNR increased.

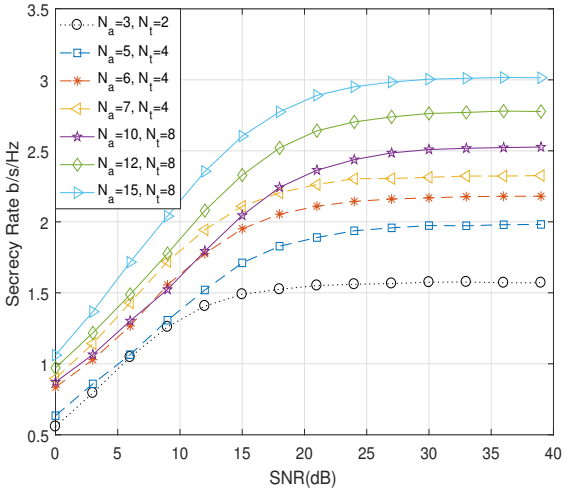

Figure 6. Comparison of $\bar{R}_s$ for the proposed scheme according to N_a and N_t.

Figure 7 shows the secrecy rate against the SNR with varying channel estimation error, ρ^2, where N_a and N_t were set to six and four, respectively. As we can easily deduce, the secrecy rate decreased as ρ^2 increased. Finally, Figure 8 compares the bit error rate (BER) performances of the proposed scheme. We employed the BPSK modulation scheme and various numbers of N_a and N_t at Alice. It was shown that the BER performance at Bob decreased rapidly with SNR for varying estimation error. However, BER at Eve was nearly 0.5 for all SNRs, which indicated that there was no information leaked to Eve.

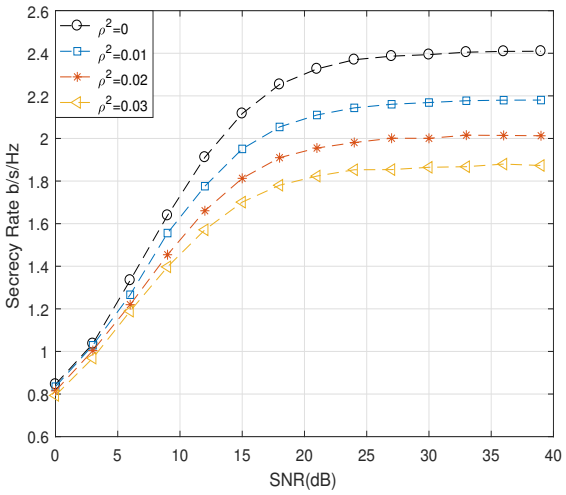

Figure 7. Comparison of $\bar{R}_s$ for the proposed scheme with varying ρ^2.

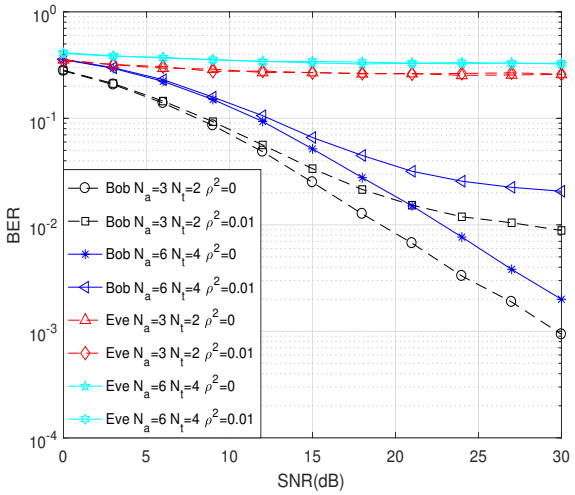

Figure 8. The BER performance under BPSK modulation and various numbers of N_a and N_t.

6. Conclusions

In this paper, we presented a new secrecy-enhancing scheme for the SM system. The proposed scheme employed two AN sequences, which were designed to be canceled each other perfectly only at the legitimate receiver. The AN sequences were designed by exploiting imperfect CSI of the legitimate channel by considering a practical system environment. In addition, an optimum antenna selection scheme was proposed by reducing the complexities of finding the solution from the exhaustive search. With the proposed scheme, the passive eavesdropper would suffer from the interference induced by the AN, resulting in secrecy rate enhancement of the legitimate receiver. We analyzed the secrecy performance over a Rayleigh fading channel by considering imperfect CSI. The simulation results demonstrated that the secrecy performance of the proposed scheme was enhanced compared to the conventional scheme.

Author Contributions: Conceptualization, P.S. and X.-Q.J.; data curation, P.S.; funding acquisition, S.K.; software, W.Y. and K.Z.; supervision, S.K.; validation, X.-Q.J.; writing, original draft, P.S.; writing, review and editing, S.K.

Funding: This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03027939).

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

References

1. Mesleh, R.Y.; Haas, H.; Sinanovic, S.; Ahn, C.W.; Yun, S.B. Spatial Modulation. *IEEE Trans. Veh. Technol.* **2008**, *57*, 2228–2241. [CrossRef]
2. Renzo, M.D.; Haas, H.; Ghrayeb, A.; Sugiura, S.; Hanzo, L. Spatial Modulation for Generalized MIMO: Challenges, Opportunities, and Implementation. *Proc. IEEE* **2008**, *102*, 56–103. [CrossRef]
3. Basar, E. Index modulation techniques for 5G wireless networks. *IEEE Commun. Mag.* **2016**, *54*, 168–175. [CrossRef]
4. Guo, S.S.; Zhang, H.X.; Zhang, P.; Wu, D.L.; Yuan, D.F. Generalized 3D Constellation Design for Spatial Modulation. *IEEE Trans. Commun.* **2017**, *65*, 3316–3327.
5. Guo, S.S.; Zhang, H.X.; Jin, S.; Zhang, P. Spatial Modulation via 3D Mapping. *IEEE Commun. Lett.* **2016**, *20*, 1096–1099. [CrossRef]
6. Rajashekar, R.; Hari, K.V.S.; Hanzo, L. Antenna Selection in Spatial Modulation Systems. *IEEE Commun. Lett.* **2013**, *17*, 521–524. [CrossRef]

7. Rajashekar, R.; Hari, K.V.S.; Hanzo, L. Quantifying the Transmit Diversity Order of Euclidean Distance Based Antenna Selection in Spatial Modulation. *IEEE Signal Process. Lett.* **2015**, *22*, 1434–1437. [CrossRef]
8. Hamamreh, J.M.; Furqan, H.M.; Arslan, H. Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1773–1828. [CrossRef]
9. Guan, X.R.; Cai, Y.M.; Yang, W.W. On the Secrecy Mutual Information of Spatial Modulation with Finite Alphabet. In Proceedings of the 2012 International Conference on Wireless Communications and Signal Processing (WCSP), Huangshan, China, 25–27 October 2012; pp. 1–4.
10. Wang, L.; Bashar, S.; Wei, Y.M.; Li, R.G. Secrecy Enhancement Analysis Against Unknown Eavesdropping in Spatial Modulation. *IEEE Commun. Lett.* **2015**, *19*, 1351–1354. [CrossRef]
11. Wang, Y.; Zhang, T.; Yang, W.W.; Guo, J.B.; Liu, Y.X.; Shang, X.H. Secure Transmission for Differential Quadrature Spatial Modulation with Artificial Noise. *IEEE Access* **2018**, *7*, 7641–7650. [CrossRef]
12. Yu, W.C.; Zhang, K.; Shang, P.P.; Jiang, X.Q.; Wen, M.W.; Li, J.; Hai, H. Security Enhancing Spatial Modulation Using Antenna Selection and Artificial Noise Cancellation. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 105–109.
13. Jiang, X.Q.; Wen, M.W.; Hai, H.; Li, J.; Kim, S.Y. Secrecy-Enhancing Scheme for Spatial Modulation. *IEEE Commun. Lett.* **2018**, *22*, 550–553. [CrossRef]
14. Wang, X.; Wang, X.; Sun, L. Spatial Modulation aided Physical Layer Security Enhancement for Fading Wiretap Channels. In Proceedings of the 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), Yangzhou, China, 13–15 October 2016; pp. 1–5.
15. Shu, F.; Wang, Z.W.; Chen, R.Q.; Wu, Y.P.; Wang, J.Z. Two High-performance Schemes of Transmit Antenna Selection for Secure Spatial Modulation. *IEEE Trans. Veh. Technol.* **2018**, *67*, 8969–8973. [CrossRef]
16. Sadek, M.; Tarighat, A.; Sayed, A.H. Active Antenna Selection in Multiuser MIMO Communications. *IEEE Trans. Signal Process.* **2007**, *55*, 1498–1510. [CrossRef]
17. Lei, H.J.; Ansari, I.S.; Pan, G.F.; Alomair, B.; Alouini, M.S. Secrecy Capacity Analysis Over α-μ Fading Channels. *IEEE Commun. Lett.* **2017**, *21*, 1445–1448. [CrossRef]