Artificial-Noise-Aided CQI-Mapped Generalized Spatial Modulation

Weijun Yin, Zhengmin Kong, *Senior Member, IEEE*, Yusha Liu, Yuli Yang and Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—The artificial noise (AN) aided channel quality indicator (CQI) mapped generalized spatial modulation (GSM) philosophy is proposed for improving the security of legitimate links. Given the randomness of the legitimate CQI, eavesdroppers cannot successfully decode the confidential information. We analyse both the secrecy rate as well as the eavesdropper's error rate and reveal that the proposed scheme outperforms its CQI-mapped modulation counterpart. Theoretically, the secrecy rate approaches the achievable data rate of the legitimate link, which is equal to the GSM capacity.**

***Index Terms*—Artificial noise (AN), channel quality indicator (CQI), generalized spatial modulation (GSM), physical layer security.**

I. Introduction

Generalized spatial modulation (GSM) [1] constitutes a promising multiple input multiple output (MIMO) technique, which activates a unique antenna pattern in each transmission of classic amplitude and phase modulation (APM) symbols to convey information. It stems from the idea of spatial modulation (SM) conceived in reference [2], which exploits the antenna index for carrying extra information via choosing a unique transmit antenna from a set of transmit antennas. The key ingredient of SM is to map a group of information bits into two information-carrying subchannels, one of which is used to decide the ON/OFF state of the transmit antennas. To elaborate, SM constitutes an innovative digital modulation technique having a reduced deployment cost as characterized in [3]. An an evolution from SM, the GSM philosophy proposed in reference [4] improves its potential by allowing multiple antennas being selected simultaneously. More explicitly, GSM conveys the information in two ways: (1) the combination of activated transmit antennas (TAs); (2) the classic APM symbols transmitted from each active TA. The underlying assumption in GSM is that the mapping from the information bits to the TAs and the APM symbols is predefined. Generally, the Gray mapping guarantees that the binary representations associated with two adjacent constellation symbols differ in only a single bit. In this context, it has been revealed that the distinct bit-to-symbol mapping patterns have a substantial impact on both the bit error rate (BER) and the physical layer security (PLS) performance attained [5]–[7] . Moreover, artificial noise (AN) aided schemes have been proposed to enhance the PLS of MIMO systems [8], [9]. In an AN-aided transmission scheme, a certain fraction of power is dedicated to deliberately interfering the eavesdropper (Eve) in reference [10]. Several prior contributions exploit that the secrecy rate of the eavesdropper (Eve) is improved by mitigating the inference imposed by the AN via adopting zero-forcing based receive beamforming in [11]. Consequently the system's security may become compromised. However, as a remedy, the system's security may still be guaranteed by the time-varying CQI mapping pattern proposed.

Our objective is to further improve the PLS of GSM in the context of time division duplexing (TDD) systems, where the channel's reciprocity is guaranteed between the legitimate transmitter and receiver. Originally, GSM was proposed for increasing the spectral efficiency of open-loop MIMO systems, where the transmitter is unaware of the legitimate receiver's channel state information (CSI) [5]. Its performance has been considered in various networks. Recently, an optimal GSM design and its power allocation scheme have been studied in a closed-loop MIMO system for increasing the achievable data rate, where the CSI of the desired link was assumed to be available at the transmitter [6]. Furthermore, several schemes have been proposed for maximizing the Euclidean distances in GSM, e.g., [12] and [13]. As a further advance, the PLS of SM was improved in [7], [14], [15] through randomly controlling the bit-to-symbol mapping patterns based on the random channel quality indicator (CQI). In this paper, we further enhance the PLS by appropriately designing the AN for confusing the eavesdroppers. Hence, our scheme is referred to as AN-aided CQI-mapped GSM. Since the eavesdroppers have no knowledge of the legitimate CQI, they are unable to correctly decode the confidential information. Even in the context of Eve's being capable to eliminate the AN signal, the security of this system could be guaranteed by introducing the CQI concept.

Against the above backdrop, the novel contributions of this paper are boldly and explicitly contrasted to the related literature in Table I.

- Explicitly, the CQI-mapped concepts are further advanced by the introduction of AN.
- The analytical expressions of both the secrecy rate and the average BER (ABER) are derived for GSM using

Weijun Yin, Zhengmin Kong are with the Automation Department, School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China. (e-mail: weijun_yin@whu.edu.cn, zmkong@whu.edu.cn)

Yusha Liu is with School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China. (yusha.liu@uestc.edu.cn)

Corresponding Author: Prof. Zhengmin Kong

L. Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk)

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/W016605/1 and EP/P003990/1 (COALESCE) as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028)

TABLE I: Overview of Related Works

Contributions	**This paper**	[7,13,14]	[8]	[16]	[16]
GSM	✓			✓	
CQI-mapped pattern	✓	✓			✓
BER analysis	✓			✓	✓
Power allocation	✓		✓	✓	
Artificial noise	✓		✓	✓	
Zero-forcing beamforming	✓		✓	✓	
Secrecy capacity	✓	✓	✓		
Complexity analysis	✓				

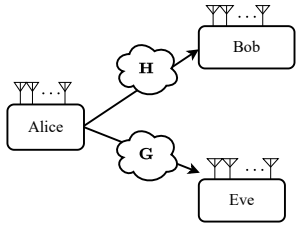


Fig. 1: The MIMO wiretap channel

finite-alphabet input.

The rest of this paper is organized as follows. Section II describes a MIMO wiretap channel model and reviews the advances in CQI-mapped SM, culminating in conceiving our AN-aided CQI-mapped GSM. Section III analyses the secrecy rate and ABER in the presence of an eavesdropper. Section IV quantifies the secrecy rate and ABER improvements. Finally, our conclusions are offered in Section V.

Notations: $\mathbf{A}^{\mathrm{H}}$, $\mathbf{A}^{-1}$, and $|\mathbf{A}|$ represent the conjugate transpose, the inverse, and the determinant of matrix $\mathbf{A}$, respectively; $\|\mathbf{v}\|$ is the Euclidean norm of vector $\mathbf{v}$; $\mathbf{I}_N$ stands for the identity matrix of size N; $\mathbf{A}\otimes\mathbf{B}$ is the Kronecker product of matrices $\mathbf{A}$ and $\mathbf{B}$; $\mathbb{C}^{M\times N}$ denotes the set containing all complex matrices of size $M\times N$; $Q(x)$ is the Q-function; $E_{\mathbf{w}}\{\cdot\}$ is the expectation of a variable over all possible $\mathbf{w}$; $\log(x)$ is used for base 2 unless specified otherwise; $\binom{M}{N}$ is the binomial coefficient; the column vector $\mathbf{e}_n$ has 1 in the n^{th} entry alongside all other entries being zero.

II. System Model

A. CQI-Mapped Spatial Modulation

Consider a MIMO wiretap channel model in Fig. 1, where Alice, Bob and Eve have N_t, N_r and N_e antennas, respectively. The fading channels spanning from Alice to Bob and Eve are represented by the $N_r\times N_t$ matrix $\mathbf{H}=[\mathbf{h}_1,\mathbf{h}_2,\cdots,\mathbf{h}_{N_t}]\in\mathbb{C}^{N_r\times N_t}$ and the $N_e\times N_t$ matrix $\mathbf{G}=[\mathbf{g}_1,\mathbf{g}_2,\cdots,\mathbf{g}_{N_t}]\in\mathbb{C}^{N_e\times N_t}$, respectively. Herein, the $N_r\times 1$ column vector $\mathbf{h}_n$, $n=1,2,\ldots,N_t$, represents the gain of the link spanning from the n^{th} TA of Alice to Bob, and the $N_e\times 1$ vector, $\mathbf{g}_m$, $m=1,2,\ldots,N_e$, is the corresponding counterpart for Eve. Indeed, the path-loss of the channel response is not taken into account, because we assume having perfect power control. This allows us to ignore the path-loss. Hence, $\mathbf{H}$ and $\mathbf{G}$ are Rayleigh channels. In GSM, N_a TAs are activated.

Bob's CSI is available at Alice as a benefit of using TDD. Our CQI-mapped GSM relies on the CQI $\gamma_n=\mathbf{h}_n^{\dagger}\mathbf{h}_n$ for mapping the binary input stream to the classic APM symbol and to the TA combination according to the mapping patterns given by [7]. Explicitly, the specific order of N_t CQIs determines the mapping pattern. For example, in a 4×4 MIMO system, $\gamma_1\geq\gamma_2\geq\gamma_3\geq\gamma_4$ could use the ordinary Gray-mapping APM constellation and one of the $N_t!$ TA combination patterns. Similarly, the number of APM constellation mapping patterns is $M!$ for M-point APM. The basic scheme is detailed in the [7].

With GSM, Alice's input bits are grouped as $\mathbf{x}=[\mathbf{x}_a,\mathbf{x}_d]$, where $\mathbf{x}_a$ and $\mathbf{x}_d$ represent the TA pattern and the classic APM symbol, respectively, whose cardinalities are typically different. Diverse strategies may be adopted to resolve this problem. If $N_t>M$, multiple mapping patterns are associated with the same APM symbol and conversely if $N_t<M$, multiple APM symbols are conveyed by the same TA-pattern associated with the same CQI. This implies that all possible CQI mapping patterns are utilized. In an arbitrary time slot, if the p^{th} CQI pattern is encountered by the legitimate channel, the APM symbol $\mathbf{x}_d$ is transmitted by Alice from the alphabet according to $\mathfrak{M}_q$ and via the TA-pattern $\mathbf{x}_a$ of the alphabet $\mathfrak{T}_p$. The mapping $\mathfrak{T}_p\colon \mathbf{x}_a\rightarrow n$, $n=1,\ldots,N_t$, here is used to obtain the index n of the antenna activated by the antenna information $\mathbf{x}_a$ under the p^{th} mapping pattern $\mathfrak{T}_p(\cdot)$ predefined in Table I in [7]. Moreover, the mapping $\mathfrak{M}_q\colon \mathbf{x}_d\rightarrow s_k$, $k=1,\ldots,M$, is utilized for obtaining the k^{th} APM symbol accompanied by the $\mathbf{x}_d$ via the mapping $\mathfrak{M}_q(\cdot)$ and the symbol $\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_d)}^{\mathfrak{T}_p(\mathbf{x}_a)}\overset{\text{def}}{=}e_{\mathfrak{T}_p(\mathbf{x}_a)}\mathfrak{M}_q(\mathbf{x}_d)$. Therefore, the baseband signals received at Bob and Eve are formulated as

$$\begin{aligned}\mathbf{y}&=\mathbf{h}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathfrak{M}_q(\mathbf{x}_d)+\mathbf{u}\\&=\mathbf{H}\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_d)}^{\mathfrak{T}_p(\mathbf{x}_a)}+\mathbf{u}\end{aligned}\tag{1}$$

and

$$\begin{aligned}\mathbf{z}&=\mathbf{g}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathfrak{M}_q(\mathbf{x}_d)+\mathbf{v}\\&=\mathbf{G}s_{\mathfrak{M}_q(\mathbf{x}_d)}^{\mathfrak{T}_p(\mathbf{x}_a)}+\mathbf{v},\end{aligned}\tag{2}$$

respectively, where the $N_r\times 1$ vector $\mathbf{y}$ is Bob's received signal and $\mathbf{u}$ is the additive white Gaussian noise (AWGN). Similarly, the $N_e\times 1$ vector $\mathbf{z}$ is Eve's received signal and $\mathbf{v}$ is AWGN. The AWGN vectors $\mathbf{u}$ and $\mathbf{v}$ obey the complex circularly symmetric normal distribution with mean $\mathbf{0}$ and covariance matrices $\sigma_u^2\mathbf{I}_{N_r}$ and $\sigma_v^2\mathbf{I}_{N_e}$. Bob's maximum likelihood (ML) detector is formulated as

$$\langle\mathbf{h}_{\mathfrak{T}_p(\mathbf{x}_a)},\mathfrak{M}_q(\mathbf{x}_d)\rangle=\arg\min\|\mathbf{y}-\mathbf{h}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathfrak{M}_q(\mathbf{x}_d)\|.\tag{3}$$

From Eve's perspective, the information transmitted by Alice will be detected as

$$\langle\mathbf{g}_{\mathfrak{T}_p(\mathbf{x}_a)},\mathfrak{M}_q(\mathbf{x}_d)\rangle=\arg\min\|\mathbf{z}-\mathbf{g}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathfrak{M}_q(\mathbf{x}_d)\|.\tag{4}$$

B. AN-aided CQI-mapped Generalized Spatial Modulation

For the sake of mitigating the risk of information leakage and improving the spectral efficiency, we propose a novel AN-aided CQI-mapped GSM scheme, in which the AN is

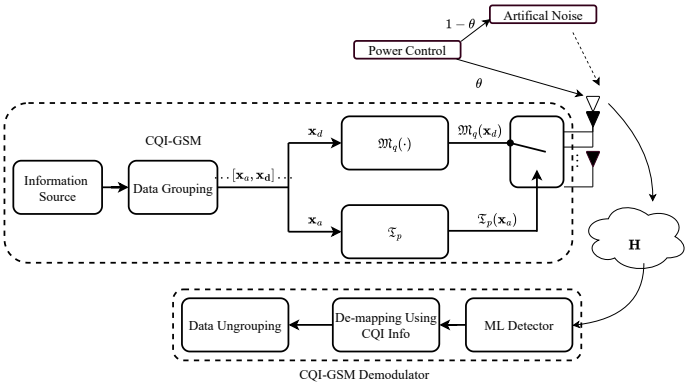


Fig. 2: AN-aided CQI-mapped generalized spatial modulation.

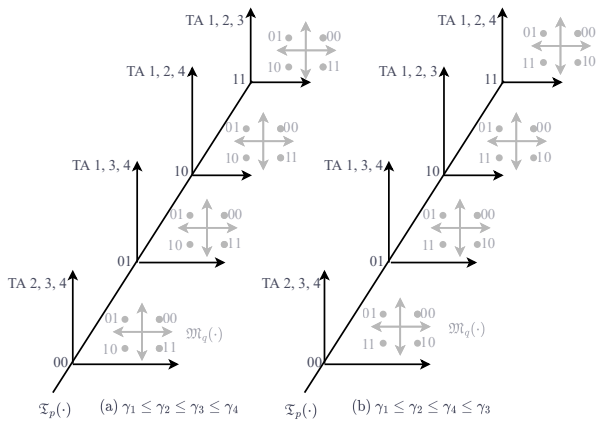


Fig. 3: Two possible instances of $\mathfrak{T}_p$ and $\mathfrak{M}_q$ in the context of $N_t = 4$, $N_a = 3$, $M = 4$.

transmitted via multiple active TAs. The whole scheme is illustrated in Fig. 2

As seen in (2), Alice's information can be overheard under the assumption that Eve knows the CSI $\mathbf{G}$, which may indeed be extracted by a sophisticated Eve. Therefore, we aim for confusing Eve by the AN which is harmless to Bob.

Firstly, if multiple TAs are used, we may constitute $\mathbf{H}_{\mathfrak{T}_p(\mathbf{x}_a)}$ to deactivate specific TAs, where the corresponding columns become zero vectors. Note that in contrast to its CQI-SM counterpart, $\mathfrak{T}_p(\cdot)$ is extended to the multiple-antenna case. A pair of instances of $\mathfrak{T}_p(\cdot)$ and $\mathfrak{M}_q(\cdot)$ are characterized in Fig. 3 and Table II. The mapping $\mathfrak{T}_p$ here maps the bit string $\mathbf{x}_a$ to a N_a-tuple, rather than to a scalar n. Accordingly, we highlight these changes. Upon assuming that the N_a-tuple is $(1, 2, 3)$, the vector $\mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_a}_{\mathfrak{M}_q(x_d)}$ is defined as $(\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3)\mathfrak{M}_q(x_d)$, while all elements of the vector $\mathbf{s}_{\mathfrak{M}_q(\mathbf{x_d})}$ are equal to $\mathfrak{M}_q(\mathbf{x}_d)$. The symbol $\mathbf{H}_{\mathfrak{T}_p(\mathbf{x}_a)}$ represents the matrix by setting all but the columns $(1, 2, 3)$ of $\mathbf{H}$ to zero and the vector $\mathbf{h}_{\mathfrak{T}_p(\mathbf{x}_a)}$ represents the associated sum of all columns. Assume that $\gamma_1 \le \gamma_2 \le \gamma_4 \le \gamma_3$, an example is that the bit string 0001 means the symbol s_1 is transmitted via TA (2,3,4). Upon applying the singular value decomposition (SVD) to $\mathbf{H}_{\mathfrak{T}_p(\mathbf{x}_a)}$, we have

$$\mathbf{H}_{\mathfrak{T}_p(\mathbf{x}_a)} = \mathbf{U}[\mathbf{D} \quad 0][\mathbf{V}_1 \ \mathbf{V}_0]^{\mathrm{H}}, \tag{5}$$

where $\mathbf{U}$ is a unitary matrix and $[\mathbf{D}\ 0] \in \mathbb{C}^{N_r \times N_t}$ has diagonal elements that are the singular values of $\mathbf{H}_{\mathfrak{T}_p(\mathbf{x}_a)}$. Furthermore, $\mathbf{V}_0 \in \mathbb{C}^{N_t \times (N_t - N_r)}$ represents the null space of $\mathbf{H}_{\mathfrak{T}_p(\mathbf{x}_a)}$, i.e., $\mathbf{H}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathbf{V}_0 = \mathbf{0}$. According to [6], the AN-aided signal can be expressed as

$$\tilde{\mathbf{s}}^{\mathfrak{T}_p(\mathbf{x}_a)}_{\mathfrak{M}_q(\mathbf{x}_d)} = \zeta \mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_a)}_{\mathfrak{M}_q(\mathbf{x}_d)} + \mathbf{V}\mathbf{r}, \tag{6}$$

where $\mathbf{V}(\mathfrak{T}_p(\mathbf{x}_a), :) = \mathbf{V}_0$ and the AN vector $\mathbf{r} \sim \mathcal{CN}(\mathbf{0}, \sigma_r^2 \mathbf{I}_{N_a - N_r})$. Upon substituting (6) into (1), we have

$$\begin{aligned}\mathbf{y} &= \mathbf{H}\mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_a)}_{\mathfrak{M}_q(\mathbf{x}_d)} + \mathbf{u} \\ &= \mathbf{H}(\zeta \mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_a)}_{\mathfrak{M}_q(\mathbf{x}_d)} + \mathbf{V}\mathbf{r}) + \mathbf{u} \\ &= \mathbf{H}_{\mathfrak{T}_p(\mathbf{x}_a)}(\zeta \mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_d)} + \mathbf{V}_0\mathbf{r}) + \mathbf{u} \\ &= \zeta \mathbf{h}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathfrak{M}_q(\mathbf{x}_d) + \mathbf{u}. \end{aligned} \tag{7}$$

Thus, Bob will use the same ML detector as (3). By contrast, the AN adds interference to Eve's received signal, yielding

$$\begin{aligned}\mathbf{z} &= \mathbf{G}(\zeta \mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_a)}_{\mathfrak{M}_q(\mathbf{x}_d)} + \mathbf{V}\mathbf{r}) + \mathbf{v} \\ &= \mathbf{G}_{\mathfrak{T}_p(\mathbf{x}_a)}(\zeta \mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_d)} + \mathbf{V}_0\mathbf{r}) + \mathbf{v} \\ &= \zeta \mathbf{g}_{\mathfrak{T}_p}(\mathbf{x}_a)\mathfrak{M}_q(\mathbf{x}_d) + \mathbf{G}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathbf{V}_0\mathbf{r} + \mathbf{v}. \end{aligned} \tag{8}$$

where these symbols are defined similarly.

In the worst case considered, Eve has perfect knowledge of $\mathbf{G}$ and applies the ML detection based on (4) as

$$\langle \mathbf{g}_{\mathfrak{T}_p}(\mathbf{x}_a), \mathfrak{M}_q(\mathbf{x}_d) \rangle = \arg\min \| z - \zeta \mathbf{g}_{\mathfrak{T}_p}(\mathbf{x}_a)\mathfrak{M}_q(\mathbf{x}_d) \|. \tag{9}$$

TABLE II: The mapping pattern of $\mathfrak{T}_p$ and $\mathfrak{M}_q$ with $N_t = 4$, $N_a = 3$, $M = 4$

CQI Pattern p	$\mathfrak{T}_p$		$\mathfrak{M}_q$	
$\gamma_1 \le \gamma_2 \le \gamma_3 \le \gamma_4$	$00 \leftrightarrow (2,3,4)$	$01 \leftrightarrow (1,3,4)$	$00 \leftrightarrow s_1$	$01 \leftrightarrow s_2$
	$10 \leftrightarrow (1,2,4)$	$11 \leftrightarrow (1,2,3)$	$10 \leftrightarrow s_3$	$11 \leftrightarrow s_4$
$\gamma_1 \le \gamma_2 \le \gamma_4 \le \gamma_3$	$00 \leftrightarrow (2,3,4)$	$01 \leftrightarrow (1,3,4)$	$00 \leftrightarrow s_1$	$01 \leftrightarrow s_2$
	$10 \leftrightarrow (1,2,3)$	$11 \leftrightarrow (1,2,4)$	$10 \leftrightarrow s_4$	$11 \leftrightarrow s_3$
$\gamma_1 \le \gamma_3 \le \gamma_2 \le \gamma_4$	$00 \leftrightarrow (2,3,4)$	$01 \leftrightarrow (1,2,4)$	$00 \leftrightarrow s_1$	$01 \leftrightarrow s_3$
	$10 \leftrightarrow (1,3,4)$	$11 \leftrightarrow (1,2,3)$	$10 \leftrightarrow s_2$	$11 \leftrightarrow s_4$
$\gamma_1 \le \gamma_3 \le \gamma_4 \le \gamma_2$	$00 \leftrightarrow (2,3,4)$	$01 \leftrightarrow (1,2,4)$	$00 \leftrightarrow s_1$	$01 \leftrightarrow s_3$
	$10 \leftrightarrow (1,2,3)$	$11 \leftrightarrow (1,3,4)$	$10 \leftrightarrow s_4$	$11 \leftrightarrow s_2$
$\gamma_1 \le \gamma_4 \le \gamma_2 \le \gamma_3$	$00 \leftrightarrow (2,3,4)$	$01 \leftrightarrow (1,2,3)$	$00 \leftrightarrow s_1$	$01 \leftrightarrow s_4$
	$10 \leftrightarrow (1,3,4)$	$11 \leftrightarrow (1,2,4)$	$10 \leftrightarrow s_2$	$11 \leftrightarrow s_3$
$\gamma_1 \le \gamma_4 \le \gamma_3 \le \gamma_2$	$00 \leftrightarrow (2,3,4)$	$01 \leftrightarrow (1,2,3)$	$00 \leftrightarrow s_1$	$01 \leftrightarrow s_4$
	$10 \leftrightarrow (1,2,4)$	$11 \leftrightarrow (1,3,4)$	$10 \leftrightarrow s_3$	$11 \leftrightarrow s_2$
$\gamma_2 \le \gamma_1 \le \gamma_3 \le \gamma_4$	$00 \leftrightarrow (1,3,4)$	$01 \leftrightarrow (2,3,4)$	$00 \leftrightarrow s_2$	$01 \leftrightarrow s_1$
	$10 \leftrightarrow (1,2,4)$	$11 \leftrightarrow (1,2,3)$	$10 \leftrightarrow s_3$	$11 \leftrightarrow s_4$
$\gamma_2 \le \gamma_1 \le \gamma_4 \le \gamma_3$	$00 \leftrightarrow (1,3,4)$	$01 \leftrightarrow (2,3,4)$	$00 \leftrightarrow s_2$	$01 \leftrightarrow s_1$
	$10 \leftrightarrow (1,2,3)$	$11 \leftrightarrow (1,2,4)$	$10 \leftrightarrow s_4$	$11 \leftrightarrow s_3$
$\gamma_2 \le \gamma_3 \le \gamma_1 \le \gamma_4$	$00 \leftrightarrow (1,3,4)$	$01 \leftrightarrow (1,2,4)$	$00 \leftrightarrow s_2$	$01 \leftrightarrow s_3$
	$10 \leftrightarrow (2,3,4)$	$11 \leftrightarrow (1,2,3)$	$10 \leftrightarrow s_1$	$11 \leftrightarrow s_4$
$\vdots$	$\vdots$		$\vdots$	
$\gamma_4 \le \gamma_3 \le \gamma_2 \le \gamma_1$	$00 \leftrightarrow (1,2,3)$	$01 \leftrightarrow (1,2,4)$	$00 \leftrightarrow s_4$	$01 \leftrightarrow s_3$
	$10 \leftrightarrow (1,3,4)$	$11 \leftrightarrow (2,3,4)$	$10 \leftrightarrow s_2$	$11 \leftrightarrow s_1$

* The $\leftrightarrow$ here is to reveal the correspondence.

III. Performance analysis

A. Secrecy Rate with Finite-Alphabet Inputs

The power ratio of the data and AN allocated to $\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_d)}^{\mathfrak{T}_p(\mathbf{x}_a)}$ is θ $(0 < \theta \leq 1)$, which implies that

$$\zeta^2 E\{\|\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_d)}^{\mathfrak{T}_p(\mathbf{x}_a)}\|^2 = \theta E_s \tag{10}$$

$$E\{\|\mathbf{Vr}\|^2\} = (1-\theta)E_s. \tag{11}$$

Consequently, we arrive at

$$\zeta = \sqrt{\theta}, \qquad \sigma_r^2 = \frac{(1-\theta)E_s}{N_t - N_r}. \tag{12}$$

The secrecy rate of our AN-aided CQI-mapped GSM is formulated for the scenario that the input has a finite alphabet. Without loss of generality, the total power of transmitting the signal plus AN is assumed to be 1, hence the SNR is $\rho = 1/\sigma_u^2$.

By definition, the secrecy rate is given by the positive difference between the achievable data rate of Bob and Eve, which is formulated as

$$R_s = \max\{0, R_B - R_E\}. \tag{13}$$

Based on the analysis in [17] and [18], R_B is formulated as

$$R_B = \log_2 M\binom{N_t}{N_a} - \frac{1}{\binom{N_t}{N_a}} \sum_{m_1=1}^{M} \sum_{n_1=1}^{\binom{N_t}{N_a}} E_v \left[\log_2 \Big(\sum_{m_2=1}^{M} \sum_{n_2=1}^{\binom{N_t}{N_a}} \phi \Big) \right], \tag{14}$$

where we have

$$\phi = \exp\Big(- \frac{\|\zeta^2(\mathbf{h}_{n_1}^* x_{m_1} - \mathbf{h}_{n_2}^* x_{m_2}) + \mathbf{u}\|^2 - \|\mathbf{u}\|^2}{\sigma_{\mathbf{u}}^2} \Big) \tag{15}$$

and for simplicity $\mathbf{h}_{n_1}$ denotes the sum of the chosen channel gains and s_{m_1} represents a specific PSK/QAM symbol.

Let $\mathbf{w} = \mathbf{GV}r + \mathbf{v}$ represent the interference caused by the transmitter and the environment. Similarly, the Eve's data rate may be expressed for the TA-bits as

$$R_{E_a} = \log_2 \binom{N_t}{N_a} - \frac{1}{M\binom{N_t}{N_a}} \sum_{m_1=1}^{M} \sum_{n_1=1}^{\binom{N_t}{N_a}} E_{\mathbf{w}}[\log_2(1 + \sum_{n_2=1, n_2 \neq n_1}^{\binom{N_t}{N_a}} (2,3,4))], \tag{16}$$

where

$$\Phi_1 = \exp\left(-\Re\{(\zeta(\mathbf{g}_{n_1}^* - \mathbf{g}_{n_2}^*)s_{m_1} + \mathbf{w})^H \Sigma^{-1} (\zeta(\mathbf{g}_{n_1}^* - \mathbf{g}_{n_2}^*)s_{m_1} + \mathbf{w}) - \mathbf{w}^H \Sigma^{-1}\mathbf{w}\}\right). \tag{17}$$

By contrast, for the PSK/QAM bits, Eve's rate is:

$$R_{E_d} = \log_2 M - \frac{1}{M\binom{N_t}{N_a}} \sum_{m_1=1}^{M} \sum_{n_1=1}^{\binom{N_t}{N_d}} E_{\mathbf{w}}\{\Delta_1 - \Delta_2\}, \tag{18}$$

where

$$\Delta_1 = \log_2 \Big(\sum_{m_2=1}^{M} \sum_{n_2=1}^{\binom{N_t}{N_a}} \exp -\Re\{(\zeta(\mathbf{g}_{n_1}^* s_{m_1} - \mathbf{g}_{n_2}^* s_{m_2}) + \mathbf{w})^{\mathrm{H}} \Sigma^{-1} (\zeta(\mathbf{g}_{n_1}^* s_{m_1} - \mathbf{g}_{n_2}^* s_{m_2}) + \mathbf{w}) - \mathbf{w}^H \Sigma^{-1}\mathbf{w}\} \Big) \tag{19}$$

$$\Delta_2 = \log_2 \Big(\sum_{n_2=1}^{\binom{N_t}{N_a}} \exp\left(-\Re\{(\zeta(\mathbf{g}_{n_1}^* - \mathbf{g}_{n_2}^*)s_{m_1} + \mathbf{w})^{\mathrm{H}} \Sigma^{-1} (\zeta(\mathbf{g}_{n_1}^* - \mathbf{g}_{n_2}^*)s_{m_1} + \mathbf{w})\}\right) \Big). \tag{20}$$

The covariance matrix of the random variable $\mathbf{w}$ is $\Sigma = \mathbf{GVV^T G^T}\sigma_r^2 + \sigma_v^2 \mathbf{I}_{N_e \times N_e}$.

As shown in (14), the secrecy rate increases with the SNR ρ, and converges to $\log_2 M\binom{N_t}{N_a}$ when the SNR tends to infinity. Explicitly, we have $\lim_{\mathrm{SNR}\to\infty} R_B = \log_2 M\binom{N_t}{N_a}$, which is the upper bound on the data rate of classical GSM. As a benefit of CQI-mapping, Eve could only successfully detect the TA bits $\mathbf{x}_a$ with probability $1/\binom{N_t}{N_a}$ and successfully decode the PSK/QAM bits $\mathbf{x}_d$ with probability $1/M$. Therefore, the final achievable rate over the wiretap channel relying on finite alphabet inputs is formulated as

$$R_E = \frac{1}{\binom{N_t}{N_a}} R_{E_a} + \frac{1}{M} R_{E_d}, \tag{21}$$

where R_{E_a} and R_{E_d} are the data rates associated with the transmissions of $\mathbf{x}_a$ and $\mathbf{x}_d$ over the wiretap channel, respectively. As usual, the data rates R_{E_a} and R_{E_d} are increasing functions of the SNR, where we have

$$\lim_{\mathrm{SNR}\to\infty} R_{E_a} = \log_2 \binom{N_t}{N_a} \tag{22}$$

$$\lim_{\mathrm{SNR}\to\infty} R_{E_d} = \log_2 M. \tag{23}$$

Substituting (22) and (23) into (13), we get

$$\lim_{\mathrm{SNR}\to\infty} R_s = \frac{\binom{N_t}{N_a} - 1}{\binom{N_t}{N_a}} \log_2 \binom{N_t}{N_a} + \frac{M-1}{M} \log_2 M. \tag{24}$$

In practice, the cardinality of the TA-pattern and PSK/QAM is far higher than 1. Hence, we have

$$\lim_{\mathrm{SNR}\to\infty} R_s = \log_2 \binom{N_t}{N_a} + \log_2 M, \tag{25}$$

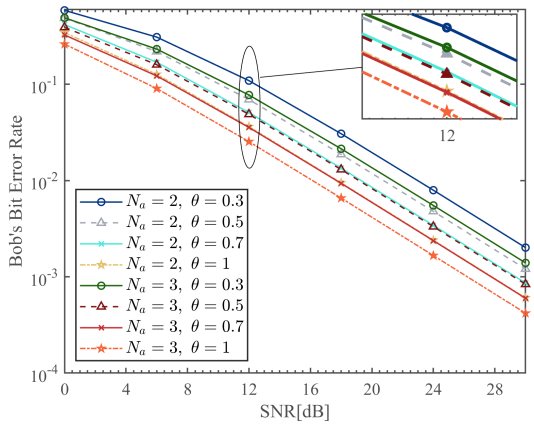
which implies that the data rate in the high SNR region is dominated by Bob's data rate over the legitimate link, provided that M and N_t are much larger than 1.

B. BER Analysis

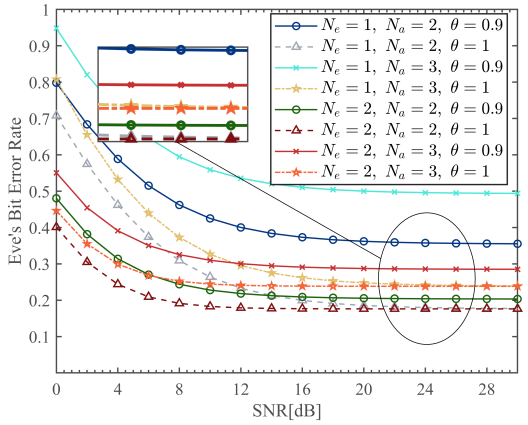
Since each pattern is equally likely, the average bit error rate (ABER) is the expectation of the individual mapping pattern:

$$\mathrm{ABER}_B \leq \frac{1}{2^\eta P} \times \sum_{p=1}^{N_t!} \sum_{q=1}^{M!} \sum_{l_x, m_1} \sum_{ly, m_2} \frac{D(\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_{d_1})}^{\mathfrak{T}_p(\mathbf{x}_{a_1})}, \mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_{d_2})}^{\mathfrak{T}_p(\mathbf{x}_{a_2})})}{\eta} E_H\{P_{error}\}, \tag{26}$$

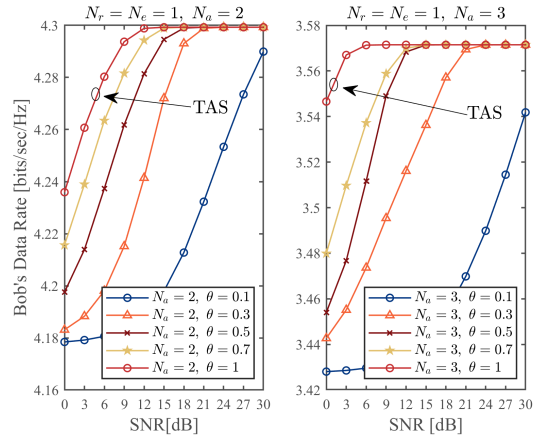
where $D(\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_{d_1})}^{\mathfrak{T}_p(\mathbf{x}_{a_1})}, \mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_{d_2})}^{\mathfrak{T}_p(\mathbf{x}_{a_2})})$ denotes the number of bits in the pair of transmitted symbols $\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_d)}^{\mathfrak{T}_p(\mathbf{x}_a)}$ and $\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_d)}^{\mathfrak{T}_p(\mathbf{x}_a)}$, along with $\mathbf{s}_{\mathfrak{M}_q(\mathbf{x}_{d_1})}^{\mathfrak{T}_p(\mathbf{x}_{a_1})}$ representing the symbol when the l_x^{th} antenna combination and m^{th} constellation symbol are chosen. Herein, $P = N_t! M!$, and $E_H\{P_{error}\}$ represents the expectation of the pairwise error probability (PEP) of the channel $\mathbf{H}$.



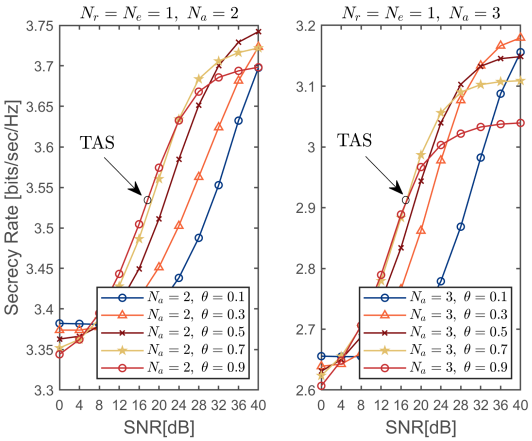
(a) BER performance of Eve for $N_t = 4, N_r = 1, M = 4, N_e = 1, 2$ and $\theta = 0.9, 1$



(b) BER performance of Eve for $N_t = 4, N_r = 1, M = 4, N_e = 1, 2$ and $\theta = 0.9, 1$



(c) Bob's data rate for $N_r = 1$ antenna at Bob and $N_e = 1$ antenna at Eve. Bob's data rate equals to the data rate of traditional GSM when $\theta = 1$.



(d) Secrecy rate of the proposed scheme with $N_r = 1$ antenna at Bob and $N_e = 1$ antenna at Eve. In the case of finite-alphabet input over Rayleigh channel, the mapping patterns substantially increase the secrecy rate.

According to (3), the PEP in (26) can be formulated as

$$P_{error}=\Pr\left(||y-\zeta\mathbf{H}\mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_{a_1})}_{\mathfrak{M}_q(\mathbf{x}_{d_1})}||^2 > ||y-\zeta\mathbf{H}\mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_{a_2})}_{\mathfrak{M}_q(\mathbf{x}_{d_2})}||^2\right)$$
$$= Q\left(\sqrt{\frac{\theta||\mathbf{H}\Phi_{p,q}||}{2\sigma_u^2}}\right), \tag{27}$$

where we have $\Phi_{p,q} = \mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_{a_1})}_{\mathfrak{M}_q(\mathbf{x}_{d_1})} - \mathbf{s}^{\mathfrak{T}_p(\mathbf{x}_{a_2})}_{\mathfrak{M}_q(\mathbf{x}_{d_2})}$. Based on the analysis in [19], the ABER is bounded as in (26), yielding

$$E_H\{P_{error}\} \leq \frac{1}{2|I_{N_rN_t} + \frac{\theta}{2\sqrt{2}\sigma_u^2}\Lambda_{p_1,m_1}|}, \tag{28}$$

where we have $\Lambda_{p_1,m_1} = \mathbf{I}_{N_r} \otimes \Phi_{p1,m1}\Phi^{\mathrm{H}}_{p_1,m_1}$. This gives a tight upper bound of the expectation of the PEP. With further reference to [19], the ABER of Eve may be approximated as

$$\mathrm{ABER}_E \leq \frac{1}{2^\eta P^2}\sum_{p_1=1}^{N_t!}\sum_{q_1=1}^{M!}\sum_{p_2=1}^{N_t!}\sum_{q_2=1}^{M!}$$
$$\sum_{l_x,m_1}\sum_{l_y,m_2}\frac{D(\mathbf{s}^{\mathfrak{T}_{p_1}(\mathbf{x}_{a_1})}_{\mathfrak{M}_{q_1}(\mathbf{x}_{d_1})}, \mathbf{s}^{\mathfrak{T}_{p_2}(\mathbf{x}_{a_2})}_{\mathfrak{M}_{q_2}(\mathbf{x}_{d_2})})}{\eta}E_H\{P_{error}\}, \tag{29}$$

where we have

$$E_H\{P_{error}\} \leq \frac{1}{2|I_{N_eN_t} + \frac{\theta}{2\sqrt{2}[\sigma_u^2+(1-\theta)N_a]}\Lambda^{p_2,m_2}_{p_1,m_1}|} \tag{30}$$

along with $\Lambda_{p_1,m_1} = \mathbf{I}_{N_r} \otimes \Phi^{p_2,m_2}_{p1,m1}\Phi^{p_2,m_2\,H}_{p_1,m_1}$ and $\Phi^{p_2,m_2}_{p1,m1} = \mathbf{s}^{\mathfrak{T}_{p_1}(\mathbf{x}_{a_2})}_{\mathfrak{M}_{q_1}(\mathbf{x}_{d_1})} - \mathbf{s}^{\mathfrak{T}_{p_2}(\mathbf{x}_{a_2})}_{\mathfrak{M}_{q_2}(\mathbf{x}_{d_2})}$. Therefore, the union bound of Eve's BER can be approximated by substituting (30) into (29).

C. Complexity Analysis

By referring to [20], the computational complexity of the ML receiver is formulated as

$$C = (4N_t + 4)N_r 2^\eta \tag{31}$$

where $\eta = \lfloor\binom{N_t}{N_a}\rfloor + M$. Note that each complex multiplication may be deemed equivalent to four real multiplications since $(a + jb) \times (c + jd) = (a \times c - b \times d) + j(b \times c + a \times d)$. The ML detection (3) may be written as $\sum_{j=1}^{N_r}\|y(j) - \sum_{i=1}^{N_t}\mathbf{H}(j,i)\mathbf{s}^{\mathfrak{T}_{p(\mathbf{x}_a)}}_{\mathfrak{M}_q(\mathbf{x}_d)}(i)\|^2$, where the multiplication $\mathbf{H}(j,i)\mathbf{s}^{\mathfrak{T}_{p(\mathbf{x}_a)}}_{\mathfrak{M}_q(\mathbf{x}_d)}(i)$ needs four multiplications and

the inner sum requires another N_t multiplications. Then we need another four operations to carry out the squaring. These operations are repeated N_r times and over the cardinality of the constellation graph, which equals 2^η. Therefore, our scheme needs $(4N_t + 4)N_r 2^\eta$ multiplication operations. In contrast to its CQI-SM counterpart, the complexity of our scheme slightly increases, but its security level is significantly improved. Note that these CQI-Mapping patterns are known to both Alice and Bob, hence the complexity is comparable to that of the conventional GSM and the CQI-mapping pattern is further exploited for increasing the security level.

IV. Simulation Results

In this section, numerical results are provided for characterizing both the BER and the secrecy rate, where $E_s = 1$ and $\sigma_u = \sigma_v$ are assumed.

In Fig. 4a, the BER performance of our AN-aided CQI-mapped GSM is characterized for $N_t = 4, N_r = 1, N_e = 1$. Different number of TAs and power ratios θ are used. When $\theta = 1$, the AN is eliminated to show the impact of the number of the active TAs. This corresponds the transmission antenna selection (TAS). According to (26), the ABER's upper bound shows that as expected, multiple TAs outperform a single TA. Additionally, as the power allocated to the signal grows, Bob's ABER improves to some extent. This figure indicates that the performance experienced by Bob is the same as that of ordinary GSM in the absence of AN.

The BER corresponding to different number of eavesdropper antennas is analyzed in Fig. 4b, where we have $N_e = \{1, 2\}, N_a = \{2, 3\}, \theta = \{0.9, 1\}$. Fig. 4b demonstrates the advantages of both AN and of multiple antennas. The system having $\theta = 1$ and $N_a = 2$ is adopted as the benchmark. It can be observed that Eve's performance is degraded, when AN is added. In conclusion, the employment of multiple antennas and the transmission of AN in the direction of Eve beneficially improves the system's ABER .

Figs. 4c and 4d quantify Bob's data rate and secrecy rate, when different numbers of antennas are activated. When $N_t = 4$ TAs are employed, activating $N_a = 2$ antennas at Alice is optimal, since $\binom{N_t}{N_a}$ is maximized when $N_a = \lfloor \frac{N_t}{2} \rfloor$. The power allocation coefficient θ varies when $N_a = 2$ and $N_a = 3$ antennas are active. As θ reduced, the AN power increases and the secrecy rate becomes higher. However, excessive AN may impair the performance, because the power of the signal is also reduced. When the SNR is low, the additive AN confuses the Eves and results in improved secrecy performance. As the SNR grows, the impact of AN is reduced and the secrecy rate becomes similar to that without AN added.

V. Conclusion

By exploiting all possible mapping patterns, a new AN aided GSM scheme has been conceived since the eavesdropper has no knowledge about the CQI of the legitimate channel, its ability to successfully decode the confidential information is limited. Furthermore, the theoretical BER and secrecy rate expressions are derived, which reveal that the proposed scheme outperforms the previously conceived CQI-mapped SM scheme, as a benefit of the AN added.

References

[1] N. Ishikawa, S. Sugiura, and L. Hanzo, "50 years of permutation, spatial and index modulation: From classic RF to visible light communications and data storage," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 1905–1938, 2018.

[2] R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2228–2241, 2008.

[3] M. Wen, B. Zheng, K. J. Kim, M. Di Renzo, T. A. Tsiftsis, K.-C. Chen, and N. Al-Dhahir, "A survey on spatial modulation in emerging wireless systems: Research progresses and applications," *IEEE J.Sel. A. Commun.*, vol. 37, no. 9, p. 19491972, sep 2019.

[4] A. Younis, N. Serafimovski, R. Mesleh, and H. Haas, "Generalised spatial modulation," in *2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers*, 2010, pp. 1498–1502.

[5] Y. Yang and S. Aissa, "Information guided channel hopping with an arbitrary number of transmit antennas," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1552–1555, 2012.

[6] H. Niu, X. Lei, Y. Xiao, Y. Li, and W. Xiang, "Performance analysis and optimization of secure generalized spatial modulation," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4451–4460, 2020.

[7] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 877–889, 2018.

[8] F. Wu, L.-L. Yang, W. Wang, and Z. Kong, "Secret precoding-aided spatial modulation," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1544–1547, 2015.

[9] Z. Kong, S. Yang, D. Wang, and L. Hanzo, "Robust beamforming and jamming for enhancing the physical layer security of full duplex radios," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3151–3159, 2019.

[10] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of mimoofdm systems by beamforming and artificial noise generation," *Physical Communication*, vol. 4, no. 4, pp. 313–321, 2011, special issue on Advances in MIMO-OFDM.

[11] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.

[12] J. Zheng, "Adaptive index modulation for parallel gaussian channels with finite alphabet inputs," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6821–6827, 2016.

[13] E. Aydin, F. Cogen, and E. Basar, "Code-index modulation aided quadrature spatial modulation for high-rate MIMO systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 10 257–10 261, 2019.

[14] Y. Yang, M. Ma, S. Assa, and L. Hanzo, "Physical-layer secret key generation via CQI-mapped spatial modulation in multi-hop wiretap ad-hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1322–1334, 2021.

[15] Y. Liu, Y. Yang, L.-L. Yang, and L. Hanzo, "Physical layer security of spatially modulated sparse-code multiple access in aeronautical ad hoc networking," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2436–2447, 2021.

[16] H. Niu, X. Lei, Y. Xiao, D. Liu, Y. Li, and H. Zhang, "Power minimization in artificial noise aided generalized spatial modulation," *IEEE Communications Letters*, vol. 24, no. 5, pp. 961–965, 2020.

[17] X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *2012 International Conference on Wireless Communications and Signal Processing (WCSP)*, 2012, pp. 1–4.

[18] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[19] R. Mesleh and A. Alhassi, *Information Theoretic Treatment for SMTs*. John Wiley & Sons, Ltd, 2018, ch. 5, pp. 109–140.

[20] ——, *Space Modulation Transmission and Reception Techniques*. John Wiley & Sons, Ltd, 2018, ch. 5, pp. 109–140.