Mapping-Varied Spatial Modulation for Physical Layer Security: Transmission Strategy and Secrecy Rate

Yuli Yang, *Member, IEEE*, and Mohsen Guizani, *Fellow, IEEE*

***Abstract*— In this paper, a novel transmission strategy, referred to as mapping-varied spatial modulation, is proposed for physical layer security, where the transmitter varies mapping patterns for the radiated information and the antenna information of spatial modulation, based on the instantaneous pattern of legitimate channel quality information that is unknown to eavesdroppers. Therefore, eavesdroppers cannot successfully decode the confidential information and the transmission over the legitimate link is secured from the wire-tap of eavesdroppers, without relying on higher-layer encryption. An important virtue of the proposed transmission strategy is that the transmitter does not need to know eavesdroppers' channels states at all. To further demonstrate the advantage of this scheme, its secrecy rate was formulated for the purpose of facilitating the performance evaluation. Moreover, illustrative numerical results pertaining to the metrics of ergodic secrecy rate and secrecy outage probability not only substantiate the validity of the proposed transmission strategy, but also provide useful references for the system design with the mapping-varied spatial modulation, from the view of physical layer security.**

***Index Terms*— Multiple-input-multiple-output (MIMO) wire-tap channel, physical layer security, secrecy rate, spatial modulation.**

I. Introduction

Since information-theoretic framework of secrecy communications was initiated by Shannon [1], fundamental capability of physical layer security to provide confidentiality has been characterized and developed to break the tradition that security is a higher-layer issue; see e.g., [2]–[5] and references therein. Without relying on higher-layer encryption, inherent randomness of the legitimate link is exploited to make eavesdroppers unable to extract the confidential information from their wire-tapping, thus achieving physical layer security [6], [7].

Especially in time division duplexing (TDD) systems, channel reciprocity between the transmitter and its intended receiver is validated at no additional bandwidth cost [8], [9], where the intended/legitimate receiver's channel state information (CSI) is perfectly known at the transmitter. As there is no CSI feedback signal, eavesdroppers can never obtain any knowledge of the CSI over the legitimate link.

On the other hand, a key assumption for the study of secrecy capacity is the eavesdropper's CSI known by the transmitter. In a genie-aided multiple-input-multiple-output (MIMO) wire-tap channel, where the instantaneous eavesdropper's CSI is available at the transmitter, a suitable optimization based upon this CSI over the transmitter's input covariance matrix can achieve perfect secrecy capacity [10], [11]. If only the statistics of eavesdropper's CSI is available at the transmitter, artificial noise that is orthogonal to the legitimate receiver can be injected to degrade the channel quality of the eavesdropper [12], [13].

However, in practice, it is infeasible or impossible for the transmitter to obtain the eavesdropper's CSI. If neither instantaneous CSI from the transmitter to the eavesdropper nor its statistics is available at the transmitter, an approach to power allocation is suggested in [14] for artificial noise injection over MIMO wire-tap channels. Moreover, an artificial noise scheme is proposed in [15] for single-input-single-output systems over multi-path channels.

Against this backdrop, we intend to exploit the concept of spatial modulation for the physical layer security over MIMO wire-tap channels where the eavesdropper's CSI is not known by the transmitter at all. Originally, spatial modulation is initiated to improve the spectral efficiency of multi-antenna channels in an open-loop link, where the transmitter does not know the legitimate receiver's CSI [16]–[18]. The performance of this approach has been considered in various networks [19]–[21]. Recently, optimal spatial-design [22] and power allocation [23] have been developed for spatial modulation in closed-loop links to further increase its achievable data rate, where the CSI over the legitimate link is available at the transmitter.

In the literature, spatial modulation has been investigated from the view of physical layer security. In [24], the security rate of spatial modulation with finite-alphabet input is analysed with the assumption that instantaneous eavesdropper's CSI is genie-provided at the transmitter. In [25], jamming signals are injected into the transmission of spatial modulation to enhance the security. In [26], the indices of transmit antennas in spatial modulation are defined based on the instantaneous legitimate CSI for the sake of security. In [27], the security of spatial modulation is enhanced by the full-duplex receiver's jamming signals.

Different from previous works on the security issues of traditional spatial modulation, a novel transmission strategy is proposed in this paper to achieve physical layer security. With the proposed scheme, the transmitter varies the mapping patterns of both antenna information and radiated information in the spatial modulation, according to instantaneous channel state pattern over the legitimate link. Hence, this scheme is referred to as *mapping-varied spatial modulation*. Since unauthorized eavesdroppers that are blind to the legitimate channel state cannot know the information mapping patterns

Manuscript received September 1, 2017; revised January 31, 2018; accepted February 16, 2018. *(Corresponding author: Yuli Yang.)*

Y. Yang is with the Department of Electronic and Electrical Engineering, University of Chester, Chester CH2 4NU, United Kingdom (e-mail: y.yang@chester.ac.uk).

M. Guizani is with Department of Electrical and Computer Engineering, University of Idaho, Moscow 83844-1023, USA (e-mail: mguizani@ieee.org).

of the moment, they are not able to decode the confidential information transmitted over the legitimate link.

Unlike the physical layer security schemes with precoding or artificial noise injection, the proposed mapping-varied spatial modulation does not engage the random channel properties of the legitimate link in the transmitted signal shaping, but utilizes the randomness of channel state patterns over the legitimate link to vary the information mapping patterns at the transmitter. The fundamental advantages behind this scheme are three-fold: (i) No artificial noise is injected at the transmitter. As such, the transmit power is fully taken by useful information and high energy efficiency is achieved. (ii) The transmitted signals are not precoded by instantaneous CSI of the legitimate link and, therefore, the peak-to-average power ratio at the transmitter is the same as that of the classical (open-loop) spatial modulation. (iii) The decoding complexity at the legitimate receiver is the same as that of the classical (open-loop) spatial modulation, because the alphabet set that is used to map the antenna information and the radiated information conveyed over the legitimate link is the same as that used in the classical (open-loop) spatial modulation.

The novelty and contribution of this paper are highlighted below in three aspects.

- *Principle:* To achieve high secrecy rate with low operation complexity in the implementation of physical layer security, the security key is generated by the instantaneous channel state over the legitimate link, where neither the instantaneous information nor the statistical information with respect to the channel state from the transmitter to the eavesdropper is available at the transmitter.
- *Approach:* The security key is reflected on the mapping pattern of spatial modulation, which is varied according to the instantaneous pattern of the channel state over the legitimate link. Note that, spatial modulation is a universal scenario to exploit this approach. Actually, this approach can be devoted to constellation modulation (equivalent to varying the mapping pattern of radiated information) or space keying (equivalent to varying the mapping pattern of antenna information) as well.
- *Evaluation:* To determine the confidentiality capability offered by the proposed mapping-varied spatial modulation at the presence of eavesdroppers, the instantaneous secrecy rate is formulated in simple and analytical expressions for both generalized case with Gaussian-distributed input and practical case with finite-alphabet input.

In detailing the above contributions, the remainder of this paper is organized as follows. Section II describes the MIMO wire-tap channel model under study and proposes the novel transmission strategy, i.e., mapping-varied spatial modulation, to achieve physical layer security without any eavesdroppers' CSI available at the transmitter. Besides, the bit error rate (BER) is compared between the legitimate receiver and the eavesdropper, which verifies the validity of the proposed mapping-varied spatial modulation for physical layer security. In Section III, the analysis framework of secrecy rate is established for the proposed transmission strategy at the presence of unauthorized eavesdroppers. Based on the theoretical analyses, Section IV demonstrates numerical results to substantiate the confidentiality provided by the proposed transmission strategy, in terms of ergodic secrecy rate and secrecy outage probability. Finally, this paper is concluded in Section V.

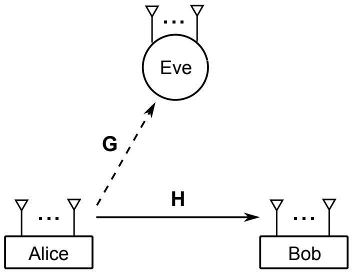

Fig. 1. MIMO wire-tap channel model.

Throughout this paper, the following mathematical notations are used: Matrices and vectors are denoted by boldface uppercase and lowercase letters, respectively. In particular, $\mathbf{0}_{M\times 1}$ denotes the $M\times 1$ zero vector and $\mathbf{I}_M$ denotes the $M\times M$ identity matrix. The transpose, the conjugate transpose and the modulus operators are denoted by $(\cdot)^{\mathrm{T}}$, $(\cdot)^{\dagger}$ and $|\cdot|$, respectively. The factorial of a non-negative integer M is denoted by $M!$. Moreover, $d^2(u,v)$ denotes the squared Euclidean distance between signals u and v. In addition, $\Pr\{\cdot\}$ denotes the probability of an event, and $\mathcal{E}\{\cdot\}$ represents the expectation (mean) operator. The probability density function (PDF) of a random variable x is denoted by $p(x)$, and the conditional PDF of x given an event A is denoted by $p(x|\mathrm{A})$.

II. Mapping-Varied Spatial Modulation for Physical Layer Security

In this section, the transmission strategy referred to as mapping-varied spatial modulation is proposed for physical layer security over MIMO wire-tap channels, where the eavesdropper's CSI is unavailable at the transmitter. Herein, the general case is presented firstly and, then, several examples are given to illustrate the proposed transmission strategy for specific scenarios. Furthermore, the BER comparisons between the legitimate receiver and the eavesdropper are reported to substantiate the security guaranteed by the proposed mapping-varied spatial modulation.

A. General Case

Consider a MIMO wire-tap channel model shown in Fig. 1, where the unauthorized eavesdropper Eve (with N_E antennas) attempts to reveal the confidential information conveyed over the legitimate link, i.e., from the transmitter Alice (with M_A antennas) to the legitimate receiver Bob (with N_B antennas). The fading channels from Alice to Bob and Eve are denoted by the $N_B\times M_A$ matrix $\mathbf{H}=[h_{nm}]_{N_B\times M_A}=[\mathbf{h}_1,\mathbf{h}_2,\cdots,\mathbf{h}_{M_A}]$ and the $N_E\times M_A$ matrix $\mathbf{G}=[g_{lm}]_{N_E\times M_A}=[\mathbf{g}_1,\mathbf{g}_2,\cdots,\mathbf{g}_{M_A}]$, respectively, where the $N_B\times 1$ vector $\mathbf{h}_m=[h_{1m},h_{2m},\cdots,h_{N_B,m}]^{\mathrm{T}}$ and the $N_E\times 1$ vector $\mathbf{g}_m=[g_{1m},g_{2m},\cdots,g_{N_E,m}]^{\mathrm{T}}$ contain the channels coefficients from the m^{th} antenna of Alice to all the antennas of Bob and Eve, respectively, $m=1,2,\cdots,M_A$. All the channels coefficients involved herein, i.e., h_{nm} and g_{lm} for $m=1,2,\cdots,M_A$, $n=1,2,\cdots,N_B$, $l=1,2,\cdots,N_E$, are assumed to be flat-fading over a common narrow-band and independent of each other.

To implement physical layer security, the legitimate receiver Bob's CSI, i.e., $\mathbf{H}$, is available at the transmitter Alice. Specifically in TDD systems, the channel reciprocity is validated at no additional bandwidth cost, which guarantees both Alice and Bob have the same knowledge of the CSI over the legitimate link.

With the initial idea of spatial modulation that is an open-loop approach, the signals conveyed over the legitimate link are not designed according to instantaneous legitimate CSI and, consequently, any (authorized or unauthorized) receivers can decode the spatially modulated signals as long as estimating the CSI from the transmitter to themselves.

Different from the traditional spatial modulation, we propose the mapping-varied spatial modulation for the purpose of physical layer security, where the transmitter Alice formats the spatially modulated signals based on instantaneous patterns of the channel quality information (CQI) over the legitimate link. The CQI from the m^{th} transmit antenna of Alice to Bob is denoted by $\gamma_m = \mathbf{h}_m^{\dagger}\mathbf{h}_m$, $m = 1, 2, \cdots, M_A$; thus, the CQI pattern of the legitimate link is defined as the permutation containing all CQI γ_m, $m = 1, 2, \cdots, M_A$, in descending or ascending order, i.e., $\gamma_{\sharp 1} \geqslant \gamma_{\sharp 2} \geqslant \cdots \geqslant \gamma_{\sharp M_A}$ or $\gamma_{\sharp 1} \leqslant \gamma_{\sharp 2} \leqslant \cdots \leqslant \gamma_{\sharp M_A}$, where $\sharp$ denotes the permutation order. If the CQI pattern is of descending order, $\sharp 1$ is the antenna index pertaining to the highest CQI while $\sharp M_A$ pertains to the lowest CQI, and so on. On the contrary, if the CQI pattern is given in ascending order, $\sharp 1$ is the antenna index pertaining to the lowest CQI and $\sharp M_A$ pertains to the highest CQI. Either in descending order or in ascending order, there are $M_A!$ CQI patterns in total over the legitimate link.

Founded on spatial modulation, the information bits to be transmitted at Alice is expressed as $\mathbf{x} = [\mathbf{x}_a, \mathbf{x}_d]$, where $\mathbf{x}_a$ and $\mathbf{x}_d$ are the antenna information and the radiated information, respectively. However, both the mapping of the antenna information $\mathbf{x}_a$ onto the antennas indices and the mapping of the radiated information $\mathbf{x}_d$ onto the constellation points are not fixed but varied in terms of instantaneous CQI pattern over the legitimate link, for the sake of physical layer security. In the case that Alice adopts M_d-point constellation for the radiated modulation, e.g., M_d-PSK or M_d-QAM, with M_A transmit antennas, there are $Q = M_d!$ mapping patterns for the radiated information and $P = M_A!$ mapping patterns for the antenna information.

In each transmission, the antenna-information mapping pattern and the radiated-information mapping pattern are determined by Alice according to the CQI pattern over the legitimate link of the moment. Note that, the number of antenna-information mapping patterns, $M_A!$, is the same as that of the CQI patterns over the legitimate link. For each CQI pattern, there is one and only one antenna-information mapping pattern corresponding to it. Furthermore, if $M_d < M_A$, the same mapping pattern for radiated information has to be activated by different CQI patterns, while the mapping patterns for antenna information are varied with different CQI patterns. If $M_d > M_A$, to make full use of all radiated-information mapping patterns, different mapping patterns for radiated information can be alternated in coherent occurrences with the same CQI pattern, where the same mapping pattern for antenna information is kept. Without loss of generality, the p^{th} mapping pattern for the antenna information is denoted by $\mathfrak{T}_p(\cdot)$, $p = 1, 2, \cdots, P$, and the q^{th} mapping pattern for the radiated information is denoted by $\mathfrak{M}_q(\cdot)$, $q = 1, 2, \cdots, Q$.

At an arbitrary time slot, if the p^{th} CQI pattern occurs in the legitimate link, the radiated information is modulated by Alice according to $\mathfrak{M}_q(\cdot)$ and transmitted from the antenna that is mapped by the antenna information according to $\mathfrak{T}_p(\cdot)$. Thereby, the received baseband signals at Bob and Eve are obtained by

$$\mathbf{y}_{\mathrm{B}} = \mathbf{h}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathfrak{M}_q(\mathbf{x}_d) + \mathbf{z}_{\mathrm{B}} \tag{1}$$

and

$$\mathbf{y}_{\mathrm{E}} = \mathbf{g}_{\mathfrak{T}_p(\mathbf{x}_a)}\mathfrak{M}_q(\mathbf{x}_d) + \mathbf{z}_{\mathrm{E}}, \tag{2}$$

respectively, where the $N_B \times 1$ vectors $\mathbf{y}_{\mathrm{B}}$ and $\mathbf{z}_{\mathrm{B}} \sim \mathcal{CN}\left(\mathbf{0}_{N_B\times 1}, \sigma_W^2\mathbf{I}_{N_B}\right)$ contain Bob's received signals and additive white Gaussian noise (AWGN) components, respectively. Meanwhile, the $N_E \times 1$ vectors $\mathbf{y}_{\mathrm{E}}$ and $\mathbf{z}_{\mathrm{E}} \sim \mathcal{CN}\left(\mathbf{0}_{N_E\times 1}, \sigma_W^2\mathbf{I}_{N_E}\right)$ contain Eve's received signals and AWGN components, respectively. The subscript "$\mathfrak{T}_p(\mathbf{x}_a)$" denotes the index of the transmit antenna activated by the antenna information $\mathbf{x}_a$ according to the p^{th} antenna-information mapping pattern $\mathfrak{T}_p(\cdot)$. Accordingly, the $N_B\times 1$ vector $\mathbf{h}_{\mathfrak{T}_p(\mathbf{x}_a)}$ and the $N_E\times 1$ vector $\mathbf{g}_{\mathfrak{T}_p(\mathbf{x}_a)}$ contain the channels coefficients from the activated transmit antenna of Alice to all the antennas of Bob and Eve, respectively. Moreover, $\mathfrak{M}_q(\mathbf{x}_d)$ stands for Alice's transmitted symbol mapped by the radiated information $\mathbf{x}_d$ according to the q^{th} radiated-information mapping pattern $\mathfrak{M}_q(\cdot)$.

As Bob always knows the instantaneous CQI pattern of the legitimate link, the radiated-information mapping pattern $\mathfrak{M}_q(\cdot)$ and the antenna-information mapping pattern $\mathfrak{T}_p(\cdot)$ adopted by Alice are obvious to Bob. Upon receiving the signals $\mathbf{y}_{\mathrm{B}}$, Bob may decode the radiated information $\mathbf{x}_d$ and the antenna information $\mathbf{x}_a$ via the following two-step maximum-likelihood algorithm [16]: First, the candidate decisions are made in terms of

$$\mathfrak{M}_q(\hat{\mathbf{x}}_{d,m}) = \arg\min_{s\in\mathfrak{M}_q(\cdot)} d^2\left(\mathbf{h}_m^{\dagger}\mathbf{h}_m s, \mathbf{h}_m^{\dagger}\mathbf{y}_{\mathrm{B}}\right), \quad m = 1, 2, \cdots, M_A; \tag{3}$$

and then, choose $\hat{\mathbf{x}}_d = \hat{\mathbf{x}}_{d,\mathfrak{T}_p(\hat{\mathbf{x}}_a)}$ while getting $\hat{\mathbf{x}}_a$ if and only if

$$\mathfrak{T}_p(\hat{\mathbf{x}}_a) = \arg\min_{m\in\{1,2,\cdots,M_A\}} d^2\left(\mathbf{h}_m^{\dagger}\mathbf{h}_m\mathfrak{M}_q(\hat{\mathbf{x}}_{d,m}), \mathbf{h}_m^{\dagger}\mathbf{y}_{\mathrm{B}}\right), \tag{4}$$

where $\hat{\mathbf{x}}_d$ and $\hat{\mathbf{x}}_a$ are Bob's final decodings of $\mathbf{x}_d$ and $\mathbf{x}_a$, respectively.

However, since Eve does not know the CQI pattern over the legitimate link at all, it has to decode Alice's spatial modulation by use of anticipated/arbitrary radiated-information mapping pattern and antenna-information mapping pattern, denoted by $\mathfrak{M}_{\mathrm{E}}(\cdot)$ and $\mathfrak{T}_{\mathrm{E}}(\cdot)$, respectively. Similar with Bob's decoding procedure, the decoding at Eve starts with candidate decisions made by

$$\mathfrak{M}_{\mathrm{E}}(\tilde{\mathbf{x}}_{d,m}) = \arg\min_{s\in\mathfrak{M}_{\mathrm{E}}(\cdot)} d^2\left(\mathbf{g}_m^{\dagger}\mathbf{g}_m s, \mathbf{g}_m^{\dagger}\mathbf{y}_{\mathrm{E}}\right), \quad m = 1, 2, \cdots, M_A. \tag{5}$$

Subsequently, Eve's final decoding for Alice's antenna information $\mathbf{x}_a$, denoted by $\tilde{\mathbf{x}}_a$, is obtained if and only if

$$\mathfrak{T}_{\rm E}(\tilde{\mathbf{x}}_a) = \mathop{\arg\min}_{m\in\{1,2,\cdots,M_A\}} d^2\left(\mathbf{g}_m^\dagger\mathbf{g}_m\mathfrak{M}_{\rm E}(\tilde{\mathbf{x}}_{d,m}), \mathbf{g}_m^\dagger\mathbf{y}_{\rm E}\right), \tag{6}$$

whilst Eve's final decoding for Alice's radiated information $\mathbf{x}_d$ is $\tilde{\mathbf{x}}_d = \tilde{\mathbf{x}}_{d,\mathfrak{T}_{\rm E}(\tilde{\mathbf{x}}_a)}$.

After this decoding, Eve can obtain neither correct radiated information nor correct antenna information, because the probability that the mapping patterns adopted by Eve in its decoding, $\mathfrak{M}_{\rm E}$ and $\mathfrak{T}_{\rm E}$, are the same as those adopted by Alice in spatial modulation, $\mathfrak{M}_q$ and $\mathfrak{T}_p$, is very low. In detail, $\Pr\{\mathfrak{M}_{\rm E}(\cdot) = \mathfrak{M}_q(\cdot)\} = 1/(M_d!)$, and $\Pr\{\mathfrak{T}_{\rm E}(\cdot) = \mathfrak{T}_p(\cdot)\} = 1/(M_A!)$. Hence, the secrecy of the confidential information conveyed over the legitimate link can be guaranteed by the mapping-varied spatial modulation that is formatted on the basis of legitimate CQI pattern, and the confidentiality is improved with the increase in M_d and/or M_A.

B. Examples

In practice, the key of the mapping-varied spatial modulation design is to make full use of all the radiated-information mapping patterns and all the antenna-information mapping patterns, so that eavesdroppers cannot successfully decode the transmitter's spatial-modulated information.

Three examples are demonstrated herein to describe the proposed transmission strategy for physical layer security over MIMO wire-tap channels, in various cases concerning the number of radiated constellation points, M_d, and the number of Alice's transmit antennas, M_A.

1) $M_d = M_A$: For this case, we take $M_d = M_A = 4$ as an example, where Alice adopts QPSK constellation for the modulation of $\mathbf{x}_d$ and has 4 transmit antennas for the modulation of $\mathbf{x}_a$. The symbols in the QPSK constellation are denoted by $s_1 = +1$, $s_2 = +\sqrt{-1}$, $s_3 = -1$, $s_4 = -\sqrt{-1}$, and the $m^{\rm th}$ transmit antenna at Alice is denoted by $\o m$, $m = 1, 2, 3, 4$. In this example, there are 24 CQI patterns over the legitimate link. The number of antenna-information mapping patterns and that of radiated-information mapping patterns are the same, i.e., $P = Q = 24$.

An illustration of the correspondence that pairs the CQI pattern with the antenna/radiated-information mapping pattern in this example is provided in Table I, where the CQI patterns over the legitimate link are given in descending order, with $\gamma_1 = \mathbf{h}_1^\dagger\mathbf{h}_1$, $\gamma_2 = \mathbf{h}_2^\dagger\mathbf{h}_2$, $\gamma_3 = \mathbf{h}_3^\dagger\mathbf{h}_3$, $\gamma_4 = \mathbf{h}_4^\dagger\mathbf{h}_4$. For instance, in the first CQI pattern, the antennas indices $\sharp m = m$, $m = 1, 2, 3, 4$, while in the third CQI pattern, $\sharp 1 = 1$, $\sharp 2 = 3$, $\sharp 3 = 2$, $\sharp 4 = 4$. In the mapping patterns for both antenna information and radiated information, the arrow "↔" represents the processing that maps the information bits on its left-hand side into the transmit antenna or the constellation symbol on its right-hand side.

In this illustration, the $p^{\rm th}$ antenna-information mapping pattern can be expressed as $\mathfrak{T}_p(\mathbf{x}_a \leftrightarrow \o\sharp m) : \mathcal{B}(\mathbf{x}_a)+1 = \sharp m$, $p = 1, 2, \cdots, 24$, and the $q^{\rm th}$ radiated-information mapping pattern can be expressed as $\mathfrak{M}_q(\mathbf{x}_d \leftrightarrow s_{\sharp m}) : \mathcal{B}(\mathbf{x}_d)+1 = \sharp m$, $q = 1, 2, \cdots, 24$, where $\mathcal{B}(\cdot)$ denotes the function of binary coded decimals, and $\sharp m$ is the antenna index in the CQI pattern. Given a CQI pattern, the antenna information $\mathbf{x}_a = 00, 01, 10, 11$ is mapped onto the transmit antenna in the order $\sharp 1, \sharp 2, \sharp 3, \sharp 4$, and the radiated information $\mathbf{x}_d = 00, 01, 10, 11$ is mapped onto the QPSK symbols in the order $\sharp 1, \sharp 2, \sharp 3, \sharp 4$ as well. Note that, this rule is for illustration purpose and the correspondence is not limited by it. In practice, the correspondence design is very flexible and any one-to-one correspondence is suitable for pairing the CQI pattern with $\mathfrak{T}_p$ or $\mathfrak{M}_q$.

TABLE I
ILLUSTRATION OF CORRESPONDENCE BETWEEN CQI PATTERN AND ANTENNA/RADIATED-INFORMATION MAPPING PATTERN IN MAPPING-VARIED SPATIAL MODULATION WITH $M_d = M_A = 4$.

CQI Pattern p	Antenna-Information Mapping Pattern ($\mathfrak{T}_p$)	Radiated-Information Mapping Pattern ($\mathfrak{M}_q$)
$\gamma_1 \geqslant \gamma_2 \geqslant \gamma_3 \geqslant \gamma_4$	$00 \leftrightarrow \o 1$ $01 \leftrightarrow \o 2$ $10 \leftrightarrow \o 3$ $11 \leftrightarrow \o 4$	$00 \leftrightarrow s_1$ $01 \leftrightarrow s_2$ $10 \leftrightarrow s_3$ $11 \leftrightarrow s_4$
$\gamma_1 \geqslant \gamma_2 \geqslant \gamma_4 \geqslant \gamma_3$	$00 \leftrightarrow \o 1$ $01 \leftrightarrow \o 2$ $10 \leftrightarrow \o 4$ $11 \leftrightarrow \o 3$	$00 \leftrightarrow s_1$ $01 \leftrightarrow s_2$ $10 \leftrightarrow s_4$ $11 \leftrightarrow s_3$
$\gamma_1 \geqslant \gamma_3 \geqslant \gamma_2 \geqslant \gamma_4$	$00 \leftrightarrow \o 1$ $01 \leftrightarrow \o 3$ $10 \leftrightarrow \o 2$ $11 \leftrightarrow \o 4$	$00 \leftrightarrow s_1$ $01 \leftrightarrow s_3$ $10 \leftrightarrow s_2$ $11 \leftrightarrow s_4$
$\gamma_1 \geqslant \gamma_3 \geqslant \gamma_4 \geqslant \gamma_2$	$00 \leftrightarrow \o 1$ $01 \leftrightarrow \o 3$ $10 \leftrightarrow \o 4$ $11 \leftrightarrow \o 2$	$00 \leftrightarrow s_1$ $01 \leftrightarrow s_3$ $10 \leftrightarrow s_4$ $11 \leftrightarrow s_2$
$\gamma_1 \geqslant \gamma_4 \geqslant \gamma_2 \geqslant \gamma_3$	$00 \leftrightarrow \o 1$ $01 \leftrightarrow \o 4$ $10 \leftrightarrow \o 2$ $11 \leftrightarrow \o 3$	$00 \leftrightarrow s_1$ $01 \leftrightarrow s_4$ $10 \leftrightarrow s_2$ $11 \leftrightarrow s_3$
$\gamma_1 \geqslant \gamma_4 \geqslant \gamma_3 \geqslant \gamma_2$	$00 \leftrightarrow \o 1$ $01 \leftrightarrow \o 4$ $10 \leftrightarrow \o 3$ $11 \leftrightarrow \o 2$	$00 \leftrightarrow s_1$ $01 \leftrightarrow s_4$ $10 \leftrightarrow s_3$ $11 \leftrightarrow s_2$
$\gamma_2 \geqslant \gamma_1 \geqslant \gamma_3 \geqslant \gamma_4$	$00 \leftrightarrow \o 2$ $01 \leftrightarrow \o 1$ $10 \leftrightarrow \o 3$ $11 \leftrightarrow \o 4$	$00 \leftrightarrow s_2$ $01 \leftrightarrow s_1$ $10 \leftrightarrow s_3$ $11 \leftrightarrow s_4$
$\gamma_2 \geqslant \gamma_1 \geqslant \gamma_4 \geqslant \gamma_3$	$00 \leftrightarrow \o 2$ $01 \leftrightarrow \o 1$ $10 \leftrightarrow \o 4$ $11 \leftrightarrow \o 3$	$00 \leftrightarrow s_2$ $01 \leftrightarrow s_1$ $10 \leftrightarrow s_4$ $11 \leftrightarrow s_3$
$\gamma_2 \geqslant \gamma_3 \geqslant \gamma_1 \geqslant \gamma_4$	$00 \leftrightarrow \o 2$ $01 \leftrightarrow \o 3$ $10 \leftrightarrow \o 1$ $11 \leftrightarrow \o 4$	$00 \leftrightarrow s_2$ $01 \leftrightarrow s_3$ $10 \leftrightarrow s_1$ $11 \leftrightarrow s_4$
$\gamma_2 \geqslant \gamma_3 \geqslant \gamma_4 \geqslant \gamma_1$	$00 \leftrightarrow \o 2$ $01 \leftrightarrow \o 3$ $10 \leftrightarrow \o 4$ $11 \leftrightarrow \o 1$	$00 \leftrightarrow s_2$ $01 \leftrightarrow s_3$ $10 \leftrightarrow s_4$ $11 \leftrightarrow s_1$
$\gamma_2 \geqslant \gamma_4 \geqslant \gamma_1 \geqslant \gamma_3$	$00 \leftrightarrow \o 2$ $01 \leftrightarrow \o 4$ $10 \leftrightarrow \o 1$ $11 \leftrightarrow \o 3$	$00 \leftrightarrow s_2$ $01 \leftrightarrow s_4$ $10 \leftrightarrow s_1$ $11 \leftrightarrow s_3$
$\gamma_2 \geqslant \gamma_4 \geqslant \gamma_3 \geqslant \gamma_1$	$00 \leftrightarrow \o 2$ $01 \leftrightarrow \o 4$ $10 \leftrightarrow \o 3$ $11 \leftrightarrow \o 1$	$00 \leftrightarrow s_2$ $01 \leftrightarrow s_4$ $10 \leftrightarrow s_3$ $11 \leftrightarrow s_1$
$\gamma_3 \geqslant \gamma_1 \geqslant \gamma_2 \geqslant \gamma_4$	$00 \leftrightarrow \o 3$ $01 \leftrightarrow \o 1$ $10 \leftrightarrow \o 2$ $11 \leftrightarrow \o 4$	$00 \leftrightarrow s_3$ $01 \leftrightarrow s_1$ $10 \leftrightarrow s_2$ $11 \leftrightarrow s_4$
$\gamma_3 \geqslant \gamma_1 \geqslant \gamma_4 \geqslant \gamma_2$	$00 \leftrightarrow \o 3$ $01 \leftrightarrow \o 1$ $10 \leftrightarrow \o 4$ $11 \leftrightarrow \o 2$	$00 \leftrightarrow s_3$ $01 \leftrightarrow s_1$ $10 \leftrightarrow s_4$ $11 \leftrightarrow s_2$
$\gamma_3 \geqslant \gamma_2 \geqslant \gamma_1 \geqslant \gamma_4$	$00 \leftrightarrow \o 3$ $01 \leftrightarrow \o 2$ $10 \leftrightarrow \o 1$ $11 \leftrightarrow \o 4$	$00 \leftrightarrow s_3$ $01 \leftrightarrow s_2$ $10 \leftrightarrow s_1$ $11 \leftrightarrow s_4$
$\gamma_3 \geqslant \gamma_2 \geqslant \gamma_4 \geqslant \gamma_1$	$00 \leftrightarrow \o 3$ $01 \leftrightarrow \o 2$ $10 \leftrightarrow \o 4$ $11 \leftrightarrow \o 1$	$00 \leftrightarrow s_3$ $01 \leftrightarrow s_2$ $10 \leftrightarrow s_4$ $11 \leftrightarrow s_1$
$\gamma_3 \geqslant \gamma_4 \geqslant \gamma_1 \geqslant \gamma_2$	$00 \leftrightarrow \o 3$ $01 \leftrightarrow \o 4$ $10 \leftrightarrow \o 1$ $11 \leftrightarrow \o 2$	$00 \leftrightarrow s_3$ $01 \leftrightarrow s_4$ $10 \leftrightarrow s_1$ $11 \leftrightarrow s_2$
$\gamma_3 \geqslant \gamma_4 \geqslant \gamma_2 \geqslant \gamma_1$	$00 \leftrightarrow \o 3$ $01 \leftrightarrow \o 4$ $10 \leftrightarrow \o 2$ $11 \leftrightarrow \o 1$	$00 \leftrightarrow s_3$ $01 \leftrightarrow s_4$ $10 \leftrightarrow s_2$ $11 \leftrightarrow s_1$
$\gamma_4 \geqslant \gamma_1 \geqslant \gamma_2 \geqslant \gamma_3$	$00 \leftrightarrow \o 4$ $01 \leftrightarrow \o 1$ $10 \leftrightarrow \o 2$ $11 \leftrightarrow \o 3$	$00 \leftrightarrow s_4$ $01 \leftrightarrow s_1$ $10 \leftrightarrow s_2$ $11 \leftrightarrow s_3$
$\gamma_4 \geqslant \gamma_1 \geqslant \gamma_3 \geqslant \gamma_2$	$00 \leftrightarrow \o 4$ $01 \leftrightarrow \o 1$ $10 \leftrightarrow \o 3$ $11 \leftrightarrow \o 2$	$00 \leftrightarrow s_4$ $01 \leftrightarrow s_1$ $10 \leftrightarrow s_3$ $11 \leftrightarrow s_2$
$\gamma_4 \geqslant \gamma_2 \geqslant \gamma_1 \geqslant \gamma_3$	$00 \leftrightarrow \o 4$ $01 \leftrightarrow \o 2$ $10 \leftrightarrow \o 1$ $11 \leftrightarrow \o 3$	$00 \leftrightarrow s_4$ $01 \leftrightarrow s_2$ $10 \leftrightarrow s_1$ $11 \leftrightarrow s_3$
$\gamma_4 \geqslant \gamma_2 \geqslant \gamma_3 \geqslant \gamma_1$	$00 \leftrightarrow \o 4$ $01 \leftrightarrow \o 2$ $10 \leftrightarrow \o 3$ $11 \leftrightarrow \o 1$	$00 \leftrightarrow s_4$ $01 \leftrightarrow s_2$ $10 \leftrightarrow s_3$ $11 \leftrightarrow s_1$
$\gamma_4 \geqslant \gamma_3 \geqslant \gamma_1 \geqslant \gamma_2$	$00 \leftrightarrow \o 4$ $01 \leftrightarrow \o 3$ $10 \leftrightarrow \o 1$ $11 \leftrightarrow \o 2$	$00 \leftrightarrow s_4$ $01 \leftrightarrow s_3$ $10 \leftrightarrow s_1$ $11 \leftrightarrow s_2$
$\gamma_4 \geqslant \gamma_3 \geqslant \gamma_2 \geqslant \gamma_1$	$00 \leftrightarrow \o 4$ $01 \leftrightarrow \o 3$ $10 \leftrightarrow \o 2$ $11 \leftrightarrow \o 1$	$00 \leftrightarrow s_4$ $01 \leftrightarrow s_3$ $10 \leftrightarrow s_2$ $11 \leftrightarrow s_1$

During the setting of the legitimate link, a table with respect to the correspondence between CQI pattern and antenna/radiated-information mapping pattern, e.g., Table I, is supposed to be recognized by both Alice and Bob, via signaling exchange. By looking up this table, Alice prescribes the mapping patterns of antenna information and radiated information, according to instantaneous CQI pattern of the

TABLE II

Illustration of Correspondence between CQI Pattern and Antenna/Radiated-Information Mapping Pattern in Mapping-Varied Spatial Modulation with $M_d = 2, M_A = 4$.

CQI Pattern p	Antenna-Information Mapping Pattern ($\mathfrak{T}_p$)	Radiated-Information Mapping Pattern ($\mathfrak{M}_q$)
$p = 1, 2, 3, 4,$ $5, 6, 7, 8,$ $9, 10, 11, 12.$	$\mathfrak{T}_1$ $\mathfrak{T}_2$ $\mathfrak{T}_3$ $\mathfrak{T}_4$ $\mathfrak{T}_5$ $\mathfrak{T}_6$ $\mathfrak{T}_7$ $\mathfrak{T}_8$ $\mathfrak{T}_9$ $\mathfrak{T}_{10}$ $\mathfrak{T}_{11}$ $\mathfrak{T}_{12}$	$0 \leftrightarrow s_1$ $1 \leftrightarrow s_2$
$p = 13, 14, 15, 16,$ $17, 18, 19, 20,$ $21, 22, 23, 24.$	$\mathfrak{T}_{13}$ $\mathfrak{T}_{14}$ $\mathfrak{T}_{15}$ $\mathfrak{T}_{16}$ $\mathfrak{T}_{17}$ $\mathfrak{T}_{18}$ $\mathfrak{T}_{19}$ $\mathfrak{T}_{20}$ $\mathfrak{T}_{21}$ $\mathfrak{T}_{22}$ $\mathfrak{T}_{23}$ $\mathfrak{T}_{24}$	$1 \leftrightarrow s_1$ $0 \leftrightarrow s_2$

legitimate link, in each transmission. As Bob knows the legitimate CQI pattern of the moment as well, it can comprehend the mapping patterns adopted by Alice and, then, successfully decode $\mathbf{x}_a$ and $\mathbf{x}_d$ transmitted from Alice.

Meanwhile, Eve cannot correctly anticipate the mapping patterns adopted by Alice in the spatial modulation, because it does not know the CQI pattern of the legitimate link at all. The probability that the antenna/radiated-information mapping patterns anticipated by Eve and adopted by Alice are the same is $\Pr\{\mathfrak{T}_{\mathrm{E}}(\cdot) = \mathfrak{T}_p(\cdot)\} = \Pr\{\mathfrak{M}_{\mathrm{E}}(\cdot) = \mathfrak{M}_p(\cdot)\} = 1/24$, which guarantees that Eve only has the probability of $1/M_d = 1/4$ to correctly guess $\mathbf{x}_d$ and the probability of $1/M_A = 1/4$ to correctly guess $\mathbf{x}_a$, although figuring out the symbols transmitted from Alice.

2) $M_d < M_A$: For this case, we take $M_d = 2, M_A = 4$ as an example, where Alice employs BPSK constellation for the modulation of $\mathbf{x}_d$ and has 4 transmit antennas for the modulation of $\mathbf{x}_a$.

In this example, there are 24 CQI patterns over the legitimate link and 24 antenna-information mapping patterns, while the number of radiated-information mapping patterns is $Q = M_d! = 2$. An illustration of the correspondence that pairs the CQI pattern with the antenna/radiated-information mapping pattern for this example is shown in Table II, where the CQI patterns and the antenna-information mapping patterns $\mathfrak{T}_p$, $p = 1, 2, \cdots, 24$, are the same as those given in Table I. In the radiated-information mapping patterns $\mathfrak{M}_q$, $q = 1, 2$, the BPSK symbols are denoted by $s_1 = +1$ and $s_2 = -1$.

As the number of radiated-information mapping patterns is less than that of CQI patterns, either of the radiated-information mapping patterns is shared by 12 CQI patterns, where Eve successfully decodes $\mathbf{x}_d$ at the probability of $1/2$ and $\mathbf{x}_a$ at the probability of $1/4$.

3) $M_d > M_A$: For this case, we take $M_d = 4, M_A = 2$ as an example, where Alice employs QPSK constellation for the modulation of $\mathbf{x}_d$ and has 2 transmit antennas for the modulation of $\mathbf{x}_a$.

In this example, there are 24 radiated-information mapping patterns, while the number of CQI patterns and that of the antenna-information mapping patterns are both equal to $P = M_A! = 2$. An illustration of the correspondence that pairs the CQI pattern with the antenna/radiated-information mapping pattern for this example is shown in Table III, where the radiated-information mapping patterns $\mathfrak{M}_q$, $q = 1, 2, \cdots, 24$, are the same as those listed in Table I.

To make full use of all the radiated-information mapping patterns in this example, $\mathfrak{M}_q$, $q = 1, 2, \cdots, 24$, they are divided into 12 groups and each group is composed of 2 radiated-information mapping patterns that are paired with the 2 CQI patterns in one transmission (time slot). The 12 groups of radiated-information mapping patterns are alternated in 12 successive transmissions and, then, start over for the next 12 transmissions. This process is repeated for every 12 time slots. For a given 12 consecutive time slots, at the l^{th} time slot (i.e., TS l), $l = 1, 2, \cdots, 12$, Alice adopts $\mathfrak{M}_{2l-1}$ for the modulation of $\mathbf{x}_d$ if the first CQI pattern ($\gamma_1 \geqslant \gamma_2$) occurs in the legitimate link, where $\mathfrak{T}_1$ is exploited for the mapping of $\mathbf{x}_a$, while $\mathfrak{M}_{2l}$ is adopted for the modulation of $\mathbf{x}_d$ if the second CQI pattern ($\gamma_2 \geqslant \gamma_1$) occurs, where $\mathfrak{T}_2$ is exploited for the mapping of $\mathbf{x}_a$. Thereupon, the probability that Eve correctly decodes $\mathbf{x}_a$ is $1/2$, and the probability that Eve correctly decodes $\mathbf{x}_d$ is $1/4$.

TABLE III

Illustration of Correspondence between CQI Pattern and Antenna/Radiated-Information Mapping Pattern in Mapping-Varied Spatial Modulation with $M_d = 4, M_A = 2$.

CQI Pattern p		$\mathfrak{T}_p$	$\mathfrak{M}_q$
TS 1	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_1$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_2$
TS 2	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_3$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_4$
TS 3	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_5$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_6$
TS 4	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_7$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_8$
TS 5	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_9$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_{10}$
TS 6	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_{11}$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_{12}$
TS 7	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_{13}$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_{14}$
TS 8	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_{15}$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_{16}$
TS 9	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_{17}$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_{18}$
TS 10	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_{19}$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_{20}$
TS 11	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_{21}$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_{22}$
TS 12	$p = 1$: $\gamma_1 \geqslant \gamma_2$	$\mathfrak{T}_1$: $0 \leftrightarrow$ ø1 $1 \leftrightarrow$ ø2	$\mathfrak{M}_{23}$
	$p = 2$: $\gamma_2 \geqslant \gamma_1$	$\mathfrak{T}_2$: $0 \leftrightarrow$ ø2 $1 \leftrightarrow$ ø1	$\mathfrak{M}_{24}$

We remark that, since the number of CQI patterns is always the same as that of antenna-information mapping patterns, $P = M_A!$, the pairs between CQI patterns and $\mathfrak{T}_p$, $p = 1, 2, \cdots, P$, hold one-to-one correspondence on all occasions. However, if the number of CQI patterns, P, is not equal to that of radiated-information mapping patterns, $Q = M_d!$, the pairs between CQI patterns and $\mathfrak{M}_q$, $q = 1, 2, \cdots, Q$, have either many-to-one correspondence (for $P > Q$) or one-to-many correspondence (for $P < Q$).

C. Bit Error Rate

The BER comparisons between Bob and Eve with the proposed mapping-varied spatial modulation are reported in Figs. 2 and 3 for the aforementioned examples with $N_B, N_E = 2, 4$ receiving antennas at Bob and Eve.

As is shown in these figures, Bob's performance is the same as that of the classical spatial modulation. However, Eve's BER converges to 0.5 as the signal-to-noise power ratio (SNR) increases, which means that Eve cannot obtain any information

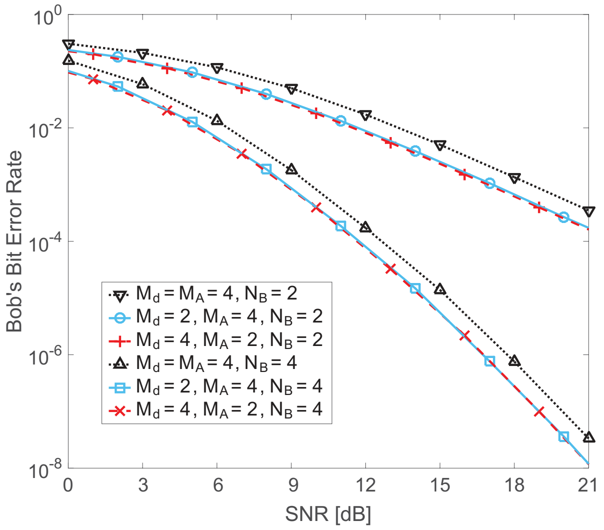

Fig. 2. Bob's bit error rate (BER) with $N_B = 2, 4$ receiving antennas.

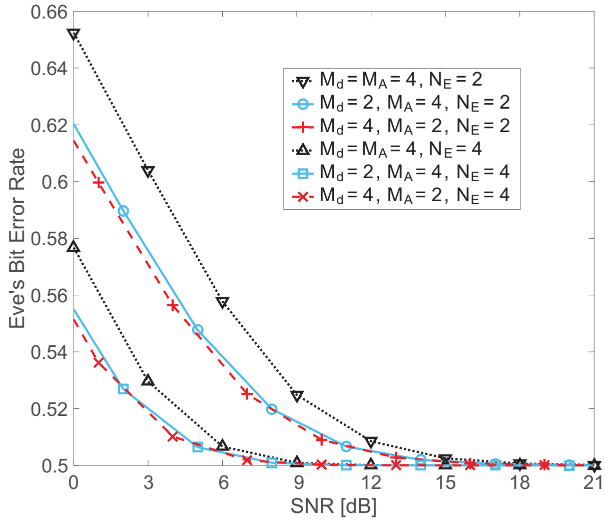

Fig. 3. Eve's bit error rate (BER) with $N_E = 2, 4$ receiving antennas.

conveyed over the legitimate link if the mapping-varied spatial modulation is exploited at Alice.

III. Secrecy Rate of Mapping-Varied Spatial Modulation

To evaluate the performance of the proposed mapping-varied spatial modulation for physical layer security over MIMO wire-tap channels, the analysis framework of its secrecy rate is established in this section, for both theoretical and practical cases.

A. Gaussian-Distributed Input

First, the secrecy rate expression of mapping-varied spatial modulation is formulated with Gaussian-distributed input to demonstrate the full benefit for physical layer security that is derived from the proposed transmission strategy. In the case of Gaussian-distributed input, we are concerned with the upper bounds on achievable data rates with finite-alphabet inputs/modulations in both the legitimate link (Alice–Bob) and the wire-tapper link (Alice–Eve), by assuming that Alice's transmitted signals are restricted to be the random variables chosen from complex Gaussian distributed codebooks $\mathcal{CN}(0, \sigma_X^2)$ with the transmit power σ_X^2.

The secrecy rate of a wire-tap channel is defined as the positive difference between the achievable data rates obtained by the legitimate receiver (Bob) and the eavesdropper (Eve), i.e., if the legitimate link data rate is higher than the wire-tapper link data rate [6], [7]. Grounded on this definition, the secrecy rate of the mapping-varied spatial modulation with Gaussian-distributed input, denoted by C_s, is expressed as

$$C_s = \max\{0, C_{\mathrm{B}} - C_{\mathrm{E}}\}, \tag{7}$$

where C_{B} and C_{E} denote Bob's and Eve's achievable data rates in the case of Gaussian-distributed input, respectively.

As all the legitimate CQI patterns occur at the same probability $1/P$, Bob's and Eve's achievable data rates can be obtained by

$$C_{\mathrm{B}} = \frac{1}{P}\sum_{p=1}^{P} C_{\mathrm{B}}^{(p)} \tag{8}$$

and

$$C_{\mathrm{E}} = \frac{1}{P}\sum_{p=1}^{P} C_{\mathrm{E}}^{(p)}, \tag{9}$$

respectively, where $C_{\mathrm{B}}^{(p)}$ and $C_{\mathrm{E}}^{(p)}$ denote Bob's and Eve's data rates pertaining to the p^{th} CQI pattern over the legitimate link, respectively. Since their data rates pertaining to all the legitimate CQI patterns are the same, i.e., $C_{\mathrm{B}}^{(1)} = C_{\mathrm{B}}^{(2)} = \cdots = C_{\mathrm{B}}^{(P)}$ and $C_{\mathrm{E}}^{(1)} = C_{\mathrm{E}}^{(2)} = \cdots = C_{\mathrm{E}}^{(P)}$, Bob's and Eve's achievable data rates are equal to their own data rates with an arbitrary CQI pattern of the legitimate link, i.e., $C_{\mathrm{B}} = C_{\mathrm{B}}^{(p)}$ and $C_{\mathrm{E}} = C_{\mathrm{E}}^{(p)}$, $p = 1, 2, \cdots, P$.

Given a legitimate CQI pattern, the proposed mapping-varied spatial modulation is equivalent to the classical spatial modulation for Bob. As such, the instantaneous data rate of the legitimate link, i.e., Bob's achievable data rate C_{B}, is equal to the instantaneous data rate of the classical spatial modulation, calculated using

$$C_{\mathrm{B}} = C_{\mathrm{B}a} + C_{\mathrm{B}d}, \tag{10}$$

where $C_{\mathrm{B}a}$ and $C_{\mathrm{B}d}$ stand for the achievable data rates of Alice's antenna information $\mathbf{x}_a$ and radiated information $\mathbf{x}_d$, respectively, accessing Bob with an arbitrary CQI pattern of the legitimate link.

Based on the derivations in [16] and [28], the item $C_{\mathrm{B}a}$ can be obtained by

$$\begin{aligned} C_{\mathrm{B}a} = \frac{1}{M_A}\sum_{m=1}^{M_A}\int_{\bar{y}_{\mathrm{B}}} & p\left(\bar{y}_{\mathrm{B}} | \mathbf{x}_a \leftrightarrow \text{\o} m\right) \\ & \times \log_2 \frac{p\left(\bar{y}_{\mathrm{B}} | \mathbf{x}_a \leftrightarrow \text{\o} m\right)}{p(\bar{y}_{\mathrm{B}})} d\bar{y}_{\mathrm{B}}, \end{aligned} \tag{11}$$

where $\bar{y}_{\mathrm{B}} = \mathbf{h}_m^{\dagger}\mathbf{y}_{\mathrm{B}}$ is the signal used by Bob's decoder, as shown in (3) and (4), with the $N_B \times 1$ vector $\mathbf{y}_{\mathrm{B}}$ given in (1). Since the radiated information $\mathbf{x}_d$ is complex-Gaussian distributed, the conditional PDF of $\bar{y}_{\mathrm{B}}$ given the antenna information $\mathbf{x}_a$ is denoted by

$$p\left(\bar{y}_{\mathrm{B}}|\mathbf{x}_a \leftrightarrow \text{ø}m\right) = \frac{1}{\pi\sigma^2_{\bar{y}_{\mathrm{B}}}} \exp\left(-\frac{|\bar{y}_{\mathrm{B}}|^2}{\sigma^2_{\bar{y}_{\mathrm{B}}}}\right), \tag{12}$$

where $\sigma^2_{\bar{y}_{\mathrm{B}}} = (\mathbf{h}^{\dagger}_m\mathbf{h}_m)^2\sigma^2_X + (\mathbf{h}^{\dagger}_m\mathbf{h}_m)\sigma^2_W$ is the variance of $\bar{y}_{\mathrm{B}}$ with respect to the radiated information $\mathbf{x}_d$ transmitted from the m^{th} antenna of Alice, and the PDF of $\bar{y}_{\mathrm{B}}$ is characterized as

$$p(\bar{y}_{\mathrm{B}}) = \frac{1}{M_A}\sum_{m=1}^{M_A} p\left(\bar{y}_{\mathrm{B}}|\mathbf{x}_a \leftrightarrow \text{ø}m\right). \tag{13}$$

Additionally, the second item on the right-hand side of (10), $C_{\mathrm{B}d}$, is given by

$$C_{\mathrm{B}d} = \frac{1}{M_A}\sum_{m=1}^{M_A} \log_2\left(1 + \frac{\sigma^2_X}{\sigma^2_W}\mathbf{h}^{\dagger}_m\mathbf{h}_m\right). \tag{14}$$

By substituting (11) and (14) into (10), the instantaneous data rate of the legitimate link from Alice to Bob, C_{B}, is achieved.

On the other hand, with the mapping-varied spatial modulation for physical layer security, the probability that eavesdroppers successfully decode $\mathbf{x}_a$ is $1/M_A$, and the probability that eavesdroppers successfully decode $\mathbf{x}_d$ is $1/M_d$. Hence, the eavesdropper Eve's achievable data rate is formulated by

$$C_{\mathrm{E}} = \frac{1}{M_A}C_{\mathrm{E}a} + \frac{1}{M_d}C_{\mathrm{E}d}, \tag{15}$$

where $C_{\mathrm{E}a}$ and $C_{\mathrm{E}d}$ denote the data rates of $\mathbf{x}_a$ and $\mathbf{x}_d$ accessing Eve, respectively, in the case that Eve could successfully decode them, given an arbitrary CQI pattern of the legitimate link.

For the Gaussian-distributed input, the number of constellation points, M_d, is infinite and, accordingly, the second item on the right-hand side of (15), $C_{\mathrm{E}d}/M_d$, equals to 0. In this case, if Alice's radiated-information mapping patterns are varied, the probability that Eve can successfully decode $\mathbf{x}_d$ approaches 0. Consequently, Eve's achievable data rate, given by (15), is re-written as

$$C_{\mathrm{E}} = \frac{1}{M_A}C_{\mathrm{E}a}, \tag{16}$$

and $C_{\mathrm{E}a}$ is calculated using [16], [28]

$$\begin{aligned} C_{\mathrm{E}a} = \frac{1}{M_A}\sum_{m=1}^{M_A} \int_{\bar{y}_{\mathrm{E}}} & p\left(\bar{y}_{\mathrm{E}}|\mathbf{x}_a \leftrightarrow \text{ø}m\right) \\ & \times \log_2 \frac{p\left(\bar{y}_{\mathrm{E}}|\mathbf{x}_a \leftrightarrow \text{ø}m\right)}{p(\bar{y}_{\mathrm{E}})} d\bar{y}_{\mathrm{E}}, \end{aligned} \tag{17}$$

where $\bar{y}_{\mathrm{E}} = \mathbf{g}^{\dagger}_m\mathbf{y}_{\mathrm{E}}$ is the signal used by Eve's decoder, as shown in (5) and (6), with the $N_E \times 1$ vector $\mathbf{y}_{\mathrm{E}}$ given in (2). The conditional PDF of $\bar{y}_{\mathrm{E}}$ given the antenna information $\mathbf{x}_a$ is characterized as

$$p\left(\bar{y}_{\mathrm{E}}|\mathbf{x}_a \leftrightarrow \text{ø}m\right) = \frac{1}{\pi\sigma^2_{\bar{y}_{\mathrm{E}}}} \exp\left(-\frac{|\bar{y}_{\mathrm{E}}|^2}{\sigma^2_{\bar{y}_{\mathrm{E}}}}\right), \tag{18}$$

where $\sigma^2_{\bar{y}_{\mathrm{E}}} = (\mathbf{g}^{\dagger}_m\mathbf{g}_m)^2\sigma^2_X + (\mathbf{g}^{\dagger}_m\mathbf{g}_m)\sigma^2_W$ is the variance of $\bar{y}_{\mathrm{E}}$ with respect to the radiated information $\mathbf{x}_d$ transmitted from the m^{th} antenna of Alice, and the PDF of $\bar{y}_{\mathrm{E}}$ is obtained by

$$p(\bar{y}_{\mathrm{E}}) = \frac{1}{M_A}\sum_{m=1}^{M_A} p\left(\bar{y}_{\mathrm{E}}|\mathbf{x}_a \leftrightarrow \text{ø}m\right). \tag{19}$$

Then, the instantaneous data rate of the wire-tapper link from Alice to Eve, C_{E}, is obtained by substituting (17) into (16).

As a result, the secrecy rate of the proposed mapping-varied spatial modulation over MIMO wire-tap channels with Gaussian-distributed input, defined in (7), can be established by

$$C_s = \max\left\{0, C_{\mathrm{B}a} + C_{\mathrm{B}d} - \frac{1}{M_A}C_{\mathrm{E}a}\right\}, \tag{20}$$

where $C_{\mathrm{B}a}$, $C_{\mathrm{B}d}$ and $C_{\mathrm{E}a}$ are given by (11), (14) and (17), respectively.

B. Finite-Alphabet Input

Herein, the secrecy rate of the mapping-varied spatial modulation is formulated for the practical case with finite-alphabet input. To keep the consistency in expression, Alice's transmit power in this case, i.e., the average energy of Alice's finite-alphabet input, is denoted by σ^2_X and, thereby, the SNR is $\rho = \sigma^2_X/\sigma^2_W$.

The definition of secrecy rate over a wire-tap channel [6], [7] leads to the secrecy rate expression of the mapping-varied spatial modulation with finite-alphabet input, denoted by R_s, as

$$R_s = \max\{0, R_{\mathrm{B}} - R_{\mathrm{E}}\}, \tag{21}$$

where R_{B} and R_{E} stand for the data rates achieved by Bob and Eve, respectively, with finite-alphabet input at Alice.

The data rate achieved by Bob in the mapping-varied spatial modulation, R_{B}, is equal to that of the classical spatial modulation with finite-alphabet input. Based on the analysis in [24], R_{B} can be obtained by (22) at the top of next page, where the $N_B \times 1$ vector $\mathbf{u}^{k,k'}_{m,m'} = \mathbf{h}_m s_k - \mathbf{h}_{m'} s_{k'}$, and $(m', k') \neq (m, k)$ excludes the event when $m' = m$ and $k' = k$ occur together from the summation, i.e., the summation is taken over $m' = 1, 2, \cdots, M_A$, $k' = 1, 2, \cdots, M_d$ in three conditions: (i) $m' \neq m$ while $k' \neq k$; (ii) $m' = m$ while $k' \neq k$; (iii) $m' \neq m$ while $k' = k$. Moreover, $\mathcal{E}_{z_{\mathrm{B}}}\{\cdot\}$ represents the expectation with respect to Bob's received AWGN, i.e., $\mathbf{z}_{\mathrm{B}}$ in (1).

As is shown in (22), for a given channel realization, $f_{\mathrm{B}}(\rho)$ is a decreasing function of the SNR ρ and converges to 1 when ρ goes to infinity, i.e., $\lim\limits_{\rho\to+\infty} f_{\mathrm{B}}(\rho) = 1$. Consequently, as ρ approaches infinity, the limit of Bob's instantaneous data rate R_B is

$$\lim_{\rho\to+\infty} R_{\mathrm{B}}(\rho) = \log_2 M_A M_d, \tag{23}$$

which is equal to the upper bound on the data rate of classical spatial modulation with M_A transmit antennas and M_d-point constellation.

With the mapping-varied spatial modulation adopted by the transmitter Alice, the eavesdropper Eve successfully decodes Alice's antenna information $\mathbf{x}_a$ at the probability $1/M_A$ and successfully decodes Alice's radiated information $\mathbf{x}_d$ at the probability $1/M_d$. Hence, the achievable data rate over the wire-tapper link with finite-alphabet input, R_{E}, is given by

$$R_{\mathrm{E}} = \frac{1}{M_A}R_{\mathrm{E}a} + \frac{1}{M_d}R_{\mathrm{E}d}, \tag{24}$$

where $R_{\mathrm{E}a}$ and $R_{\mathrm{E}d}$ denote the data rates pertaining to the transmissions of $\mathbf{x}_a$ and $\mathbf{x}_d$ over the wire-tapper link, respectively, if they were decoded correctly by Eve.

$$R_{\mathrm{B}} = \log_2 M_A M_d - \frac{1}{M_A M_d}\sum_{m=1}^{M_A}\sum_{k=1}^{M_d}\mathcal{E}_{\mathbf{z}_{\mathrm{B}}}\left\{\log_2\left(\underbrace{1+\sum_{\substack{m'=1\\(m',k')\neq(m,k)}}^{M_A}\sum_{k'=1}^{M_d}\exp\left(-\rho\left[\left(\mathbf{u}_{m,m'}^{k,k'}+\mathbf{z}_{\mathrm{B}}\right)^{\dagger}\left(\mathbf{u}_{m,m'}^{k,k'}+\mathbf{z}_{\mathrm{B}}\right)-\mathbf{z}_{\mathrm{B}}^{\dagger}\mathbf{z}_{\mathrm{B}}\right]\right)}_{f_{\mathrm{B}}(\rho)}\right)\right\} \tag{22}$$

$$R_{\mathrm{E}a} = \log_2 M_A - \frac{1}{M_A M_d}\sum_{m=1}^{M_A}\sum_{k=1}^{M_d}\mathcal{E}_{\mathbf{z}_{\mathrm{E}}}\left\{\log_2\left(\underbrace{1+\sum_{\substack{m'=1\\m'\neq m}}^{M_A}\exp\left(-\rho\left[\left(\mathbf{v}_{m,m'}+\mathbf{z}_{\mathrm{E}}\right)^{\dagger}\left(\mathbf{v}_{m,m'}+\mathbf{z}_{\mathrm{E}}\right)-\mathbf{z}_{\mathrm{E}}^{\dagger}\mathbf{z}_{\mathrm{E}}\right]\right)}_{f_{\mathrm{E}a}(\rho)}\right)\right\} \tag{25}$$

$$\begin{aligned}R_{\mathrm{E}d} = \log_2 M_d - \frac{1}{M_A M_d}\sum_{m=1}^{M_A}\sum_{k=1}^{M_d}\mathcal{E}_{\mathbf{z}_{\mathrm{E}}}\Bigg\{&\log_2\left(\underbrace{1+\sum_{\substack{m'=1\\(m',k')\neq(m,k)}}^{M_A}\sum_{k'=1}^{M_d}\exp\left(-\rho\left(\mathbf{v}_{m,m'}^{k,k'}+\mathbf{z}_{\mathrm{E}}\right)^{\dagger}\left(\mathbf{v}_{m,m'}^{k,k'}+\mathbf{z}_{\mathrm{E}}\right)\right)}_{f_{\mathrm{E}d1}(\rho)}\right)\\ &-\log_2\left(\underbrace{1+\sum_{\substack{m'=1\\m'\neq m}}^{M_A}\exp\left(-\rho\left(\mathbf{v}_{m,m'}+\mathbf{z}_{\mathrm{E}}\right)^{\dagger}\left(\mathbf{v}_{m,m'}+\mathbf{z}_{\mathrm{E}}\right)\right)}_{f_{\mathrm{E}d2}(\rho)}\right)\Bigg\}\end{aligned} \tag{26}$$

In detail, $R_{\mathrm{E}a}$ and $R_{\mathrm{E}d}$ are calculated using (25) and (26), respectively, where the $N_E \times 1$ vectors $\mathbf{v}_{m,m'} = \mathbf{g}_m s_k - \mathbf{g}_{m'} s_k$ and $\mathbf{v}_{m,m'}^{k,k'} = \mathbf{g}_m s_k - \mathbf{g}_{m'} s_{k'}$, with $k, k' = 1, 2, \cdots, M_d$, $m, m' = 1, 2, \cdots, M_A$. Additionally, $\mathcal{E}_{z_{\mathrm{E}}}\{\cdot\}$ stands for the expectation with respect to Eve's received AWGN, i.e., $\mathbf{z}_{\mathrm{E}}$ in (2).

For a given channel realization, the function $f_{\mathrm{E}a}(\rho)$ in (25) converges to 1 as the SNR ρ approaches infinity, i.e., $\lim_{\rho\to+\infty} f_{\mathrm{E}a}(\rho) = 1$, and so the limit of $R_{\mathrm{E}a}$ is obtained by

$$\lim_{\rho\to+\infty} R_{\mathrm{E}a}(\rho) = \log_2 M_A. \tag{27}$$

Subsequently, in (26), we also have $\lim_{\rho\to+\infty} f_{\mathrm{E}d1}(\rho) = 1$ and $\lim_{\rho\to+\infty} f_{\mathrm{E}d2}(\rho) = 1$, which leads to the limit of $R_{\mathrm{E}d}$ as

$$\lim_{\rho\to+\infty} R_{\mathrm{E}d}(\rho) = \log_2 M_d. \tag{28}$$

Thus, as ρ goes to infinity, (24) yields the limit of Eve's instantaneous data rate as

$$\lim_{\rho\to+\infty} R_{\mathrm{E}}(\rho) = \frac{1}{M_A}\log_2 M_A + \frac{1}{M_d}\log_2 M_d. \tag{29}$$

As a consequence, the secrecy rate of the mapping-varied spatial modulation with finite-alphabet input, R_s, is achieved by substituting (22) and (24) into (21). Further, based on (23) and (29), the limit of the secrecy rate in (21) at the SNR $\rho \to +\infty$ is

$$\lim_{\rho\to+\infty} R_s(\rho) = \frac{M_A - 1}{M_A}\log_2 M_A + \frac{M_d - 1}{M_d}\log_2 M_d. \tag{30}$$

Note that, this limit is a constant, unchanged with varying channel realizations. Specifically, in the case of large M_A and M_d, i.e., $M_A \gg 1$, $M_d \gg 1$, we have

$$\lim_{\rho\to+\infty} R_s(\rho) = \log_2 M_A + \log_2 M_d, \tag{31}$$

which equals to the limit of Bob's data rate in (23), i.e., $\lim_{\rho\to+\infty} R_s(\rho) = \lim_{\rho\to+\infty} R_{\mathrm{B}}(\rho)$. That is, if the number of Alice's transmit antennas, M_A, and the number of radiated constellation points, M_d, are much greater than 1, the limit of the secrecy rate with mapping-varied spatial modulation is the same as the limit of the achievable data rate over the legitimate link, in high-SNR region.

IV. Numerical Results and Discussions

To verify the capability of physical layer security offered by the mapping-varied spatial modulation and get further insights on its merits, in this section we numerically illustrate the security performance of the proposed transmission strategy in the metrics of ergodic secrecy rate and secrecy outage probability, based on the mathematical establishment in Section III.

Without loss of generality, the security performance of the proposed transmission strategy will be investigated over Rayleigh fading channels, for two scenarios:

i> The legitimate and wire-tapper links are independent and identically distributed (i.i.d.), where all the channels coefficients, over both the legitimate link and the wire-tapper link, satisfy independent and identical complex Gaussian distribution with zero-mean and unit-variance, i.e., $h_{nm}, g_{lm} \sim \mathcal{CN}(0,1)$, $\forall m \in \{1, 2, \cdots, M_A\}, n \in \{1, 2, \cdots, N_B\}, l \in \{1, 2, \cdots, N_E\}$.

ii> The legitimate and wire-tapper links are independent and non-identically distributed (i.n.i.d.), where the channel power gain of the wire-tapper link is twice that of the legitimate link. In detail, the channels coefficients in the legitimate link, $h_{nm} \sim \mathcal{CN}(0,1)$, $\forall m \in \{1, 2, \cdots, M_A\}, n \in \{1, 2, \cdots, N_B\}$, whereas the channels coefficients in the wire-tapper link, $g_{lm} \sim \mathcal{CN}(0,2)$, $\forall m \in \{1, 2, \cdots, M_A\}, l \in \{1, 2, \cdots, N_E\}$.

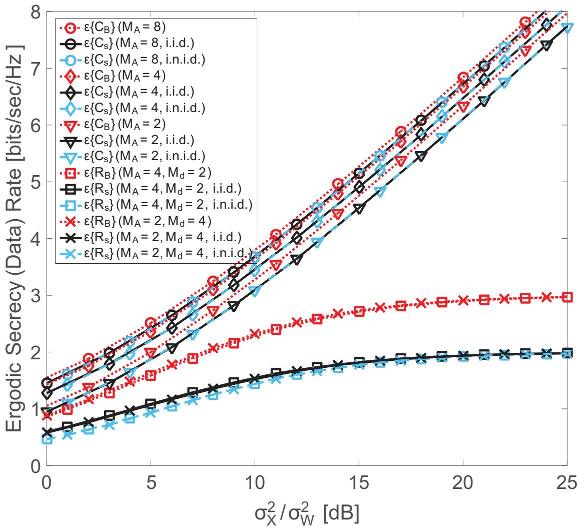

Fig. 4. Ergodic secrecy rate of the proposed mapping-varied spatial modulation with $N_B = 1$ antenna at Bob and $N_E = 1$ antenna at Eve, over i.i.d. and i.n.i.d. links. Also shown is Bob's ergodic date rate, which is equal to the ergodic data rate of classical spatial modulation.

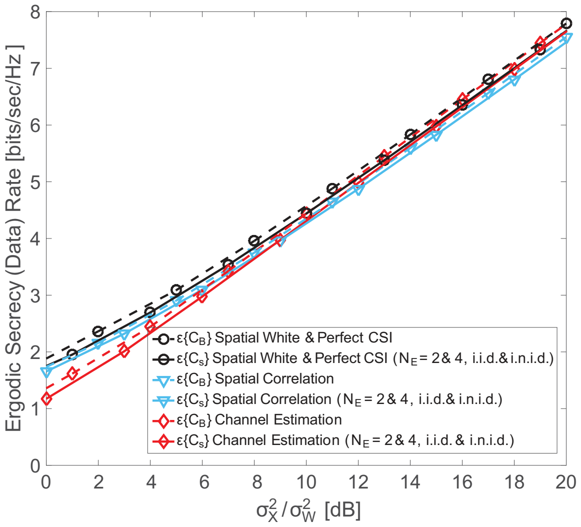

Fig. 5. Ergodic secrecy rate of the proposed mapping-varied spatial modulation with $M_A = 4$ antennas at Alice and $N_B = 2$ antennas at Bob, in the case of Gaussian-distributed input over i.i.d. and i.n.i.d. links. Also shown is Bob's ergodic data rate, which is equal to the ergodic data rate of classical spatial modulation.

A. *Ergodic Secrecy Rate*

To begin with, we consider the metric of ergodic secrecy rate that is defined as $\mathcal{E}\{C_s\}$ in the case of Gaussian-distributed input and $\mathcal{E}\{R_s\}$ in the case of finite-alphabet input, where C_s and R_s are given by (7) and (21), respectively.

In the case of Gaussian-distributed input, if the legitimate link and the wire-tapper link are i.i.d., the ergodic date rate of Alice's antenna information $\mathbf{x}_a$ accessing Bob is equal to that of $\mathbf{x}_a$ accessing Eve if Eve could successfully decode it, i.e., $\mathcal{E}\{C_{\mathrm{B}a}\} = \mathcal{E}\{C_{\mathrm{E}a}\} = \mathcal{E}\{C_a\}$, and so does the ergodic date rates pertaining to Alice's radiated information $\mathbf{x}_d$, i.e., $\mathcal{E}\{C_{\mathrm{B}d}\} = \mathcal{E}\{C_{\mathrm{E}d}\} = \mathcal{E}\{C_d\}$, where $\mathcal{E}\{C_a\}$ and $\mathcal{E}\{C_d\}$ denote the ergodic data rates of $\mathbf{x}_a$ and $\mathbf{x}_d$ in the classical spatial modulation, respectively.

From (20), the ergodic secrecy rate of the mapping-varied spatial modulation with Gaussian-distributed input, $\mathcal{E}\{C_s\}$, in the i.i.d. scenario, is approximately equal to $\frac{M_A-1}{M_A}\mathcal{E}\{C_a\} + \mathcal{E}\{C_d\}$. If $M_A \gg 1$, this ergodic secrecy rate converges to the ergodic date rate of the legitimate link, which is also equal to the ergodic date rate of classical spatial modulation, i.e., $\mathcal{E}\{C_a\} + \mathcal{E}\{C_d\}$.

In Fig. 4, the ergodic secrecy rates of the mapping-varied spatial modulation, $\mathcal{E}\{C_s\}$ and $\mathcal{E}\{R_s\}$, are reported for the i.i.d. and i.n.i.d. scenarios, where both Bob and Eve are single-antenna devices, i.e., $N_B = N_E = 1$. For the sake of comparison, Bob's ergodic data rates with Gaussian-distributed input, $\mathcal{E}\{C_{\mathrm{B}}\}$, and with finite-alphabet input, $\mathcal{E}\{R_{\mathrm{B}}\}$, are also plotted in this figure, where C_{B} and R_{B} are given by (10) and (22), respectively. Elaborating slightly further, the gap between $\mathcal{E}\{C_s\}$ and $\mathcal{E}\{C_{\mathrm{B}}\}$ is equivalent to Eve's ergodic data rate with Gaussian-distributed input, $\mathcal{E}\{C_{\mathrm{E}}\}$, whilst the gap between $\mathcal{E}\{R_s\}$ and $\mathcal{E}\{R_{\mathrm{B}}\}$ is equivalent to Eve's ergodic data rate with finite-alphabet input, $\mathcal{E}\{R_{\mathrm{E}}\}$, where C_{E} and R_{E} are given in (16) and (24), respectively.

As is shown in Fig. 4, $\mathcal{E}\{C_s\}$ approaches $\mathcal{E}\{C_{\mathrm{B}}\}$ with the increase in the number of antennas at the transmitter Alice, M_A. When $M_A = 8$, the gap between $\mathcal{E}\{C_s\}$ and $\mathcal{E}\{C_{\mathrm{B}}\}$ is negligible. These phenomena hold in both i.i.d. and i.n.i.d. scenarios. That is, even if the channel condition of the wire-tapper link is better than that of the legitimate link, the eavesdropper's ergodic data rate cannot be improved at all in the case of Gaussian-distributed input. On the other hand, with finite-alphabet input, the gap between $\mathcal{E}\{R_s\}$ and $\mathcal{E}\{R_{\mathrm{B}}\}$ converges to a constant $\log_2 M_A/M_A + \log_2 M_d/M_d$ as the SNR ρ increases, in both i.i.d. and i.n.i.d. scenarios. At low SNRs, $\mathcal{E}\{R_s\}$ in the i.n.i.d. scenario is a bit lower than that in the i.i.d. scenario.

Then, the effects of spatial correlation and channel estimation over the legitimate link on the security performance $\mathcal{E}\{C_s\}$ and Bob's performance $\mathcal{E}\{C_{\mathrm{B}}\}$ with the mapping-varied spatial modulation are presented in Fig. 5, where $M_A = 4$, $N_B = 2$, $N_E = 2, 4$, and the MIMO channel over the wire-tapper link, $\mathbf{G}$, is spatially white and perfectly known at Eve.

The spatially correlated MIMO channel over the legitimate link, denoted by $\mathbf{H}_{SC}$, is expressed by the exponential correlation model as [29], [30]

$$\mathbf{H}_{SC} = (\mathbf{\Lambda}_B)^{1/2}\mathbf{H}(\mathbf{\Lambda}_A)^{1/2}, \tag{32}$$

where the $N_B \times N_B$ matrix $\mathbf{\Lambda}_B = \left[\lambda_B^{|i-j|}\right]_{i,j=1,2,\cdots,N_B}$ specifies the correlation between Bob's antennas and the $M_A \times M_A$ matrix $\mathbf{\Lambda}_A = \left[\lambda_A^{|i-j|}\right]_{i,j=1,2,\cdots,M_A}$ specifies the correlation between Alice's antennas, with $\lambda_B, \lambda_A \in (0, 1)$ defining the correlation parameters for Bob and Alice, respectively. The $N_B \times M_A$ matrix $\mathbf{H}$ is the spatially white MIMO channel over the legitimate link, as described in Section II-A. In Fig. 5, the correlation parameters $\lambda_B = \lambda_A = 0.8$. Due to the spatial correlation, both $\mathcal{E}\{C_s\}$ and $\mathcal{E}\{C_{\mathrm{B}}\}$ have less than 1dB loss; i.e., spatial correlation has very little influence on the performance of mapping-varied spatial modulation.

With channel estimation, the channels coefficients from the m^{th} antenna of Alice to all the antennas of Bob can be

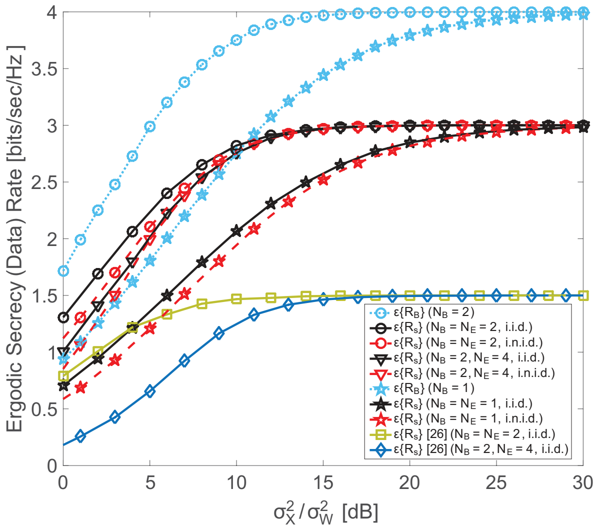

Fig. 6. Ergodic secrecy rate of the proposed mapping-varied spatial modulation with finite-alphabet input, in the case of $M_d = M_A = 4$, over i.i.d. and i.n.i.d. links. Also shown is Bob's ergodic data rate, which is equal to the ergodic data rate of classical spatial modulation.

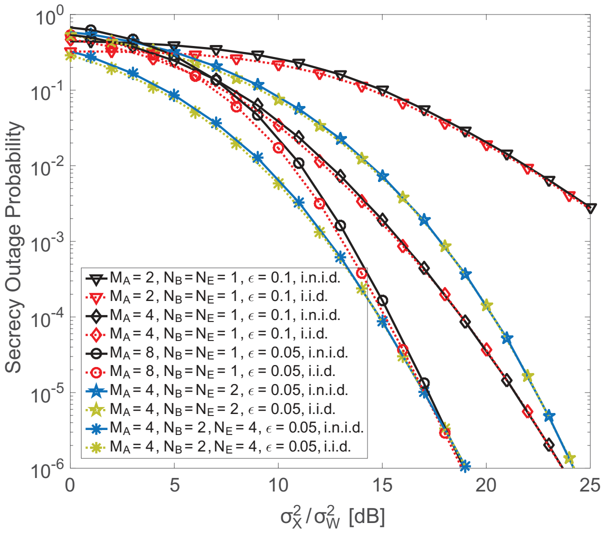

Fig. 7. Secrecy outage probability of the proposed mapping-varied spatial modulation with Gaussian-distributed input, $\mathcal{P}_{out}^{\mathrm{Gau}}(\epsilon)$, over i.i.d. and i.n.i.d. links.

expressed by [28], [30]

$$\mathbf{h}_m = \hat{\mathbf{h}}_m + \tilde{\mathbf{h}}_m, \tag{33}$$

where the $N_B \times 1$ vector $\hat{\mathbf{h}}_m$ is the minimum mean square error (MMSE) estimation of the real channels coefficients, and the $N_B \times 1$ vector $\tilde{\mathbf{h}}_m$ represents the channel estimation error. In Fig. 5, a single pilot symbol is appropriately interspersed with the data at each transmit antenna and, thus, the variance of the channel estimation error, i.e., the MMSE, is given by $\sigma^2_{\tilde{\mathbf{h}}} = 1/(1+\rho)$. As the channel fading block length is much greater than 1, the resource consumption of a single pilot can be neglected. As is shown in the figure, both $\mathcal{E}\{C_s\}$ and $\mathcal{E}\{C_{\mathrm{B}}\}$ get worse at low SNRs due to the channel estimation error; however, there is no difference between the performance with channel estimation and the performance with perfect CSI in the high-SNR region.

Moreover, Fig. 5 also manifests that, in the case of Gaussian-distributed input, neither more receiving antennas at eavesdroppers nor higher channel power gain over wire-tapper links will result in a decline in the security performance of the mapping-varied spatial modulation.

Furthermore, we investigate the impact of multiple receiving antennas on the ergodic secrecy rate of mapping-varied spatial modulation with finite-alphabet input in Fig. 6, where $\mathcal{E}\{R_s\}$ is compared with $\mathcal{E}\{R_{\mathrm{B}}\}$ in the i.i.d. and i.n.i.d. scenarios with $M_d = M_A = 4$. As illustrated in this figure, with the increase in the number of receiving antennas at Bob, N_B, both $\mathcal{E}\{R_{\mathrm{B}}\}$ and $\mathcal{E}\{R_s\}$ are improved a lot. When the number of receiving antennas at Eve, N_E, gets larger, the security performance $\mathcal{E}\{R_s\}$ decreases a bit at low SNRs. As the SNR increases, $\mathcal{E}\{R_{\mathrm{B}}\}$ converges to $\log_2 M_A + \log_2 M_d$ and $\mathcal{E}\{R_s\}$ converges to $\frac{M_A-1}{M_A}\log_2 M_A + \frac{M_d-1}{M_d}\log_2 M_d$, with our proposed mapping-varied spatial modulation.

In Fig. 6, the ergodic secrecy rate $\mathcal{E}\{R_s\}$ of the scheme proposed in [26] is included as well, which converges to $\frac{M_A-1}{M_A}\log_2 M_A$ as the SNR increases. Apparently, our proposed mapping-varied spatial modulation achieves better security performance than the scheme in [26], thanks to extra decoding uncertainty at eavesdroppers introduced by varying the radiated-information mapping patterns.

B. Secrecy Outage Probability

Herein, we consider the secrecy outage probability, which is an important metric for physical layer security over fading channels, defined as the probability that the instantaneous secrecy rate is less than a target data rate [31], [32]. In the mapping-varied spatial modulation with Gaussian-distributed input, the secrecy outage probability is denoted by

$$\mathcal{P}_{out}^{\mathrm{Gau}}(\epsilon) = \Pr\{C_s < (1-\epsilon)C_{\mathrm{B}}\}, \tag{34}$$

where $\epsilon \in (0,1)$ is a predetermined small positive quantity, claiming on the maximum allowable ratio of Eve's performance to Bob's performance. The target secrecy rate $(1-\epsilon)C_{\mathrm{B}}$ is an approximation to Bob's data rate C_{B}. In particular, $\epsilon \to 0$ implies stringent requirement on the target secrecy rate, while larger ϵ corresponds to a looser requirement on the target.

In Fig. 7, the secrecy outage probability of the mapping-varied spatial modulation with Gaussian-distributed input is plotted versus SNR, where the secrecy outage probability decreases dramatically with the increase in the number of antennas at Alice, M_A, even if ϵ gets smaller. An interesting phenomenon is that the secrecy outage probability gets lower when the number of receiving antennas at Eve, N_E, gets larger. The main reason behind this is that, in the case of Gaussian-distributed input, the difference among equivalent fading behaviours of spatial modulation is reduced with the increase in N_E, which results in lower data rate of the antenna information $\mathbf{x}_a$ accessing Eve, i.e., lower $C_{\mathrm{E}a}$. Therefore, even if eavesdroppers set up more receiving antennas than the legitimate receiver, the security performance of the mapping-varied spatial modulation is not diminished at all.

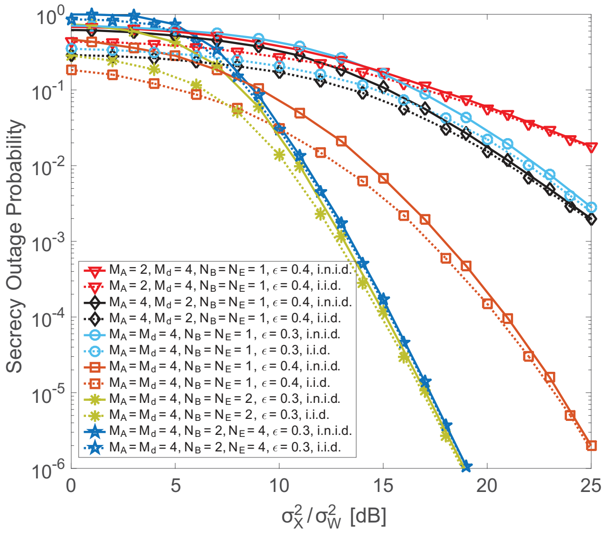

Fig. 8. Secrecy outage probability of the proposed mapping-varied spatial modulation with finite-alphabet input, $\mathcal{P}_{out}^{\mathrm{Fin}}(\epsilon)$, over i.i.d. and i.n.i.d. links.

In the case of finite-alphabet input, the secrecy outage probability is expressed as

$$\mathcal{P}_{out}^{\mathrm{Fin}}(\epsilon) = \Pr\{R_s < (1-\epsilon)R_{\mathrm{B}}\}, \tag{35}$$

where $\epsilon \in (\epsilon_0, 1)$. Based on the limits given in (23) and (30), we have

$$\epsilon_0 = \frac{\log_2 M_A/M_A + \log_2 M_d/M_d}{\log_2 M_A + \log_2 M_d}. \tag{36}$$

The secrecy outage probability of the mapping-varied spatial modulation with finite-alphabet input is shown in Fig. 8, where four main insights can be reached for the purpose of system design concerning physical layer security. Firstly, the secrecy outage probability decreases with the increase in any of M_A, M_d, N_B, ϵ or ρ. Secondly, the secrecy outage probability gets higher when the number of antennas at Eve, N_E, increases. Thirdly, at the same data rate of spatial modulation, $\log_2 M_A + \log_2 M_d$, lower secrecy outage probability is achieved with larger M_A and smaller M_d. Fourthly, once the configuration of M_A and M_d is fixed, suitable SNR region guarantees the secure operation with respect to a target ϵ.

In addition, by comparing the i.i.d. and i.n.i.d. scenarios in Figs. 7 and 8, we may find the same phenomenon in both cases of Gaussian-distributed input and finite-alphabet input: In the low-SNR region, the secrecy outage probability in the i.n.i.d. scenario is higher than that in the i.i.d. scenario; i.e., the secrecy performance gets worse when Eve's channel power gain is higher than Bob's. However, as the SNR increases, the secrecy outage probability in the i.n.i.d. scenario approaches that in the i.i.d. scenario. That is, at high SNRs, the security performance over a legitimate link is guaranteed by the mapping-varied spatial modulation even if eavesdroppers' channel condition is better than the legitimate receiver's.

V. Conclusion

In this paper, the concept of spatial modulation was embraced by physical layer security and, thereby, a novel transmission strategy, named mapping-varied spatial modulation, was proposed to guarantee the confidential information conveyed over the legitimate link, when eavesdroppers' CSI is unavailable at the transmitter. With the proposed scheme, the confidential information is modulated and transmitted on the basis of spatial modulation, while the mapping patterns of radiated information and antenna information are varied according to instantaneous CQI pattern of the legitimate link. As eavesdroppers are blind to the CQI over the legitimate link, they cannot successfully decode the confidential information.

Subsequently, the secrecy rate of this scheme was formulated and analysed, based on which illustrative numerical results pertaining to the metrics of ergodic secrecy rate and secrecy outage probability substantiated the confidentiality provided by the proposed mapping-varied spatial modulation: Theoretically, with Gaussian-distributed input, the secrecy rate approaches the legitimate link data rate, even if an eavesdropper sets up more receiving antennas than the legitimate receiver and/or the channel condition of the wire-tapper link is better than that of the legitimate link; In practice, with finite-alphabet input, there is a gap between the secrecy rate and the legitimate link data rate, while this gap becomes negligible as the number of input alphabets or the number of transmit antennas increases.

We remark that, the security key introduced by the mapping-varied spatial modulation lies in varying the mapping patterns of spatial modulation, while spatial modulation is a generalized context as it is composed of traditional constellation modulation and space shift keying. Therefore, varying mapping patterns can be exploited by traditional constellation modulation or space shift keying as well, to achieve physical layer security.

Acknowledgment

The authors would like to thank the editors and the anonymous reviewers for their comments to improve the presentation of this paper.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. Journ.*, vol. 28, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journ.*, vol. 54, pp. 1355–1387, 1975.

[3] A. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[5] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[6] Y. Shiu, S. Chang, H. Wu, S. Huang, and H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[7] A. Mukherjee, S.Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[8] R. Esmailzadeh, M. Nakagawa, and A. Jones, "TDD-CDMA for the 4th generation of wireless communications," *IEEE Wireless Commun.*, vol. 10, no. 4, pp. 8–15, Aug. 2003.

[9] C. Chiang, W. Liao, T. Liu, I. Chan, and H. Chao, "Adaptive downlink and uplink channel split ratio determination for TCP-based best effort traffic in TDD-based WiMAX networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 2, pp. 182–190, Feb. 2009.

[10] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian MIMO wiretap channel," *Proc. IEEE Int. Sym. Inf. Theory (ISIT'07)*, June 2007.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[12] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[13] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[14] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[15] Y. Yang and B. Jiao, "Artificial-noise strategy for single-antenna systems over multi-path fading channels," in *Proc. IEEE Int. Wireless Commun. and Mobile Computing Conf. (IWCMC'15)*, Aug. 2015.

[16] Y. Yang and B. Jiao, "Information-guided channel-hopping for high data rate wireless communication," *IEEE Commun. Lett.*, vol. 12, no. 4, pp. 225–227, Apr. 2008.

[17] M. D. Renzo, H. Haas, and P. M. Grant, "Spatial modulation for multiple-antenna wireless systems: A survey," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 182–191, Dec. 2011.

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

[19] Y. Yang, "Information-guided relay selection for high throughput in half-duplex relay channels," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2009.

[20] Y. Yang and S. Aissa, "Information-guided transmission in decode-and-forward relaying systems: Spatial exploitation and throughput enhancement," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2341–2351, July 2011.

[21] Y. Yang, "Spatial modulation exploited in non-reciprocal two-way relay channels: Efficient protocols and capacity analysis," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 2821–2834, July 2016.

[22] C. Liu, M. Ma, Y. Yang, and B. Jiao, "Optimal spatial-domain design for spatial modulation capacity maximization," *IEEE Commun. Lett.*, vol. 10, no. 6, pp. 1092–1095, June 2016.

[23] Y. Shi, M. Ma, Y. Yang, and B. Jiao, "Optimal power allocation in spatial modulation systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1646–1655, Mar. 2017.

[24] X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2012.

[25] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1351–1354, Aug. 2015.

[26] X. Wang, X. Wang, and L. Sun, "Spatial modulation aided physical layer security enhancement for fading wiretap channels," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2016.

[27] C. Liu, L. Yang, and W. Wang, "Secure spatial modulation with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 838–841, Dec. 2017.

[28] Y. Yang, N. Bonello, and S. Aissa, "An information-guided channel-hopping scheme for block-fading channels with estimation errors," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2010.

[29] D. Chizhik, G. Foschini, M.Gans, and R. Valenzuela, "Keyholes, correlations, and capacities of multielement transmit and receive antennas," *IEEE Trans. Wireless Commun.*, vol. 1, no. 2, pp. 361–368, Apr. 2002.

[30] Y. Yang and S. Aissa, "Information guided communications in MIMO systems with channel state impairments," *Wireless Commun. and Mobile Computing*, vol. 15, no. 5, pp. 868–878, Apr. 2015.

[31] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Sym. Inf. Theory (ISIT'05)*, Sept. 2005.

[32] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Sym. Inf. Theory (ISIT'06)*, July 2006.

Yuli Yang (S'04-M'08) received her Ph.D. degree in Communications & Information Systems from Peking University, China, in July 2007. She has been a Lecturer with the University of Chester, United Kingdom, since January 2016.

Before joining the University of Chester, she was an Assistant Professor with Meliksah University, Turkey, from January 2014 to December 2015, and a Postdoctoral Fellow with King Abdullah University of Science and Technology, Saudi Arabia, from January 2010 to December 2013. Her industry experience includes working as a Research Scientist with Bell Labs Shanghai, from August 2007 to December 2009, and a Research Intern with Huawei Technologies, from June 2006 to July 2007. Her research interests include modelling, design and performance analysis of wireless systems and networks, specifically on multi-antenna transmissions, cognitive radio and cooperative communications, heterogeneous networking and physical layer security.

Mohsen Guizani (S'85-M'89-SM'99-F'09) received the B.S. (with distinction) and M.S. degrees in electrical engineering, the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor and the ECE Department Chair at the University of Idaho, USA. Previously, he served as the Associate Vice President of Graduate Studies, Qatar University, Chair of the Computer Science Department, Western Michigan University, and Chair of the Computer Science Department, University of West Florida. He also served in academic positions at the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University, and Kuwait University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He currently serves on the editorial boards of several international technical journals and the Founder and the Editor-in-Chief of Wireless Communications and Mobile Computing journal (Wiley). He is the author of nine books and more than 500 publications in refereed journals and conferences. He guest edited a number of special issues in IEEE journals and magazines. He also served as a member, Chair, and General Chair of a number of international conferences. He received the teaching award multiple times from different institutions as well as the best Research Award from three institutions. He received the 2017 IEEE ComSoc Recognition Award for his contribution to Wireless Communications. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker from 2003 to 2005. He is a Fellow of IEEE and a Senior Member of ACM.