Phased-Array Transmission for Secure mmWave Wireless Communication via Polygon Construction

Xuejing Zhang, *Member, IEEE*, Xiang-Gen Xia, *Fellow, IEEE*, Zishu He, and Xuepan Zhang

***Abstract*— This paper presents two secure transmission algorithms for millimeter-wave wireless communication, which are computationally attractive and have analytical solutions. In the proposed algorithms, we consider phased-array transmission structure and focus on phase shift keying (PSK) modulation. It is found that the traditional constellation synthesis problem can be solved with the aid of polygon construction in the complex plane. A detailed analysis is then carried out and an analytical procedure is developed to obtain a qualified phase solution. For a given synthesis task, it is derived that there exist infinite weight vector solutions under a mild condition. Based on this result, we propose the first secure transmission algorithm by varying the transmitting weight vector at symbol rate, thus resulting exact phases at the intended receiver and producing randomnesses at the undesired eavesdroppers. To improve the security without significantly degrading the symbol detection reliability for target receiver, the second secure transmission algorithm is devised by allowing a relaxed symbol region for the intended receiver. Compared to the first algorithm, the second one incorporates an additional random phase rotation operation to the transmitting weight vector and brings extra disturbance for the undesired eavesdroppers. Different from the existing works that are only feasible for the case of single-path mmWave channels, our proposed algorithms are applicable to more general multi-path channels. Moreover, all the antennas are active in the proposed algorithms and the on-off switching circuit is not needed. Simulations are presented to demonstrate the effectivenesses of the proposed algorithms under various situations.**

***Index Terms*—Secure millimeter-wave wireless communication, phased-array transmission architecture, physical layer security, symbol error rate, geometric approach.**

Manuscript received March 26, 2019; revised July 26, 2019; accepted September 10, 2019. Date of publication October 2, 2019; date of current version January 10, 2020. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Stefano Tomasin. This work was supported in part by the National Nature Science Foundation of China under Grants 61671139, 61671137, 61701499, and 61871085 and in part by the Fundamental Research Funds for the Central Universities under Grant 2672018ZYGX2018J010. *(Corresponding author: Xuepan Zhang.)*

Xuejing Zhang is with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China, and also with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: xjzhang7@163.com).

X.-G. Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: xxia@ee.udel.edu).

Z. He is with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: zshe@uestc.edu.cn).

Xuepan Zhang is with the Qian Xuesen Lab of Space Technology, Beijing 100094, China (e-mail: zhangxuepan@qxslab.cn).

This paper has supplementary downloadable multimedia material available at http://ieeexplore.ieee.org provided by the authors.

Digital Object Identifier 10.1109/TSP.2019.2944751

I. Introduction

MILLIMETER-WAVE (mmWave) wireless communication has been considered as a promising technique for future mobile networks [1]–[3]. Due to the small wavelengths in mmWave band, the eligible antenna space can be very small, and hence large-scale arrays are feasible in both transmitter and receiver sides in mmWave communication systems. Similar to the conventional wireless systems, mmWave communication is accessible by eavesdroppers as well and secure transmission becomes necessary to avoid information leakage.

In the past years, quite a number of approaches have been developed to improve the physical layer security and achieve secure transmission [4]–[6]. With the precise knowledge of channel state information (CSI), deep nulls can be formed towards the directions of the undesired eavesdroppers, thus blocking their data reception and signal copy. However, this approach may not work well in practice, since the eavesdroppers are usually non-cooperative and thus it's hard to obtain their full knowledge of CSI [7]–[9]. To achieve secure transmission when the eavesdropper's channel is unknown or when only partial CSI is available, the concept of artificial noise (AN) is developed in [10], where AN is superimposed on the information-bearing signal to mask the transmission of the confidential message. In this scheme, the AN is added in the orthogonal subspace of the main channel, such that only the eavesdropper's channel is degraded. Although the use of AN can effectively deteriorate the channel of eavesdropper, it may decrease the power to be utilized for data transmission and indirectly reduce the signal-to-interference-plus-noise ratio (SINR) at the destination [11].

Recently, there has been growing research interest on secure transmission using directional modulation (DM) technique. In this approach, adesired constellation is produced along an intended direction, while intentionally scrambling the received constellation at other directions. In particular, the authors of [12] use a phased array at the transmitter, and achieve enhanced security by changing the phase weightings at symbol rate. Moreover, this technique is implemented in [13] using a four-element patch array, where the genetic algorithm is employed to derive the phase values in order to directionally modulate the symbols of quadratic phase shift keying (QPSK) modulation. However, only approximate solutions can be obtained in the above approach and the calculation of phase values is time-consuming especially when a large-scale array is applied. Note also that the above DM approach is mainly investigated for sub-6 GHz.

Focusing on a mmWave communication system, a low-complexity DM technique called antenna subset modulation (ASM) is presented in [14]. In ASM, the array radiation pattern is modulated at radio frequency (RF) domain with symbol rate to achieve direction-dependent data transmission. More specifically, the antenna subset used for transmission is randomly selected from the set of all subsets with the same number of active antennas, such that additional randomness in constellations can be resulted at angles except the intended one. The authors of [15] propose a new transmission architecture called switched phase-array (SPA), by modifying the above ASM scheme. In SPA, only one antenna is switched off to produce the constellation distortion in undesired directions, thus increasing the number of active antennas compared to ASM. Another variant of ASM can be found in [16], where a novel programmable weight phased-array (PWPA) architecture and the corresponding schemes for secure mmWave wireless communications are developed. Exploiting DM with new array systems for secure mmWave wireless communications is presented in [17], where the authors develop a hybrid multiple-input multiple-output (MIMO) phased-array time-modulated DM for physical layer security.

It should be pointed out that the above secure transmission strategies in [14]–[17] are only effective for single-path mmWave channel, as they actually utilize the constant-modulus property of the target channel vector and follow the maximum ratio transmission (MRT) strategy. For multipath channels, the channel vectors may not be constant-modulus. As a result, the noiseless received signal at the target user can not be obtained as desired with the schemes in [14]–[17], since different weighting selections lead to different outputs. Moreover, the schemes in [14]–[17] are only applicable to phase shift keying (PSK) modulations, and the extension to other modulation types, e.g., quadrature amplitude modulation (QAM), has not been presented.

Motivated from these works, in this paper we devise two secure transmission algorithms with a novel polygon construction approach for general multi-path fading channels. The proposed two algorithms provide analytical solutions and have low computational complexities. Moreover, all antennas are active in the proposed algorithms and the on-off switching circuit is not needed. Following the existing DM framework, the proposed scheme uses phased-array transmission architecture. More specifically, we focus on multiple-input single-output (MISO) downlink with PSK modulation and reformulate the constellation synthesis problem in a geometric manner [18]. Note that the assumption of PSK modulation is made for simplicity only, and the extension to other modulation types (e.g., QAM) is straightforward and will be investigated as well. It is shown that one can synthesize a desired constellation at the target user, with the assistance of polygon construction in the complex plane. We then elaborate the procedure of polygon construction and obtain an analytical solution for the transmitting weight vector. Moreover, a detailed analysis is presented and we find that there exist infinite qualified solutions for a given constellation synthesis task under a quite mild condition. This further allows us to scramble the received symbols towards the undesired eavesdroppers by changing the transmitting weight vector at symbol rate, as similar to the concept of symbol-level precoding presented in [19]–[21].

Following the above idea, we propose two secure transmission algorithms. In the first algorithm, we vary the transmitting weight vector such that the received phases by the intended receiver are exactly equal to those of the symbols of interest. Since different weight vectors are applied, the received symbols along undesired directions can thus be randomized. To improve the security and enhance the randomnesses for the unintended receivers, we devise the second secure transmission algorithm by utilizing a relaxed symbol region as reported in [22]–[25]. The second algorithm modifies the first one by introducing an additional phase rotation operation on the transmitting weight vector. The phase rotation improves the ability on scrambling the received signal at undesired eavesdroppers, while guaranteeing the received symbols of the intended user located in a relaxed symbol region. For both algorithms, only simple additions or comparison operations are needed, thus having low computational complexities. The main contributions of this paper can be summarized as follows:

1) We propose a unit-modulus weight vector design algorithm with the assistance of polygon construction in the complex plane. The proposed algorithm has analytical solution and low computational complexity.
2) We derive several properties about the problem of solving phase equality with constant modulus constraint. In particular, we obtain a necessary and sufficient condition for the constant-modulus phase equality having infinite solutions.
3) We propose two secure transmission schemes based on phased-array. Different from the existing works in [14]–[17] that are only feasible for the single-path mmWave channels, the proposed algorithms are applicable to more general multi-path channels. Moreover, the on-off switching circuit is not needed in the proposed algorithms.
4) The presented transmission schemes are not limited to PSK modulations and are applicable to other modulation types, e.g., QAM.

The rest of the paper is organized as follows. In Section II, the system model is introduced and problem formulation is given. In Section III, a polygon construction approach to solving a specific phase equation is presented. The proposed two secure transmission algorithms are developed in Section IV. Representative simulations are presented in Section V and conclusions are drawn in Section VI.

Notations: We use bold upper-case and lower-case letters to represent matrices and vectors, respectively. $j \triangleq \sqrt{-1}$. $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\mathrm{H}}$ denote the transpose and Hermitian transpose, respectively. $|\cdot|$ is the absolute value and $\|\cdot\|_2$ denotes the l_2 norm. $\Re(\cdot)$ and $\Im(\cdot)$ denote the real and imaginary parts, respectively. $\mathbb{C}$ denotes the sets of complex numbers. $\angle(\cdot)$ outputs the phase of the input. $(\cdot)_{2\pi}$ is the mod 2π operation, i.e., it returns to the remainder after division of input by 2π. $\mathrm{Mean}(\cdot)$ outputs the expectation of the input random variable. $\mathcal{I}(y;x)$ stands for the mutual information between y and x. $\Pr(\cdot)$ outputs the probability of the input event. Finally, $\mathcal{CN}(u,\sigma^2)$ represents the circularly symmetric complex Gaussian distribution with mean u and variance σ^2.

II. System Model and Problem Formulation

A. System Model

We consider a MISO downlink system, where a base station (BS) equipped with N transmitting antennas sending data to a desired receiver (Bob) in the presence of Q possible eavesdroppers (Eves). For simplicity, we consider a uniform linear array (ULA) with N isotropic antennas for BS, while its extension to other configurations is straightforward. The Bob and Eves are all equipped with a single antenna. At discrete-time k, the signals received by Bob and the q-th Eve are given, respectively, by

$$y_d(k) = \mathbf{h}^{\mathrm{H}}\mathbf{x}(k) + \eta(k) \tag{1}$$

$$y_q(k) = \mathbf{g}_q^{\mathrm{H}}\mathbf{x}(k) + \nu_q(k), \quad q = 1, \ldots, Q \tag{2}$$

where $\mathbf{h} \in \mathbb{C}^N$ stands for the channel vector between the transmitter and Bob, $\mathbf{g}_q$ represents the channel vector between the transmitter and the q-th Eve, $\mathbf{x}$ is the transmit signal vector, $\eta \sim \mathcal{CN}(0, \sigma_d^2)$ and $\nu_q \sim \mathcal{CN}(0, \sigma_q^2)$ are the additive Gaussian noises at Bob and the q-th Eve, respectively, $q = 1, \ldots, Q$.

Different from the single-path mmWave channels considered in [14]–[17], in this paper we follow [26] and consider an extended Saleh-Valenzuela geometric model with multi-path channel [27]. More specifically, the channel vector $\mathbf{h}$ is given by

$$\mathbf{h} = \sqrt{1/L_d}\sum_{l=1}^{L_d} \alpha_l \mathbf{a}(\psi_l) \tag{3}$$

where L_d is the number of channel paths, $\alpha_l \sim \mathcal{CN}(0, 1)$ is the gain of the l-th path, ψ_l is the angle of departure (AoD) of the l-th path, $\mathbf{a}(\psi) \in \mathbb{C}^N$ represents the array response vector at ψ as

$$\mathbf{a}(\psi) = \left[1, e^{j2\pi d \sin(\psi)/\lambda}, \ldots, e^{j2\pi(N-1)d\sin(\psi)/\lambda}\right]^{\mathrm{T}} \tag{4}$$

where λ denotes the wavelength, d stands for the distance between adjacent sensors. Similarly, the channel vector $\mathbf{g}_q$ is given by

$$\mathbf{g}_q = \sqrt{1/L_q}\sum_{l=1}^{L_q} \alpha_{q,l}\mathbf{a}(\psi_{q,l}), \quad q = 1, \ldots, Q \tag{5}$$

where the parameter meanings are similar to those in (3). The multi-path mmWave channel estimation problem has been addressed in [28], by exploiting the sparse nature of the channel. According to [28], the mmWave channel can be estimated by calculating the parameters (i.e., AoD and gain) of the channel paths. Once the CSI is estimated at the receiver, it can be communicated back to the transmitter through various feedback techniques [29]. As a common assumption, in this paper we assume that the Bob's CSI (i.e., $\mathbf{h}$) is precisely known by the transmitter, while the Eves' CSI (i.e, $\mathbf{g}_q$, $q = 1, \ldots, Q$) are unavailable.

We consider the phased-array transmission structure [30]. The corresponding block diagram is presented in Fig. 1, where a common RF chain is adopted, followed by an analog beamforming in the RF domain. Finally, the phase shifted signal at each branch is amplified by a power amplifier (PA) before coupling onto the antenna.

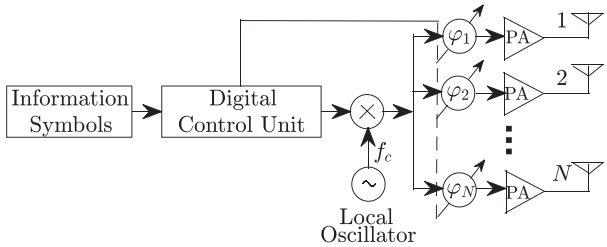


Fig. 1. Illustration of phased-array transmission structure.

For the sake of simplicity, we consider PSK modulated signals, although the extension to other modulations (e.g., QAM) are straightforward and will be examined later in Section V-C. In this case, the transmitted vector at time instant k is given by

$$\mathbf{x}(k) = \mathbf{w}(k)x(k) \tag{6}$$

where $\mathbf{w}(k) \in \mathbb{C}^N$ is the transmitting weight vector, $x(k) = \sqrt{E_s}e^{j\zeta(k)}$ represents the modulated transmitting signal, $\sqrt{E_s}$ denotes the baseband modulation amplitude, $\zeta(k)$ is the phase value of the transmitted message. Note that only phase shifters can be controlled in the above architecture. Thus, the transmitting weight vector $\mathbf{w}$ is constrained to have constant moduli at each time instant. Without loss of generality, we assume that

$$|w_n(k)| = 1, \quad n = 1, \ldots, N \tag{7}$$

where $w_n(k)$ stands for the n-th entry of $\mathbf{w}(k)$, $n = 1, \ldots, N$.

B. Problem Formulation

From (1) and (6), the symbol received by Bob is

$$y_d(k) = \mathbf{h}^{\mathrm{H}}\mathbf{w}(k)x(k) + \eta(k) \tag{8}$$

and the instantaneous receiving SNR (denoted by SNR_k) is given by $E_s|\mathbf{h}^{\mathrm{H}}\mathbf{w}(k)|^2/\sigma_d^2$. If a fixed weight vector is applied at all time instants, it may not be hard for Eve to track the weight vector and then decode the data. Thus, the time-varying weight vectors are needed to improve the security. Since $\mathbf{w}(k)$ changes over the time k, Bob does not know $\mathbf{w}(k)$. In this case, to demodulate $x(k)$ correctly by Bob, its noiseless received symbol should satisfy $\angle(\mathbf{h}^{\mathrm{H}}\mathbf{w}(k)x(k)) = \angle x(k) = \zeta(k)$, $k = 1, \ldots, K$, or equivalently

$$\mathbf{h}^{\mathrm{H}}\mathbf{w}(k) > 0, \quad k = 1, \ldots, K. \tag{9}$$

In addition, to achieve a reliable communication for Bob, the receiving SNR_k should be greater than a specific threshold Γ_d, i.e., $E_s|\mathbf{h}^{\mathrm{H}}\mathbf{w}(k)|^2/\sigma_d^2 > \Gamma_d$. It can be readily derived that

$$\mathbf{h}^{\mathrm{H}}\mathbf{w}(k) > \sqrt{\Gamma_d\sigma_d^2/E_s} \triangleq \rho \tag{10}$$

where the prerequisite in (9) is incorporated. Thus, a qualified weight vector $\mathbf{w}(k)$ should satisfy both (7) and (10).

As mentioned earlier, in order to improve the security, the weight vectors need to vary along the time, otherwise Eves may be able to track them and therefore decode the transmitted data. In this paper, we propose two effective secure transmission algorithms to avoid information leakage by designing time-varying weight vectors, i.e., changing weight vector at symbol rate.

III. Polygon Construction Approach to Solving Phase Equation

Before presenting the proposed secure transmission algorithms, we first consider how to find a qualified weight vector $\mathbf{w}$ satisfying (7) and (10). For notational convenience in this part, the time index k may be omitted if necessary.

A. Geometric Interpretation of Qualified Weight Seeking

Denote $\varphi_n = \angle w_n$ and $\vartheta_n = \angle h_n$, $n = 1, \ldots, N$. One can express $\mathbf{h}^{\mathrm{H}}\mathbf{w}$ as

$$\mathbf{h}^{\mathrm{H}}\mathbf{w} = \sum_{n=1}^{N} h_n^* e^{j\varphi_n} = \sum_{n=1}^{N} |h_n| e^{j(\varphi_n - \vartheta_n)} \tag{11}$$

where the constraint (7) has been incorporated, h_n represents the n-th entry of $\mathbf{h}$, $n = 1, \ldots, N$. Define

$$\phi_n \triangleq (\varphi_n - \vartheta_n)_{2\pi}, \quad n = 1, \ldots, N. \tag{12}$$

Then, a qualified weight vector $\mathbf{w}$ can be obtained by solving the following equation with respect to the phases $\phi_1, \ldots, \phi_N$:

$$\sum_{n=1}^{N} |h_n| e^{j\phi_n} = |h_0| \tag{13}$$

where $|h_0|$ is introduced for the later use convenience and stands for a pre-assigned real-valued constant. Note that h_0 is not a channel coefficient but just an auxiliary number to be defined in details later. Once ϕ_n's are obtained, since the channel $\mathbf{h}$ is known at the transmitter, we can recover the phases φ_n of the weight vector $\mathbf{w}$ by

$$\varphi_n = (\phi_n + \vartheta_n)_{2\pi}, \quad n = 1, \ldots, N \tag{14}$$

from which the corresponding weight vector can be expressed as $\mathbf{w} = [e^{j\varphi_1}, \ldots, e^{j\varphi_N}]^{\mathrm{T}}$.

In the complex plane, $|h_n|e^{j\phi_n}$ in (13) corresponds to a vector, denoted as $\overrightarrow{|h_n|e^{j\phi_n}} \triangleq (\Re(|h_n|e^{j\phi_n}), \Im(|h_n|e^{j\phi_n}))$. With this geometric concept, one can rewrite (13) as

$$\overrightarrow{|h_0|e^{j\phi_{0,\star}}} + \sum_{n=1}^{N} \overrightarrow{|h_n|e^{j\phi_n}} = \overrightarrow{\mathbf{0}} \tag{15}$$

where $\phi_{0,\star} \triangleq \pi$ is defined for the later use convenience. The problem of solving (15) with respect to ϕ_n becomes how to rotate the edges $|h_n|$, $n = 1, \ldots, N$, in the complex plane, such that the left hand side of Eqn.(15) sums up to zero, as geometrically demonstrated in Fig. 2. As a matter of fact, this is equivalent to constructing a polygon with edges $|h_i|$, $i = 0, 1, \ldots, N$. Note that the authors of [31]–[33] have presented geometric approaches to solve Eqn. (15) using triangle construction in the complex plane. Nevertheless, since only one solution is obtained with these methods, i.e., one weighting vector $\mathbf{w}(k)$ is obtained, it is not enough for our application in this paper as mentioned earlier. In this paper, we develop a new polygon construction approach to solve the equation (13) or (15) with as many solutions as possible.

To preceding, we provide the following important lemma, which has been proved in [31]–[33].

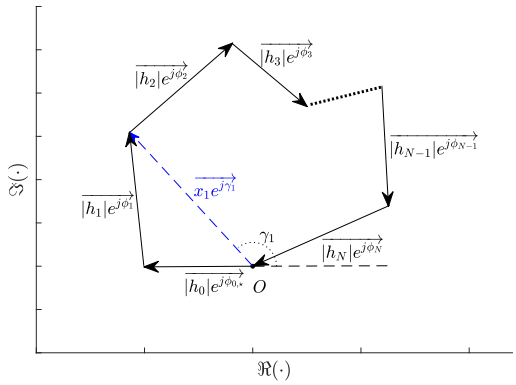


Fig. 2. Geometric illustration of Eqn. (15).

Lemma 1: Given $|h_0|, |h_1|, \ldots, |h_N| > 0$, there exists a solution for Eqn. (13) (or equivalently, the edges $|h_i|$, $i = 0, 1, \ldots, N$, can form a polygon), if and only if:

$$2\max\{|h_0|, |h_1|, \ldots, |h_N|\} \leq \sum_{i=0}^{N} |h_i|. \tag{16}$$

Note that the above Lemma 1 is not the contribution of this work, and the result has been presented in [31]–[33]. With a geometric perspective, the above Lemma 1 indicates that all the edges $|h_i|$ $(i = 0, 1, \ldots, N)$ can form a polygon in the complex plane after necessary rotations, if and only if the largest edge is not greater than the summation of the remaining ones. Interestingly, if $N = 2$ applies, Lemma 1 leads to a common sense for triangle construction. With the above important observations, one can analyze the solution of equation (13) or (15), as presented in what follows.

B. Phase Solving via Polygon Construction

With the geometric interpretation presented in Section III-A, we next provide a polygon construction method to solve the qualified phases ϕ_n in Eqn. (15), $n = 1, \ldots, N$. For notational convenience, we define

$$S(n) \triangleq \sum_{i=n}^{N} |h_i| \tag{17a}$$

$$|h|_{\max}(n) \triangleq \max_{i \in \{n, n+1, \ldots, N\}} |h_i| \tag{17b}$$

where $n \in \{1, \ldots, N\}$.

We first analyze the feasible set of ϕ_1. To do so, we draw an auxiliary vector $\overrightarrow{x_1 e^{j\gamma_1}}$ pointing from $\overrightarrow{\mathbf{0}}$ to $\overrightarrow{|h_0|e^{j\phi_{0,\star}}} + \overrightarrow{|h_1|e^{j\phi_1}}$, i.e.,

$$\overrightarrow{x_1 e^{j\gamma_1}} = \overrightarrow{|h_0|e^{j\phi_{0,\star}}} + \overrightarrow{|h_1|e^{j\phi_1}} \tag{18}$$

where γ_1 represents the phase of the auxiliary vector, as demonstrated in Fig. 2. Then, to form a polygon using $|h_0|, |h_1|, \ldots, |h_N|$, the following two conditions must be satisfied:

- The edges $|h_0|$, $|h_1|$ and x_1 can form a triangle.
- The edges x_1, $|h_2|$, …, $|h_N|$ can form a polygon.

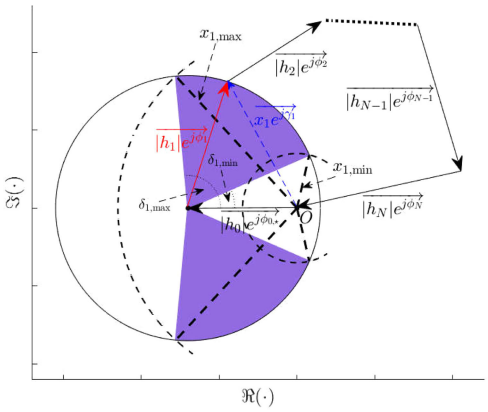


Fig. 3. Geometric illustration on the determination of the feasible set of ϕ_1.

Recalling Lemma 1, the above two conditions are satisfied if and only if:

$$\big||h_0|-|h_1|\big| \le x_1 \le |h_0|+|h_1| \tag{19a}$$

$$|h|_{\max}(2) \ge x_1, 2|h|_{\max}(2) \le x_1 + S(2) \tag{19b}$$

or

$$\big||h_0|-|h_1|\big| \le x_1 \le |h_0|+|h_1| \tag{20a}$$

$$x_1 > |h|_{\max}(2), \quad x_1 \le S(2). \tag{20b}$$

After some manipulations, one can further obtain the feasible set of x_1 (denoted by $\mathbb{X}_1$) as shown in (21) on the bottom of this page.

With the auxiliary vector $\overrightarrow{x_1e^{j\gamma_1}}$ and the set $\mathbb{X}_1$ in (21), we can further determine the feasible set of ϕ_1, as geometrically demonstrated in Fig. 3. More specifically, since the edges $|h_0|$, $|h_1|$ and x_1 can form a triangle, the included angle between the edges $|h_0|$ and $|h_1|$ (denote as δ_1) can be expressed as

$$\delta_1 = \operatorname{acos}\left(\frac{|h_0|^2+|h_1|^2-x_1^2}{2|h_0|\cdot|h_1|}\right). \tag{22}$$

Recalling that $x_1 \in \mathbb{X}_1$, we can obtain that

$$\delta_1 \in [\delta_{1,\min}, \delta_{1,\max}] \tag{23}$$

where

$$\delta_{1,\min} = \operatorname{acos}\left(\frac{|h_0|^2+|h_1|^2-x_{1,\min}^2}{2|h_0|\cdot|h_1|}\right) \tag{24a}$$

$$\delta_{1,\max} = \operatorname{acos}\left(\frac{|h_0|^2+|h_1|^2-x_{1,\max}^2}{2|h_0|\cdot|h_1|}\right) \tag{24b}$$

and see (21) for the definitions of $x_{1,\min}$ and $x_{1,\max}$. Note that the edge $|h_1|$ can be rotated in both clockwise and counterclockwise manners (with an angle δ_1) along the vector $-\overrightarrow{|h_0|e^{j\phi_{0,\star}}}$. Then, it is not hard to obtain the feasible set of ϕ_1 as

$$\Phi_1 \triangleq ([-\delta_{1,\max}, -\delta_{1,\min}] \cup [\delta_{1,\min}, \delta_{1,\max}])_{2\pi}. \tag{25}$$

To better understand the above descriptions, we have presented more details in Fig. 3. A feasible $\overrightarrow{|h_1|e^{j\phi_1}}$ with red arrow has been depicted in Fig. 3, and the purple zone is the corresponding swept area when ϕ_1 varied in Φ_1. Once ϕ_1 is selected from Φ_1 as $\phi_{1,\star}$, the resulting $\overrightarrow{x_1e^{j\gamma_{1,\star}}}$ ($\gamma_{1,\star}$ represents the ultimate selection of γ_1) satisfies

$$\overrightarrow{x_1e^{j\gamma_{1,\star}}} = \overrightarrow{|h_0|e^{j\phi_{0,\star}}} + \overrightarrow{|h_1|e^{j\phi_{1,\star}}}. \tag{26}$$

For the given $\overrightarrow{|h_0|e^{j\phi_{0,\star}}}$, $\overrightarrow{|h_1|e^{j\phi_{1,\star}}}$ and the resulting $\overrightarrow{x_1e^{j\gamma_{1,\star}}}$, we can further obtain the feasible set of ϕ_2 similarly, by drawing an auxiliary vector $\overrightarrow{x_2e^{j\gamma_2}}$ pointing from $\overrightarrow{\mathbf{0}}$ to $\overrightarrow{x_1e^{j\gamma_{1,\star}}} + \overrightarrow{|h_2|e^{j\phi_2}}$. More general, for a given $n \in \{1,\ldots,N-2\}$, if $\overrightarrow{x_{n-1}e^{j\gamma_{n-1}}}$ has been determined as $\overrightarrow{x_{n-1}e^{j\gamma_{n-1,\star}}}$ satisfying

$$\overrightarrow{x_{n-1}e^{j\gamma_{n-1,\star}}} = \overrightarrow{x_{n-2}e^{j\gamma_{n-2,\star}}} + \overrightarrow{|h_{n-1}|e^{j\phi_{n-1,\star}}} \tag{27a}$$

$$= \sum_{i=0}^{n-1} \overrightarrow{|h_i|e^{j\phi_{i,\star}}} \tag{27b}$$

one can calculate the feasible set of ϕ_n, by drawing an auxiliary vector $\overrightarrow{x_ne^{j\gamma_n}}$ pointing from $\overrightarrow{\mathbf{0}}$ to $\overrightarrow{x_{n-1}e^{j\gamma_{n-1,\star}}} + \overrightarrow{|h_n|e^{j\phi_n}}$, as depicted in Fig. 4. Note that in (27), we have implicitly defined x_0 and $\gamma_{0,\star}$, respectively, as

$$x_0 \triangleq |h_0| \tag{28a}$$

$$\gamma_{0,\star} \triangleq \phi_{0,\star} = \pi. \tag{28b}$$

Since the edges $|h_0|,\ldots,|h_{n-1}|$ and x_{n-1} have already shaped a polygon, according to Fig. 4, all the edges $|h_i|$, $i=0,1,\ldots,N$, can form a polygon if and only if x_{n-1} can form a polygon with the remaining edges $|h_n|,\ldots,|h_N|$. With similar manipulations, we can obtain the feasible set of x_n (denoted as $\mathbb{X}_n$) as shown in (29) on the bottom of next page, where $n \in \{1,\ldots,N-2\}$.

Fig. 5 presents a geometric interpretation on how to determine the feasible set of a generalized ϕ_n, $n=1,\ldots,N-2$. To have a comprehensive description, two cases, i.e., $x_{n-1} \ge |h_n|$ and $x_{n-1} < |h_n|$, are considered in Fig. 5(a) and Fig. 5(b), respectively. As illustrated, the included angle between the edges x_{n-1} and $|h_n|$ (denoted as δ_n) can be expressed in both scenarios as

$$\delta_n = \operatorname{acos}\left(\frac{x_{n-1}^2+|h_n|^2-x_n^2}{2x_{n-1}\cdot|h_n|}\right), \quad n=1,\ldots,N-2. \tag{30}$$

Combining (29), one can find that

$$\delta_n \in [\delta_{n,\min}, \quad \delta_{n,\max}] \tag{31}$$

$$x_1 \in \Bigg[\underbrace{\max\big\{\big||h_0|-|h_1|\big|, \quad 2|h|_{\max}(2)-S(2)\big\}}_{\triangleq x_{1,\min}}, \underbrace{\min\big\{|h_0|+|h_1|, S(2)\big\}}_{\triangleq x_{1,\max}}\Bigg] \triangleq \mathbb{X}_1 \tag{21}$$

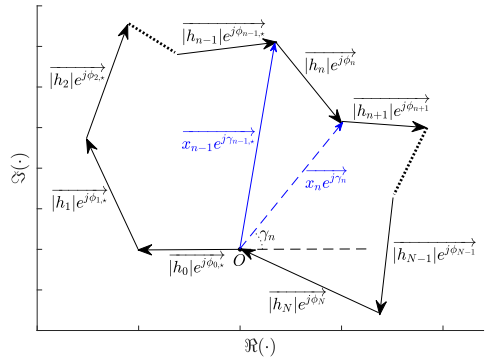
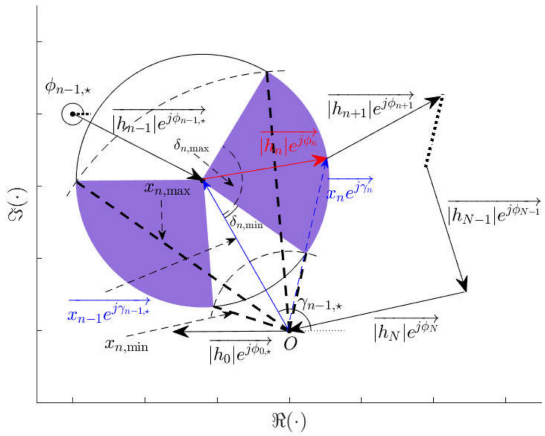
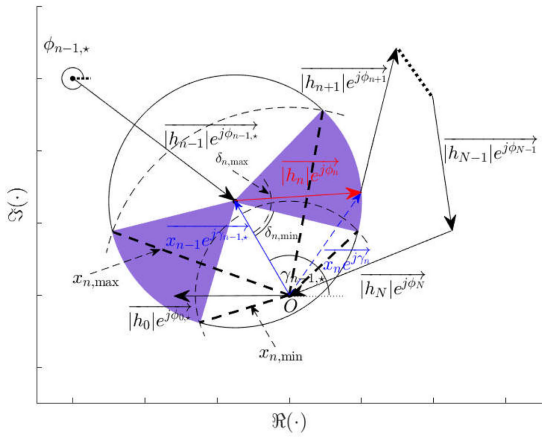


Fig. 4. Geometric illustration on the drawing of $\overrightarrow{x_n e^{j\gamma_n}}$.



(a)



(b)

Fig. 5. Geometric illustration on the determination of the feasible set of a generalized ϕ_n, $n = 1, \ldots, N-2$. The red arrow gives an illustration for the qualified $\overrightarrow{|h_n|e^{j\phi_n}}$. The purple zone is the resulting swept area when ϕ varied in Φ_n. (a) $x_{n-1} \geq |h_n|$. (b) $x_{n-1} < |h_n|$.

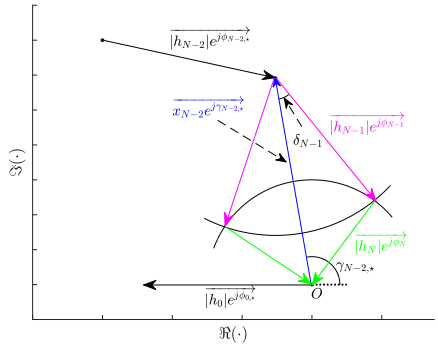


Fig. 6. Geometric illustration on the determination of the feasible sets of ϕ_{N-1} and ϕ_N.

with

$$\delta_{n,\min} = \operatorname{acos}\left(\frac{x_{n-1}^2 + |h_n|^2 - x_{n,\min}^2}{2x_{n-1}\cdot|h_n|}\right) \tag{32a}$$

$$\delta_{n,\max} = \operatorname{acos}\left(\frac{x_{n-1}^2 + |h_n|^2 - x_{n,\max}^2}{2x_{n-1}\cdot|h_n|}\right) \tag{32b}$$

where both $x_{n,\min}$ and $x_{n,\max}$ are defined as in (29), $n = 1, \ldots, N-2$. Thus, the feasible set of ϕ_n, $n = 1, \ldots, N-2$, can be given by

$$\Phi_n = \big([\gamma_{n-1,\star} + \pi - \delta_{n,\max}, \gamma_{n-1,\star} + \pi - \delta_{n,\min}] \cup [\gamma_{n-1,\star} + \pi + \delta_{n,\min}, \gamma_{n-1,\star} + \pi + \delta_{n,\max}]\big)_{2\pi}. \tag{33}$$

If ϕ_n is selected from Φ_n as $\phi_{n,\star}$, the resulting $\overrightarrow{x_n e^{j\gamma_{n,\star}}}$, $n = 1, \ldots, N-2$, can be expressed as

$$\overrightarrow{x_n e^{j\gamma_{n,\star}}} = \overrightarrow{x_{n-1}e^{j\gamma_{n-1,\star}}} + \overrightarrow{|h_n|e^{j\phi_{n,\star}}} \tag{34}$$

which is useful in the determinations of the follow-up phases, i.e., $\phi_{n+1}, \ldots, \phi_N$.

In the above discussions, we have specified the feasible set of ϕ_n for $n \in \{1, \ldots, N-2\}$. Note that if $n = N-2$ applies, the resulting x_{N-2} can form a triangle (the unique type of polygon with three edges) with the other two edges $|h_{N-1}|$ and $|h_N|$, as presented in Fig. 6. In this case, the included angle between the edges x_{N-2} and $|h_{N-1}|$ can be expressed as

$$\delta_{N-1} = \operatorname{acos}\left(\frac{x_{N-2}^2 + |h_{N-1}|^2 - |h_N|^2}{2x_{N-2}\cdot|h_{N-1}|}\right). \tag{35}$$

With the geometric interpretation in Fig. 6, one can learn that there are two candidates at most for ϕ_{N-1} and its feasible set is given by

$$\Phi_{N-1} \triangleq \big\{(\gamma_{N-2,\star} + \pi - \delta_{N-1})_{2\pi}, (\gamma_{N-2,\star} + \pi + \delta_{N-1})_{2\pi}\big\}. \tag{36}$$

$$x_n \in \Big[\underbrace{\max\big\{\big||x_{n-1} - |h_n|\big|, 2|h|_{\max}(n+1) - S(n+1)\big\}}_{\triangleq x_{n,\min}}, \underbrace{\min\{x_{n-1} + |h_n|, S(n+1)\}}_{\triangleq x_{n,\max}}\Big] \triangleq \mathbb{X}_n, \quad 1 \leq n \leq N-2 \tag{29}$$

Algorithm 1: Polygon Construction Solver for Eqn. (13).

Input: $\{h_0, h_1, \ldots, h_N\}$
Initialize: $x_0 = |h_0|$, $\gamma_{0,\star} = \phi_{0,\star} = \pi$
for $n = 1, 2, \ldots, N$ **do**
  if $n <= N-2$ **then**
    $x_{n,\min} = \max\{\big||x_{n-1} - |h_n|\big|, 2|h|_{\max}(n+1) - S(n+1)\}$
    $x_{n,\max} = \min\{x_{n-1} + |h_n|, S(n+1)\}$
    $\delta_{n,\min} = \operatorname{acos}\left(\frac{x_{n-1}^2 + |h_n|^2 - x_{n,\min}^2}{2x_{n-1}\cdot|h_n|}\right)$
    $\delta_{n,\max} = \operatorname{acos}\left(\frac{x_{n-1}^2 + |h_n|^2 - x_{n,\max}^2}{2x_{n-1}\cdot|h_n|}\right)$
    $\Phi_n = ([\gamma_{n-1,\star} + \pi - \delta_{n,\max}, \gamma_{n-1,\star} + \pi - \delta_{n,\min}] \cup [\gamma_{n-1,\star} + \pi + \delta_{n,\min}, \gamma_{n-1,\star} + \pi + \delta_{n,\max}])_{2\pi}$
    randomly select $\phi_{n,\star} \in \Phi_n$
    $\overrightarrow{x_n e^{j\gamma_{n,\star}}} = \overrightarrow{x_{n-1}e^{j\gamma_{n-1,\star}}} + \overrightarrow{|h_n|e^{j\phi_{n,\star}}}$
  else if $n == N-1$ **then**
    $\delta_{N-1} = \operatorname{acos}\left(\frac{x_{N-2}^2 + |h_{N-1}|^2 - |h_N|^2}{2x_{N-2}\cdot|h_{N-1}|}\right)$
    $\Phi_{N-1} = \{(\gamma_{N-2,\star} + \pi - \delta_{N-1})_{2\pi}, (\gamma_{N-2,\star} + \pi + \delta_{N-1})_{2\pi}\}$
    randomly select $\phi_{N-1,\star} \in \Phi_{N-1}$
  else
    $\phi_{N,\star} = \left(\pi + \angle\big(\overrightarrow{x_{N-2}e^{j\gamma_{N-2,\star}}} + \overrightarrow{|h_{N-1}|e^{j\phi_{N-1,\star}}}\big)\right)_{2\pi}$
  end if
end for
Output: $\{\phi_{1,\star}, \ldots, \phi_{N,\star}\}$

Moreover, from Fig. 6 we have

$$\overrightarrow{|h_N|e^{j\phi_N}} = -\left(\overrightarrow{x_{N-2}e^{j\gamma_{N-2,\star}}} + \overrightarrow{|h_{N-1}|e^{j\phi_{N-1}}}\right). \tag{37}$$

If ϕ_{N-1} is selected as $\phi_{N-1,\star}$, there is only one choice for ϕ_N, which can be expressed accordingly as

$$\phi_{N,\star} = \left(\pi + \angle\big(\overrightarrow{x_{N-2}e^{j\gamma_{N-2,\star}}} + \overrightarrow{|h_{N-1}|e^{j\phi_{N-1,\star}}}\big)\right)_{2\pi}. \tag{38}$$

For consistency, we can express the feasible set of ϕ_N as

$$\Phi_N \triangleq \left\{\left(\pi + \angle\big(\overrightarrow{x_{N-2}e^{j\gamma_{N-2,\star}}} + \overrightarrow{d_{N-1}e^{j\phi_{N-1,\star}}}\big)\right)_{2\pi}\right\}. \tag{39}$$

To make the above description clear, we summarize the procedure of polygon construction based solver for Eqn. (13) in Algorithm 1. Note that in Algorithm 1, we randomly select the ultimate $\phi_{n,\star}$ from its feasible set Φ_n, $n = 1, \ldots, N-1$. By doing so, we have implicitly assumed that Φ_n is feasible whenever $\phi_{n-1,\star} \in \Phi_{n-1}$, $n = 2, \ldots, N$. In fact, this is a reasonable assumption as we studied in the next subsection. Once ϕ_n is obtained, $n = 1, \ldots, N$, the corresponding weight vector can be expressed as

$$\mathbf{w} = \left[e^{j(\phi_{1,\star}+\vartheta_1)_{2\pi}}, \ldots, e^{j(\phi_{N,\star}+\vartheta_N)_{2\pi}}\right]^{\mathrm{T}}. \tag{40}$$

Remark 1: In the above discussions, the feasible sets of ϕ_n are specified according to their natural order. In other words, the determinations of Φ_{n-1} and ϕ_{n-1} are earlier than those of Φ_n and ϕ_n. In fact, with the same concept, one can exchange arbitrarily the order of phase determinations, although the expressions of $\mathbb{X}_n$ and Φ_n will change accordingly.

C. Solution Analysis

With the polygon construction approach, we next present a solution analysis for Eqn. (13). To do so, we first derive the following lemma that guarantees the non-nullity of the set $\mathbb{X}_n$, $n = 1, \ldots, N-2$.

Lemma 2: The set $\mathbb{X}_1$ is non-empty if (16) is satisfied. The set $\mathbb{X}_n$ is non-empty if $x_{n-1} \in \mathbb{X}_{n-1}$, $n = 2, \ldots, N-2$.

Proof: See Appendix A. ■

Note that if $\mathbb{X}_n$ is non-empty, the corresponding set Φ_n is also non-empty, $n = 1, \ldots, N-2$. This can be validated according to the expression of Φ_n in (33). Then it is not hard to obtain the following lemma that guarantees the feasibilities of Φ_n's, $n = 1, \ldots, N$.

Lemma 3: The set Φ_1 is non-empty if (16) is satisfied. The set Φ_n is non-empty if $\phi_{n-1,\star} \in \Phi_{n-1}$, $n = 2, \ldots, N-2$. Moreover, if $\phi_{N-2,\star} \in \Phi_{N-2}$, both Φ_{N-1} and Φ_N are non-empty.

According to Lemma 3, if (16) is satisfied and $\phi_{n,\star}$ is selected in sequence from the corresponding set Φ_n, $n = 1, \ldots, N$, the resulting $\{\phi_{1,\star}, \ldots, \phi_{N,\star}\}$ will be a feasible solution for Eqn. (13). With this result, one can obtain a qualified solution for Eqn. (13) by randomly selecting $\phi_{n,\star}$ from Φ_n in order ($n = 1, \ldots, N-1$), as described in Algorithm 1. Moreover, we can obtain the following proposition laying the foundation for secure transmission studied in the next subsection.

Proposition 1: Given $|h_0|, |h_1|, \ldots, |h_N| > 0$, there exist infinite solutions[1] for Eqn. (13), if and only if:

$$2\max\{|h_0|, |h_1|, \ldots, |h_N|\} < \sum_{i=0}^{N} |h_i|. \tag{41}$$

Proof: See Appendix B. ■

Note that a strict inequality is applied in (41), which is different from the result in (16). Proposition 1 shows that Eqn. (13) has infinite solutions if and only if the largest edge among $\{|h_0|, |h_1|, \ldots, |h_N|\}$ is strictly less than the summation of the remaining ones. This leads to the idea to find infinite qualified weight vectors and achieve secure transmission by changing weights at symbol rate. It should be noted that there may be strong correlations between different qualified weights, even though infinitely many weight candidates are available. More details about this will be presented later in Section IV-A and Section V-B.

[1] All phase solutions are within the range $[0, 2\pi)$, i.e., no phase wrapping occurred.

In addition, by combining Lemma 1 and Proposition 1, we can obtain the following interesting corollary.

Corollary 1: Given $|h_0|, |h_1|, \ldots, |h_N| > 0$, Eqn. (13) has finite solutions[2] if and only if:

$$2\max\{|h_0|, |h_1|, \ldots, |h_N|\} = \sum_{i=0}^{N} |h_i|. \tag{42}$$

IV. The Proposed Secure Transmission Algorithms

On the basis of the polygon construction approach discussed in Section III, we next present two secure transmission algorithms.

A. Secure Transmission via Polygon Construction

As studied earlier, under the condition (41), there are infinitely many solutions of $\{\phi_{1,\star}, \ldots, \phi_{N,\star}\}$ for Eqn. (13), the resulting weight vectors in (40) all satisfy $\mathbf{h}^{\mathrm{H}}\mathbf{w} = |h_0|$. As mentioned earlier, $|h_0|$ is a pre-assigned constant. To avoid any confusion, in the following study we replace $|h_0|$ with a new notation β, which has a physical meaning and stands for the beam gain at Bob. Again, β and $|h_0|$ are exchangeable and they always take the same value. As a result, we have

$$\mathbf{h}^{\mathrm{H}}\mathbf{w} = \beta. \tag{43}$$

This means that all these infinitely many weight vectors can guarantee the same beam gain for Bob. One can see that these weight vectors are designed for the channel vector $\mathbf{h}$ of Bob, while they may not fit to other channels, such as Eves' channels. This brings an idea to apply different weight vectors at different transmission time instants by randomly selecting $\mathbf{w}$ from its feasible set. Before presenting more details about the proposed secure transmission schemes, we next specify the feasible set of β that makes the condition (41) satisfied.

Following the notations used in Section III, one can see that the inequality (41) is satisfied if and only if:

$$|h|_{\max}(1) \le \beta < S(1) \tag{44}$$

or

$$\beta < |h|_{\max}(1) < \beta + S(1) - |h|_{\max}(1). \tag{45}$$

After some manipulations, we can obtain the following compact version of (44) and (45) as

$$\max\{2|h|_{\max}(1) - S(1), 0\} < \beta < S(1) \tag{46}$$

under which one can always find infinitely many $\mathbf{w}$ satisfying (43).

Going back to the secure transmission problem developed in Section II and recalling (10), the following additional constraint:

$$\beta > \rho \tag{47}$$

should be imposed on β to guarantee a reliable communication. Combining (46) and (47), one gets

$$r < \beta < S(1) \tag{48}$$

[2]In fact, only one solution (within $[0, 2\pi)$) exists in this case.

where

$$r \triangleq \max\{2|h|_{\max}(1) - S(1), \rho\}. \tag{49}$$

Note that the condition $\rho < S(1)$ has been implicitly assumed.

Then, for $\forall\beta$ satisfying (48), one can obtain infinite weight vectors that all can achieve desired transmission towards Bob. In practice, Eve's location is usually unknown without its cooperation. Nevertheless, since different weight vectors produce different results towards the undesired receivers, the received signals at Eves can be scrambled if different weight vectors are applied at different time instants.

On one hand, the larger β contributes to the higher receiving SNR for Bob. This means that the closer of β to $S(1)$ results in the higher SNR for Bob. On the other hand, the closer of β to $S(1)$ is, the more correlated of the solutions of the weight vectors $\mathbf{w}(k)$ in (40) will be. It implies that Eves may be easier to track these weight vectors $\mathbf{w}(k)$, i.e., the transmission is less secure. For example, in the extreme case when $\beta = S(1)$, all the solutions of the weight vectors are identical as described in Corollary 1.

One possible way to balance the detection performance (i.e., the SNR) for Bob and the security is to select a moderate β within the interval $(r, S(1))$. In such a manner, the distribution of $\angle(\mathbf{g}_q^{\mathrm{H}}\mathbf{w}(k))$ $(k = 1, 2\ldots)$ can be decentralized, without violating the SNR constraint. Nevertheless, without the knowledge of Eves' CSI, one has to select β empirically.

In this paper, we propose an alternative by randomly changing β at symbol rate. More specifically, at each time instant k, we randomly choose one β within $(r, S(1))$. On this basis, we select an arbitrary phase solution for the corresponding equation in (13) with the polygon construction approach in Algorithm 1. Finally, we apply the resulting weight vector in (40) to transmit signal at the transmitter. In the above transmission scheme, both larger β and smaller β are adopted, and their combination enhances the randomness along the undesired directions. In addition to changing β, for each selected β we choose the weight vector randomly to further scramble the distribution of the received symbols at Eves. With infinite weight vector candidates, it increases the difficulties for Eves in decoding information. In addition, note from *Remark 1* that the variable sequence can be randomly re-arranged when solving Eqn. (13). For this reason, we can randomly exchange the solving order in the phase determination procedure. To make the above proposed secure transmission algorithm clear, we summarize its implementation steps in Algorithm 2. Note that in the 8th line of Algorithm 2, we have utilized the fact that $\mathbf{J}^{-1} = \mathbf{J}^{\mathrm{T}}$, according to which the computational complexity can be reduced.

B. Modified Secure Transmission With Relaxed Symbol Region

In Section IV-A, we propose a secure transmission scheme, in which the received signal phases by Bob are strictly equal to those of the symbols of interest, i.e., $\zeta(k)$. The strict phase constraint decreases the degrees of freedom (DOF) in designing the weight vector $\mathbf{w}$. To increase the DOF and further scramble the received symbols along the undesired directions, we next present a modified secure transmission algorithm using a relaxed

Algorithm 2: Secure Transmission via Polygon Construction.

Input: $\mathbf{h} = [h_1, \ldots, h_N]^{\mathrm{T}}$, $\sqrt{E_s}$, σ_d^2, Γ_d
Initialize: $|h|_{\max}(1) = \max\{|h_1|, \ldots, |h_N|\}$, $S(1) = |h_1| + \cdots + |h_N|$, $\rho = \sqrt{\Gamma_d \sigma_d^2 / E_s}$, $r = \max\{2|h|_{\max}(1) - S(1), \rho\}$, $\vartheta_n = \angle h_n$, $n = 1, \ldots, N$
for $k = 1, 2, \ldots$ **do**
  randomly set $\beta \in (r, S(1))$
  randomly select an $N \times N$ permutation matrix $\mathbf{J}$
  $[|h'_1|, |h'_2|, \ldots, |h'_N|]^{\mathrm{T}} = \mathbf{J}[|h_1|, |h_2|, \ldots, |h_N|]^{\mathrm{T}}$
  apply the polygon construction algorithm in Algorithm 1 to solve $|h'_1|e^{j\phi'_1} + \cdots + |h'_N|e^{j\phi'_N} = \beta$, denote the solution as $\{\phi'_{1,\star}, \ldots, \phi'_{N,\star}\}$
  $[\phi_{1,\star}, \ldots, \phi_{N,\star}]^{\mathrm{T}} = \mathbf{J}^{\mathrm{T}}[\phi'_{1,\star}, \ldots, \phi'_{N,\star}]^{\mathrm{T}}$
  Output: $\mathbf{w}(k) = [e^{j(\phi_{1,\star}+\vartheta_1)_{2\pi}}, \ldots, e^{j(\phi_{N,\star}+\vartheta_N)_{2\pi}}]^{\mathrm{T}}$
end for

symbol region and allowing relaxed received signal phases by Bob to locate within the range, such as, $[\zeta(k) - \Delta, \zeta(k) + \Delta]$. This leads to the idea to incorporate an additional phase rotation operation (at each transmission instant) to the resulting weight vectors of Algorithm 2. Note that the concept of relaxed symbol region is not new and has been used in [22]–[25]. With a relaxed symbol region for Bob, the randomnesses of the received symbols at Eves can be further improved.

More specifically, to guarantee a reliable communication with Bob, we rotate the resulting weight vector $\mathbf{w}(k)$ of Algorithm 2 by a phase ψ_k satisfying

$$\psi_k \in [-\Delta, \Delta] \tag{50}$$

where Δ depends on the selection of β. After some calculation, it is not hard to obtain

$$\begin{aligned}\Delta &= \frac{\pi}{M} - \arcsin\left(\frac{\tau}{\beta}\right) \\ &= \frac{\pi}{M} - \arcsin\left(\frac{\rho \cdot \sin(\pi/M)}{\beta}\right)\end{aligned} \tag{51}$$

where M represents the order of the modulation, τ stands for the safety margin that separates the relaxed symbol region from the decision thresholds [22]. In (51), we have used the fact that $\tau = \rho \cdot \sin(\pi/M)$. An intuitive illustration for QPSK modulation is presented in Fig. 7 to make the above descriptions clear. Finally, we summarize the modified secure transmission algorithm in Algorithm 3.

Remark 2: Note that in the above discussions, we assume that there is only one intended user. The reason is that the transmitter has a single RF chain, as presented in Fig. 1, and only single stream can be supported. Nevertheless, even with a single RF chain, we can extend the polygon construction concept to create multiple symbols to more than one intended user, by using the concept of DM [12]. Different from the traditional transmission schemes in which the transmitted signal vector is expressed

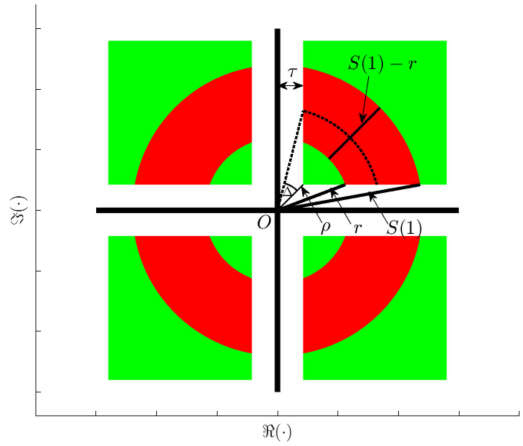


Fig. 7. Illustration of relaxed symbol region for QPSK modulation (the green rectangles stands for the relaxed symbol regions, the red rings are Bob's received symbols with the modified algorithm).

as the product of a symbol vector and a precoding matrix, in DM one can design a common transmitted signal vector (i.e., $\mathbf{x}$) directly in the RF domain, and synthesize the desired symbols with $\mathbf{x}$ for multiple intended users [19]. Since multiple users need to be supported simultaneously, a more complicated improved polygon construction algorithm is required. The basic idea of the improved algorithm is to construct multiple polygons with different edges and phases. On the other hand, with the improved polygon construction algorithm, we can also realize multi-user analog precoding and secure transmission by using a transmitter with multiple RF chains. In this case, one can design a precoding matrix with constant modulus constraint, and then obtain the transmitted signal vector by multiplying the desired user symbol vector with the designed precoding matrix. All the above points will be addressed in our future work.

Remark 3: Note that Algorithm 2 and Algorithm 3 are developed for PSK modulations for the sake of simplicity. For other modulation types (e.g., QAM) with different detection regions, the same rationale can be straightforwardly applied as presented later in Section V-C.

Remark 4: Different from the switched array techniques in [14] and [15] that select a few antennas for beamforming, the proposed algorithms do not require antenna switches and all the antennas are active. As a result, the undesirable grating lobe and high sidelobe level can be alleviated. On the other hand, by creating a codebook of weighting vectors that possess low sidelobes and selecting the transmitting weights from the codebook, the sidelobe level can be further lowered as presented in [14] and [16].

C. Computational Complexity

In this part, we analyze the computational complexities of the proposed algorithms. According to the descriptions in Algorithm 2 and Algorithm 3, the proposed two secure transmission algorithms only require some simple additions or comparison operations with low computational complexities. Among them, the main computation attributes to the calculation of

Algorithm 3: Modified Secure Transmission with Relaxed Symbol Region.

Input: $\mathbf{h} = [h_1, \ldots, h_N]^{\mathrm{T}}$, $\sqrt{E_s}$, σ_d^2, Γ_d, M
Initialize: $|h|_{\max}(1) = \max\{|h_1|, \ldots, |h_N|\}$, $S(1) = |h_1| + \cdots + |h_N|$, $\rho = \sqrt{\Gamma_d \sigma_d^2 / E_s}$, $r = \max\{2|h|_{\max}(1) - S(1), \rho\}$, $\vartheta_n = \angle h_n$, $n = 1, \ldots, N$
for $k = 1, 2, \ldots$ **do**
  randomly set $\beta \in (r, S(1))$
  $\Delta = \pi/M - \arcsin(\rho \cdot \sin(\pi/M)/\beta)$
  randomly set $\psi_k \in [-\Delta, \Delta]$
  randomly select an $N \times N$ permutation matrix $\mathbf{J}$
  $[|h'_1|, |h'_2|, \ldots, |h'_N|]^{\mathrm{T}} = \mathbf{J}[|h_1|, |h_2|, \ldots, |h_N|]^{\mathrm{T}}$
  apply the polygon construction algorithm in Algorithm 1 to solve $|h'_1|e^{j\phi'_1} + \cdots + |h'_N|e^{j\phi'_N} = \beta$, denote the solution as $\{\phi'_{1,\star}, \ldots, \phi'_{N,\star}\}$
  $[\phi_{1,\star}, \ldots, \phi_{N,\star}]^{\mathrm{T}} = \mathbf{J}^{\mathrm{T}}[\phi'_{1,\star}, \ldots, \phi'_{N,\star}]^{\mathrm{T}}$
  Output: $\mathbf{w}(k) = e^{j\psi_k}[e^{j(\phi_{1,\star}+\vartheta_1)_{2\pi}}, \ldots, e^{j(\phi_{N,\star}+\vartheta_N)_{2\pi}}]^{\mathrm{T}}$
end for

$|h|_{\max}(n+1)$ in the determination of $\mathbb{X}_n$ in (29). Overall, this is equivalent to a sorting of N real numbers, with a computational complexity $\mathcal{O}(N\log_2 N)$. All other manipulations have computational complexity $\mathcal{O}(N)$. Therefore, both of the two proposed algorithms are computationally attractive with the same computational complexity $\mathcal{O}(N\log_2 N)$.

V. Numerical Results

In this section, simulations are presented to demonstrate the effectivenesses of the proposed secure transmission algorithms. Unless otherwise specified, we use a 20-element ULA and consider multi-path mmWave channels described in (3) and (5). The number of channel paths, i.e., L_d in (3) or L_q in (5), is fixed as 5. The AoD of each path is assumed to be uniformly distributed in $[-\pi/2, \pi/2]$. For simplicity, we set $\Gamma_d = 160$, $\sqrt{E_s} = 1$ and $\sigma_d^2 = 0.1$, thus resulting $\rho = 4$. We define $\mathrm{SNR} \triangleq E_s/\sigma_d^2$ and assume that the noise powers at Bob and Eve are always identical. The simulation trial number is taken as 2×10^7 if not explicitly specified.

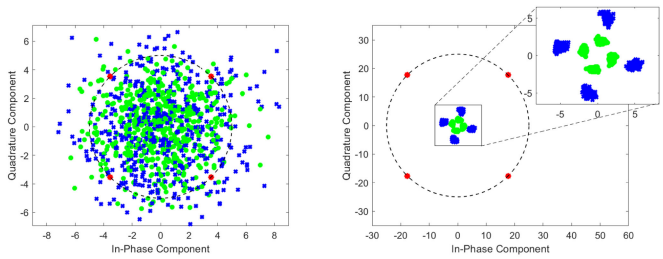
A. Constellation Synthesis Results With Fixed β

In the first example, we consider two Eves and present the constellation synthesis results with QPSK modulation using the proposed polygon construction approach. Table I provides the entry values of the channel vector $\mathbf{h}$ in one realization. After some calculation, one can obtain that $|h|_{\max}(1) = 2.2073$, $S(1) = 25.1194$ and $r = \rho = 4$. Thus, the feasible set of β is $(4, 25.1194)$ in this scenario. We next depict the noiseless received constellations at Bob and Eves, by fixing β as different values. The number of time instants is taken as 500.

In the first case, we set $\beta = 5$. The noise-free received constellations are shown in Fig. 8(a). The red color points stand for the synthesized constellations at Bob, and the green and blue ones denote the resulting constellations at the first Eve and the second Eve, respectively. From Fig. 8(b), one can clearly observe that only 4 points are synthesized at Bob and the resulting constellation is undistorted. In contrast, the corresponding constellations at the two Eves are randomized with no evident pattern. Table II lists the resulting phases of $\mathbf{w}$ at the first four time instants. It can be checked that the phases at different time

TABLE I
Element Values of $\mathbf{h}$

n	h_n	n	h_n
1	$0.6928e^{j0.5258}$	11	$1.7020e^{j0.9018}$
2	$1.8808e^{j4.2005}$	12	$1.8871e^{j4.9358}$
3	$1.9896e^{j2.9017}$	13	$2.2073e^{j3.5416}$
4	$0.6173e^{j0.1126}$	14	$0.7611e^{j3.2271}$
5	$1.1198e^{j0.9779}$	15	$1.8750e^{j0.9515}$
6	$0.3202e^{j0.3919}$	16	$1.3125e^{j5.5432}$
7	$1.1921e^{j1.9526}$	17	$1.6447e^{j2.9199}$
8	$1.3517e^{j5.0372}$	18	$1.0155e^{j3.0950}$
9	$0.4221e^{j3.7346}$	19	$1.0307e^{j1.0637}$
10	$0.6968e^{j0.3450}$	20	$1.4003e^{j5.7674}$



(a) (b)

Fig. 8. Noiseless received constellations at Bob and Eves with differently fixed β (the red color points represent the resulting constellation at Bob, the green and blue ones stand for the synthesized constellations at the first Eve and the second Eve, respectively). (a) $\beta = 5$. (b) $\beta = 25$.

TABLE II
List of the Resulting Phases of $\mathbf{w}$ With Fixed $\beta = 5$

n	φ_n $(k=1)$	φ_n $(k=2)$	φ_n $(k=3)$	φ_n $(k=4)$
1	1.9517	1.4511	1.0168	3.3933
2	1.8604	5.9012	3.1134	1.9504
3	2.8630	5.8596	3.4043	5.1718
4	5.7267	4.0771	1.3960	0.3418
5	0.8386	1.3212	1.9330	1.1697
6	2.3831	0.6743	1.5510	0.2101
7	2.1855	5.9466	5.2997	2.2920
8	5.5607	1.0405	4.5414	1.6418
9	2.5413	3.1089	1.7841	1.6560
10	2.5522	4.5091	4.7127	0.7534
11	6.1551	1.2735	4.7225	2.0872
12	5.4707	4.2889	3.0177	4.8844
13	0.5388	5.4028	0.7744	3.3036
14	4.0629	2.5959	4.0591	3.1579
15	2.6219	0.4193	1.4561	5.8194
16	5.3100	4.7956	0.4320	5.4314
17	6.2123	1.9759	3.1458	5.7188
18	0.4828	2.4595	5.9337	3.2369
19	1.7200	0.3658	2.1094	0.3506
20	4.5290	1.5707	5.7127	2.7096

TABLE III
LIST OF THE RESULTING PHASES OF $\mathbf{w}$ WITH FIXED $\beta = 25$

n	$\varphi_n\ (k=1)$	$\varphi_n\ (k=2)$	$\varphi_n\ (k=3)$	$\varphi_n\ (k=4)$
1	0.5392	0.5848	0.4990	0.4633
2	4.2218	4.1897	4.1739	4.1852
3	2.9222	2.9140	2.8727	2.8389
4	0.1348	0.1148	0.0817	0.6843
5	1.2105	1.0053	0.9478	1.0126
6	0.3663	1.2028	0.3564	0.3708
7	1.9767	1.9705	1.9236	1.9338
8	5.0350	5.0299	5.0775	5.0289
9	3.7773	3.7591	3.7345	3.7215
10	0.0459	0.3619	0.3141	0.3308
11	0.7359	0.8945	0.9397	0.8460
12	4.9604	4.9404	4.9107	5.0377
13	3.5614	3.5370	3.5139	3.5245
14	3.2489	3.2355	3.0190	3.1964
15	0.9688	0.8493	0.9495	0.9346
16	5.5882	5.5180	5.5114	5.5252
17	2.9445	2.8290	2.9468	2.9067
18	3.1050	3.1114	3.0637	3.0721
19	0.8319	1.0625	1.4938	1.0404
20	5.8224	5.7838	5.7650	5.7448

instants are dispersed. In addition, one can see from Fig. 8(a) that the magnitudes of received symbol clusters of Eves are comparable to that of Bob.

In the second case, we increase the value of β and set $\beta = 25$. The resulting noise-free constellations are depicted in Fig. 8(b), from which one can see that a clear constellation result is maintained for Bob. In this scenario, the magnitudes of received symbol clusters of Eves are less than that of Bob. Although the synthesized constellations at Eves appear randomized, the resulting shapes of symbol clusters are identical with that of Bob after scaling and rotation. This is resulted by the limited DOF when a big β is taken. The resulting phases of the weight vector $\mathbf{w}$ at different time instants are randomized and concentrated with small differences, as presented in Table III for the first four time instants. With the synthesized constellations in Fig. 8(b), it is not difficult for a smart eavesdropper to decode the data.

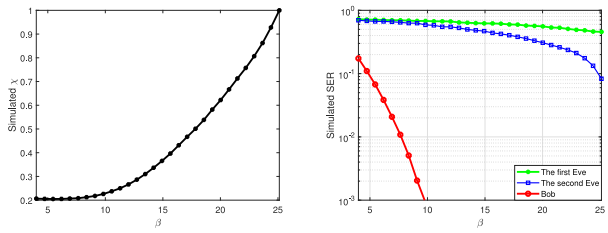
B. Performance Investigation by Varying β

Following the setting in Section II-A, we next explore the correlations between weight vectors at different time instants. More specifically, we define

$$\chi \triangleq \text{Mean}(|\varrho|) \tag{52}$$

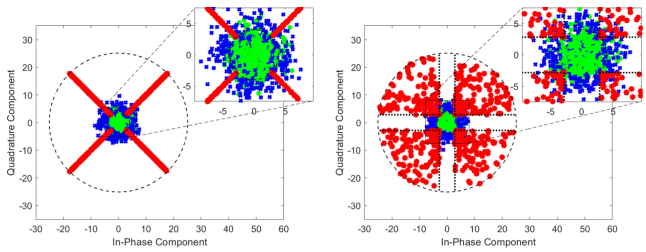
where ϱ measures the correlation coefficient between weight vectors at two different time instants, and the resulting χ in (52) is a measure of average correlations of the distinct weight vectors. The curve of simulated χ versus β is presented in Fig. 9(a) with the channel vector $\mathbf{h}$ of Bob given in Table I. As predicted, one can clearly see from Fig. 8(a) that the correlation of weight vectors at different time instants improves as β increases.

In addition to the above investigation on χ, we next examine the symbol error rates (SER) at Bob and the undesired Eves using the transmission scheme with a fixed β. In this scenario, we set $\text{SNR} = -5$ dB and constrain the received signal phases by Bob strictly equal to those of the symbols of interest. The



(a) (b)

Fig. 9. Performance curves versus β. (a) Simulated χ versus β. (b) The resulting simulated SERs versus β (SNR $= -5$ dB).



(a) (b)

Fig. 10. Noiseless received constellations at Bob and Eves using the proposed algorithms with QPSK modulation (the red color points represent the resulting constellation at Bob, the green and blue ones stand for the synthesized constellations at the first Eve and the second Eve, respectively). (a) The 1st proposed algorithm. (b) The 2nd proposed algorithm.

resulting curves of SERs versus β are depicted in Fig. 9(b). One can observe that the SER of Bob decreases with the increase of β and becomes lower than 10^{-3} when β is greater than 10. The corresponding SERs of the two Eves are much higher than that of Bob. However, it can be seen that the resulting SERs of Eves also declines especially when β approaches to its maximal allowable value $S(1)$. Thus, a much lower SER can be obtained by Eve in the higher SNR scenario, and the data may be revealed with the fixed β scheme.

C. Synthesis Results of the Proposed Algorithms

In this subsection, we present the constellation synthesis results of the two proposed algorithms. We follow Section V-A and use the channel vector specified in Table I. To show the wide applicabilities of the proposed algorithms, we next examine different modulation types.

1) QPSK Modulation: For comparison purpose, we first consider the QPSK modulation as it has been investigated in Section II-A. The noiseless received constellations at Bob and Eves with the 1st proposed algorithm presented in Algorithm 2 are depicted in Fig. 10(a). One can clearly see from Fig. 10(a) that the received constellation points at Bob form four regular segments. This is a necessary result of the 1st proposed algorithm, due to the random selection of β in the range $(r, S(1))$ in each transmission instant. Fig. 10(a) also shows the scrambled received constellations at the two undesired Eves. In general, the received symbols at Eves have small magnitudes and the corresponding distributions are irregular.

With the same configurations of the channel vectors, we next present the noiseless constellations received at Bob and Eves

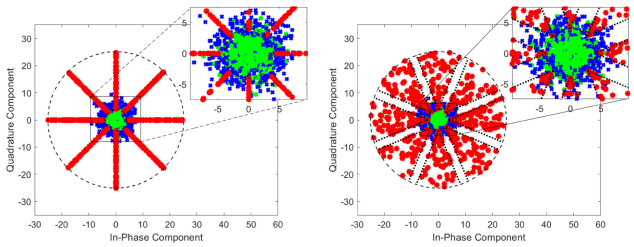


Fig. 11. Noiseless received constellations at Bob and Eves using the proposed algorithms with 8-PSK modulation (the red color points represent the resulting constellation at Bob, the green and blue ones stand for the synthesized constellations at the first Eve and the second Eve, respectively). (a) The 1st proposed algorithm. (b) The 2nd proposed algorithm.

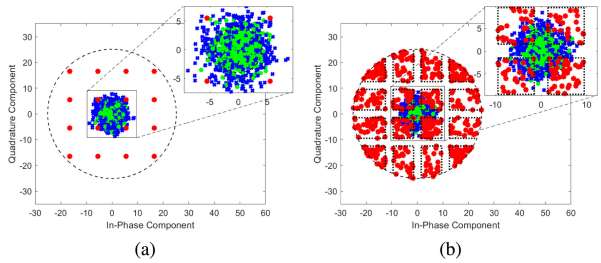


Fig. 12. Noiseless received constellations at Bob and Eves with 16-QAM using the proposed algorithms after slight modifications (the red color points represent the resulting constellation at Bob, the green and blue ones stand for the synthesized constellations at the first Eve and the second Eve, respectively). (a) The 1st proposed algorithm. (b) The 2nd proposed algorithm.

using the 2nd proposed algorithm in Algorithm 3. The results are shown in Fig. 10(b), from which one can see that the received symbols at Bob are all within the relaxed symbol region. The received constellations at Eves are randomized and no regular pattern can be observed. In fact, since an additional phase rotation procedure is employed, the 2nd proposed algorithm obtains a better security performance comparing to the 1st one, as investigated more specifically in Section V-D.

2) 8-PSK Modulation: In this case, we improve the modulation order and examine the resulting constellations with 8-PSK modulation. Fig. 11 depicts the noiseless received constellations at Bob and Eves with the two proposed algorithms. Similar to the QPSK case, the received constellation points at Bob form regular pattern with the 1st proposed algorithm (see Fig. 11(a)) and fall within the relaxed symbol region with the 2nd proposed algorithm (see Fig. 11(b)). As predicted, it can be seen from Fig. 11 that the received constellations at Eves are randomized and no regular pattern is resulted with both of the proposed algorithms.

3) 16-QAM: We next show the resulting constellations for 16-QAM using the proposed algorithms after slight modifications. Different from the PSK modulation schemes in which the symbols are distinguished mainly according to their phases, the constellation points of QAM are usually distinct in both phase and amplitude. For QAM, we modify the 1st algorithm by using several fixed β with appropriate values, such that the desired symbols at Bob can be synthesized. In this case, only finite β are available and the selections of β depend on the transmitting symbols. Nevertheless, under mild conditions, we can obtain infinitely many weight vector candidates for each symbol and its corresponding β. The received constellations at Eves can thus be scrambled by changing the weight vector at symbol rate. Similarly, the 2nd algorithm can be also extended to QAM, by allowing the in-phase and quadrature components of the received signals at Bob falling with the corresponding relaxed symbol region. In this case, β can be selected from different ranges, whose specific values depend on the transmitting symbols.

Fig. 12 depicts the noiseless received constellations at Bob and Eves with 16-QAM using the two proposed algorithms after slight modifications. More specifically, the noiseless received constellations of the 1st proposed algorithm are presented in Fig. 12(a). We can see clearly from Fig. 12(a) that the desired constellations are synthesized at Bob, while the received constellations at the two Eves are randomized. Fig. 12(b) shows the received constellations of the 2nd algorithm with the concept of relaxed symbol region for QAM [21]. From Fig. 12(b), one can see that the received symbols at Bob are all within the relaxed symbol region and the received constellations at Eves are randomized with no regular pattern.

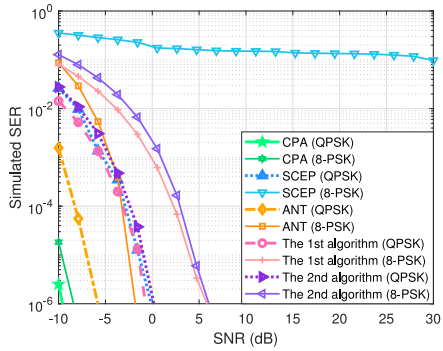


Fig. 13. Simulated SER for Bob versus SNR.

D. Security Performance of the Proposed Algorithms

In this subsection, we consider one Eve and investigate the security performance of the proposed algorithms. For comparison purpose, the performances of the conventional phased-array (CPA) transmission, the secure constant-envelope precoding (SCEP) transmission in [6] and the artificial noise transmission (ANT) in [33] will also be presented. Note that the SCEP algorithm may result noise leakage for Bob and the cost of ANT scheme is the additional RF chains.

1) SER Simulation: By varying the SNR from -10 dB to 30 dB, the resulting simulated SERs at Bob of different algorithms are presented in Fig. 13, with QPSK and 8-PSK modulations, respectively. We can see that the resulting SERs of 8-PSK modulation are higher than those of the QPSK modulation, and the performances of the proposed algorithms are worse than those of CPA and ANT. The resulting SER of SCEP is higher than 10^{-1} for 8-PSK modulation. Moreover, Fig. 13 shows that the SER of the 2nd proposed algorithm is slightly higher than that of the 1st one, under the same SNR setting.

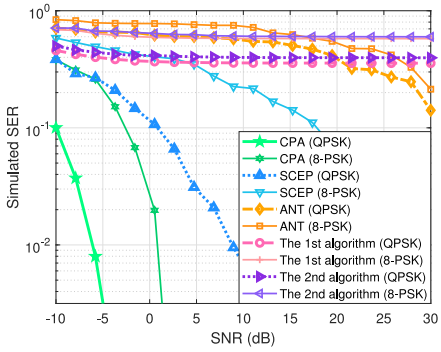


Fig. 14. Simulated SER for Eve versus SNR.

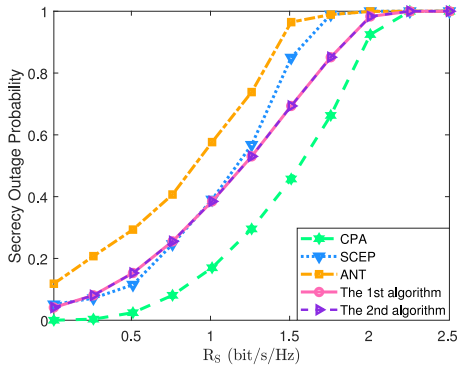


Fig. 15. Secrecy outage probability versus the threshold R_S.

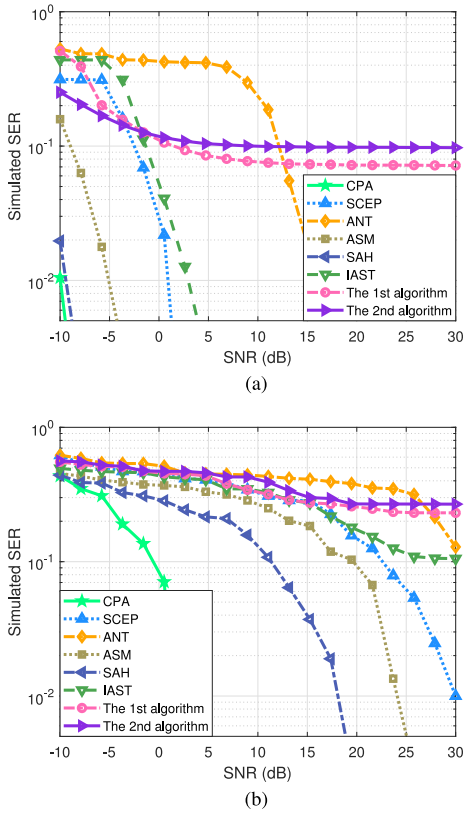


Fig. 16. SER comparison for Eve with single-path channels. (a) 8-PSK modulation. (b) 16-PSK modulation.

The corresponding simulated SERs for Eve versus the SNR are depicted in Fig. 14, from which we can see that the resulting SERs of 8-PSK modulation are higher than those of the QPSK modulation, for all the algorithms tested. For each modulation, one can clearly see from Fig. 14 that the resulting SERs of CPA, SCEP, ANT schemes decrease evidently with the increase of SNR, and the performances of the proposed algorithms are almost unchanged as SNR increases. For the proposed two algorithms, the resulting SERs at Eve are always greater than 0.3 for all SNRs tested. Moreover, it can be observed from Fig. 14 that the 2nd proposed algorithm obtains a higher SER than that of the 1st one. This result is not surprising and is consistent with the theoretical prediction, since an extra phase rotation procedure is incorporated in the 2nd devised algorithm.

2) Secrecy Outage Probability Simulation: We next explore the secrecy outage probabilities of different algorithms using 8-PSK modulation. According to [34]–[36], a secrecy outage event is declared when the instantaneous secrecy capacity drops below a predefined threshold R_S. For a given threshold R_S, the secrecy outage probability is defined as

$$P_{\text{out}} \triangleq \Pr(C_S < R_S) \tag{53}$$

where $C_S = \max\{\mathcal{I}(y_d; x) - \mathcal{I}(y_Q; x), 0\}$ is the secrecy capacity in the case of finite-alphabet input [37], the symbol x is drawn from the discrete uniform probability mass function of the 8-PSK constellation, y_d and y_Q are the received signals by Bob and Eve, respectively.

We apply the simulated counterparts to calculate the secrecy outage probability in (53). Taking $\text{SNR} = -5$ dB, Fig. 15 compares the resulting curves of secrecy outage probability versus the threshold R_S. One can see from Fig. 15 that the proposed two algorithms obtain identical secrecy outage probabilities that are lower than those of the SCEP and ANT algorithms, especially when R_S is greater than 1 bit/s/Hz.

E. Single-Path Channel Investigation

In the above simulations, multi-path mmWave channels are used. We next simplify the model as single-path mmWave channels and compare the performances of the proposed two algorithms with those of the existing works. In this case, we assume that Bob is located along $\theta_T = 30^\circ$. There is an Eve with angular location $\theta_U = 28^\circ$. Note that the direction of Eve is near to Bob. With the assumption of single-path mmWave channel, we have $\mathbf{h} = \mathbf{a}(\theta_T)$ and $\mathbf{g} = \mathbf{a}(\theta_U)$, where $\mathbf{a}(\theta)$ stands for the array response vector and its expression can be found in (4). In this case, we evaluate the simulated SER at Eve with 8-PSK and 16-PSK modulations, respectively. In addition to the CPA, SCEP and ANT schemes as presented in Section V-D, we also compare the performances of the proposed algorithms with those of the antenna subset modulation (ASM) scheme in [14], the silent antenna hopping (SAH) scheme in [15] and the inverted antenna subset transmission (IAST) scheme in [16].

The resulting SERs for Eve versus SNR with 8-PSK modulation are presented in Fig. 16(a). One can see that the existing CPA, SCEP, ASM, SAH and IAST schemes obtain lower SERs with values close to zero, in the case where SNR is higher than 5 dB. The resulting SER of ANT scheme drops rapidly

when SNR is greater than 15 dB. The proposed two algorithms outperform the existing algorithms and obtain SERs that are greater than $10^{-1.5}$ in the high SNR scenarios. Therefore, the received constellation at Eve can be still scrambled by the proposed two algorithms, although the Eve is located near to Bob and their channel vectors may have some similarities.

Fig. 16(b) presents the resulting SERs for Eve versus SNR with 16-PSK modulation. Similar to the case of 8-PSK modulation, the proposed two algorithms obtain higher SERs than the existing ones, especially in the high SNR scenarios. In this case, the performance of the ANT algorithm is comparable to those of the proposed algorithms. However, as aforementioned, the ANT scheme requires additional RF chains to generate the artificial noise. Comparing to the result in Fig. 16(a), the resulting SERs of different algorithms in Fig. 16(b) have been increased, due to the increase of the modulation order.

VI. Conclusions

In this paper, we have presented two secure transmission algorithms for mmWave wireless communication using a geometric approach. Considering a phased-array transmission structure and focusing on the PSK modulation, we have shown that the traditional constellation synthesis problem can be solved with the aid of polygon construction in the complex plane. Moreover, for a given constellation synthesis task, a detailed analysis has been presented to show that there exist infinite qualified transmitting weight vectors under a mild condition. On this basis, we have developed two secure transmission algorithms, in which the transmitting weight vectors are varied at symbol rate, and the received symbols at the undesired receivers can be scrambled. The proposed algorithms have analytical solutions with low computational complexities. Comparing to the existing approaches, our algorithms enhance the security and have no limitation on the channel model. The extensions of the proposed schemes to other modulation types are applicable and have been examined in the case of QAM. Moreover, all the antennas are active in the proposed algorithms and the on-off switching circuit is not needed. Simulations have been presented to verify the effectivenesses of the proposed two algorithms under various scenarios.

Appendix A
Proof of Lemma 2

To prove Lemma 2, we first study the non-nullity of $\mathbb{X}_1$. Suppose that (16) is true, we then have

$$\big||h_0|-|h_1|\big| < |h_0|+|h_1|. \tag{54}$$

Noting that $\big||h_0|-|h_1|\big| = 2\max\{|h_0|,|h_1|\}-|h_0|-|h_1|$, one can obtain

$$\begin{aligned}\big||h_0|-|h_1|\big| &\le 2\max\{|h_0|,|h_1|,\ldots,|h_N|\}-|h_0|-|h_1| \\ &\le \sum_{i=0}^{N}|h_i|-|h_0|-|h_1| = S(2).\end{aligned} \tag{55}$$

Moreover, according to (16), we can derive that

$$\begin{aligned}2|h|_{\max}(2)-S(2) &\le 2\max\{|h_0|,|h_1|,\ldots,|h_N|\}-S(2) \\ &\le \sum_{i=0}^{N}|h_i|-S(2) = |h_0|+|h_1|.\end{aligned} \tag{56}$$

In addition, since $|h|_{\max}(2) < S(2)$, it yields

$$2|h|_{\max}(2)-S(2) < S(2). \tag{57}$$

Recalling the expression of $\mathbb{X}_1$ in (21) and combining the results (54)–(57), one has $x_{1,\min} \le x_{1,\max}$. Thus, $\mathbb{X}_1$ is non-empty if (16) is satisfied.

In the following derivations, we will show that the set $\mathbb{X}_n$ is non-empty if $x_{n-1} \in \mathbb{X}_{n-1}$, $n = 2,\ldots,N-2$.

To carry out the proof, we give $\forall n \in \{2,\ldots,N-2\}$. Note that $x_{n-1} \ge 0$ if $x_{n-1} \in \mathbb{X}_{n-1}$. Then, one has

$$\big|x_{n-1}-|h_n|\big| \le x_{n-1}+|h_n|. \tag{58}$$

Besides, it is not hard to find

$$2|h|_{\max}(n+1)-S(n+1) \le S(n+1). \tag{59}$$

Moreover, the following inequalities are satisfied:

$$|h_n|-S(n+1) \le 2|h|_{\max}(n)-|h_n|-S(n+1) \tag{60a}$$

$$\le 2|h|_{\max}(n)-S(n) \tag{60b}$$

$$\le x_{n-1} \le S(n) = |h_n|+S(n+1) \tag{60c}$$

which further implies

$$\big|x_{n-1}-|h_n|\big| \le S(n+1). \tag{61}$$

Note that in (60), we have utilized the fact that $|h|_{\max}(n) \ge |h_n|$ and $x_{n-1} \in \mathbb{X}_{n-1}$. Furthermore, according to (60), it is not difficult to see

$$\begin{aligned}2|h|_{\max}(n+1)-S(n+1) &\le 2|h|_{\max}(n)-S(n)+|h_n| \\ &\le x_{n-1}+|h_n|.\end{aligned} \tag{62}$$

Combining (58), (59), (61) and (62), and recalling the definitions of $x_{n,\min}$ and $x_{n,\max}$ in (29), we have

$$x_{n,\min} \le x_{n,\max} \tag{63}$$

which indicates the set $\mathbb{X}_n$ is non-empty, where n can be taken as $2,\ldots,N-2$. This completes the proof.

Appendix B
Proof of Proposition 1

1) Proof of sufficiency: According to the analysis in Section III-B, one can see that the set Φ_1 is an uncountable set, provided that $x_{1,\min} < x_{1,\max}$. Moreover, according to Lemma 3, given the set Φ_1 and $\forall \phi_{1,\star} \in \Phi_1$, there always exists a solution for Eqn. (13). This indicates that Eqn. (13) has infinite solutions, provided that $x_{1,\min} < x_{1,\max}$.

On the other hand, we note from *Remark 1* that the order in solving the phases $\phi_1, \ldots, \phi_N$ for Eqn. (13) can be exchanged. Combing the above analysis, it is not hard to learn that Eqn. (13) has infinite solutions if $\exists p \in \{1, \ldots, N\}$, such that

$$x_{\min}^{(p)} < x_{\max}^{(p)} \tag{64}$$

where $x_{\min}^{(p)}$ and $x_{\max}^{(p)}$ are similarly defined to $x_{1,\min}$ and $x_{1,\max}$ in (21), respectively, and represent the corresponding parameters when placing the phase ϕ_p in the first solving step. More specifically, $x_{\min}^{(p)} \triangleq \max\{\big||h_0| - |h_p|\big|, d(p)\}$ and $x_{\max}^{(p)} \triangleq \min\{|h_0| + |h_p, S(1) - |h_p\}$ with $d(p) \triangleq 2\max\{|h_1|, \ldots, |h_{p-1}|, |h_{p+1}|, \ldots, |h_N|\} - S(1) + |h_p|$. We next show that there always exists $p \in \{1, \ldots, N\}$ such that (64) is satisfied, provided that (41) is true.

To do so, we reformulate the inequality (64) as

$$\big||h_0| - |h_p|\big| < |h_0| + |h_p| \tag{65a}$$

$$\big||h_0| - |h_p|\big| < S(1) - |h_p| \tag{65b}$$

$$d(p) < |h_0| + |h_p| \tag{65c}$$

$$d(p) < S(1) - |h_p|. \tag{65d}$$

Since $|h_0|, |h_1|, \ldots, |h_N| > 0$, we know that the first inequality (65a) is satisfied for $\forall p \in \{1, \ldots, N\}$. According to (41), it is not difficult to derive

$$\begin{aligned}\big||h_0| - |h_p|\big| &= 2\max\{|h_0|, |h_p|\} - |h_0| - |h_p| \\ &\le 2\max\{|h_0|, |h_1|, \ldots, |h_N|\} - |h_0| - |h_p| \\ &< \sum_{i=0}^{N} |h_i| - |h_0| - |h_p| = S(1) - |h_p| \end{aligned} \tag{66}$$

which is consistent with (65b) whenever $p \in \{1, \ldots, N\}$. The third inequality (65c) can be reshaped as

$$2\max\{|h_1|, \ldots, |h_{p-1}|, |h_{p+1}|, \ldots, |h_N|\} < \sum_{i=0}^{N} |h_i| \tag{67}$$

which is also true, provided that (41) is satisfied. As for the fourth inequality (65d), it is equivalent to

$$\max\{|h_1|, \ldots, |h_{p-1}|, |h_{p+1}|, \ldots, |h_N|\} + |h_p| < S(1)$$

which is always established for $\forall p \in \{1, \ldots, N\}$. Consequently, (65) or its equivalent version (64) is actually satisfied for $\forall p \in \{1, \ldots, N\}$. Thus, Eqn. (13) has infinite solutions if (41) is satisfied. This completes the proof of sufficiency.

2) Proof of necessity: We next prove that if Eqn. (13) has infinite solutions, then the inequality (41) holds.

To do so, we assume that Eqn. (13) has infinite solutions but (41) is not satisfied. In this case, one can recall Lemma 1 and obtain that

$$2\max\{|h_0|, |h_1|, \ldots, |h_N|\} = \sum_{i=0}^{N} |h_i|. \tag{68}$$

In fact, the above equation indicates that Eqn. (13) has a unique solution rather than infinite ones. To see this, we assume without loss of generality that $|h_p| = \max\{|h_0|, |h_1|, \ldots, |h_N|\}$, $p \in \{1, \ldots, N\}$. In this scenario, all the resulting solutions should satisfy

$$\left||h_0| - \sum_{i=1, i\neq p}^{N} |h_i| e^{j\phi_i}\right| = |h_p| = \sum_{i=0, i\neq p}^{N} |h_i|. \tag{69}$$

One can check that Eqn. (13) is established if taking $\phi_1 = \phi_2 = \cdots = \phi_{p-1} = \phi_{p+1} = \cdots = \phi_N = \pi$ and $\phi_p = 0$. With any other different phase settings (denoted as ϕ_i', $i = 1, \ldots, N$) within the set $[0, 2\pi)$, it yields

$$\left||h_0| - \sum_{i=1, i\neq p}^{N} |h_i| e^{j\phi_i'}\right| < \sum_{i=0, i\neq p}^{N} |h_i| \tag{70}$$

which is contradictory to (69). In the case that $|h_0| = \max\{|h_0|, |h_1|, \ldots, |h_N|\}$, the same result can be obtained. Therefore, Eqn. (13) only has one solution if (41) is not satisfied. This proves the necessity.

REFERENCES

[1] M. R. Akdeniz *et al.*, "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1164–1179, Jun. 2014.

[2] W. Roh *et al.*, "Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 106–113, Feb. 2014.

[3] R. Ford, M. Zhang, M. Mezzavilla, S. Dutta, S. Rangan, and M. Zorzi, "Achieving ultra-low latency in 5G millimeter wave cellular networks," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 196–203, Mar. 2017.

[4] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008.

[5] Y. Pei, Y. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[6] J. Zhu, N. Wang, and V. K. Bhargava, "Per-antenna constant envelope precoding for secure transmission in large-scale MISO systems," in *Proc. IEEE/CIC Int. Conf. Commun. China*, 2015, pp. 1–6.

[7] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[8] T. Lv, H. Gao, X. Li, S. Yang, and L. Hanzo, "Space-time hierarchical-graph based cooperative localization in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 64, no. 2, pp. 322–334, Jan. 2016.

[9] A. Hu, T. Lv, H. Gao, Z. Zhang, and S. Yang, "An ESPRIT-based approach for 2-D localization of incoherently distributed sources in massive MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 996–1011, Oct. 2014.

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

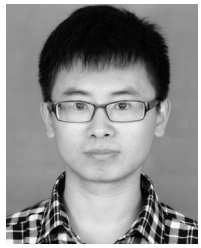
[11] Y. P. Hong, P. Lan, and C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[12] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[13] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[14] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[15] N. N. Alotaibi and K. A. Hamdi, "Switched phased-array transmission architecture for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1303–1312, Mar. 2016.
[16] Y. Hong, X. Jing, and H. Gao, "Programmable weight phased-array transmission for secure millimeter-wave wireless communications," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 2, pp. 399–413, May 2018.
[17] W. Wang and Z. Zheng, "Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1383–1396, Jul. 2018.
[18] X. Zhang, Z. He, B. Liao, and X. Zhang, "Fast array response adjustment with phase-only constraint: A geometric approach," *IEEE Trans. Antennas Propag.*, vol. 67, pp. 6439–6451, 2019.
[19] M. Alodeh *et al.*, "Symbol-level and multicast precoding for multiuser multiantenna downlink: A state-of-the-art, classification, and challenges," *IEEE Commun. Surv. Tuts.*, vol. 20, no. 3, pp. 1733–1757, Thirdquarter 2018.
[20] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Constructive multiuser interference in symbol level precoding for the MISO downlink channel," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2239–2252, May 2015.
[21] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Symbol-level multiuser MISO precoding for multi-level adaptive modulation," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5511–5524, Aug. 2017.
[22] H. Jedda, A. Mezghani, A. L. Swindlehurst, and J. A. Nossek, "Quantized constant envelope precoding with PSK and QAM signaling," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8022–8034, Dec. 2018.
[23] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1478–1493, Dec. 2016.
[24] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Energy-efficient symbol-level precoding in multiuser MISO based on relaxed detection region," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3755–3767, May 2016.
[25] C. Masouros and G. Zheng, "Exploiting known interference as green signal power for downlink beamforming optimization," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3628–3640, Jul. 2015.
[26] Y. Huang, J. Zhang, and M. Xiao, "Constant envelope hybrid precoding for directional millimeter-wave communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 845–859, Apr. 2018.
[27] X. Yu, J. Shen, J. Zhang, and K. B. Letaief, "Alternating minimization algorithms for hybrid precoding in millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 485–500, Apr. 2016.
[28] A. Alkhateeb, O. E. Ayach, G. Leus, and R. W. Heath, "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 831–846, Oct. 2014.
[29] O. E. Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath, "Spatially sparse precoding in millimeter wave MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1499–1513, Mar. 2014.
[30] S. Domouchtsidis, C. G. Tsinos, S. Chatzinotas, and B. Ottersten, "Symbol-level precoding for low complexity transmitter architectures in large-scale antenna array systems," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 852–863, Feb. 2019.
[31] J. Zhang, Y. Huang, J. Wang, B. Ottersten, and L. Yang, "Per-antenna constant envelope precoding and antenna subset selection: A geometric approach," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6089–6104, Dec. 2016.
[32] J. Pan and W. Ma, "Constant envelope precoding for single-user large-scale MISO channels: Efficient precoding and optimal designs," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 982–995, Oct. 2014.
[33] W. Zhao, S.-H. Lee, and A. Khisti, "Phase-only zero forcing for secure communication with multiple antennas," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1334–1345, Dec. 2016.
[34] 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, Jun. 2008.
[35] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 2, pp. 247–258, Feb. 2014.
[36] Y. Zou, X. Li, and Y. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.
[37] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3816–3825, Dec. 2012.



Xuejing Zhang (M'19) was born in Hebei, China. He received the B.S. degree in electrical engineering from Huaqiao University, Xiamen, China, and the M.S. degree in signal and information processing from Xidian University, Xi'an, China, and the Ph.D. degree in signal and information processing from University of Electronic Science and Technology of China, Chengdu, China, in 2011, 2014, and 2019, respectively.

From 2017 to 2019, he was a visiting student with the University of Delaware, Newark, DE, USA. His research interests include array signal processing and wireless communications.

Xiang-Gen Xia (M'97–S'00–F'09) received the B.S. degree in mathematics from Nanjing Normal University, Nanjing, China, and the M.S. degree in mathematics from Nankai University, Tianjin, China, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1983, 1986, and 1992, respectively.

He was a Senior/Research Staff Member with Hughes Research Laboratories, Malibu, California, during 1995–1996. In September 1996, he joined the Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware, where he is the Charles Black Evans Professor. His current research interests include space-time coding, multiple-input multiple-output and orthogonal frequency division multiplexing systems, digital signal processing, and synthetic aperture radar and inverse synthetic aperture radar imaging. He is the author of the book *Modulated Coding for Intersymbol Interference Channels* (New York, Marcel Dekker, 2000).

Dr. Xia was the recipient of the National Science Foundation Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He is currently serving and has served as an Associate Editor for numerous international journals including IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE TRANSACTIONS ON SIGNAL PROCESSING, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He is Technical Program Chair of the Signal Processing Symposium, Globecom 2007 in Washington D.C. and the General Co-Chair of International Conference on Acoustics, Speech and Signal Processing 2005 in Philadelphia.

Zishu He was born in Sichuan, China, in 1962. He received the B.S., M.S. , and Ph.D. degrees in signal and information processing from University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1984, 1988, and 2000, respectively.

He is currently a Professor with the School of Information and Communication Engineering, UESTC in signal and information processing. His current research interests are involved in array signal processing, digital beam forming, the theory on multiple-input multiple-output (MIMO) communication and MIMO radar, adaptive signal processing and interference cancellation.

Xuepan Zhang was born in Hebei, China. He received the B.S. and Ph.D. degrees in electrical engineering from National Laboratory of Radar Signal Processing, Xidian University, Xian, China, in 2010 and 2015, respectively. He is currently working as Principal Investigator with Qian Xuesen Laboratory of Space Technology, Beijing, China. His research interests include synthetic aperture radar, ground moving target indication, and deep learning.