Phased-Array Transmission for Secure Multiuser mmWave Communication via Kronecker Decomposition

Chentao Liang and Xuejing Zhang, *Member, IEEE*

***Abstract*— This paper proposes a multiuser physical layer secure transmission scheme for millimeter-wave communication. We use Kronecker decomposition to design the common transmit vector to synthesize the desired symbols for multiple legitimate receivers in the proposed scheme. Specifically, the algorithm converts the design of common transmit weight for multiuser into the design of sub-weight vectors having the Vandermonde structure. By using Kronecker decomposition, the sub-weight vectors are decomposed into Kronecker factors and designed. To eliminate the message sending towards the undesired directions while guaranteeing the quality of transmission in the target directions, we separate the Kronecker factors into two parts by using the property of the Kronecker product. The first part (the interference cancellation factor) cancels the interference between legitimate users; the second part (the signal enhancement factor) achieves signal enhancement. For a given information symbol, multiple solutions of transmit weight are obtained. By utilizing this time-varying transmit weight, we realize the secure transmission for multiuser. In addition, the proposed algorithm has no restrictions on modulation, and it also has analytical solutions with low computational complexities. Simulations are presented to verify the effectiveness of the algorithm under various situations.**

***Index Terms*— Secure millimeter-wave wireless communication, multiuser communication, phased-array transmission architecture, physical layer security, Kronecker decomposition.**

I. Introduction

MILLIMETER-WAVE (mmWave) wireless communication is regarded as a promising technology for mobile devices [1]–[5]. The small wavelength minimizes the eligible antenna space, making it possible to implement large-scale arrays on both transmitter and receiver sides. Similar to the conventional wireless communication system, communication via the mmWave wireless system may be illegally accessed by eavesdroppers as well. Enhancing the security of mmWave in the physical layer has become an indispensable part of avoiding information leakage [6]–[9].

Over the past several years, a wide range of measures have been developed to enhance security in the physical layer and achieve secure transmission [10]–[14]. The primary approach is to form a deep null towards the direction of unexpected eavesdroppers under the condition that the transmitter acknowledges the precise information of channel state information (CSI) [15]–[17]. However, such an approach might not perform well in practical situations since the eavesdroppers are usually not cooperative. In order to realize secure transmission with unknown eavesdropper channels or CSI partially known, the concept of artificial noise (AN) is proposed in [18], in which artificial noise is imposed on the information-carrying signal to cover the confidential messages up. With AN being added on the orthogonal subspace of the main channel, the eavesdropper channel is degraded, which increases the difficulty for the eavesdropper to acquire valid information efficiently. However, this might lower the effective power and decrease the signal-to-interference-plus-noise ratio (SINR) at the destination [19].

In recent years, the study of secure transmission using the directional modulation (DM) technique has received considerable research interest. In DM, an expected constellation towards the preset direction is produced while scrambling the received constellation at other undesired directions. For instance, the authors of [20] used a phased array at the transmitter to enhance the transmission security by altering the phase excitation at the symbol rate. Note that the phase excitation in [20], [21] is obtained by a genetic algorithm, which is time-consuming, and only approximate solutions can be conducted eventually. The above DM method is mainly discussed under the condition of sub-6 GHz.

Focusing on the millimeter-wave communication system, the author in [22] proposed a low-complexity technology named antenna subset modulation (ASM). In ASM, the direction-dependent data transmission is realized by modulating the array radiation pattern at the radio frequency (RF) domain with symbol rate. More precisely, the antenna subset for transmission from the set of all subsets is randomly selected with the same number of active antennas, resulting in the additional randomness in constellations at angles except the intended one. By modifying the ASM scheme, a new architecture of transmission named switched phase array (SPA)

Manuscript received 10 July 2021; revised 24 October 2021 and 6 January 2022; accepted 10 January 2022. Date of publication 21 January 2022; date of current version 12 August 2022. This work was supported by the National Natural Science Foundation of China under Grant 62101101. The associate editor coordinating the review of this article and approving it for publication was C.-K. Wen. *(Corresponding author: Xuejing Zhang.)*

The authors are with the University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: 610074045@qq.com; xjzhang7@163.com).

This article has supplementary material provided by the authors and color versions of one or more figures available at https://doi.org/10.1109/TWC.2022.3142908.

Digital Object Identifier 10.1109/TWC.2022.3142908

is proposed in [23]. Only one antenna is switched off in SPA to distort the constellation towards the eavesdroppers, resulting in an augmented number of active antennas compared with ASM. Another variant of ASM is proposed in [24]. It develops a novel programmable weight phased-array (PWPA) architecture and the accompanying schemes for secure mmWave wireless communications. The authors of [25] exploit DM with new array systems to achieve secure mmWave wireless communications, where a hybrid multiple-input multiple-output (MIMO) phased-array time-modulated DM for physical layer security is constructed. It should be pointed out that the above secure transmit approaches in [22]- [25] for mmWave communication are only applicable to the single-user case. To our best knowledge, designing a common weight vector for secure multiuser transmission has not been reported.

The drawbacks of the existing work motivate us to develop a secure transmission scheme for multiuser communication. Based on the secure multiuser mmWave communication algorithm we proposed in [26], we refined the procedure of weight vector design. In our work, an algorithm for secure multiuser mmWave communication via Kronecker decomposition is proposed, with the dual-phase shifter [27] applied to achieve the transmission. The dual-phase shifter implies that the signal coupled onto one of the antennas is executed by two phase shifters. It provides a continuous interval constraint instead of constant magnitude comparing with the antenna with a single-phase shifter. In the proposed algorithm, we convert the design of common transmit weight for multiuser into the design of sub-weight vectors. In particular, the common weight vector is split into the sum of sub-weight vectors with the Vandermonde structure [28]. The sub-weight vectors are then decomposed into Kronecker factors via Kronecker decomposition. Using the property of the Kronecker product, the obtained Kronecker factors are separated into two parts to achieve interference cancellation among different legitimate receivers and signal enhancement towards target directions. For a desired information symbol, multiple solutions can be obtained through the proposed secure transmission algorithm. The security is achieved by using the time-varying transmission weight. Our algorithm only requires simple addition and comparison operation, thus having low computational complexity. The main contributions of this paper can be summarized as follows:

1) We propose a weight vector design algorithm for secure multiuser mmWave communication with the assistance of Kronecker decomposition and the properties of the Kronecker product.
2) The presented transmission scheme has no restrictions on modulation, and different users can perform different modulation.
3) This algorithm provides a cost-effective approach with analytical solutions to achieve transmission for multiuser and secures transmission safety, eliminating the messages received by eavesdroppers in undesired directions.

The rest of the paper is organized as follows. In Section II, the system model and problem formulation are introduced and constructed. In Section III, the analytical solution for selecting interference cancellation factors is conducted, and sub-weight vectors are designed based on Kronecker decomposition. The common transmit weight is then synthesized eventually. Representative simulations are presented in Section VI, and conclusions are drawn in Section VII.

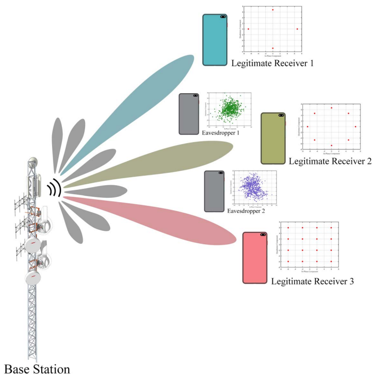


Fig. 1. System model of secure multiuser mmWave communication.

II. System Model and Problem Formulation

A. System Model

We consider a downlink system where the base station is equipped with an N-element phased-array for transmission. As presented in Fig. 1, the base station transmits messages to multiple legitimate receivers, with the existence of several eavesdroppers. Assume that there are K legitimate receivers and E eavesdroppers, and the subscript set for all legitimate receivers is represented as $\mathbb{K} = \{1, 2, \ldots, K\}$. For simplicity, the legitimate receivers and eavesdroppers are all equipped with a single antenna.

At the moment t, the signals received by legitimate receivers and eavesdroppers are given respectively as follows:

$$\begin{aligned} y_k(t) &= \mathbf{h}_k^T \bar{\mathbf{w}}(t) + \eta_k(t), \quad k \in \mathbb{K} \\ y_e(t) &= \mathbf{g}_e^T \bar{\mathbf{w}}(t) + \chi_e(t), \quad e = 1, 2, \ldots, E \end{aligned} \tag{1}$$

where $(\cdot)^T$ denotes the transpose operation, $\mathbf{h}_k \in \mathbb{C}^N$ is the channel vector that reflects the channel state of the k-th legitimate receiver, while $\mathbf{g}_e \in \mathbb{C}^N$ stands for the channel vector of the e-th eavesdropper, η_k and χ_e signify the additive Gaussian noise at the k-th receiver and the e-th eavesdropper respectively. Note that in (1), the weight vector $\bar{\mathbf{w}}(t)$ can be designed to synthesize desired symbols at the legitimate receivers, and it is possible that different receivers have different modulations.

We consider an extended Saleh-Valenzuela geometric model [30] with a single-path channel. Specifically, the channel vector can be simplified to

$$\mathbf{h}_k = \mathbf{a}(\gamma_k) \tag{2}$$

where γ_k is the angle of departure (AoD) of the single path to the k-th receiver, and $\mathbf{a}(\gamma_k) \in \mathbb{C}^N$ denotes the antenna array response vector [31], which is formulated as

$$\mathbf{a}(\gamma_k) = [1, e^{\mathrm{j}2\pi d \cdot \sin(\gamma_k)/\lambda}, \ldots, e^{\mathrm{j}2\pi (N-1) d \cdot \sin(\gamma_k)/\lambda}]^T \tag{3}$$

where $\mathrm{j} \triangleq \sqrt{-1}$, d denotes the distance between sensors of the uniform linear array and λ denotes the wavelength. It is

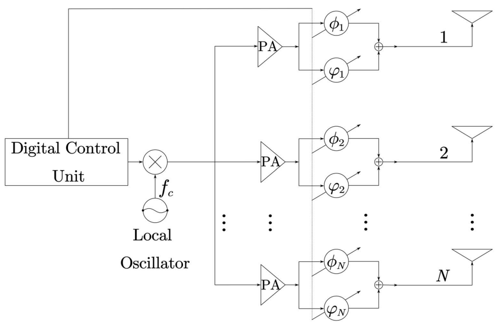


Fig. 2. Phased-array transmission structure with dual-phase shifters.

the same situation for channel state of eavesdroppers, which is given by

$$\mathbf{g}_e = \mathbf{a}(\gamma_{l,e}) \tag{4}$$

The phased-array transmission structure is considered in the proposed algorithm. For the transmitter side, an analog-only transmitter architecture shown in Fig. 2 is applied. The whole process is completed in the RF domain, where the output is equally divided into two signals and driven to the corresponding phase shifter, respectively. The structure[1] of the dual-phase shifter allows the moduli to change in a continuous interval instead of constant magnitudes imposed by a single-phase shifter, greatly improving the structure's flexibility in weight vector design. After that, the signals processed by two phase shifters are combined and go through the power amplifier (PA) before being coupled onto the antenna.

For the demodulation on the receiver side, the single antenna reads an instantaneous magnitude and phase provided that the power of the received signal at the single-antenna receiver is higher than that of the noise [29]. In terms of demodulation, the received magnitude and phase information corresponding to different modulation such as QPSK, 8PSK, and 16QAM is stored, and the transmitted information is then demodulated based on the in-phase and quadrature constellation at each instant.

B. Problem Formulation

In the previous subsection, the transmission structure is illustrated. It should be emphasized again that the two parallel-connected phase shifters in Fig. 2 allow to design complex signals that lie inside the complex disk enclosed by the circle with radius one. This improves the flexibility compared with the architecture with a single-phase shifter. Under such circumstances, the final designed weight vector should follow[2]:

$$||\bar{\mathbf{w}}(t)||_\infty \leq 1 \tag{5}$$

where $||\cdot||_\infty$ denotes infinite norm. It implies the maximum modulus of the elements in $\bar{\mathbf{w}}(t)$ are no greater than 1. To transmit messages, the final designed common weight vector is also supposed to satisfy

$$\mathbf{h}_k^T \bar{\mathbf{w}}(t) = \alpha_k, \;\; k \in \mathbb{K} \tag{6}$$

where α_k is the desired symbol drawn from the constellation graph of the k-th legitimate receiver.

To avoid information leakage, the transmit weight vector $\bar{\mathbf{w}}(t)$ should be time-varying even if the transmitted message remains the same. Otherwise, the eavesdroppers may have chances to decode the information.

III. The Design of Transmit Weight Vector via Kronecker Decomposition

To satisfy the constraints (5) and (6), we next present an algorithm of weight vector design with the aid of Kronecker decomposition. For the sake of simplicity, we assume that the number of antenna satisfies $N = 2^M$, where M is a positive integer. [3]

A. Convert the Design of Transmit Weight to the Design of Sub-Weight Vectors

Before designing the desired weight vector that satisfies (5) and (6), we first introduce a new vector $\check{\mathbf{w}}(t)$, which follows the structure

$$\check{\mathbf{w}}(t) = \sum_{q=1}^{K} \mathbf{w}_q(t) \tag{7}$$

In (7), $\mathbf{w}_q(t) \in \mathbb{C}^N$ is the transmitted sub-weight vector for the q-th legitimate receiver. $\mathbf{w}_q$ should satisfies

$$\mathbf{h}_k^T \mathbf{w}_q = 0, \quad k \neq q \tag{8a}$$
$$\mathbf{h}_k^T \mathbf{w}_q = K \cdot \alpha_k, \quad k = q \tag{8b}$$
$$||\mathbf{w}_q||_\infty \leq 1 \tag{8c}$$

where k, $q \in \mathbb{K}$. Based on (7) and (8c), it is not difficult to find out that the result of the element value in the sum of sub-weight vectors over K is less than 1, that is

$$||\check{\mathbf{w}}(t)||_\infty \cdot \frac{1}{K} \leq 1 \tag{9}$$

which qualifies for (5). Thus, we can design the final weight vector by designing the sub-weight vectors, that is

$$\bar{\mathbf{w}}(t) = \check{\mathbf{w}}(t) \cdot \frac{1}{K} = \frac{1}{K} \sum_{q=1}^{K} \mathbf{w}_q(t) \tag{10}$$

which satisfies condition (6).

From the above description, it can be found that the design of the common weight vector $\bar{\mathbf{w}}(t)$ can be converted to the design of the vectors $\mathbf{w}_q(t)$ satisfying both interference cancellation among different legitimate receivers and signal enhancement at transmitting angles concurrently. The cancellation and enhancement are equivalent to satisfy the condition (8), where (8a) is used to eliminate the messages

[1] Note that the PAs are situated before the dual-phase shifters. This arrangement aims to ensure the stability of voltage that goes into the PAs to keep the operating range within the saturated nonlinear region.

[2] In a practical situation, the output power will be no greater than the input power when passive components are used. To reflect this fact, we scale each point to 1/2 after splitting. As a result, the maximum modulus of elements in each common transmit weight $\bar{\mathbf{w}}(t)$ should be one.

[3] The presented algorithm is also applicable in the generic case, where the number of antenna N is an arbitrary-positive number, as to be discussed in detail at the end of this section.

sending in the undesired directions, canceling the interference for different users. In contrast, (8b) is aimed to strengthen the signal transmitted towards target directions. Next, we will introduce a method for designing vectors $\mathbf{w}_q(t)$ based on Kronecker decomposition.

B. Kronecker Decomposition of Channel Vectors and Sub-Weight Vectors

To preceding, an important lemma concerning the Kronecker decomposition is first introduced. The time variable t is omitted for convenience in the following content.

Lemma 1 (Kronecker Decomposition [28]): Let $\tilde{\mathbf{b}}$ *be a* $\tilde{N} \times 1$ *vector with uni-modulus elements having the following Vandermonde structure*:

$$\tilde{\mathbf{b}} = [1, e^{\mathrm{j}\Theta}, e^{\mathrm{j}2\Theta}, \ldots, e^{\mathrm{j}(\tilde{N}-1)\Theta}]^T \tag{11}$$

with Θ *fixed. Given* $\tilde{N} = n_1 n_2 \ldots n_M$ *with* $\{n_m\}_{m=1}^{M}$ *being positive integers, the vector* $\tilde{\mathbf{b}}$ *can be decomposed as*

$$\tilde{\mathbf{b}} = \mathbf{b}^{(M)} \otimes \mathbf{b}^{(M-1)} \otimes \ldots \otimes \mathbf{b}^{(1)} \tag{12}$$

where $\otimes$ *represents the Kronecker product and the* m*-th factor having the length of* n_m *is given by* $\mathbf{b}^{(m)} = [1, e^{jn_{m-1}\ldots n_1 n_0 \Theta}, e^{j2n_{m-1}\ldots n_1 n_0 \Theta} \ldots, e^{\mathrm{j}(n_m-1)n_{m-1}\ldots n_1 n_0 \Theta}]^T$ *with* $n_0 = 1$.

Note when $n_m = 2$, $\mathbf{b}^{(m)}$ in *Lemma 1* is simplified to

$$\mathbf{b}^{(m)} = [1, e^{\mathrm{j}2^{m-1}\Theta}]^T \tag{13}$$

Recalling the channel vector $\mathbf{h}_k$ in (2) and (3), we can check that $\mathbf{h}_k$ follows the Vandermonde structure as described in *Lemma 1*. Thus, the channel vector of the k-th legitimate receiver can be decomposed as follows

$$\mathbf{h}_k = \mathbf{u}_k^{(M)} \otimes \mathbf{u}_k^{(M-1)} \otimes \ldots \otimes \mathbf{u}_k^{(m)} \otimes \ldots \otimes \mathbf{u}_k^{(1)} \tag{14}$$

where $\mathbf{u}_k^{(m)} \in \mathbb{C}^2$ is given by

$$\mathbf{u}_k^{(m)} = [1, e^{\mathrm{j}2^{m-1}\Theta_k}]^T \tag{15}$$

where Θ_k is expressed as $\Theta_k = 2\pi d \cdot \sin(\gamma_k)/\lambda$.

As afore-mentioned in Section III.A, $\mathbf{w}_q$ must meet (8a) for interference cancellation and (8b) for signal enhancement. In order to satisfy these requirements and for the simplicity of the algorithm, the sub-weight vectors $\mathbf{w}_q$ is assumed to have the Vandermonde structure. Thus, the weight vector $\mathbf{w}_q$ is decomposed as

$$\mathbf{w}_q = \mathbf{v}_q^{(M)} \otimes \mathbf{v}_q^{(M-1)} \otimes \ldots \otimes \mathbf{v}_q^{(m)} \otimes \ldots \otimes \mathbf{v}_q^{(1)} \tag{16}$$

where $\mathbf{v}_q^{(m)}$ is the m-th Kronecker factor for the weight vector of the q-th legitimate user, $m = 1, \ldots, M, q = 1, \ldots, K$. Under this structure, the design of weight vectors $\mathbf{w}_q$ for every legitimate user can be transformed into the design of Kronecker factors $\mathbf{v}_q^{(m)}$ as presented next.

C. Design Weight Vectors by Using Properties of Kronecker Product

In the previous subsection, we decompose the channel and weight vectors by using Kronecker decomposition. Based on (14) and (16), for the given subscripts $k, q \in \mathbb{K}$, we can express $\mathbf{h}_k^T \mathbf{w}_q$ as

$$\begin{aligned} \mathbf{h}_k^T \mathbf{w}_q &= (\mathbf{u}_k^{(M)T} \otimes \ldots \otimes \mathbf{u}_k^{(1)T})(\mathbf{v}_q^{(M)} \otimes \ldots \otimes \mathbf{v}_q^{(1)}) \\ &= \prod_{m=M}^{1} \mathbf{u}_k^{(m)T} \mathbf{v}_q^{(m)} \end{aligned} \tag{17}$$

where we have utilized the property of the Kronecker product. Observing formula (17), we can find out that for a given subscript k, an arbitrary $\mathbf{v}_q^{(m)}$ needs to be designed to make $\mathbf{h}_k^T \mathbf{w}_q$ equals 0 to satisfy the constraint (8a) for interference cancellation. Note that for different subscript k, the superscript m in $\mathbf{v}_q^{(m)}$ is not repeatable, since for every given k and m, an $\mathbf{u}_k^{(m)T}$ can only be used once to cancel the interference of the q-th user over the k-th channel. Similarly, to satisfy signal enhancement constraint (8b), we need to design the rest of $\mathbf{v}_q^{(m)}$ to make $\mathbf{h}_k^T \mathbf{w}_q = K \cdot \alpha$.

For ease of expression, we name the selected Kronecker factors that satisfy constraint (8a) as interference cancellation factors, denoting their subscript set as $\mathbb{B}_1^{(q)}$, while the rest of the Kronecker factors that are used to satisfy (8b) are named as signal enhancement factors, whose subscript set are denoted as $\mathbb{B}_2^{(q)}$ for the q-th legitimate user, respectively. All subscripts of Kronecker factors are represented as $\mathbb{A} = \{1, 2 \ldots, M\}$, where $\mathbb{B}_1^{(q)} \cup \mathbb{B}_2^{(q)} = \mathbb{A}$. Thus, the design procedure is divided into two parts: 1) the design of interference cancellation factors and 2) the design of signal enhancement factors of the sub-weight vector for every legitimate receiver.

1) The Design of Interference Cancellation Factors: The expected vector elements in weight vector set $\check{\mathbf{w}} = [\mathbf{w}_1 + \ldots + \mathbf{w}_K]$ are supposed to satisfy constraint (8a). With the equation (17), the constraint (8a) for one of the sub-weight vectors $\mathbf{w}_q$ is equivalent to equation (18)

$$(\mathbf{u}_k^{(M)T} \mathbf{v}_q^{(M)}) \ldots (\mathbf{u}_k^{(m)T} \mathbf{v}_q^{(m)}) \ldots (\mathbf{u}_k^{(1)T} \mathbf{v}_q^{(1)}) = 0 \tag{18}$$

where $q \in \mathbb{K},\ k = 1, 2, \ldots, K,\ q \neq k$.

Equation (18) implies that for every sub-weight vector $\mathbf{w}_q,\ q \in \mathbb{K}$, it has to attenuate the product result with any other $K-1$ channel vectors $\mathbf{h}_k,\ k \neq q$ to be zero so that the unexpected receivers are not able to receive the transmitted massage. In (18), for each subscript k, it requires only one Kronecker product factor $\mathbf{u}_k^{(m)T} \mathbf{v}_q^{(m)}, k \neq q$ to be selected in order to make the k-th equation equals zero. The process of selecting Kronecker product factor from (18) is equivalent to choose Kronecker factor in equation (16). The selected Kronecker factor (interference cancellation factor) is mapped to the corresponding Kronecker product factor in every k-th equation in (18) for each $q \in \mathbb{K}$. Denoting the subscript of selected interference cancellation factors as $\hat{m}_j$, where $j = 1, \ldots, K-1$, the chosen Kronecker product factors based on the selecting rule to be elaborated in the following content in every k-th equation for each $q \in \mathbb{K}$ can form a new function set

$$\mathbf{u}_k^{(\hat{m}_j)T}\mathbf{v}_q^{(\hat{m}_j)} = 0 \tag{19}$$

where $\hat{m}_j \in \mathbb{B}_1^q,\ q = 1, \ldots, K$. Recall that $\mathbf{w}_k$ has the Vandermonde structure, the specific form of every $\mathbf{v}_k^{(m)}$ with dimension of 2×1 is

$$\mathbf{v}_k^{(m)} = [e^{\mathrm{j}\psi_{k,1}^{(m)}}, e^{\mathrm{j}\psi_{k,2}^{(m)}}]^T \tag{20}$$

By substituting (15) and (20) into (19), a function set for an $\mathbf{v}_q^{(\hat{m}_j)}$ with unknown phase variable is obtained as

$$e^{\mathrm{j}\psi_{q,1}^{(\hat{m}_j)}} + e^{\mathrm{j}(2^{\hat{m}_j-1}\Theta_k + \psi_{q,2}^{(\hat{m}_j)})} = 0 \tag{21}$$

The phase solutions to (21) are

$$\psi_{q,2,*}^{(\hat{m}_j)} = 0 \tag{22}$$

$$\psi_{q,1,*}^{(\hat{m}_j)} = \left(\pi + \angle(e^{\mathrm{j}2^{\hat{m}_j-1}\Theta_k})\right)_{2\pi} \tag{23}$$

where $\angle(\cdot)$ returns the phase of $(\cdot)$, and $(\cdot)_{2\pi}$ calculates the remainder after division of input by 2π.

Note that not arbitrarily chosen $\hat{m}_j$ can make equation (8b) obtain the final $K \cdot \alpha_k$. Once the interference cancellation factors are determined, they need to be shifted to the right side of the equation (8b) in order to design the signal enhancement factors further. Equation (24) illustrates the situation.

$$\prod_{i=1}^{M-K+1}(\mathbf{u}_k^{(m_i)T}\mathbf{v}_q^{(m_i)}) = \frac{K\alpha_k}{\prod_{j=1}^{K-1}(\mathbf{u}_k^{(\hat{m}_j)T}\mathbf{v}_q^{(\hat{m}_j)})} \triangleq \beta_k \tag{24}$$

One can observe from (24) that the determined interference cancellation factors become the denominator of the gain. If the product result of the selected interference cancellation factors is tiny, the $|\beta_k|$ will become a large number, leading to an insufficient number of signal enhancement factors to solve the equation. Therefore, a selection is needed to obtain a suitable set of $\hat{m}_j$ for every $q \in \mathbb{K}$.

Recall (15) and (20), and bring the obtained result (22) and (23) into $\mathbf{u}_q^{(m)T}$ and $\mathbf{v}_k^{(m)}$, we can derive the Kronecker factors of $\mathbf{h}_q^T\mathbf{w}_k$ when $k = q$

$$\mathbf{u}_k^{(\hat{m}_j)T}\mathbf{v}_q^{(\hat{m}_j)} = 1 - e^{\mathrm{j}\triangle} \tag{25}$$

where the $\triangle$ can be written as

$$\triangle = 2^{\hat{m}_j-1}(\Theta_q^{(\hat{m}_j)} - \Theta_k^{(\hat{m}_j)}),\ q \neq k \tag{26}$$

Equation (25) implies the expression of the selected interference cancellation factors.

In order to enlarge the possibility of solution for the signal enhancement factors, the result of $|1 - e^{\mathrm{j}\triangle}|$ in (25) should makes β_k in (24) within interval $|\beta_k| \leq 2^{M-K-1}$ when $n_m = 2$, since it is easy to find out that the range of the signal enhancement factors $\mathbf{u}_k^{(m_i)T}\mathbf{v}_q^{(m_i)}$ on the left side of equation (24) are at most $[0, 2]$, if the gain for signal enhancement factors is too large, there may be not sufficient number of signal enhancement factors to compensate the equation when designing signal enhancement part, resulting in absence of $K \cdot \alpha_k$ no matter how to design the Kronecker factor $\mathbf{v}_k^{(m)}$. This is equivalent to find the most appropriate subscript $\hat{m}_j$ to obtain the suitable $\triangle$.

Algorithm 1 Design of Interference Cancellation Factors

```
Input: $N$, $K$, $\{\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_K\}$
Output: The Interference Cancellation Factors $\mathbf{v}_q^{(\hat{m}_j)}$
$N = 2^M$
for $k = 1, \ldots, K$ do
    $\mathbf{h}_k^T = \mathbf{u}_k^{(M)} \otimes \mathbf{u}_k^{(M-1)} \otimes \ldots \otimes \mathbf{u}_k^{(1)}$
end
for $k = 1, \ldots, K$ do
    for $q = 1, \ldots, K,\ q \neq k$ do
        for $m = 1, \ldots, M$ do
            $\Delta_{q,k}^{(m)} = \pi - \left(|2^{m-1}(\Theta_q^{(m)} - \Theta_k^{(m)})|\right)_\pi$
        end
    end
    Randomly select $K - 1$ $\hat{m}_j$ from every $\Delta_{q,k}^{(m)}$ that
    makes $\beta_k$ satisfy $|\beta_k| \leq 2^{M-K-1}$, with each row $k$
    pick only one term.
end
for $q = 1, \ldots, K$ do
    for $\hat{m}_j \in \mathbb{B}_1^{(q)},\ j = 1, \ldots, K-1$ do
        $\psi_{q,2,*}^{(\hat{m}_j)} = 0$
        $\psi_{q,1,*}^{(\hat{m}_j)} = \left(\pi + \angle(e^{\mathrm{j}2^{\hat{m}_j-1}\Theta_p})\right)_{2\pi}$
        $\mathbf{v}_q^{(\hat{m}_j)} = [e^{\mathrm{j}\psi_{q,1,*}^{(\hat{m}_j)}}, e^{\mathrm{j}\psi_{q,2,*}^{(\hat{m}_j)}}]^T$
    end
end
```

The selection of interference cancellation factors provides randomness to the determination of the weight vector. Each transmission allows more than one combination of interference cancellation factors selected to eliminate the message transmitted at undesired angles. The specific procedure to select and design the interference cancellation factors is presented in Algorithm 1.

2) The Design of Signal Enhancement Factors: Having designed the $K - 1$ interference cancellation factors in every $\mathbf{w}_q, q = 1, \ldots, K$ under the constraint (8a), there are still $M - (K - 1)$ signal enhancement factors. In other words, $M - (K - 1)$ Kronecker product factors in every $\mathbf{h}_k^T\mathbf{w}_q$, $k = q$ and $k, q \in \mathbb{K}$ need to be designed to achieve the purpose of signal enhancement, and their determination must satisfy condition (8b).

By moving the designed interference cancellation factors to the right side, the equivalent expression of constraint (8b) is obtained as (24), where $m_i \in \mathbb{B}_2^{(q)}$, $i = 1, \ldots, M - K + 1$. Denoting the subscript of any one of the signal enhancement factors as $\tilde{m}$, according to (15) and (20), we know the module of the $\tilde{m}$-th signal enhancement factors is no larger than 2, that is,

$$\mathbf{u}_k^{(\tilde{m})T}\mathbf{v}_q^{(\tilde{m})} = \varepsilon_{\tilde{m}},\ |\varepsilon_{\tilde{m}}| \in (0, 2] \tag{27}$$

In (24), by shifting this $\tilde{m}$ signal enhancement factor to the right side, denoting the subscript of the rest of the signal enhancement factors as $\check{m}_i$, where i becomes

Algorithm 2 The Design of Signal Enhancement Factors

```
Input: $N$, $K$, $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_K\}$, $\{\mathbf{v}_q^{(\hat{m}_j)}\}$, $\alpha_k$
Output: The Signal Enhancement Factors $\mathbf{v}_q^{(m_i)}$
for $k = 1, \dots, K$ do
    $\beta_k = \frac{K\alpha_k}{\prod_{j=1}^{K-1}(\mathbf{u}_k^{(\hat{m}_j)T}\mathbf{v}_q^{(\hat{m}_j)})}$
    for $i = 1, \dots, M-K$ do
        Randomly select a $\varepsilon_{\check{m}_i} \in [\sqrt[M-K]{|\beta_k|/2}, 2]$
    end
    Select a $\varepsilon_{\tilde{m}}$ where $|\varepsilon_{\tilde{m}}| \in [0, 2]$ to compensate the
    equation
    for $q = 1 : K$ do
        for $m_i \in \mathbb{B}_2^{(q)}$, $i = M-K+1$ do
            $\psi_{q,1,*}^{(m_i)} = \angle\varepsilon_{m_i} + \arccos(|\varepsilon_{m_i}|/2)$
            $\psi_{q,2,*}^{(m_i)} = \angle\varepsilon_{m_i} - \arccos(|\varepsilon_{m_i}|/2) - 2^{m_i-1}\Theta_k$
            $\mathbf{v}_q^{(m_i)} = [e^{\mathrm{j}\psi_{q,1,*}^{(m_i)}}, e^{\mathrm{j}\psi_{q,2,*}^{(m_i)}}]^T$
        end
    end
end
```

$i = 1, \dots, M-K$ we can get

$$\prod_{i=1}^{M-K}(\mathbf{u}_k^{(\check{m}_i)T}\mathbf{v}_q^{(\check{m}_i)}) = |\frac{\beta_k}{\mathbf{u}_k^{(\tilde{m})}\mathbf{v}_q^{(\tilde{m})}}| \geq \frac{\beta_k}{2} \tag{28}$$

Since the rest of the signal enhancement factors on the left side are conform with each other, their boundary can be regarded as the same. Thus, a more tight range for the rest of the signal enhancement factors is acquired, which is given as

$$\mathbf{u}_k^{(\check{m}_i)T}\mathbf{v}_q^{(\check{m}_i)} = \varepsilon_{\check{m}_i} \in [\sqrt[M-K]{|\beta_k|/2}, 2] \tag{29}$$

The signal enhancement factors are able to be determined based on the boundary of (27) and (29). The determination of signal enhancement factors $\mathbf{v}_q^{(m)}$, $m \in \mathbb{B}_2^{(q)}$ of a sub-weight vector resembles the process of solving interference cancellation factors, only with infinite solutions instead, i.e., solving equation (30) to obtain the phase of each signal enhancement factor.

$$e^{\mathrm{j}\psi_{q,1}^{(m)}} + e^{\mathrm{j}(2^{m-1}\Theta_k + \psi_{q,2}^{(m)})} = \varepsilon_m \tag{30}$$

where $m \in \mathbb{B}_2^{(q)}$. Denote the randomly chosen phase as $\psi_{q,2,*}^{(m)} \in [-\pi/2,\ \pi/2]$, the phase of the first term in (30) can be obtained by law of cosines, which is conducted as

$$\psi_{q,1,*}^{(m)} = \angle\varepsilon_m + \arccos(|\varepsilon_m|/2) \tag{31}$$

$$\psi_{q,2,*}^{(m)} = \angle\varepsilon_m - \arccos(|\varepsilon_m|/2) - 2^{m-1}\Theta_k \tag{32}$$

The determination of signal enhancement factors also contributes to the multiple solutions of the weight vector. Since the subscript $\tilde{m}$ and $\varepsilon_{\check{m}_i}$ are randomly selected from set $\mathbb{B}_2^{(q)}$ and $[\sqrt[M-K]{|\beta_k|/2}, 2]$, which increases the uncertainty of the final results. A specific elucidation is given in Algorithm 2.

After the two above steps, we can determine the value of each freely-product term $\mathbf{u}_k^{(m)T}\mathbf{v}_q^{(m)}$. Having acquired both interference cancellation factors and signal enhancement factors of sub-weight vectors, the sub-weight vector of the q-th legitimate user is obtained by using Kronecker product, the specific equation is given in (16). Algorithm 3 gives the procedure for designing weight vectors.

Algorithm 3 Using Kronecker Decomposition to Design Weight Vectors $\mathbf{w}_{k_2}$

```
Input: $N$, $K$, $\{\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_K\}$, $\alpha_k$
Output: The proposed common weight vector $\bar{\mathbf{w}}$
Apply algorithm 1 to select and design interference
cancellation factors
Apply algorithm 2 to design signal enhancement factors
$\mathbf{w}_k = \mathbf{v}_k^{(M)} \otimes \mathbf{v}_k^{(M-1)} \dots \otimes \mathbf{v}_k^{(1)}$
$\bar{\mathbf{w}} = \frac{\sum_{k=1}^{K}\mathbf{w}_k}{K}$
```

Remark 1: The design of the weight vector for the general condition when the number of antennae $N = 2^n$ is no longer necessary follows the same procedure as what we reveal in this section. After the Kronecker decomposition of $\mathbf{h}_k$ and $\mathbf{w}_k$, the Kronecker factors with dimension of $n_m \times 1$ can be written as equation (33) and (34) respectively.

$$\mathbf{u}_k^{(m)} = \begin{bmatrix} 1 \\ e^{jn_{m-1}\dots n_1 n_0 \Theta_k} \\ e^{j2n_{m-1}\dots n_1 n_0 \Theta_k} \\ \vdots \\ e^{\mathrm{j}(n_m-1)n_{m-1}\dots n_1 n_0 \Theta_k} \end{bmatrix} \tag{33}$$

$$\mathbf{v}_k^{(m)} = [e^{\mathrm{j}\psi_{k,1}^{(m)}}, e^{\mathrm{j}\psi_{k,2}^{(m)}}, \dots, e^{\mathrm{j}\psi_{k,n_m}^{(m)}}]^T \tag{34}$$

The ensuing interference cancellation factor selecting process is analogous to the procedure we mentioned above with multiple optimal solutions instead of one choice. The phase of every Kronecker factor of the sub-weight vector can be obtained following the same train of thought mentioned in the content above.

D. Computation Complexity

Following the reference [28], we now analyze the computation complexity of the proposed algorithm. The proposed secure multiuser mmWave algorithm based on Kronecker decomposition and property of Kronecker product is characterized by its low computational complexity. The main parts of the proposed algorithm lie in the design of the interference cancellation factor and the solution of the signal enhancement factor. In the interference cancellation part, the main computations attribute to the calculation of $\Delta_{q,k}^{(m)}$ and the calculation of the phase solution $\psi_{q,1,*}^{(\hat{m}_j)}$ of the selected interference factors. Recall that they are illustrated in (26), (22) and (23). The computational complexity is $\mathcal{O}(K)$. In the signal enhancement part, the calculations are mainly derived from solving for the phase of the signal enhancement factor mentioned in (31) and (32). These two manipulations have computational complexity $\mathcal{O}(K)$. As a consequence, the computational complexity of the proposed algorithm is $\mathcal{O}(K)$.

IV. The Proposed Security Algorithm

In the previous section, we introduced the specific procedures to design the common weight vector towards desired transmit directions. The proposed algorithm is suitable for secure multiuser transmission in different modulation situations such as PSK and QAM. It can be seen that the common weight vector described in the proposed algorithm is designed for the channel vector of legitimate receivers, which are not applicable to other channels such as eavesdroppers' channels since the selection of interference cancellation factors and the determination of signal enhancement factors provides the randomness to the designed weight vectors. When partial Kronecker products are selected as interference cancellation factors to design the weight vector that satisfies (8a) for the interference cancellation, the selection judgment only needs to make β_k satisfy $|\beta_k| \leq 2^{M-K-1}$. Hence for a given subscript k, we can arbitrarily select a m-th Kronecker factor from different q to construct $\mathbf{u}_k^{(m)T}\mathbf{v}_q^{(m)}$ every time. The selection adds randomness to the design of the weight vector.

When designing the signal enhancement factors, we first need to randomly select one signal enhancement factor as $\mathbf{u}_k^{(\tilde{m})T}\mathbf{v}_q^{(\tilde{m})}$ to compensate the equation. On the basis of this selection, we also need to choose arbitrary values for the remaining signal enhancement factor, as long as their range is within the interval $[\sqrt[M-K]{|\beta_k|/2}, 2]$. This second value choice further improves the randomness of the proposed algorithm in the design of common transmit weight. Multiple different solutions can eventually be generated at different times in the final result. Based on this principle, we can impose different common weight vectors at every single transmit time scale to send valid symbols by arbitrarily selecting a transmit weight from its multiple solutions for a certain legitimate receiver. The results produced are different with various weight vectors transmitted at undesired directions, and the symbols the eavesdroppers receive may be scrambled if the applied weight vectors $\bar{\mathbf{w}}$ vary over time. In such a manner, the physical layer security is eventually enhanced at the legitimate receivers' side. The overall process for implementing the algorithm for secure transmission is first to specify the number of antennas N, the total time point T, the number of users K, and then call Algorithm 3 at each time point to calculate the transmit weight vector for transmission.

V. Performance Analysis

In this section, we evaluate the performances of the proposed secure multiuser mmWave transmission algorithm with the parameters of signal-to-noise ratio (SNR), symbol error rate (SER) and secrecy capacity (SC). We assume that the transmitted signal is Quadrature Phase Shift Keying (QPSK).

A. Average Signal-to-Noise Ratio

The instantaneous SNR of the proposed architecture at direction θ is a random variable, depending on the random set of interference cancellation factors $\mathbb{B}_1^{(q)}$. We denote the randomized transmit weight vector set generated from the random set $\mathbb{B}_1^{(q)}$ in time T as $\mathcal{W}$. Therefore

$$\mathrm{SNR}(\theta, t) = \left|\frac{\mathbf{h}_k^T(\theta)\bar{\mathbf{w}}(t)}{N_0}\right|^2 \tag{35}$$

The average SNR is expressed as

$$\mathrm{SNR}(\theta) = \frac{1}{|\mathcal{W}|}\sum_{\bar{\mathbf{w}}(i)\in\mathcal{W}}\left|\frac{\mathbf{h}_k^T(\theta)\bar{\mathbf{w}}(i)}{N_0}\right|^2 \tag{36}$$

B. Average Symbol Error Rate

The exact symbol error probability of the QPSK modulation given in [23] can be expressed as

$$P_{QPSK} = \mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR}(\theta)}{2}}\right) - \frac{1}{4}\mathrm{erfc}^2\left(\sqrt{\frac{\mathrm{SNR}(\theta)}{2}}\right) \tag{37}$$

where erfc denotes the complementary error function defined as

$$\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}\mathrm{d}t \tag{38}$$

C. Secrecy Capacity

The secrecy capacity of a channel can be defined as the maximum bit rate that a legitimate receiver can recover reliably and securely [33]. The outage probability, defined as the probability of failing to achieve the instantaneous secrecy capacity C_k is given by

$$\mathrm{Pr}_{\mathrm{out}}(R_s) = \mathrm{Pr}\{C_k(\mathrm{SNR}(\theta_K), \mathrm{SNR}(\theta_e)) < R_s\} \tag{39}$$

where $\mathrm{SNR}(\theta_K)$, $\mathrm{SNR}(\theta_e)$ denote the average SNR of the k-th legitimate receiver and the eavesdroppers, and R_s is the minimum required secrecy capacity for a desired service. The instantaneous secrecy capacity C_k is expressed as

$$C_k(\mathrm{SNR}(\theta_K), \mathrm{SNR}(\theta_e)) = \left[\log_2\left(\frac{1+\mathrm{SNR}(\theta_K)}{1+\mathrm{SNR}(\theta_e)}\right)\right]^+ \tag{40}$$

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

VI. Simulation Results

In this section, simulation results are given to demonstrate the effectiveness of the proposed algorithm in securing transmission. A ULA with single-path mmWave channel that is mentioned in (2) and (4) are considered. Unless otherwise specified, the number of legitimate receivers is set to be $K = 3$, whose gain for transmitting signals $|\alpha_k|$ are 20.33, 18.83 and 19.92, and the element number is 512, with the transmit angle for three legitimate receivers located at $-50°, -5°$, and $80°$, eavesdroppers at $35°$ and $-15°$ respectively.

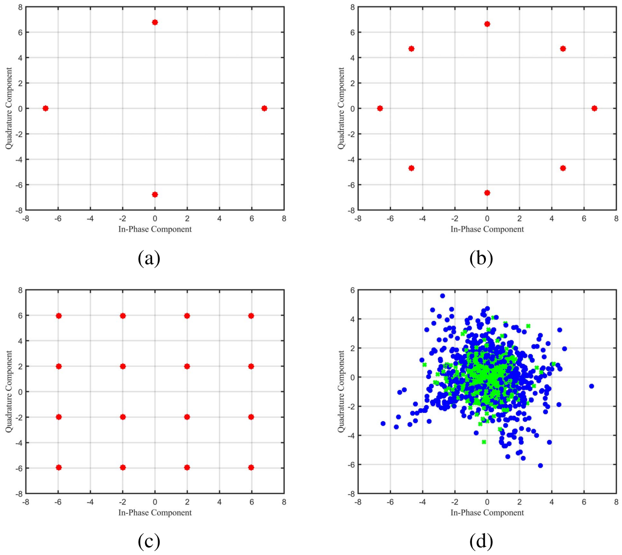


Fig. 3. Noiseless received constellations results at each legitimate receiver using the proposed algorithm (the red points denote the constellation at legitimate receiver, the blue and green represent the synthesized constellation at eavesdroppers, respectively). (a) The constellation of the first legitimate receiver based on QPSK; (b) The constellation of the second legitimate receiver based on 8PSK; (c) The constellation of the third legitimate receiver based on 16-QAM; (d) The constellation of the two eavesdroppers.

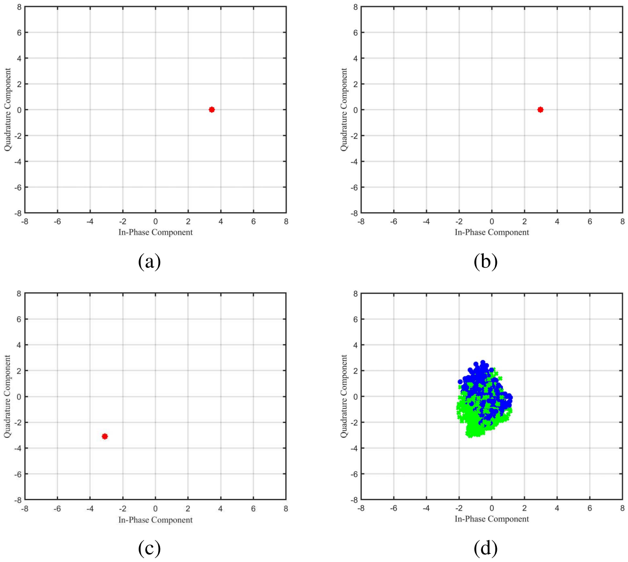


Fig. 4. Noiseless received constellations results at each legitimate receiver using the proposed algorithm with same transmit symbol at different time scale. (the red points denote the constellation at legitimate receiver, the blue and green represent the synthesized constellation at eavesdroppers, respectively). (a) The constellation of the first legitimate receiver based on QPSK; (b) The constellation of the second legitimate receiver based on 8PSK; (c) The constellation of the third legitimate receiver based on 16-QAM; (d) The constellation of the two eavesdroppers.

A. Constellation Synthesis Results

In this subsection, we present the constellation synthesis results of the proposed algorithms to illustrate the received messages at the legitimate receivers and eavesdroppers. According to reference in [32], the BS can serve each signal user with a separate modulation. Thus, three different modulation types are imposed on corresponding legal receivers to illustrate the proposed algorithm's applicability (QPSK, 8PSK, and 16QAM, respectively). The total time scale is set to 800 in the following simulation.

1) Constellation Synthesis With Different Transmit Message: First, to demonstrate the reception at the legitimate receivers and the eavesdroppers and verify the security of the proposed transmission algorithm in the general case, the constellation synthesis is implemented. The transmit symbols for three legitimate receivers vary over time. In the procedure of this algorithm, the channel vectors are obtained and transmitted for all three legitimate users. Fig. 3 illustrates the noiseless received constellations results for all three legal users and two eavesdroppers, respectively. It can be observed from Fig. 3 that the corresponding constellation synthesized at each legitimate user and the result is undistorted, while two eavesdroppers are randomized with no evident pattern. This conclusion applies to all of the three modulations.

2) Constellation Synthesis With Same Transmit Message: In order to further illustrate the security of the proposed algorithm, verifying that the weight vector designed by the proposed algorithm with the same transmission symbol still holds multiple solutions, a scenario that the transmitter transmits the same symbol for each of the legitimate receivers is inspected at every time scale. To facilitate the presentation of data, we sightly reduce the gain and set the number of antennas to be 128. Three legitimate receivers are positioned at $-87°$, $10°$, $74°$, respectively. The eavesdroppers are situated at $-21°$, $-25°$.

Fig. 4 shows the constellation diagram. By observing it, one can find that the three legitimate receivers continuously receive the same transmission symbols during the 800-time interval, respectively, with a smaller modulus than constellation synthesis in Fig. 3. The constellation points of two eavesdroppers in their synthesis figure distribute around the zero point. This is because, for the same transmission symbol, we have multiple alternatives to the weight vector. The specific statistics of the common weight vectors at different time scales are presented from Table I to Table VI in Parameters of Weight Vectors at Different Time Scales (see supplementary for details), where one can see that the transmit weights are different in different time scales for the same transmitted symbol.

B. Performance Investigation With BER

In this subsection, we exam the performance of the algorithm with respect to distinct BER. To demonstrate the variation of the BER versus SNR by using the proposed algorithm, in addition to the theoretical analysis illustrated in the last section, we added the curves of BER for phase-shift keying modulation calculated by a nearest-neighbor approximation (NEA) approach that proposed in [20].

Under the ideal circumstance, by using the proposed transmission approach, the demodulation of a signal in legitimate receivers' directions should keep the bit error rate as low as possible while with as much bit error rate as possible on the eavesdroppers' side. The following two simulations are based

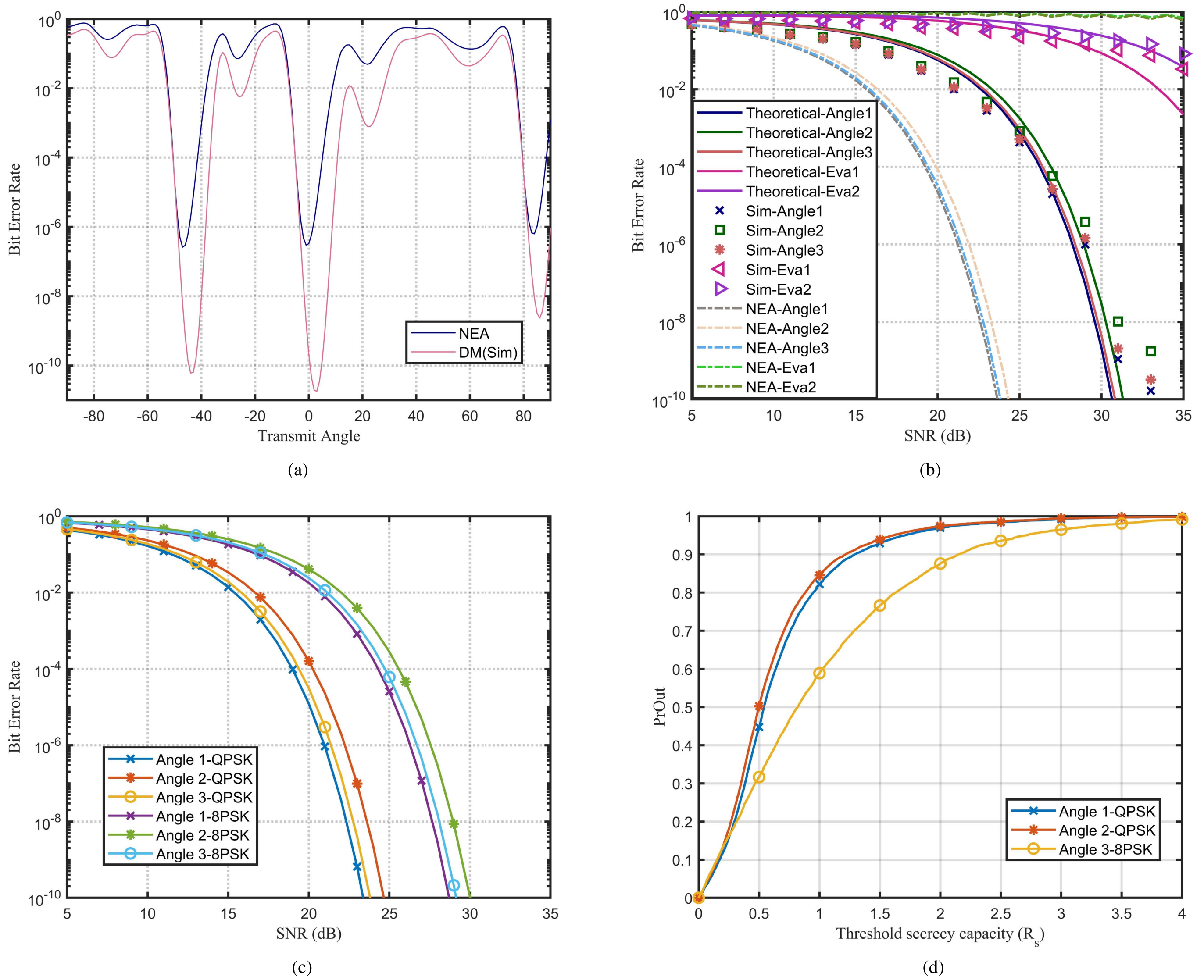


Fig. 5. Three different simulation results. (a)BER when desired receivers are at broadside of three different transmit directions using QPSK (b)The variation of BER with respect to SNR in desired transmitting directions (c)The variation of BER with respect to SNR in desired transmitting directions, with the same modulation imposed on all three legitimate receivers (d)The variation of secrecy outage probability with respect to R_s of difference legitimate receivers.

on the ULA with 512 elements, and the total time is set to be a thousand.

1) Curve of BER Versus Transmit Angle: In the first case, we consider the situation that three legitimate receivers use the same quadrature phase-shift keying modulation to demodulate the received signal. The SNR in this simulation is set to be 20 dB. The result of BER with three different transmit angles is illustrated in Fig. 5(a).

By inspecting the curves of the simulation program, one can find that the main valleys are situated near -50°, -5°, 80° respectively, with negligible BER magnitude, compared with other undesired directions. It is apparent from Fig. 5(a) that the BER values of eavesdroppers at the angle of 35° and -15° are much higher than that of three legitimate receivers. This result implies that the proposed algorithm maintains a good performance in transmitting the signal to legitimate receivers.

2) The Simulation of BER Versus SNR: In this simulation, the BER of three different legitimate receivers and two eavesdroppers versus SNR are examined. By varying the SNR from 5 dB to 35 dB, the resulting theoretical and simulated BERs at three legitimate receivers and eavesdroppers are presented in Fig. 5(b), with QPSK for legitimate receivers at -50°, -5°, 80°, and two eavesdroppers at 35°, -15°, respectively. We also implement the nearest-neighbor approximation (NEA) approach mentioned above to approximate the BER versus SNR.

In Fig. 5(b) there is a clear trend of decreasing value of BER with the increase of SNR for all five receivers. What is interesting in this figure is the BER values of the legitimate receivers in the desired directions are lower than that of eavesdroppers, with sharper slopes compared with the trend of the curve for eavesdroppers. As Fig. 5(b) shows, there is a negligible difference between the simulated and theoretical results for legitimate receivers at three different angles and two eavesdroppers, which is acceptable. Among the legitimate users, the BER of 8-PSK modulation is higher than that of both the QPSK modulations in the directions of legitimate users. To further illustrate the relationship between the modulation order and the BER value using the proposed algorithm, we implemented an extra simulation to reveal the variation of BER versus SNR in desired transmitting directions, with the same modulation imposed on all three legitimate receivers each time. One can observe from Fig. 5(c) that the BER curves of all of the three legitimate receivers using QPSK are underneath the curves using 8PSK. This result suggests that the higher the modulation order one implements, the higher the bit error rate the modulation will have. The above analysis verifies the effectiveness of the proposed algorithm in a secure transmission.

C. Secrecy Outage Probability Simulation

Following the configuration in the previous experiment, we next explore the secrecy outage probabilities of three different legitimate users. According to [33], a statistical method for measuring secrecy outage is declared when the instantaneous secrecy capacity is less than a predefined threshold R_S.

In this simulation, three different legitimate receivers use the same modulation approach as in the BER simulation. Fig. 5(d) compares the resulting curves of secrecy outage probability versus the threshold R_S. It is evident that the secrecy outage probabilities of the 8-PSK are lower than QPSK, growing more smoothly from 0 to 1 bit/s/Hz.

VII. CONCLUSION

In this paper, we have presented a secure multiuser mmWave communication algorithm in the physical layer based on Kronecker decomposition. The phased-array transmission structure with dual-phase shifters is considered at the transmitter side. Unlike the previous work focusing on the signal legitimate receiver, the algorithm proposed in this paper provides an approach to achieve the transmission in multiple legitimate receivers. The proposed algorithm converts the design of common transmit weight for multiuser into the design of sub-weight vectors that satisfies the Kronecker decomposition structure. On this basis, the design of the sub-weight vectors are further decomposed into Kronecker factors, and they are separated into interference cancellation factors and signal enhancement factors by using Kronecker decomposition and the property of the Kronecker product. It achieves secure transmission with multiple transmit weight solutions at different time scales for the same legitimate receiver and different weight vectors towards different transmit angles. The proposed algorithm has an analytical solution with low computational complexities. The extensions of the proposed schemes to other modulation types are applicable. Simulations are also presented to verify the effectiveness of the proposed algorithms in various situations.

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] J. Qiao, Y. He, and X. S. Shen, "Proactive caching for mobile video streaming in millimeter wave 5G networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 7187–7198, Oct. 2016.

[3] M. Alrabeiah and A. Alkhateeb, "Deep learning for mmWave beam and blockage prediction using sub-6 GHz channels," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5504–5518, Sep. 2020.

[4] L. Yan *et al.*, "Machine learning-based handovers for sub-6 GHz and mmWave integrated vehicular networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 10, pp. 4873–4885, Oct. 2019.

[5] J. Huang, C.-X. Wang, R. Feng, J. Sun, W. Zhang, and Y. Yang, "Multi-frequency mmWave massive MIMO channel measurements and characterization for 5G wireless communication systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1591–1605, Jul. 2017.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

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

[8] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.

[9] Z. Kong, J. Song, C. Wang, H. Chen, and L. Hanzo, "Hybrid analog-digital precoder design for securing cognitive millimeter wave networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4019–4034, 2021.

[10] 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.

[11] Y. Pei, Y.-C. 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.

[12] J. Zhu, N. Wang, and V. K. Bhargava, "Per-antenna constant envelope precoding for secure transmission in large-scale MISO systems," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6089–6104, Dec. 2016.

[13] Y. Hong, X. Jing, H. Gao, and Y. He, "Fixed region beamforming using frequency diverse subarray for secure mmWave wireless communications," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2706–2721, 2020.

[14] W. Wang, K. C. Teh, and K. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

[15] 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.

[16] 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.

[17] 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.

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

[19] Y.-W. P. Hong, P.-C. Lan, and C.-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.

[20] 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.

[21] 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.

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

[23] 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.

[24] 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.

[25] W. Q. 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.

[26] C. Liang and X. Zhang, "Phased-array transmission for secure multiuser mmWave communication via Kronecker decomposition," in *Proc. 34th Gen. Assem. Sci. Symp. Int. Union Radio Sci. (URSI GASS)*, Aug. 2021, pp. 1–4.

[27] Y.-P. Lin, "On the quantization of phase shifters for hybrid precoding systems," *IEEE Trans. Signal Process.*, vol. 65, no. 9, pp. 2237–2246, May 2017.

[28] G. Zhu, K. Huang, V. K. N. Lau, B. Xia, X. Li, and S. Zhang, "Hybrid beamforming via the Kronecker decomposition for the millimeter-wave massive MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 9, pp. 2097–2114, Sep. 2017.

[29] M. A. B. Abbasi, V. Fusco, U. Naeem, and O. Malyuskin, "Physical layer secure communication using orbital angular momentum transmitter and a single-antenna receiver," *IEEE Trans. Antennas Propag.*, vol. 68, no. 7, pp. 5583–5591, Jul. 2020.

[30] X. Yu, J.-C. 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, May 2016.

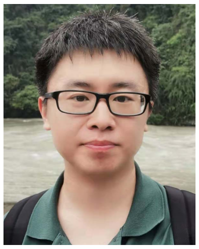
[31] X. Zhang, X. Xia, Z. He, and X. Zhang, "Phased-array transmission for secure mmWave wireless communication via polygon construction," *IEEE Trans. Signal Process.*, vol. 68, pp. 327–342, 2020.

[32] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Symbol-level multiuser MISO precoding for multi-level adaptive modulation," *IEEE Trans. Signal Process.*, vol. 16, no. 8, pp. 5511–5524, Aug. 2017.

[33] D. B. Rawat, T. White, S. Parwez, C. Bajracharya, and M. Song, "Evaluating secrecy outage of physical layer security in large-scale MIMO wireless communications for cyber-physical systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1987–1993, Dec. 2017.

Chentao Liang was born in Sichuan, China. He is currently pursuing the bachelor's degree in communication engineering with the University of Electronic Science and Technology of China, Chengdu, China.

He is preparing to pursue his master's degree at the National Key Laboratory of Science and Technology on Communication. His current research interests include precoding in wireless transmission systems and beam tracking.



Xuejing Zhang (Member, IEEE) was born in Hebei, China. He received the B.S. degree in electrical engineering from Huaqiao University, Xiamen, China, in 2011, the M.S. degree in signal and information processing from Xidian University, Xi'an, China, in 2014, and the Ph.D. degree in signal and information processing from the University of Electronic Science and Technology of China, Chengdu, China, in 2019. From 2017 to 2019, he was a Visiting Student with the University of Delaware, Newark, DE, USA. He is currently a Lecturer at the School of Information and Communication Engineering, University of Electronic Science and Technology of China. His research interests include array signal processing and tensor signal processing, with applications to radar and communications.

He was awarded the Young Scientists Award for Excellence in Scientific Research by the International Union of Radio Science (URSI) in 2020. He received the Prize for Excellent Doctor Degree Dissertation of the Chinese Institute of Electronics in 2020.