Received 29 February 2024; accepted 29 April 2024. Date of publication 8 May 2024; date of current version 23 May 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3398511

On Multiple-Antenna Techniques for Physical-Layer Range Security in the Terahertz Band

WEIJUN GAO[1] (Graduate Student Member, IEEE), CHONG HAN[1,2,3] (Senior Member, IEEE), XUYANG LU[4] (Member, IEEE), AND ZHI CHEN[5] (Senior Member, IEEE)

[1]Terahertz Wireless Communications Laboratory, Shanghai Jiao Tong University, Shanghai 200240, China

[2]Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

[3]Cooperative Medianet Innovation Center, Shanghai Jiao Tong University, Shanghai 200240, China

[4]Laboratory of Ultrafast Integrated Systems, Shanghai Jiao Tong University, Shanghai 200240, China

[5]National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

CORRESPONDING AUTHOR: C. HAN (e-mail: chong.han@sjtu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62171280, and in part by the Fundamental Research Funds for the Central Universities of China.

ABSTRACT Terahertz (THz) communications have naturally promising physical layer security (PLS) performance since narrow beams created by antenna arrays can effectively prevent eavesdroppers outside the beam from overhearing legitimate messages. However, eavesdroppers residing in the THz beam sector are still threatening even with the equipment of traditional multi-antenna techniques. This security challenge is referred to range security, since the range of the legitimate receiver and the eavesdropper differs. To address this problem, in this paper, a fundamental theoretical analysis on multiple-antenna techniques to provide range security is studied. Based on this, the frequency diverse array, as a candidate multiple-antenna technique, is proven ineffective in addressing the range security problem. Moreover, a widely-spaced array and beamforming design for THz range security is demonstrated. A non-constrained optimum approaching (NCOA) algorithm is proposed to achieve sub-optimal performance based on a THz-specific multiple-antenna array structure. Simulation results illustrate that our proposed widely-spaced antenna communication scheme can ensure a 6 bps/Hz secrecy rate when the transmit power is 10 dBm and the propagation distance is 10 m.

INDEX TERMS Terahertz communications, widely-spaced array.

I. INTRODUCTION

A. BACKGROUND

With an increasing demand for high-speed, reliable, and private information exchange, a new spectrum and advanced security technologies are awaited to be developed for next-generation wireless networks. The Terahertz (THz) band, with frequencies ranging from 0.1 to 10 THz, is envisioned to realize multi-gigabit-per-second or even terabit-per-second data rates owing to the abundant bandwidth resource [1], [2], [3]. In addition to the bandwidth merit, the potential of THz communications to improve information security is envisioned in [4], [5], [6]. As an essential technique in addition to the conventional encryption-based methods, physical layer security (PLS) ensures information privacy at the physical layer of the wireless networks by exploiting transceiver and channel properties, including beamforming, fading, noise, and interference [7]. Compared with the encryption-based methods, the PLS has the advantage of having reduced overhead for secret key distribution. Moreover, PLS can ensure information secrecy even with an eavesdropper having infinite computational power.

With the equipment of ultra-massive multiple-input multiple-output (UM-MIMO) arrays for THz communications, the narrow and directional beams powered by multiple-antenna techniques bring substantial benefits to PLS [5], [8], [9]. Typically, a THz beam is directed towards the legitimate user through the beam training and tracking

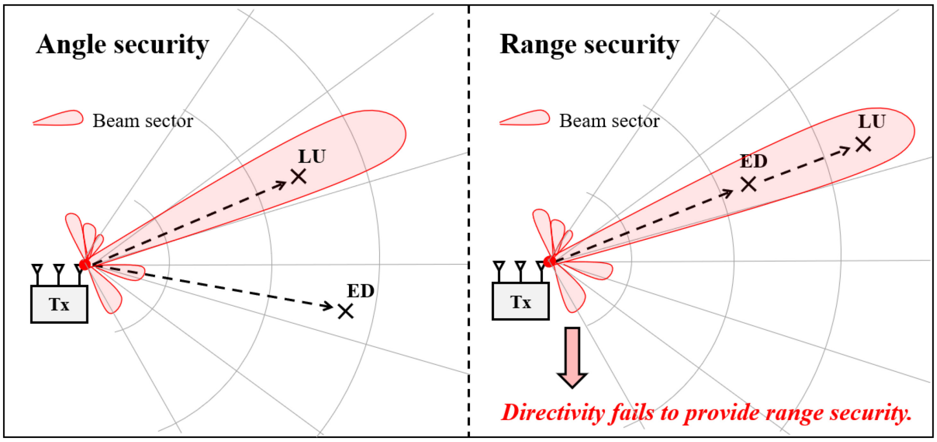


FIGURE 1. Illustration of range and angle security with a transmitter (Tx), a legitimate user (LU) and an eavesdropper (ED).

processes. With an eavesdropper being located outside or inside the beam, the THz PLS can be divided into two categories, namely, *angle security* and *range security*, as illustrated in Fig. 1. On the one hand, for the angle security, the aim is to prevent the eavesdropper from being located inside the beam sector, which improves the PLS in the angular domain. On the other hand, the range security aims at enhancing the secrecy rate when the legitimate user and the eavesdropper are both located inside the beam sector, i.e., when their propagation angles are the same while their ranges differ. Although the traditional multiple-antenna techniques of THz communications can enhance angle security, it fails to provide range security.

Despite the promising confidentiality of THz angle security thanks to high directivity, solutions to the THz range security problem are still awaited to be explored for the following challenges [5]. First, the signals received by the eavesdropper inside the beam benefit from the same antenna gain as legitimate users, which suggests that the THz directivity and traditional multiple-antenna techniques are ineffective in enhancing the range security. Second, due to the sparsity feature of the THz channel, the PLS technique using multi-paths to aid the security proposed in [10] might not be helpful. More critically, when Eve inside the beam sector is located nearer than the legitimate receiver, i.e., in close proximity, secure communication is significantly jeopardized since the secret codewords decodable by Bob are even easier decodable by the eavesdropper who has an even higher received signal-to-noise ratio (SNR) [9]. This research gap motivates this work aiming at addressing the range security for THz communications.

B. RELATED WORK

The fundamental limit of a wiretap channel model has been analyzed in [11] including a transmitter Alice (A), a legitimate receiver Bob (B), and an eavesdropper Eve (E). The key metric is characterized by the *secrecy rate*, defined as the maximum data rate that can be transmitted reliably and confidentially. Traditional multiple-antenna technologies can only improve the secrecy rate in the angular domain. For example, the secrecy capacity with the multiple antennas is calculated in [12], while the multi-antenna-based secure beamforming techniques are proposed in [13] In [14], it has been experimentally presented that the massive MIMO can enhance the physical layer security. Then, some low-complexity architectures including antenna selection and hybrid analog-digital precoding methods are robust against passive eavesdropping [15], where almost no cost is paid to achieve the security, known as “secrecy for free”. The extended MIMO-based physical layer security approach with active eavesdroppers are studied in [16]. In [17], [18], [19], [20], as an extension to MIMO-based secure beamforming, the authors develop the artificial noise (AN)-aided beamforming technique to combat eavesdroppers in close proximity. In particular, AN signals are designed to be injected into the transmitted confidential signal to jam Eve’s channel and enhance the secrecy rate, known as transmit AN (TAN) techniques.

Range security technologies, however, are rarely investigated for micro-wave band communications. Since the micro-wave channel contains rich scattering, angle security techniques can utilize the spatial degree of freedoms (SDoFs) to mitigate eavesdropping attacks. However, as also pointed out in [21], the correlation of non-Rayleigh fading channels in the angle domain may lead to eavesdropper advantage. Specifically for THz communications, the feature of limited SDoFs in THz channels makes the range security problem essential to be addressed. One useful range security technique in the literature is the receive AN (RAN) technique, where the receiver side sends the jamming signals while receiving the confidential signals [22], [23], [24]. On the downside, this technique requires a high-complexity self-interference cancellation (SIC) to transmit the AN signal and receive the information signal simultaneously. Another range security technique is the distance-adaptive molecular absorption modulation scheme, which hides the signal under the molecular absorption peaks in the THz band [8]. In recent years, frequency diverse array (FDA) has been recognized as a good candidate to address the range security problem [25]. By introducing a small frequency offset among different antennas in the antenna array, the FDA shows a periodical range-, angle-, and time-varying beam pattern. FDA has been widely used in security applications by taking advantage of the time-varying property, e.g., in [25]. However, the effectiveness of the FDA-based techniques in providing THz range security requires investigation.

C. MOTIVATIONS AND CONTRIBUTIONS

The goals of this paper are two-fold. First, we lay out a theoretical analysis of the multiple-antenna techniques under the range security condition. We revisit the FDA communication model as one particular design of multiple-antenna techniques and prove that previous FDA models in the literature [17], [18], [19], [20] are ineffective in providing range security. Second, motivated by the failure of compact-spaced array (CSA) operating in far-field regions, we propose a THz widely-spaced array (WSA) and a hybrid beamforming design as a near-field THz range security solution. Specifically, we present a multiple-antenna-assisted THz range security system model and develop the secrecy capacity, based on which the FDA system model is revisited and revised. Moreover, we propose a THz WSA and beamforming design to enhance the THz range security. An optimization problem is formulated based on the system model in Section II and a sub-optimal algorithm is proposed to determine the precoding matrix. The trade-off analysis between the antenna size and the secrecy rate demonstrates that the THz WSA phased array can maintain a reasonable size thanks to the sub-millimeter wavelengths of THz waves. The comparison between the proposed algorithm and existing related works in terms of their capability to provide angle and range security is summarized in Table 1. The proposed WSA technique can provide range security while maintaining reasonable complexity. The contributions of this paper are summarized as follows:

- *We perform theoretical analysis on multiple-antenna techniques for THz range security.* The secrecy capacity is derived based on which multiple-antenna techniques operating in the far-field regions are proven ineffective in providing range security. As a traditional candidacy for range security, the FDA communication model is analyzed and revised.
- *We propose a novel THz WSA and hybrid beamforming scheme to enhance the THz range security.* A non-constrained optimum approaching (NCOA) algorithm is developed to solve the non-convex secrecy rate maximization problem, which determines the optimal hybrid beamformer design. Moreover, the trade-off between array size and secrecy rate enhancement of WSA is investigated.
- *We evaluate our proposed scheme against the existing PLS techniques.* Monte-Carlo simulation demonstrates the convergence of the proposed NCOA algorithm. Extensive numerical results show that for a propagation distance at 10 m and transmit power of 10 dBm, the proposed method can achieve a secrecy rate of 6 bps/Hz, while the CSA fails to guarantee range security.

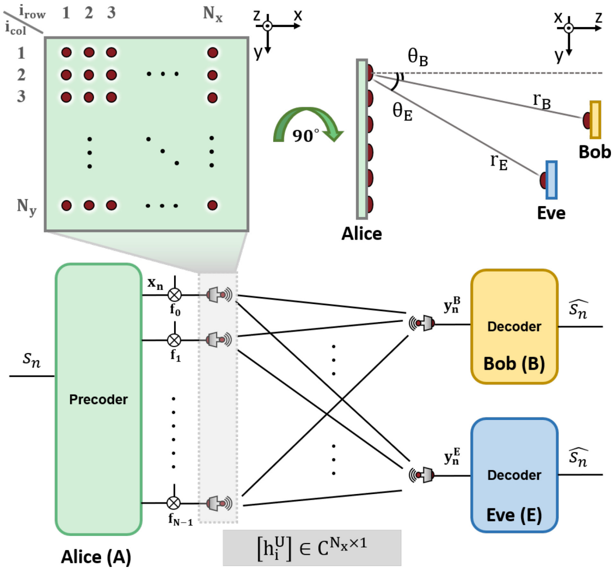


FIGURE 2. System model of multiple-antenna-assisted THz secure communication.

TABLE 1. Typical techniques for physical layer security.

Technique	Range Security	Angle Security	Complexity
FDA [25]	No	Yes	Low
WSA	Yes	Yes	Medium
CSA [12]	No	Yes	Low
TAN [18]	No	Yes	Low
RAN [17]	Yes	Yes	High

The remainder of the paper is organized as follows. Section II presents multiple-antenna-assisted THz secure communication system model. Section III conducts a theoretical analysis on multiple-antenna techniques for THz range security, where the FDA technique is proven ineffective in providing range security. This conclusion is extended to the general multiple-antenna techniques operating in the far-field region. The proposed WSA communication and hybrid beamforming scheme are proposed in Section IV, where the NCOA hybrid beamforming algorithm is elaborated, and the trade-off between array size and maximum secrecy rate is investigated. Numerical results are described in Section V to verify the convergence of the proposed algorithm and the secrecy rate enhancement compared with existing methods. The paper is concluded in Section VI.

Notations: matrices and vectors are denoted by boldface upper and lower case letters, respectively. $[\,\cdot\,]^+ \triangleq \max(0,\cdot)$. $\langle\cdot,\cdot\rangle$ denotes inner product. $*$ is the convolution operation with respect to time t. $\mathbf{A}^T$, and $\mathbf{A}^\dagger$ are the transpose, and conjugate transpose of the matrix $\mathbf{A}$, respectively.

II. SYSTEM MODEL

In this section, we present a multiple-antenna-assisted THz secure communication model in Fig 2, which consists of a transmitter Alice (A), a legitimate receiver Bob (B), and a passive eavesdropper Eve (E). Thanks to the small wavelength of the THz signal in the order of millimeter down to sub-millimeter, an UM-UPA is equipped at Alice to overcome the large propagation loss. Bob and Eve are assumed to be equipped with a single antenna. The UM-UPA is comprised of $N_\mathrm{t} = N_\mathrm{x} \times N_\mathrm{y}$ antennas placed uniformly in a rectangular shape, with N_x antennas in each row and N_y antennas in each column. The antenna spacing between neighboring antennas is denoted by d. A three-dimensional Cartesian coordinate system is adopted, where the antenna in the $i_\mathrm{row}^\mathrm{th}$ row and the $i_\mathrm{col}^\mathrm{th}$ column is located at $(\mu_i, \nu_i, \xi_i) = ((i_\mathrm{row}-1)d, (i_\mathrm{col}-1)d, 0)$. The antenna index is represented by $i = N_\mathrm{x} \times (i_\mathrm{row} - 1) + i_\mathrm{col}$. The distance from the i^th antenna at Alice to the receiver U are denoted by $r_{\mathrm{U},i}$. The receiving nodes including Bob and Eve, denoted by B and E, are assumed to be located at $(r_\mathrm{U} \sin\theta_\mathrm{U}, 0, r_\mathrm{U}\cos\theta_\mathrm{U})$, where $\mathrm{U} \in \{\mathrm{B}, \mathrm{E}\}$, r_U represents the propagation distance between Alice and U, and θ_U defines the propagation angle of the receiver U.

The normalized transmitted symbol stream is denoted by s_n satisfying $\mathbb{E}[|s_n|^2] = 1$, where n represents the symbol index and $\mathbb{E}[\,\cdot\,]$ returns the expectation. The symbols are modulated into a baseband waveform $m(t)$ given by [8]

$$m(t) = \sum_{n=-\infty}^{\infty} \sqrt{P} s_n \cdot g(t - nT_\mathrm{s}), \tag{1}$$

where P denotes transmit power, t represents time, $g(t)$ represents a normalized pulse shape, and T_s denotes a symbol time. Note that we do not omit the notation t to simplify the analysis because the inappropriate assumption made in FDA is about the synchronization between transmit and receive symbols. We consider that the baseband bandwidth $B_g = 1/T_\mathrm{s}$ is smaller than the coherence bandwidth, which implies narrowband communications. This is reasonable since with directional antennas, the coherence bandwidth can reach 60 GHz [26]. The baseband waveform $m(t)$ is first precoded by a linear time-varying precoder $\mathbf{W}(t) \triangleq [w_1(t), \ldots, w_{N_\mathrm{t}}(t)]$, satisfying $\sum_{i=1}^{N_\mathrm{t}} |w_i(t)|^2 = 1$. The carrier frequency of the i^th antenna is denoted by f_i, and the transmit signal represented by $\mathbf{x} = [x_1, \ldots, x_{N_\mathrm{t}}]^T$ is therefore expressed as [27]

$$x_i(t) = m(t) w_i(t) \mathrm{e}^{-j2\pi f_i t}, \tag{2}$$

where $x_i(t)$ denotes the signal transmitted by the i^th antenna of Alice. Due to the sparsity of the THz channel and the high directivity, the path gains of the reflected, scattered, and diffracted paths are negligibly weak compared to the line-of-sight (LoS) path. It is assumed that the channel state information, represented by propagation distance in this paper, is known at the transmitter. Thus, we consider to model the THz channel impulse response $h_{\mathrm{U},i}(t)$ from the i^th antenna of Alice to node $\mathrm{U} \in \{\mathrm{B}, \mathrm{E}\}$ as the result of the LoS path only [26], [28], [29], which is represented as

$$h_{\mathrm{U},i}(t) = a\big(f_i, r_{\mathrm{U},i}\big)\delta\Big(t - \frac{r_{\mathrm{U},i}}{c}\Big), \tag{3}$$

where $a(f_i, r_{\mathrm{U},i}) = \frac{c}{4\pi f_i r_{\mathrm{U},i}}$ denotes the free-space LoS path gain according to Friis' law. c denotes the speed of light. The delay is $\frac{r_{\mathrm{U},i}}{c}$ and $\delta(\cdot)$ stands for the Dirac Delta function. To simplify the notations, we use $a(r_{\mathrm{U},i})$ to represent $a(f_i, r_{\mathrm{U},i})$. The superimposed received signal $y_\mathrm{U}(t)$ at node U from the transmit antenna array is thus given by

$$y_\mathrm{U}(t) = \sum_{i=1}^{N_\mathrm{t}} x_i(t) * h_{\mathrm{U},i}(t) + n_\mathrm{U}(t), \tag{4}$$

where $n_\mathrm{U}(t)$ stands for the additive Gaussian white noise (AWGN) noise variance σ_U^2. In this work, we assume that the noise variances for Bob and the Eve are the same and both equal to σ^2, i.e., $\sigma_\mathrm{B}^2 = \sigma_\mathrm{E}^2 = \sigma^2$.

According to the relationship between the antenna array size and the communication distance, multiple-antenna communications can be classified into near-field and far-field communications. If the propagation distance of the receiving node U is larger than the Fraunhofer distance [30], [31], i.e., $r_\mathrm{U} \geq 2d^2 N_\mathrm{t}/\lambda$, the node U is considered to be in the far-field region of the transmitter. This distance relationship determines how we could further simplify the expression of the received signal represented in (1)-(4). In general, we represent the distance $r_{\mathrm{U},i}$ as

$$r_{\mathrm{U},i} = r_\mathrm{U} + \mathcal{R}_i(\theta_\mathrm{U}, r_\mathrm{U}), \tag{5}$$

where $\mathcal{R}_i(\theta_\mathrm{U}, r_\mathrm{U})$ denotes the residual propagation distance of the i^th antenna to the receiver. This residual term depends on the antenna index i, the propagation angle θ_U, and the propagation distance r_U. If the receiver is located in the far-field region of the transmitter antenna array, the following far-field approximation is satisfied by neglecting the high-order term related to r_U as

$$\mathcal{R}_i(\theta_\mathrm{U}, r_\mathrm{U}) \approx \mathcal{P}_i(\theta_\mathrm{U}), \tag{6}$$

where $\mathcal{P}_i(\theta_\mathrm{U}) \ll r_\mathrm{U}$ is range-invariant and only depends on the antenna index i and the angle θ_U. For example, if the uniform space d satisfies $d \leq c/2f_i$, the residual term of a linear antenna array can be expressed as $\mathcal{P}_i(\theta_\mathrm{U}) = id\sin\theta_\mathrm{U}$ and that of a planar antenna array can be represented by $\mathcal{P}_i(\theta_\mathrm{U}) = -(i_\mathrm{row} - 1)d\sin\theta_\mathrm{U}$. The counterpart of the far-field communication is defined as near-field communication, where the approximation (6) does not apply.

III. THEORETICAL ANALYSIS OF MULTIPLE-ANTENNA TECHNIQUES FOR TERAHERTZ RANGE SECURITY

In this section, we theoretically investigate how multiple-antenna techniques can address the THz range security problem. To reach this goal, we first analyze the secrecy capacity of the multiple-antenna secure channel under the THz range security scenario. This secrecy capacity analysis provides an upper-bound secrecy performance of general

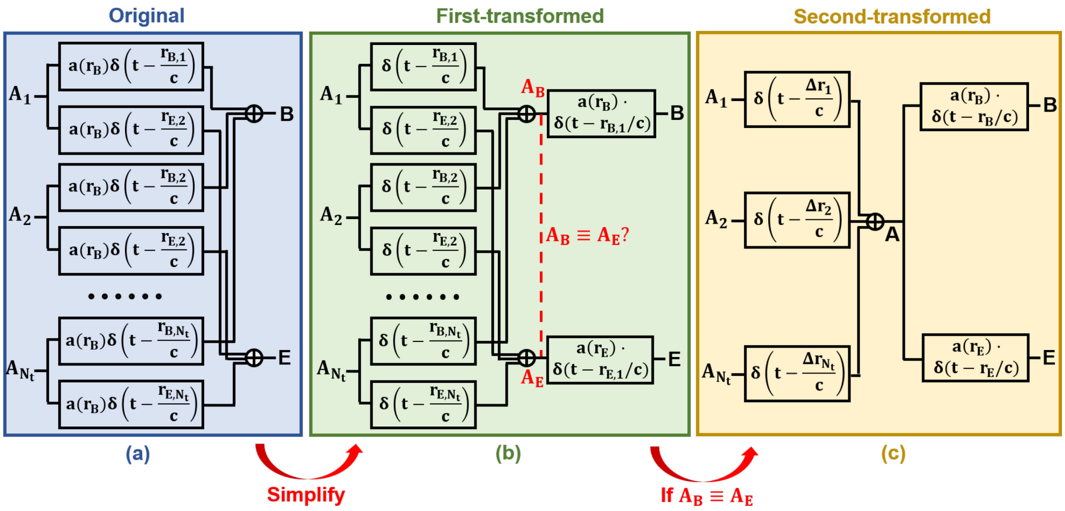

Original
First-transformed
Second-transformed
A_1
A_2
A_{N_t}
$a(r_B)\delta\left(t-\frac{r_{B,1}}{c}\right)$
$a(r_B)\delta\left(t-\frac{r_{E,2}}{c}\right)$
$a(r_B)\delta\left(t-\frac{r_{B,2}}{c}\right)$
$a(r_B)\delta\left(t-\frac{r_{E,2}}{c}\right)$
$a(r_B)\delta\left(t-\frac{r_{B,N_t}}{c}\right)$
$a(r_B)\delta\left(t-\frac{r_{E,N_t}}{c}\right)$
B
E
$\delta\left(t-\frac{r_{B,1}}{c}\right)$
$\delta\left(t-\frac{r_{E,2}}{c}\right)$
$\delta\left(t-\frac{r_{B,2}}{c}\right)$
$\delta\left(t-\frac{r_{E,2}}{c}\right)$
$\delta\left(t-\frac{r_{B,N_t}}{c}\right)$
$\delta\left(t-\frac{r_{E,N_t}}{c}\right)$
A_B
A_E
$A_B \equiv A_E?$
$a(r_B)\cdot\delta(t-r_{B,1}/c)$
$a(r_E)\cdot\delta(t-r_{E,1}/c)$
$\delta\left(t-\frac{\Delta r_1}{c}\right)$
$\delta\left(t-\frac{\Delta r_2}{c}\right)$
$\delta\left(t-\frac{\Delta r_{N_t}}{c}\right)$
A
$a(r_B)\cdot\delta(t-r_B/c)$
$a(r_E)\cdot\delta(t-r_E/c)$
(a)
(b)
(c)
Simplify
If $A_B \equiv A_E$

FIGURE 3. System block diagram transformation of the multiple-antenna secure communication system. (a) Original system block diagram. (b) First-transformed system block diagram. (c) Second-transformed system block diagram. Here A_i represents the i^{th} antenna at Alice.

multiple-antenna techniques. Then, we demonstrate that the FDA technique, as an advocated multiple-antenna technique in the literature for range security, is ineffective in enhancing THz range security.

A. SECRECY CAPACITY ANALYSIS UNDER RANGE SECURITY SCENARIO

The original channel block diagram is shown in Fig. 3(a), where the nodes $\{\mathbf{A}_i\}$, $i \in [1, N_t]$ represent the antennas in the transmit antenna array. Node $\boldsymbol{B}$ and $\mathbf{E}$ represent the single-antenna Bob and Eve, respectively. The channel impulse response from $\mathbf{A}_i$ to $\mathbf{U} \in \{\boldsymbol{B}, \mathbf{E}\}$ is expressed by $a(r_U)\delta(t - \frac{r_{U,i}}{c})$. By substituting $r_{U,i} = r_U + \Delta r_{U,i}$, the system block diagram in Fig. 3(a) can be simplified to the block diagram in Fig. 3(b), due to the following relationship

$$y_U(t) = \sum_{i=1}^{N_t} x_i(t) * a(r_U)\delta\left(t - \frac{r_{U,i}}{c}\right) \tag{7a}$$

$$= \left(\sum_{i=1}^{N_t} x_i(t) * \delta\left(t - \frac{\Delta r_{U,i}}{c}\right)\right) * a(r_U)\delta\left(t - \frac{r_U}{c}\right), \tag{7b}$$

where $x_i(t)$ represents the transmitted signal at node $\mathbf{A}_i$, and $y_U(t)$ denotes the received signal at node $\mathbf{U}$. Two intermediate nodes representing the superimposed signals at Bob and Eve in Fig. 3(b) are defined as $\mathbf{A}_{\boldsymbol{B}}$ and $\mathbf{A}_{\mathbf{E}}$, respectively. As the basic assumption for the range security problem, the propagation angles of Bob and Eve are equal, i.e., $\theta_B = \theta_E$. Additionally, as described in Section II, we assume that the receiving nodes $\boldsymbol{B}$ and $\mathbf{E}$ are in the far-field region of the antenna array. Therefore, $\Delta r_{B,i} = \Delta r_{E,i}$, and the signals at node $\mathbf{A}_{\boldsymbol{B}}$ and $\mathbf{A}_{\mathbf{E}}$ are equal. We can superimpose the two nodes and their corresponding overlapped parts in (b), as depicted in Fig. 3(c). Figure 3(c) shows a cascaded wiretap channel which exhibits as two Markov chains, e.g., $\{\mathbf{A}_i\} \to \mathbf{A} \to \boldsymbol{B}$ and $\{\mathbf{A}_i\} \to \mathbf{A} \to \mathbf{E}$.

Based on the system transformation from Fig. 3(a) to Fig. 3(c), the secrecy capacity C_s of the multiple-antenna secure communication system based on the result in [11], as

$$C_s(\mathbf{A}_i, \boldsymbol{B}, \mathbf{E}) \le C_s(\boldsymbol{A}, \boldsymbol{B}, \mathbf{E}) = \left[\log\left(1 + \frac{P_A a(r_B)^2}{\sigma_B^2}\right) - \log\left(1 + \frac{P_A a(r_E)^2}{\sigma_E^2}\right)\right]^+, \tag{8}$$

where P_A denotes the maximum signal power of the combined signals at node $\mathbf{A}$. (8) implies that the secrecy rate from node $[\mathbf{A}_i]$ is upper-bounded by the secrecy rate from node $\mathbf{A}$ and

$$P_A = \max \mathbb{E}\left[\left|\sum_{i=1}^{N_t} x_i(t - \Delta r_i/c)\right|^2\right] \le \sum_{i=1}^{N_t} \max \mathbb{E}[|x_i(t)|^2] = N_t P, \tag{9}$$

whose secrecy capacity is equal to that of a fully-digital beamforming scheme. This result proves that any signal processing and multiple antenna techniques operating in the far-field regions cannot provide THz range security since the traditional fully-digital beamforming technique can reach the secrecy capacity.

Further explanation from the wave propagation perspective is provided as follows. In Fig. 3(c), the intermediate node $\mathbf{A}$ can be interpreted as the wavefront of the transmitted beam. The THz LoS signal propagation from the source to far-field regions can be divided into two phases, as depicted in Fig. 4. In the first phase, the transmitted signal propagates from array plane to the plane perpendicular to the direction of propagation in the near-field region, i.e., the wavefront $\mathbf{A}$. In the second phase, the combined signal further propagates in the far-field regions. According to the Markov chain theory, for all receiving nodes located in the far-field regions with the same propagation angle, the secrecy capacity of a MIMO channel is upper bounded by the SISO channel from the

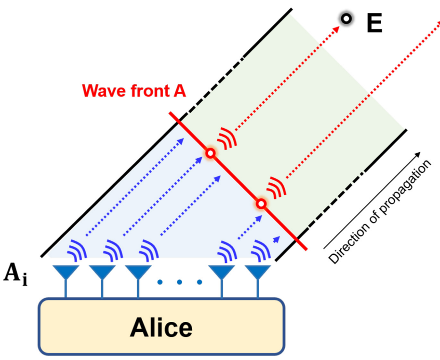


FIGURE 4. Physical meaning of the intermediate node A in the Markov chain.

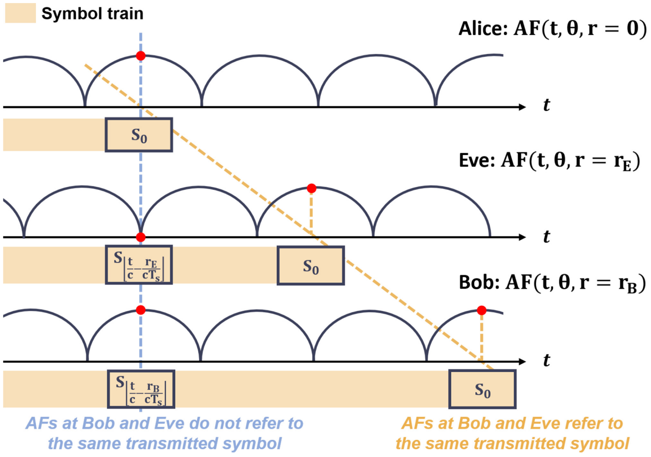

Symbol train
Alice: AF(t, θ, r = 0)
t
S_0
Eve: AF(t, θ, r = r_E)
t
$S_{\lfloor \frac{t}{c} - \frac{r_E}{cT_s} \rfloor}$
S_0
Bob: AF(t, θ, r = r_B)
t
$S_{\lfloor \frac{t}{c} - \frac{r_B}{cT_s} \rfloor}$
S_0
AFs at Bob and Eve do not refer to the same transmitted symbol
AFs at Bob and Eve refer to the same transmitted symbol

FIGURE 5. Illustration of the synchronization problem between AF and symbol in traditional FDA range security model.

wavefront to the receiving node. This wavefront acts like a bottleneck of the wiretap channel, preventing multiple-antenna techniques from distinguishing Bob and Eve in the far-field region. Therefore, any multiple-antenna schemes operating in the far-field region cannot enhance THz range security.

B. CAN FDA PROVIDE TERAHERTZ RANGE SECURITY?

FDA introduces different small frequency offsets on each antenna to obtain a range, angle, and time-dependent array factor, which can steer the beam automatically [32]. The range-dependency of the beam can simultaneously enhance the received SNR at Bob while mitigating the received SNR at Eve and achieve range security [25]. However, this idea contradicts our secrecy capacity analysis in Section III-A since their derived data rate exceeds the derived secrecy capacity. Therefore, we rigorously revisit the traditional FDA range security model and revise the model to demonstrate that the FDA cannot provide THz range security.

1) TRADITIONAL FREQUENCY DIVERSE ARRAY RANGE SECURITY MODEL

In the traditional FDA model adopted in [33], [34], [35], [36], [37], the carrier frequency of the i^{th} antenna is assumed to be $f_i = f_0 + \Delta f_i$, where $\Delta f_i \ll f_0$. For analysis simplicity, we assume the FDA to be a uniform linear array here. By assuming the all-one vector for the precoding vector and far-field condition $\mathcal{R}_i(\theta_U) = id \sin\theta_U$, the equivalent antenna gain, i.e., the array factor (AF), is given by [33]

$$AF(t, \theta_U, r_U) = \sum_{i=1}^{N_t} e^{j2\pi\left[\Delta f_i\left(t - \frac{r_U}{c}\right) + \frac{i f_i d \sin\theta_U}{c}\right]}, \tag{10}$$

and the secrecy rate is given by

$$R_s = \left[\log\left(1 + \frac{P|AF(t,\theta,r_B)|^2 a(r_B)^2}{\sigma^2}\right) - \log\left(1 + \frac{P|AF(t,\theta,r_E)|^2 a(r_E)^2}{\sigma^2}\right)\right]^+, \tag{11}$$

where $\theta_B = \theta_E = \theta$ for range security scenario. Since (10) depends on range parameter r, it can be designed that the AF at Bob can be larger than AF at the Eve, which seems to be beneficial to range security.

2) INAPPROPRIATE ASSUMPTION IN TRADITIONAL FDA MODEL

The derivation from the array factor in (10) to the secrecy rate in (11) adopts an inappropriate assumption. it is incorrectly assumed that the array factor $AF(t, \theta, r_B)$ and $AF(t, \theta, r_E)$ at the same time t refer to the same symbol. Suppose Alice transmits a secret symbol at time t_0, then Bob and Eve can receive this symbol at time $t_0 + \frac{r_B}{c}$ and $t_0 + \frac{r_E}{c}$, respectively. Therefore, when we analyze the array factor at the receiver sides, $AF(t, \theta, r_B)$ represents the AF of the symbol transmitted at $t - \frac{r_B}{c}$ while $AF(t, \theta, r_B)$ stands for the AF of the symbol transmitted at $t - \frac{r_E}{c}$. These two AFs do not refer to the same symbol transmitted from Alice, and therefore it is incorrect to compute the secrecy capacity based on them. This example is illustrated in Fig. 5. The blue line captures the derived traditional AF at Alice, Bob, and Eve, and we observe that it refers to different symbols. The correct way to study the secrecy rate is to track one secret symbol and focus on the AF of the same symbol received by Bob and Eve at different times, as the yellow line illustrates. Specifically in this example, we should compare the AF of the symbol at Bob and Eve at $t + \frac{r_B}{c}$ and $t + \frac{r_E}{c}$, respectively, which leads to the following observation that

$$AF\left(t_0 + \frac{r_B}{c}, \theta, r_B\right) = AF\left(t_0 + \frac{r_E}{c}, \theta, r_E\right). \tag{12}$$

Therefore, the AF of one symbol created by the FDA is the same at Bob and Eve, which cannot provide range security.

The illustration from the beam pattern point of view is provided as follows. Since the confidential message is modulated on the EM wave, which travels at the speed of light, we should investigate the joint range-time beam pattern of FDA instead of a "snapshot" one. Unfortunately, although the FDA has a range-varying and time-varying beam pattern, the joint range-time beam pattern propagating at the speed of light is constant, as depicted in Eq. (2) of [25], where the FDA beam pattern is only dependent on the term $t-\frac{r_{\mathrm{U}}}{c}$. The interpretation of the FDA beam pattern in previous related studies neglects the synchronization between symbol and array factor, and therefore their secrecy rate analysis is problematic.

3) REVISED FREQUENCY DIVERSE ARRAY RANGE SECURITY MODEL

We first rigorously derive the end-to-end received signals at Bob and Eve. For expression simplicity, we adopt the rectangular pulse waveform, which is given by

$$g(t)=g_{\mathrm{rect}}(t)=\begin{cases}\frac{1}{\sqrt{T_{\mathrm{s}}}}, & t\in[0,T_{\mathrm{s}}),\\ 0, & \text{otherwise},\end{cases}\tag{13}$$

The superimposed signal at the receiver U can be computed by

$$\begin{aligned}y_{\mathrm{U}}(t,\theta,r_{\mathrm{U}})=&\sqrt{\frac{P}{T_{\mathrm{s}}}}\sum_{i=1}^{N_{\mathrm{t}}}s_{\lfloor\frac{t}{T_{\mathrm{s}}}-\frac{r_{\mathrm{U},i}}{cT_{\mathrm{s}}}\rfloor}w_i\Big(t-\frac{r_{\mathrm{U},i}}{c}\Big)a(r_{\mathrm{U},i})\\&\cdot\exp\Big\{-j2\pi(f_0+\Delta f_i)\Big(t-\frac{r_{\mathrm{U},i}}{c}\Big)\Big\}\qquad(14\mathrm{a})\\\approx&\sqrt{\frac{P}{T_{\mathrm{s}}}}s_{\lfloor\frac{t}{T_{\mathrm{s}}}-\frac{r_{\mathrm{U}}}{cT_{\mathrm{s}}}\rfloor}a(r_{\mathrm{U}})\sum_{i=1}^{N_{\mathrm{t}}}w_i\Big(t-\frac{r_{\mathrm{U}}}{c}\Big)\\&\cdot\exp\Big\{-j2\pi(f_0+\Delta f_i)\Big(t-\frac{r_{\mathrm{U},i}}{c}\Big)\Big\}\qquad(14\mathrm{b})\\\approx&\sqrt{\frac{P}{T_{\mathrm{s}}}}s_{\lfloor\frac{t}{T_{\mathrm{s}}}-\frac{r_{\mathrm{U}}}{cT_{\mathrm{s}}}\rfloor}a(r_{\mathrm{U}})\mathrm{e}^{-j2\pi f_0(t-\frac{r_{\mathrm{U}}}{c})}\\&\sum_{i=1}^{N_{\mathrm{t}}}w_i\Big(t-\frac{r_{\mathrm{U}}}{c}\Big)\\&\cdot\exp\Big\{-j2\pi\Big[f_0\frac{\mathcal{P}_i(\theta)}{c}+\Delta f_i\Big(t-\frac{r_{\mathrm{U}}}{c}\Big)\Big]\Big\},\\&\qquad(14\mathrm{c})\end{aligned}$$

where $\lfloor x\rfloor$ returns the largest integer smaller or equal to x. In (14a), $a(r_{\mathrm{U},i})$ represents the channel gain and the superimposed signal is expressed by the summation of signals transmitted from each antenna. The approximation in (14b) applies the assumption that the symbol, the precoding vector, and the path loss are uniform for all the antenna pairs, i.e., $s_{\lfloor\frac{t}{T_{\mathrm{s}}}-\frac{r_{\mathrm{U},i}}{cT_{\mathrm{s}}}\rfloor}\approx s_{\lfloor\frac{t}{T_{\mathrm{s}}}-\frac{r_{\mathrm{U}}}{cT_{\mathrm{s}}}\rfloor}$, $w_i(t-\frac{r_{\mathrm{U},i}}{c})\approx w_i(t-\frac{r_{\mathrm{U}}}{c})$, and $a(r_{\mathrm{U},i})\approx a(r_{\mathrm{U}})$. Finally, (14c) is derived by expanding $r_{\mathrm{U},ij}$ according to (6) and then ignoring the second-order small term $-j2\pi\frac{\Delta f_i\cdot\mathcal{P}_i(\theta)}{c}$.

According to (14), the term discarding the symbol index term $s_{\lfloor\frac{t}{T_{\mathrm{s}}}-\frac{r_{\mathrm{U}}}{cT_{\mathrm{s}}}\rfloor}$ is the same as the array factor computed by previous FDA security work [33]. However, omitting the $s_{\lfloor\frac{t}{T_{\mathrm{s}}}-\frac{r_{\mathrm{U}}}{cT_{\mathrm{s}}}\rfloor}$ term is inappropriate it shows that the received symbol by Bob and Eve at time t are different. Instead, we focus on one specific symbol transmitted Alice, and analyze how it is received by Bob and Eve. For a symbol s_{n_0}, Alice transmits the symbol at time $t=n_0T_{\mathrm{s}}$, while Bob and Eve receive this symbol at time $t=n_0T_{\mathrm{s}}+\frac{r_{\mathrm{B}}}{c}$ and $t=n_0T_{\mathrm{s}}+\frac{r_{\mathrm{E}}}{c}$, respectively. Therefore, the corresponding received signals $y_{\mathrm{B}}(n_0T_{\mathrm{s}}+\frac{r_{\mathrm{B}}}{c},\theta,r_{\mathrm{B}})$ and $y_{\mathrm{E}}(n_0T_{\mathrm{s}}+\frac{r_{\mathrm{E}}}{c},\theta,r_{\mathrm{E}})$ can be expressed as

$$\begin{aligned}y_{\mathrm{B}}\Big(n_0T_{\mathrm{s}}+\frac{r_{\mathrm{B}}}{c},\theta,r_{\mathrm{B}}\Big)=&\,s_{n_0}a(r_{\mathrm{B}})\mathrm{e}^{-j2\pi f_0(n_0T_{\mathrm{s}})}\sum_{i=1}^{N_{\mathrm{t}}}w_i\\&\times\exp\Big\{-j2\pi\Big[f_0\frac{\mathcal{P}_i(\theta)}{c}-\Delta f_i(n_0T_{\mathrm{s}})\Big]\Big\}+n(t),\ (15\mathrm{a})\\y_{\mathrm{E}}\Big(n_0T_{\mathrm{s}}+\frac{r_{\mathrm{E}}}{c},\theta,r_{\mathrm{E}}\Big)=&\,s_{n_0}a(r_{\mathrm{E}})\mathrm{e}^{-j2\pi f_0(n_0T_{\mathrm{s}})}\sum_{i=1}^{N_{\mathrm{t}}}w_i\\&\times\exp\Big\{-j2\pi\Big[f_0\frac{\mathcal{P}_i(\theta)}{c}-\Delta f_i(n_0T_{\mathrm{s}})\Big]\Big\}+n(t).\ (15\mathrm{b})\end{aligned}$$

We observe that except for the term $a(r_{\mathrm{U}})$ in (15a) and (15b), the other terms are exactly the same. Furthermore, since the precoding vector satisfies $\sum_{i=1}^{N_{\mathrm{t}}}|w_i|^2=1$, the array factor term is upper-bounded by N_{t} based on Cauchy inequality, which is given by

$$\begin{aligned}&\left|\sum_{i=1}^{N_{\mathrm{t}}}w_i(n_0T_{\mathrm{s}})\exp\Big\{-j2\pi\Big[f_0\frac{\mathcal{R}_i(\theta)}{c}-\Delta f_i(n_0T_{\mathrm{s}})\Big]\Big\}\right|^2\\&\le N_{\mathrm{t}}\sum_{i=1}^{N_{\mathrm{t}}}|w_i(n_0T_{\mathrm{s}})|^2=N_{\mathrm{t}}.\end{aligned}\tag{16}$$

Therefore, the maximum equivalent array gain of FDA is no difference from that of a conventional antenna array, i.e., by setting $\Delta f_i=0$. This leads that the FDA does not enhance the range security, which suggests the incorrect conclusion of previous studies on FDA [17], [18], [19], [20].

This conclusion can be further explained intuitively according to the principle of electromagnetic wave propagation. The carried symbols propagate at the speed of light, which has the same motion as the wavefront of the transmitted signal. Therefore, the beamforming gain corresponding to a symbol is determined by the beamforming pattern superimposed at the wavefront. An important fact about wavefronts is that the frequency of EM waves only determines the speed of phase shift between consecutive wavefronts, but the phase of one wavefront does not change. Without loss of generality, we suppose the phase of the wavefront emitted at time t is zero. Then, the wavefront phase emitted at time $t+\tau$ is given by $f\tau$. This phase of the wavefront does not change as it propagates outwards, which implies that changing the frequency of the antenna array, as FDA does, cannot affect the beamforming pattern superimposed by the wavefront. The signals superimposed at Bob can superimpose in the same pattern at Eve, and therefore it is useless to introduce a frequency offset among different antennas.

From the perspective of communication system, it is worth noticing that a synchronizer is a fundamental part of the receiver in a communication system. Unlike time-invariant

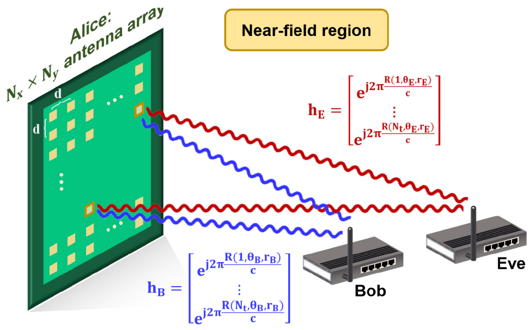

Alice: $N_x \times N_y$ antenna array
d
d
Near-field region
$\mathbf{h}_{\mathrm{E}} = \begin{bmatrix} e^{j2\pi\frac{R(1,\theta_E,r_E)}{c}} \\ \vdots \\ e^{j2\pi\frac{R(N_t,\theta_E,r_E)}{c}} \end{bmatrix}$
$\mathbf{h}_{\mathrm{B}} = \begin{bmatrix} e^{j2\pi\frac{R(1,\theta_B,r_B)}{c}} \\ \vdots \\ e^{j2\pi\frac{R(N_t,\theta_B,r_B)}{c}} \end{bmatrix}$
Bob
Eve

FIGURE 6. THz widely-spaced antenna array.

channels, the FDA system is not time-invariant, which makes it necessary to treat the synchronization problem carefully. Moreover, based on (14), we discover that the addition of a frequency offset Δf_i is equivalent with replacing $w_i(t)$ as $w_i(t) \cdot \exp\{-j2\pi\Delta f_i t\}$, i.e., adding the phase of the i^{th} antenna by $\Delta f_i t$. This reminds us of the equivalence of adding a constant frequency and a time-varying phase from the perspective of an EM wave. Therefore, except for the different hardware implementation methods, a constant-frequency antenna array with time-variable phase shifters is equivalent to an FDA. Therefore, FDA cannot address the range security problem that the traditional phase-shifter-based multiple-antenna techniques cannot address.

IV. OUR PROPOSED WIDELY-SPACED ANTENNA DESIGN FOR TERAHERTZ RANGE SECURITY

Motivated by our conclusion that multiple antenna techniques operating in the far-field regions fail to provide THz range security in Section III, we discover multiple-antenna techniques operating in near-field regions. In this section, we propose a THz WSA communication scheme to safeguard the THz range security. Specifically, We first develop the WSA model with hybrid beamforming and formulate a secrecy rate maximization problem. Then, we provide a hybrid beamforming design strategy for our WSA transmission scheme based on an NCOA algorithm. Finally, we analyze the trade-off between the enlarged antenna array size and the enhanced secrecy rate, which clarifies that the proposed scheme is realistic yet unique for THz band communications.

A. WIDELY-SPACED ARRAY AND HYBRID BEAMFORMING

The THz WSA model is illustrated in Fig. 6, where the spacing between antennas in the antenna array is widened such that the Alice-Bob distance and the Alice-Eve is comparable to the antenna size. The goal is that Bob and Eve can be located in the near-field region of the transmitter antenna array, and the closed-form expression for the residual propagation distance term in (5) can be expressed as

$$\mathcal{R}_i(\theta_{\mathrm{U}}, r_{\mathrm{U}}) = r_{\mathrm{U},i} - r_{\mathrm{U}} \tag{17a}$$

$$= \sqrt{(r_{\mathrm{U}}\sin\theta_{\mathrm{U}} - \mu_i)^2 + \nu_i^2 + r_{\mathrm{U}}^2\cos^2\theta_{\mathrm{U}}} - r_{\mathrm{U}}. \tag{17b}$$

Remarkably, (17b) is the ground-truth model, since it considers the spherical-wave propagation nature for EM waves.

For the beamformer design at the transmitter side, since traditional fully-digital beamformer structure brings tremendous hardware cost for THz communications with the same number of radio frequency (RF) chains as antennas, hybrid beamforming technology is therefore proposed as a promising yet lower-complexity structure for UM-UPA [27]. Specifically, the fully-connected hybrid beamforming structure is composed of a digital beamformer represented by $\mathbf{P}_{\mathrm{D}} \in \mathbb{C}^{N_{\mathrm{RF}}\times 1}$ and an analog beamformer expressed as $\mathbf{P}_{\mathrm{A}} \in \mathbb{C}^{N_{\mathrm{t}}\times N_{\mathrm{RF}}}$. Each element of the matrices $\mathbf{P}_{\mathrm{D}}$ and $\mathbf{P}_{\mathrm{A}}$ represents the complex gain from the baseband signal to the RF chain, and from the RF chain to the antenna via phase shifters, respectively. N_{RF} denotes the number of RF chains. The analog beamformer matrix is expressed in the form of

$$\mathbf{P}_{\mathrm{A}} = \frac{1}{\sqrt{N_{\mathrm{t}}}}\begin{pmatrix} e^{j\phi_{11}} & \dots & e^{j\phi_{1N_{\mathrm{RF}}}} \\ \vdots & \ddots & \vdots \\ e^{j\phi_{N_{\mathrm{t}}1}} & \dots & e^{j\phi_{N_{\mathrm{t}}N_{\mathrm{RF}}}} \end{pmatrix}, \tag{18}$$

where $\phi_{pq} \in [0, 2\pi), p \in \{1, \dots, N_{\mathrm{t}}\}, q \in \{1, \dots, N_{\mathrm{RF}}\}$ denotes the phase output of the phase shifter which connects the p^{th} RF chain with the q^{th} antenna. We assume that the hybrid beamforming does not affect the transmit power, i.e., $|\mathbf{P}_{\mathrm{A}}\mathbf{P}_{\mathrm{D}}|^2 = 1$. The overall normalized beamforming vector is denoted by $\mathbf{w} = \mathbf{P}_{\mathrm{A}}\mathbf{P}_{\mathrm{D}}$. We assume that the carrier frequency of each antenna in the WSA is uniform and denoted as f_0. The received signal at the receiving node U after down-converting and synchronization of symbol n_0 can be expressed as

$$y_{\mathrm{U}}(n_0, \theta_{\mathrm{U}}, r_{\mathrm{U}}) = \sqrt{\frac{P}{T_{\mathrm{s}}}} s_{n_0} a(r_{\mathrm{U}}) \sum_{i=1}^{N_{\mathrm{t}}} w_i e^{j2\pi f_0 \frac{\mathcal{R}_i(\theta_{\mathrm{U}}, r_{\mathrm{U}})}{c}} + n(t), \tag{19}$$

or equivalently we can express the received signal in vector form as

$$y_{\mathrm{U}}(n_0, \theta_{\mathrm{U}}, r_{\mathrm{U}}) = \sqrt{\frac{P}{T_{\mathrm{s}}}} s_{n_0} a(r_{\mathrm{U}}) \mathbf{w}^T \mathbf{h}_{\mathrm{U}} + n(t), \tag{20}$$

where the array steering vector $\mathbf{h}_{\mathrm{U}}$ is expressed as

$$\mathbf{h}_{\mathrm{U}} = \left[e^{j2\pi\frac{\mathcal{R}_1(\theta_{\mathrm{U}}, r_{\mathrm{U}})}{c}}, \dots, e^{j2\pi\frac{\mathcal{R}_{N_{\mathrm{t}}}(\theta_{\mathrm{U}}, r_{\mathrm{U}})}{c}} \right]^T. \tag{21}$$

B. PROBLEM FORMULATION: SECRECY RATE MAXIMIZATION

The secrecy rate, defined as the capacity difference between Bob's and Eve's channels, is used as the performance metric of our THz system model. As the focus of our THz secure communication system, the aim is to design transmit power P, hybrid beamformer, i.e., $\mathbf{P}_{\mathrm{A}}$ and $\mathbf{P}_{\mathrm{D}}$, to maximize the secrecy rate. Thus, we formulate the hybrid secure beamforming design problem as a secrecy rate maximization (SRM) optimization problem $\mathbf{Q}_1$ as

$$\max_{P,\mathbf{P}_\mathrm{D},\mathbf{P}_\mathrm{A}} \ R_s = \left[\log\left(1+\frac{P|\mathbf{w}^\dagger\mathbf{h}_\mathrm{B}|^2 a(r_\mathrm{B})^2}{\sigma^2}\right) - \log\left(1+\frac{P|\mathbf{w}^\dagger\mathbf{h}_\mathrm{E}|^2 a(r_\mathrm{E})^2}{\sigma^2}\right)\right]^+ \quad (22a)$$

$$\text{s.t.} \quad P \le P_\mathrm{Tx}, \quad (22b)$$

$$|\mathbf{P}_\mathrm{A}\mathbf{P}_\mathrm{D}|^2 = 1, \quad (22c)$$

$$\mathbf{P}_\mathrm{A} = \frac{1}{\sqrt{N_\mathrm{t}}}\begin{pmatrix} e^{j\phi_{11}} & \cdots & e^{j\phi_{1N_\mathrm{RF}}} \\ \vdots & \ddots & \vdots \\ e^{j\phi_{N_\mathrm{t}1}} & \cdots & e^{j\phi_{N_\mathrm{t}N_\mathrm{RF}}} \end{pmatrix}, \quad (22d)$$

where (22a) denotes the secrecy rate of the THz secure communication system. Equation (22b) states the transmit power constraint with the maximum power P_Tx. Equation (22c) describes the normalization constraint of a hybrid beamformer. The maximal secrecy rate is denoted by R_s^opt and the optimal transmit beamformer is represented by $\mathbf{w}^\mathrm{opt} = [\mathbf{P}_\mathrm{A}^\mathrm{opt}\mathbf{P}_\mathrm{D}^\mathrm{opt}]$. Solving the problem $\mathbf{Q}_1$ yields the optimal hybrid beamforming strategy achieving maximum secrecy. Due to the non-convexity of (22a) with respect to $\mathbf{w}$, the optimization problem $\mathbf{Q}_1$ is non-convex and cannot be tackled directly. Remarkably, according to (21), for the range security problem where $\theta_\mathrm{B} = \theta_\mathrm{E}$, if the far-field approximation $\mathcal{R}_i(\theta_\mathrm{U}, r_\mathrm{U}) \approx -(i_\mathrm{row}-1)d\sin\theta_\mathrm{U}$ is applied, we have $\mathcal{R}_i(\theta_\mathrm{B}, r_\mathrm{B}) = \mathcal{R}_i(\theta_\mathrm{E}, r_\mathrm{E})$. In such case, Bob's and Eve's channels are perfectly correlated, i.e., $\mathbf{h}_\mathrm{B} = \mathbf{h}_\mathrm{E}$. As a result, their beamforming gains satisfy $|\mathbf{w}^\dagger\mathbf{h}_\mathrm{B}|^2 = |\mathbf{w}^\dagger\mathbf{h}_\mathrm{E}|^2$. Therefore, by considering that $|\mathbf{w}^\dagger\mathbf{h}_\mathrm{U}|^2 \in [0, N_\mathrm{t}]$, the maximum secrecy rate is upper bounded by $\log(1+\frac{P_\mathrm{Tx}N_\mathrm{t}a(r_\mathrm{B})^2}{\sigma^2}) - \log(1+\frac{P_\mathrm{Tx}N_\mathrm{t}a(r_\mathrm{E})^2}{\sigma^2})$, which is exactly the maximum secrecy rate without adopting any security technique.

C. HYBRID BEAMFORMING DESIGN: NCOA ALGORITHM

We design a hybrid beamformer to maximize the secrecy rate in (22a) for our WSA transmission scheme. Given the transmission distances r_B and r_E, solving the SRM problem $\mathbf{Q}_1$ yields our hybrid beamformer design. We propose an NCOA algorithm to solve this non-convex problem. First, we temporarily relax the non-convex constraint to transform $\mathbf{Q}_1$ into a convex optimization problem $\mathbf{Q}_2$. We discover that by doing this the original optimization problem becomes a Rayleigh Quotient maximization problem, and a globally optimal solution $\tilde{\mathbf{w}}$ to $\mathbf{Q}_2$ can be then derived, referred to as the non-constrained optimum. However, this solution does not necessarily meets the hybrid beamforming constraints. Therefore, we should finally reconsider the non-convex constraint and find an epsilon-convergent sub-optimal solution by approaching $\tilde{\mathbf{w}}$.

1) PROBLEM TRANSFORMATION AND NON-CONSTRAINED OPTIMAL SOLUTION

We first temporarily neglect the constraint (22d). As a result, the remaining problem is converted to a convex optimization problem where a global optimum can be derived in a closed form. By maximizing the transmit power $P = P_\mathrm{Tx}$ and allowing the condition that $|\mathbf{w}|^2 = 1$, the secrecy rate in (22a) is calculated as

$$R_s = \log\left[1 + \frac{\mathbf{w}^\dagger\left(\mathbf{h}_\mathrm{B}\mathbf{h}_\mathrm{B}^\dagger a(r_\mathrm{B})^2 - \mathbf{h}_\mathrm{E}\mathbf{h}_\mathrm{E}^\dagger a(r_\mathrm{E})^2\right)\mathbf{w}}{\mathbf{w}^\dagger\left(\frac{\sigma^2}{P_\mathrm{Tx}}\mathbf{I} + \mathbf{h}_\mathrm{E}\mathbf{h}_\mathrm{E}^\dagger \cdot a(r_\mathrm{E})^2\right)\mathbf{w}}\right], \quad (23)$$

where $\mathbf{I} \in \mathbb{R}^{N_\mathrm{t}\times N_\mathrm{t}}$ represents a $N_\mathrm{t} \times N_\mathrm{t}$ identity matrix. Let $\mathbf{A} \triangleq \mathbf{h}_\mathrm{B}\mathbf{h}_\mathrm{B}^\dagger a(r_\mathrm{B})^2 - \mathbf{h}_\mathrm{E}\mathbf{h}_\mathrm{E}^\dagger a(r_\mathrm{E})^2$ and $\boldsymbol{B} \triangleq \frac{\sigma^2}{P_\mathrm{Tx}}\mathbf{I} + \mathbf{h}_\mathrm{E}\mathbf{h}_\mathrm{E}^\dagger a(r_\mathrm{E})^2$, maximizing R_s is equivalent to maximizing the generalized Rayleigh quotient $\lambda_\Sigma \triangleq \frac{\mathbf{w}^\dagger\mathbf{A}\mathbf{w}}{\mathbf{w}^\dagger\boldsymbol{B}\mathbf{w}}$. The transformation of the optimization problem from $\mathbf{Q}_1$ to $\mathbf{Q}_2$ is depicted in the following theorem.

Theorem 1: The SRM problem $\boldsymbol{Q}_1$ without the non-convex constraint (22c) is equivalent to the problem $\boldsymbol{Q}_2$

$$\boldsymbol{Q}_2 : \max_{\mathbf{w}} \ \lambda_\Sigma = |\langle\mathbf{w}', \mathbf{v}^{(a)}\rangle|^2\lambda_a + |\langle\mathbf{w}', \mathbf{v}^{(b)}\rangle|^2\lambda_b \quad (24a)$$

$$|\mathbf{w}|^2 = 1, \quad (24b)$$

where $\mathbf{w}' = \frac{\boldsymbol{B}^{1/2}\mathbf{w}}{|\boldsymbol{B}^{1/2}\mathbf{w}|}$, λ_a and λ_b denote the only two non-zero eigenvalues of the matrix $\boldsymbol{B}^{-\frac{1}{2}}\mathbf{A}\boldsymbol{B}^{-\frac{1}{2}}$ with $\lambda_a \ge \lambda_b$. $\mathbf{v}^{(a)}$ and $\mathbf{v}^{(b)}$ represent their corresponding normalized eigenvectors, respectively.

Proof: The detailed proof is provided in Appendix. ■

Since $|\langle\mathbf{w}', \mathbf{v}^{(a)}\rangle| \le |\langle\mathbf{v}^{(a)}, \mathbf{v}^{(a)}\rangle| = 1$, the non-constraint optimal solution to $\mathbf{Q}_2$ is achieved when $\mathbf{w}'$ coincides with the eigenvector of the maximum eigenvalue $\mathbf{v}^{(a)}$. This leads the non-constrained optimal solution as

$$\tilde{\mathbf{w}} = \frac{\boldsymbol{B}^{-\frac{1}{2}}\mathbf{v}^{(a)}}{||\boldsymbol{B}^{-\frac{1}{2}}\mathbf{v}^{(a)}||}, \quad \lambda_\Sigma = \lambda_a, \quad R_s = \log_2(1+\lambda_a), \quad (25)$$

where setting the beamforming matrix as $\tilde{\mathbf{w}}$ achieves the maximum secrecy rate without any constraints, which is an upper bound for the secrecy rate maximization problem $\mathbf{Q}_1$.

2) NCOA ALGORITHM

Given the non-constrained optimal solution $\tilde{\mathbf{w}}$ obtained in (25), our aim is to approach $\mathbf{w} = [\mathbf{P}_\mathrm{A}^\mathrm{opt}\mathbf{P}_\mathrm{D}^\mathrm{opt}]$ to $\tilde{\mathbf{w}}$ under the analog beamforming constraint (22d). In [27], it is shown that when $N_\mathrm{RF} \ge 2$, there exists a solution P_A and $\mathbf{P}_\mathrm{D}$ that satisfies $[\mathbf{P}_\mathrm{A}\mathbf{P}_\mathrm{D}] = \tilde{\mathbf{w}}$. Therefore, we divide the two cases, (i) the hybrid beamforming case where $N_\mathrm{RF} \ge 2$, and (ii) the fully-analog (FA) beamforming case where $N_\mathrm{RF} = 1$, as follows.

Case (i): For the hybrid beamforming case $N_\mathrm{RF} \ge 2$, fortunately, it is possible to discover a feasible solution satisfying the constraint (22d) and $\tilde{\mathbf{w}} = [\mathbf{P}_\mathrm{A}\mathbf{P}_\mathrm{D}]$, which is expressed as

$$\mathbf{P}_\mathrm{A}^\mathrm{HB} = \left[e^{j\angle\tilde{\mathbf{w}}+\arccos\frac{||\tilde{\mathbf{w}}||}{2}}, e^{j\angle\tilde{\mathbf{w}}-\arccos\frac{||\tilde{\mathbf{w}}||}{2}}, 0, \ldots, 0\right], \quad (26a)$$

$$\mathbf{P}_\mathrm{D}^\mathrm{HB} = \frac{1}{\sqrt{2}}[1, 1, 0, \ldots, 0]^T, \quad (26b)$$

where $\angle(\cdot)$ returns the angle of the input complex element. By setting the hybrid beamformer as (26), the non-constrained optimal solution can be achieved, and the secrecy rate performance of the hybrid beamforming is maximized. According to (26), it is worth noticing that by using the first two RF chains, the hybrid beamforming achieves the optimal performance, and using more than two RF chains cannot further improve the secrecy rate. This is consistent with an intuitive understanding that for one Tx and two single-antenna Bob and Eve with LoS transmissions, there are two SDoFs, which are equal to the DoF between Alice and Bob plus the DoF between Alice and Eve. Therefore, with two or more RF chains exceeding the number of SDoFs, the WSA communication system cannot further benefit from the increased RF chains.

Case (ii): For the fully-analog beamforming case with $N_{\mathrm{RF}} = 1$, since $\mathbf{P}_{\mathrm{D}}^{\mathrm{FA}}$ is a 1×1 scalar number, we set $\mathbf{P}_{\mathrm{D}}^{\mathrm{FA}} = 1$ without loss of generality. Then, the solution $\mathbf{P}_{\mathrm{A}}^{\mathrm{FA}} = \tilde{\mathbf{w}}$ does not satisfy the constraint in (22d). We use a gradient descent algorithm to recursively approach the optimal solution, where the gradient of the term (24a) versus $\mathbf{P}_{\mathrm{A}}$ is represented by

$$\nabla \mathbf{P}_{\mathrm{A}}^{\mathrm{FA}} = \left[\frac{\partial \lambda_\Sigma}{\partial \phi_1}, \ldots, \frac{\partial \lambda_\Sigma}{\partial \phi_{N_{\mathrm{t}}}}\right]^T, \tag{27}$$

where the term $\frac{\partial \lambda_\Sigma}{\partial \phi_i}$ is expressed as

$$\frac{\partial \lambda_\Sigma}{\partial \phi_i} = -\frac{2}{\sqrt{N_{\mathrm{t}}}} \sum_{k \in \{a,b\}} \mathrm{Re}\left(\mathbf{v}_k^{\boldsymbol{B}\dagger} \mathbf{P}_{\mathrm{A}}^{\mathrm{FA}} \mathbf{e}^{-j\phi_i} \mathbf{e}_i \mathbf{v}_k^{\boldsymbol{B}}\right) \lambda_k, \tag{28}$$

where $\mathbf{v}_k^{\boldsymbol{B}} = \frac{\boldsymbol{B}^{-1/2}\mathbf{v}^{(k)}}{||\boldsymbol{B}^{-1/2}\mathbf{v}^{(k)}||}$, and the vector $\mathbf{e}_i = [0, \ldots, 0, 1, 0, \ldots, 0]$ with the one in the i^{th} column, $\mathrm{Re}(\cdot)$ returns the real part of a complex number. By recursively updating $\mathbf{P}_{\mathrm{A}}^{\mathrm{FA}}$ via computing the gradient in each step, a near-optimal solution for the fully-analog case can be achieved.

By combining the two solutions for the hybrid beamforming ($N_{\mathrm{RF}} \geq 2$) and fully-analog beamforming ($N_{\mathrm{RF}} = 1$) cases, the NCOA algorithm for the hybrid beamforming design is summarized in Algorithm 1. ϵ denotes the step parameter controlling the convergence speed, and δ is the convergence threshold determining the convergence destination. In this work, we choose $\epsilon = 10$ rad and $\delta = 0.003$, which results in good convergence performance. By applying WSA communications for range security and considering the narrow beam nature with a UM-UPA, the range security for THz communications is thereby ensured.

D. DESIGN TRADE-OFF BETWEEN ARRAY SIZE AND OPTIMAL SECRECY RATE

When our proposed method is applied to far-field communications, the largest eigenvalue λ_a approaches to zero when $r_{\mathrm{E}} \leq r_{\mathrm{B}}$, which implies that the secrecy rate of the CSA-based method is upper-bounded by zero. An ensuing drawback of the WSA-based method is the increased array size. However, thanks to the millimeter down to sub-millimeter THz wavelength, the THz WSA structure can maintain a reasonable array size. A sample comparison between the mmWave and THz WSA designs is provided as follows. For a 4×4 micro-wave communication system where the wavelength is on the order of sub-meters, e.g., 0.3 m for the 1 GHz system, the near-field expression in (17b) is valid when the side length of the array $3d \approx 4.0$ m, which is an impractically large antenna array. However, for THz communications, with a wavelength on the order of millimeter, e.g., 1 mm for a 300 GHz system, the near-field expression is valid when $3d \approx 0.08$ m. Therefore, a 0.08 m $\times$ 0.08 m THz antenna array can well accommodate the near-field communication requirement.

Algorithm 1 NCOA Algorithm

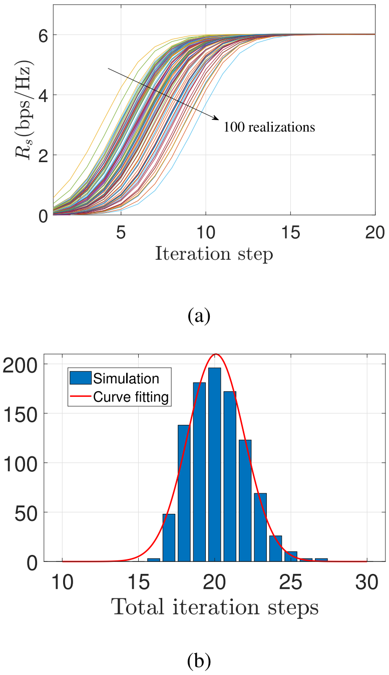
```
Step 1: eigenvalue decomposition (EVD)
    Compute the channel matrix $\mathbf{C} = \boldsymbol{B}^{-\frac{1}{2}}\mathbf{A}\boldsymbol{B}^{-\frac{1}{2}}$;
    Perform EVD on $\mathbf{C}$ to get $\lambda_a$, $\lambda_b$, $\mathbf{v}^{(a)}$, and $\mathbf{v}^{(b)}$;
Step 2: NCOA
    Case (i): If $N_{\mathrm{RF}} \geq 2$,
        Compute $\mathbf{P}_{\mathrm{A}}^{\mathrm{HB}}$,$\mathbf{P}_{\mathrm{D}}^{\mathrm{HB}}$ according to (26);
        $\lambda_\Sigma$ according to (24a);
        $P^{\mathrm{opt}} = P_{\mathrm{Tx}}$, $\mathbf{P}_{\mathrm{A}}^{\mathrm{opt}} = \mathbf{P}_{\mathrm{A}}^{\mathrm{HB}}$, $\mathbf{P}_{\mathrm{D}}^{\mathrm{opt}} = \mathbf{P}_{\mathrm{D}}^{\mathrm{HB}}$;
        $R_s^{\mathrm{opt}} = \log(1 + \lambda_\Sigma)$;
    Case (ii): If $N_{\mathrm{RF}} = 1$,
        $\mathbf{P}_{\mathrm{D}}^{\mathrm{FA}} = 1$;
        Randomly initialize $\mathbf{P}_{\mathrm{A,0}}^{\mathrm{FA}}$, and compute $\lambda_{\Sigma,0}$;
        repeat
            Compute $\nabla \mathbf{P}_{\mathrm{A,i}}^{\mathrm{FA}}$ and $\lambda_{\Sigma,i}$ according to (27);
            Update $\mathbf{P}_{\mathrm{A,i+1}}^{\mathrm{FA}} \leftarrow \mathbf{P}_{\mathrm{A,i}}^{\mathrm{FA}} + \epsilon \nabla \mathbf{P}_{\mathrm{A,i}}^{\mathrm{FA}}$;
            Compute $\lambda_{\Sigma,i+1}$;
            $i \leftarrow i + 1$;
        until $\frac{|\lambda_{\Sigma,i+1} - \lambda_{\Sigma,i}|}{|\lambda_{\Sigma,i}|} < \delta$;
        $P^{\mathrm{opt}} = P_{\mathrm{Tx}}$, $\mathbf{P}_{\mathrm{A}}^{\mathrm{opt}} = \mathbf{P}_{\mathrm{A,i+1}}^{\mathrm{FA}}$, $\mathbf{P}_{\mathrm{D}}^{\mathrm{opt}} = 1$;
        $R_s^{\mathrm{opt}} = \log(1 + \lambda_{\Sigma,i+1})$;
```

V. NUMERICAL RESULTS

In this section, we evaluate the numerical results of the THz WSA scheme. First, we conduct Monte Carlo simulations on our recursion-based NCOA algorithm and demonstrate its convergence performance. Second, we analyze how system parameters, including the maximum transmit power, antenna spacing, and transmission distances affect the maximum secrecy rate. Moreover, the robustness of the proposed WSA scheme is studied, i.e., how the maximum secrecy rate degrades with the estimation error of the location of the Eve. Finally, the proposed scheme is compared with existing algorithms to demonstrate its improved range security performance. Unless specified, the system parameters used in the simulation are described in Table 2. Note that the distances are of several meters due to the limited range of the near-field regions at the THz frequencies.

TABLE 2. Simulation parameters.

Notation	Definition	Value	Unit
P_{Tx}	Maximum transmit power	10	dBm
N_{x}	Number of row antennas	32	-
N_{y}	Number of column antennas	32	-
σ^2	Noise variance	-80	dBm
θ	Propagation angle	$\pi/6$	rad
f	Carrier frequency	300	GHz
r_{B}	Alice-Bob distance	10	m
r_{E}	Alice-Eve distance	5	m
ϵ	Step parameter	10	rad
δ	Convergence threshold	0.003	-



(a)

(b)

FIGURE 7. The Monte Carlo simulation on the convergence analysis of NCOA algorithm. (a) Convergence performance (100 simulations for illustration); (b) Statistical result of total iteration steps until convergence.

A. CONVERGENCE AND COMPLEXITY ANALYSIS OF THE NCOA ALGORITHM

We analyze the convergence and the computational complexity of the entire algorithm. We perform Monte Carlo simulations on the initial value of $\mathbf{P}_{\text{A},0}^{\text{FA}}$ in step 9 of Algorithm 1. By setting 1,000 different random initial values, the secrecy rate versus the number of iterations is depicted in Fig. 7. Figure 7(a) shows that all simulations achieve nearly the same maximum secrecy rate within 20 iterations, which implies good convergence performance. Fig. 7(b) presents statistical analysis on the distribution of the total number of iterations until convergence. Among 1,000 simulations, a Gaussian distribution with a mean of 20 is fitted, while no alias effect occurs.

In Fig. 8, we explore how the step parameter ϵ in step 12 in Algorithm 1 affects the maximum secrecy rate and the total iteration step reaching the termination condition. We can observe that when $\epsilon < 20$, the mean secrecy rate approximately reaches the maximum value. By contrast, when $\epsilon > 20$, the mean secrecy rate decays rapidly. Moreover, the number of total iteration steps decreases as ϵ increases, as the right y-axis of Fig. 8 presents. The numerical results demonstrate that setting ϵ within [10, 20] results in a good balance between performance and complexity.

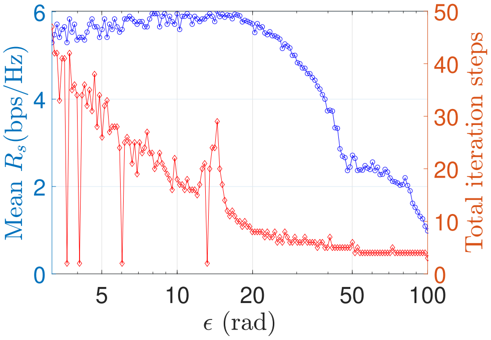


FIGURE 8. Mean secrecy rate and total iteration steps versus step parameter ϵ.

The running time of the proposed algorithm is shown in Fig. 11, where the running time of step 1 and step 2 versus the different transmit antenna array sizes are computed and compared. We can observe that the running time of the step 2 is approximately 10ms for a 1024×1024 antenna array, while the dominant process is the matrix inverse operation in step 1.

B. MAXIMUM SECRECY RATE

We compute the maximum secrecy rate versus different system parameters for our proposed WSA scheme for THz range security. The maximum secrecy rates with different maximum transmit power values are shown in Fig. 9(a) for the different antenna spacing, in Fig. 9(b) for the different eavesdropping distances, and in Fig. 9(c) for the different antenna array sizes. In general, the secrecy rate increases with a wider antenna spacing, a nearer Eve distance, and larger array size. Moreover, with $d = 5\lambda$, $r_{\text{E}} = 5$ m, and $N_{\text{t}} = 1024$, the secrecy rate with maximum transmit power of 10 dBm is 6 bps/Hz. An interesting phenomenon captured in Fig. 9(b) is that as r_{E} becomes smaller, i.e., Eve approaches the Tx, the secrecy shows an increasing trend. This is explained that when Eve is nearer to Alice or, equivalently, farther from the B, Eve's channel is more uncorrelated with Bob's channel, which enhances the secrecy rate though Eve's channel gain increases.

C. ROBUSTNESS TO LOCATION ESTIMATION ERROR OF EAVESDROPPERS

The proposed NCOA algorithm needs to acquire Eve's location, i.e., the Alice-Eve distance and angle, and we estimate these two values as the input of our beamformer design. Therefore, we need to study the robustness of our scheme to the location estimation error of Eve, i.e., the robustness of the Alice-Eve distance and angle. The estimation error

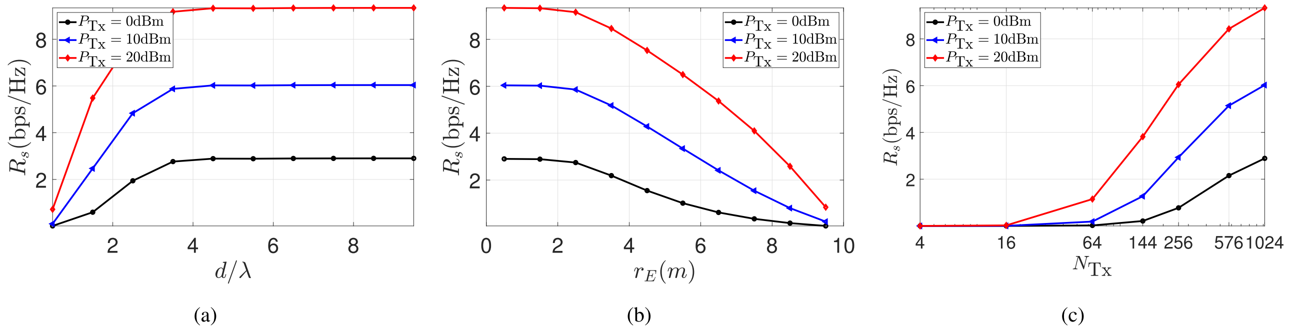


FIGURE 9. Secrecy rate versus different system parameters ($N_{\mathrm{RF}} = 2$). (a) With varying antenna spacing d. (b) With varying Alice-Eve distance r_{E}. (c) With varying array size N_{t}.

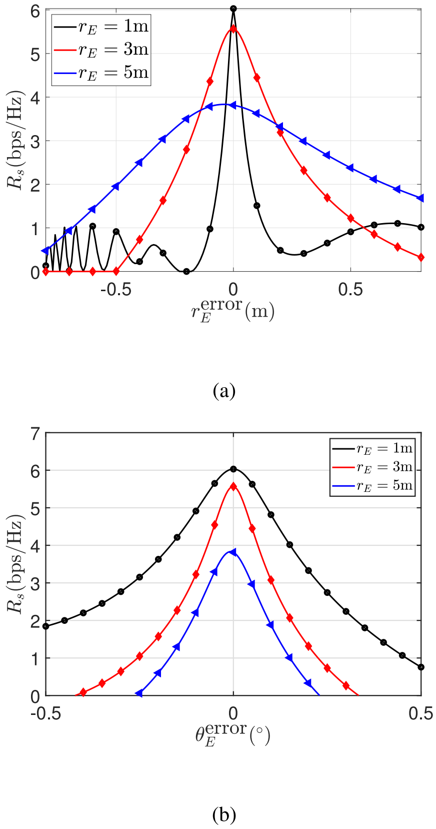


FIGURE 10. Robustness of secrecy rate to the location estimation error of Eve's position. (a) Secrecy rate versus the distance estimation error $r_{\mathrm{E}}^{\mathrm{error}}$. (b) Secrecy rate versus the angle estimation error $\theta_{\mathrm{E}}^{\mathrm{error}}$.

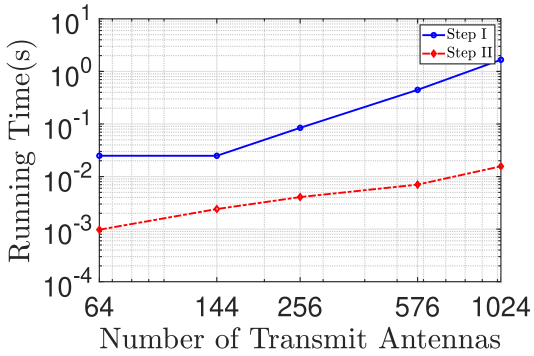
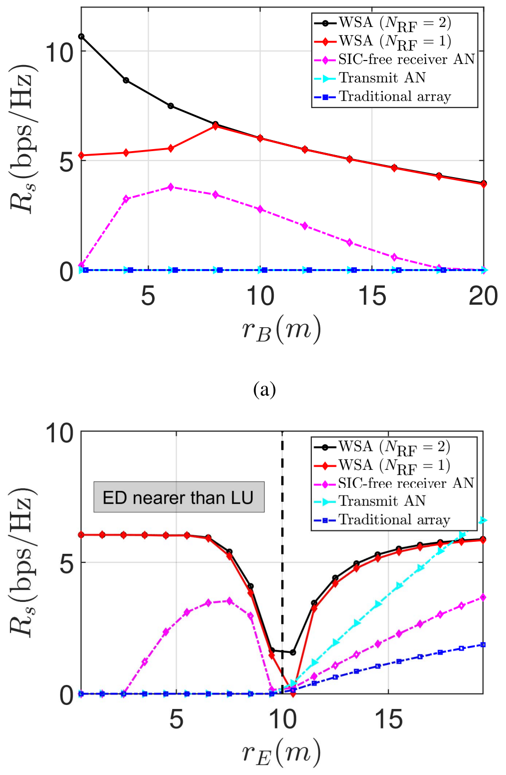


FIGURE 11. Running time of the proposed algorithm.

is defined as the difference between the estimated value and the nominal value, and the estimation errors of the Alice-Eve distance and angle are denoted as $r_{\mathrm{E}}^{\mathrm{error}}$ and $\theta_{\mathrm{E}}^{\mathrm{error}}$, respectively. The maximum secrecy rates versus $r_{\mathrm{E}}^{\mathrm{error}}$ and $\theta_{\mathrm{E}}^{\mathrm{error}}$ are plotted in Fig. 10. In our simulations, r_{E} denotes the true Alice-Eve distance. In Fig. 10(a), we observe that the secrecy rate degrades dramatically as the Alice-Eve distance estimation error increases. Moreover, as r_{E} decreases, the degradation becomes severer with the estimation error at short transmission distances. This can be explained that at short distances, a small distance estimation error leads to a large phase error on each antenna. In Fig. 10(b), we observe that for the different Alice-Eve distances, the maximum secrecy rate degrades by 10% when the Alice-Eve angle has a ±0.03° error. This result implies that the robustness of the WSA communication scheme to the Alice-Eve estimation error is highly dependent on the Alice-Eve distance. Moreover, it is suggested that the estimation error of the Alice-Eve angle should be less than 0.03° to ensure a less than 10% secrecy rate degradation.

D. PERFORMANCE COMPARISON WITH DIFFERENT METHODS

We evaluate and compare the maximum secrecy rate achieved by our proposed WSA scheme with existing schemes in the literature. Specifically, the TAN scheme [19], the SIC-free RAN scheme [9], and traditional CSA-based method [27] are compared in Fig. 12. In Fig. 12(a), the secrecy rate versus the Alice-Bob distance is plotted. For the $N_{\mathrm{RF}} \geq 2$ case, the maximum secrecy rate decreases as r_{B} increases. At $r_{\mathrm{B}} = 10$ m, the secrecy rate achieves 6 bps/Hz. The secrecy rate of the $N_{\mathrm{RF}} \geq 1$ case, as an inferior but low-complexity architecture of the $N_{\mathrm{RF}} = 2$ case, can achieve near-optimal performance when r_{B} is larger than 8 m. This implies that the performance degradation due to the sub-optimality of hybrid beamforming becomes severer when the distance between Alice and Bob is small. Moreover, compared with the SIC-free RAN scheme [9], the proposed WSA scheme can double the secrecy rate at $r_{\mathrm{B}} = 10$ m. This significant improvement originates from the different security-enhancing strategies used by the two schemes. Specifically, the WSA scheme directly mitigates the received power by Eve, while the SIC-free RAN is to



(a)

(b)

FIGURE 12. **Performance comparison between different methods. (a) With varying Alice-Bob distance r_{B}. (b) With varying Alice-Eve distance r_{E}.**

jam Eve's signal. We observe that the secrecy rates achieved by the TAN scheme and traditional hybrid beamforming are nearly zero, which is consistent with our analysis in Section IV-B that the secure communication in the far field fails to achieve a positive secrecy rate.

In Fig. 12(b), we plot the maximum secrecy rate versus the different Alice-Eve distances varying from 0.5 m to 20 m, where the Alice-Bob distance is 10 m. We see that when r_{E} increases from 0.5 m to 10 m, the secrecy rate of WSA scheme decreases as r_{E} increases. Moreover, the secrecy rate increases as r_{E} increases when r_{E} is larger than 10 m. This is due to the fact that as r_{E} approaches 10 m, Bob's channel and the Eve's channel become correlated, which leads that the WSA scheme cannot distinguish the two receivers in the range domain. Moreover, the WSA scheme with two RF chains can achieve the secrecy rate of approximately 6 bps/Hz, as r_{E} approaches zero. However, this does not imply that the proposed scheme can effectively combat the extremely near eavesdropping since the robustness against the Alice-Eve distance estimation error degrades significantly as r_{E} approaches zero.

VI. CONCLUSION

This paper investigates the multiple-antenna technologies for THz range security, including the FDA and WSA. Specifically, we first present a multiple-antenna-assisted THz range security model and theoretically derive the secrecy capacity of multiple antenna channels. We prove that the secrecy capacity for Bob and Eve in the far-field region is equal to the secrecy rate achieved by traditional beamforming schemes. Based on this conclusion, we revisited and revised the FDA range security model. Then, we proposed a WSA scheme and a hybrid beamforming design to enhance the secrecy rate. The WSA transmission is realized by increasing the antenna spacing to place Bob and Eve in the near-field region of the antenna array. For the optimal hybrid beamformer design, we develop an NCOA algorithm to achieve the closed-form optimal solution for the hybrid beamforming case and an epsilon-convergent sub-optimal solution for the fully-analog beamforming case, respectively. Numerical results verify the outstanding convergence of the NCOA algorithm and demonstrate that under the range security condition, the secrecy rate of the WSA communication scheme reaches 6 bps/Hz with 10 dBm transmit power.

APPENDIX
PROOF OF THEOREM 1

Due to the monotonicity of the logarithmic function, Maximizing R_s in (22a) is equivalent to maximizing $\frac{\mathbf{w}^\dagger\mathbf{A}\mathbf{w}}{\mathbf{w}^\dagger\boldsymbol{B}\mathbf{w}}$. We have $\mathbf{x}^\dagger\boldsymbol{B}\mathbf{x} = \frac{\sigma^2}{P_{\text{Tx}}}|\mathbf{x}|^2+|\mathbf{h}_{\text{E}}^\dagger\mathbf{x}|^2\cdot a(r_{\text{E}})^2 > 0$, so $\boldsymbol{B}$ is positive definite and $\boldsymbol{B}^{-\frac{1}{2}}$ exists. Thus, we can assume $\mathbf{w}' = \frac{\boldsymbol{B}^{1/2}\mathbf{w}}{|\boldsymbol{B}^{1/2}\mathbf{w}|}$ and $\mathbf{C} = \boldsymbol{B}^{-\frac{1}{2}}\mathbf{A}\boldsymbol{B}^{-\frac{1}{2}}$, we have $\frac{\mathbf{w}^\dagger\mathbf{A}\mathbf{w}}{\mathbf{w}^\dagger\boldsymbol{B}\mathbf{w}} = \mathbf{w}'^\dagger\mathbf{C}\mathbf{w}'$. We denote the two eigenvalues as λ_a and λ_b with their corresponding eigenvectors $\mathbf{v}^{(a)}$ and $\mathbf{v}^{(b)}$.

Next, we decompose the vector $\mathbf{w}'$ onto the orthonormal basis, composed of all normalized eigenvectors of $\mathbf{C}$ denoted by $\{\mathbf{v}^{(i)}\}$, $i = 1, \ldots, N_{\text{t}}$. As $\mathbf{w}' = \sum_{i=1}^{N_{\text{t}}}\langle\mathbf{w}', \mathbf{v}^{(i)}\rangle\mathbf{v}^{(i)}$,

$$\begin{aligned}\mathbf{w}'^\dagger\mathbf{C}\mathbf{w}' &= \sum_{i=1}^{N_{\text{t}}}\langle\mathbf{w}', \mathbf{v}^{(i)}\rangle\mathbf{v}^{(i)}\mathbf{C}\sum_{j=1}^{N_{\text{t}}}\langle\mathbf{w}', \mathbf{v}^{(j)}\rangle\mathbf{v}^{(j)} \\ &= |\langle\mathbf{w}', \mathbf{v}^{(a)}\rangle|^2\lambda_a + |\langle\mathbf{w}', \mathbf{v}^{(b)}\rangle|^2\lambda_b, \end{aligned} \tag{29}$$

which completes the proof. ■

REFERENCES

[1] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020.

[2] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.

[3] I. F. Akyildiz, C. Han, Z. Hu, S. Nie, and J. M. Jornet, "Terahertz band communication: An old problem revisited and research directions for the next decade," *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4250–4285, Jun. 2022.

[4] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," *Phys. Commun.*, vol. 12, pp. 16–32, Sep. 2014.

[5] J. Ma et al., "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018.

[6] C. Han, W. Gao, N. Yang, and J. M. Jornet, "Molecular absorption effect: A double-edged sword of terahertz communications," *IEEE Wireless Commun.*, vol. 30, no. 4, pp. 140–146, Aug. 2023.

[7] S. R. Aghdam, A. Nooraiepour, and T. M. Duman, "An overview of physical layer security with finite-alphabet signaling," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1829–1850, 2nd Quart., 2018.

[8] W. Gao, Y. Chen, C. Han, and Z. Chen, "Distance-adaptive absorption peak modulation (DA-APM) for terahertz covert communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 2064–2077, Mar. 2021.

[9] W. Gao, C. Han, and Z. Chen, "DNN-powered SIC-free receiver artificial noise aided terahertz secure communications with randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 563–576, Jan. 2022.

[10] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5G networks," in *Proc. IEEE INFOCOM*, 2019, pp. 865–872.

[11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[13] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2016.

[14] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[15] A. Bereyhi, S. Asaad, R. R. Müller, R. F. Schaefer, G. Fischer, and H. V. Poor, "Securing massive MIMO systems: Secrecy for free with low-complexity architectures," *IEEE Trans. Wireless Commun.*, vol. 20, no. 9, pp. 5831–5845, Sep. 2021.

[16] A. Bereyhi, S. Asaad, R. R. Müller, R. F. Schaefer, and H. V. Poor, "Secure transmission in IRS-assisted MIMO systems with active eavesdroppers," in *Proc. IEEE Asilomar Conf. Signals, Syst., Comput.*, 2020, pp. 718–725.

[17] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[18] T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.

[19] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[20] B. Ning et al., "Joint power allocation and passive beamforming design for IRS-assisted physical-layer service integration," *IEEE Trans. Wireless Commun.*, vol. 20, no. 11, pp. 7286–7301, Nov. 2021.

[21] C.-Y. Yeh and E. W. Knightly, "Eavesdropping in massive MIMO: New vulnerabilities and countermeasures," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6536–6550, Oct. 2021.

[22] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[23] G. Chen, J. P. Coon, A. Mondal, B. Allen, and J. A. Chambers, "Performance analysis for multihop full-duplex IoT networks subject to poisson distributed interferers," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3467–3479, Apr. 2019.

[24] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Secret channel training to enhance physical layer security with a full-duplex receiver," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 2788–2800, 2018.

[25] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 671–684, 2018.

[26] C. Han, A. O. Bicen, and I. F. Akyildiz, "Multi-ray channel modeling and wideband characterization for wireless communications in the terahertz band," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2402–2412, May 2015.

[27] L. Yan, C. Han, and J. Yuan, "A dynamic array-of-subarrays architecture and hybrid precoding algorithms for terahertz wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 9, pp. 2041–2056, Sep. 2020.

[28] B. Peng, K. Guan, A. Kuter, S. Rey, M. Patzold, and T. Kuerner, "Channel modeling and system concepts for future terahertz communications: Getting ready for advances beyond 5G," *IEEE Veh. Technol. Mag.*, vol. 15, no. 2, pp. 136–143, Jun. 2020.

[29] Y. Chen, L. Yan, C. Han, and M. Tao, "Millidegree-level direction-of-arrival estimation and tracking for terahertz ultra-massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 21, no. 2, pp. 869–883, Feb. 2022.

[30] N. J. Myers and R. W. Heath, "InFocus: A spatial coding technique to mitigate misfocus in near-field LoS beamforming," *IEEE Trans. Wireless Commun.*, vol. 21, no. 4, pp. 2193–2209, Apr. 2022.

[31] Y. Chen, L. Yan, and C. Han, "Hybrid spherical- and planar-wave modeling and DCNN-powered estimation of terahertz ultra-massive MIMO channels," *IEEE Trans. Commun.*, vol. 69, no. 10, pp. 7063–7076, Oct. 2021.

[32] W.-Q. Wang, "Frequency diverse array antenna: New opportunities," *IEEE Antennas Propag. Mag.*, vol. 57, no. 2, pp. 145–152, Apr. 2015.

[33] Q. Cheng, V. Fusco, J. Zhu, S. Wang, and F. Wang, "WFRFT-aided power-efficient multi-beam directional modulation schemes based on frequency diverse array," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5211–5226, Nov. 2019.

[34] Q. Cheng, V. Fusco, J. Zhu, S. Wang, and C. Gu, "SVD-aided multi-beam directional modulation scheme based on frequency diverse array," *IEEE Wireless Commun. Lett.*, vol. 9, no. 3, pp. 420–423, Mar. 2020.

[35] B. Qiu, M. Tao, L. Wang, J. Xie, and Y. Wang, "Multi-beam directional modulation synthesis scheme based on frequency diverse array," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 2593–2606, 2019.

[36] S. Ji, W.-Q. Wang, H. Chen, and S. Zhang, "On physical-layer security of FDA communications over rayleigh fading channels," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 3, pp. 476–490, Sep. 2019.

[37] S. Wang, S. Yan, J. Zhang, N. Yang, R. Chen, and F. Shu, "Secrecy zone achieved by directional modulation with random frequency diverse array," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 2001–2006, Feb. 2021.

WEIJUN GAO (Graduate Student Member, IEEE) received the B.Eng. degree from the UM-SJTU Joint Institute, Shanghai Jiao Tong University, China, in 2019, where he is currently pursuing the Ph.D. degree with the Terahertz Wireless Communications Laboratory. His research interests include terahertz communications and physical layer security.

CHONG HAN (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, USA, in 2016. He is currently a John Wu and Jane Sun Endowed Associate Professor with the University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai Jiao Tong University, China, and the Director of the Terahertz Wireless Communications Laboratory. Since 2021, he is also affiliated with the Department of Electronic Engineering and Cooperative Medianet Innovation Center, Shanghai Jiao Tong University. He is a Co-Founder and the Vice-Chair of IEEE ComSoc Special Interest Group on Terahertz Communications since 2021. He is the recipient of the 2024 Bessel Research Award from Alexander von Humboldt Foundation, the 2023 IEEE ComSoc Asia–Pacific Outstanding Young Researcher Award, among other wards. His research interests include Terahertz and millimeter-wave communications. He is a Guest Editor of IEEE TRANSACTION WIRELESS COMMUNICATIONS, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING. He is the TPC chair to organize multiple IEEE and ACM conferences and workshops, including GC'2023 SAC THz communications.

XUYANG LU (Member, IEEE) received the B.S. degree in electrical engineering from Rice University, Houston, TX, USA, in 2014, and the M.A. and Ph.D. degrees in electrical engineering from Princeton University, Princeton, NJ, USA, in 2016 and 2020, respectively. In 2021, he joined as an Assistant Professor with the University of Michigan–Shanghai Jiao Tong University Joint Institute. He was dually appointed to the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China, in October 2021, where he is currently affiliated with the State Key Laboratory of Radio Frequency Heterogeneous Integration and the Department of Electronic Engineering. His research spans high-speed programmable RF and mmWave integrated systems, integrated terahertz systems, integrated photonics, on-chip antenna optimization, and the intersection of machine learning with analog circuit design.

ZHI CHEN (Senior Member, IEEE) received the B.Eng., M.Eng., and Ph.D. degrees in electrical engineering from the University of Electronic Science and Technology of China (UESTC) in 1997, 2000, and 2006, respectively. In April 2006, he joined the National Key Lab of Science and Technology on Communications, UESTC, where he has been working as a Professor since 2013. He was a Visiting Scholar with University of California at Riverside, Riverside, from 2010 to 2011. He is also the Deputy Director of the Key Laboratory of Terahertz Technology, Ministry of Education. His current research interests include terahertz communication, 5G mobile communications, and tactile Internet.