Hindawi
Security and Communication Networks
Volume 2020, Article ID 4198595, 11 pages
https://doi.org/10.1155/2020/4198595

Research Article

Secure Multiusers Directional Modulation Scheme Based on Random Frequency Diverse Arrays in Broadcasting Systems

Jianbang Gao,[1,2] **Zhaohui Yuan,**[1] **Bin Qiu,**[3] **and Jing Zhou**[2]

[1]*School of Automation, Northwestern Polytechnical University, Xi'an 710072, China*
[2]*School of Electronic Engineering, Xi'an Shiyou University, Xi'an 710000, China*
[3]*School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China*

Correspondence should be addressed to Jianbang Gao; gjbang2008@126.com

Received 20 December 2019; Revised 16 March 2020; Accepted 22 May 2020; Published 24 June 2020

Academic Editor: Kaitai Liang

In this paper, we research a synthesis scheme for secure wireless communication in the broadcasting multiusers directional modulation system, which consists of multiple legitimate users (LUs) receiving the same confidential messages and multiple eavesdroppers (Eves) intercepting the confidential messages. We propose a new type of array antennas, termed random frequency diverse arrays (RFDA), to enhance the security of confidential messages due to its angle-range dependent beam patterns. Based on RFDA, we put forward a synthesis scheme to achieve multiobjective secure wireless communication. First, with known locations of Eves, the beamforming vector is designed to minimize Eves' receiving power of confidential message (Min-ERP) while satisfying the power requirement of LUs. Furthermore, we research a more practical scenario, where locations of Eves are unknown. Unlike the scenario of known locations of Eves, the beamforming vector is designed to maximize the sum received power of LUs (Max-LRP) while satisfying a minimum received power constraint at each LU. Second, the artificial-noise projection matrix (ANPM) is calculated to reduce artificial-noise (AN) impact on LUs and enhance the interference on Eves. Numerical results verify the superior secure performance of the proposed schemes in the broadcasting multiusers system.

1. Introduction

Wireless communications allow information flow through broadcasting to legitimate user (LU) in free space. However, due to the broadcasting nature and lack of physical boundaries of wireless communication, eavesdropper (Eve) in free space can intercept the confidential message. Due to the characteristics of wireless communications, researchers have turned their interest towards the lower physical layer (PHY) security [1, 2]. Directional modulation (DM), which is highly employed in PHY security of wireless communication, preserves the confidential message along a predefined communication direction while disturbing the constellation of the confidential message in other directions [3, 4]. Secure wireless communication has mainly relied on phased arrays directional modulation technology (PA-DM), but the transmit beam pattern only is angle-focusing independent of range. Therefore, in this paper, we propose frequency diversity arrays directional modulation technology (FDA-DM) [5–8] for secure wireless communication due to its angle-range dependent transmit beam pattern. FDA-DM draws into a small frequency offset across the transmit element to produce a beam pattern that changes as time, range, angle, and frequency offsets change. However, the beam pattern of the FDA is highly coupled with angle and range; i.e., Eves which locate at other angle-range pairs can also effectively receive the confidential message. To address this problem, much work focused on trying a different form of the frequency offset to decouple range-angle beam pattern [9, 10]. In [9], the authors employed a logarithmical frequency offset scheme, but its side lobe suppression is not satisfactory. The authors employed square and cubic frequency increments method [10]. Multi-Input-Multi-Output (MIMO) combining with FDA is an effective method to decouple direction-range beam pattern [11]. However, the system is extremely complex because each LU requires multiple transmit channels. A new array structure, termed random frequency diverse arrays (RFDA), is proposed in [12]. RFDA assigns each transmit element with a random carrier frequency, and its beam pattern is thumbtack-like, which means the angle-range correlation can be effectively decoupled in active sensing. Furthermore, in [13], a synthesis strategy based on RFDA is proposed to enhance the secrecy performance of wireless communication. Therefore, in this paper, we consider RFDA configuration. In addition, we also optimize the beamforming vector to control the power distribution of confidential messages in free space.

Besides the above technology on the radio frequency (RF) frontend, the authors paid attention to baseband signal processing technology to further improve the security of confidential message [14, 15]. In this technology, adding artificial-noise (AN) to baseband signal is an effective method to reduce the probability of Eves intercepting the confidential message without influencing LUs. The authors in [16–18] focused on AN-aided baseband technology, which can impose AN at Eves without influencing signal-to-noise-ratio (SNR) at LUs. The authors in [19] proposed an orthogonal AN method to improve secure performance of wireless communication in the baseband. An artificial-noise-aided cooperative jamming scheme was proposed in [20] to improve the security of the primary network. The artificial-noise-aided beamforming design problems were investigated subject to the practical secrecy rate and energy harvesting constraints. In [21], the problem of robust, secure artificial noise-aided beamforming and power splitting design was investigated under imperfect channel state information (CSI). But these two references mainly focused on simultaneous wireless communication and power transfer based on multiple-input single-output cognitive radio downlink network. In our previous work [22], RFDA with AN multiobjective DM scheme was proposed under the scenario with unknown locations of Eves. Based on [22], we further study synthesis schemes to achieve multiobjective security wireless communication under known/unknown locations of Eves, respectively.

Most of the prior researches on beamforming design assumed either a single LU or a single Eve. There is limited research interest in the multibeam system scenario. In [14, 23–27], the authors achieved secure wireless communication for the multibeam system scenario. Especially, the authors in [23] creatively proposed WFRFT-aided DM synthesis scheme, which is more power-efficient than the conventional multibeam AN-DM scheme. However, in [14, 24, 25], the authors researched the multibeam scenario based PA-DM, which cannot achieve range-independent wireless communication. Furthermore, in [23, 26, 27], the beamforming vector of each LU is individually designed that ensures the effective reception of intended LU and no interference from others based on FDA-DM. In this paper, we consider a broadcasting multiusers communication scenario, where all LUs receive common confidential messages and only one beamforming vector is needed to design. Therefore, the method of [23, 27] is not suitable for our considered scenario. In [28], the authors achieved broadcasting multiusers secure communication based on FDA with frequency offsets obtained by iterative ABSLM algorithm with high computational complexity. Furthermore, the secure scheme in [28] focused on the Max-SLNR method that must calculate the curve integral of Eves wiretap area. The secure scheme in [28] is extremely complex. In this paper, combined with convenient RFDA and AN, two proposed optimization methods of beamforming vector with known/unknown Eves' locations also can achieve multiusers secure communications. Consequently, the main objective is to broadcast the common confidential message towards different LUs and impose AN at other regions to avoid the interception by Eves.

The rest of this paper is organized as follows: Section 2 details the model of broadcasting multiusers FDA-DM system. Then, in Section 3, we propose novel synthesis schemes under two cases: unknown and known locations of Eves. Simulation and performance analysis are shown in Section 4. Finally, the conclusions of this paper are drawn in Section 5.

Notations: normal-faced lower-case letters denote scalars, while bold-faced lower-case and uppercase letters denote vectors and matrices, respectively. The superscripts $(\cdot)^T$, $(\cdot)^{-1}$, and $(\cdot)^H$ are used to denote transpose, inverse, and Hermitian operators, respectively. Operations $k\cdot k_2$, and $(\cdot)$ stand for `$_2$-norm and modulus, respectively. $E[\cdot]$ and $tr(\cdot)$ refer to the expectation and trace operators, respectively. In addition, the notations R and C are used to indicate the real and complex number domains, respectively.

2. System Model

As shown in Figure 1(a), the broadcasting multiusers directional modulation system consists of a transmitter with an N-elements linear antenna array, M LUs with a single antenna, and K single-antenna Eves. In this paper, we consider RFDA configurations. RFDA brings small random frequency offsets across the transmit elements. The radiation frequency of the nth element is $f_n = f_c + \Delta f_n$, for $n = 1, 2, \ldots, N$, where f_c is the carrier frequency, $\Delta f_n = \eta_n \Delta f$ is a random frequency offset, and η_n is a random variable being chosen as independent and identically distributed. The distribution of η_n determines one specific random mapping rule to assign the carrier frequencies of the different elements.

Generally, set the first element as the reference and suppose all LUs locations are known. Moreover, for simplicity, the normalized line-of-sight (LOS) channel in free space is considered throughout this paper. Thus, for an arbitrary user located at (r, θ) the instantaneous normalized steering vector can be calculated by the following equation [29]:

$$\mathbf{h}(\theta, r, t, \mathbf{f}) = \frac{\rho(r)}{\sqrt{N}}\left[e^{-j2\pi f_1 (t-(r/c))}, e^{-j2\pi f_2 (t-((r-d\sin\theta)/c))}, \ldots, e^{-j2\pi f_N (t-((r-(N-1)d\sin\theta)/c))}\right]^T, \quad (1)$$

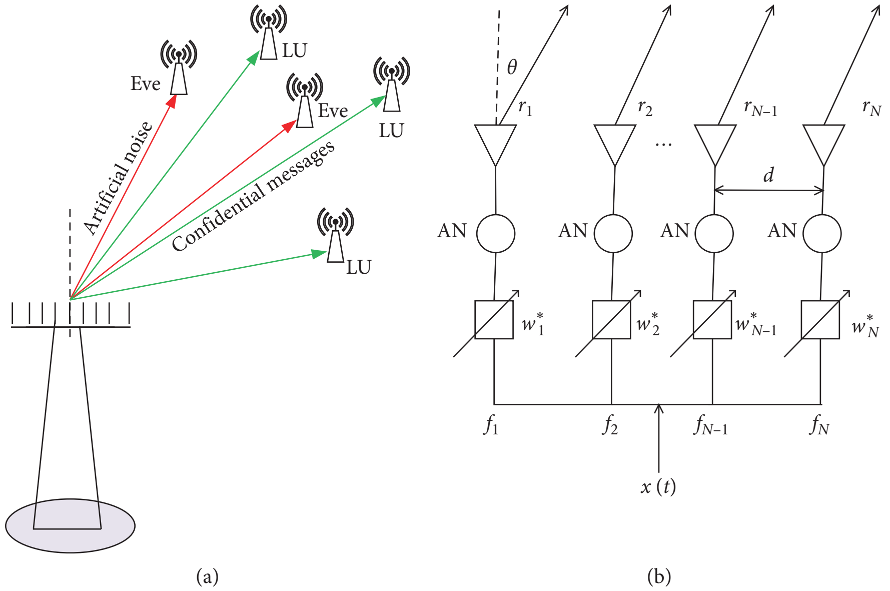


Figure 1: (a) FDA directional modulation for the scenario of multiusers. (b) The architecture of the transmit station for the proposed scheme.

where c refers to the light speed, and$\rho(r_n)$ is the path loss factor due to the free space propagation from the nth element to the receiver. Based on the fact that $r \gg (N-1)d$, we can have a reasonable approximation $\rho(r) = \rho(r_1) = \cdots = \rho(r_N)$.

For simplicity, $\mathbf{h}(t)$ is defined as the normalized steering vector of a user located at (r, θ), i.e., $\mathbf{h}(t) \triangleq \mathbf{h}(r, \theta, t, \mathbf{f})$. To simplify the expression, the steering vectors of LUs can compose a steering matrix as follows:

$$\mathbf{H}_L(t) \triangleq \left[\mathbf{h}_{L_1}(t), \mathbf{h}_{L_2}(t), \dots, \mathbf{h}_{L_m}(t), \dots, \mathbf{h}_{L_M}(t)\right], \quad (2)$$

where $\mathbf{h}_{L_m}(t)$ is the instantaneous normalized steering vector of mth LU at (r_{L_m}, θ_{L_m}).

AN-aided in baseband signal can be employed in wireless communication based on PHY security. The AN vector $\mathbf{z} \sim \mathrm{CN}(0, \mathbf{I}_N)$ consists of complex Gaussian random variables with zero-mean and unit variance. Furthermore, we design a matrix $\mathbf{T}_{AN}(t)$ that can project $\mathbf{z}$ into the null space of the steering vector at LU location, but the signal-to-interference-plus-noise ratio (SINR) will be significantly reduced at Eves. Therefore, the method of AN-aided in the baseband signal will effectively improve the security of wireless communication. As shown in Figure 1(b), the radiating signal for the N antenna elements can be expressed as follows:

$$\mathbf{s}(t) = \mathbf{w}(t)x(t) + \alpha\sqrt{P_{\mathrm{AN}}}\mathbf{T}_{\mathrm{AN}}(t)\mathbf{z}, \quad (3)$$

where $x(t)$ is normalized baseband signal with average power $\mathrm{E}[|x(t)|^2] = 1$, P_{AN} is the power of AN,α denotes the normalization factor with $\alpha\mathrm{E}\{tr[\mathbf{T}_{\mathrm{AN}}(t)\mathbf{z}\mathbf{z}\mathbf{T}_{\mathrm{AN}}^H(t)]\} = 1$, and $\mathbf{w}(t)$ is the array beamforming vector, which is mixed with the phase shifters at time t with the following expression:

$$\mathbf{w}(t) = \left[w_1(t), w_2(t), \dots, w_n(t), \dots, w_N(t)\right]^T, \quad (4)$$

where $w_n(t)$ is beamforming element of the nth antenna for processing confidential baseband signal $x(t)$.

The normalized LOS channel is considered in this paper. Therefore, the received signal vector of all LUs is obtained by the following:

$$\begin{aligned}\mathbf{y}_L(t) &= \mathbf{H}_L^H(t)\mathbf{s}(t) + \mathbf{n}_L(t)\\ &= \mathbf{H}_L^H(t)\mathbf{w}(t)x(t) + \alpha\sqrt{P_{\mathrm{AN}}}\mathbf{H}_L^H(t)\mathbf{T}_{\mathrm{AN}}(t)\mathbf{z} + \mathbf{n}_L(t),\end{aligned} \quad (5)$$

where $\mathbf{n}_L(t) = [n_{L_1}(t), n_{L_2}(t), \dots, n_{L_m}(t), \dots, n_{L_M}(t)]^T$ is the complex AWGN noises vector between the transmitter and LUs with the distribution $\mathbf{n}_L(t) \sim \mathrm{CN}(\mathbf{0}_{M\times 1}, \sigma_L^2\mathbf{I}_M)$.

3. Proposed Beamforming Profile

3.1. Optimal Beamforming Vector with Known Locations of Eves. In the following, we assume the transmitter can estimate Eves' locations and ignore the estimated errors. Define the steering matrix of all Eves as follows:

$$\mathbf{H}_E(t) \triangleq \left[\mathbf{h}_{E_1}(t), \mathbf{h}_{E_2}(t), \dots, \mathbf{h}_{E_k}(t), \dots, \mathbf{h}_{E_K}(t)\right], \quad (6)$$

where $\mathbf{h}_{E_k}(t)$ is the instantaneous normalized steering vector of kth Eve at (r_{E_k}, θ_{E_k}).

After passing through the LOS channel, the received signal vector of Eves is as follows:

$$\begin{aligned}\mathbf{y}_E(t) &= \mathbf{H}_E^H(t)\mathbf{s}(t) + \mathbf{n}_E(t)\\ &= \mathbf{H}_E^H(t)\mathbf{w}(t)x(t) + \alpha\sqrt{P_{\mathrm{AN}}}\mathbf{H}_E^H(t)\mathbf{T}_{\mathrm{AN}}(t)\mathbf{z} + n_E(t),\end{aligned} \quad (7)$$

where $\mathbf{n}_E(t)$ is the complex AWGN noises vector between the transmitter and Eves with the distribution $\mathbf{n}_E(t) \sim \mathrm{CN}(\mathbf{0}_{K\times 1}, \sigma_E^2\mathbf{I}_K)$.

Without loss of generality, the total transmit power P_s is fixed. In this section, our major goal is to optimize the beamforming vector such that high secrecy performance can be achieved for broadcasting the confidential message. Therefore, firstly we devise the Min-ERP method to let Eves receive power as little as possible while satisfying the basic requirements of LUs. However, other passive unknown Eves may be hiding in free space, so we minimize confidential message power, which means we can allocate more AN power to prevent passive unknown Eves intercepting the broadcasting confidential message. Based on these rules, the instantaneous beamforming vector $\mathbf{w}(t)$ can be obtained by the optimization problem:

$$\begin{aligned} \min_{\mathbf{w}(t)} \quad & \|\mathbf{w}(t)\|_2^2 \\ \text{s.t.} \quad & \mathbf{H}_L^H \mathbf{w}(t) \geq \zeta_{M\times 1} \\ & \mathbf{H}_E^H(t)\mathbf{w}(t)x(t) = 0, \end{aligned} \tag{8}$$

where $\zeta \triangleq [\sqrt{\zeta_1}, \sqrt{\zeta_2}, \ldots, \sqrt{\zeta_m}, \ldots, \sqrt{\zeta_M}$, in which ζ_m is the minimum desired received power of the mth LU, for $m = 1, 2, \ldots, M$.

To solve problem (8), we first decompose the complement of the steering matrix of Eves $\mathbf{H}_E^H(t)$ by using SVD method, i.e.,

$$\mathbf{H}_E^H(t) = \left[\mathbf{U}_E^{(1)}(t) \;\; \mathbf{U}_E^{(0)}(t)\right] \begin{bmatrix} \mathbf{\Sigma}_E^{(1)}(t) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \left[\mathbf{V}_E^{(1)}(t) \;\; \mathbf{V}_E^{(0)}(t)\right]^H, \tag{9}$$

where $\Sigma_E^{(1)}(t)$ is the $K \times K$ diagonal matrix. Based on the SVD characteristic [30], we know that $\mathbf{V}_E^{(0)}(t)$ consists of $N-K$ right singular vectors corresponding to $N-K$ zero singular values, i.e., $\mathbf{H}_E^H(t)\mathbf{v}_i(t) = \mathbf{0}$, for $\{\mathbf{v}_1(t), \ldots, \mathbf{v}_i(t), \ldots, \mathbf{v}_{N-K}(t)\} \in \mathbf{V}_E^{(0)}(t)$. Define $\mathbf{D}(t) \triangleq \mathbf{V}_E^{(0)}(t)$ and $\mathbf{w}(t) \triangleq \mathbf{D}(t)\mathbf{u}(t), \mathbf{u}(t) \in \mathbb{C}^{(N-K)\times 1}$. Problem (8) can be converted to the following problem:

$$\begin{aligned} \min_{\mathbf{u}(t)} \quad & \mathbf{u}^H(t)\mathbf{D}^H(t)\mathbf{D}(t)\mathbf{u}(t) \\ \text{s.t.} \quad & \mathbf{H}_L^H \mathbf{D}(t)\mathbf{u}(t) \geq \zeta_{M\times 1}. \end{aligned} \tag{10}$$

Problem (10) can be solved by Lagrange multiplier. Thus, the optimal beamforming vector $\mathbf{w}^\star(t)$ is given by the following:

$$\begin{aligned} \mathbf{w}^\star(t) = {} & \mathbf{D}(t)\left(\mathbf{D}^H(t)\mathbf{D}(t)\right)^{-1}\mathbf{D}^H(t)\mathbf{H}_L(t) \\ & \cdot \left[\mathbf{H}_L^H(t)\mathbf{D}(t)\left(\mathbf{D}^H(t)\mathbf{D}(t)\right)^{-1}\mathbf{D}^H(t)\mathbf{H}_L(t)\right]^{-1} \zeta. \end{aligned} \tag{11}$$

3.2. Optimal Beamforming Vector with Unknown Locations of Eves. With unknown locations of Eves, the steering vectors of Eves cannot be calculated, so the optimized method mentioned in the previous subsection is not applicable. Under this scenario, the beamforming vector $\mathbf{w}(t)$ is optimized by the Max-LRP method. Under the fixed confidential messages power P_C, this method is to maximize the confidential messages power focusing on LUs in free space. Based on these rules, the instantaneous beamforming vector $\mathbf{w}(t)$ can be obtained by the optimization problem:

$$\begin{aligned} \max_{\mathbf{w}(t)} \quad & \mathbf{w}^H(t)\mathbf{H}_L(t)\mathbf{H}_L^H(t)\mathbf{w}(t) \\ \text{s.t.} \quad & \mathbf{H}_L^H w(t) \geq \zeta_{M\times 1} \\ & \|\mathbf{w}(t)\|_2^2 = P_C, \end{aligned} \tag{12}$$

where P_C is the power of confidential messages and $P_C \leq P_S$.

To solve problem (12), we first rewrite the sum received confidential messages power of LUs R_s as follows:

$$R_s = \mathbf{w}^H(t)\mathbf{H}_L(t)\mathbf{H}_L^H(t)\mathbf{w}(t) = \mathbf{C}^H\mathbf{x}, \tag{13}$$

where $\mathbf{C} = [h_{11}^2 + h_{12}^2 + \cdots + h_{1M}^2, \ldots, h_{n1}^2 + h_{n2}^2 + \cdots + h_{nM}^2, \ldots, h_{N1}^2 + h_{N2}^2 + \cdots + h_{NM}^2]^H$, in which h_{nm} is the n-row and the m-column term of $\mathbf{H}_L$, for $m = 1, 2, \ldots, M$, $n = 1, 2, \ldots, N$. $\mathbf{x} = [x_1(t), x_2(t), \ldots, x_n(t), \ldots, x_N(t)]^H$, in which $x_n(t) = w_n^2(t)$, for $n = 1, 2, \ldots, N$.

In this subsection, when we maximize the sum received confidential message power of LUs, we also ensure each LU receives sufficient confidential message power. Then, we rewrite each LU received power as follows:

$$\mathbf{Ax} \geq \boldsymbol{\zeta}, \tag{14}$$

where $\mathbf{A}$ is $M \times N$ matrix, and the m-row and the n-column term of $\mathbf{A}$ is calculated as $A_{mn} = h_{nm}^2$, $\zeta \triangleq [\zeta_1, \zeta_2, \ldots, \zeta_m, \ldots, \zeta_M]$, in which ζ_m is the minimum desired received power of the mth LU,, for $m = 1, 2, \ldots, M$, $n = 1, 2, \ldots, N$.

Therefore, problem (12) is equivalent to the following problem:

$$\begin{aligned} \max_{\mathbf{x}} \quad & \mathbf{C}^H\mathbf{x} \\ \text{s.t.} \quad & \mathbf{I}_N\mathbf{x} = P_C \\ & \mathbf{Ax} \geq \boldsymbol{\zeta}. \end{aligned} \tag{15}$$

Actually, the optimized problem (15) can be converted to standard linear programming (LP), which can be solved by numerical solvers. Therefore, it is easy to compute the optimal transmit beamforming vector $\mathbf{w}^\star(t)$.

3.3. AN Projection Matrix. Under the scenario with known locations of Eves, we have optimized the beamforming vector that Eves cannot intercept confidential message. Therefore, there is no need to impose AN interference in Eves locations. However, other passive unknown Eves may be hiding in free space, so we still use AN for improving secure communication. Under the scenario with unknown locations of Eves, it is impossible to obtain the steering vector of Eves, so AN cannot be imposed only in Eves locations. Therefore, we distribute AN evenly in free space outside LUs locations with known and unknown locations of Eves, respectively. The artificial-noise vector $\mathbf{z}$ generally does not lie in span $(\mathrm{H}_L(t))$. Therefore, in this subsection, we design the ANPM $\mathbf{T}_{AN}(t)$ to project the aided AN to the null space of the steering vectors of all LUs; i.e., AN is intended to interfere with Eves without affecting LUs. Then, the ANPM can be designed by the following equation [14, 16]:

$$tr\left\{\mathbf{T}_{AN}^H(t)\mathbf{H}_L(\mathbf{f}, t)\mathbf{H}_L^H(\mathbf{f}, t)\mathbf{T}_{AN}(t)\right\} = 0. \tag{16}$$

Based on the null-space projection rule, the number of transmit antennas should be greater than the total number of all LUs, i.e., $N > M$. Then, we construct orthogonal projection matrix as follows:

$$\mathbf{T}_{AN}(t) = \mathbf{I}_N - \mathbf{H}_L(t)\left[\mathbf{H}_L^H(t)\mathbf{H}_L(t)\right]^{-1}\mathbf{H}_L^H(t). \quad (17)$$

4. Simulation and Performance Analysis

In this section, we illustrate the secrecy performance of the broadcasting multiusers system based on our proposed schemes through intensive numerical simulations. The carrier frequency is $f_c = 1\,\text{GHz}$. The uniform linear array consists of $N = 32$ elements with an interelement spacing of $d = (1/2\lambda) \approx (c/2f_c)$. We assume that the received noise power for both LUs and Eves is $-100\,\text{dBm}$, i.e., $10\log(\sigma_l^2) = 10\log(\sigma_e^2) = -100\,\text{dBm}$. The minimum desired received power of each LU is $-90\,\text{dBm}$. LUs' locations are $(r_{L_1}, \theta_{L_1}) = (3000\,\text{m}, 30^\circ)$, $(r_{L_2}, \theta_{L_2}) = (3500\,\text{m}, 60^\circ)$, $(r_{L_3}, \theta_{L_3}) = (4000\,\text{m}, -30^\circ)$, and $(r_{L_4}, \theta_{L_4}) = (4500\,\text{m}, -60^\circ)$.

4.1. Analysis of AN Power Distribution. In this paper, we design matrix $\mathbf{T}_{AN}(t)$ to project AN into the null space of steering vector at LUs under the scenarios with known/unknown Eves locations, respectively. In the subsection, we plot AN energy distribution versus range-angle dimensions to validate our design of ANPM $\mathbf{T}_{AN}(t)$.

According to Figure 2, we can observe that (1) there are four deep nulls at coordinates of LUs, which means AN cannot influence LUs receiving confidential messages; (2) power of AN is uniformly distributed versus angle-range dimensions outside the main lobes of all LUs coordinates. The reason for this is that, under the scenario with known the locations of Eves, we have an optimized beamforming vector that Eves cannot receive a confidential message, so the uniformly distributed AN power is to prevent the confidential message from interception by other unknown passive Eves. And under unknown Eves locations, we can only uniformly distribute AN power in free space outside LUs locations to prevent Eves intercepting the confidential message, since Eves could exist anywhere. Moreover, in Figure 2(c), it can be seen that the power of AN decreases as the distance increases.

4.2. Focusing Performance Analysis of the Proposed Schemes. As previously mentioned, FDA focusing depends on range-angle dimensions whereas the focusing of the phased array only depends on the angle dimension. However, the beam pattern is highly coupled with angle and range. In this subsection, we plot SINR distribution versus range-angle dimensions to measure the focusing performance of our proposed schemes.

In the scenario with prior known locations of Eves, the SINR distribution versus angle and range is explored in Figure 3. It can be observed that SINR values only reach peaks at LUs locations and is low at other places, which means (1) the LUs can receive the confidential message effectively; (2) angle-range beam pattern has been successfully decoupled by the optimization method in Section 3.1. To show the result more clearly, we further plot the SINR versus angle dimension and range dimension in Figures 3(b) and 3(c), respectively. Moreover, the SINR of each LU is equal to 10 dB, which means the receive power requirement is satisfied for each LU and indicates the accurate control of each broadcasting messages.

In the scenario with unknown the locations of Eves, Figure 4(a) illustrates SINR distribution in free space versus angle-range dimensions of the optimization method in Section 3.2. To show the result more clearly, we further plot the SINR versus angle dimension and range dimension in Figures 4(b) and 4(c), respectively. It also can be observed that the SINR distribution is thumbtack-like, and only peak is synthesized around the locations of LUs. This indicates that (1) the angle-range beam pattern has been successfully decoupled by the optimization approach in Section 3.2; (2) LUs can receive the confidential message effectively. Meanwhile Eves that may exist anywhere are seriously influenced by AN based on the method in Section 3.3. Compared with Figure 3, we can observe that the SINR values at LUs locations are not equal, but they all satisfy the secure requirement of the broadcasting system. This indicates that we guarantee the effectiveness of LUs based on our proposed scheme under the scenario with unknown locations of Eves.

4.3. Secrecy Performance Analysis of the Proposed Schemes. Secrecy capacity and bit error rate (BER) are important metrics to measure the secrecy performance of wireless communication systems. In this subsection, we will analyze the BER and secrecy capability of the proposed two novel broadcasting multiusers schemes with known/unknown Eves' locations. Then we define the average secrecy capacity as follows:

$$C(t) \triangleq \left|C_L(t) - C_E(t)\right|^+, \quad (18)$$

where $C_L(t)$ and $C_E(t)$ are the average achievable rate of the link from the transmitter to LUs and Eves at time *t*, respectively.

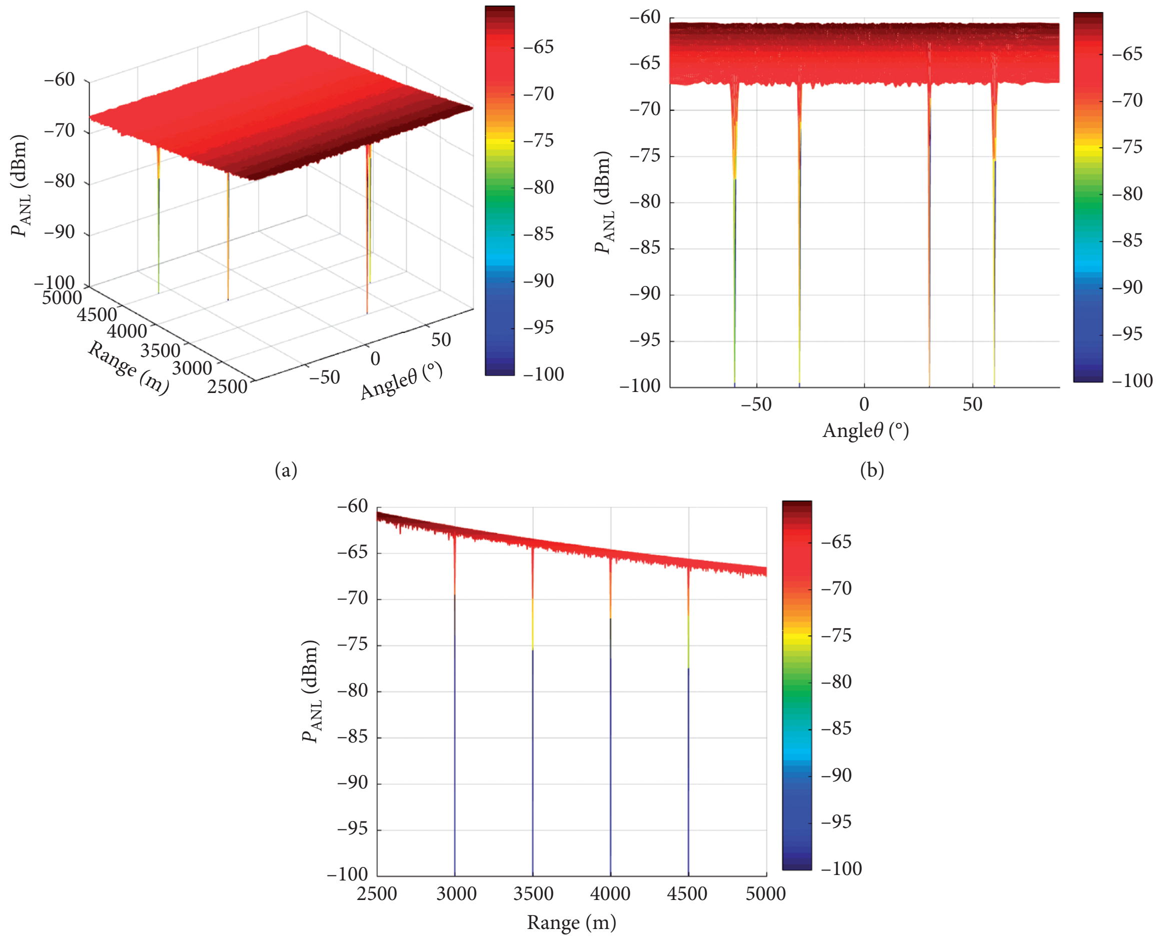
First, with known locations of Eves, we calculate $C_L(t)$ and $C_E(t)$ as the following formulas based on the optimized method in Section 3.1:

$$\begin{aligned} C_L(t) &\triangleq \frac{1}{M}\sum_{m=1}^{M}\log_2(1+\zeta_m), \\ C_E(t) &\triangleq 0. \end{aligned} \quad (19)$$

It is easy to find that $C(t) \triangleq (1/M)\sum_{m=1}^{M}\log_2(1+\zeta_m)$, which is a function of the parameter ζ_m. Therefore, in the scenario with known Eves locations, we can control the secrecy rate by setting the received confidential message power ζ_m based on our proposed optimized method.

In the following, with unknown locations of Eves, we treat all locations outside the main lobes of the LUs' locations as the wiretap area of Eves. Thus, the location interval of Eves can be defined as follows:

$$\begin{aligned} \Theta_E &\triangleq \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \bigcup_{m=1}^{M} \Theta_L^m, \\ \Omega_E &\triangleq [r_{\min}, r_{\max}] \backslash \bigcup_{m=1}^{M} \Omega_L^m, \end{aligned} \quad (20)$$

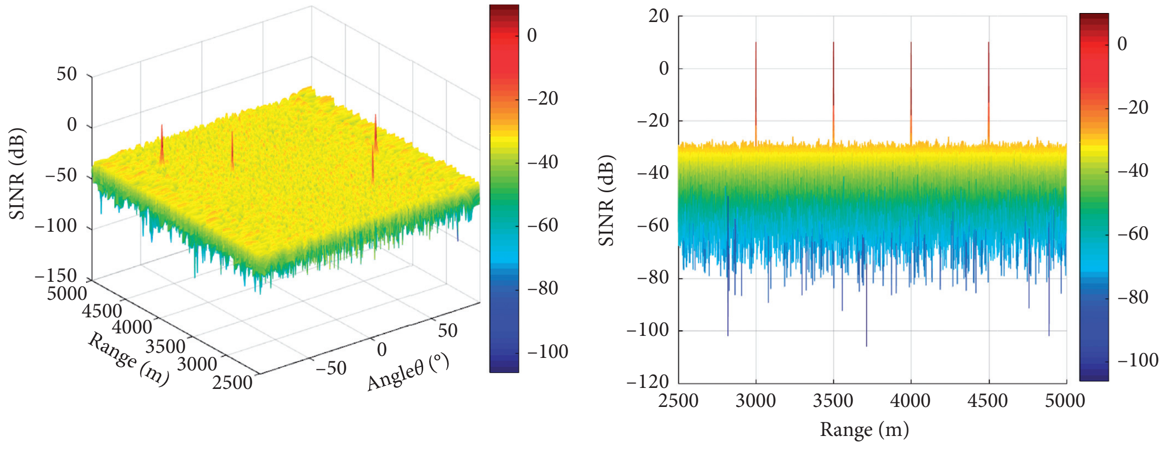


(a)

(b)

(c)

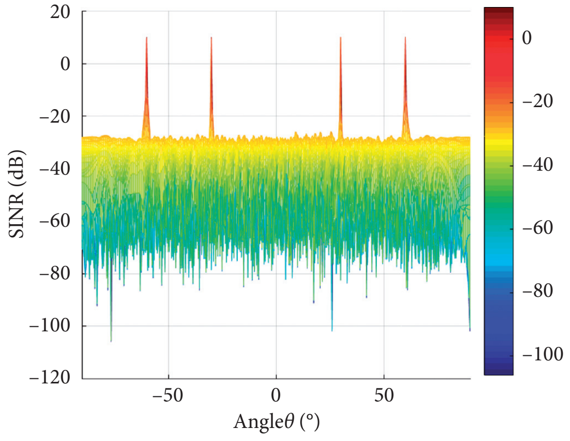
Figure 2: The AN power spatial performance versus (a) angle-range, (b) angle dimension, and (c) range dimension, where $N = 32$ and $P_s = 40$ dBm.



(a)

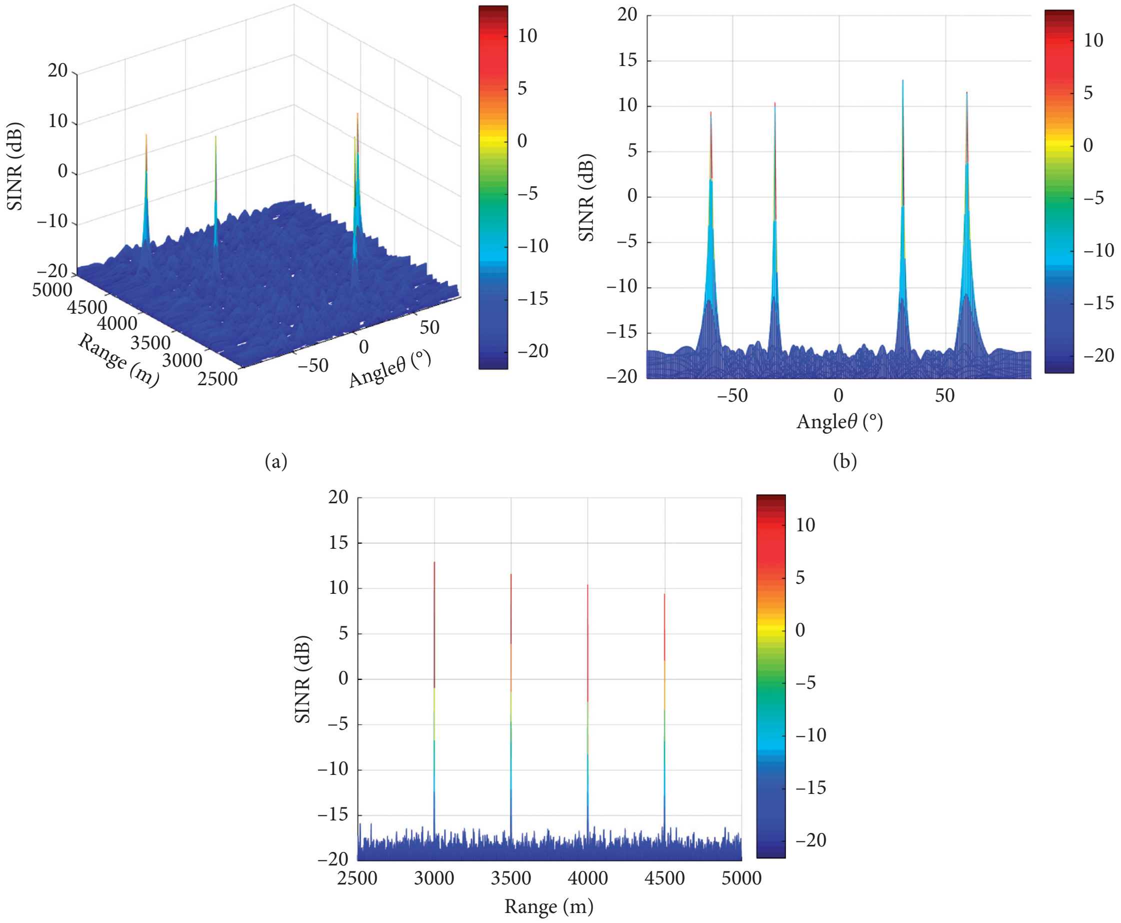
(b)

Figure 3: Continued.



(c)

Figure 3: The SINR performance with known locations of Eves based on the proposed method versus (a) angle-range, (b) angle dimension, and (c) range dimension, where $N = 32$ and $P_s = 40\,\text{dBm}$.



(a)

(b)

(c)

Figure 4: The SINR performance with unknown locations of Eves based on the proposed method versus (a) angle-range, (b) angle dimension, and (c) range dimension, where $N = 32$ and $P_s = 40\,\text{dBm}$.

where $\Theta_L^m = [(\theta_L^m - \theta_{BW}/2), (\theta_L^m + \theta_{BW}/2)]$ and $\Omega_L^m = [(r_L^m - r_{BW}/2), (r_L^m + r_{BW}/2)]$ denote the main lobes of the mth LU, for $m = 1, 2, \ldots, M$, with θ_{BW} and r_{BW} being the beam width of angle and range, respectively. To simplify the expression, we define the wiretap area as $S_{\text{wire}} \triangleq [\Theta_E, \Omega_E]$.

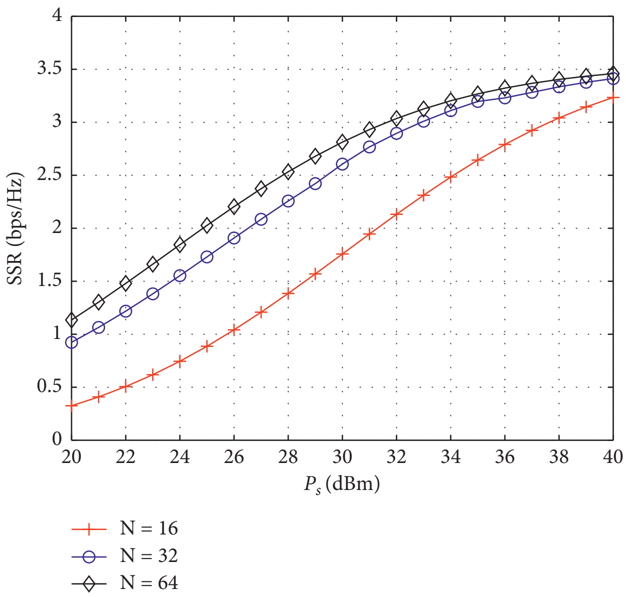
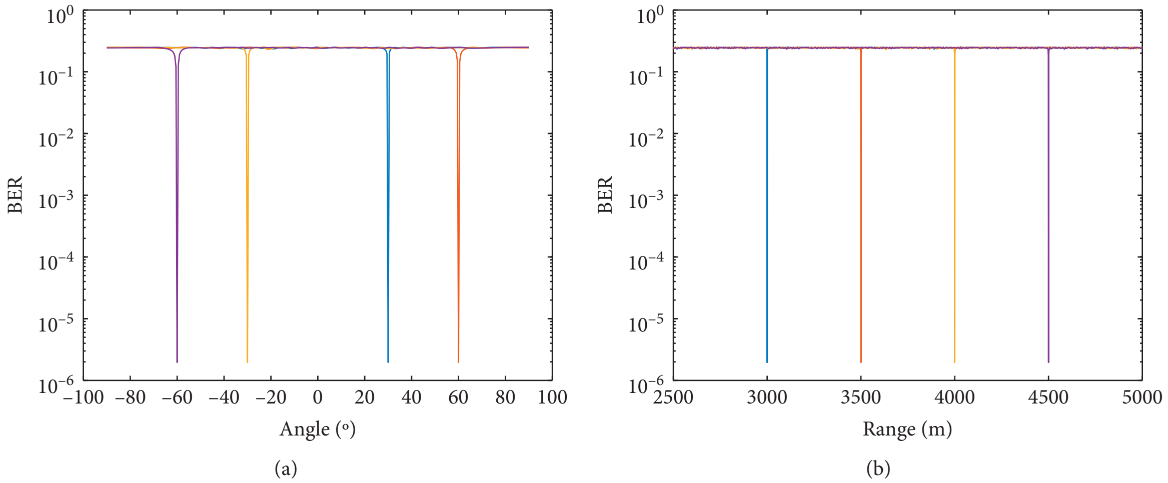


Figure 5: The secrecy capacity under a scenario with unknown locations of Eves versus total power P_s.



(a)

(b)

Figure 6: The BER performances under a scenario with known locations of Eves, (a) angle dimension, and (b) range dimension, where $N = 32$ and $P_s = 40\,\mathrm{dBm}$.

We obtain $C_L(t)$ and $C_E(t)$ by the following formula:

$$\begin{aligned} C_L(t) &\triangleq \frac{1}{M}\log_2\left(1+\mathrm{SINR}_L\right) \\ &= \frac{1}{M}\log_2\left(1+\frac{\left\|\mathbf{H}_L^H(t)\mathbf{w}(t)\right\|^2}{\alpha^2 P_{AN}\mathrm{E}\left[\left\|\mathbf{H}_L^H(t)\mathbf{T}_{AN}(t)\mathbf{z}\right\|^2\right]+\sigma_m^2}\right). \end{aligned} \tag{21}$$

$$\begin{aligned} C_E(t) &\triangleq \log_2\left(1+\max_{(\theta_E,r_E)\in S_{\mathrm{wire}}}\mathrm{SINR}_E\right) \\ &= \log_2\left(1+\max_{(\theta_E,r_E)\in S_{\mathrm{wire}}}\frac{\left|\mathbf{h}_E^H(t)\mathbf{w}(t)\right|^2}{\alpha^2 P_{AN}\mathrm{E}\left[\left|\mathbf{h}_E^H(t)\mathbf{T}_{AN}(t)\mathbf{z}\right|^2\right]+\sigma_E^2}\right). \end{aligned} \tag{22}$$

Then, we analyze the secrecy capacity versus P_s for the proposed broadcasting multiusers scheme under a scenario with unknown locations of Eves. Figure 5 illustrates the secrecy capacity in three scenarios that transmit array elements set as $N = 16$ for scenario 1, $N = 32$ for scenario 2, and $N = 64$ for scenario 3. For the proposed scheme, it can be seen that the broadcasting multiusers system shows a better secrecy capacity performance as the increment of P_s. It is because that our proposed scheme optimizes beamforming vector while also fixing the power of the confidential message, and more power can be allocated to AN to suppress the SINR of Eves as the increment of total transmit power P_s. What's more, we also find that with the same total transmit power P_s, more transmit array elements can promote better

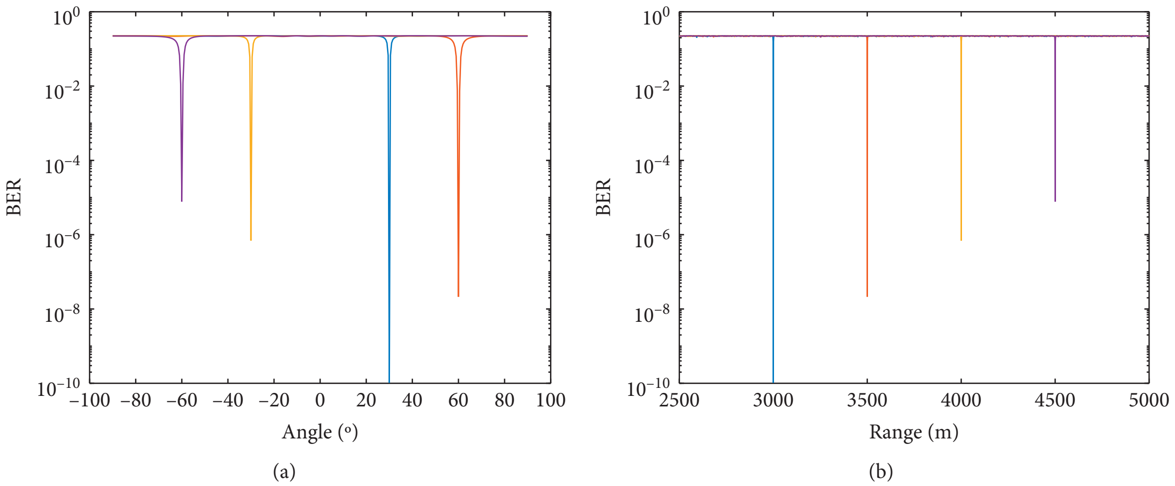


FIGURE 7: The BER performances under a scenario with unknown locations of Eves, (a) angle dimension, and (b) range dimension, where $N = 32$ and $P_s = 40$ dBm.

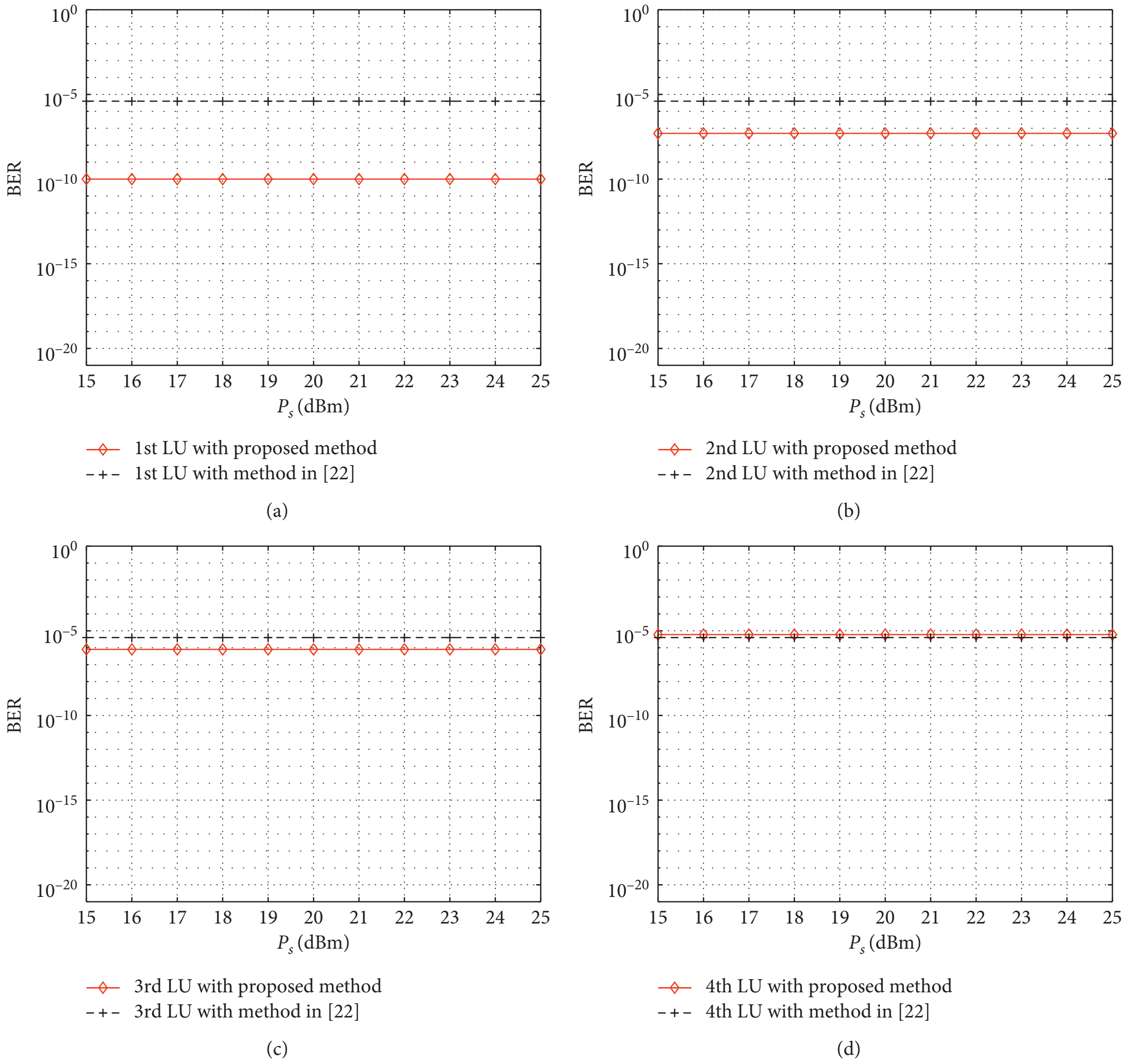


FIGURE 8: The BER comparison for different DM schemes versus P_s: (a) 1st LU; (b) 2nd LU; (c) 3rd LU; (d) 4th LU.

secrecy capacity performance, and the gap between different numbers of transmit antennas is decrement as the increment of total transmit power P_s. This phenomenon is because (1) the transmit array has a narrower beam as the increment of array elements; (2) The power of AN is enough to ensure the secrecy capacity regardless of the number of array elements in high P_s region.

In the last experiment, we illustrate the BER performances versus angle and range for the proposed scheme under known/unknown locations of Eves, respectively. The baseband modulations are set as BPSK.

In Figure 6, we illustrate the BER performances under the scenario with known locations of Eves. We can observe that from Figures 6(a) and 6(b): (1) the BER of broadcasting a confidential message is low only at the corresponding LU locations, and BER of all LUs are all approximately equal to 10–5, which demonstrate effective reception of the LUs; (2) the BER at each Eve and other regions outside all LUs locations are almost equal to 0.5, which means Eves and other undesired users are unable to obtain any meaningful confidential information.

In Figure 7, we illustrate the BER performances under the scenario with unknown Eves locations. Figures 7(a) and 7(b) plot the curves of BER versus angle and range of the proposed method in Section 3.2. Compared with Figure 6, the BER of each LU is not equal, but they all satisfy the secure communication requirement. Furthermore, the BER of 1st LU is low to 10–10, which achieves a better secrecy performance. And, the BER at other regions outside all LUs locations are almost equal to 0.5. Therefore, we can conclude that the proposed method in Section 3.2 maximizes the reception of the LUs, and its security performance satisfies the secure communication requirement.

Under the scenario with unknown locations of Eves, the BER curves of the LUs versus P_s for the proposed method and the method in [22] are given in Figure 8. As shown in the figure, the BER at each LU of the proposed method outperforms the BER obtained by the method in [22]. The BER of 1st LU for proposed method is almost low to 10–10, which achieves a better secrecy performance. The worst BER of 4th LU for the proposed method is almost identical to the BER of 4th LU for the method in [22]. In [22], the beamforming vector of the confidential message is designed by maximizing the AN transmit power; i.e., the optimal power distribution ratio between AN and confidential messages is obtained. Based on the optimal power distribution ratio, we further optimize the beamforming vector to make the confidential messages power more concentrated on LUs. And, this is also why BER of the proposed method and the method in [22] are all constant versus P_s.

5. Conclusion

With the assistance of the RFDA technology, two AN-aided secure broadcasting multiusers wireless communication schemes with known/unknown locations of Eves were proposed, respectively. We consider multiusers communication mode that common confidential message is simultaneously transmitted to all LUs. To achieve the goal, we design the beamforming vector by Min-ERP with known locations of Eves. Furthermore, the beamforming vector is designed by Max-LRP with unknown locations of Eves. In addition, we judiciously design the ANPM to enhance PHY security. The optimized beamforming vector with the help of AN generates high SINR peaks only at the positions of LUs, meanwhile a low flat SINR plane for other regions. Therefore, in this paper, we effectively achieve the security of the broadcasting system since the confidential message is only transmitted to the locations of LUs. Finally, the effectiveness of the proposed scheme has been verified via extensive numerical simulations.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. 51874238) and the Innovation Foundation for Doctor Dissertation of Northwestern Polytechnical University (Grant no. CX202038).

References

[1] B. Li, Z. Fei, C. Zhou, and Y. Zhang, “Physical layer security in space information networks: a survey,” *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2019.

[2] B. Li, Z. Fei, Z. Chu, and Y. Zhang, “Secure transmission for heterogeneous cellular networks with wireless information and power transfer,” *IEEE Systems Journal*, vol. 12, no. 4, pp. 3755–3766, 2018.

[3] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, “Directional modulation via symbol-level precoding: a way to enhance security,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1478–1493, 2016.

[4] J. Xiong, S. Y. Nusenu, and W.-Q. Wang, “Directional modulation using frequency diverse array for secure communications,” *Wireless Personal Communications*, vol. 95, no. 3, pp. 2679–2689, 2017.

[5] J. Li, L. Xu, P. Lu et al., “Performance analysis of directional modulation with finite-quantized rf phase shifters in analog beamforming structure,” *IEEE Access*, vol. 7, pp. 97457–97465, 2019.

[6] T. Shen, S. Zhang, R. Chen et al., “Two practical random-subcarrier-selection methods for secure precise wireless transmissions,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9018–9028, 2019.

[7] M. Mahmood and H. Mir, “Frequency diverse array beamforming using nonuniform logarithmic frequency increments,” *IEEE Antennas and Wireless Propagation Letters*, vol. 17, no. 10, pp. 1817–1821, 2018.

[8] C. Mai, S. Lu, J. Sun, and G. Wang, “Beampattern optimization for frequency diverse array with sparse frequency waveforms,” *IEEE Access*, vol. 5, pp. 17914–17926, 2017.

[9] W. Khan, I. M. Qureshi, and S. Saeed, “Frequency diverse array radar with logarithmically increasing frequency offset,”

IEEE Antennas and Wireless Propagation Letters, vol. 14, pp. 499–502, 2014.

[10] K. Gao, J. Xiong, J. Cai, and W.-Q. Wang, "Decoupled frequency diverse array range-angle-dependent beampattern synthesis using non-linearly increasing frequency offsets," *IET Microwaves, Antennas & Propagation*, vol. 10, no. 8, pp. 880–884, 2016.

[11] P. F. Sammartino, C. J. Baker, and H. D. Griffiths, "Frequency diverse mimo techniques for radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 1, pp. 201–222, 2013.

[12] Y. Liu, H. Ruan, L. Wang, and A. Nehorai, "The random frequency diverse array: a new antenna structure for uncoupled direction-range indication in active sensing," *IEEE Journal of Selected Topics in Signal Processing*, vol. 11, no. 2, pp. 295–308, 2016.

[13] F. Shu, X. Wu, J. Hu, J. Li, R. Chen, and J. Wang, "Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 890–904, 2018.

[14] T. Xie, J. Zhu, and Y. Li, "Artificial-noise-aided zero-forcing synthesis approach for secure multibeam directional modulation," *IEEE Communications Letters*, vol. 22, no. 2, pp. 276–279, 2017.

[15] J. Hu, F. Shu, and J. Li, "Robust synthesis method for secure directional modulation with imperfect direction angle," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1084–1087, 2016.

[16] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust synthesis scheme for secure multibeam directional modulation in broadcasting systems," *IEEE Access*, vol. 4, pp. 6614–6623, 2016.

[17] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.

[18] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-noise-aided secure multicast precoding for directional modulation systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6658–6662, 2018.

[19] Y. Ding and V. F. Fusco, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 1, pp. 361–370, 2014.

[20] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 918–931, 2018.

[21] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2450–2464, 2017.

[22] J. Xie, B. Qiu, Q. Wang, and J. Qu, "Broadcasting directional modulation based on random frequency diverse array," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 5051490, 12 pages, 2019.

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

[24] M. Hafez, T. Khattab, T. Elfouly, and H. Arslan, "Secure multiple-users transmission using multi-path directional modulation," in *Proceedings of the ICC International Conference on Communications*, May 2016.

[25] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure spatial multiple access using directional modulation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 1, pp. 563–573, 2018.

[26] T. Xie, J. Zhu, Q. Cheng, and Y. Guan, "Secure point-to-multipoint communication using the spread spectrum assisted orthogonal frequency diverse array in free space," *IEICE Transactions on Communications*, vol. E102.B, no. 6, pp. 1188–1197, 2019.

[27] Q. Cheng, V. Fusco, J. Zhu, S. Wang, and C. Gu, "SVD-aided multibeam directional modulation scheme based on frequency diverse array," *IEEE Wireless Communications Letters*, vol. 9, no. 3, pp. 420–423, 2020.

[28] B. Qiu, M. Tao, L. Wang, J. Xie, and Y. Wang, "Multi-beam directional modulation synthesis scheme based on frequency diverse array," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2593–2606, 2019.

[29] S. Y. Nusenu and A. Basit, "Frequency diverse array antennas: from their origin to their application in wireless communication systems," *Journal of Computer Networks and Communications*, vol. 2018, Article ID 5815678, 12 pages, 2018.

[30] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, UK, 2012.