Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 4715929, 14 pages
https://doi.org/10.1155/2020/4715929

Research Article

Artificial-Noise-Aided Energy-Efficient Secure Multibeam Wireless Communication Schemes Based on Frequency Diverse Array

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

[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 26 November 2019; Revised 3 February 2020; Accepted 21 February 2020; Published 24 June 2020

Academic Editor: Hui Cheng

In this paper, we research synthesis scheme for secure wireless communication in multibeam directional modulation (MBDM) system, which consists of multiple legitimate users (LUs) receiving their own individual confidential messages, respectively, and multiple eavesdroppers (Eves) intercepting confidential messages. We propose a new type of array antennas, termed frequency diverse arrays (FDA), to enhance security of confidential messages. Leveraging FDA technology and artificial noise (AN) technology, we aim to address the PHY security problem for MBDM by jointly optimizing the frequency offsets, the precoding matrix and the AN projection matrix. In the first stage, with known locations of Eves, precoding matrix is designed to minimize Eve's receiving power of confidential message (Min-ERP), while satisfying power requirement of LUs. And then artificial-noise projection matrix (ANPM) is calculated to enhance AN impact on Eves without influencing LUs. Furthermore, we research a more practical scenario, where locations of Eves are unknown. Unlike the scenario of the known locations of Eves, precoding matrix is designed to maximize AN transmit power (Max-ATP), while satisfying each LU's requirement received power of confidential message. In the second stage, we analyze and further optimize secrecy capacity. The problem is solved by optimizing frequency offsets through modified artificial bee colony (M-ABC) algorithm. Numerical results show that the proposed scheme can achieve a secure transmission in MBDM system.

1. Introduction

Wireless communication systems have gained considerable growth rate due to its merits, such as flexibility and convenience. However, Eves in free space may also receive confidential message due to broadcasting nature and lacking of physical boundaries of wireless communication. Therefore, many researchers have studied physical layer security of wireless communication in recent years. They focus on how to ensure confidential message with low probability of interception (LPI) and low probability of detection (LPD) on physical layer security [1, 2]. Antenna array technology has been put forward to achieve confidential message wireless communication with LPI and LPD.

Phased array, as a traditional antenna array, has been so far mainly employed in wireless communication. The directional gain offered by phased array antenna makes confidential message transmit in the desired directions. In [3, 4], the author optimized a group of phase shifters to transmit the baseband symbols along a desired direction. In [5], the author provided a bit error rate (BER) directional modulation (DM) method that the predefined BER is precisely controlled along a desired direction. More recently, the authors proposed a robust DM synthesis method for secure transmission in the presence of direction angle measurement errors [6]. But the above DM methods are dependent on phased array. Phased-array antenna produces only an angle focusing transmit beampattern. In free space, the ability of angle-range steering is necessary for secure wireless communication, and thus, a new type of antenna arrays should be considered.

In this paper, we abandon phased array and propose FDA for secure wireless communication due to its angle-range-dependent transmit beampattern [7–12]. FDA draws into small frequency offset across transmit element to produce a beampattern that changes as time, range, angle, and the frequency offset. However, the beampattern of FDA is highly coupled with angle and range, i.e., Eves which locate at other angle-range pairs can also receive the confidential message. To address this problem, much work focused on trying different form of the frequency offsets to decouple range-angle beampattern [13–15]. In [13], the authors employed a logarithmical frequency offset increment scheme, but its side lobe suppression is not satisfactory. The author employed square and cubic frequency increment method [14]. A new array structure, termed random frequency diverse arrays (RFDA), is proposed in [15] to decouple angle and range. Furthermore, in [16], synthesis strategy to optimize the beamforming vector based on RFDA is proposed to enhance secrecy performance of wireless communication. Multi-Input-Multi-Output (MIMO) combining with FDA is an effective method to decouple direction-range beampattern [17]. However, the system is extremely complex because each LU requires multiple transmit channels.

Moreover, in order to further improve secrecy performance, [18–20] focused on the AN-aided baseband technology, which can impose AN at Eves without influencing signal-to-noise-ratio (SNR) at LUs. An orthogonal AN-based approach was proposed in [21] to perform DM synthesis in the baseband. The authors in [11] proposed a dynamic synthesis method constructing a projection matrix to form artificial noises along undesired directions. The AN-based synthesis method was also combined with FDA to implement angle-range-dependent wireless communication. In [22], RFDA with AN DM scheme was proposed. The scheme achieves a better secrecy performance, but it cannot guarantee the maximum secrecy capacity due to its frequency randomness. In [23], the AN-aided secure transmission with FDA was proposed to achieve the security requirement for proximal LU and Eve. In [24], the authors investigated a multibeam synthesis scenario in broadcasting system, where the beamforming vector and frequency offsets are optimized by minimizing confidential message power leakage at the transmitter to Eves.

Unicast is the point-to-point communication. Multicast is the point to multipoint communication. But the basic concept of multicast is groups. Each point in a multicast group is called multicast group member, which receives specific data stream. Broadcasting is the point-to-all-point communication. And transmitter station broadcasts same message to all users. Actually, the system model in our paper is the special form of multicast, i.e., each multicast group has one LU. Therefore, we redefined our communication mode as multibeam wireless communication. Apart from the above-mentioned FDA-based wireless communication schemes only for unicast system, MBDM synthesis schemes with multiple LUs should also be investigated. Legitimate transmitter tries to transmit multiple independent streams of message to the multiple LUs located at different places in free space, respectively. Two novel energy-efficient MBDM schemes with known/unknown Eve's locations are proposed, respectively, in this paper. The secure wireless communication includes two aspects: preventing confidential message from being received by undesired LUs and minimizing the leakage of all confidential messages from transmitter to Eves. To address these secure problems, AN-based synthesis scheme combined with FDA is employed. Overall, the main contributions of our work are as follows:

(1) We extend secure wireless communications based on FDA from previous point-to-point communication to MBDM system. Unlike [24], the beamforming vector per LU is individually designed, which ensures the effective reception of intended LU with no interference from others. In particular, the proposed scheme achieves multiuser secure wireless communication in practical application scenario with unknown locations of Eves

(2) We design new optimization methods with known/unknown locations of Eves. These methods achieve secure multibeam wireless communication while improving the utilization of total transmit power

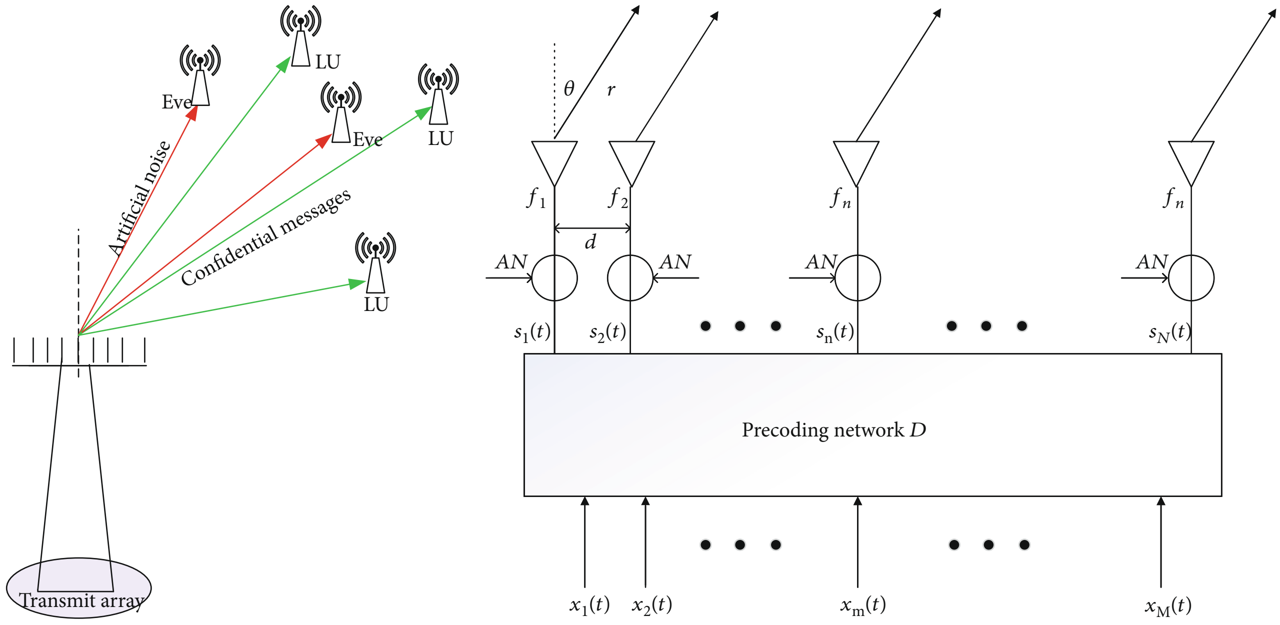
(3) We judiciously design the AN projection matrix to maximize the interference caused by AN to Eves, which makes Eves harder to decipher the confidential messages

(4) The scheme-based R-FDA can achieve a good secrecy performance, but it cannot guarantee the maximum secrecy capacity due to its frequency randomness. In view of this, in this paper, we propose a M-ABC algorithm that combines the global optimal solution idea of particle swarm optimization algorithm and crossover operation of genetic algorithm on the basis of ABC algorithm to obtain the time-invariant optimal frequency offsets, which further maximize the secrecy capacity of MBDM system

The rest of this paper is organized as follows. Section 2 details MBDM system model. Then, in Section 3, we propose high-performance MBDM synthesis schemes in two scenarios. The performance of the proposed scheme is numerically evaluated in Section 4, and then Section 5 draws conclusions.

2. System Model

In this section, we consider a basic MBDM system that transmitter station tries to transmit independent streams of message to multiple LUs located at different places in free space, respectively. And we assume there exist K passive Eves that are trying to intercept confidential messages. The architecture of MBDM system is shown in Figure 1(a), which consists of a legitimate transmitter station, M LUs, and K Eves. As shown in Figure 1(b), we assume that the transmitter array consists of N element linear antenna array with



(a)

(b)

Figure 1: (a) Model of MBDM system, (b) structure of transmit station.

uniform spacing d. The radiation frequency of nth antenna is $f_n = f_c + \Delta f_n$, for $n = 1, 2 \cdots N$, where f_c is the carrier frequency, Δf_n is the frequency offset which is controlled in $0 \le \Delta f_n \le \Delta F$ and $\Delta F \ll f_c$ in this paper. Define $f = [f_1, f_2, \cdots, f_N]^T$ is the frequency offset vector. Generally, we set the first element as the origin. 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

$$h(\theta, r, t, f) = \frac{\rho(r)}{\sqrt{N}} \left[e^{-j2\pi f_1 \left(t - \frac{r}{c}\right)}, e^{-j2\pi f_2 \left(t - \frac{r - d \sin \theta}{c}\right)}, \cdots, e^{-j2\pi f_N \left(t - \frac{r - (N-1) d \sin \theta}{c}\right)} \right]^T \in C^{N \times 1}, \tag{1}$$

where $\rho(r)$ is signal attenuation factor, and c refers to the light speed. For simplicity, $h(t)$ is defined as the instantaneous normalized steering vector of an arbitrary user located at (r, θ), i.e., $h(t) \Delta = h(\theta, r, t, f)$.

We assume that legitimate transmit station can estimate the locations of LUs and ignore estimated errors. To simplify the expression, the steering vectors of LUs can compose a steering matrix

$$H_L(t) \Delta = \left[h_{L_1}(t), h_{L_2}(t), \cdots, h_{L_m}(t), \cdots, h_{L_M}(t) \right]. \tag{2}$$

As shown in Figure 1(b), transmitter station is trying to transmit different confidential messages to M LUs located at different places in free space. $x_m(t)$ is the baseband symbol for mth LU. And the baseband symbols are assumed to be normalized, which means the average power $\mathbb{E}[|x_m(t)|^2] = 1$, for $m = 1, 2, \cdots, M$. There are M LUs in the system, so the transmitting vector x can be computed by combining the M symbol confidential messages

$$x = [x_1, x_2, \cdots, x_M]^T. \tag{3}$$

The precoding matrix D at the transmitter can be denoted as

$$D = [w_1(t, f), w_2(t, f), \cdots, w_M(t, f)], \tag{4}$$

where $w_m(t, f) = [w_{m,1}(t, f), w_{m,2}(t, f), \cdots, w_{m,N}(t, f)]^T$, for $m = 1, 2 \cdots, M$, is the beamforming vector of mth LU for processing confidential baseband signal $x_m(t)$.

AN-based DM method is also employed in wireless communication, which AN vector $z \sim \mathscr{CN}(0, I_N)$ is aided in baseband signal. Furthermore, the matrix $T_{\mathrm{AN}}(t)$ is designed to project z into the null space of steering vector at LU location, so the LU will not be affected by AN vector z. And the signal-to-interference-plus-noise ratio (SINR) will be significantly reduced at Eves, which makes Eve hard to intercept confidential messages. As shown in Figure 1(b), the radiating signal $s(t) = [s_1, s_2, \cdots, s_N]^T$ for the N antenna elements can be obtained by

$$s(t) = Dx(t) + \sqrt{P_{\mathrm{AN}}} n_{\mathrm{AN}}(t), \tag{5}$$

where P_{AN} is the power of AN, $n_{\mathrm{AN}}(t)$ is the normalized vector, which can be obtained by

$$n_{\mathrm{AN}}(t) = \frac{T_{\mathrm{AN}}(t) z}{\| T_{\mathrm{AN}}(t) z \|_2}. \tag{6}$$

The normalized LOS channel is considered in this paper. After passing through the LOS channel, the received signal of the mth LU is obtained by

$$\begin{aligned} y_{Lm}(t) &= h_{L_m}^H(t)s(t) + n_m(t) \\ &= h_{L_m}^H(t)w_m(t,f)x_m(t) + h_{L_m}^H(t)\sum_{i=1,i\neq m}^{M} w_i(t,f)x_i \\ &\quad + \sqrt{P_{\mathrm{AN}}}h_{L_m}^H(t)n_{\mathrm{AN}}(t) + n_m(t), \end{aligned} \tag{7}$$

where $n_m(t) \sim \mathscr{C}\mathscr{N}(0,\sigma_m^2)$ is the complex additive white Gaussian noise (AWGN) in mth LU channel with zero mean and variance σ_m^2.

3. Proposed Synthesis Schemes

In this section, we try to enhance secrecy performance of MBDM system by designing or optimizing the frequency offsets across transmit elements, the precoding matrix, and ANPM. The frequency offsets across transmit elements are optimized by M-ABC algorithm, and ANPM is calculated to interfere Eves without affecting the LUs. Specifically, in the first scenario with the prior known locations of Eves, the precoding matrix is designed by Min-ERP method. In the second scenario, with the unknown locations of Eves, the precoding matrix is designed by Max-ATP method.

3.1. Proposed Synthesis Scheme for MBDM with Known Eves. In the following, we assume that transmitter can estimate the location of Eve and ignore the estimated errors. Define the steering matrix of all Eves as

$$H_E(t)\Delta = \left[h_{E_1}(t), h_{E_2}(t), \cdots, h_{E_k}(t), \cdots, h_{E_k}(t)\right], \tag{8}$$

where $h_{E_k}(t)$ is the steering vector of kth Eve at (r_{E_k},θ_{E_k}), which can be expressed as

$$h_{E_k}(t) = \left[h_{E_{k1}}(t), h_{E_{k2}}(t), \cdots, h_{E_{kn}}(t), \cdots, h_{E_{kN}}(t)\right]^T, \tag{9}$$

where $h_{E_{kn}}(t) = a(r)e^{-j2\pi(f_c+\Delta f_n)[t-r_{Ek}-(n-1)dsin\theta_{E_k}/c]}$, $n = 1, 2, \cdots, N$, for the kth Eve at (r_{E_k},θ_{E_k}). The received signal vector of kth Eve is

$$\begin{aligned} y_{E_k}(t) &= h_{E_k}^H(t)s(t) + n_E(t) \\ &= h_{E_k}^H(t)\sum_{i=1}^{M} w_i(t,f)x_i + \sqrt{P_{\mathrm{AN}}}h_{E_k}^H(t)n_{\mathrm{AN}}(t) + n_{E_k}(t), \end{aligned} \tag{10}$$

where $n_{E_k}(t) \sim \mathscr{C}\mathscr{N}(0,\sigma_{E_k}^2)$ is the complex AWGN in kth Eve channel with zero mean and variance $\sigma_{E_k}^2$.

Without loss of generality, the total transmit power P_s is fixed. The scheme devises the Min-ERP to let Eves receive power as little as possible, while satisfying the basic secure requirements of LUs. Then, instantaneous precoding matrix $D(t)$ based on FDA can be expressed as $\min_{D(t)}\sum_{k=1}^{K}|h_{E_k}^H D(t)x|^2$, while the LU only receives its own confidential message and achievies the required receiving power.

$|h_{E_k}^H D(t)x|^2$ can be expressed as

$$\left|h_{E_k}^H D(t)x\right|^2 = \left|\sum_{i=1}^{i=M} h_{E_k}^H w_i(t,f)x_i\right|^2. \tag{11}$$

The precoding matrix $D(t)$ can be optimized by optimizing $w_m(m = 1, 2, \cdots, M)$ one by one. Therefore, the optimization problem can be equivalently expressed

$$\begin{aligned} &\min_{w_m(t,f)} \left|h_{E_k}^H(t)w_m(t,f)x_m(t)\right|^2 \\ &\text{s.t.}\mathrm{H}_L^H w_m(t,f) = \xi_{M\times1}, \end{aligned} \tag{12}$$

where $\xi_{M\times1} = [0, 0, \cdots, \sqrt{\xi_m}, \cdots, 0]^T$, in which ξ_m is the confidential message power received by mth LU, which satisfies the minimum secure requirement of MBDM system, for $m = 1, 2, \cdots, M$. The constraint in (12) is to make mth LU receive minimum desired received power of confidential message. Based on this, we can accurately control the received power of each LU by setting minimum desired received power of LUs.

According to $\mathbb{E}[|x_m(t)|^2] = 1$, positive definite quadratic form of (12) can be expressed as

$$\begin{aligned} &\min_{w_m(t,f)} \frac{1}{2}w_m^H(t,f)h_{E_k}(t)h_{E_k}^H(t)w_m(t,f) \\ &\text{s.t.}\mathrm{H}_L^H w_m(t) = \xi_{M\times1}. \end{aligned} \tag{13}$$

Actually, problem (13) can be solved by Lagrange multiplier. Thus, the optimal beamforming vector $w_m^*(t,f)$ is given by

$$w_m^*(t,f) = \left[\left(H_L^H(t)\left(h_{E_k}(t)h_{E_k}^H(t)\right)^{-1}H_L(t)\right)^{-1}H_L^H(t)\left(h_{E_k}(t)h_{E_k}^H(t)\right)^{-1}\right]^T\xi_{M\times1}. \tag{14}$$

Next, we design the projection matrix according to the rule that AN reduces the SINR of Eves seriously without affecting LUs receiving confidential messages. And we assume $N \geq M$. Thus, the optimization problem can be expressed as

$$\begin{aligned} &\max_{T_{\mathrm{AN}}(t)} \mathrm{tr}\left\{T_{\mathrm{AN}}^H(t)H_E(t)H_E^H(t)T_{\mathrm{AN}}(t)\right\} \\ &\text{s.t.}\mathrm{tr}\left\{T_{\mathrm{AN}}^H(t)T_{\mathrm{AN}}(t)\right\} = N - M, \\ &H_L^H(t)T_{\mathrm{AN}}(t) = 0. \end{aligned} \tag{15}$$

We first decompose the $H_L^H(t)$ by singular value decomposition (SVD)

$$H_L^H(t) = \left[U_L^{(1)}(t)U_L^{(0)}(t)\right] \begin{bmatrix} \overset{(1)}{\underset{L}{\sum}}(t) & 0 \\ 0 & 0 \end{bmatrix}, \left[V_L^{(1)}(t)V_L^{(0)}(t)\right] \tag{16}$$

where $\Sigma_L^{(1)}(t)$ is the $M \times M$ diagonal matrix. Based on the SVD characteristic [25], we know that $V_L^{(0)}(t)$ consists of $N-M$ right singular vectors corresponding to $N-M$ zero singular values, i.e., $H_L^H(t)v_i(t) = \mathbf{0}$, for $\{v_1(t), \cdots, v_i(t), \cdots, v_{N-M}(t)\} \in V_L^{(0)}(t)$. Define $B(t)\Delta = V_L^{(0)}(t)$ and $T_{\mathrm{AN}}(t)\Delta = B(t)X(t)$. Thus, problem (15) can be equivalently expressed as

$$\begin{gathered} \max_{X(t)} \mathrm{tr}\left\{X^H(t)B^H(t)H_E(t)H_E^H(t)X(t)B(t)\right\} \\ \mathrm{s.t.tr}\left\{X^H(t)X(t)\right\} = N-M. \end{gathered} \tag{17}$$

Problem (17) can be converted to

$$\begin{gathered} \max_{X(t)} \frac{(N-M)\mathrm{tr}\left\{X^H(t)B^H(t)H_E(t)H_E^H(t)X(t)B(t)\right\}}{\mathrm{tr}\left\{X^H(t)X(t)\right\}} \\ \mathrm{s.t.tr}\left\{X^H(t)X(t)\right\} = N-M. \end{gathered} \tag{18}$$

Actually, problem (18) is a Rayleigh quotient. Based on the generalized Rayleigh-Ritz theorem [25], the optimal solution $X^*(t)$ can be easily obtained. The optimal solution $X^*(t)$ is composed of eigenvectors corresponding to the $N-M$ largest eigenvalues of the matrix given by

$$(N-M)\left[B^H(t)H_E(t)H_E^H(t)B(t)\right]. \tag{19}$$

3.2. Proposed Synthesis Scheme for MBDM with Unknown Eves. In this subsection, we consider a more practical scenario, where the transmitter station does not estimate locations of Eves. With unknown locations of Eves, the steering vectors of Eves cannot be calculated. Thus, we propose Max-ATP method to optimize precording matrix $D(t)$. In this method, total transmit power P_s is fixed. We allocate ξ_m power to confidential message, which ξ_m is the minimum power secure requirement of MBDM system. Therefore, AN will obtain more power to prevent Eve intercepting confidential messages. Meanwhile, the remaining LUs cannot receive the confidential baseband signal $x_m(t)$ to mth LU. Therefore, the instantaneous beamforming vector $w_m(t,f)$ is obtained by the following maximized problem

$$\begin{gathered} \max_{w_m(t,f)} P_{\mathrm{AN}}(t) \\ \mathrm{s.t.}H_L^H(t)w_m(t,f) = \xi_{M\times 1}, \end{gathered} \tag{20}$$

where $\xi_{M\times 1} = \left[0, 0, \cdots, \sqrt{\xi_m}, \cdots, 0\right]^T$, in which ξ_m is the confidential message power received by mth LU, which satisfies the minimum secure requirement of MBDM system, for $m = 1, 2, \cdots, M$. Based on the fact $P_{\mathrm{AN}}(t) = P_s - \sum_{i=1}^M P_{L_i}(t)$, where P_s is the total transmit power, $P_{L_m}(t)$, for $m = 1, 2, \cdots, M$, is the power of confidential message in mth LU and $P_{L_m} = \|w_m(t,f)\|_2^2$, for $m = 1, 2, \cdots, M$. Thus, we can rewrite (20) as

$$\begin{gathered} \min_{w_m(t,f)} \|w_m(t,f)\|_2^2 \\ \mathrm{s.t.}H_L^H(t)w_m(t,f) = \xi_{M\times 1}. \end{gathered} \tag{21}$$

Actually, positive definite quadratic form of (21) can be expressed as

$$\begin{gathered} \min_{w_m(t,f)} \frac{1}{2} w_m^H(t,f)w_m(t,f) \\ \mathrm{s.t.}H_L^H(t)w_m(t,f) \geq \xi_{M\times 1}. \end{gathered} \tag{22}$$

Problem (22) can be solved by Lagrange multiplier. Thus, the optimal beamforming vector $w_m^*(t,f)$ is given by

$$w_m^*(t,f) = H_L(t)\left(H_L(t)^{\mathrm{H}}H_L(t)\right)^{-1}\xi_{M\times 1}^H. \tag{23}$$

The artificial noise vector z generally does not lie in $\mathrm{span}(H_L(\mathrm{t}))$. And next, we design the ANPM $T_{\mathrm{AN}}(t)$ to project the aided AN to the null space of the steering vectors of all LUs. Based on the null-space projection rule and according to formula (7), the ANPM is designed by

$$\sum_{m=1}^M \left|h_{L_m}^H(t)n_{\mathrm{AN}}(t)\right|^2 = 0. \tag{24}$$

Note that $\mathbb{E}[zz^H] = I_N$ and $n_{\mathrm{AN}}(t) = T_{\mathrm{AN}}(t)z/\|T_{\mathrm{AN}}(t)z\|_2$ (24) can be equivalently expressed as

$$\mathrm{tr}\left\{T_{\mathrm{AN}}^H(t)H_L(t)H_L^H(t)T_{\mathrm{AN}}(t)\right\} = 0. \tag{25}$$

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

$$T_{\mathrm{AN}}(t) = I_N - H_L(t)\left[H_L^H(t)H_L(t)\right]^{-1}H_L^H(t). \tag{26}$$

3.3. Analysis and Optimize Average Secrecy Capacity. In this subsection, we first analyze the secrecy performance of aforementioned schemes. In this paper, we adopt the secrecy sum rate (SSR) as the main performance metric to evaluate the secrecy performance, which is defined as

$$C(t) \triangleq |C_L(t) - C_E(t)|^2, \tag{27}$$

where $C_L(t)$ is the achievable rate of the link from transmitter to LUs, which can be expressed as

$$C_L(t) \triangleq \sum_{m=1}^{M} \log_2(1+\xi_m), \tag{28}$$

$C_E(t)$ is the achievable rate of the link from transmitter to Eve at the time t. Firstly, we assume transmitter knows the locations of Eves. We obtain $C_E(t)$ by the following formula

$$\begin{aligned} C_E(t) &\triangleq \sum_{k=1}^{K} C_{E_k}(t) \\ &= \sum_{k=1}^{K} \log_2\left(1+\mathrm{SINR}_{E_k}\right) \\ &= \sum_{k=1}^{K} \log_2\left(1+\frac{\left|h_{E_k}^H(t)\sum_{i=1}^{M} w_i(t,f)\right|^2}{P_{\mathrm{AN}}\mathbb{E}\left[\left|h_{E_k}^H(t) n_{\mathrm{AN}}(t)\right|^2\right]+\sigma_E^2}\right). \end{aligned} \tag{29}$$

In the following, we consider the scenario that transmitter station does not know or estimate locations of Eves. In the scenario, Eves can exist everywhere outside the main lobes of all LUs. Thus, the location interval of Eve can be defined as

$$\begin{aligned} \Theta_E &\triangleq \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \setminus \bigcup_{m=1}^{M} \Theta_L^m, \\ \Omega_E &\triangleq [r_{\min}, r_{\max}] \setminus \bigcup_{m=1}^{M} \Omega_L^m, \end{aligned} \tag{30}$$

where $\Theta_L^m = [(\theta_L^m - \theta_{\mathrm{BW}})/2, (\theta_L^m + \theta_{\mathrm{BW}})/2]$ and $\Omega_L^m = [(r_L^m - r_{\mathrm{BW}})/2, (r_L^m + r_{\mathrm{BW}})/2]$ denote the main lobes of the mth LU, for $m = 1, 2, \cdots, M$, with θ_{BW} and r_{BW} being the beamwidth of angle and range, respectively. To simplify the expression, we define the wiretap area as $S_{\mathrm{wire}}\Delta = [\Theta_E, \Omega_E]$. Then, $C_{E_k}(t)$ can be expressed as the following form:

$$\begin{aligned} C_E(t) &\triangleq \sum_{k=1}^{K} C_{E_k}(t) \le K\log_2\left(1+\max_{\left(\theta_{E_k}, r_{E_k}\right)\in S_{\mathrm{wire}}} \mathrm{SINR}_{E_k}\right) \\ &= K\log_2\left(1+\max_{\left(\theta_{E_k}, r_{E_k}\right)\in S_{\mathrm{wire}}} \frac{\left|h_{E_k}^H(t)\sum_{i=1}^{M} w_i(t,f)\right|^2}{P_{\mathrm{AN}}\mathbb{E}\left[\left|h_{E_k}^H(t) n_{\mathrm{AN}}(t)\right|^2\right]+\sigma_E^2}\right). \end{aligned} \tag{31}$$

It is obvious to find that SSR $C(t)$ of proposed scheme is a complex expression of parameter f in the scenario with known/unknown locations of Eves, respectively. Our target is to achieve secure wireless communication of MBDM system. To this end, we can further maximize SSR by appropriately selecting the frequency offsets. Mathematically, the maximized problem is formulated as

$$\begin{aligned} &\max_f C(t) \triangleq \left|C_L(t) - C_E(t)\right|^2 \\ &\text{s.t.} f_c \le f_n \le f_c + \Delta F, \forall n. \end{aligned} \tag{32}$$

According to (28), the optimization problem is equivalent to the following expression:

$$\begin{aligned} &\min_f C_E(t) \\ &\text{s.t.} f_c \le f_n \le f_c + \Delta F, \forall n. \end{aligned} \tag{33}$$

According to Equations (29) and (31), the objective function $C_E(t)$ is intractable because of the nonconvex characteristic and tightly coupled variables. Therefore, we employ suboptimal intelligent algorithm to solve this difficult optimization problem. The artificial bee colony (ABC) algorithm has advantage in dealing with high dimensional optimization complex problems, so compared with other intelligent algorithms, ABC algorithm is more suitable for large-scale array antennas. And ABC algorithm was inspired by the particular foraging behavior of honeybee in nature, which consists of honey source and three kinds of bees. Honey source represents all possible solutions in the global scope, and the three kinds of bees represent the employed bees, the onlooker bees, and the scout bees, respectively. The number of employed bees and onlooker bees is set as NP, and the number of honey source is equal to them. Therefore, the group of solutions is composed of NP N-dimensional vectors, where the ith solution vector is expressed as $f_i = [f_{i_1}, f_{i_2}, \cdots, f_{i_N}]$, for $i = 1, 2, \cdots, \mathrm{NP}$. In the process of studying the ABC algorithm, we found its two shortcomings as follows:

(1) The search formula of ABC algorithm is expressed as

$$f_{i_n}^{g} = f_{i_n}^{g-1} + \varphi\left(f_{i_n}^{g-1} - f_{k_n}^{g-1}\right), i \ne k. \tag{34}$$

where g represents the current iteration number, $f_{i_n}^{g}$ is the new nth element of the ith solution vector in g iteration, $f_{i_n}^{g-1}$ is the old nth element of the ith solution vector in $g-1$ iteration, $f_{k_n}^{g-1}$ is the old nth element of the kth solution vector in $g-1$ iteration, for $n = 1, 2, \cdots, N$, $i = 1, 2, \cdots, \mathrm{NP}$, and $k = 1, 2, \cdots, \mathrm{NP}$. φ is the random number between [-1, 1]. From (34), we observe that the search formula only iterates in the vector direction of $\varphi(f_{i_n}^{g-1} - f_{k_n}^{g-1})$ and is lack of consideration for global optimality. Therefore, the algorithm may fall into the local optimal solution due to insufficient global exploration ability. In order to help the algorithm to jump out of the local extremum and avoid prematurity, we modify the search formula by referring to the particle swarm optimization algorithm,

$$f_{i_n}^{g} = f_{i_n}^{g-1} + \varphi\left(f_{i_n}^{g-1} - f_{k_n}^{g-1}\right) + \beta\left(f_{\text{global}_n} - f_{i_n}^{g-1}\right), i \neq k. \quad (35)$$

where f_{global_n} represents the current optimal nth element of all solution vectors, β is the random number between $[0, 1]$. Compared with (34), we add the global guiding factor $(f_{\text{global}_n} - f_{i_n}^{g-1})$, so that the bee search has a strong direction and purpose. Furthermore, we add an influence factor β in front of the global factor, which is used to constrain the search amplitude. From the factor composition, it can be seen that if there is a big gap between the current solution and the optimal solution, the updated step size will increase dynamically. Otherwise, it approaches slowly.

(2) The employed bee that has been eliminated in iteration process will be transformed into a scout bee, which will randomly initialize a honey source for search mission. However, in the next iteration, the new honey source will be compared with other honey sources that have evolved many times. The new honey source has a small chance of winning, so it will lead to the rapid loss of individual diversity, and the algorithm will quickly converge to the local extremum. To solve this problem, the search formula (35) is further optimized by combining the crossover operation in genetic algorithm. In each iteration, a specified number of honey sources were randomly selected according to the crossover rate to produce the same number of filial generation.

$$f_{i_n}^{g} = \begin{cases} f_{i_n}^{g-1} + \varphi\left(f_{i_n}^{g-1} - f_{k_n}^{g-1}\right) + \\ \beta\left(f_{\text{global}_n} - f_{i_n}^{g-1}\right), i \neq k, \text{rand } (0, 1) < cr, \\ \lambda f_{i_n}^{g-1} + (1-\lambda) f_{j_n}^{g-1}, i \neq j, \text{else}. \end{cases} \quad (36)$$

where cr is the crossover rate, and λ is the random number between $[0, 1]$.

Therefore, in this paper, we propose a M-ABC algorithm that combines the global optimal solution idea of particle swarm optimization algorithm and crossover operation of genetic algorithm on the basis of ABC algorithm.

In summary, the detailed procedure of M-ABC algorithm is given in:

Step 1. Initialize the settings. In this paper, the solution vector is frequency offset vector. Randomly generate the initial frequency offset vector $f_i = [f_{i_1}, f_{i_2}, \cdots, f_{i_N}]$, for $i = 1, 2, \cdots, \text{NP}$. The fitness value was calculated according to $\text{fit} = 1/1 + C_E$.

Step 2. The employed bees search new solution according to modified search formula (36) and calculate its fitness value. If the fitness value of the new solution is better than the old solution, solution is updated; otherwise, the old solution is retained.

Table 1: Simulation parameters.

Parameter	Value
Carrier frequency f_c	1 GHz
Number of FDA elements N	32
Interelement spacing d	$c/2f_c$
Number of LUs M	4
Number of Eves K	2
Receive noise power for both LUs, 10 log (σ_m^2)	-100 dBm
Receive noise power for both Eves, 10 log (σ_E^2)	-100 dBm
Location of LU1, $(r_{L1}), \theta_{L1})$	(3500 m, 30°)
Location of LU2, $(r_{L2}), \theta_{L2})$	(3500 m, 40°)
Location of LU3, $(r_{L3}), \theta_{L3})$	(4000 m, 35°)
Location of LU4, $(r_{L4}), \theta_{L4})$	(4500 m, 40°)
Location of Eve1, $(r_{E1}), \theta_{E1})$	(4000 m, 45°)
Location of Eve2, $(r_{E2}), \theta_{E2})$	(3750 m, 35°)

Step 3. Calculate all fitness values of f_i, and calculate the probability values according to the following formula

$$p_i = \frac{\text{fit}_i}{\sum_{i=1}^{\text{NP}} \text{fit}_i}. \quad (37)$$

Step 4. The onlooker bees choose the honey source f_i by the roulette method, and search new solution according to modified search formula (36), and calculate its fitness value.

Step 5. Judge whether there is a discarded honey source. If there is, the employed bee transforms into scout bee. The scout bee generates new random honey source according to formula

$$f_{i_n} = f_{\min} + \text{rand } (0, 1)(f_{\max} - f_{\min}), \quad (38)$$

where $f_{\min}$ and $f_{\max}$ represent the lower limit and upper limit of the search space, respectively.

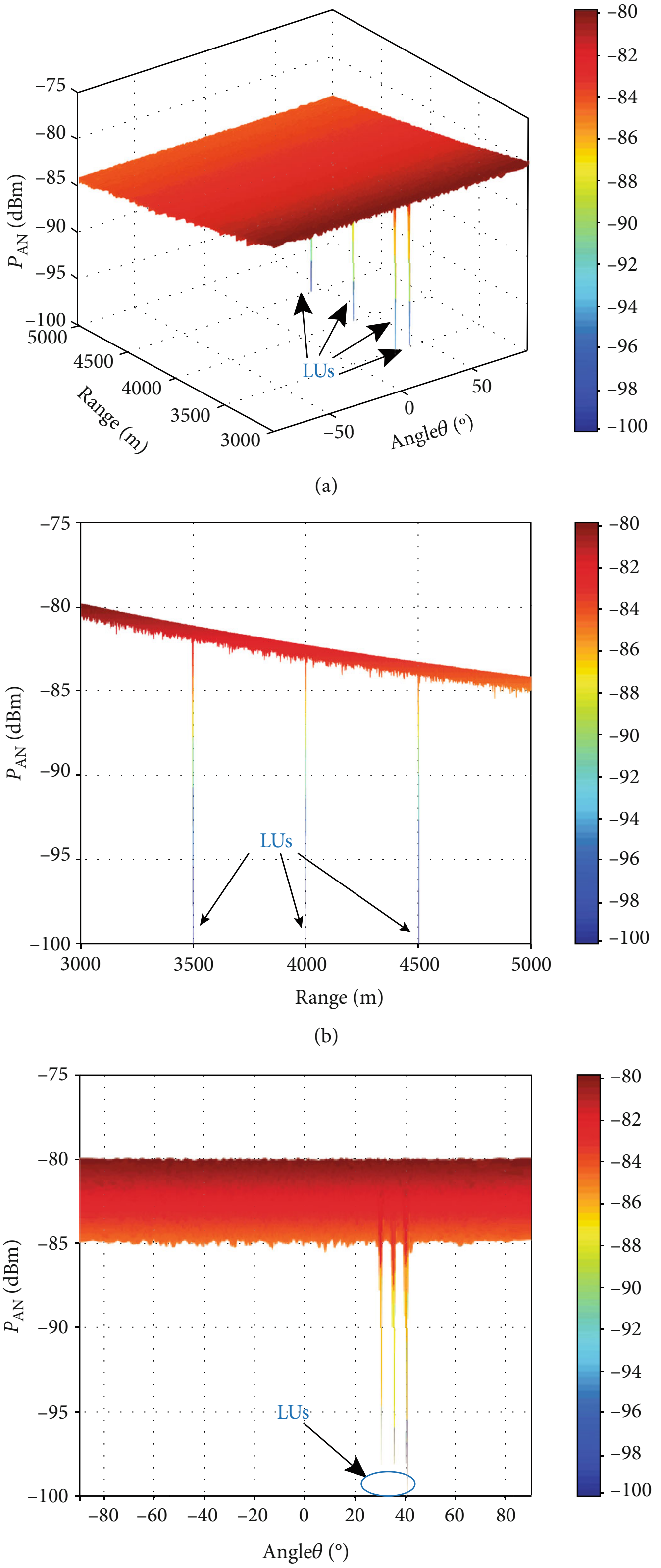
Step 6. Record the best frequency offset vector so far.

Step 7. Rerun from step 2 until the maximal iterations G are achieved or a threshold is obtained.

Step 8. Determine the optimal frequency offset vector f^*.

4. Performance Analysis and Simulation

In this section, we analyze and numerically simulate AN power distribution, focusing performance and secrecy performance of the proposed energy-efficient MBDM synthesis schemes. The considered application scenario and structure of FDA array are determined as shown in Figure 1. Unless



(a)

(b)

(c)

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

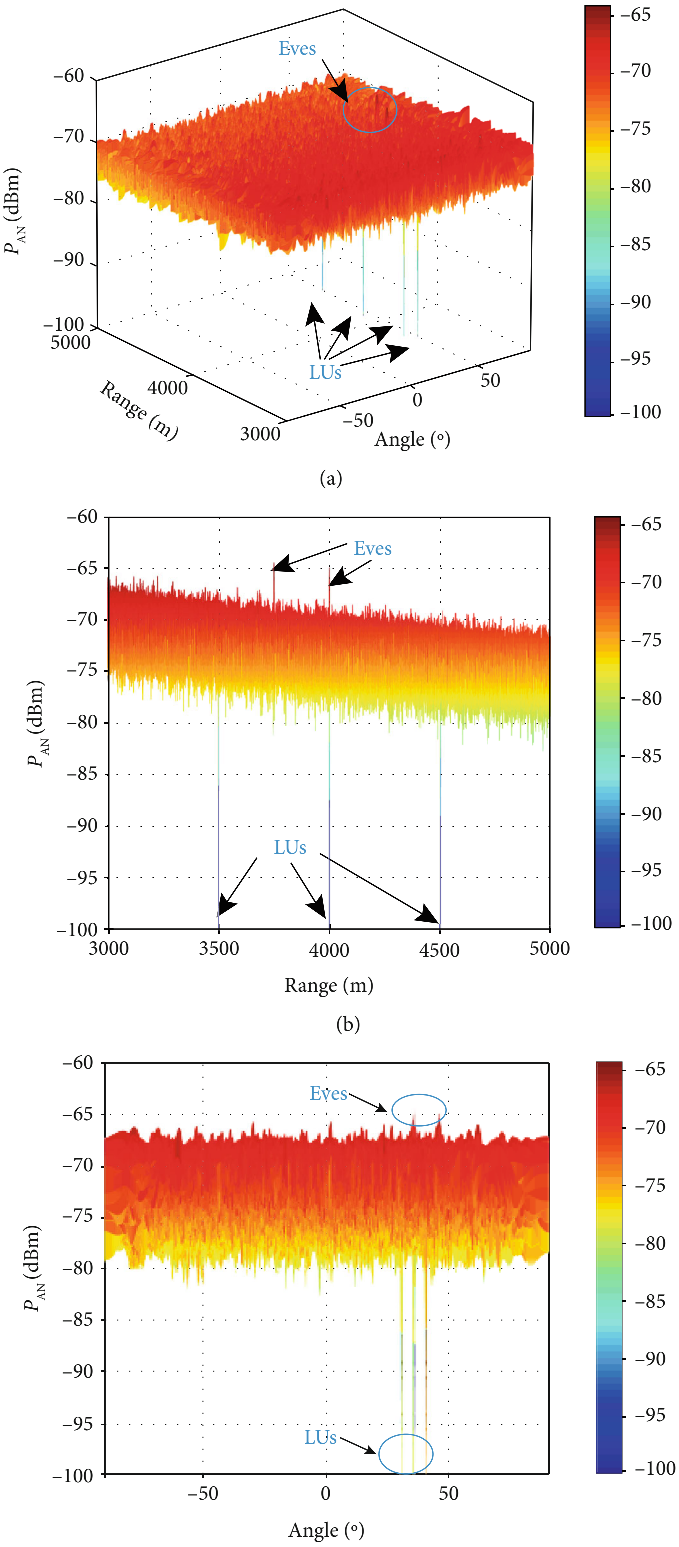


Figure 3: The AN power spatial performance versus with the known locations of Eves (a) angle-range, (b) angle dimension, and (c) range dimension, where $N = 32$, $P_s = 40$ dBm.

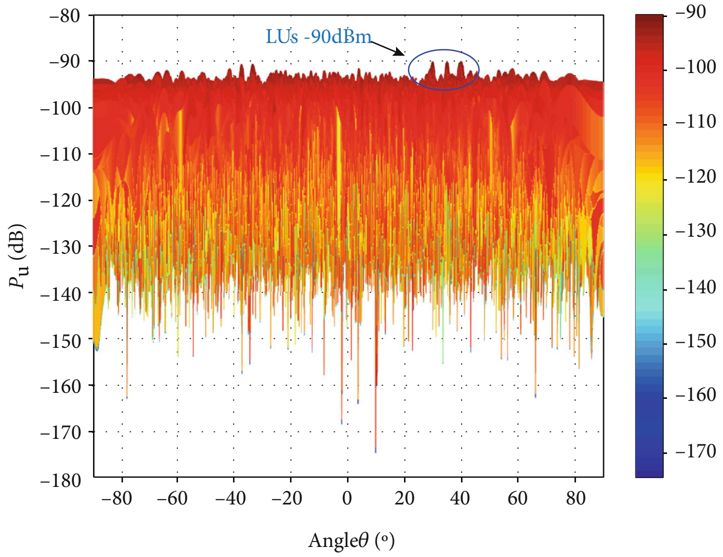


FIGURE 4: The confidential message power spatial performance versus angle-range, where $N = 32$, $P_s = 40$ dBm.

stated otherwise, the simulation parameters are listed in Table 1. The signal attenuation factor $\rho(r)$ is obtained by the free space path loss formula of radio wave propagation (39), i.e.,

$$\begin{aligned}\mathrm{Lfs(dB)} &= -20\log\left[\rho(r)\right]\\ &= 32.5 + 20\log\left[f_c(\mathrm{MHz})\right] + 20\log\left[r(\mathrm{km})\right],\end{aligned} \tag{39}$$

where f_c is carrier frequency in megahertz (MHz), and r is the range in kilometer.

4.1. Analysis of AN Power Distribution. In this paper, we design matrix $T_{\mathrm{AN}}(t)$ to project AN vector z into the null space of steering vector at LUs. Meanwhile, the SINR of Eves is significantly reduced. In the subsection, we plot AN energy distribution versus range-angle dimensions to validate our design of ANPM $T_{\mathrm{AN}}(t)$.

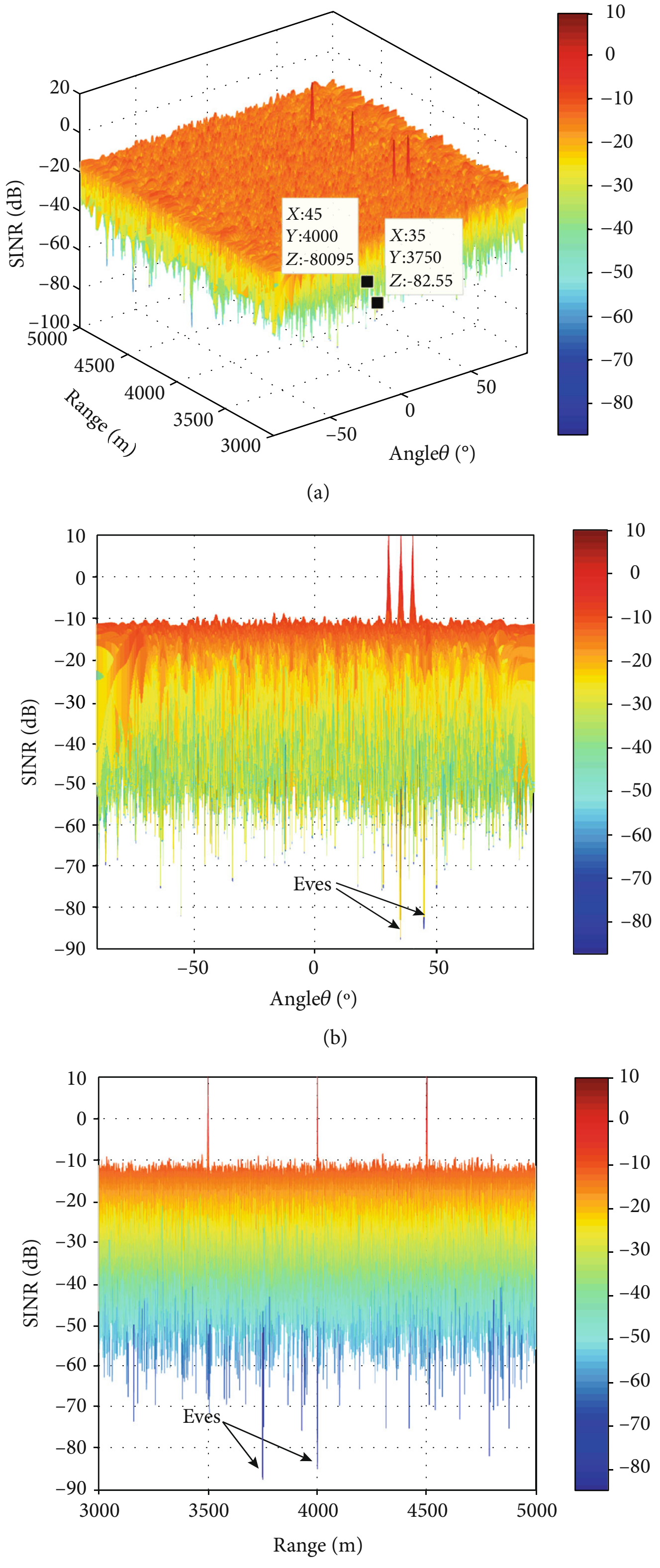
Figure 2 plots AN energy distribution versus range-angle dimensions with unknown locations of Eves and Figure 3 plots AN energy distribution versus range-angle dimensions with the known locations of Eves. From Figures 2 to 3, we can observe that (1) there are four minimal values at coordinates of LUs in Figures 2 and 3, respectively, which means AN cannot influence LUs receiving confidential messages and (2) there are three peaks at the locations of Eves in Figure 3, which means that, with known locations of Eves, we can design ANPM based on the method to maximize AN influence on Eve. Moreover, AN is uniformly distributed versus angle-range dimensions outside the main lobes of all LU coordinates in Figure 2. This is because, without prior known Eves' locations, we can only uniformly distribute AN power in free space outside LUs' locations to prevent Eves intercepting confidential messages, since Eves could exist anywhere.

4.2. Proposed Schemes Focusing Performance Analysis. As previously mentioned, FDA focusing depends on range-angle dimensions whereas the focusing of phased array only depends on angle dimension. In this subsection, we plot confidential message energy distribution versus range-angle dimensions and SINR distribution versus range-angle dimensions to measure the focusing performance of MBDM system. In this simulation, the minimum required receiving power of all LUs are set as $\sqrt{\xi_1} = \sqrt{\xi_2} = \sqrt{\xi_3} = \sqrt{\xi_4} = -90$ dBm in the two scenarios.

In this simulation, the spatial power distribution of the confidential messages (i.e., with no AN) in the range dimension without prior knowledge of Eves' location is explored in Figure 4. It is clear that there are four sharp peaks corresponding to each of the LU. Moreover, all of these power values are almost equal to -90 dBm, which confirm the accurate control of minimum required received power, and therefore, the energy efficiency can be effectively improved. The spatial power distribution of the confidential message (i.e., with no AN) with known locations of Eves has similar results.

In the scenario with prior knowing the locations of Eves, Figure 5 illustrates SINR distribution in free space versus angle-range dimensions of the optimization scheme in Section 3.1. It is easy to see from Figure 5 that there are four sharp peaks corresponding to each of the LU. Meanwhile, values of SINR are low at other place, especially at the Eves locations. This illustrates that (1) the LUs can receive the confidential message effectively; (2) in the Eves locations, it is hard to detect the message; (3) the angle-range beampattern has been successfully decoupled by the optimization approach in Section 3.1; and (4) we achieve satisfaction focusing on the performance of the MBDM system in the scenario with prior knowing the locations of Eves.

In the scenario with the unknown locations of Eves, Figure 6 illustrates SINR distribution in free space versus angle-range dimensions of the optimization scheme in Section 3.2. It also can be observed that SINR distribution

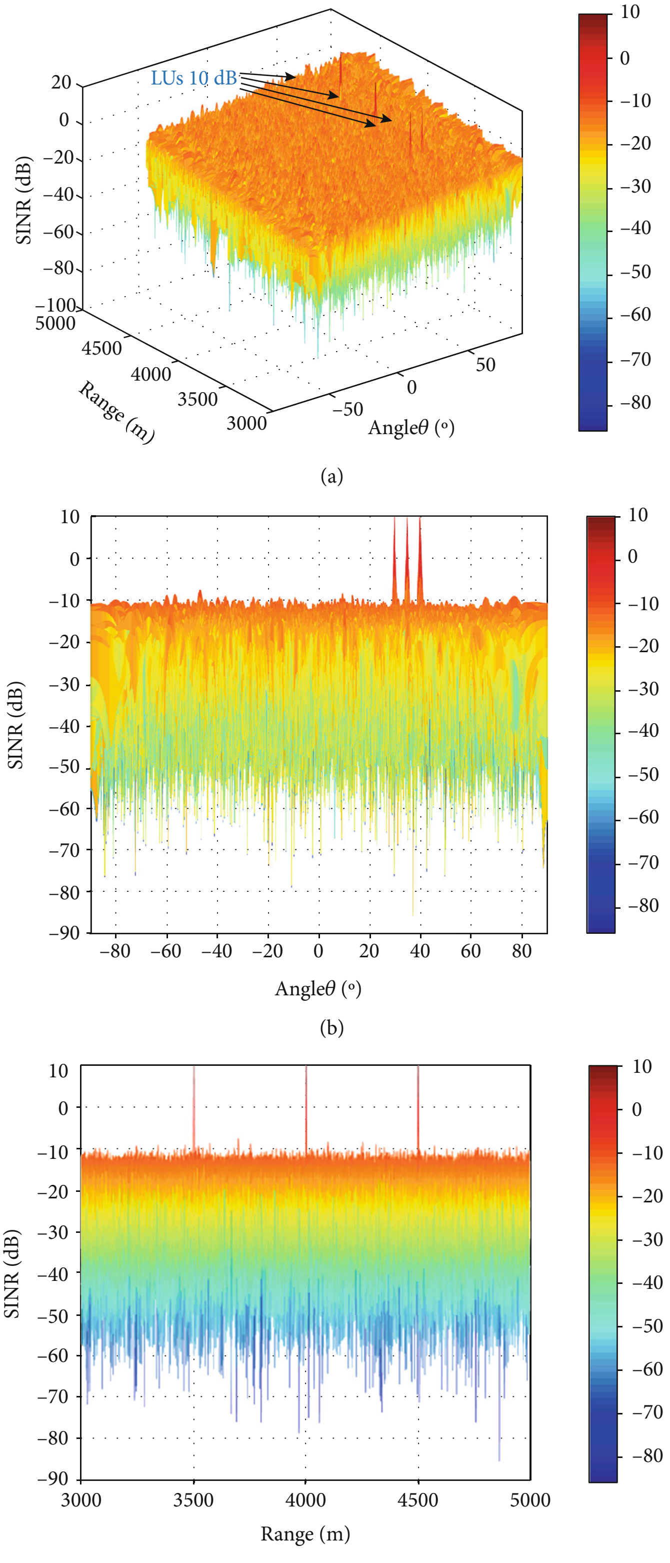


(a)

(b)

(c)

Figure 5: The SINR performance with known locations of Eves based on proposed method (a) versus angle-range, (b) angle dimension, and (c) range dimension, where $N = 32$, $P_s = 40$ dBm.



(a)

(b)

(c)

Figure 6: The SINR performance with unknown locations of Eves based on proposed method (a) versus angle-range, (b) angle dimension, and (c) range dimension, where $N = 32$, $P_s = 40$ dBm.

is thumbtack-like, and only peak is synthesized around the locations of LUs. This indicates that the angle-range beampattern has been successfully decoupled by the optimization approach in Section 3.2, and we achieve satisfaction focusing on the performance of the MBDM system in the scenario with the unknown locations of Eves.

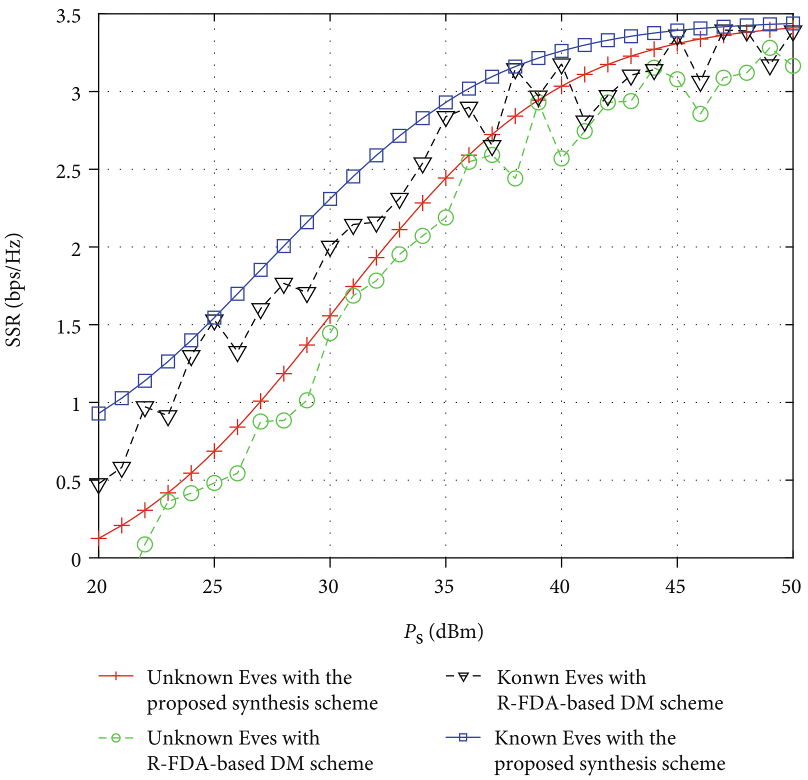


FIGURE 7: The SSR comparison for different FDA configurations versus total power P_s, where $N = 32$.

4.3. Proposed Schemes Secrecy Performance Analysis. Secrecy capability is an important metric to measure the secrecy performance of wireless communication systems. In this subsection, we will analyze the secrecy capability of the energy-efficient multicast directional modulation schemes.

Here, we adopt SSR to evaluate the secrecy capability. In the subsection, we consider two FDA configurations. One is the proposed FDA which uses the frequency offsets optimized by M-ABC algorithm, and the other is the R-FDA using random increasing frequency offsets [15], i.e., $f_n = f_c + \Delta f_n$, $n = 1, 2 \cdots, N$, where f_c is the carrier frequency and $\Delta f_n = \eta_n \Delta f$ is a random frequency increment.

In the simulation, we illustrate the secrecy capacity versus the total transmit power P_s among the proposed synthesis scheme and R-FDA-based DM scheme. From Figure 7, it is clear that (1) the secrecy capacity of the proposed scheme is consistently better than another method; (2) the secrecy capacity of the R-FDA-based scheme is unstable since the frequency offsets are randomly chosen, and hence, it cannot guarantee the secrecy capacity; and (3) with the increment of total transmit power, the secrecy capacity can be enhanced.

5. Conclusion

With the assistance of the FDA technology, two AN-aided energy-efficient secure multibeam wireless communication schemes with known/unknown locations of Eves were proposed, respectively. The operation mode was extended from previous point-to-point communication to the point to multipoint mode. We achieve wireless physical layer secure transmissions for multiple LUs in free space receiving their own confidential messages, respectively. To accomplish this goal, several important tools have been utilized like frequency offsets optimization, precoding matrix optimization, and null space projection of AN. AN power distribution, focusing performance, and secrecy performance were analyzed and simulated, which verified the advantages of the proposed schemes.

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 is no conflict of interest.

Acknowledgments

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

References

[1] 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.

[2] 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.

[3] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Transactions on Antennas and Propagation*, vol. 57, no. 9, pp. 2633–2640, 2009.

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

[5] Y. Ding and V. F. Fusco, "Directional modulation far-field pattern separation synthesis approach," *IET Microwaves, Antennas & Propagation*, vol. 9, no. 1, pp. 41–48, 2015.

[6] 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.

[7] 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.

[8] W. Q. Wang, "Range-angle dependent transmit beampattern synthesis for linear frequency diverse arrays," *IEEE Transactions on Antennas and Propagation*, vol. 61, no. 8, pp. 4073–4081, 2013.

[9] 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.

[10] 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.

[11] 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 Transactions on Information Forensics and Security.*, vol. 13, no. 3, pp. 671–684, 2018.

[12] W. Q. Wang, "Retrodirective frequency diverse array focusing for wireless information and power transfer," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 61–73, 2019.

[13] 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, no. 1, pp. 499–502, 2015.

[14] 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.

[15] 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, 2017.

[16] 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.

[17] 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.

[18] S. Yan, N. Yang, I. Land, I. Malaney, and J. Yuan, "Three articial-noise aided secure transmission schemes in wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 1–1, 2018.

[19] S. Wan, F. Shu, J. Lu et al., "Power allocation strategy of maximizing secrecy rate for secure directional modulation networks," *IEEE Access*, vol. 6, no. 99, pp. 38794–38801, 2018.

[20] 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.

[21] 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.

[22] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Articial-noise aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 99, pp. 1658–1667, 2017.

[23] B. Qiu, J. Xie, L. Wang, and Y. Wang, "Artificial-noise-aided secure transmission for proximal legitimate user and eavesdropper based on frequency diverse arrays," *IEEE Access*, vol. 6, pp. 52531–52543, 2018.

[24] 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.

[25] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge,U.K., 1987.