Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 5051490, 11 pages
https://doi.org/10.1155/2019/5051490

Research Article

Broadcasting Directional Modulation Based on Random Frequency Diverse Array

Jian Xie,[1,2] **Bin Qiu**,[2] **Qiuping Wang**,[2] **and Jiaqing Qu**[3]

[1]*Research and Development Institute of Northwestern Polytechnical University in Shenzhen, Shenzhen 518057, China*
[2]*Electronics and Information School, Northwestern Polytechnical University, Xi'an, 710072, China*
[3]*Shanghai Radio Equipment Research Institute, Shanghai, 200090, China*

Correspondence should be addressed to Jian Xie; xiejian@nwpu.edu.cn

Received 8 January 2019; Revised 10 April 2019; Accepted 5 May 2019; Published 20 May 2019

Academic Editor: Minseok Kim

Frequency diverse array- (FDA-) based directional modulation (DM) is a promising technique for physical layer security, due to its angle-range dependent transmit beampattern. However, the existing schemes are not suitable for the broadcasting scenario, where there are multiple legitimate users (LUs) to receive the confidential message. In this paper, we propose a novel random frequency diverse array- (RFDA-) based DM scheme to realize the point to multi-point broadcasting secure transmission in both angle and range dimension. In the first stage, the beamforming vector is designed to maximize the artificial noise (AN) power, while satisfying the power requirement of LUs for transmitting the confidential message simultaneously. In the second stage, the AN projection matrix is obtained by maximizing signal-to-interference-plus-noise ratio (SINR) at the LUs. The proposed scheme only broadcasts the confidential message to the locations of LUs while the other regions are covered by AN, which promotes the security of the wireless broadcasting system. Moreover, it is energy efficient since the power of each LU is under accurate control. Numerical simulations are presented to validate the performance of the proposed scheme.

1. Introduction

Compared with wired communication, the evolution of wireless technology has brought many advancements with its effective features, such as flexibility, scalability, and low cost. However, the openness nature of wireless communication also makes it vulnerable to interception. Unintended receivers may also receive the confidential information, with eavesdroppers (Eves) amongst them. Therefore, the security problem of physical layer wireless transmission has attracted considerable attention in recent years.

Directional modulation (DM), as a new type of physical layer wireless security technology, allows preserving the signal format along a predefined secure communication direction while disturbing the constellation of the signal along other directions. Therefore, the low probability of interception (LPI) and low probability of detection (LPD) can be obtained for security wireless transmission. In [1, 2], based on near-field direct antenna modulation, an analogue transmit architecture was proposed, which can prevent the eavesdroppers from correctly demodulating the signal. For the far-field scenario, a similar modulation scheme was demonstrated by adjusting each element's phase shift properly [3, 4], so that the constellation of each symbol can be obtained in the derided direction and purposely distorted in other directions. However, these synthesis schemes require high speed radio frequency switches or phase shifters to be switched at the modulation rate, which limits their realization and application. In [5, 6], the authors proposed novel orthogonal vector synthesis approaches based on the combination of excitation signal and artificial noise (AN) vectors, which can be realized digitally at baseband. Note that AN-aided DM can guarantee the signal-to-noise-ratio (SNR) at the legitimate user (LU) location and impose AN at the location of eavesdropper. To enhance the robustness against direction measurement error, Hu et al. proposed a DM synthesis algorithm based on conditional minimum mean square error [7]. In [8], an orthogonal projection (OP) scheme was generalized for the synthesis of multi-beam DM systems. In [9], the authors proposed an AN-aided

zero-forcing synthesis approach for multi-beam DM, which is efficient and simple in realization. Shu et al. in [10] proposed a robust multi-beam DM synthesis algorithm by considering imperfect and unknown eavesdropper directions, respectively. In [11], the robust scheme has been generalized for the multi-user multiple-input and multiple output (MU-MIMO) scenario. To maximize the secrecy rate of the AN-based DM systems, Yu et al. [12] and Wan et al. [13] proposed two novel optimization schemes: general power iterative based beamforming scheme and secrecy rate based power allocation strategy. Moreover, Zhou et al. [14] proposed a robust and secure DM technique for amplify-and-forward relaying networks.

However, all of these DM methods are based on phased array. Accordingly, the physical layer transmission security is not guaranteed when the LUs and Eves are located along an identical direction. Therefore, it is natural to investigate other schemes that can achieve secure wireless communications at joint range-angle dimension.

As a promising technique, frequency diverse array (FDA) delivers new opportunities for secure wireless communications and has received abundant attention recently. Even though FDA can be deemed as a special transmit beamforming on phased array, there are some differences between them. The essential difference between phased array and FDA lies in that there are small frequency increments across FDA's elements [15–17], while the phased array's elements share the same carrier frequency. Consequently, the beampattern of phased array is only dependent on the angle, while FDA's beampattern depends on both angle and range parameters [18–21]. Due to this property, FDA has promising potentials in the applications of radar [22–24], sensing [25], and wireless communication systems [26]. However, the coupling of angle and range in FDA's beampattern still limits its capability in some specific applications. To address this problem, several non-linearly increasing frequency offsets approaches have been investigated to decouple FDA's range-angle beampattern [27–29]. In [27], a logarithmic frequency increments scheme has been proposed, but its range dimension performance is not satisfactory. In [28], square and cubic frequency increments are proposed, which performs better in both decoupled transmit beamforming and target localization. Furthermore, by assigning FDA's each element with a random carrier frequency, the authors in [29] proposed a random frequency diverse array (RFDA). Its beampattern is thumbtack-like, which means the angle-range correlation can be effectively decoupled in active sensing.

Based on these properties, FDA has become an efficacious technique for DM to achieve LPI and LPD at joint range-angle dimension. Specifically, utilizing the uniform linear array and symmetrical configuration of frequency increments, the authors in [26] proposed an FDA-based DM scheme. By scrambling the constellation at undesired regions in both range and angle dimensions, the solution can provide secure point-to-point communications. In [30], the authors extended their previous work to secure QPSK and 16-ary wireless communications by using 2-bit phase controls across the array elements. Furthermore, Hu et al. [31] first and normally propose to combine RFDA and DM for secure wireless communication. By maximizing the SNR at the desired user location and transmitting AN at Eve's location, its secrecy capacity is superior to phased array-based DM and linear FDA. Unfortunately, the phase shifters are synthesized by complicated optimization algorithms, which cause the optimal position to be time-variant. Therefore, by utilizing nonlinear logarithmically increasing frequency offsets, the authors in [32] developed a time-invariant angle-range dependent DM based on FDA. In [33], an AN-based DM technique with RFDA was proposed to address the physical layer security problem for closely located legitimate user and eavesdropper. In [34], the authors further proposed a multi-beam DM synthesis scheme based on FDA, where the beamforming vector and frequency offsets are obtained by maximizing the signal-to-leakage-noise ratio (Max-SLNR) from the transmitter to Eves. Taking the receiver complexity into consideration, Shu et al. [35] proposed a secure and precise wireless transmission scheme by replacing RFDA with random subcarrier selection based on OFDM, which can effectively reduce the hardware budget in the medium-scale and large-scale systems.

Despite the various advantages of FDA-based DM scheme that were manifested in the approaches cited above, there are some fundamentally inherent problems to be overcome in view of the previous analyses.

(1) Most of the above-mentioned RFDA-based DM schemes focus on the point to point communication; the broadcasting point to multipoint scenario without any prior knowledge of the Eves' location has not been addressed.

(2) The received power of the legitimate user cannot be precisely controlled according to its link budget; thus the percentage of total transmission energy used for legitimate user's confidential message is not optimized.

Aiming at addressing the above-mentioned problems for wireless broadcasting systems, in this paper, we propose a novel energy-efficient multi-beam DM scheme based on RFDA. More specifically, we consider the scenario that multiple legitimate users are located at different positions known a priori, while the locations of Eves are unavailable at the transmitter. Consequently, the main objective of our synthesis method is to broadcast the confidential message towards different legitimate users with each power under control and impose AN at other regions to avoid the interception by Eves. First, the beamforming vector of the confidential message is designed by maximizing the AN transmit power budget (Max-ATP). Then, the AN projection matrix is obtained by maximizing signal-to-interference-plus-noise ratio (Max-SINR) at the LUs. The main contributions in this paper can be summarized as follows:

(1) We proposed an energy efficient broadcasting DM scheme based on RFDA, in which the power of each LU is under accurate control. Particularly, the link budget of each LU can be taken into account to assure that the power of the confidential message at each legitimate receiver is large enough for a satisfactory communication performance. Consequently, the proposed approach has the ability to accurately control the efficiency of the total radiated energy.

(2) It does not require any prior knowledge of the Eves' location, which is more suitable for the practical applications.

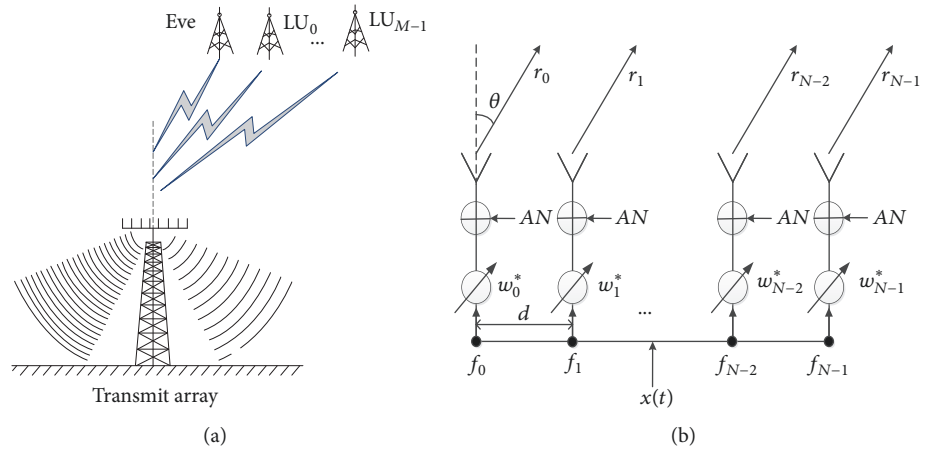


Figure 1: (a) Model of broadcasting RFDA-DM system; (b) AN-based RFDA-DM structure.

And the corresponding secrecy capacity of the proposed broadcasting system has been evaluated theoretically.

2. System Model

As is shown in Figure 1(a), the secure multi-beam broadcasting system is composed of one transmitter with an N-element uniform linear array (ULA) antenna and M LUs as receivers. Unlike the traditional phased array-based broadcasting system, in RFDA, the radiation frequency of the nth element is

$$f_n = f_c + \Delta f_n, \quad n = 0, 1, \ldots, N-1, \tag{1}$$

where f_c is the carrier frequency and $\Delta f_n = \eta_n \Delta f$ is a random frequency increment. It is assumed that $\eta_n, n = 0, \ldots, N-1$, are independent and identically distributed random variables. Therefore, the distribution of η_n determines a random mapping rule for the radiating frequencies of each array elements. Even though the methods in [31] are applicable for any mapping rule, in this paper, we utilize the continuous uniform frequency allocation algorithm. Thus, η_n is a random variable with its probability density function (PDF) being $p(\eta_n) = 1$ and $\eta_n \in [-0.5, 0.5]$.

In the far-field scenario, the range between a receiver and the n-th element can be expressed as

$$r_n = r - nd \sin\theta, \quad n = 0, 1, \ldots, N-1, \tag{2}$$

where (θ,r) is a specific angle and range parameter pair of the receiver's location with the first element being the reference point, d is the inter-element spacing of the ULA.

AN-aided DM beamforming scheme has been widely utilized in the context of secure wireless communication owing to its robustness and secrecy performance. In view of these previous works, we establish a unified framework for AN-aided broadcasting DM system based on RFDA. Considering the DM scheme for secure wireless transmission, as shown in Figure 1(b), the broadcasting message at the antenna array is given by

$$\mathbf{s}(t) = \mathbf{w}(t)\, x(t) + \sqrt{P_{AN}}\mathbf{n}_{AN}(t), \tag{3}$$

where $x(t)$ is the symbol of complex transmitting confidential message with average power $\mathbb{E}[|x(t)|^2] = 1$, $\mathbf{w}(t) = [w_0(t), w_1(t), \ldots, w_{N-1}(t)]^T$ is the beamforming vector for broadcasting the message to desired LUs. P_{AN} is the power of AN, $\mathbf{n}_{AN}(t)$ is the normalized AN, which can be expressed as

$$\mathbf{n}_{AN}(t) = \frac{\mathbf{T}_{AN}(t)\,\mathbf{z}}{\left\|\mathbf{T}_{AN}(t)\,\mathbf{z}\right\|_2}, \tag{4}$$

where $\mathbf{T}_{AN}(t)$ is the projection matrix for controlling the spatial distribution of AN, $\mathbf{z}$ is the artificial noise vector with its PDF being $\mathbf{z} \sim \mathcal{CN}(0, \mathbf{I}_N)$.

To simplify, we assume that the channels between transmitter and receivers are line of sight (LOS). Therefore, the instantaneous steering vector of a LU located at (θ,r) is written as

$$\begin{aligned}\mathbf{h}(\theta, r, t) = \frac{1}{\sqrt{N}} \Big[& \rho(r)\, e^{-j2\pi f_0 (t - r/c)}, \rho(r_1) \\ & \cdot e^{-j2\pi f_1 (t - (r - d\sin\theta)/c)}, \ldots, \rho(r_{N-1}) \\ & \cdot e^{-j2\pi f_{N-1} (t - (r - (N-1)d\sin\theta)/c)} \Big]^T,\end{aligned} \tag{5}$$

where $\rho(r_n)$ is the path loss factor due to the free space propagation from the n-th element to the receiver. Based on the fact that $r \gg (N-1)d$, we can have a reasonable approximation $\rho(r) = \rho(r_0) = \ldots = \rho(r_{N-1})$. To simplify the expression, $\mathbf{h}_{U_m}(t)$ is denoted as the instantaneous steering vector of the m-th LU, i.e., $\mathbf{h}_{U_m}(t) \triangleq \mathbf{h}(\theta_{U_m}, r_{U_m}, t)$. Since all DM transmitters should know the desired direction angle (position) of the legitimate users in advance before beamforming, the DOA estimation or source localization methods in [36, 37] can be utilized for the estimation of these parameters.

Consider that there are M LUs at different locations; therefore, the broadcasting channel steering matrix can be defined as

$$\mathbf{H}_U(t) \triangleq \left[\mathbf{h}_{U_0}(t), \mathbf{h}_{U_1}(t), \ldots, \mathbf{h}_{U_m}(t), \ldots, \mathbf{h}_{U_{M-1}}(t)\right]. \tag{6}$$

Without loss of generality, we assume that all LUs are corrupted by additive white Gaussian noise (AWGN). Therefore, the received signal vector of the LUs can be expressed as

$$\begin{aligned}\mathbf{y}_U(t) &= \mathbf{H}_U^H(t)\,\mathbf{s}(t) + \mathbf{n}_U(t)\\ &= \underbrace{\mathbf{H}_U^H(t)\,\mathbf{w}(t)\,x(t)}_{\text{Broadcasting message}} + \underbrace{\sqrt{P_{AN}}\mathbf{H}_U^H(t)\,\mathbf{n}_{AN}(t)}_{\text{Artificial noise}}\\ &\quad + \underbrace{\mathbf{n}_U(t)}_{\text{Noise}},\end{aligned} \tag{7}$$

where $\mathbf{n}_U(t) = [n_{U_0}(t), n_{U_1}(t), \ldots, n_{U_{M-1}}(t)]^T$ is the complex AWGN noises vector with the distribution $n_m(t) \sim \mathcal{CN}(0, \sigma_m^2)$.

Based on the system and signal model of RFDA-DM presented above, an efficient synthesis scheme is prposed in the next section for secure multi-beam DM in broadcasting systems.

3. Proposed Broadcasting RFDA-DM Scheme

3.1. Synthesis Scheme for the RFDA-DM. In this section, our major goal is to design or optimize the beamforming vector such that high secrecy performance can be achieved for broadcasting the confidential message to multiple LUs while the location of Eve is unknown. Without loss of generality, for a given total transmit power budget P_s, the proposed scheme first maximizes the AN transmit power (Max-ATP) to allocate power to AN as much as possible while satisfying the power requirement of LUs. Consequently, the instantaneous beamforming vector $\mathbf{w}(t)$ can be synthesized by the following optimization problem:

$$\begin{aligned}\max_{\mathbf{w}(t)} \quad & P_{AN}(t)\\ \text{s.t.} \quad & \mathbf{w}^H(t)\,\mathbf{H}_U(t) \geq \boldsymbol{\zeta},\end{aligned} \tag{8}$$

where $\boldsymbol{\zeta} \triangleq [\sqrt{\zeta_0}, \sqrt{\zeta_1}, \ldots, \sqrt{\zeta_m}, \ldots, \sqrt{\zeta_{M-1}}]$. ζ_m is the minimum required receiving power of the mth LU, for $m = 0, 1, ..M-1$. Actually, due to the fixed total transmit power, less useful signal transmit power means more allocation of AN allocation power, which makes Eve hard to detect the broadcasting useful signals.

Utilizing the allocation power of AN, we can rewrite (8) as

$$\begin{aligned}\max_{\mathbf{w}(t)} \quad & P_s - P_U(t)\\ \text{s.t.} \quad & \mathbf{w}^H(t)\,\mathbf{H}_U(t) \geq \boldsymbol{\zeta},\end{aligned} \tag{9}$$

where P_U is the power of the broadcasting signal and $P_U = \|\mathbf{w}(t)\|_2^2$, P_s is the total transmit power. Therefore, the optimization problem in (9) is equivalent to the following problem:

$$\begin{aligned}\min_{\mathbf{w}(t)} \quad & P_U(t)\\ \text{s.t.} \quad & \mathbf{w}^H(t)\,\mathbf{H}_U(t) \geq \boldsymbol{\zeta},\end{aligned} \tag{10}$$

Actually, the problem in (10) can be solved by the method of Lagrange multipliers [38]. For simplicity, we can omit the arguments of (t) in the following derivation. The cost function can be constructed as

$$L(\mathbf{w}) = \mathbf{w}^H\mathbf{w} + \left(\mathbf{w}^H\mathbf{H}_U - \boldsymbol{\zeta}\right)\boldsymbol{\lambda}^H, \tag{11}$$

where $\boldsymbol{\lambda}$ is the Lagrange multiplier vector. Based on the Lagrange multiplier theorem [38], the optimum solution of $\mathbf{w}^*$ can be obtained when the gradient of L equals $\mathbf{0}$, i.e.,

$$\frac{\partial L(\mathbf{w})}{\partial(\mathbf{w}^H)} = \mathbf{w} - \mathbf{H}_U\boldsymbol{\lambda}^H = \mathbf{0}, \tag{12}$$

Therefore, we have

$$\mathbf{w} = \mathbf{H}_U\boldsymbol{\lambda}^H. \tag{13}$$

Inserting (13) into $\mathbf{w}^H\mathbf{H}_U = \boldsymbol{\zeta}$, the Lagrange multiplier vector can be calculated as

$$\boldsymbol{\lambda} = \boldsymbol{\zeta}\left(\mathbf{H}_U^{\mathrm{H}}\mathbf{H}_U\right)^{-1}. \tag{14}$$

Therefore, the Max-ATP problem (8) can be solved by

$$\mathbf{w}^*(t) = \mathbf{H}_U(t)\left(\mathbf{H}_U(t)^{\mathrm{H}}\,\mathbf{H}_U(t)\right)^{-1}\boldsymbol{\zeta}^H. \tag{15}$$

In the following stage, our objective is to design the AN projection matrix $\mathbf{T}_{AN}(t)$. Based on the null-space projection rule and assuming that $N \geq M$, the AN projection matrix can be calculated by maximizing the average receive SINR at the desired receivers

$$\max_{\mathbf{T}_{AN}(t)} \quad \text{SINR}, \tag{16}$$

where $\text{SINR} \triangleq \text{tr}\{\mathbf{H}_U^H(t)\mathbf{w}(t)\mathbf{w}^H(t)\mathbf{H}_U(t)\}/(P_{AN}\mathbb{E}\{\text{tr}[\mathbf{H}_U^H(t)\mathbf{n}_{AN}(t)\mathbf{n}_{AN}^H(t)\mathbf{H}_U(t)]\} + \sigma_U^2)$. Following the derivation presented in [38], it can be converted to the following equivalent problem:

$$\min_{\mathbf{T}_{AN}(t)} \frac{P_{AN}\text{tr}\left\{\mathbf{H}_U^H(t)\,\mathbf{n}_{AN}(t)\,\mathbf{n}_{AN}^H(t)\,\mathbf{H}_U(t)\right\}}{\text{tr}\left\{\mathbf{H}_U^H(t)\,\mathbf{w}(t)\,\mathbf{w}^H(t)\,\mathbf{H}_U(t)\right\}}. \tag{17}$$

Note that $\mathbb{E}[\mathbf{z}\mathbf{z}^H] = \mathbf{I}_N$. Given the beamforming vector, the denominator of objective function is constant, then the minimization of the objective function means that

$$\text{tr}\left\{\mathbf{T}_{AN}^H(t)\,\mathbf{H}_U(t)\,\mathbf{H}_U^H(t)\,\mathbf{T}_{AN}(t)\right\} = 0. \tag{18}$$

Therefore, the AN projection matrix is given by [38]

$$\mathbf{T}_{AN}(t) = \mathbf{I}_N - \mathbf{H}_U(t)\left[\mathbf{H}_U^H(t)\,\mathbf{H}_U(t)\right]^{-1}\mathbf{H}_U^H(t). \tag{19}$$

3.2. Analysis of Average Secrecy Capacity. In this section, we analyze the secrecy performance of the proposed broadcasting RFDA-DM scheme. Specifically, we adopt the secrecy capacity as the main performance metric to evaluate the secrecy performance. Firstly, as the locations of Eves are

unavailable at the transmitter, all locations outside the main lobes of the LUs' locations are defined as the potential location of Eve, which can be expressed as

$$\Theta_E \triangleq \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \setminus \bigcup_{m=0}^{M-1} \Theta_U^m,$$
$$\Omega_E \triangleq [r_{\min}, r_{\max}] \setminus \bigcup_{m=0}^{M-1} \Omega_U^m, \tag{20}$$

where $\Theta_U^m = [\theta_U^m - \theta_{BW}/2, \theta_U^m + \theta_{BW}/2]$ and $\Omega_U^m = [r_U^m - r_{BW}/2, r_U^m + r_{BW}/2]$ denote the main lobes of the mth LU, for $i = 0, 1, \ldots, M-1$, with θ_{BW} and r_{BW} being the beamwidth of angle and range, respectively. To simplify the expression, we define the wiretap area as $S_{wire} \triangleq [\Theta_E, \Omega_E]$. Then we define the instantaneous secrecy capacity as

$$C(t) \triangleq \max\left\{0, \min_{(\theta_E, r_E) \in S_{wire}} \left(\overline{C}_U - C_E(t)\right)\right\}, \tag{21}$$

where $\overline{C}_U$ is the average achievable capacity of LUs, and $C_E(t)$ is the achievable capacity of Eve at the time t, which is of the following form:

$$\overline{C}_U \triangleq \frac{1}{M} \sum_{m=0}^{M-1} \log_2\left(1 + \zeta_m\right), \tag{22}$$

and

$$C_E(t) \triangleq \log_2\left(1 + \mathrm{SINR}_E\right) = \log_2\left(1 + \frac{\left|\mathbf{h}^H(\theta_E, r_E, t)\,\mathbf{w}(t)\right|^2}{P_{AN}\mathbb{E}\left[\left|\mathbf{h}^H(\theta_E, r_E, t)\,\mathbf{n}_{AN}(t)\right|^2\right] + \sigma_E^2}\right). \tag{23}$$

4. Simulation Results and Analysis

In this section, numerical simulations are conducted to illustrate the secrecy performance of the proposed broadcasting RFDA-DM scheme. The geometry of the RFDA-DM array is illustrated in Figure 1. The carrier frequency is f_c = 1GHz. The receiver noise power of both LUs and Eve is assumed to be −100dBm, i.e.,$10\log(\sigma_U^2) = 10\log(\sigma_E^2) = -100$dBm. And the inter-element spacing is half a wavelength, i.e., $d = c/2f_c$. The locations of four LUs are set as $(r_{U_0}, \theta_{U_0}) = (1500\text{m}, 30^\circ)$, $(r_{U_1}, \theta_{U_1}) = (2000\text{m}, 60^\circ)$, $(r_{U_2}, \theta_{U_2}) = (2500\text{m}, -30^\circ)$, and $(r_{U_3}, \theta_{U_3}) = (3000\text{m}, -60^\circ)$. The signal attenuation factor $\rho(r)$ is determined by the free space path loss formula of radio wave propagation [39], i.e.,

$$\begin{aligned}\mathrm{Lfs}\,(\mathrm{dB}) &= -20\log\left[\rho(r)\right] \\ &= 32.5 + 20\log\left[f_c\,(\mathrm{MHz})\right] \\ &\quad + 20\log\left[r\,(\mathrm{km})\right],\end{aligned} \tag{24}$$

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

In the first experiment, we investigate the spatial power distribution of the AN. The number of array elements is set as $N = 64$, and the total power of the transmitter is P_S = 40dBm. According to Figure 2, it is clear that power of the AN is uniformly distributed in the joint angle-range spatial dimension. This is because that, without priori knowledge of Eves' location, it is reasonable to impose AN uniformly to prevent the confidential message from interception as much as possible, since Eves could exist anywhere in the 2D spatial dimension. However, note that, from Figures 2(b) and 2(c), there are four deep nulls at the the locations of LUs, which means the LUs will not be affected by the artificial noise. Moreover, it is obvious from Figure 2(b) that the power of the AN attenuates as the distance increases from the transmitter, which is more suitable for the practicable applications.

In the second experiment, the spatial power distribution of the confidential broadcasting signal is explored. The same parameters as the first experiment are adopted, and the four LUs have the same minimum required receiving power, which is set as $\sqrt{\zeta_0} = \sqrt{\zeta_1} = \sqrt{\zeta_2} = \sqrt{\zeta_3} = -90$dBm. In Figure 3(a), we illustrate the power distribution of useful signal in the angle-range dimension, (i.e., without AN). It is clear that, due to the free space path loss of radio wave propagation, the power of useful signal decreases as the distance increases from the transmitter. Moreover, from Figure 3(b), one can observe that there are four sharp peaks corresponding to each of the LU. Moveover, all of these power values almost equal −90dBm, which confirms the accurate control of each broadcasting signal and therefore, the energy efficiency can be effectively improved.

In the third experiment, the SINR distribution is studied with different parameter settings. We consider three scenarios with different values of array elements N and total transmit power P_s. It is assumed that $N = 16$ and P_s = 40dBm for scenario 1, $N = 64$ and P_s = 40dBm for scenario 2, and $N = 16$ and P_s = 50dBm for scenario 3. The four LUs have the same minimum required receiving power, which is set as $\sqrt{\zeta_0} = \sqrt{\zeta_1} = \sqrt{\zeta_2} = \sqrt{\zeta_3} = -90$dBm in all of the three scenarios. The SINR distributions of the three scenarios are illustrated in Figures 4(a), 4(b), and 4(c), respectively. In Figure 4(c), it can be seen that there are only four SINR peaks values at the locations of LUs, which means (1) the LUs can receive the confidential message effectively; (2) in the other locations, it is hard for the interceptors to detect the message; (3) the angle and range correlation have been successfully decoupled. From the comparison between Figures 4(a) and 4(b), we can conclude that, with the increment of the array elements, the secrecy of the proposed RFDA-DM scheme improves. This phenomenon is in agreement with the theoretical analyses that the transmit array has a narrower beam and the degree of freedom (DoF) for the weight vector has increased. From the comparison between Figures 4(a) and 4(c), it is clear that as the total transmit power increases, the secrecy of the proposed scheme also enhances. This can be explained that, for a given receiver power constraint, more transmit power can be assigned to AN, and therefore, the SINR of non-LU locations can be effectively suppressed to promote the secrecy.

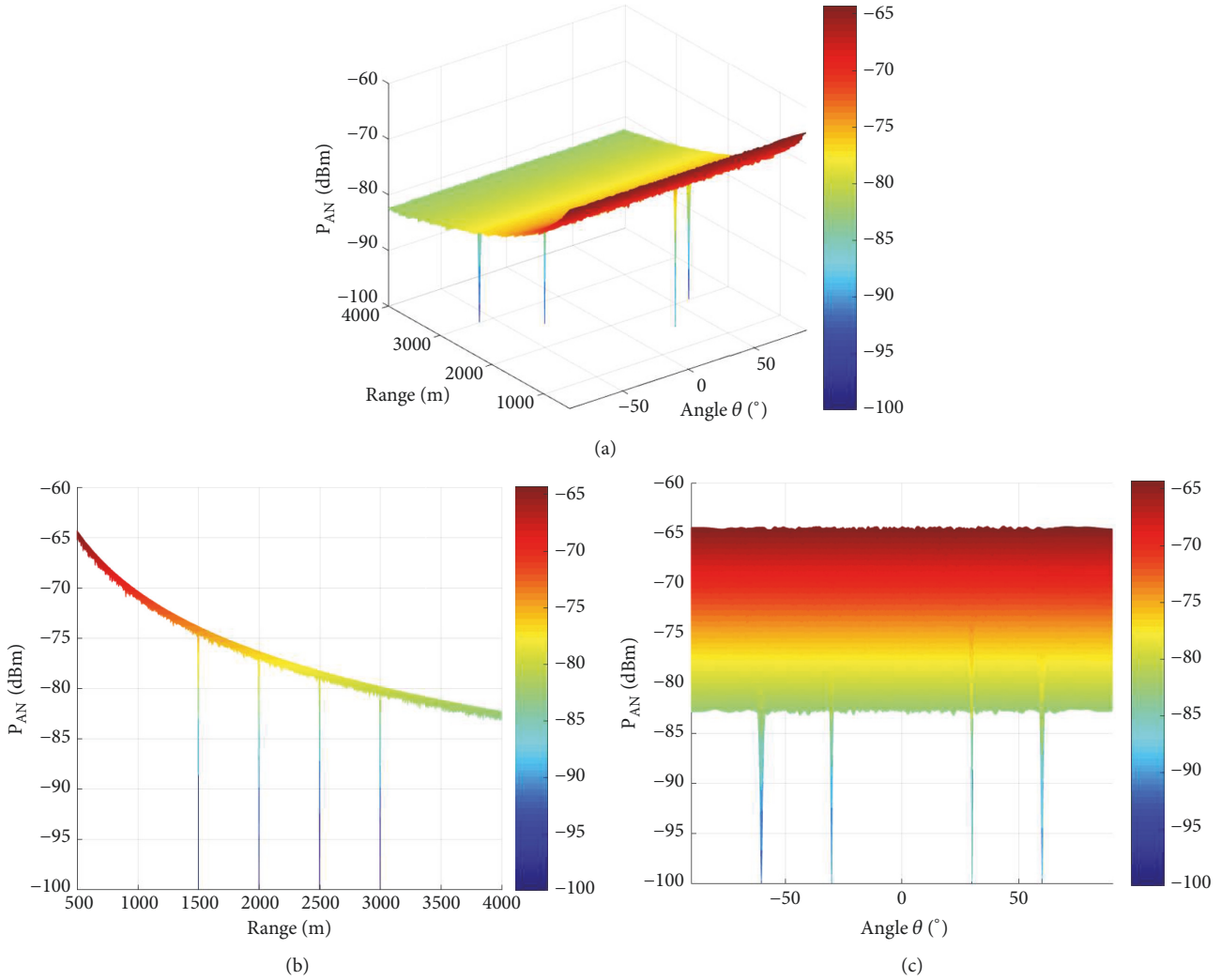


Figure 2: The power distribution of the AN versus (a) angle-range dimension, (b) range dimension, and (c) angle dimension.

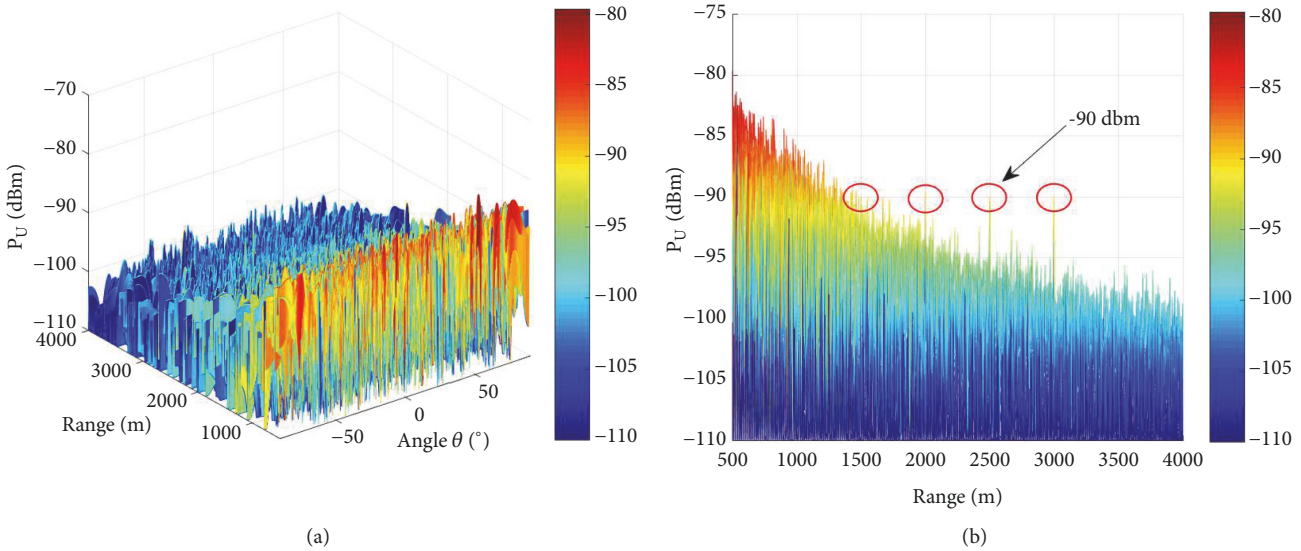


Figure 3: Power distribution of confidential message versus (a) angle-range, (b) range dimension, where N=64, P_s=40 dBm.

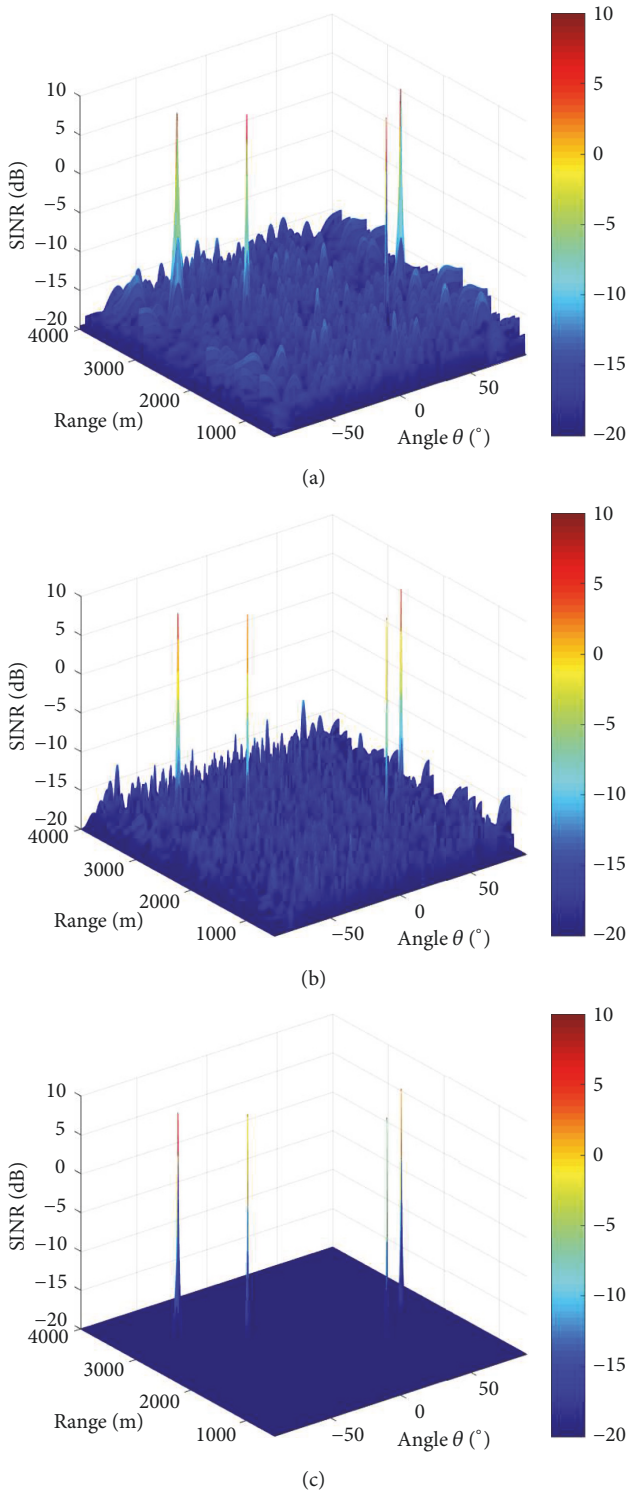


FIGURE 4: The SINR distribution of the proposed method (a)N=16, P_s=40 dBm. (b)N=64, P_s=40 dBm. (c)N=16, P_s=50 dBm.

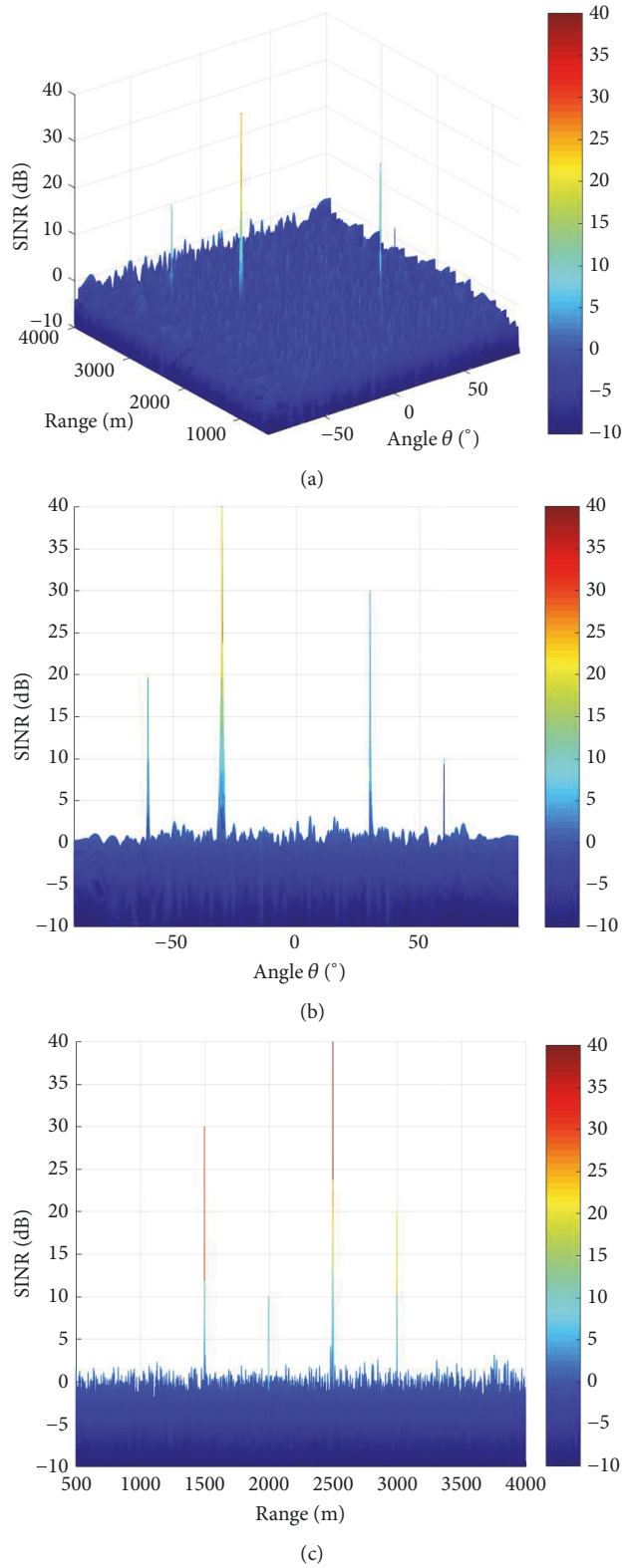
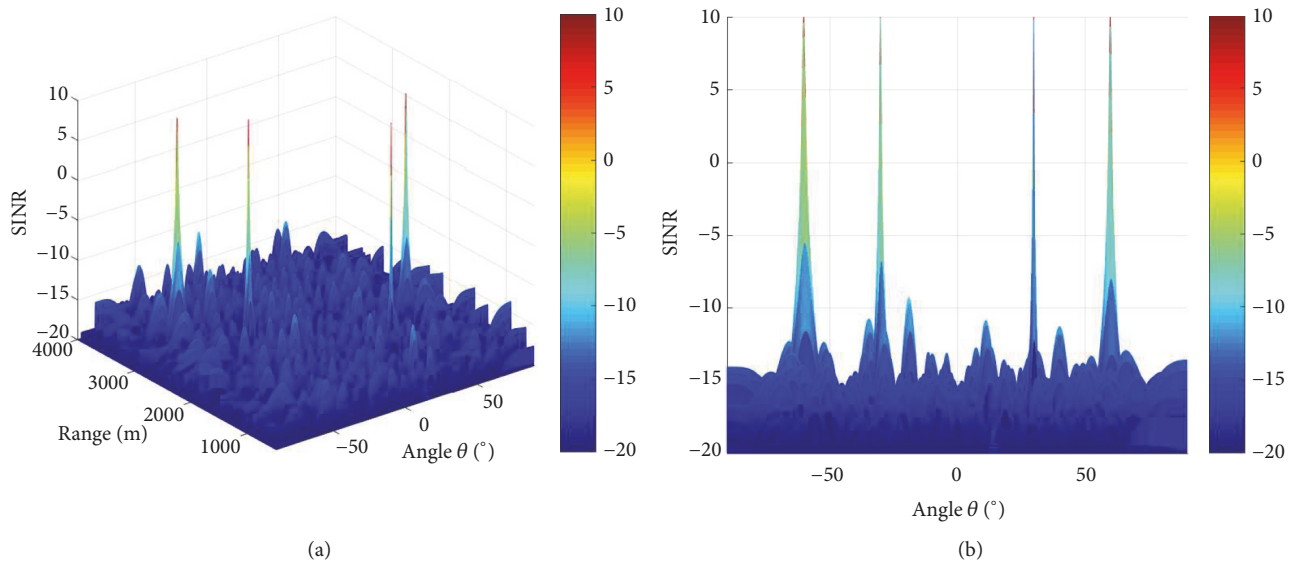


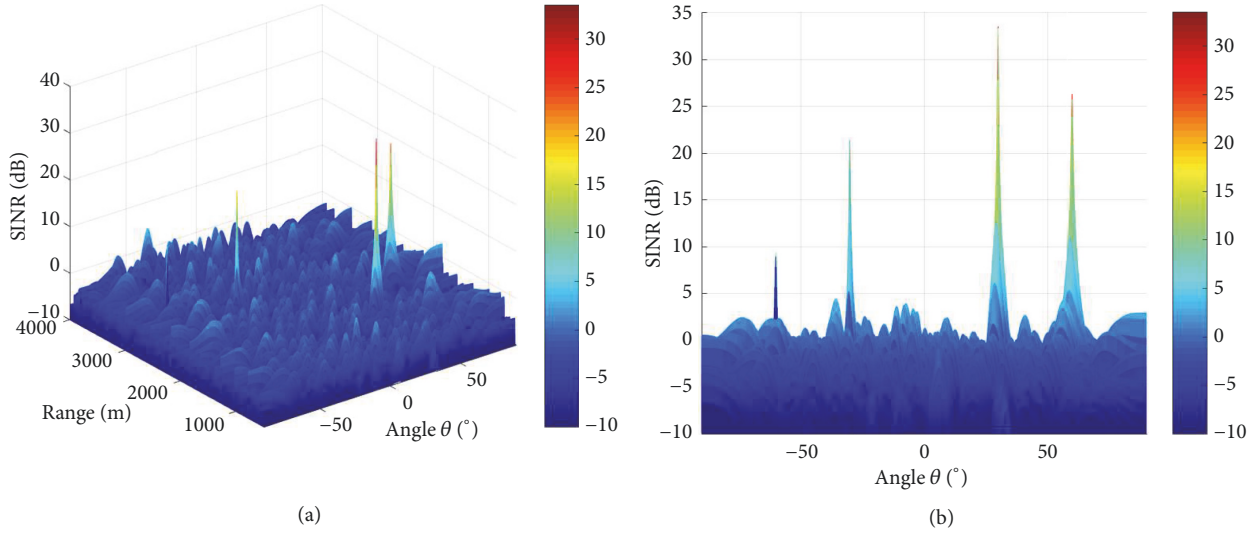
FIGURE 5: The SINR distribution with different minimum required receiving power versus (a) angle-range. (b) range dimension, where P_s = 50dBm, ζ_0 = −70 dBm, ζ_1 = −90 dBm, ζ_2 = −60 dBm, ζ_3 = −80 dBm.

In the fourth experiment, we investigate the SINR distribution of different receiving power requirement for each LU. The same parameters as the first experiment are adopted except that P_s = 50dBm and the minimum required receive power of the four LUs is set as ζ_0 = −70dBm, ζ_1 = −90dBm, ζ_2 = −60dBm and ζ_3 = −80dBm, respectively. From Figure 5,



(a) (b)

FIGURE 6: The SINR distribution of the proposed Max-ATP-based DM schemes (a) versus angle-range, (b) range dimension, where N=16, P_s=40 dBm.



(a) (b)

FIGURE 7: The SINR distribution of Max-SLNR-based DM schemes (a) versus angle-range, (b) angle dimension, where N=16, P_s=40 dBm.

it is clear that there are four sharp peaks corresponding to each of the LU, while the SINR is low in other regions where Eve potentially exists. Moveover, the different receive power requirement is satisfied for each LU, which confirms the accurate control of each broadcasting signal and therefore, the energy efficiency can be effectively improved.

In the fifth experiment, we compare the SINR distribution of the Max-SLNR scheme and the proposed method. The same parameters as the first experiment are adopted except that the number of array elements is set as $N = 16$. From Figures 6 and 7, we can observe that, for the proposed method, the power of each LU is under accurate control, which can guarantee the reception performance at the LUs. However, for the Max-SLNR scheme, the SINRs at the LUs are different, which implies inefficient power allocation. Moreover, compared with the Max-SLNR scheme, the proposed one achieves lower SINR at all locations outside the main lobes of the locations of LUs. Therefore, the proposed scheme can promote the wireless communication security performance without prior information of the Eve's location, since more power can be allocated to AN for the undesired communication region.

In the sixth experiment, we compare the BER performance of the Max-SLNR scheme and the proposed method. The same parameters as the first experiment are adopted except that P_s varies from 35dBm to 55dBm. Figure 8 shows the BER curves of the LUs versus total power budget for the proposed method and the max-SLNR method. It is obvious that the BER at each LU of the proposed methods remains nearly constant which is about 10^{-5}. Therefore, it can ensure

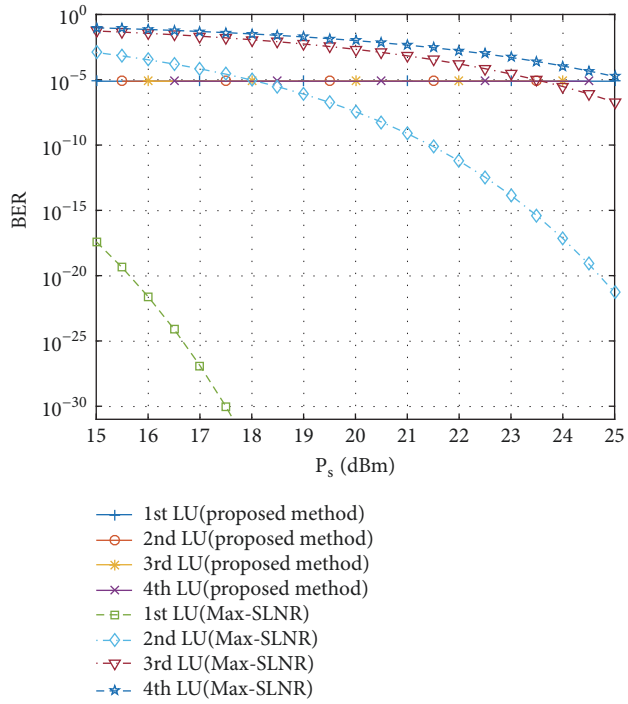


Figure 8: The BERs at each LU for the proposed method and Max-SLNR.

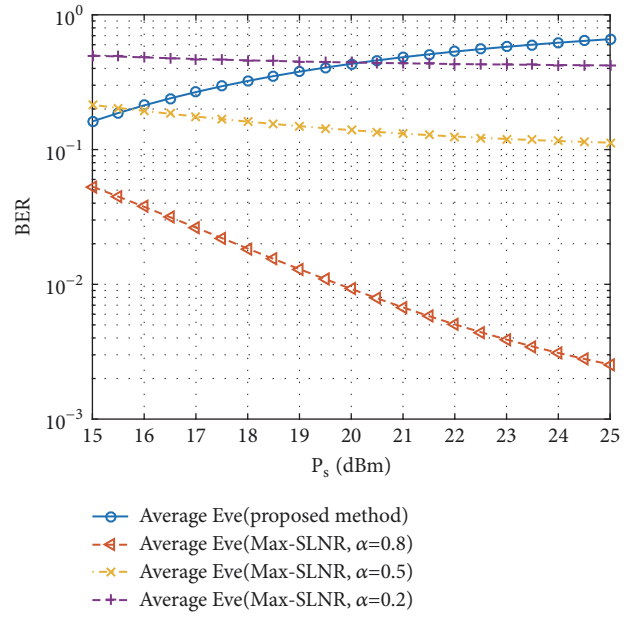


Figure 9: The average BER at Eve for the proposed method and Max-SLNR.

the effective reception of the LUs. On the contrary, the BERs of different LUs for the Max-SLNR method vary from each other. Thus, for the max-SLNR method, the power of each LU cannot be accurately controlled. Figure 9 shows the BER curves of Eve versus total power budget for the proposed method and the max-SLNR method. It is obvious that, for the proposed method, the BER of Eve increases as the increment of the total transmit power P_s since more power can be assigned to AN. However, for the Max-SLNR method, the average BER of Eve decreases with the increment of the total transmit power. This is because the fact that the objective function of the max-SLNR method is to maximize the signal-to-leakage noise ratio. Consequently, the receiver power at Eve also increases with the total transmit power budget, which causes the decrement of Eve's BER. Therefore, we can conclude that the proposed approach can accurately control

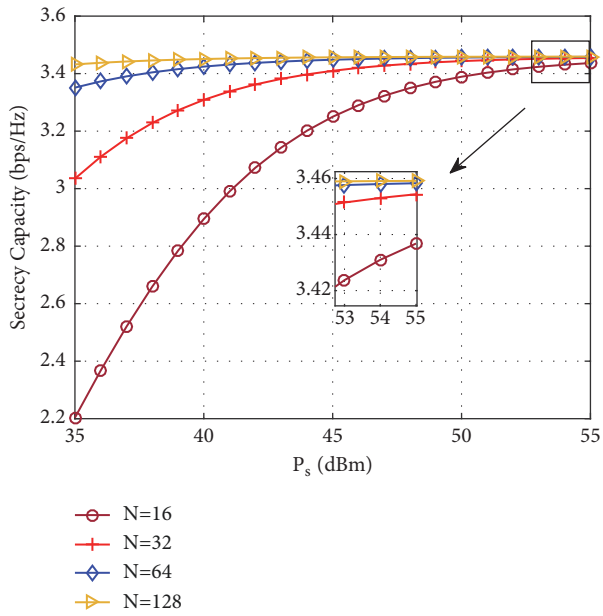


Figure 10: The secrecy capacity comparison for different parameters versus total power P_s.

the efficiency of the total radiated energy, and its security performance is superior to that of max-SLNR.

In the last experiment, the secrecy capacity of the proposed scheme is explored as a function of the total transmit power P_s. The same parameters as the first experiment are adopted except that P_s varies from 35dBm to 55dBm, and the number of elements varies from 16 to 128. From Figure 10, it is clear that the increment of array elements can promote the secrecy capacity. Similarly, with the increment of total transmit power, the secrecy capacity can be enhanced and secrecy capacity curves with different elements get closer, since more power can be assigned to AN.

5. Conclusions

In this paper, we proposed a RFDA-based DM scheme for secure wireless broadcasting system. The operation mode was extended from previous point to point communication to the point to multipoint mode. It does not require any prior knowledge of the Eves' location, which is more suitable for practical applications. In addition, it can effectively promote the security of the broadcasting system since the confidential message is only broadcasted to the locations of LUs. Moreover, the proposed approach is energy efficient because the power of each LU is under accurate control. The secrecy capacity of the proposed broadcasting system has been evaluated theoretically and verified by simulation results.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was funded by the National Natural Science Foundation of China under Grant No. 61601372, Shenzhen Science and Technology Innovation Committee of Basic Research Projects under Grant No. JCYJ20170306154016149 and JCYJ20170815154325384, China Postdoctoral Science Foundation under Grant No. 2017M613200, Natural Science Basic Research Plan in Shaanxi Province of China under Grant No. 2017JQ6068, Shanghai Aerospace Science and Technology Innovation Fund under Grant No. sast2017-077.

References

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

[2] A. Babakhani, D. Rutledge, and A. Hajimiri, "Near-field direct antenna modulation," *IEEE Microwave Magazine*, vol. 10, no. 1, pp. 36–46, 2009.

[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, "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.

[6] 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.

[7] 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.

[8] Y. Ding and V. Fusco, "Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters," *IEEE Antennas and Wireless Propagation Letters*, vol. 14, pp. 1330–1333, 2015.

[9] T. Xie, J. Zhu, and Y. Li, "Artificial-noise-aided zero-forcing synthesis approach for secure multi-beam directional modulation," *IEEE Communications Letters*, vol. 22, no. 2, pp. 276–279, 2018.

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

[11] F. Shu, W. Zhu, X. Zhou, J. Li, and J. Lu, "Robust Secure transmission of using main-lobe-integration-based leakage beamforming in directional modulation MU-MIMO systems," *IEEE Systems Journal*, vol. 12, no. 4, pp. 3775–3785, 2018.

[12] H. Yu, S. Wan, W. Cai et al., "GPI-based secrecy rate maximization beamforming scheme for wireless transmission with an-aided directional modulation," *IEEE Access*, vol. 6, pp. 12044–12051, 2018.

[13] S. Wan, F. Shu, J. Lu et al., "Power allocation strategy of maximizing secrecy rate for secure directional modulation networks," *IEEE Access*, vol. 6, pp. 38794–38801, 2018.

[14] X. Zhou, J. Li, F. Shu et al., "Secure SWIPT for directional modulation-aided AF relaying networks," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 2, pp. 253–268, 2019.

[15] P. Antonik, M. C. Wicks, H. D. Griffiths, and C. J. Baker, "Frequency diverse array radars," in *Proceedings of the IEEE Radar Conference*, pp. 215–217, Verona, NY, USA, April 2006.

[16] M. C. Wicks and P. Antonik, "Frequency diverse array with independent modulation of frequency, amplitude, and phase," U.S.A. Patent 7,319,427, 2018.

[17] P. Antonik, *An investigation of a frequency diverse array [Ph.D. thesis]*, University College London, 2009.

[18] T. Eker, S. Demir, and A. Hizal, "Exploitation of linear frequency modulated continuous waveform (LFMCW) for frequency diverse arrays," *IEEE Transactions on Antennas and Propagation*, vol. 61, no. 7, pp. 3546–3553, 2013.

[19] Y. Wang, W.-Q. Wang, and H. Chen, "Linear frequency diverse array manifold geometry and ambiguity analysis," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 984–993, 2015.

[20] 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.

[21] W.-Q. Wang and H. C. So, "Transmit subaperturing for range and angle estimation in frequency diverse array radar," *IEEE Transactions on Signal Processing*, vol. 62, no. 8, pp. 2000–2011, 2014.

[22] W.-Q. Wang, "Subarray-based frequency diverse array radar for target range-angle estimation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 50, no. 4, pp. 3057–3067, 2014.

[23] 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.

[24] H. Shao, J. Li, H. Chen, and W.-Q. Wang, "Adaptive frequency offset selection in frequency diverse array radar," *IEEE Antennas and Wireless Propagation Letters*, vol. 13, pp. 1405–1408, 2014.

[25] H. Huang and W.-Q. Wang, "FDA-OFDM for integrated navigation, sensing, and communication systems," *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 5-6, pp. 34–42, 2018.

[26] W.-Q. Wang, "DM using FDA antenna for secure transmission," *IET Microwaves, Antennas & Propagation*, vol. 11, no. 3, pp. 336–345, 2017.

[27] 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.

[28] K. Gao, W.-Q. Wang, J. Cai, and J. Xiong, "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.

[29] 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.

[30] S. Y. Nusenu, W. Wang, and S. Ji, "Secure directional modulation using frequency diverse array antenna," in *Proceedings of the 2017 IEEE Radar Conference (RadarConf17)*, pp. 378–382, Washington, DC, USA, May 2017.

[31] 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.

[32] Q. Cheng, J. Zhu, T. Xie, J. Luo, and Z. Xu, "Time-invariant angle-range dependent directional modulation based on time-modulated frequency diverse arrays," *IEEE Access*, vol. 5, pp. 26279–26290, 2017.

[33] 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.

[34] 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*, 2019.

[35] 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.

[36] F. Shu, Y. Qin, T. Liu et al., "Low-complexity and high-resolution DOA estimation for hybrid analog and digital massive MIMO receive array," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2487–2501, 2018.

[37] F. Shu, S. Yang, Y. Qin, and J. Li, "Approximate analytic quadratic-optimization solution for TDOA-based passive multi-satellite localization with earth constraint," *IEEE Access*, vol. 4, pp. 9283–9292, 2016.

[38] G. H. Golub and C. F. Van Loan, *Matrix Computations*, Johns Hopkins Studies in the Mathematical Sciences, Johns Hopkins University Press, Baltimore, Md, USA, 4th edition, 2012.

[39] A. Goldsmith, *Wireless Communications*, Cambridge University Press, New York, NY, USA, 1st edition, 2005.