Hindawi
Security and Communication Networks
Volume 2020, Article ID 2194840, 13 pages
https://doi.org/10.1155/2020/2194840

Research Article

Authentication and Secrecy of Multicast Communication Scenario: Artificial Noise-Aided Costas Sequence Matrix FDA Approach

Shaddrack Yaw Nusenu

Koforidua Technical University (KTU), Koforidua, Ghana

Correspondence should be addressed to Shaddrack Yaw Nusenu; nusenu2012gh@yahoo.com

Received 20 September 2019; Revised 14 March 2020; Accepted 8 June 2020; Published 30 June 2020

Academic Editor: Jiankun Hu

In multicast communication scenario, the desired users are decomposed into M groups to receive private M useful data from the transmitter, while eavesdroppers (Eves) group tries to intercept. Since wireless security system consists of authentication and secure transmission, we propose directional modulation (DM) artificial noise (AN) matrix-aided Costas sequence (CS) matrix frequency diverse array (FDA) in multicast precoding systems in this paper. Specifically, we utilize the CS matrix for desired groups authentication (i.e., group identity), and it is shared via a low-speed forward link in advance. Next, we design AN matrix-aided FDA to offer robust antieavesdropping method based on leakage concept. Furthermore, we devise secrecy metrics, namely, secrecy outage probability (SOP), asymptotic Eve's detectability error probability, and average useful data leakage rate, based on the scenario where Eve's instantaneous channel state information (CSI) is unavailable. In addition, we numerically analyze the proposed energy beamforming focusing and evaluate the secrecy energy efficiency. Via simulation results, the proposed scheme gives important insights into how to design and measure secrecy performances in multicast scenarios.

1. Introduction

The exponential growth of wireless communication services has attracted an emerging technology as well as a lot of researches, primarily focusing on wireless design transmission techniques, particularly to provide security for the useful information that needs to be transmitted via wireless channels. Because of the feature of wireless channels (i.e., broadcasting nature), eavesdroppers may have the ability to receive the useful information. In order to offer perfect security, we need to prevent eavesdroppers from intercepting the useful information intended to the desired receiver(s). Existing security techniques have been implemented using higher layers based on traditional cryptographic methods using encryption techniques [1]. Over recent years, physical layer security (PLS) has attracted a lot of attention from both industry and academia [2–10] over its counterpart traditional cryptographic methods. The PLS employs information theoretic method to provide information confidentiality without encryption techniques [3, 4, 7]. One main performance metric employed for PLS is the secrecy rate, at which the useful data can be transmitted secretly. Normally, the secrecy rate is determined by the difference between desired channel and eavesdropper capacities. Several authors have proposed different PLS methods, for example, directional modulation (DM) [11] and AN-aided methods [12–15].

Recently, secure communication in millimeter wave (mmWave) is being put forward. For instance, the authors in [16] proposed two secure transmission algorithms using polygon construction approach, specifically for general multipath fading channels. In this scheme, all antennas are activated and no on-off switching circuit is needed. In [17], antenna subset modulation was investigated, which introduces

artificial randomness in the received constellation via antenna subset selection. This scheme combines the advantages of security and directional transmission. Reference [18] studied secure transmissions under slow fading channels with multipath propagation in millimeter wave systems. Due to propagation features of millimeter wave, the authors discussed three transmission schemes, namely, maximum ratio transmitting (MRT) beamforming, artificial noise (AN) beamforming, and partial MRT (PMRT) beamforming. In [19], the authors investigated secure communication of mmWave relaying networks in the presence of multiple spatial randomly eavesdroppers, which are modelled under a stochastic geometry framework. Reference [20] studied physical layer security in a multi-input single-output (MISO) millimeter wave system, where multiple single-antenna eavesdroppers are randomly located. Moreover, two secure transmission schemes, namely, maximum ratio transmitting (MRT) beamforming and artificial noise (AN) beamforming, are investigated and closed-form expressions of the connection probability are derived for the two techniques.

In [21], the authors proposed symbol-level precoder to improve security. This scheme adopted constructive interference in DM with the aim to reduce the transmitter energy consumption. In [22, 23], the authors put forward a PLS for multicasting cochannel groups. In this scheme, independent data streams are sent to the groups of users for communication purposes employing multiple transmit antennas. In this context, an open research issue is how to secure the data transmission, in case eavesdropper group appears. Very recently, an interesting technique was proposed in [15] to provide security for the independent data streams in multicast precoding systems employing AN-aided DM method based on leakage concept.

Nevertheless, the above-mentioned schemes may fail to guarantee better secrecy, especially in the case where the statistical independence assumption of the desired group reception and Eves group reception may not be held. For instance, in PLS, we normally make this assumption that the Eve location information is unavailable at the transmitter side. In real case, Eve is passive. This means that Eve never sends signals; thus, obtaining such location information will be difficult to realize. In practical scenario, an Eve group may be exactly located closed and/or may have knowledge of the desired group(s) directions. In this context, the DM-based phased array (PA) in the literature and also DM PA multicast method [15] may not offer better security performance for the desired group. This is because, using PA antennas, signals can be distorted at the direction(s) different from the intended one.

Most PLS literature only considered secure transmission of useful information towards the desired user(s) directions and neglected authentication procedure between the transmitter and desired users. It should be mentioned that, in wireless security, authentication and secure transmission are very essential [24]. In this case, the authentication is meant for user identification and prevents Eves from accessing the transmission, while secure transmission provides protection for the useful information so that Eves cannot intercept. Thus, it is necessary to exploit new array schemes for authentication and secure transmissions.

Frequency diverse array (FDA) in [25–28] has distinct possibilities to realize DM to further improve PLS system as mentioned in the above scenario, where the desired group and Eve group are located in the same direction but distinct ranges [29]. This is because FDA can create angle-range beamforming focusing due to the tiny frequency increment across the element index, which is completely different from PA beamforming. Adopting standard FDA with linear frequency increment, creating angle-range coupling beamforming issues will certainly compromise the secure transmission towards the desired group. Recently, the authors in [30] devised CS matrix to design frequency increment for FDA. This proposed FDA owns two unique features, namely, (1) low probability of detection (LPD) beamforming, which is randomly distributed beamforming without obvious peak, and this means that only the desired receiver can retrieve the information with specified CS matrix and (2) decoupling the correlation between angle-range dependent profiles. In fact, the CS matrix properties are more suitable for providing authentication in wireless communication applications.

Inspired by the above potential benefits, this paper investigates FDA in multicast precoding scenarios. Specifically, we adopt AN matrix-aided DM design for secure communication. In FDA, the frequency increment plays a vital role in angle-range focusing transmission. So, we utilize CS matrix to design the frequency increment which provides authentication characteristics for the desired groups before secure transmission. Next, we take the advantage of the leakage concept to devise the proposed scheme precoding vector and AN matrix. Also, secrecy metrics such as secrecy outage probability (SOP), asymptotic Eve's detectability error probability, and average useful data leakage rate are derived based on the scenario where Eve's instantaneous CSI is unavailable at the transmitter side. The theoretical analysis reveals significant insights into the design of AN matrix-aided FDA multicast secure communications. Finally, we evaluate the energy focusing capability and secrecy energy efficiency of the proposed scheme.

Actually, our proposed scheme is different from [15, 29]. Firstly, in [15], the authors employed leakage concept to design signal-to-leakage-noise ratio (SLNR) and artificial noise (AN) to leakage-and-noise ratio (ANLNR) in multicast precoding. However, they can offer only one-dimensional angular-dependent PLS communications; that is, they can project information along a secure corridor but not to a particular position in free space. Also, authenticating the desired group(s) was not taken into account. In [29], the frequency increments are selected randomly for each antenna element and employed AN to provide PLS without also authenticating desired user. In addition, instability is created because of the randomly selected frequency increments.

The proposed scheme's major contributions are listed as follows:

(1) We investigate a multicast precoding scenario based on frequency diverse array (FDA) to achieve desired group(s) PLS in two-dimensional angle-range-dependent direction. Since a secure wireless transmission system comprises authentication and secure transmission, firstly, we utilize the Costas sequence (CS) matrix to design the frequency increment that provides authentication characteristics for the desired group(s) in order to prevent any malicious receiver(s) from accessing the system before secure transmission.

(2) We take the advantage of the leakage concept to devise the proposed scheme precoding vector by minimizing the confidential information power leakage at the FDA transmitter towards Eve group(s), namely, maximizing signal-to-leakage-noise ratio (SLNR). Afterwards, artificial noise (AN) projection matrix is developed and sent to eavesdropper (Eve) group in angle-range direction, with maximizing AN to leakage-and-noise ratio (ANLNR).

(3) Since in wireless communication security system it is useful to have a great insight into the desired group(s) confidential information leakage and Eve group(s) decodability along the angle-range direction when an outage has occurred, we analyze the proposed scheme using the following metrics: secrecy outage probability (SOP), asymptotic Eve's detectability error probability, and average useful data leakage rate based on the scenario where Eve group(s) instantaneous CSI is unavailable at the transmitter side. The proposed scheme can also provide secure transmission in millimeter wave (mmWave) communication applications.

2. System Design Model for Multicast Communication Scenario

2.1. Costas Sequence (CS) Matrix Authentication Based on Frequency Diverse Array. As demonstrated in Figure 1, we assume N element linear transmit antenna array. As opposed to PA antennas, FDA utilizes tiny frequency increments across the antenna indexes. Particularly, the radiated frequency of the nth element is described as $f_n = f_0 + \Delta f_n(t)$, where $\Delta f_n(t) = c_{s_n} \Delta f(t), n = 0, 1, ..., N-1$. f_0 is the carrier frequency, $\Delta f(t)$ denote the frequency increments, and c_{s_n} is the utilized Costas sequence (CS) matrix for nth element.

Herein and without loss of generality, we consider CS matrix, that is, $N = 11$, namely {1, 3, 7, 2, 5, 11, 10, 8, 4, 9, 6} [31]. In Figures 2(a) and 2(b), we have depicted CS matrix for $N = 11$ and its difference matrix, respectively.

The difference matrix shown in Figure 2(b) can be calculated by $\Psi_{i,j} = \alpha_{i+j} - \alpha_j$ with $i + j \le M$. Note that α_i denotes the ith coding element and $i + j > M$ locations are left blank. It should be noted that the computed difference matrix reveals that the adopted CS matrix is feasible for the proposed scheme. With the chosen CS matrix, we design the array elements with frequency increments indexed as $c_{s_N} \Delta f(t)$ with $c_{s_N} = \{1, 3, 7, 2, 5, 11, 10, 8, 4, 9, 6\}$ and $\Delta f(t)$ is the frequency hopping step. Note that the transmitter exchanges the utilized CS matrix via a low-speed forward link in advance [32] to facilitate group identification as well as decoding of the useful information during transmission. Moreover, without the specific CS matrix for identification, the transmitter remains silent, since the transmitter cannot identify the desired groups.

2.2. Signal Model Formulation. Generally, we select the first array element to be the reference. Then, we give the FDA normalized steering vector at certain time t for ith user of the mth desired group at the location of $(\theta_{d,mi}, r_{d,mi})$ as (1)

$$\mathbf{h}\left(\mathbf{f}, t, \theta_{d,mi}, r_{d,mi}\right) \triangleq \frac{1}{\sqrt{N}} \begin{bmatrix} h_0\left(f, t, \theta_{d,mi}, r_{d,mi}\right), \ldots, h_n\left(f, t, \theta_{d,mi}, r_{d,mi}\right), \\ \ldots, h_{N-1}\left(f_{N-1}, t, \theta_{d,mi}, r_{d,mi}\right) \end{bmatrix}^T, \tag{1}$$

where $h_n(f_n, t, \theta_{d,mi}, r_{d,mi})$ is given as (2)

$$h_n\left(f_n, t, \theta_{d,mi}, r_{d,mi}\right) \triangleq \exp\left(-j2\pi f_n\left(t - \frac{r_n}{c}\right)\left(t - \frac{r_{d,mi} - n\,d \sin\,\theta_{d,mi}}{c}\right)\right), \tag{2}$$

with c being the light speed and d being the element spacing, and $r_n = r_{d,mi} - n\,d \sin\,\theta_{d,mi}$. The frequency increment vector is $\mathbf{f} \triangleq [f_0 + c_{s_0}\Delta f(t), f_0 + c_{s_1}\Delta f(t), \ldots, f_0 + c_{s_{N-1}}\Delta f(t)]^{\mathrm{T}}$. For the sake of simplicity, let $\mathbf{h}_{dm}(\mathbf{f}, t) \triangleq \mathbf{h}(\mathbf{f}, t, \theta_{dm}, r_{dm})$ denote mth desired group and Eve group is denoted as $\mathbf{h}_e(\mathbf{f}, t) \triangleq \mathbf{h}(\mathbf{f}, t, \theta_e, r_e)$ at time t. Hence, we can define the steering channel matrix for mth desired group as

$$\mathbf{H}_{dm}(\mathbf{f}, t) = \left[\mathbf{h}_{dm,1}(\mathbf{f}, t), \mathbf{h}_{dm,2}(\mathbf{f}, t), \ldots, \mathbf{h}_{dm,T_m}(\mathbf{f}, t)\right], \tag{3}$$

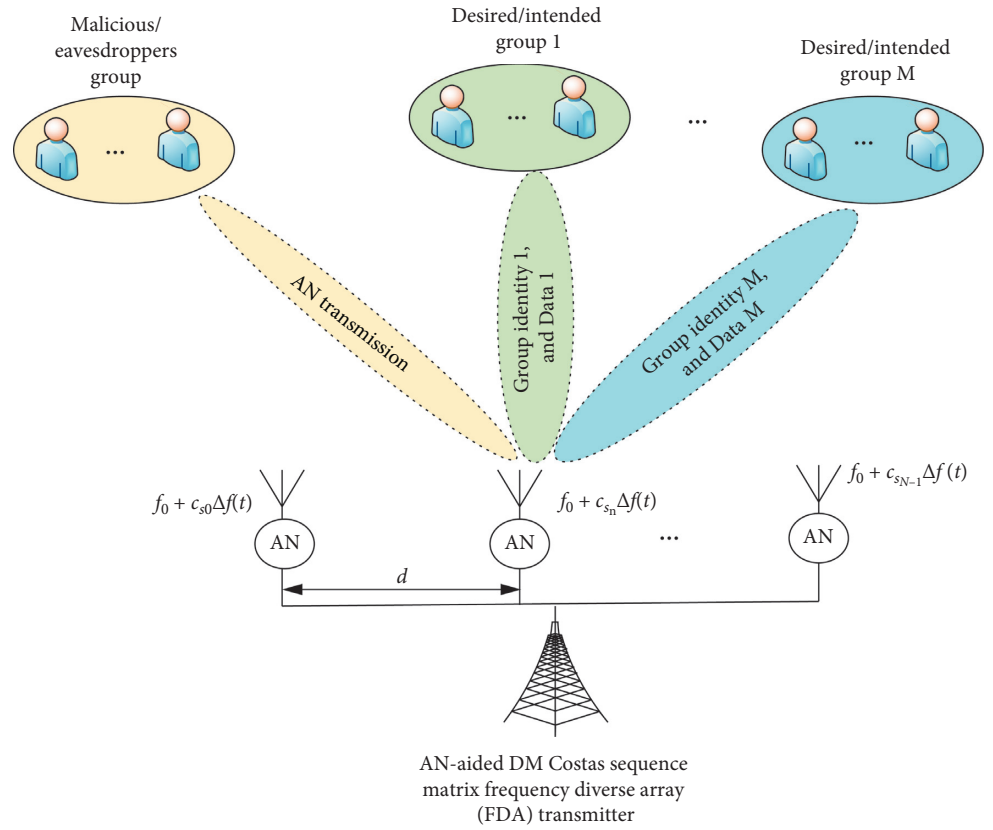
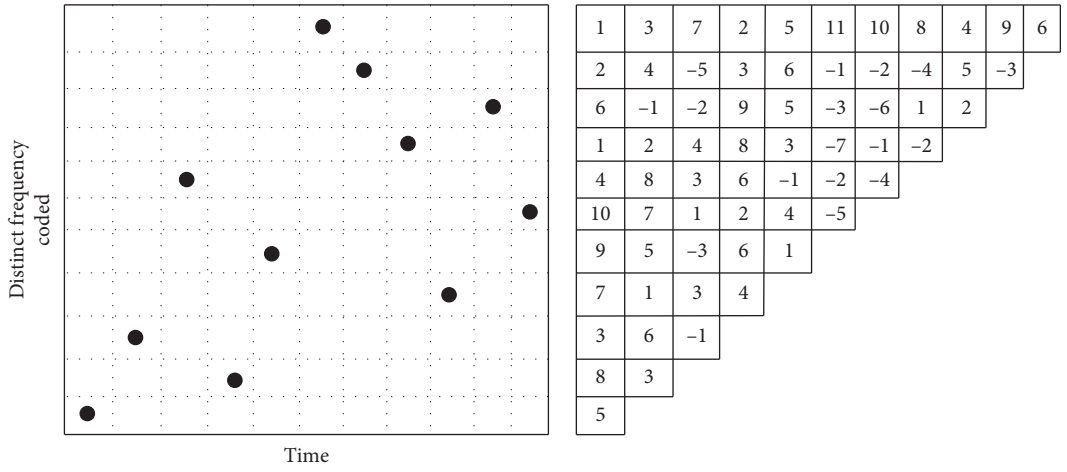


FIGURE 1: Illustration of AN-aided DM FDA multicast communications scenario. $c_{s_n} = \{c_{s_0}, c_{s_1}, \ldots, c_{s_{N-1}}\}$ denotes the CS matrix employed for the frequency increments Δf, namely, {1, 3, 7, 2, 5, 11, 10, 8, 4, 9, 6}, which is used for authentication purpose.



1	3	7	2	5	11	10	8	4	9	6
2	4	−5	3	6	−1	−2	−4	5	−3	
6	−1	−2	9	5	−3	−6	1	2		
1	2	4	8	3	−7	−1	−2			
4	8	3	6	−1	−2	−4				
10	7	1	2	4	−5					
9	5	−3	6	1						
7	1	3	4							
3	6	−1								
8	3									
5										

FIGURE 2: (a) Authentication coding sequence (CS) matrix c_s, $N = 11$: {1, 3, 7, 2, 5, 11, 10, 8, 4, 9, 6}. (b) Difference matrix.

where T_m is the number of intended/desired users in mth group. $\mathbf{h}_{dm}(\mathbf{f}, t)$ is $N \times T_m$ matrix. Likewise, the Eve steering channel matrix is expressed as

$$\mathbf{H}_e(\mathbf{f}, t) = \left[\mathbf{h}_{e,1}(\mathbf{f}, t), \mathbf{h}_{e,2}(\mathbf{f}, t), \ldots, \mathbf{h}_{e,K}(\mathbf{f}, t)\right]. \quad (4)$$

As depicted in Figure 1, the radiated baseband signal is given as

$$s(t) = \alpha_1\phi_1\sqrt{P_t}\sum_{m=1}^{M}\mathbf{w}_m(t)x_m(t) + \alpha_2\phi_2\sqrt{P_t}\mathbf{P}_{AN}(t), \quad (5)$$

where P_t denotes the total available power at the transmitter, $x_m(t)$ is the useful secret information sent to the mth desired group, and $\mathbf{w}_m(t)$ is the mth desired group beamforming vector at time t. The AN projection matrix is given as

$\mathbf{P}_{\mathrm{AN}}(t) = (\mathbf{I}_{N-\sum_{m=1}^{M} T_m} - \mathbf{h}_{dm}(\mathbf{f},t)\mathbf{h}_{dm}^{H}(\mathbf{f},t))z$ with z being the AN vector, which is expressed as $\mathbf{z} \sim CN(0, \mathbf{I}_{N-\sum_{m=1}^{M} T_m})$. Herein, the matrix $(\mathbf{I}_{N-\sum_{m=1}^{M} T_m} - \mathbf{h}_{dm}(\mathbf{f},t)\mathbf{h}_{dm}^{H}(\mathbf{f},t))$ can project z into the null space of $\mathbf{h}_{dm}^{H}(\mathbf{f},t)$. ϕ_1 and ϕ_2 represent power allocation factors for useful secret information and AN matrix, respectively. Note that the power constraint is $\phi_1^2 + \phi_2^2 = 1$. A large value of $\phi 1$ implies that more power can be allocated to send the secret information and less power is utilized for secure protection. Importantly, how to select the optimal values of ϕ_1 and ϕ_2 is a hard problem and may depend on the type of secrecy applications. Also, α_1 and α_2, respectively, denote the normalized power factors for useful secret information and AN matrix. Note that, in order to achieve a maximum constructive combination at the mth desired group, we have $\mathbf{w}_m(t) = \mathbf{h}_m(\mathbf{f},t)$. Additionally, we utilize AN matrix $\mathbf{P}_{\mathrm{AN}}(t)$ to force AN towards Eve group location at time t.

The signals vectors received at desired group m and Eve group are, respectively, expressed in equations (6) and (7), where $\mathbf{n}_{dm} \sim CN(0, \sigma_d^2\mathbf{I}_{T_m})$ and $\mathbf{n}_e \sim CN(0, \sigma_e^2\mathbf{I}_K)$.

$$\begin{aligned}\mathbf{y}_{dm}(\mathbf{f},t) = {} & \alpha_1\phi_1\sqrt{P_t}\mathbf{H}_{dm}^{H}(\mathbf{f},t)\mathbf{w}_m(t)x_m(t) + \alpha_1\phi_1\sqrt{P_t}\mathbf{H}_{dm}^{H}(\mathbf{f},t) \\ & \sum_{i=1,i\neq m,}^{M} \mathbf{w}_i(t)x_i(t) + \alpha_2\phi_2\sqrt{P_t}\mathbf{H}_{dm}^{H}(\mathbf{f},t)\mathbf{P}_{\mathrm{AN}}(t) + \mathbf{n}_{dm}(t),\end{aligned} \tag{6}$$

$$\mathbf{y}_e(\mathbf{f},t) = \alpha_1\phi_1\sqrt{P_t}\mathbf{H}_e^{H}(\mathbf{f},t)\sum_{m=1}^{M}\mathbf{w}_m(t)x_m(t) + \alpha_2\phi_2\sqrt{P_t}\mathbf{H}_e^{H}(\mathbf{f},t)\mathbf{P}_{\mathrm{AN}}(t) + \mathbf{n}_e(t). \tag{7}$$

2.3. Design of Precoding Vector and Artificial Noise (AN) Matrix Based on Leakage Concept. In this section, we design the precoding vector $\mathbf{w}_m(t)$ for the useful information and AN matrix $\mathbf{P}_{\mathrm{AN}}(t)$ based on the concept of leakage analysis. The maximized signal-to-leakage-noise ratio (SLNR) optimization problem corresponding to the precoding vector $\mathbf{w}_m(t)$ is

$$\begin{aligned}&\max_{\{w_m(t)\}} \mathrm{SLNR}(\mathbf{w}_m(t)), \\ &\mathrm{s.t}\left\|\mathbf{w}_m(t)\right\|^2 = 1,\end{aligned} \tag{8}$$

where SLNR $(\mathbf{w}_m(t))$ is expressed as

$$\mathrm{SLNR}(\mathbf{w}_m(t)) = \left(\alpha_1^2\phi_1^2P_t tr\left\{\mathbf{w}_m^{H}(t)\mathbf{H}_{dm}(\mathbf{f},t)\mathbf{H}_{dm}^{H}(\mathbf{f},t)\mathbf{w}_m(t)\right\}\right)\cdot\left[tr\left(\begin{array}{c}\alpha_1^2\phi_1^2P_t\sum_{i=1,i\neq m}^{M}\mathbf{w}_m^{H}(t)\mathbf{H}_{di}(\mathbf{f},t)\mathbf{H}_{di}^{H}(\mathbf{f},t)\mathbf{w}_m(t)+ \\ \alpha_1^2\phi_1^2P_t\mathbf{w}_m^{H}(t)\mathbf{H}_e(\mathbf{f},t)\mathbf{H}_e^{H}(\mathbf{f},t)\mathbf{w}_m(t) + \sigma_{dm}^2\end{array}\right)\right]. \tag{9}$$

Utilizing the generalized Rayleigh theorem [33], we can obtain the maximum SLNR solution from the eigenvector which corresponds to the largest eigenvalue of matrix as

$$\left[\sum_{i=1,i\neq m}^{M}\mathbf{H}_{di}(\mathbf{f},t)\mathbf{H}_{di}^{H}(\mathbf{f},t) + \mathbf{H}_e(\mathbf{f},t)\mathbf{H}_e^{H}(\mathbf{f},t) + \frac{\sigma_{dm}^2}{\alpha_1^2\phi_1^2P_t}\mathbf{I}_N\right]^{-1}\cdot\mathbf{H}_{dm}(\mathbf{f},t)\mathbf{H}_{dm}^{H}(\mathbf{f},t). \tag{10}$$

Next, we design the AN matrix $\mathbf{P}_{\mathrm{AN}}(t)$, which is considered as useful signal towards the Eve group to create interference and prevent useful information from being intercepted. We also consider that the AN matrix $\mathbf{P}_{\mathrm{AN}}(t)$ should not be leaked towards the M desired groups. The optimization problem for maximizing AN matrix leakage-to-noise ratio (ANLNR) is

$$\begin{aligned}&\max_{\mathbf{P}_{AN}(t)} \mathrm{ANLNR}(\mathbf{P}_{\mathrm{AN}}(t)), \\ &\mathrm{s.t}\, tr\left(\mathbf{P}_{\mathrm{AN}}^{H}(t)\mathbf{P}_{\mathrm{AN}}(t)\right) = N - \sum_{m=1}^{M} T_m,\end{aligned} \tag{11}$$

where ANLNR $(\mathbf{P}_{\mathrm{AN}}(t))$ is given as

$$\mathrm{ANLNR}\left(\mathbf{P}_{\mathrm{AN}}(t)\right)=\frac{tr\left\{\mathbf{P}_{\mathrm{AN}}^{H}(t)\mathbf{P}_{\mathrm{AN}}(t)\mathbf{H}_{e}(\mathbf{f},t)\mathbf{H}_{e}^{H}(\mathbf{f},t)\right\}}{tr\left\{\mathbf{P}_{\mathrm{AN}}^{H}(t)\left(\sum_{i=1}^{M}\mathbf{H}_{di}(\mathbf{f},t)\mathbf{H}_{di}^{H}(\mathbf{f},t)+\left(\sigma_{e}^{2}/\alpha_{2}^{2}\phi_{2}^{2}\mathbf{P}_{t}\left(N-\sum_{i=1}^{M}T_{m}\right)\right)\mathbf{I}_{N}\right)\mathbf{P}_{\mathrm{AN}}(t)\right\}}. \tag{12}$$

Based on Rayleigh theorem [33] and similar to equation (10), we can also determine the eigenvalue matrix as

$$\left[\sum_{i=1}^{M}\mathbf{H}_{di}(\mathbf{f},t)\mathbf{H}_{di}^{H}(\mathbf{f},t)+\frac{\sigma_{e}^{2}}{\alpha_{1}^{2}\phi_{1}^{2}P_{t}\left(N-\sum_{m=1}^{M}T_{m}\right)}\mathbf{I}_{N}\right]^{-1}\cdot\mathbf{H}_{e}(\mathbf{f},t)\mathbf{H}_{e}^{H}(\mathbf{f},t). \tag{13}$$

Important remarks: since the proposed transmitter should acquire prior knowledge of the intended angle-range direction before beamforming, the source localization techniques or direction of arrival (DOA) estimation in [34, 35] can be employed to estimate the angle-range direction parameters. It is important to mention that these two factors, namely, noise and interference in the channel, may affect the measurement of DOAs, that is, introducing errors. Improving the DOAs measurement is out of the scope of this paper, but certainly this will be a future work.

3. Theoretical Performance Evaluation

In this section, we devise the proposed scheme secrecy metrics to give insights into secure communication transmission. Furthermore, we formulate the energy focusing capability and also evaluate the energy efficiency of the proposed scheme.

3.1. Secrecy Metrics Analysis

3.1.1. Secrecy Outage Probability. We express the achievable rate from the proposed scheme transmitter to the mth desired group as

$$C_{dm}(\mathbf{f},t)=\log_{2}\left(1+\gamma_{dm}(t)\right), \tag{14}$$

where

$$\gamma_{dm}(t)=\sigma_{dm}^{-2}\left|\mathbf{w}^{H}(t)\mathbf{h}_{dm}\left(\mathbf{f},t+\frac{r_{dm}}{c}\right)\right|^{2}, \tag{15}$$

is defined as the received instantaneous signal-to-noise ratio (SNR) at a particular time t. In equation (15), $\mathbf{w}(t)$ denotes the transmitter weight vector in a generic way (for convenience sake), σ_{dm}^{2} is the desired group variance, and r_{dm}/c represents the confidential information emitted at particular time t which will arrive at the desired group receiver.

Similarly, we can determine the achievable rate from the proposed transmitter to Eve group as

$$C_{e}(\mathbf{f},t)=\log_{2}\left(1+\gamma_{e}(t)\right), \tag{16}$$

where

$$\gamma_{e}(t)=\sigma_{e}^{-2}\left|\mathbf{w}^{H}(t)\mathbf{h}_{e}\left(\mathbf{f},t+\frac{r_{e}}{c}\right)\right|^{2}. \tag{17}$$

Note that equation (17) has the same physical meaning as equation (15). According to [36], we can determine the secrecy sum rate (SSR) of the proposed scheme as

$$C_{\mathrm{sec}}=\left[\log_{2}\left(\frac{1+\sigma_{dm}^{-2}\left|\mathbf{w}^{H}\mathbf{h}_{dm}\left(\mathbf{f},t+\left(r_{dm}/c\right)\right)\right|^{2}}{1+\sigma_{e}^{-2}\left|\mathbf{w}^{H}\mathbf{h}_{e}\left(\mathbf{f},t+\left(r_{e}/c\right)\right)\right|^{2}}\right)\right]^{+}, \tag{18}$$

where $[\tau]^{+}=\max\{\tau,0\}$.

The channel fading adopted is quasi-static Rayleigh. The exponential distributions of the desired group and Eve group at particular time t can be presented, respectively, as follows:

$$f_{dm}\left(\gamma_{dm}(t)\right)=\frac{1}{\overline{\gamma}_{dm}(t)}\exp\left(-\frac{\gamma_{dm}(t)}{\overline{\gamma}_{dm}(t)}\right), \tag{19}$$

$$f_{e}\left(\gamma_{e}(t)\right)=\frac{1}{\overline{\gamma}_{e}(t)}\exp\left(-\frac{\gamma_{e}(t)}{\overline{\gamma}_{e}(t)}\right). \tag{20}$$

The reader can refer to [37] for better understanding of equations (19) and (20). For the sake of simplicity, the received average SNRs along the desired group and Eve group are given, respectively, as $\overline{\gamma}_{dm}(t)=P_{t}\sigma_{dm}^{-2}$ and $\overline{\gamma}_{e}(t)=P_{t}\sigma_{e}^{-2}$. Wiretap encoding technique [3] is adopted at the proposed transmitter to facilitate secure transmission to the mth desired group.

Herein, the proposed transmitter needs to choose two rates, namely, codeword rate R_{dm} and secrecy data rate R_{s}. The difference $R_{e}\triangleq R_{dm}-R_{s}$ is the rate cost that offers antieavesdropping. In this scheme, we consider reality scenario, where the Eve group is passive. Thus, instantaneous CSI of the Eve's channel is unavailable at the proposed transmitter. In this case, the proposed transmitter assumes $\widetilde{C}_{e}(\mathbf{f},t)$ as the Eve's channel capacity. The wiretap codes can be designed as $R_{dm}=C_{dm}(\mathbf{f},t)$ and $R_{s}=C_{dm}(\mathbf{f},t)-\widetilde{C}_{e}(\mathbf{f},t)$. It is important to mention that, in passive Eve scenario, achieving perfect secrecy is not always guaranteed, because it is realized that some useful information transmitted by the transmitter is likely to be leaked along the Eve angle-range direction(s).

To provide a great insight into the desired group(s) confidential information leakage and the Eve group(s) decodability along the angle-range direction when an outage has occurred, we follow the secrecy outage probability P_{sop} guidelines of [38]. However, P_{sop} in [38] can achieve only one-dimensional angle dependence. Hence, we investigate P_{sop} in two dimensions, namely, angle-range dimension. The

proposed scheme's wiretap code maximum achievable fractional equivocation can be written as

$$\beta = \begin{cases} 1, & \text{if } C_e(\mathbf{f},t) \le R_{dm} - R_s, \\ \dfrac{R_{dm} - C_e(\mathbf{f},t)}{R_s}, & \text{if } R_{dm} - R_s < C_e(\mathbf{f},t) < R_{dm}, \\ 0, & \text{if } R_{dm} \le C_e(\mathbf{f},t). \end{cases} \tag{21}$$

Therefore, P_{sop} is equivalently expressed as

$$\begin{aligned} P_{sop} &= P(\beta < \xi) \\ &= P\left(2^{R_{dm}} - 1 \le \gamma_e(t)\right) + P\left(2^{R_{dm}-R_s} - 1 < \gamma_e(t) < 2^{R_{dm}} - 1\right) \cdot P\left(\frac{R_{dm} - C_e(\mathbf{f},t)}{R_s} < \xi \,\middle|\, 2^{R_{dm}-R_s} - 1 < \gamma_e(t) < 2^{R_{dm}} - 1\right) \\ &= \exp\left(-\frac{2^{R_{dm}-\xi R_s} - 1}{\overline{\gamma}_e(t)}\right). \end{aligned} \tag{22}$$

From equation (22), we can be able to provide an insight into how to achieve different secrecy requirement performances using the relation $0 < \xi \le 1$. Note that when $\xi = 1$, it means perfect secrecy is attained; thus, the classical SOP is realized as seen in many studies (see [39] and the references therein).

3.1.2. Asymptotic Eve's Detectability Error Probability ($\overline{\beta}$). In this subsection, we devise an expression that gives insight of the lower bound on Eve's detecting error probability asymptotically. In other words, since it is hard for the desired group to identify which information is securely transmitted, we devise this performance metric as

$$\begin{aligned} \overline{\beta} &= E\{\beta\} \\ &= \int_0^{2^{R_{dm}-R_s}-1} f_e(\gamma_e(t))\mathrm{d}\gamma_e + \int_{2^{R_{dm}-R_s}-1}^{2^{R_{dm}}-1} \left(\frac{R_{dm} - C_e(\mathbf{f},t)}{R_s}\right) f_e(\gamma_e(t))\mathrm{d}\gamma_e \\ &= 1 - \frac{1}{R_s \mathrm{In}2} \exp\left(\overline{\gamma}_e(t)\right)^{-1} \cdot \left(E_i\left(-\frac{2^{R_{dm}}}{\overline{\gamma}_e(t)}\right) - E_i\left(-\frac{2^{R_{dm}-R_s}}{\overline{\gamma}_e(t)}\right)\right), \end{aligned} \tag{23}$$

where $E_i(\tau) = \int_{-\infty}^{\tau} \exp(t)/t \, \mathrm{dt}$ is defined as the exponential integral. It is important to mention that equation (23) can be utilized to analyze the error probability of Eve in angle-range direction to ascertain how the private information can be detected.

3.1.3. Average Useful Data Leakage Rate ($A_{leakage}$). By adopting fixed transmission rate, we can determine how the private information can be leaked towards Eve's group angle-range direction and the expression is described as

$$\begin{aligned} A_{\text{leakage}} &= (1 - \overline{\beta})R_s \\ &= \frac{1}{\mathrm{In}\ 2} \exp\left(\overline{\gamma}_e(t)\right)^{-1} \left(E_i\left(-\frac{2^{R_{dm}}}{\overline{\gamma}_e(t)}\right) - E_i\left(-\frac{2^{R_{dm}-R_s}}{\overline{\gamma}_e(t)}\right)\right). \end{aligned} \tag{24}$$

Note that the desired group is unable to know which useful information is leaked along the angle-range direction of Eve group. Hence, equation (24) can highlight how the transmitted private information can be leaked towards Eve location during the transmission process, especially in passive Eve scenarios.

3.2. Energy Beamforming Focusing Analysis. As stated before, the FDA depends on some parameters, namely, range, angular direction, time, and even frequency diverse increment, to offer energy beamforming focusing. For the sake of simplicity, we derive the energy beamforming focusing in a general way. Referring to equation (1), we can reformulate it as

$$\mathbf{h}(\mathbf{f},\theta,r,t) \triangleq \left[h_0(f_0,\theta,r,t),\ldots,h_{(N-1)}\left(f_{(N-1)},\theta,r,t\right)\right]^{\mathrm{T}}. \tag{25}$$

Now, the energy beamforming focusing can be analyzed numerically as follows:

$$E_{\text{nergy}}^{\text{Proposed scheme}} \triangleq \iint_{\Omega_0} \frac{\left|\mathbf{w}^H(t)\mathbf{h}(\mathbf{f},\theta,r,t)\right|^2}{\mathbf{w}(t)\mathbf{w}^H(t)} \mathrm{d}f\,\mathrm{d}\theta\,\mathrm{d}r\,\mathrm{d}t, \tag{26}$$

where $\Omega_f \triangleq 0 \le \mathbf{f} \le \Delta f_r$ with Δf_r denoting the frequency diverse increment resolution, $\Omega_\theta \triangleq 0 \le \theta = \theta_{in} \le \Xi_\theta$ with Ξ_θ being the angular resolution, $\Omega_r \triangleq 0 \le r \le \Xi_r$ with Ξ_r being the range resolution, and $\Omega_t \triangleq 0 \le t \le T_{in}$ with T_{in} being the time frame interval. Note that $\|\mathbf{w}(t)\|^2 = 1$.

Accordingly, we can write $\mathbf{w}(t) = \mathbf{h}(\mathbf{f},\theta,r,t)$; and $\mathbf{w}(t)$ can be decomposed as

$$\mathbf{w}(t) = \mathbf{w}_f(t) \odot \mathbf{w}_\theta(t) \odot \mathbf{w}_r(t) \odot \mathbf{w}_t(t), \tag{27}$$

where $\odot$ denotes Hadamard product operator. Using equation (26), we can rewrite the energy beamforming focusing as

$$E_{\text{nergy}}^{\text{Proposed scheme}} \triangleq \int_{\Omega_f} \left|\mathbf{w}_f^H(t)\mathbf{h}(\mathbf{f})\right|^2 \mathrm{d}f \cdot \int_{\Omega_\theta} \left|\mathbf{w}_\theta^H(t)\mathbf{h}(\theta)\right|^2 \mathrm{d}\theta \cdot \int_{\Omega_r} \left|\mathbf{w}_r^H(t)\mathbf{h}(r)\right|^2 \mathrm{d}r \cdot \int_{\Omega_t} \left|\mathbf{w}_t^H(t)\mathbf{h}(t)\right|^2 \mathrm{d}t. \tag{28}$$

Supposing that phased array has been utilized, the energy beamforming focusing can be likewise given as

$$E_{\text{nergy}}^{\text{Phased-array}} \triangleq \int_{\Omega_\theta} \left|\mathbf{w}_\theta^H(t)\mathbf{h}(\theta)\right|^2 \mathrm{d}\theta. \tag{29}$$

By inspecting equations (28) and (29), we can see that using FDA offers better energy beamforming focusing capability than phased array.

3.3. Secrecy Energy Efficiency Analysis. In order to create a balance between the power consumed by the proposed transmitter and SSR, we resort to secrecy energy efficiency (SEE) metric, which can be written as [40]

$$\eta_{\text{EES}}(\text{bit/joule/Hz}) = \frac{C_{\text{sec}}}{P_T}, \tag{30}$$

where C_{sec} is expressed in equation (18) and $P_T = \ell\|\mathbf{w}\|_F^2 + NP_C + P_B$ with P_T denoting the total consumed power at the proposed transmitter and $\ell \ge 1$ representing the power amplifier inefficiency factor. P_c is defined as the antenna circuit power, P_B is the power consumption of the baseband, and $\|\cdot\|_F^2$ denotes Frobenius norm.

4. Simulation Analysis

We consider similar simulation parameters in [15] unless otherwise stated. Additionally, the following parameters were assumed: in desired group 1, the respective users are located at 70°, 300 m and 110°, 800 m. The radiated signals will arrive at $t_1 = 1\,\mu$s and $t_2 = 2.66\,\mu$s, respectively. $f_0 = 30$ GHz, $\Delta f = 20$ kHz, and $R_s = 6$. Note that we adopted $R_s = 6$ to capture quality of service (QoS) during transmission with the wiretap code, because the actual rate of the information is the secrecy data rate, while codeword rate is the total rate of the information and rate cost to achieve secrecy. For instance, desired group with high codeword rate transmission with low secrecy data rate actually gets the confidential information slowly, which affects QoS. Simulation parameters and their values are given in Table 1. Note that line of propagation channel is assumed.

Table 1: Simulation parameters and their values.

Parameters	Values
N	10, 11, and 15
d	$\lambda/2$
Δf	20 kHz
(θ_{u_1}, r_{u_1}) and (θ_{u_2}, r_{u_2})	70°, 300 m and 110°, 800 m
R_s	6
f_0	30 GHz
t_1 and t_2	1 μs and 2.66 μs

Since we employ Costas sequence (CS) matrix to design the frequency increments, which offers authentication procedure, Figure 3 shows beamforming performances for distinct CS matrix adopted for desired group(s) authentication process. From Figure 3(a) to 3(c), it can be noticed that, by employing the CS matrix for the frequency increment, it will be very difficult for any Eve group to have the knowledge of the sequence used, since there are no obvious peaks along angle-range direction in the figures. Hence, the CS matrix adopted is more suitable for the desired group(s) authentication before the useful information transmission.

In Figure 4, we have depicted the BER curves as a function of angle and range dimension of the proposed scheme considering one desired group. Also, leakage-based method in [15, 41] was employed as a benchmark. From Figure 4(a), it was observed that the three schemes offer better performances along the desired two main angle beams dimensions. But outside the two main angle beams dimensions, the performance of BER curves is seriously degraded. This implies that it will be difficult for Eve to retrieve the useful information successfully outside the two main angle beam dimensions.

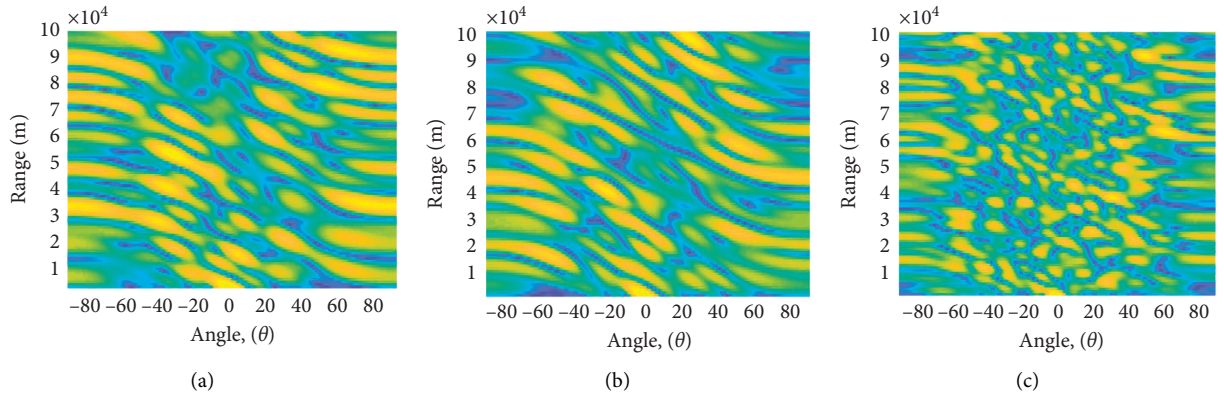


Figure 3: Angle-range beamforming performances for distinct Costas sequence (CS) matrix adopted for desired group(s) authentication process: (a) $N = 10$, {1, 2, 4, 8, 5, 10, 9, 7, 3, 6}, (b) $N = 11$, {1, 3, 7, 2, 5, 11, 10, 8, 4, 9, 6}, and (c) $N = 15$, {2, 8, 9, 12, 4, 14, 10, 15, 13, 7, 6, 3, 11, 1, 5} with adopted $\Delta f = 10$ kHz.

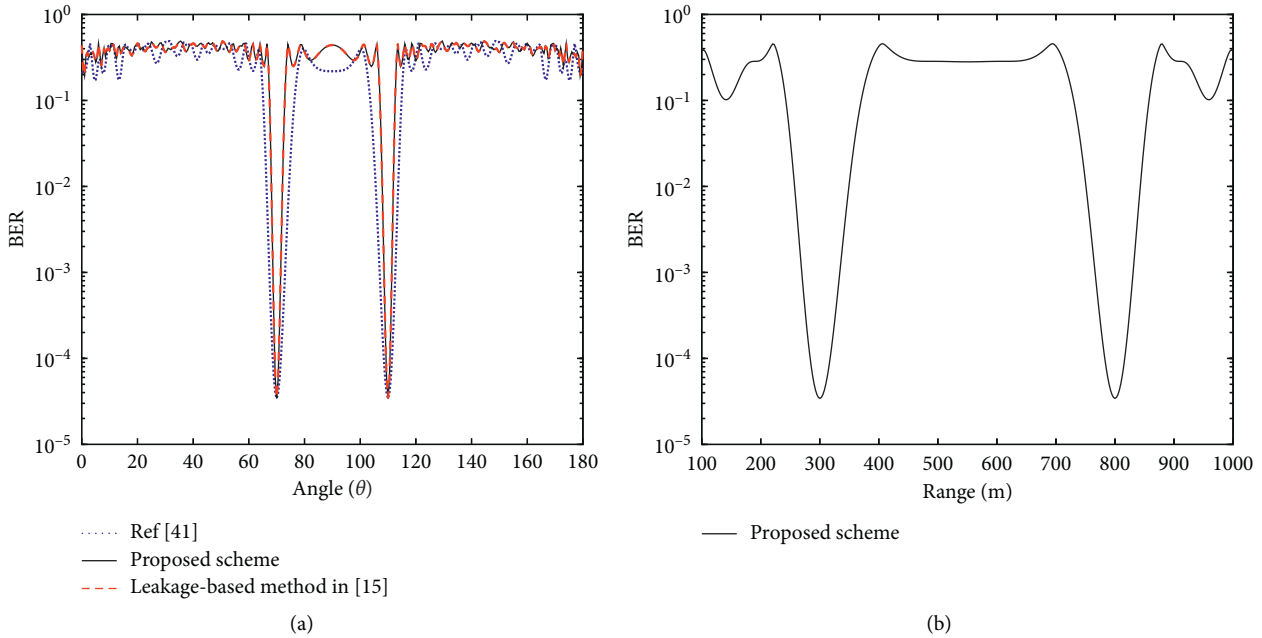


Figure 4: BER curves for desired group: (a) two main beams along angle dimension; (b) two main beams along range dimension.

Moreover, the proposed scheme and [15] have narrower main beamwidth than that of [41] in angle focusing directions. In Figure 4(b), we only show the two main range beams dimensions for the proposed scheme since the leakage-based method in [15, 41] has no range-dependent beamforming capability as this certainly limits the benefit in security. Again, it can be noticed that better BER curves towards the two main range beams have been achieved. This means that the proposed scheme can provide security in both angle and range dimensions and not just angle dimension in the leakage-based method in [15, 41].

As stated before, since it is hard to offer perfect security, in Figure 5, we have shown the SOP curves for different values of secrecy performances for the proposed scheme. It can be seen from the figure that as SOP increases, the useful information data rate increases. This means that the more the values of ξ are increased, the more the proposed scheme can achieve better system secrecy. More importantly, the figure gives insight into how to design different secrecy performance requirement for the proposed scheme. Note that when $\xi = 1$ has been attained, perfect secrecy is ensured.

Figure 6 depicts the asymptotic Eve's detectability error probability $\overline{\beta}$ for distinct values of $\overline{\gamma}_e(t)$. From the figure, we find that Eve achieved relatively high error decoding probability values, for instance, around 0.71 when $\overline{\gamma}_e(t) = 1$, 0.53 when $\overline{\gamma}_e(t) = 2$, and 0.43 when $\overline{\gamma}_e(t) = 3$.

Figure 7 plotted average useful data leakage rate A_{leakage} for different values of $\overline{\gamma}_e(t)$. We observed that both A_{leakage} and R_s increase. This means that not all the useful information is leaked along Eve's angle-range directions. It is worth pointing out that, to provide good secrecy performances, the wireless channel has a great influence.

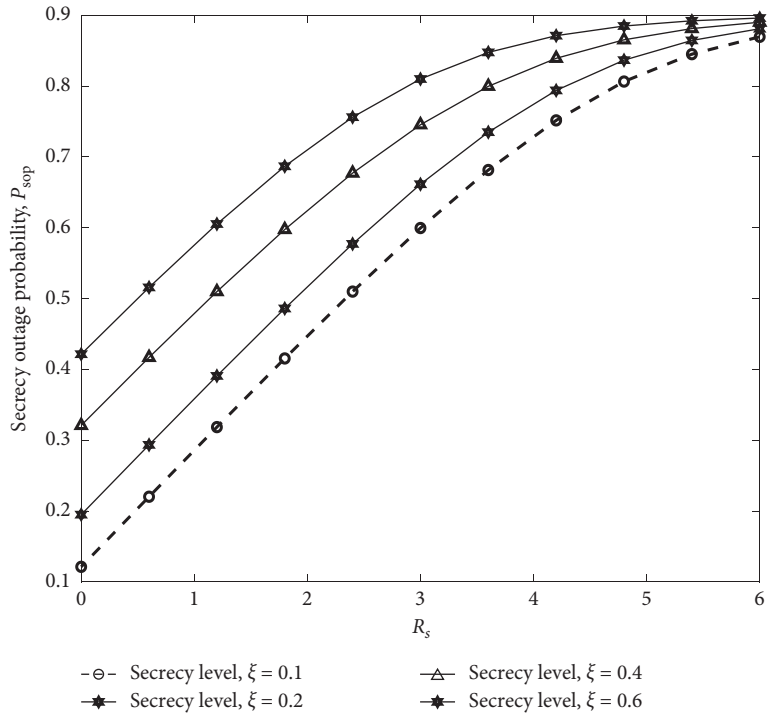


Figure 5: SOP curves for different levels of secrecy performances versus R_s.

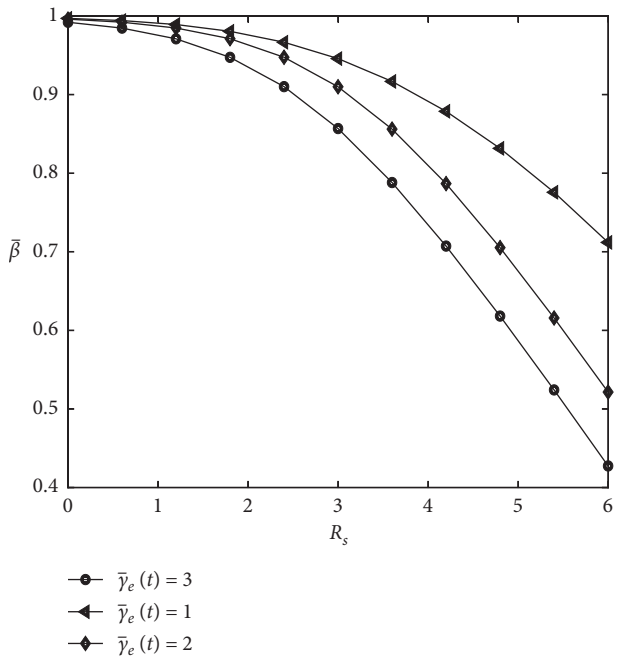


Figure 6: Asymptotic Eve's detectability error probability $\bar{\beta}$ versus R_s for distinct values of $\bar{\gamma}_e(t)$.

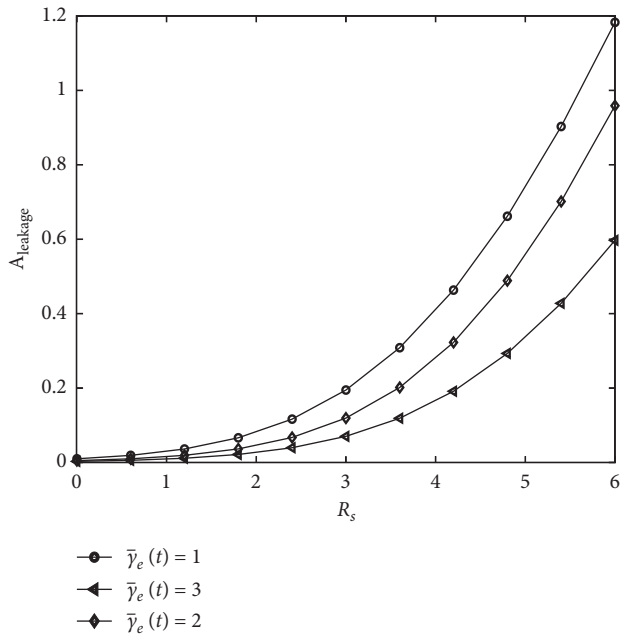


Figure 7: Average useful data leakage rate versus R_s for distinct values of $\bar{\gamma}_e(t)$.

We illustrate the SSR of the desired group for the proposed scheme and compare it with that of leakage-based method in [15, 41] and random FDA technique (RFDA) [29] in Figure 8. The SSR curve of the proposed scheme exceeds the leakage-based method in [15] and [41] in both low and high SNR regimes. Also, it exceeds RFDA technique [29] in low and medium SNR regions. This is due to the fact that RFDA technique has randomly selected frequency increments, making it unstable. On the other hand, the proposed Costas sequence matrix is presented in a concise way with better stability than the RFDA technique. Moreover, the values of SSR in the figure for the proposed scheme, using RFDA technique [15, 29, 41], respectively, are around 13.5

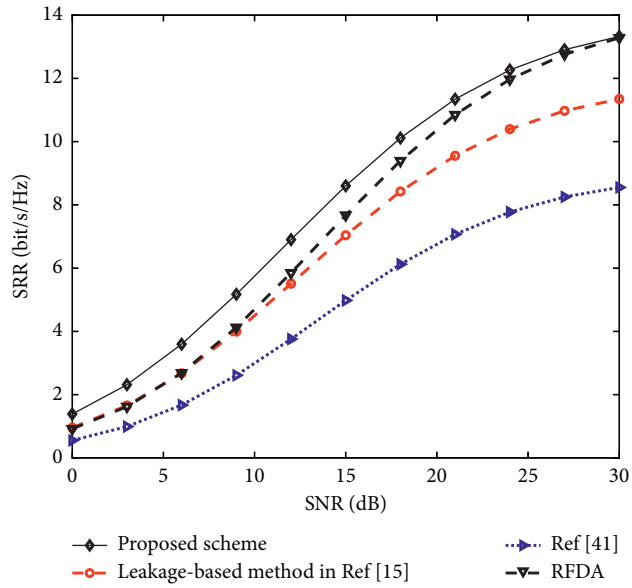


Figure 8: Desired group SSR as a function of SNR.

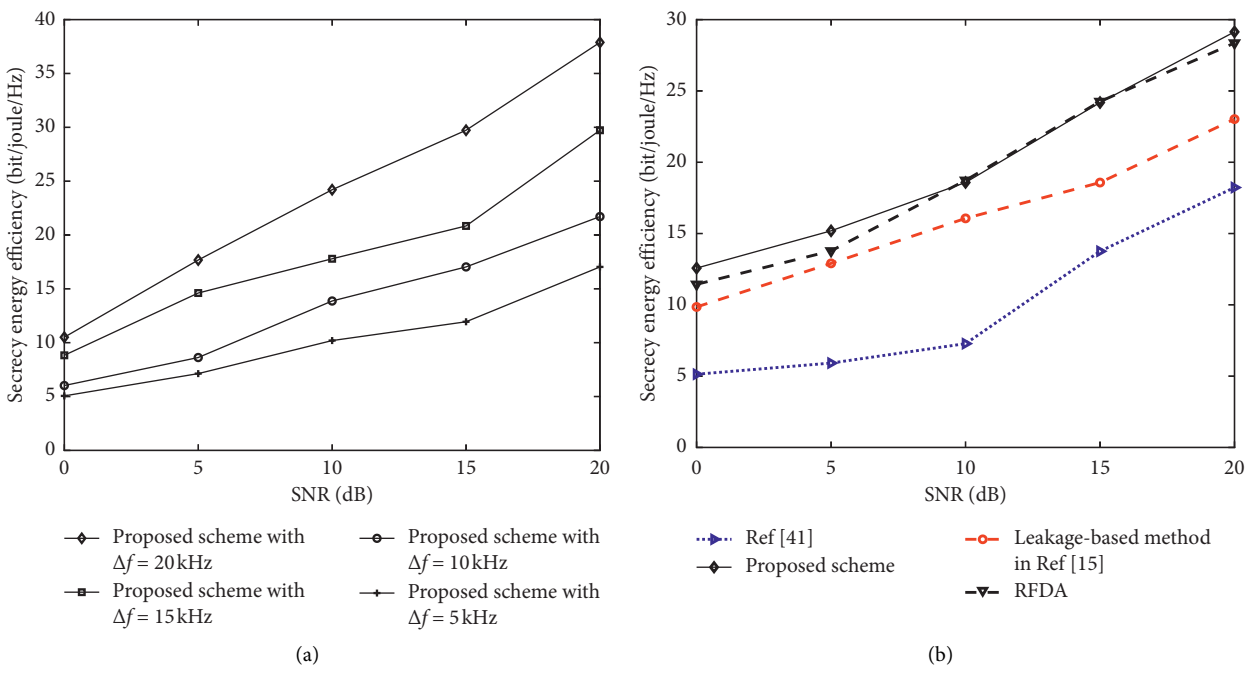


Figure 9: Secrecy energy efficiency (SEE) versus SNR: (a) proposed scheme with different values of Δf; (b) SEE curves comparisons between proposed scheme, leakage-based method in [15], and RFDA [29, 41].

(bps/Hz), 13.5 (bps/Hz), 11.3 (bps/Hz), and 8.3 (bps/Hz). The result of the proposed scheme is very promising.

In Figure 9, secrecy energy efficiency (SEE) versus SNR has been illustrated. In Figure 9(a), we show SEE curves for distinct values of Δf. In FDA analysis [27, 28], as Δf increases, we achieve better resolution. Therefore, with increasing Δf, it is evident that SEE curves get better (higher SEE). In Figure 9(b), we compare the SEE performances of the proposed scheme, random FDA (RFDA) [29], and leakage-based method in [15, 41]. The proposed scheme has better SEE performance than leakage-based method in [15, 41] in low and high SNR regions. In addition, it is easily noticed that the proposed scheme exceeds the RFDA [29] from around 0 dB to 10 dB in SNR regions. This is because the employment of Costas sequence (CS) matrix has narrow peak and low sidelobes [31], which can improve the energy efficiency than randomly selected frequency increments (RFDA) [29].

5. Conclusions

This paper proposes authentication and secrecy metrics in multicast scenarios using Costas sequence (CS) matrix FDA directional modulation aided with AN matrix. We formulate authentication technique using CS matrix and analyze secrecy metrics for the proposed scheme. Further, we derive the energy beamforming focusing and evaluate secrecy energy efficiency (SEE). From simulation analysis, the proposed scheme has potential advantages compared to leakage-based method in [15, 41]. More importantly, the secrecy metrics provide us with useful insights, namely, distinct levels of secrecy performances requirement to ensure perfect secrecy, Eve's error decoding probability (i.e., Eve detectability), and, finally, how likely the private data can be leaked towards Eve's angle-range directions. It is realized that, in several realistic cases, the transmitter may be unable to acquire the angle-range direction information. Therefore, in the future work, this problem will be addressed.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

References

[1] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[2] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: transmission optimization in multi-input single-output wiretap channelsficial noise: transmission optimization in multi-input single-output wiretap channels," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1771–1783, 2015.

[3] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[5] M. R. A. Khandaker, C. Masouros, and K.-K. Wong, "Constructive interference based secure precoding: a new dimension in physical layer security," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2256–2268, 2018.

[6] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[8] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, 2015.

[9] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[10] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 425–430, 2011.

[11] 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.

[12] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximizationficial–noise aided transmit optimization for MISO multi–eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.

[13] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust Cooperative Beamforming and Artificial Noise Design for Physical-Layer Secrecy in AF Multi-Antenna Multi-Relay Networksficial noise design for physical–layer secrecy in AF multi–antenna multi–relay networks," *IEEE Transactions on Signal Processing*, vol. 63, no. 1, pp. 206–220, 2015.

[14] X. Zhang, X. Zhou, and M. R. McKay, "On the design of Artificial-Noise-Aided secure multi-antenna transmission in slow fading Channelsficial noise–aided secure multi–antenna transmission in slow fading channels," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, 2013.

[15] 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, 2018.

[16] X. Zhang, X. G. Xia, Z. He, and X. Zhang, "Phased-array transmission for secure mmWave wireless communication via polygon construction," *IEEE Transactions on Signal Processing*, vol. 68, pp. 327–342, 2019.

[17] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3231–3245, 2013.

[18] Y. Ju, H. M. Wang, T. X. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2114–2127, 2017.

[19] R. Ma, W. Yang, X. Sun, L. Tao, and T. Zang, "Secure communication in millimeter wave relaying networks," *IEEE Access*, vol. 7, pp. 31218–31232, 2019.

[20] Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2675–2689, 2018.

[21] A. Kalantari, M. Soltanalian, S. Maleki et al., "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.

[22] A. Chatzinotas, D. Spano, A. Kalantari et al., "Symbol–level and multicast precoding for multiuser multiantenna downlink: a survey, classification and challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 1–21, 2018, http://arxiv.org/abs/1703.03617.

[23] E. Karipidis, N. D. Sidiropoulos, and Z.-Q. Luo, "Far-Field Multicast Beamforming for Uniform Linear Antenna Arraysfield multicast beamforming for uniform linear antenna arrays," *IEEE Transactions on Signal Processing*, vol. 55, no. 10, pp. 4916–4927, 2007.

[24] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1–39, 2016.
[25] P. Antonik, *An investigation of a frequency diverse array*, University College London, London, UK, Ph.D. dissertation, 2009.
[26] Y. Liu, H. Rui, 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.
[27] 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.
[28] S. Y. Nusenu, "Development of frequency modulated array antennas for millimeter-wave communications," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 6940708, 15 pages, 2019.
[29] J. Hu, S. Yan, F. Shu et al., "Artificial-Noise-Aided Secure Transmission with Directional Modulation Based on Random Frequency Diverse Arraysficial–noise–aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.
[30] S. Y. Wang, Z. Wang, and W. Q. Wang, "FDA radar using Costas sequence modulated frequency increments," in *Proceedings of the 2016 CIE International Conference on Radar (RADAR)*, Guangzhou, China, October 2016.
[31] N. Levanon and E. Mozeson, *Radar Signals*, Wiley, Hoboken, NJ, USA, 2004.
[32] F. Shu, Z. Wang, R. Chen, Y. Wu, and J. Wang, "Two high-performance schemes of transmit antenna selection for secure spatial modulation," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8969–8973, 2018.
[33] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, U.K, 1987.
[34] 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.
[35] 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.
[36] N. Li, X. Tao, and J. Xu, "Ergodic secrecy sum–rate for downlink multiuser MIMO systems with limited CSI feedback," *IEEE Communications Letters*, vol. 18, no. 6, pp. 969–972, 2014.
[37] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels: A Unified Approach to Performance Analysis*, Wiley, Hoboken, NJ, USA, 2000.
[38] B. He, X. Zhou, and A. Lee Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Transactions on Wireless Communication*, vol. 15, no. 10, p. 6913, 2016.
[39] X. Zhou, M. R. McKay, B. Maham, and A. Hjrungnes, "Rethinking the secrecy outage formulation: a secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302–304, 2011.
[40] M. El–Halabi, T. Liu, and C. N. Georghiades, "Secrecy capacity per unit cost," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1909–1920, 2013.
[41] L.-U. Choi and R. D. Murch, "A transmit preprocessing technique for multiuser MIMO systems using a decomposition approach," *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 20–24, 2004.