Proceedings Paper:
Li, W, Ghogho, M, Zhang, J et al. (2019) Design of an Energy-Efficient Multidimensional Secure Constellation for 5G Communications. In: 2019 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE ICC 2019, 20-24 May 2019, Shanghai, China. IEEE. ISBN: 978-1-7281-2374-5. ISSN: 2474-9133. EISSN: 2474-9133.

https://doi.org/10.1109/ICCW.2019.8756862

Design of an Energy-Efficient Multidimensional Secure Constellation for 5G Communications

Wei Li[1], Mounir Ghogho[2,4], Junqing Zhang[3], Des McLernon[4], Jing Lei[1] and Syed Ali Raza Zaidi[4]
[1]College of Electronic Science and Engineering, National University of Defense Technology, China.
Email: liwei.nudt.cn@gmail.com
[2]International University of Rabat, Morocco. Email: m.ghogho@ieee.org
[3]Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, U.K.
Email: Junqing.Zhang@liverpool.ac.uk
[4]University of Leeds, Leeds LS2 9JT, U.K. Email: d.c.mclernon@leeds.ac.uk; S.A.Zaidi@leeds.ac.uk

***Abstract*—Energy efficiency and security are two important metrics for the fifth generation (5G) wireless networks. Existing constellation designs often consider spectral efficiency but neglect energy efficiency and security. We define the concept of energy efficiency of constellations and propose a multidimensional secure constellation (MSC) design to improve the energy efficiency, security, and bit error rate (BER) performance. A general closed-form algorithm to construct the n-dimensional constellation mapping codebook is proposed. A multi-dimensional rotation method is proposed to enhance the security and prevent eavesdroppers from recovering symbols. A closed-form expressions for the upper bound on the BER for the proposed MSC is obtained. Simulation results show that when the dimension reaches 255, MSC can achieve a BER performance of the order of 10^{-4} at SNR = -8dB without binary channel coding. For the same throughput, the proposed method is shown to outperform polar coding (1-2 dB SNR gain at BER=10^{-4}).**

***Index Terms*—Energy-efficient, constellation, communication system, security, orthogonal frequency-division multiplexing (OFDM)**

I. Introduction

In 5G communication scenarios such as the internet of things (IoT), low power consumption, high reliability, and secure communication are challenging problems. For example, some wireless sensor devices require more than 10 years of working time, but the battery capacity is limited. There is thus an urgent need for high energy efficient communication technologies.

Constellation mapping, as a basic module in digital communications, converts a stream of bits into a stream of complex vectors. The mapping plays an important role in determining bit error rate (BER) performance and energy efficiency. Traditional methods, such as pulse-amplitude modulation (PAM), phase shift keying (PSK), and quadrature amplitude modulation (QAM), consider signal constellations in one or two-dimensional signal space.

The multidimensional signal constellation proposed by [1] maps binary symbols to vectors in the n-dimensional Euclidean space ($n > 2$). Thanks to multidimensional diversity, it can achieve BER gain over standard 2-D constellation. The design of constellation mapping in high dimensional space provides greater flexibility. A multi-dimensional hypercube is built from QPSK constellation in a bit-interleaved coded modulation (BICM) system [2]. A multidimensional subcarrier mapping for bit-interleaved coded OFDM was proposed in [3]; the results show that multidimensional mapping can successfully exploit the multipath diversity and provide remarkable coding gains.

However, the above works are still based on traditional 2-D constellations such as PSK and QAM, where the design flexibility and dimension diversity of the multidimensional space are not fully utilized. In addition, the existing literature on multidimensional constellation design does not consider the energy efficiency and cannot be used in low signal-to-noise ratio (SNR) scenarios. Indeed, energy efficiency is limited in 2-D constellations; hence, to improve energy efficiency, it is necessary to extend the constellation design to a higher dimensional space.

Wireless communication is vulnerable to eavesdropping because of its broadcast nature. There is a recent research trend to enhance the wireless security using encryption at the physical layer of the communication stack. This technique is referred to as physical layer encryption (PLE), and can protect data at the physical layer modulation stages, e.g., constellation mapping, subcarrier obfuscation, etc [4], [5]. PLE methods have been prototyped with many wireless systems, such as OFDM systems [6], [7], massive MIMO systems [8]–[10], untrusted relaying systems [11], IEEE 802.15.4 protocols [12], rateless codes [13] and sparse code multiple access (SCMA) [14]. However, the existing PLE methods also do not consider energy efficiency and low SNR communication scenarios. Designing a new constellation in a multidimensional space can therefore not only improve energy efficiency but also achieve secure communication.

Motivated by the above observations, this paper proposes a novel multidimensional and secure constellation design to achieve security and energy efficiency. We can use dimension diversity to carry additional information, which can reduce the required constellation energy consumption and achieve greater energy efficiency. In addition, the Euclidean distance between points of the multidimensional constellation is larger than that in the 2-D constellation counterparts, so that better

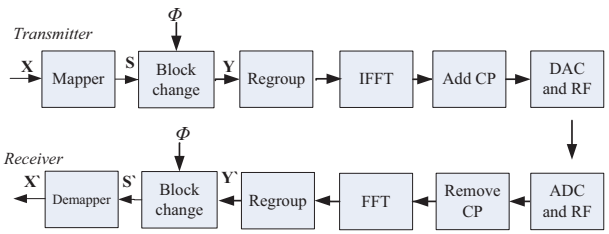

Fig. 1: The transmitter and receiver structure.

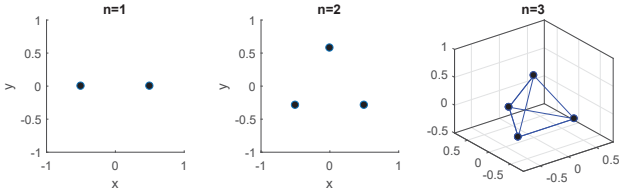

Fig. 2: Regular polyhedron in the n-dimensional space as constellation points.

BER performance can be obtained. Therefore, in Euclidean n-space, we need to design new constellations in order to get better performance.

Our main contributions are as follows.

1) A multidimensional secure constellation (MSC) design is proposed with a closed-form codebook generation algorithm for arbitrary dimensions. A secure multidimensional constellation rotation method based on polar coordinate system rotation is proposed.
2) The upper bounds on the symbol error rate (SER) and BER performance for the proposed MSC are derived. It is shown that MSC has very good BER performance.
3) The concept of constellation energy efficiency is defined. The energy efficiencies of different constellation diagrams are compared for a given SER.

The rest of this paper is organized as follows. Section II introduces the system model and proposed method. Performance analysis and simulations of the proposed scheme are presented in Section III and Section IV, respectively. Section IV concludes the paper

Notation: We will use $\|\cdot\|$ to denote the L_2 norm of a vector. $\mathbb{R}^{m\times n}$ represent the space of all $m \times n$ real-valued matrices.

II. System Model and Proposed Method

A. Overview

The system consists of a legitimate transmitter (Tx), Alice, who wants to communicate securely with a legitimate receiver (Rx), Bob, in the presence of an eavesdropper, Eve. An OFDM-based transceiver structure is shown in Fig. 1.

The transmitter first divides the input message into groups, each with *l* bits, i.e., $\mathbf{x} = \{x_1, x_2, ..., x_l\}$. The multidimentional mapper converts an *l*-bit binary vector into a real *n*-element vector:

$$\mathbf{S} = map(\mathbf{x}) : \mathbf{x} = \{x_1, x_2, \ldots, x_l\} \rightarrow \mathbf{S} = \{S_1, S_2, \ldots, S_n\}, \tag{1}$$

where $\mathbf{S} \in \mathbb{R}^{n\times 1}$ is the constellation signal in a multidimensional space. The details of the design will be discussed in Section II-B.

Block change module uses a phase vector to map a real *n*-element vector into another real *n*-element vector:

$$T(\mathbf{S}, \Phi) : \mathbf{S} = \{S_1, S_2, \ldots, S_n\} \overset{\Phi}{\rightarrow} \mathbf{Y} = \{Y_1, Y_2, \ldots, Y_n\}, \tag{2}$$

where $\mathbf{Y} \in \mathbb{R}^{n\times 1}$. The block change modules is designed to rotate the constellation symbols in order to obtain an even distribution, which will be discussed in Section II-C.

The steam of codewords are loaded onto the in-phase (I) and quadrature (Q) channels of the data subcarriers. When the number of available channel used in one OFDM frame (i.e. the number of data subcarriers times the number of OFDM symbol in one frame) is not a multiple of $2n$, zero padding is used, in order to decode the frames separately.

Demodulation at the receiver is the reverse of the above process:

$$\mathbf{S}' = D(\mathbf{Y}', \Phi), \tag{3}$$

where D is the decryption function, $\mathbf{Y}'$ is the received signal after the FFT module and $\mathbf{S}'$ is the recovered constellation symbols. The demapper module at the receiver converts the constellations into binary sequences as

$$\mathbf{X}' = demap(\mathbf{S}'). \tag{4}$$

B. Multidimensional Initial Constellation Design

In order to achieve energy efficiency and good BER performance, the multidimensional constellation design aims to ensure that each constellation point has the same energy and that the distance between any two constellation points is a constant.

The vertices of a regular polyhedron in the n-dimensional space are used as the initial constellation points, and the side length is fixed to 1. Three examples of regular polyhedral constellations are shown in Fig. 2. The distances between each constellation point and the centre point are the same in regular polyhedrons. In the *n*-dimensional space, we can only construct $n + 1$ vertices/codewords that satisfy the following conditions: i) the codewords have the same energy, and ii) the distance between *any* two codewords is a constant. Orthogonality of the codewords, which has been used in the literature for other codebook constructions, is not a design criterion in the proposed method.

The distance between these constellation points and the centre point determines the energy of the constellation, which is given in the next theorem.

Theorem 1. *For a regular polyhedron with side length 1 in an n-dimensional Euclidean space, the distance between the centre point O and each vertex is given by*

$$y_n = \sqrt{\frac{n}{2(n+1)}},\ n = 1, 2, 3, ... \tag{5}$$

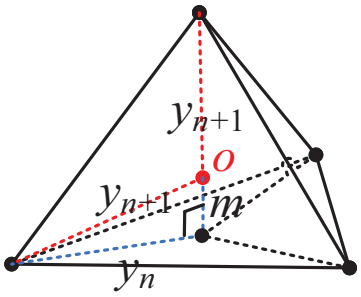

Fig. 3: Schematic diagram of the distance between the constellation points and the centre of gravity in the n-dimensional Euclidean space.

Proof: The proof is based on the mathematical induction.

Base case: Show that the statement holds for n = 1.

$$y_1 = 1/2 = \sqrt{\frac{n}{2(n+1)}}. \tag{6}$$

Inductive step: Show that if the expression for y_k holds true, then that for y_{k+1} also holds true.

As shown in Fig. 3, m is the distance between O and bottom surface of the regular polyhedron. According to Pythagorean Theorem, we have that:

$$\begin{cases} y_n^2 + m^2 = y_{n+1}^2 \\ y_n^2 + (y_{n+1} + m)^2 = 1. \end{cases} \tag{7}$$

Solving the equations, we get

$$y_{n+1} = \sqrt{\frac{1}{4(1-y_n^2)}}. \tag{8}$$

So

$$\begin{aligned} y_{k+1} &= \sqrt{\frac{1}{4(1-y_k^2)}} = \sqrt{\frac{1}{4(1-\frac{k}{2(k+1)})}} \\ &= \sqrt{\frac{k+1}{2((k+1)+1)}}. \end{aligned} \tag{9}$$

Thereby showing that the expression for y_{k+1} indeed holds true.

As the base case and inductive step have been validated, by mathematical induction the statement holds true for all natural numbers $n = 1, 2, 3, .$ The proof is completed. ■

Next, we need to generate an n-dimensional constellation mapping codebook $\mathcal{C}_n = \{C_{i,j}\}, i = 1, 2, ..., n+1; j = 1, 2...n$, whose generation algorithm is given in **Algorithm 1**. The n elements of each row in $\{C_{i,j}\}$ form the coordinates of a constellation point in n-dimensional space. For example, $(0.5, -0.2886, -0.2041, -0.1581, -0.1291)$ in (10) is the coordinate of the first point in the 5-D space.

Algorithm 1 n-dimensional constellation codebook generation algorithm.

Require:
Dimension, n;
Ensure:
Constellation codebook, $\{C_{i,j}\}, i = 1, 2, ..., n+1; j = 1, 2...n.$;
for k= 1 to n **do**
  $y_k = \sqrt{\frac{k}{2(k+1)}}$; // the distance between the constellation points and the centre point
end for
$C_{1,1} = y_1, C_{2,1} = -y_1$;
for k= 2 to n **do**
  $C_{k+1,t} = 0, (t = 1, 2, ..., k-1)$;
  $C_{t,k} = -\sqrt{y_k^2 - y_{k-1}^2}, (t = 1, 2, ..., k)$;
  $C_{k+1,k} = y_k$;
end for
return $\{C_{i,j}\}, i = 1, 2, ..., n+1; j = 1, 2...n.$

$$\mathcal{C}_5 = \left\{ \begin{array}{ccccc} 0.5 & -0.2886 & -0.2041 & -0.1581 & -0.1291 \\ -0.5 & -0.2886 & -0.2041 & -0.1581 & -0.1291 \\ 0 & 0.5773 & -0.2041 & -0.1581 & -0.1291 \\ 0 & 0 & 0.6123 & -0.1581 & -0.1291 \\ 0 & 0 & 0 & 0.6324 & -0.1291 \\ 0 & 0 & 0 & 0 & 0.645 \end{array} \right\}. \tag{10}$$

After getting the codebook, the next step is mapping. There are $n+1$ rows in the codebook, and the i-th row is marked as $\mathbf{c}_i = \{C_{i,1}, C_{i,2}, ..., C_{i,n}\}$. The length of the corresponding input message $\mathbf{x}$ is $l = \log_2(n+1)$. Since the distances between any two codewords are equal to each other and the codewords have the same energy, the mapping relationship between the message and the codeword does not affect the performance. Therefore, we can choose a mapping relationship arbitrarily. For example, we redefine (1) as

$$S = \mathbf{c}_{[\mathbf{x}]}, \tag{11}$$

where $[\mathbf{x}]$ represents the row index corresponding to the binary vector x in the codebook.

C. Multidimensional Rotation Design

We can see that the codewords in (10) are not evenly distributed, which results in a high peak-to-average power ratio of the output signal (after the IFFT operation). We hence rotate the constellation to spread the energy of each constellation more evenly across the n dimensions. This rotation can also serve as an encryption method. The knowledge of the phase vector, Φ, is required to recover the transmitted message, without undermining SER performance. The required n-D rotation is different from the existing 2-D rotation in [9]. The proposed design consists of the following steps.

- The same phase vector

$$\Phi = \{\phi_1, \phi_2, ..., \phi_{n-1}\}, \phi_i \in [0, 2\pi) \tag{12}$$

is generated at both transmitter and receiver through channel reciprocity. The phase vectors generation method can be found in our previous work [9]. When there is an inconsistency in the phase vectors between transmitter and receiver, it is necessary to eliminate the inconsistency through error correction or negotiation. The information reconciliation technique in key generation can be adopted for this purpose [15].

- Alice and Bob transform the constellation symbols S and S' based on the phase vector Φ, respectively.

In order to ensure that the distance of the constellation point does not change, we operate in the polar coordinate space by only changing the phase of the constellation, and does not change the amplitude of the constellation. The conversion method between Cartesian coordinates and polar coordinates is available in [16]. Assume that the polar coordinates of the constellations S and S' at Alice and Bob are $(r, \mathbf{\Theta})$ and $(r', \mathbf{\Theta}')$, respectively. We have that

$$r = r'; \tag{13}$$

$$\mathbf{\Theta} = \{\theta_1, \theta_2, \theta_3, ..., \theta_{n-1}\}; \tag{14}$$

$$\mathbf{\Theta}' = \{\theta'_1, \theta'_2, \theta'_3, ..., \theta'_{n-1}\}. \tag{15}$$

The encryption operation at Alice is

$$\mathbf{\Theta}_Y = \{\theta_1 + \phi_1, \theta_2 + \phi_2, \theta_3 + \phi_3, ..., \theta_{n-1} + \phi_{n-1}\}. \tag{16}$$

Then, we convert $(r, \mathbf{\Theta}_Y)$ to Cartesian coordinates, and generate the encrypted symbol $\mathbf{Y}$ for subsequent processing.

The reverse process is operated at the receiver, Bob. After receiving the Cartesian coordinates $\mathbf{Y}'$, they are converted to polar coordinates $(r_Y, \mathbf{\Theta}_{Y'})$. Then, the following phase conversion is performed to get the decrypted polar coordinates $\mathbf{\Theta}'$:

$$\mathbf{\Theta}' = \{\theta_{Y_1} - \phi_1, \theta_{Y_2} - \phi_2, \theta_{Y_3} - \phi_3, ..., \theta_{Y_{N-1}} - \phi_{N-1}\}. \tag{17}$$

Then convert the polar coordinates $(r', \mathbf{\Theta}')$ back to Cartesian coordinates $\mathbf{S}'$ for subsequent processing.

After the rotation, the codebook example in (10) is changed to (18).

$$\mathcal{C}'_5 = \left\{ \begin{array}{ccccc} 0.0633 & -0.3592 & -0.4681 & -0.0391 & 0.2509 \\ 0.5861 & 0.1225 & 0.2134 & -0.0776 & 0.0814 \\ -0.0429 & -0.3345 & 0.1908 & 0.3363 & -0.3917 \\ -0.1289 & 0.1913 & -0.1571 & -0.4351 & -0.3866 \\ -0.3388 & -0.0702 & 0.3842 & -0.1811 & 0.3414 \\ -0.1389 & 0.4501 & -0.1632 & 0.3965 & 0.1046 \end{array} \right\}. \tag{18}$$

The codewords are now more evenly distributed across the n dimensions.

III. Performance Analysis

We will evaluate the performance of the proposed constellation from the perspectives of error rates, energy efficiency, throughput, and security.

A. SER and BER

As the encryption and decryption rotations are isometric transformations, they do not change the SER performance and energy distribution of the constellation [5]. We thus only need to consider the constellation before the encryption transformation when analyzing the SER and energy efficiency. Assuming that the additive noise is isotropic in the n-dimensional Euclidean space and follows the Gaussian distribution, the maximum likelihood (ML) detector of the signal constellation $\mathbf{S}'$ is:

$$\arg\min_{\mathbf{S}\in\mathbf{C}} \left\|\mathbf{S}' - \mathbf{S}\right\|. \tag{19}$$

When n = 1, it is a BPSK modulation, we have the SER and BER as

$$P_e(1) = Q\left(\frac{d_{\min}}{2\delta}\right), \tag{20}$$

where $d_{\min}$ is the minimum distance of any pair of symbols in the signal constellation, δ^2 is the variance of the noise, and the function $Q(z)$ is defined as

$$Q(z) = \int_z^\infty \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx. \tag{21}$$

When $n > 1$, because the distance between any pair of points in the signal constellation is equal, we can replace the n-D detection algorithm with n binary decisions. We have the upper bound of SER as

$$P_e(n) \leq 1 - (1 - P_e(1))^n \approx nP_e(1) = nQ\left(\frac{d_{\min}}{2\delta}\right). \tag{22}$$

From (5), the SNR can be written as

$$\gamma = \frac{y_n^2}{n\delta^2} = \frac{1}{(2n+1)\delta^2}, \tag{23}$$

where the power of the symbol is y_n^2 and the power of noise in a n-dimensional space is $n\delta^2$.

Because the positions of points in our constellation are symmetrical, it is reasonable to assume that on average half of the bits are wrong in each error symbol. The approximate value of BER is

$$P_b(n) \approx 1/2 \cdot P_e(n) \leq 1/2 \cdot nQ(\sqrt{\frac{n+1}{2}\gamma}). \tag{24}$$

It can thus be concluded that the BER will decrease significantly when n increases.

B. Energy Efficiency

In order to measure the energy efficiency of the constellation, we define the following indicator.

Definition 2. For a constellation set $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, ...\mathbf{c}_\tau\}, \mathbf{c}_i \in \mathbb{R}^n$, $d_{\min} = \min_{i\neq j} \|\mathbf{c}_i - \mathbf{c}_j\|$, the energy efficiency of $\mathcal{C}$ is defined as

$$E_{\mathcal{C}} = \frac{\log_2\tau}{\sum_{i=1}^{\tau} \|\mathbf{c}_i\|^2/(\tau d_{\min^2})} = \frac{\tau d_{\min}^2 \log_2\tau}{\sum_{i=1}^{\tau} \|\mathbf{c}_i\|^2}. \tag{25}$$

The energy efficiency of the constellation indicates the amount of information that can be transmitted per energy unit under a given BER boundary (minimum distance of constellation). The spectral efficiency indicates the amount of information that can be transmitted per dimension.

For the proposed MSC in n-dimensional space, $\tau = n+1$ and $d_{\min} = 1$. From (6), we have that

$$E_{\mathcal{C},n} = \frac{\log_2(n+1)}{\|y_n\|^2} = \frac{2(n+1)\log_2(n+1)}{n}. \tag{26}$$

C. Throughput

In an OFDM system, the throughput is

$$R_{\text{OFDM}} = \frac{2N_d \times \frac{\log_2 \tau}{n}}{T_{\text{OFDM}}} \text{bit/s}, \tag{27}$$

where N_d is the number of data subcarriers and T_{OFDM} is the OFDM symbol duration. We can see that the throughput will decrease as n increases and increase as τ increase.

D. Security Analysis

Assuming that Eve can carry out the synchronization, channel estimation and equalization correctly. The recovered signal can be expressed as

$$\mathbf{Y}_e = \mathbf{Y} + \mathbf{n}_e = \mathbf{S}\mathbf{G}_t + \mathbf{n}_e, \tag{28}$$

where $\mathbf{G}_t \in \mathbb{R}^{N\times N}$ is the equivalent encryption matrix, and $\mathbf{n}_e \in \mathbb{R}^{N\times N}$ is a noise matrix. Because Eve does knows neither the noise $\mathbf{n}_e$ nor $\mathbf{G_t}$, it is extremely challenging for her to recover $\mathbf{S}$ from $\mathbf{Y_e}$.

If Eve uses brute force attack, the size of the search space for $\mathbf{G}_t$ is λ^{N^2}, where λ is the phase resolution. If Eve searches for the phase vector Φ in (12), the size of the search space will be λ^{N-1}. Take $N = 128, \lambda = 256$, as an example, and the size of the search space reaches 2^{131072} for $\mathbf{G}_t$ and 2^{1026} for Φ. In addition, Eve cannot get the exact correspondence between $\mathbf{Y}_e$ and $\mathbf{S}$ due to noise interference. So brute force methods are impossible to implement. In order to further increase the difficulty of eavesdropping, we can change $\mathbf{G}_t$ over time t, using channel reciprocity.

IV. Numerical Results

A. Simulation Setup

The simulation model is based on the physical layer structure of IEEE 802.16 OFDM protocol. The parameters are: DFT size = 256; a cyclic prefix length = 64; the number of data subcarriers, N_d, is 192; 8 pilots at specific locations are inserted for channel tracking; 56 edge subcarriers are not used (i.e. zero padded); no binary channel coding is used; the bandwidth is 4 MHz; symbol time duration is 80 μs. The simulations are based on 20000 frames and each frame contains 10 OFDM symbol.

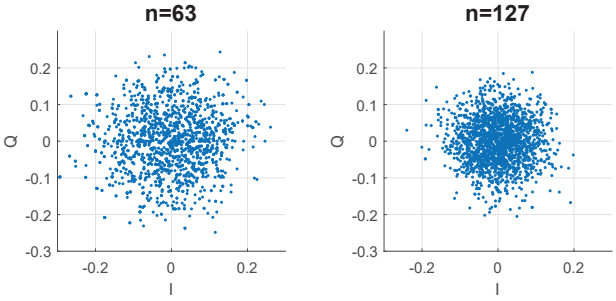

Fig. 4: The constellation scatter plot of $\mathbf{Y}$ at the transmitter.

B. Results

We project two example signal constellations of the MSC symbols $\mathbf{Y}$ onto the two-dimensional plane in Fig. 4. We can see that the output symbols of the MSC are randomly distributed in the four quadrants thanks to the multi-dimensional rotation.

The BER results of MSC (without binary channel coding) is shown in Fig. 5. We can observe that as the dimension n increases, the BER performance improves. When n = 255, the system can still obtain 10^{-4} BER performance even when SNR= -8 dB. We also compare the proposed method with binary-channel-coded QPSK, where the coding rate is set to be approximately equal to $\log_2(n+1)/n$ in order to compare the two methods at the same throughput. We chose polar codes, which are known as capacity achieving codes over binary-input discrete memoryless symmetric (BDMS) channels, with a list successive cancellation (SC) decoder. In Fig. 5 polar (256,8) indicates a polar code with code length = 256 and information bits length = 8. Polar (256,8) has the same throughput as MSC with n = 255; Polar (128,7) has the same throughput as MSC with n=128; Polar (128,12) has the same throughput as MSC with n = 63.

The results show that when the coding rate is the same, the proposed method outperforms the polar codes (1-2 dB SNR gain when BER=10^{-4}). This may be because BPSK/QPSK modulation converts the AWGN vector channel into BDMS channels and there is a performance gap between BDMS channels and AWGN channels. Note that at very low SNRs, the polarity code outperforms MSC. This is because all codeword distances in the MSC are equal, and on average, half of the bits will be wrong once the error occurs. The BER values in the region where MSC is outperformed by polar codes are however too large to be of interest in practice.

Fig. 6 shows the amount of information carried by one OFDM symbol. We can see that as n increases, the throughput will decrease. Indeed, in our system, the number of data subcarrier is 192, and the number of available channel uses per OFDM symbol is 384. The average amount of information transmitted per OFDM symbol for MSC is thus:

$$B_{n,MSC} = \frac{384}{n}\log_2(n+1), \tag{29}$$

For the system considered in this section, when $n = 255$

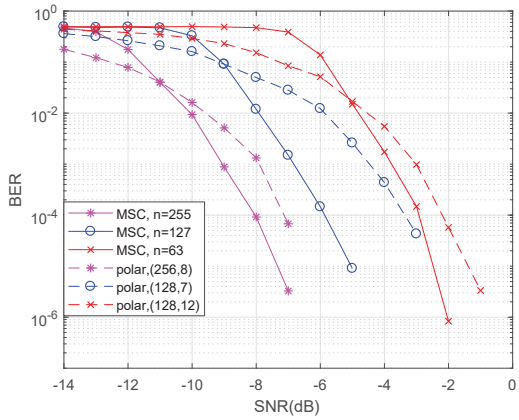

Fig. 5: BER performance of multidimensional secure constellation(without channel coding) and polar coding-QPSK in an OFDM system (n=255, 127, 63).

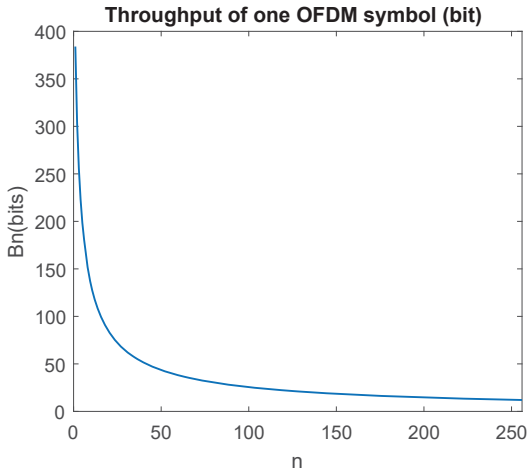

Fig. 6: The amount of information carried by one OFDM symbol. The number of data subcarriers is 192.

and the bandwidth is 4 MHz, each MSC-OFDM symbol can carry 12-bit messages, and the transmission data rate is 150 kbit/s.

As can be seen from the above results, when we increase the dimension n, the BER performance and energy efficiency will be improved significantly, but the throughput will decrease, i.e., the spectrum efficiency will decrease. Therefore, the value of n should be chosen according to the specific needs of the application.

V. Conclusions

This paper shows that multidimensional constellations have great advantages in terms of energy efficiency and BER performance, especially in low SNR regions. A general and closed-form algorithm to construct the n-dimensional constellation mapping codebook is proposed. A multi-dimensional rotation method is proposed to enhance the security and prevent eavesdropping. A closed-form expression for the upper bound on the BER is derived. A concept of energy efficiency of constellations is proposed. Simulations results show that the merits of the proposed method when compared with binary channel coding such as polar coding.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China (Numbers 61502518, 61702536 and 61601480), Natural Science Foundation of Hunan Province China (No. 2018JJ3609) and the China Scholarship Council (CSC) government-sponsored visiting scholar research program. This work was also partly supported by the UK British Council (Newton Fund) through the Project "Wireless Sensor Networks for Real Time Monitoring of Water Quality under Grant IL3264631003".

References

[1] A. Gersho and V. Lawrence, "Multidimensional signal constellations for voiceband data transmission," *IEEE J. Sel. Areas Commun.*, vol. 2, no. 5, pp. 687–702, Sep. 1984.

[2] N. H. Tran and H. H. Nguyen, "Design and performance of bicm-id systems with hypercube constellations," *IEEE Trans. Wireless Commun.*, vol. 5, no. 5, pp. 1169–1179, May 2006.

[3] N. Tran, H. Nguyen, and T. Le-Ngoc, "Multidimensional subcarrier mapping for bit-interleaved coded OFDM with iterative decoding," *IEEE Trans. Signal Process.*, vol. 55, no. 12, pp. 5772–5781, Dec. 2007.

[4] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the internet of things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, p. 420, 2017.

[5] W. Li, D. McLernon, J. Lei, M. Ghogho, S. Zaidi, and H. Hui, "Mathematical model and framework of physical layer encryption for wireless communications," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, UAE, Dec. 2018, pp. 1–6.

[6] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an ofdm physical layer encryption scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2114–2127, 2017.

[7] M. Sakai, H. Lin, and K. Yamashita, "Intrinsic interference based physical layer encryption for ofdm/oqam," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1059–1062, 2017.

[8] T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive mimo," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 5419–5436, 2017.

[9] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive mimo eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[10] S. Wang, W. Li, and J. Lei, "Physical-layer encryption in massive MIMO systems with spatial modulation," *China Communications*, vol. 15, no. 10, pp. 159–171, Oct. 2018.

[11] H. Xu and L. Sun, "Encryption over the air: Securing two-way untrusted relaying systems through constellation overlapping," *IEEE Trans. Wireless Commun.*, pp. 1–1, 2018.

[12] A. K. Nain, J. Bandaru, M. A. Zubair, and R. Pachamuthu, "A secure phase-encrypted ieee 802.15.4 transceiver design," *IEEE Trans. Comput.*, vol. 66, no. 8, pp. 1421–1427, 2017.

[13] Y. Huang, W. Li, and J. Lei, "Concatenated physical layer encryption scheme based on rateless codes," *IET Communications*, vol. 12, no. 12, pp. 1491–1497, Jul. 2018.

[14] K. Lai, J. Lei, L. Wen, G. Chen, W. Li, and P. Xiao, "Secure transmission with randomized constellation rotation for downlink sparse code multiple access system," *IEEE Access*, vol. 6, pp. 5049–5063, 2018.

[15] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Mar. 2016.

[16] L. E. Blumenson, "A derivation of n-dimensional spherical coordinates," *The American Mathematical Monthly*, vol. 67, no. 1, pp. 63–66, 1960.