



International Journal of Emerging Technologies in Computational and Applied Sciences(IJETCAS)

(Open Access, Double Blind Peer-reviewed, Refereed and Indexed Journal)

www.iasir.net

Text Message Transmission in Polar Encoded NOMA System Using Hybrid Chaotic Maps Based Cryptography and GD Approach Aided ZF Detection

Md. Humaun Kabir¹, Jinia Rahman², Shaikh Enayet Ullah²

¹Department of Computer Science and Engineering, Bangamata Sheikh Foilatunnesa Mujib Science & Technology University, Jamalpur-2010, Bangladesh

²Department of Electrical and Electronic Engineering, University of Rajshahi, Rajshahi-6205, Bangladesh

Abstract: In this paper, a comprehensive performance evaluative study has been made on a downlink multiuser 5G compatible MIMO NOMA wireless communication system. The proposed simulated system deploys Hybrid Chaotic Maps based cryptographic technique, ML decoding based Group Detection (GD) approach aided Zero Forcing (ZF) signal detection, Polar channel coding, and QAM digital modulation schemes. In our proposed system, two different text messages are transmitted simultaneously from the base station (BS) through 2×2 MIMO channel for two different users and the channel has been secured with the implemented encryption technique based on Hybrid Chaotic Maps. From the simulation results, it is observed that the system provides satisfactory performance under AWGN and Raleigh fading channels and improvement of its performance is highly linked up with the assigned allocated power to users, proper maintaining signal's phase difference between users and the system performance degrades with increase in noise power as compared to signal power.

Keywords: 5G; NOMA; Polar Coding; Hybrid Chaotic Maps based cryptography; GD aided ZF; ML decoding.

I. Introduction

To capacitate rapidly increasing number of users, non-orthogonal multiple access (NOMA) has proposed as a promising multiple radio access candidate for future generation wireless networks to increase spectral efficiency and achieve the desired throughput [1-2]. The next generation/ fifth generation (5G) of mobile communications is expected to be commercialized worldwide towards year 2020 and beyond, has become a focal point for academic and industrial research [3-4]. The key principle behind NOMA is to take advantage of the differences in channel conditions and transmit the signals with different power levels among various user equipments (UEs). In the downlink, by incorporating superposition coding (SC) at the transmitter and successive interference cancellation (SIC) at the receiver serving multiple users simultaneously over an entire transmission period and bandwidth. Each user then obtains its own message by employing SIC to decode and remove the interference of signals with greater power than its own [5-7]. On the contrary, non-overlapping time or frequency slot is allocated to each user in orthogonal multiple access (OMA) for rejecting interference. Hence achievable data rates are restricted by time/ bandwidth in OMA scheme compared to NOMA. It is proven that NOMA outperforms OMA in terms of achieving higher data rates. In addition, NOMA is able to support more users than conventional OMA techniques using the same wireless resources and to reduce the transmission latency and signaling overhead [8-10]. The purpose of this work is to demonstrate that multiuser MIMO NOMA system has the robust performance to retrieve the transmitted text messages securely by deploying Hybrid Chaotic Maps based cryptography, ML decoding based Group detection (GD) approach aided Zero Forcing (ZF) signal detection, Polar channel coding, and low order QAM digital modulation schemes.

II. Previous Works on NOMA

In [11], authors addressed the first challenge and provided system-level performance comparisons between NOMA and OFDMA based cellular downlink transmissions with the consideration of single-antenna transmitter and receivers, and [12] extended performance comparison to MIMO technology with random beamforming and it is shown that NOMA improves both the overall cell throughput and cell-edge user throughput performances over OFDMA. In [13], authors proposed a low-complexity dynamic compressive sensing (DCS) based multi-user detection (MUD) scheme for NOMA to jointly realize user activity and transmitted data detection at user equipment (UEs) with the consideration of more practical scenario that the active user sets can be changed in continuous time. A novel symbol-asynchronous downlink NOMA system is studied in [14], where authors investigated the performance of the proposed system under the implementation of whitening-and decomposing (WD) detection scheme that improve the achievable rate-regions for both rectangular pulse shape and half-sine pulse shape. The authors considered a power allocation approach to analyze the outage performance and diversity orders of two paired users according to their relative channel gains and showed that a valid power allocation strategy for NOMA always exists that outperforms OMA in terms of capacity [15]. In [16], authors proposed a

graph-based low complexity message passing receivers for MIMO-SCMA system over frequency selective channels. They introduced auxiliary variables, a stretched factor graph is constructed and a hybrid belief propagation (BP) and expectation propagation (EP) receiver, named as ‘Stretch-BP-EP’, is proposed. Simulation results proved that the performance of the proposed Conv-BP-EP receiver is superior to other methods. For the first time, authors investigated the integration of simultaneous wireless information and power transfer (SWIPT) in hybrid precoding (HP) based mmWave massive MIMO-NOMA systems to further enhance the spectrum efficiency and energy efficiency [17]. Simulation results verified that the proposed mmWave massive MIMO-NOMA systems with SWIPT can achieve higher spectrum and energy efficiency compared with mmWave massive MIMO-OMA systems. In [18], a framework of power minimization precoding design for MIMO-NOMA system with coordinated multipoint (CoMP) reception and orthogonal space-time block coding (OSTBC) is proposed and showed that the diversity can be enhanced and the transmit power is reduced with CoMP and OSTBC compared to conventional NOMA and CoMP-OMA. In [19], authors evaluated the performance of the MIMO-NOMA assisted unmanned aerial vehicles (UAVs) networks. In this article, they proposed a stochastic geometry model, a new 3D UAV framework to determine both the locations of users and the interference sources for randomly roaming NOMA users. Moreover, they derived new analytical expressions for outage probability and ergodic rate for characterizing the performance in MIMO-NOMA enhanced UAV frameworks and also showed that diversity orders and high SNR slopes were obtained from this work.

III. Signal Processing Techniques

A. ML Decoding Based GD Approach Aided ZF Signal Detection

In this section, we have introduced Group Detection (GD) approach aided efficient Zero-Forcing (ZF) signal detection scheme with integrating Maximum Likelihood (ML) decoding. In simultaneous data transmission scenario of downlink 2×2 MIMO-NOMA scheme implementation for two user case (UE₁ is a cell-center user (near user) and UE₂ is a cell-edge user (far user)), the transmitted signal $\mathbf{x}$ is given by

$$\mathbf{x} = (\mathbf{x}_1 + \mathbf{x}_2) = \sqrt{P_1} \mathbf{s}_1 e^{j\phi} + \sqrt{P_2} \mathbf{s}_2 = \sqrt{P_1} \begin{pmatrix} s_{11} \\ s_{12} \end{pmatrix} e^{j\phi} + \sqrt{P_2} \begin{pmatrix} s_{21} \\ s_{22} \end{pmatrix} \quad (1)$$

where, ϕ is the assigned phase to UE₁, P_1 and P_2 are the allocated power, and $\mathbf{s}_1$ and $\mathbf{s}_2$ are the transmitted signals with unity power for UE₁ and UE₂, (s_{11} and s_{12}) and (s_{21} and s_{22}) are the signal components of $\mathbf{s}_1$ and $\mathbf{s}_2$ transmitted in one time slot from first and second transmitting antenna respectively. With consideration of 2×2 MIMO fading channel $\mathbf{H}_1$ and $\mathbf{H}_2$ and additive white Gaussian noise (AWGN) vector $\mathbf{n}_1$ and $\mathbf{n}_2$ for UE₁ and UE₂, the received signal $\mathbf{y}_1$ for user UE₁ can be written as:

$$\mathbf{y}_1 = \mathbf{H}_1 \mathbf{x} + \mathbf{n}_1 \quad (2)$$

Equation (2) can be rewritten as:

$$\mathbf{y}_1 = [\bar{\mathbf{H}}_{11} \ \bar{\mathbf{H}}_{12}] \begin{bmatrix} \sqrt{P_1} s_{11} e^{j\phi} + \sqrt{P_2} s_{21} \\ \sqrt{P_1} s_{12} e^{j\phi} + \sqrt{P_2} s_{22} \end{bmatrix} + \begin{bmatrix} n_{11} \\ n_{12} \end{bmatrix} = [\bar{\mathbf{H}}_{11} \ \bar{\mathbf{H}}_{12}] \begin{bmatrix} \bar{s}_1 \\ \bar{s}_2 \end{bmatrix} + \begin{bmatrix} n_{11} \\ n_{12} \end{bmatrix} \quad (3)$$

where, $\bar{\mathbf{H}}_{11} \in \mathbb{C}^{2 \times 1}$ and $\bar{\mathbf{H}}_{12} \in \mathbb{C}^{2 \times 1}$ are composed of first and second columns of $\mathbf{H}_1$ respectively. Similarly, $\bar{s}_1 \in \mathbb{C}^{2 \times 1}$ and $\bar{s}_2 \in \mathbb{C}^{2 \times 1}$ are the two sub symbol vectors that are created by taking the first and second rows of $\mathbf{x}$. Defining a 1×2 sized weight matrix, $\mathbf{W}_1 = (\bar{\mathbf{H}}_{11}^H \ \bar{\mathbf{H}}_{12}^H)^{-1} \bar{\mathbf{H}}_{11}^H$, where $(\bullet)^H$ denotes Hermitian transpose operation. Multiplying both sides of Equation (3) by $\mathbf{W}_1$, we get

$$\mathbf{W}_1 \mathbf{y}_1 = \bar{s}_1 + \mathbf{W}_1 \bar{\mathbf{H}}_{12} \bar{s}_2 + \mathbf{W}_1 \begin{bmatrix} n_{11} \\ n_{12} \end{bmatrix} \quad (4)$$

or equivalently, we can write

$$\bar{s}_1 = \mathbf{W}_1 \mathbf{y}_1 - \mathbf{W}_1 \bar{\mathbf{H}}_{12} \bar{s}_2 - \mathbf{W}_1 \begin{bmatrix} n_{11} \\ n_{12} \end{bmatrix} \quad (5)$$

Substituting equation (5) into equation (3) and after some manipulation, we get

$$\mathbf{z}_2 = \tilde{\mathbf{H}}_{12} \bar{s}_2 + \mathbf{w}_2 \quad (6)$$

where, $\mathbf{z}_2 \in \mathbb{C}^{2 \times 1}$, $\tilde{\mathbf{H}}_{12} \in \mathbb{C}^{2 \times 1}$ and $\mathbf{w}_2 \in \mathbb{C}^{2 \times 1}$. The $\mathbf{z}_2$, $\tilde{\mathbf{H}}_{12}$ and $\mathbf{w}_2$ can be rewritten as

$$\mathbf{z}_2 = (\mathbf{I}_{2 \times 2} - \bar{\mathbf{H}}_{11} \mathbf{W}_1) \mathbf{y}_1 \quad (7)$$

$$\tilde{\mathbf{H}}_{12} = (\mathbf{I}_{2 \times 2} - \bar{\mathbf{H}}_{11} \mathbf{W}_1) \bar{\mathbf{H}}_{12} \quad (8)$$

$$\mathbf{w}_2 = (\mathbf{I}_{2 \times 2} - \bar{\mathbf{H}}_{11} \mathbf{W}_1) \begin{bmatrix} n_{11} \\ n_{12} \end{bmatrix} \quad (9)$$

where, $\mathbf{I}_{2 \times 2}$ is the 2×2 identity matrix, on the basis of estimated $\tilde{\mathbf{H}}_{12}$, another weight matrix $\mathbf{W}_2$ can be defined as

$$\mathbf{W}_2 = (\tilde{\mathbf{H}}_{12}^H \ \tilde{\mathbf{H}}_{12})^{-1} \tilde{\mathbf{H}}_{12}^H \quad (10)$$

The sub symbol vector $\bar{s}_2$ is estimated using $\hat{s}_2 = Q(W_2 z_2)$, where the symbol Q is indicative of quantization, the effect of $\bar{s}_2$ is cancelled out from y_1 to get $y_{11} = y_1 - \bar{H}_{12} \hat{s}_2$. The sub symbol vector $\bar{s}_1$ is estimated using $\hat{s}_1 = Q(W_1 y_{11})$. The transmitted signal vector $\mathbf{x}$ is estimated as:

$$\hat{\mathbf{x}} = \begin{bmatrix} \hat{s}_1 \\ \hat{s}_2 \end{bmatrix} = \begin{bmatrix} \sqrt{P_1} \bar{s}_{11} e^{j\Phi} + \sqrt{P_2} \bar{s}_{21} \\ \sqrt{P_1} \bar{s}_{12} e^{j\Phi} + \sqrt{P_2} \bar{s}_{22} \end{bmatrix} \quad (11)$$

In Equation (11), the power scaled signal vector components $\bar{s}_{21}$ and $\bar{s}_{22}$ are treated as interference signals for near user UE₁. Analyzing components row wise from equation (11), we can write,

$$\hat{x}_1 = \sqrt{P_1} \bar{s}_{11} e^{j\Phi} + \sqrt{P_2} \bar{s}_{21} \quad (12)$$

$$\hat{x}_2 = \sqrt{P_1} \bar{s}_{12} e^{j\Phi} + \sqrt{P_2} \bar{s}_{22} \quad (13)$$

Rescaling signal models presented in Equation (12) and (13) through multiplication with $(1/(\sqrt{P_1} e^{j\Phi}))$,

$$\hat{x}_{11} = \bar{s}_{11} + \sqrt{(P_2/P_1)} \bar{s}_{21} \quad (14)$$

$$\hat{x}_{22} = \bar{s}_{12} + \sqrt{(P_2/P_1)} \bar{s}_{22} \quad (15)$$

The power scaled signal alphabet of 4-QAM is 4. In ML decoding, with simultaneous consideration of both user's own and interference signal, the signal alphabet $\tilde{S} = \{\tilde{s}_{11,1,1}, \tilde{s}_{11,2,1}, \dots, \tilde{s}_{11,16,1}, \tilde{s}_{21,1,2}, \tilde{s}_{21,2,2}, \dots, \tilde{s}_{21,2,16}\}$ would be arranged in matrix of 16 rows $\times$ 2 columns. The signals in first column correspond to user's own signal and the signals in second column correspond to interference signal. From Equation (14), the detected user's own signal and interference signal in first receiving antenna of UE₁ are given by

$$\bar{\tilde{s}}_{11} = \arg \min |\hat{x}_{11} - \tilde{s}_{11,k,1} - \sqrt{(P_2/P_1)} \tilde{s}_{21,k,2}|, k=1,2, \dots, 16 \quad (16)$$

$$\bar{\tilde{s}}_{21} = \arg \min |\hat{x}_{11} - \tilde{s}_{11,k,1} - \sqrt{(P_2/P_1)} \tilde{s}_{21,k,2}|, k=1,2, \dots, 16 \quad (17)$$

where, $\tilde{s}_{11,k,1} \in \tilde{S}(1:16)$ and $\tilde{s}_{21,k,2} \in \tilde{S}(17:32)$

From Equation (15), the detected user's own and interference signal in 2nd receiving antenna of UE₁ are given by

$$\bar{\tilde{s}}_{12} = \arg \min |\hat{x}_{22} - \tilde{s}_{12,k,1} - \sqrt{(P_2/P_1)} \tilde{s}_{22,k,2}|, k=1,2,3, \dots, 16 \quad (18)$$

$$\bar{\tilde{s}}_{22} = \arg \min |\hat{x}_{22} - \tilde{s}_{12,k,1} - \sqrt{(P_2/P_1)} \tilde{s}_{22,k,2}|, k=1,2,3, \dots, 16 \quad (19)$$

$\tilde{\tilde{S}} = \{\tilde{\tilde{s}}_{12,1,1}, \tilde{\tilde{s}}_{12,2,1}, \dots, \tilde{\tilde{s}}_{12,16,1}, \tilde{\tilde{s}}_{22,1,2}, \tilde{\tilde{s}}_{22,2,2}, \dots, \tilde{\tilde{s}}_{22,2,16}\}$; where, $\tilde{\tilde{s}}_{12,k,1} \in \tilde{\tilde{S}}(1:16)$ and $\tilde{\tilde{s}}_{22,k,2} \in \tilde{\tilde{S}}(17:32)$.

The estimated data for user UE₁ ($\bar{\tilde{s}}_{11}$ and $\bar{\tilde{s}}_{12}$) are further processed through multiplication with a normalization factor ($=\sqrt{2}$) to produce digitally modulated complex symbols. In case of second user's data detection, the received signal y_2 for UE₂ can be written as:

$y_2 = \mathbf{H}_2 \mathbf{x} + \mathbf{n}_2 \dots (20)$; Equation (20) can be rewritten as:

$$y_2 = \bar{H}_{21} \bar{s}_1 + \bar{H}_{22} \bar{s}_2 + \begin{bmatrix} n_{21} \\ n_{22} \end{bmatrix} \quad (21)$$

where, $\bar{H}_{21} \in \mathbb{C}^{2 \times 1}$ and $\bar{H}_{22} \in \mathbb{C}^{2 \times 1}$ are composed of first and second columns of $\mathbf{H}_2$ respectively. Defining a 1×2 sized weight matrix, $\mathbf{W}_3 = (\bar{H}_{21}^H \bar{H}_{21})^{-1} \bar{H}_{21}^H$, where $(\bullet)^H$ denotes Hermitian transpose operation. Multiplying both sides of Equation (20) by $\mathbf{W}_3$, we get

$$\mathbf{W}_3 y_2 = \bar{s}_1 + \mathbf{W}_3 \bar{H}_{22} \bar{s}_2 + \mathbf{W}_3 \begin{bmatrix} n_{21} \\ n_{22} \end{bmatrix} \quad (22)$$

or equivalently, we can write

$$\bar{s}_1 = \mathbf{W}_3 y_2 - \mathbf{W}_3 \bar{H}_{22} \bar{s}_2 - \mathbf{W}_3 \begin{bmatrix} n_{21} \\ n_{22} \end{bmatrix} \quad (23)$$

Substituting equation (23) into equation (21) and after some small manipulation, we get

$y_2 = \tilde{H}_{22} \bar{s}_2 + n_2 \dots (24)$; where, $y_2 \in \mathbb{C}^{2 \times 1}$, $\tilde{H}_{22} \in \mathbb{C}^{2 \times 1}$ and $n_2 \in \mathbb{C}^{2 \times 1}$. The y_2 , $\tilde{H}_{22}$ and n_2 can be rewritten as

$$y_2 = (\mathbf{I}_{2 \times 2} - \bar{H}_{21} \mathbf{W}_3) y_2 \quad (25)$$

$$\tilde{H}_{22} = (\mathbf{I}_{2 \times 2} - \bar{H}_{21} \mathbf{W}_3) \bar{H}_{22} \quad (26)$$

$$n_2 = (\mathbf{I}_{2 \times 2} - \bar{H}_{21} \mathbf{W}_3) \begin{bmatrix} n_{21} \\ n_{22} \end{bmatrix} \quad (27)$$

where, $\mathbf{I}_{2 \times 2}$ is the 2×2 identity matrix.

On the basis of estimated $\tilde{\mathbf{H}}_{22}$, another weight matrix, $\mathbf{W}_4$ can be defined as

$$\mathbf{W}_4 = (\tilde{\mathbf{H}}_{22}^H \tilde{\mathbf{H}}_{22})^{-1} \tilde{\mathbf{H}}_{22}^H \quad (28)$$

The sub symbol vector $\tilde{\mathbf{s}}_2$ is estimated using $\hat{\mathbf{s}}_2 = \mathbf{Q}(\mathbf{W}_4 \mathbf{y}_2)$, where the symbol $\mathbf{Q}$ is indicative of quantization, the effect of $\tilde{\mathbf{s}}_2$ is cancelled out from $\mathbf{y}_2$ to get $\mathbf{y}_{22} = \mathbf{y}_2 - \tilde{\mathbf{H}}_{22} \hat{\mathbf{s}}_2$.

The sub-symbol vector $\tilde{\mathbf{s}}_1$ is estimated using $\hat{\mathbf{s}}_1 = \mathbf{Q}(\mathbf{W}_3 \mathbf{y}_{22})$. The transmitted signal vector $\mathbf{x}$ is again re-estimated for UE₂ as:

$$\hat{\mathbf{x}} = \begin{bmatrix} \hat{s}_1 \\ \hat{s}_2 \end{bmatrix} = \begin{bmatrix} \sqrt{P_1} \tilde{s}_{11} e^{j\Phi} + \sqrt{P_2} \tilde{s}_{21} \\ \sqrt{P_1} \tilde{s}_{12} e^{j\Phi} + \sqrt{P_2} \tilde{s}_{22} \end{bmatrix} \quad (29)$$

In Equation (29), the power scaled signal vector components $\tilde{s}_{11}$ and $\tilde{s}_{12}$ are treated as interference signals for UE₂. Analyzing components row wise from equation(29), we can write,

$$\hat{x}_1 = \sqrt{P_1} \tilde{s}_{11} e^{j\Phi} + \sqrt{P_2} \tilde{s}_{21} \quad (30)$$

$$\hat{x}_2 = \sqrt{P_1} \tilde{s}_{12} e^{j\Phi} + \sqrt{P_2} \tilde{s}_{22} \quad (31)$$

Rescaling signal models presented in Equation (30) and (31) through multiplication with $(1/(\sqrt{P_1} e^{j\Phi}))$, we get

$$\hat{x}_{11} = \tilde{s}_{11} + \sqrt{(P_2/P_1)} \tilde{s}_{21} \quad (32)$$

$$\hat{x}_{22} = \tilde{s}_{12} + \sqrt{(P_2/P_1)} \tilde{s}_{22} \quad (33)$$

Using signal alphabets $\tilde{\mathbf{s}}$, $\tilde{\mathbf{s}}$ and Equation (32), the detected user's own signal and interference signal in the receiving antennas of UE₂ are given by

$$\tilde{\tilde{s}}_{11} = \arg \min |\hat{x}_{11} - \tilde{s}_{11,k,1} - \sqrt{(P_2/P_1)} \tilde{s}_{21,k,2}|, k=1,2,3,\dots,16 \quad (34)$$

$$\tilde{\tilde{s}}_{21} = \arg \min |\hat{x}_{11} - \tilde{s}_{11,k,1} - \sqrt{(P_2/P_1)} \tilde{s}_{21,k,2}|, k=1,2,3,\dots,16 \quad (35)$$

$$\tilde{\tilde{s}}_{12} = \arg \min |\hat{x}_{22} - \tilde{s}_{12,k,1} - \sqrt{(P_2/P_1)} \tilde{s}_{22,k,2}|, k=1,2,3,\dots,16 \quad (36)$$

$$\tilde{\tilde{s}}_{22} = \arg \min |\hat{x}_{22} - \tilde{s}_{12,k,1} - \sqrt{(P_2/P_1)} \tilde{s}_{22,k,2}|, k=1,2,3,\dots,16 \quad (37)$$

where, $\tilde{s}_{11,k,1} \in \tilde{\mathbf{S}}(1:16)$ and $\tilde{s}_{21,k,2} \in \tilde{\mathbf{S}}(17:32)$ are the interference and user's own signal at the 1st receiving antenna and $\tilde{s}_{12,k,1} \in \tilde{\mathbf{S}}(1:16)$ and $\tilde{s}_{22,k,2} \in \tilde{\mathbf{S}}(17:32)$ are the interference and user's own signal at the 2nd receiving antenna for UE₂ respectively. The estimated data for user UE₂ ($\tilde{\tilde{s}}_{21}$ and $\tilde{\tilde{s}}_{22}$) are further processed through multiplication with a normalization factor ($= \sqrt{2}$) to produce digitally modulated complex symbols [20-21].

B. Hybrid Chaotic Maps Based Encryption

In modern communication systems, the major goal is oriented to the security and the encryption methods are very much important to maintain integrity, authentication and privacy of information from unauthorized people. In Hybrid Chaotic Maps based Encryption technique, both Henon chaotic system and logistic chaotic maps are used. The Henon random map is described by the discrete Equations as:

$$\mathbf{X}_{n+1} = 1 - a\mathbf{X}_n^2 + \mathbf{Y}_n \quad (38a)$$

$$\mathbf{Y}_{n+1} = b\mathbf{X}_n \quad (38b)$$

where, a and b are external parameter. From Equation (38b), we can write

$$\mathbf{Y}_n = b\mathbf{X}_{n-1} \quad (38c)$$

Substituting the value of $\mathbf{Y}_n$ from Equation (38c) in Equation (38b), we get

$$\mathbf{X}_{n+1} = 1 - a\mathbf{X}_n^2 + b\mathbf{X}_{n-1} \quad (39)$$

Using Equation (39), the initial values, $\mathbf{X}(0)$, and external parameter values, a and b are set at: $\mathbf{X}(0) = 0.1$ and $\mathbf{X}(0) = 0.2$, $a = 1.4$ and $a = 1.6$, $b = 0.3$ and $b = 0.4$ for near and far user respectively. As the number of ultimately estimated 8 bit integer values from text message of each user is 448, the no. of variables presented in Equation (39) from generated Henon Chaotic map is 448. Equation (39) is applicable for $n = 1, 2, 3, 4 \dots 447$. The $\mathbf{X}(0) = 0.1$ and $\mathbf{X}(0) = 0.2$ are the values of variable for near and far user at $n=0$.

The first generated encrypted keys $\mathbf{K}_1$ are obtained from transforming Henon Chaotic maps into 8-bit integer values using the relation:

$$\mathbf{K}_1(n) = \text{mod}(\text{round}(\mathbf{X}(n) \times \lambda), 256) \quad (40)$$

where, $\lambda = 12345678$ for near user and $\lambda = 87654321$ for far user. The one-dimensional Logistic chaotic map is given by

$$X_{n+1} = r * X_n * (1 - X_n) \quad (41)$$

Where, r is the control parameters with its value is in the interval of $3.57 < r \leq 4$. The initial values $X(0) = 0.1$ and $X(0) = 0.2$, $r = 3.65$ and $r = 4.00$ are assigned for near and far user. The 2nd generated encrypted keys K_2 are obtained from transforming Logistic Chaotic maps of Equation (41) into 8-bit integer values using the relation

$$K_2(n) = \text{mod}(\text{round}(X(n) \times \gamma), 256) \quad (42)$$

where, $\gamma = 23456789$ and $\gamma = 98765432$ for near and far user, If $A(n)$ and $B(n)$ are the 448×1 sized 8 bit integer values obtained from the text messages for near and far user and executing binary bitwise XOR operation, we can write

$$A_{\text{first}}(n) = A(n) \oplus K_1(n) \quad (43)$$

$$B_{\text{first}}(n) = B(n) \oplus K_1(n) \quad (44)$$

$$A_{\text{hybrid}} = A_{\text{first}}(n) \oplus K_2(n) \quad (45)$$

$$B_{\text{hybrid}} = B_{\text{first}}(n) \oplus K_2(n) \quad (46)$$

Where, the symbol $\oplus$ is indicative bitwise XOR operation. Equation (45) and Equation (46) represent Hybrid chaotic maps based encrypted text messages for near and far user [22].

C. Polar Channel Coding

Polar codes represent an emerging class of error-correcting codes with power to approach the capacity of a discrete memory less channel. In non symmetric form of polar coding for code length $N = 2^n$, $n = 1, 2, \dots$ and information length K , the binary source block $\mathbf{u} = (u_1, u_2, \dots, u_N)$ consists of K information bits and $N - K$ frozen bits. The polar encoded codeword $\mathbf{x}$ with code rate $R = K/N$ can be obtained as follows:

$$\mathbf{x} = \mathbf{u} \mathbf{G}_N = \mathbf{F}_2^{\otimes n} \quad (47)$$

where, $\mathbf{G}_N = \mathbf{B}_N \mathbf{F}_2^{\otimes n}$ is the generation matrix, $\mathbf{B}_N$ is the bit-reversal permutation matrix, $\mathbf{F}_2^{\otimes n}$ is the n^{th} Kronecker power of $\mathbf{F}_2$ and

$$\mathbf{F}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad (48)$$

is called the kernel matrix. In the present study, a polar code with $N = 8$, $K = 4$, and $R = \frac{1}{2}$ has been used. Under the scenario of implementing such non-systematic polar coding scheme in each binary source block, the information bits $\{u_4, u_6, u_7, u_8\}$ are assigned to polarized channels with the lower error probabilities and the frozen bits $\{u_1, u_2, u_3, u_5\}$ containing typically all fixed value zeros are assigned to the remaining less reliable channels. Each polarized channel is associated with a specific row of the generation matrix. The frozen bits typically take a fixed value of zeros and are assumed known at both the encoder and decoder. The polar encoded codeword $\mathbf{x}$ in binary bit form (0/1) is obtained through modulo 2 operation of $\mathbf{x}$ presented in Equation (47) [22]. In polar decoding, the received polar encoded codeword $\tilde{\mathbf{x}}$ in binary format (0/1) is BPSK modulated producing (0/1) into $(+1, -1)$ viz. $\tilde{\mathbf{x}} \in \{+1, -1\}$. It is passed through AWGN channel and noise contaminated with a random noise variable $\tilde{\mathbf{n}}$ having zero mean and variance σ^2 . The AWGN channel's output can be represented as:

$$\tilde{\mathbf{y}} = \tilde{\mathbf{x}} + \tilde{\mathbf{n}} \quad (49)$$

The transition probability for AWGN channel is given by

$$P(\tilde{\mathbf{y}}|\tilde{\mathbf{x}}) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(\tilde{\mathbf{y}} - \tilde{\mathbf{x}})^2}{2\sigma^2}\right) \quad (50)$$

The received AWGN channel LLR is calculated using the following relation [23]:

$$L(\tilde{\mathbf{y}}) = \log\left(\exp\left(\frac{-(\tilde{\mathbf{y}} - 1)^2}{2\sigma^2}\right) + \frac{-(\tilde{\mathbf{y}} + 1)^2}{2\sigma^2}\right) = \frac{2\tilde{\mathbf{y}}}{\sigma^2} \quad (51)$$

The 1×8 matrix sized noisy channel LLR, $L(\tilde{\mathbf{y}}) = \{\tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2, \tilde{\mathbf{y}}_3, \tilde{\mathbf{y}}_4, \tilde{\mathbf{y}}_5, \tilde{\mathbf{y}}_6, \tilde{\mathbf{y}}_7, \tilde{\mathbf{y}}_8\}$ undergoes bit-reversed operation forming a new modified noisy channel LLR, $L(\tilde{\tilde{\mathbf{y}}}) = \{\tilde{\tilde{\mathbf{y}}}_1, \tilde{\tilde{\mathbf{y}}}_5, \tilde{\tilde{\mathbf{y}}}_3, \tilde{\tilde{\mathbf{y}}}_7, \tilde{\tilde{\mathbf{y}}}_2, \tilde{\tilde{\mathbf{y}}}_6, \tilde{\tilde{\mathbf{y}}}_4, \tilde{\tilde{\mathbf{y}}}_8\}$. The signal vectors $L(\tilde{\tilde{\mathbf{y}}})$ and $\tilde{\tilde{\mathbf{y}}}$ are used in a subroutine available at [24-25] to estimate the retrieved information bits at the non-frozen indexed positions $\{\tilde{\tilde{u}}_4, \tilde{\tilde{u}}_6, \tilde{\tilde{u}}_7, \tilde{\tilde{u}}_8\}$.

IV. System Model

The simulated 2-user 2×2 spatially multiplexed downlink NOMA wireless communication system is graphically represented in Figure 1. The system utilizes Hybrid Chaotic Maps based encryption, ML decoding based Group detection (GD) approach aided Zero Forcing (ZF) signal detection, Polar channel coding, and low order QAM digital modulation schemes where both BS and users are equipped with 2 antennas. In this simulation work, input text messages are encrypted 3-times based on Hybrid Chaotic Maps encryption scheme. The triple encrypted data are converted into binary bits and channel encoded using Polar channel coding technique and also interleaved to

reduce the burst errors. Then the interleaved bits are digitally modulated using 4-order Quadrature Amplitude Modulation (QAM). The digitally modulated complex symbols are fed into spatial multiplexing encoder section for production of two independent data series for two users to be transmitted simultaneously from each of the two antennas after proper power allocation and phase introduction. Phase is assigned to symbols of user #1 only to make phase difference between the symbols of user #1 and user #2. In receiving section, all the transmitted signals are detected with Group Detection (GD) approach aided Zero Forcing (ZF) signal detection scheme under the implementation of ML decoding and the detected signals are subsequently sent up to spatial multiplexing decoder. The multiplexed symbols are digitally demodulated, deinterleaved, channel decoded and 3-times decrypted to recover the transmitted text messages for each user.

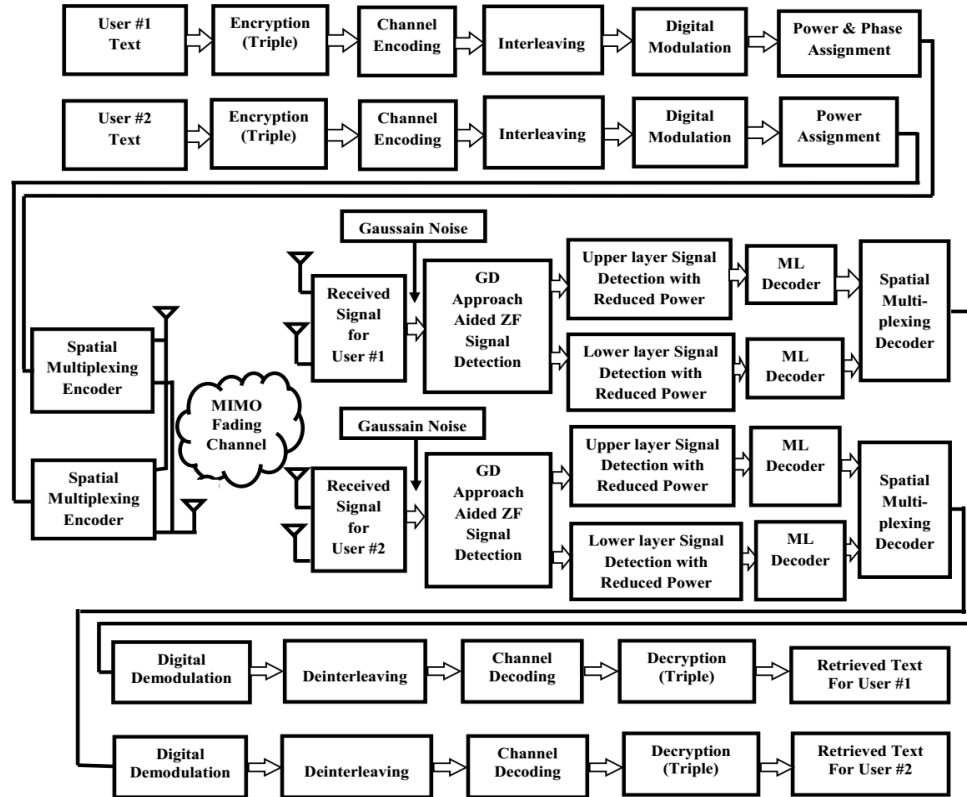


Figure1: Block diagram of 2-user 2 x 2 downlink NOMA wireless communication system.

V. Results and Discussion

In this section, we have tried to present a series of simulation results using MATLAB to illustrate the significant impact of power level assigned to user #1 and user #2 and phase difference between two users on MIMO NOMA wireless communication system performance in terms of bit error rate (BER) under implementation of polar channel coding and QAM digital modulation scheme. It is assumed that the channel state information (CSI) of MIMO fading channel is available at the receiver. The proposed model is simulated to evaluate the quality of the system performance with considering the following parameters presented in the Table

Table 1: Simulation Parameters

Parameters	Types
Data Type	Text Message (3584 Bits)
No. of User	2
Cryptographic Algorithm	Hybrid Chaotic Maps based Cryptography
Antenna Configuration	2x2 MIMO Channel
Channel Coding	Polar Coding
Digital Modulation	QAM
Signal Detection Scheme	ML decoding based GD approach aided ZF signal detection
SNR	0 to10 dB
Channel	AWGN and Rayleigh

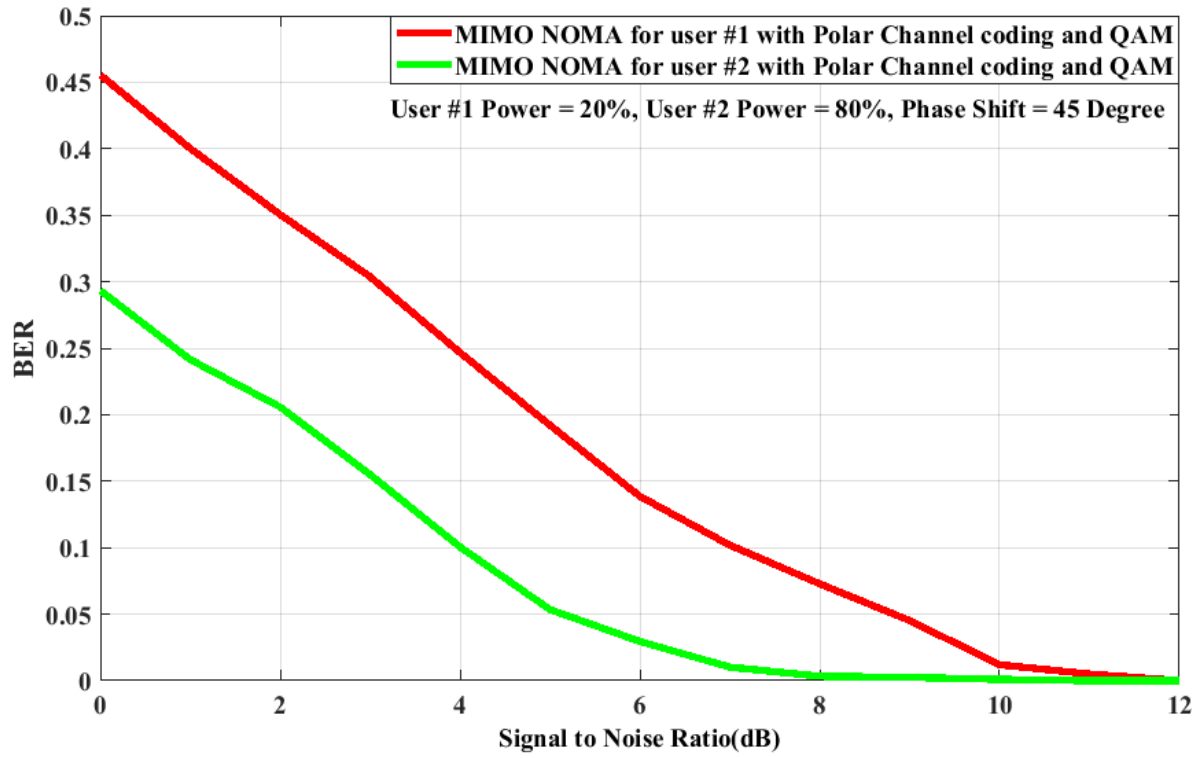


Fig. 2: BER performance of Polar channel encoded MIMO NOMA system with QAM digital modulation for text message transmission where $P_1 = 0.2P$, $P_2 = 0.8P$ and $\phi = 45^\circ$.

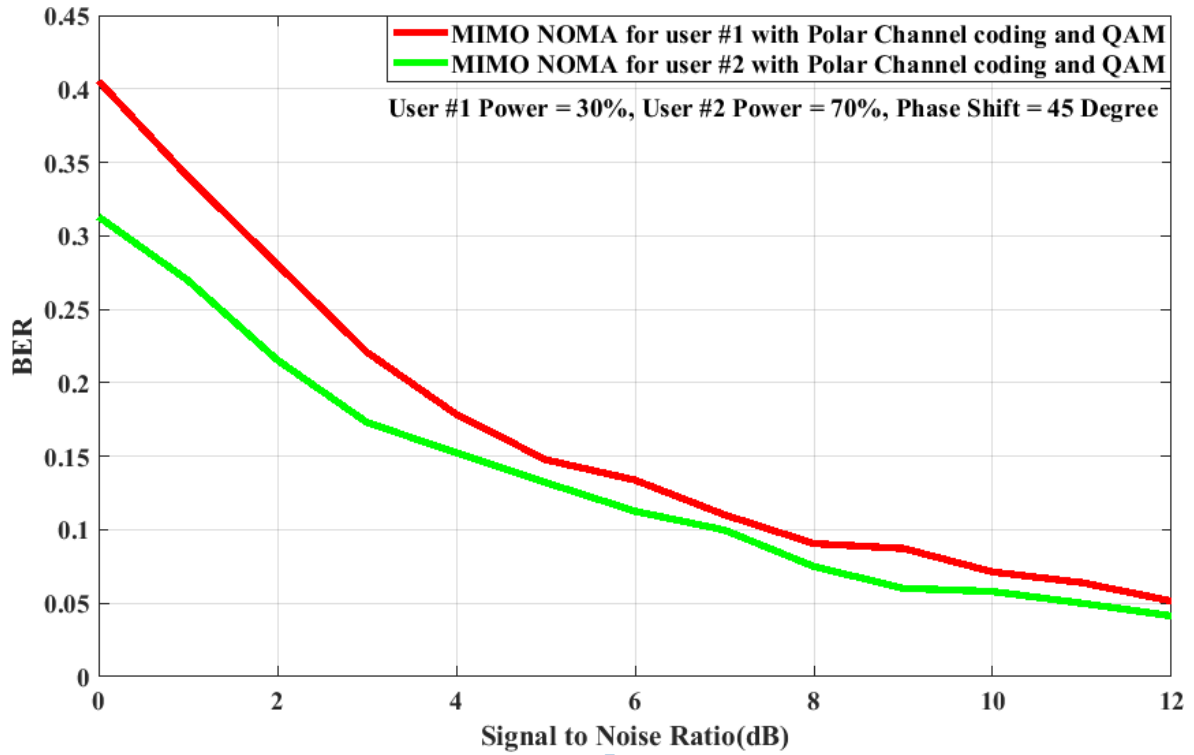


Fig. 3: BER performance of Polar channel encoded MIMO NOMA system with QAM digital modulation for text message transmission where $P_1 = 0.3P$, $P_2 = 0.7P$ and $\phi = 45^\circ$.

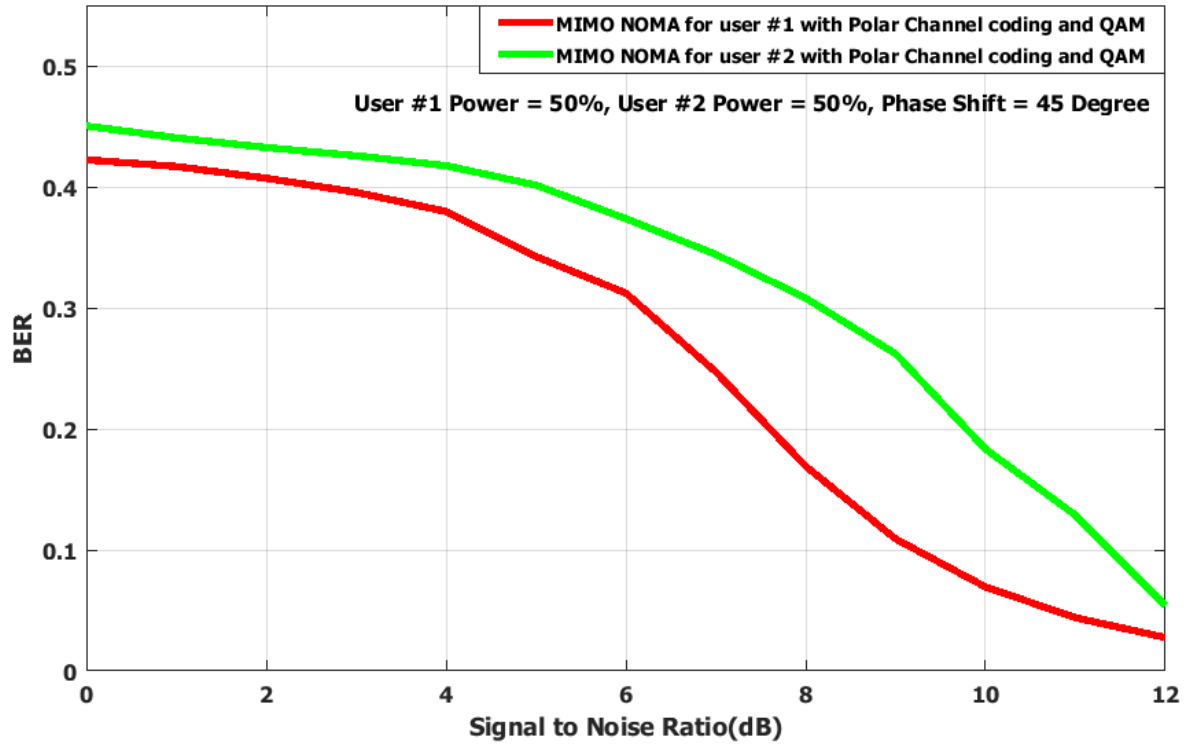


Fig. 4: BER performance of Polar channel encoded MIMO NOMA system with QAM digital modulation for text message transmission where $P_1 = 0.5P$, $P_2 = 0.5P$ and $\phi = 45^\circ$.

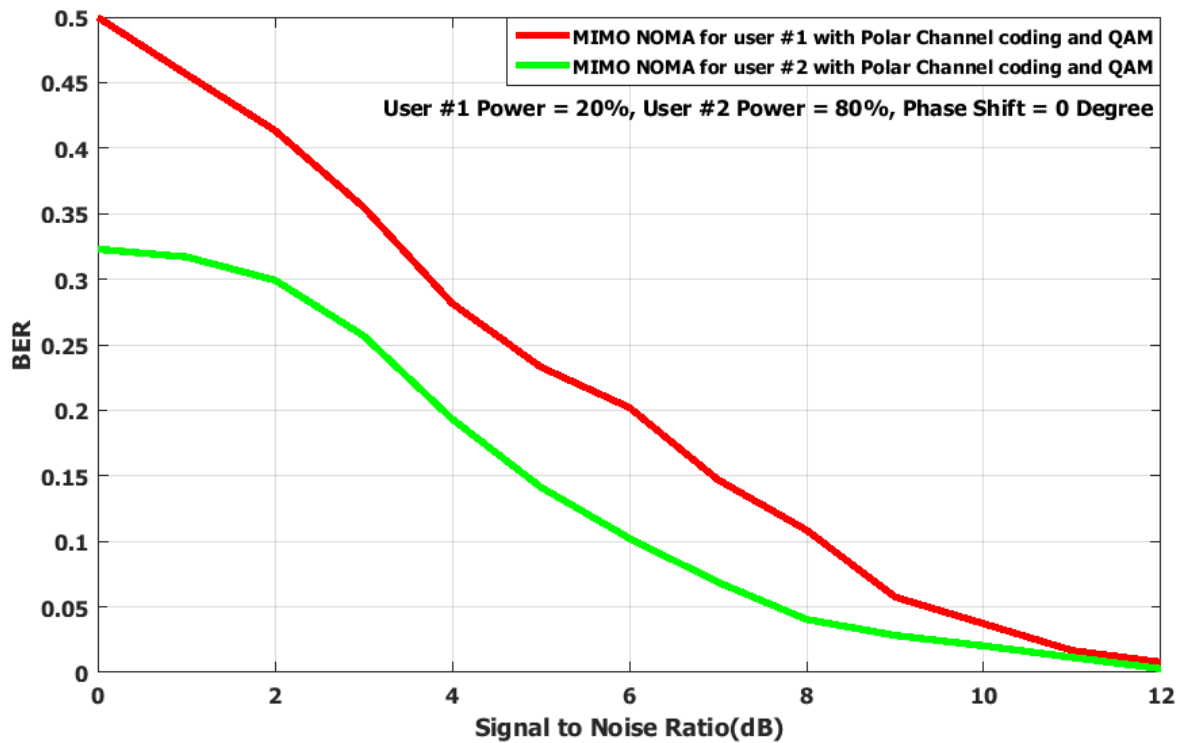


Fig. 5: BER performance of Polar channel encoded MIMO NOMA system with QAM digital modulation for text message transmission where $P_1 = 0.2P$, $P_2 = 0.8P$ and $\phi = 0^\circ$.

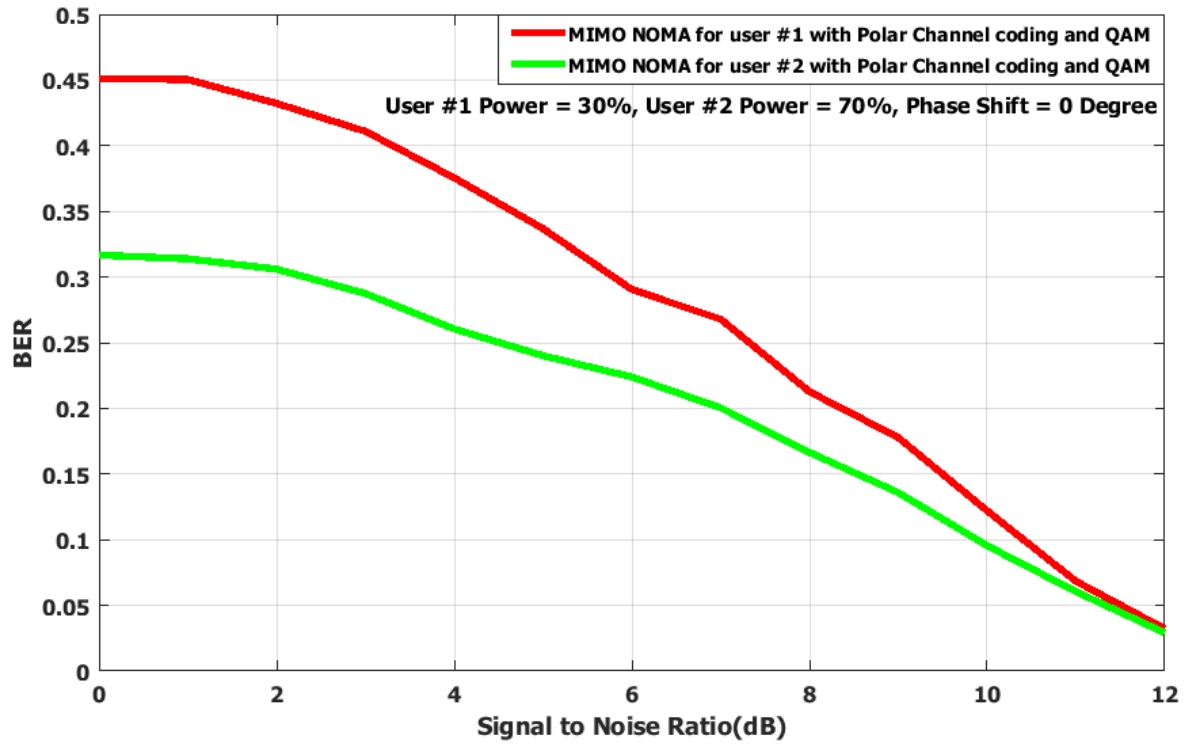


Fig. 6: BER performance of Polar channel encoded MIMO NOMA system with QAM digital modulation for text message transmission where $P_1 = 0.3P$, $P_2 = 0.7P$ and $\phi = 0^\circ$.

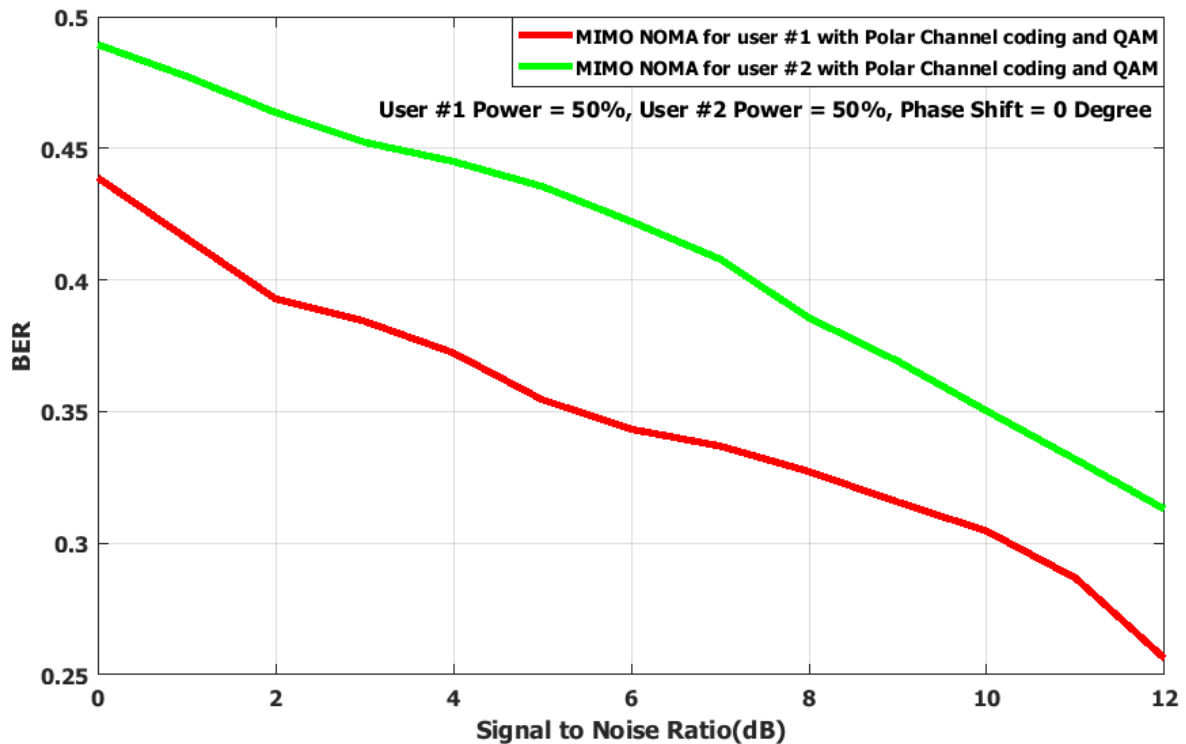


Fig. 7: BER performance of Polar channel encoded MIMO NOMA system with QAM digital modulation for text message transmission where $P_1 = 0.5P$, $P_2 = 0.5P$ and $\phi = 0^\circ$.

A series of simulation results in terms of BER values with respect to SNR values through figure 2 to figure 7 represents the estimated performance of proposed wireless communication system. The estimated results establish that the proposed 5G compatible multiuser MIMO NOMA system under the implementation of Hybrid Chaotic Maps based cryptography, ML decoding based GD approach aided ZF signal detection, Polar channel coding and

QAM digital modulation schemes provide the best performance when the near user (user #1) is allocated 20% power and far user (user #2) is allocated 80% power with 45 degrees phase difference between the users shown in figure 2. On the contrary, the system exhibit worst performance when equal power (50% power for each user) is distributed for both users with no phase difference represented in figure 7. Finally, figure 8 reveals the transmitted and retrieved text for both two users. Figure 8 indicates that the proposed system is very much robust and effective for retrieving transmitted text with 20% power allocation for near user, 80% power allocation for far user and 45 degrees phase difference between them.

User #1 Transmitted Text

With the rapid development of enhance mobile broadband service in the next generation mobile networks, there has been growing interest in the millimeter-Wave (mmWave) bands, between 20 and 300 GHz. The huge amount of available spectrum in mmWave bands makes them attractive for being utilized in the form of mmWave small cells, which are massively deployed in the next generation mobile heterogeneous networks (HetNets) to improve the capacity and tackle the incredible increase in wireless data traffic.

User #1 Retrieved Text at 10 dB SNR

With the **rqpid** development of enhance mobile broadband service in the next generation mobile networks, there has been growing interest in the millimeter-Wave (mmWave) bands, between 20 and 300 GHz. The huge amount of available spectrum in mmWave bands makes them attractive for being utilized in the form of mmWave small cells, which are massively deployed in the next generation mobile heterogeneous networks (HetNets) to **imrvove** the capacity and tackle the incredible increase in **wmreless** data traffic.

User #2 Transmitted Text

MIMO is one of the key technologies identified to improve the spectrum efficiency in LTE/LTE Advanced. In general, MIMO techniques can be categorized under two headings: single-user MIMO (SU-MIMO), where only one UE is served in data transmission multi-user MIMO (MU-MIMO), where more than one UE is served in data transmission. Because MIMO technology exploits the spatial domain and NOMA exploits the power domain, the two technologies can be combined to further boost the system spectrum efficiency.

User #2 Retrieved Text at 10 dB SNR

MIMO is one of the key technologies identified to improve the spectrum efficiency in LTE/LTE Advanced. In general, MIMO techniques can be categorized under two headings: single-user MIMO (SU-MIMO), where only one UE is served in data transmission multi-user MIMO (MU-MIMO), where more than one UE is served in data transmission. Because MIMO technology exploits the spatial domain and NOMA exploits the power domain, the two technologies can be combined to further boost the system spectrum efficiency.

Figure 8: Transmitted and retrieved text messages for proposed MIMO NOMA system with $P_1 = 0.2P$, $P_2 = 0.8P$ and $\phi = 45^\circ$ [bolded red marks indicate noise contamination].

VI. Conclusion

The simulation results of the proposed system confirm that power allocation and signal's phase difference among the users affect significantly on the performance of the system. It is also noticeable that that far user deserves more power allocation than near user for implementing NOMA technology. On the basis of numerical results presented in this paper, it can be concluded the proposed 5G compatible multiuser MIMO NOMA wireless communication system under the implementation of Hybrid Chaotic Maps based cryptography, ML decoding based GD approach aided ZF signal detection, Polar channel coding and QAM digital modulation techniques is undoubtedly a robust system in perspective of text transmission in hostile fading environment.

References

- [1] K. Higuchi, A. Benjebbour, "Non-orthogonal multiple access (NOMA) with successive interference cancellation for future radio access," IEICE Transactions on Communications, vol. 98, no. 3, pp. 403-414, 2015.
- [2] Z. Ding, F. Adachi, and H. V. Poor, "The application of MIMO to nonorthogonal multiple access," IEEE Trans. Wireless Commun., vol. 15, no. 1, pp. 537-552, 2016.
- [3] J. G. Andrews, S. Buzzi, C. Wan, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G Be?," IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065-1082, Jun. 2014.
- [4] 3rd Generation Partnership Project (3GPP), "Study on downlink multiuser superposition transmission for LTE," TSG RAN Meeting 67, Tech. Rep. RP-150496, March 2015.
- [5] Wei, Zhiqiang and Yuan, Jinhong and Ng, Derrick Wing Kwan and Elkashlan, Maged and Ding, Zhiguo, "A survey of downlink nonorthogonal multiple access for 5G wireless communication networks," ZTE Commun., vol. 14, no. 4, pp. 17-25, 2016.
- [6] P. D. Diamantoulakis, K. N. Pappi, Z. Ding, and G. K. Karagiannidis, "Wireless-powered communications with non-orthogonal multiple access," IEEE Trans. Wireless Commun., vol. 15, no. 12, pp. 8422-8436, Dec 2016.
- [7] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-Lin, and Z. Wang, "Nonorthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," IEEE Commun. Mag., vol. 53, no. 9, pp.74-81, 2015.

- [8] Z. Yang, Z. Ding, P. Fan, N. Al-Dhahir, "A General Power Allocation Scheme to Guarantee Quality of Service in Downlink and Uplink NOMA Systems," *Wireless Communications, IEEE Transactions on*, Vol 15, No 11, November 2016.
- [9] Z. Ding, L. Dai, and H. V. Poor, "MIMO-NOMA design for small packet transmission in the Internet of Things," *IEEE Access*, vol. 4, pp. 1393–1405, Apr. 2016.
- [10] J. A. Oviedo, H. R. Sadjadpour, "A Fair Power Allocation Approach to NOMA in Multi-user SISO Systems," *Vehicular Technology, IEEE Transactions on*, Vol 66, Issue 9, September 2017.
- [11] G. Wunder, *et al.*, "5G NOW: non-orthogonal, asynchronous waveforms for future mobile applications," *IEEE Communications Magazine*, vol. 52, pp. 97–105, February 2014.
- [12] K. Higuchi and Y. Kishiyama, "Non-Orthogonal Access with Random Beamforming and Intra-Beam SIC for Cellular MIMO Downlink," *IEEE 78th Vehicular Technology Conference (VTC Fall)*, pp. 1–5, Sept 2013.
- [13] Bichai Wang, Linglong Dai, Yuan Zhang, Talha Mir, and Jianjun Li, "Dynamic Compressive Sensing Based Multi-User Detection for Uplink Grant-Free NOMA," *IEEE Communications Letters*, DOI 10.1109/LCOMM.2016.2602264, 2016.
- [14] Jianxiong Cui, Guangliang Dong, Shengli Zhang, Haitao Li and Guinian Feng, "Asynchronous NOMA for Downlink Transmissions," *IEEE Communications Letters*, DOI 10.1109/LCOMM.2016.2619339, 2016.
- [15] J. A. Oviedo, H. R. Sadjadpour, "A Fair Power Allocation Approach to NOMA in Multi-user SISO Systems," *Vehicular Technology, IEEE Transactions on*, Vol 66, Issue 9, 2017.
- [16] Weijie Yuan, Nan Wu, Qinghua Guo, Yonghui Li, Chengwen Xing and Jingming Kuang, "Iterative Receivers for Downlink MIMO-SCMA: Message Passing and Distributed Cooperative Detection," *IEEE Transactions on Wireless Communications*, DOI 10.1109/TWC.2018.2813378, 2018.
- [17] Linglong Dai, Bichai Wang, Mugen Peng, and Shanzhi Chen, "Hybrid Precoding-Based Millimeter-Wave Massive MIMO-NOMA with Simultaneous Wireless Information and Power Transfer," *IEEE Journal on Selected Areas in Communications*, DOI 10.1109/JSAC.2018.2872364, 2018.
- [18] Hong Wang, Shu-Hung Leung, and Rongfang Song, "Precoding Design for Two-Cell MIMO-NOMA Uplink With CoMP Reception," *IEEE Communications Letters*, DOI 10.1109/LCOMM.2018.2874027, 2018.
- [19] Tianwei Hou, Yuanwei Liu, Zhengyu Song, Xin Sun, and Yue Chen, "Multiple Antenna Aided NOMA in UAV Networks: A Stochastic Geometry Approach," *IEEE Transactions on Communications*, DOI 10.1109/TCOMM.2018.2875081, 2018.
- [20] Md. Humaun kabir and Shaikh Enayet Ullah, "Performance analysis of multiuser downlink MIMO NOMA wireless communication system," *Global Journal of Computer Science and Technology: E Network, Web and Security*, vol.17, issue no 3, pp.13-24, 2017.
- [21] Thanh-Binh Nguyen, Tien-Dong Nguyen, Minh-Tuan Le, Vu-Duc Ngo, "Efficiency Zero-Forcing Detectors based on Group Detection for Massive MIMO systems," *IEEE Transactions on Communications*, 2017.
- [22] Ammar M. Raheema, Sattar B. Sadkhan, and Sinan M. Abdul Sattar, "Design and Implementation of Speech Encryption Based on Hybrid Chaotic Maps," *International Conference on Engineering Technologies and their Applications (ICETA)*, pp.112 – 117, 2018.
- [23] Kai Niu, Kai Chen, Jiaru Lin, and Q. T. Zhang, "Polar Codes: Primary Concepts and Practical Decoding Algorithms," *IEEE Communications Magazine*, vol. 52, issue 7, pp.192-203, 2018.
- [24] Navneet Kaur and Arvinder Pal Singh Kalsi, "Implementation of Polar Codes over AWGN and Binary Symmetric Channel," *Indian Journal of Science and Technology*, vol. 9(19), pp.1-4, 2018.
- [25] [Polar-Codes-Software-Matlab](https://github.com/Spartak0s/Polar-Codes-Software-Matlab/blob/master/main.m), <https://github.com/Spartak0s/Polar-Codes-Software-Matlab/blob/master/main.m>