Received 19 October 2022; revised 9 November 2022; accepted 29 November 2022. Date of publication 6 December 2022; date of current version 19 December 2022.

Digital Object Identifier 10.1109/OJCOMS.2022.3226883

Efficient Secure NOMA Schemes Based on Chaotic Physical Layer Security for Wireless Networks

ISRAA M. AL-MUSAWI [1] (Graduate Student Member, IEEE), WALID A. AL-HUSSAIBI [1] (Senior Member, IEEE), AND FALAH H. ALI [2] (Senior Member, IEEE)

[1]Department of Electrical Engineering Techniques, BETC, Southern Technical University, Basrah 42001, Iraq

[2]Communications Research Group, University of Sussex, BN19QT Brighton, U.K.

CORRESPONDING AUTHORS: I. M. AL-MUSAWI and W. A. AL-HUSSAIBI (e-mail: i.almusawi@fgs.stu.edu.iq; alhussaibi@stu.edu.iq)

ABSTRACT Non-orthogonal multiple access (NOMA) is considered by the 3GPP as a potential technology for beyond 5G wireless networks to support massive connectivity with robust reliability. However, the massive increase in connected users critically leads to data security problems owing to the high possibility of eavesdropping. In this paper, uplink secure NOMA (sNOMA) schemes based on chaotic physical layer security (PLS) are proposed to achieve two-fold secrecy of integrated channel coding and secret key approaches. Different code-domain and power-domain techniques are employed for sNOMA designs over realistic fading channel environments. Equal power allocation strategy is used for the transmitted chaotic signals in code-domain sNOMA (CD-sNOMA), whereas dynamic power control is employed in power-domain sNOMA (PD-sNOMA) and the hybrid code-power-domain sNOMA (CPD-sNOMA) approaches. The former design adopts joint maximum Likelihood (ML) signal detection while the later scenarios utilize integrated receiver designs based on successive interference cancellation (SIC) and ML techniques. For the proposed sNOMA schemes, power control algorithms are presented to optimize the system performance over constrained total received power and target error rate. Numerical results validate the effectiveness of sNOMA designs compared with the benchmark systems under the worst-case secrecy of unauthorized receiver with complete knowledge of the transmission scheme and associated channel. Valuable tradeoffs are demonstrated between the achieved error rate, connectivity, security gap, and complexity. Moreover, the utilized chaotic signals offer robust and cost-effective PLS solutions with a huge key-space to combat the most powerful brute-force eavesdropping attacks.

INDEX TERMS Chaotic signals, NOMA schemes, physical layer security, Rician channels, wireless communication networks.

NOMENCLATURE

3GPP	Third Generation Partnership Project
5G	Fifth Generation
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BER	Bit-Error-Rate
BPSK	Binary Phase-Shift Keying
BS	Base Station
CBSC	Chaos-Based Secure Communication
CCS	Chua Chaotic System
CD	Code-Domain
CDMA	Code Division Multiple Access
CPD	Code-Power-Domain
CSI	Channel State Information
CSK	Chaos Shift Keying
DCSK	Differential Chaos Shift Keying
DPC	Dynamic Power Control
EPA	Equal Power Allocation
HCS	Henon Chaotic System
ICs	Initial Conditions
IoT	Internet of Things
LCS	Lorenz Chaotic System
LDPC	Low-Density Parity-Check
LDS	Low-Density Spreading

LoS	Line-of-Sight
MIMO	Multiple-Input Multiple-Output
ML	Maximum Likelihood
mMTC	massive Machine-Type Communications
MUD	Multiuser Detection
MUSA	Multiuser Shared Access
MUST	Multiuser Superposition Transmission
NLoS	None Line-of-Sight
NOMA	Non-Orthogonal Multiple Access
OFDMA	Orthogonal Frequency Division Multiple Access
OMA	Orthogonal Multiple Access
PD	Power-Domain
PLS	Physical Layer Security
QoS	Quality of Service
S1	Scenario 1
S2	Scenario 2
SCCMA	Sparse Chaos Code Multiple Access
SCMA	Sparse Code Multiple Access
SIC	Successive Interference Cancellation
sNOMA	Secure Non-Orthogonal Multiple Access
SNR	Signal-to-Noise Ratio
sOMA	Secure Orthogonal Multiple Access
ULS	Upper Layer Security.

I. INTRODUCTION

OWING to the huge revolution in wireless technologies, the number of connected user equipments and smart devices is expected to be increased on a massive scale worldwide [1], [2]. Therefore, varied communication system designs have been investigated in the literature to fulfill the main requirements of future wireless networks such as high connectivity, ultra-reliability, affordable complexity, and robust security [3], [4], [5], [6], [7], [8]. In particular, non-orthogonal multiple access (NOMA) based on code-domain (CD)/power-domain (PD) has been considered by the 3rd Generation Partnership Project (3GPP) as a study-item from Release 14 to 16 [6], [9]. Therefore, intensive investigations have been conducted in this direction to enhance the user connectivity, spectral and energy efficiencies, channel capacity, and fairness compared with that of orthogonal multiple access (OMA) schemes of limited resources (dimensions) [10], [11], [12], [13], [14], [15]. Multiuser superposition transmission (MUST) represents one of the practical NOMA standards [2], [11]. Furthermore, NOMA is considered recently as a potential technology for beyond 5G to support massive connectivity with high spectrum efficiency, robust reliability and security, and low latency [1], [6], [7]. The later issues are vital for varied wireless applications such as mobile Internet, massive machine-type communications (mMTC), Internet of Things (IoT), and vehicular communications [16], [17], [18].

A. RELATED WORKS

In the existing power-domain NOMA (PD-NOMA), the allowed users are assigned different powers based on their channel gains [12], [15]. For instance, weak users in the uplink can utilize low transmit power to extend the lifetime of their batteries and satisfy the essential power difference condition with the strong users for efficient successive interference cancellation (SIC) at the Base Station (BS) receiver [12], [13]. In code-domain NOMA (CD-NOMA), the power difference between served users is not mandatory since the users' signals are separated through non-orthogonal spreading sequences. Multiuser shared access (MUSA), low-density spreading code division multiple access (LDS-CDMA), and sparse code multiple access (SCMA) are examples of such an approach [1], [16]. Moreover, NOMA can be integrated efficiently with multiple-input multiple-output (MIMO) and millimeter-wave schemes to enhance the performance of cellular, cognitive, cooperative, and heterogeneous networks significantly [8], [11], [12], [13], [14], [15].

On the other hand, the open broadcasting nature in wireless networks makes any eavesdropper or pseudo BS within the coverage area able to intercept the transmitted signals [8], [19]. Moreover, the increased number of connected users by NOMA (sharing the same spectrum) and associated data traffic increase may lead to additional security holes and users' information leaks [20], [21], [22]. For instance, in the downlink PD-NOMA, the strong user may take the advantage of SIC to eavesdrop on the other superimposed users' signals, which leads to critical multiuser security problems compared with the single-user case in OMA. Besides, unauthorized receivers or untrusted relays/cooperative nodes with pre-knowledge of the utilized uplink/downlink transmission scheme may intercept the information of intended users [4], [14]. Thus, security risks in NOMA are more serious than in OMA systems [19], [20], which motivate the research and industrial communities for effective and practical covert NOMA solutions [7], [11], [14], [22].

The traditional techniques used for securing wireless applications are mostly based on cryptographic methods at the upper layers. However, employing upper layer security (ULS) protocols in massive connectivity systems such as NOMA with power-limited devices becomes impractical due to the high cost, complexity and delay restrictions, and vast vulnerabilities in cryptographic key generation, distribution, and management [7], [19]. For instance, the requirements of two-way verifications and the large amount of signal processing at the BS may lead to undesired delay and high-power consumption [4], [5], [21]. Therefore, the physical layer security (PLS) emerges as an alternative low complexity and powerful confidentiality approach by exploiting the channel characteristics like fading, interference, noise, diversity, beamforming, and coding to enlarge the performance gap between the intended receiver and eavesdropper using adequate transmission systems [14], [19], [22], [23]. Besides, it can be used as a complementary method with the encryption-based approaches to enhance the communication system security significantly [4], [7].

For secure NOMA (sNOMA), different PLS techniques have been suggested based on the typical approach of

enhancing the received signal quality at the legitimate user for efficient data detection while destroying the decoding capability of the eavesdropper [11], [14]. This can be done, for instance, by employing artificial noise (AN) during signal transmission through the BS for downlink [19] or by friendly jammer/cooperative user in the uplink channel to degrade the reception quality at the eavesdropper side [23]. However, the transmission of AN will result in practical drawbacks such as undesired power consumption, additional signal processing requirements for AN cancellation at the intended user, and possible jamming effect on the other cooperative NOMA users [4], [7], [19]. The inherent inter-user interference in NOMA is also exploited instead of the AN strategy to achieve the desired PLS [20], [21], [22]. In [20], some critical parameters of the MIMO aided NOMA are used to achieve downlink security. A similar method is also utilized in [21] for the opportunistic multicast NOMA to support users with different security requirements. Moreover, PLS is considered in [22] for the uplink NOMA with a common multi-antenna receiver and randomly deployed eavesdroppers. Nevertheless, an untrusted NOMA user may try to intercept the confidential information of the other users. Besides, pseudo BS within the coverage zone or relay unit with a decode-and-forward scheme can detect the superimposed NOMA signals, leading to series multiuser information leakage [4], [7]. On the other side, the aforementioned PLS schemes have not used any secret keys, making them highly vulnerable to the typical exhaustive brute-force attacks.

As another PLS approach, channel coding has been utilized for covert communications through varied low-density parity-check (LDPC), polar, and lattice codes. These techniques can achieve strong secrecy, however, at the cost of low transmission rates, high complexity, and additional power consumption, and thus unpreferred for practical low-powered applications like IoT and mMTCs. Therefore, diverse chaos-based secure communication (CBSC) designs have been presented to provide robust and cost-effective channel coding-based PLS for varied single-user and multiuser systems [5], [24], [25], [26], [27], [28], [29], [30]. These schemes are designed by exploiting the attractive features of chaotic signals such as the sensitivity to initial conditions (ICs), broadband spectrum, immunity to jamming/interference, and simple generation [31], [32]. For such CBSC systems, the transmission of confidential data is usually buried into the utilized chaotic signals and emitted to the intended receiver. The high sensitivity to ICs has the potential to generate an ultra-huge number of chaotic signals (basis functions) with low cross-correlations [33], [34], [35], [36], [37]. Besides, the ICs and control parameters of the utilized chaotic systems offer a massive key-space (secret keys) to significantly enhance the security [28], [29]. It should be noted that secret keys in CBSCs are employed at the physical layer and controlled through the BS with simple overhead signalling in contrast to ULS keys [4], [7]. Moreover, the secret key represents one of the main complexity-based PLS strategies [4], [5]. Therefore, CBSC systems have the advantage of integrated channel coding and secret key PLS techniques which enable perfect confidentiality [24], [25], [26], [27], [28], [29], [30], [31].

In the literature, numerous CBSC schemes have been investigated for the CD/PD-NOMA by exploiting the aforementioned characteristics of chaotic signals [5], [24], [25], [26], [33], [34], [35], [36], [37], [38], [39]. In [38] and [39], non-orthogonal CDMA schemes with PLS have been designed based on chaotic spreading codes rather than the conventional pseudo-noise sequences. These schemes outperform the pseudo-noise OMA techniques in terms of capacity [38] and bit-error-rate (BER) [39]. In [24], chaotic signals with different ICs are used for CD-NOMA to realize a grant-free sparse chaos code multiple access (SCCMA) with PLS merit and extended capacity. Chaos shift keying (CSK) and differential CSK (DCSK) are also utilized for the multiuser systems in [33] and [36], respectively. However, these designs have been evaluated over the simple Gaussian channel rather than the more practical propagation environments. In [25], chaos-coding has been exploited in the uplink MIMO with PD-NOMA in some of the utilized subcarriers to improve the PLS, capacity, and connectivity, however at the cost of high decoding complexity. Chaos-based PD-MIMO-NOMA is also investigated in [5] for the downlink with improved security. Nevertheless, the well-known diversity gains of MIMO and orthogonal frequency division multiple access (OFDMA) in [5] and [25] are not isolated to assess the actual performance gains of the chaos-based PLS approach.

For the PLS evaluation, different metrics have been used based on information-theoretic measures such as secrecy capacity/rate [11], [14], [20], [22], secrecy outage probability [7], [19], [40] and secrecy throughput [4]. Although these metrics are commonly used, they are difficult to be achieved and measured in realistic scenarios like the case of employing practical (non-Gaussian) codes with finite block lengths such as the chaotic codes. Besides, they may not reflect the actual secrecy in practical communication systems with different services rather than the achievable bounds [4]. To address this problem, the BER performance has been adopted as an effective PLS measure when practical channel coding and modulation schemes are employed. For instance, the BER has also been used to find the security gap in [5], [7], [24], [25], [26], [27], [28], [30], [39], [40], [41], [42], [43], [44], hence providing reliable and secure transmission by enlarging the realized gap between BERs of the intended and illegal receivers. The BER-based security gap demonstrates a significant metric and can be used to provide a QoS-based security since it addresses the performance from a practical point of view rather than the information-theoretic approach [40], [41], [44]. Besides, it can be linked with the secrecy throughput (and hence secrecy capacity) by observing that the eavesdropper will not be able to extract the information of decoded message when the BER tends to 0.5 (i.e., perfect secrecy based on Shannon's definition) [4], [44]. Key-space based security metric is another important PLS measure that estimates the ability of an eavesdropper to

guess the secret keys through exhaustive search [4]. For this case, the longer secret keys will provide higher security levels even for powerful eavesdropper devices. Moreover, the impact of key mismatch between the transmit and receive sides on the system performance is a very important metric to be measured [27], [28], [29]. More details on the existing PLS metrics can be found in [4] and [7].

B. MOTIVATIONS AND CONTRIBUTIONS

Based on the aforementioned, the major motivations behind this research work can be summarized by the following:

1) The key merit of massive connectivity in NOMA may lead to critical multiuser security risks compared with the single-user problem in OMA [4], [14], [20]. Therefore, efficient design and analysis of sNOMA based on PLS strategies is considered one of the top priorities to meet the critical requests of beyond 5G systems with cost-effective solutions [7], [11], [19], and should receive more attention.

2) Diverse PLS techniques have been designed for sNOMA to mitigate the drawbacks of ULS protocols [5], [11], [14], [19], [20], [21], [22], [23], [24], [25], [42], [43], but there is a lack of research works on the security under the worst-case covert scenario of unauthorized receivers with complete knowledge of the transmission scheme and communication channel.

3) Channel coding-based PLS (e.g., LDPC codes) has been considered for strong secrecy communications and to overcome the demerits of AN/jamming/interference methods. Nevertheless, the benefit comes at the cost of unaffordable complexity and resource consumption. So, it is inappropriate for low-powered NOMA applications such as IoT, mMTCs, and mobile Internet [4], [7], [44]. Towards this aim, chaotic signals can be used for robust and cost-effective secrecy owing to several important characteristics as: integrated PLS approaches based on channel coding and secret key (i.e., two-fold PLS); reasonable code length with affordable decoding complexity; and simple design over NOMA schemes with massive key-space advantage based on the utilized ICs at the physical layer [5], [24], [25], [26].

4) Since chaos-based sNOMA enables two-fold secrecy [24], [25], [26], [34], it can be applied for critical wireless applications of strict confidentiality and power requirements such as mobile banking, e-payments, e-health, personal identity verifications, and military communications.

Motivated by the above observations, this work aims to design efficient PLS-based sNOMA schemes with robust reliability and affordable complexity to fulfill the critical requirements of next-generation systems. The chaotic signals are employed in the investigated designs to achieve strong PLS of unified channel coding and secret key techniques while attaining reasonable hardware and computational complexity. The later issues are fundamental to reduce the implementation cost and for power minimization towards green wireless networks [1], [2], [3], [8].

In this paper, a chaos-based sNOMA is proposed by employing CD and PD signal transmission approaches and multiuser detection (MUD) techniques at the BS receiver. The chaotic signals are generated using simple nonlinear dynamical systems at both of the link ends. To optimize the performance, different power control algorithms are presented for investigated schemes. The proposed system is designed to capture most of the NOMA benefits with powerful PLS advantage. The main contributions of this paper are highlighted as follows:

- A generalized system design of an uplink chaos-based sNOMA is presented including a complete signal model over realistic propagation environment (large-scale and small-scale fading with/without line-of-sight (LoS) component) rather than the simple Gaussian channel in [24], [33], [36], [38], [42] or the only small-scale Rayleigh fading in [22], [30], [34], [39], and [45]. Multiple users are supported by the proposed system in contrast to the two-user scenarios in [5], [19], [23], [25], and [43]. For powerful chaotic PLS with a very large key-space, CSK is used for the spreading chaotic-codes with diverse security levels.
- For the worst-case secrecy of unauthorized receiver with full knowledge of the transmission technique and communication channel, efficient sNOMA schemes are designed by exploiting the advantage of power control at the BS. In particular, CD-sNOMA, PD-sNOMA, and hybrid code-power-domain sNOMA (CPD-sNOMA) approaches are investigated to demonstrate the tradeoffs between system performance, security, and complexity. The former scheme adopts an equal power allocation strategy with the Maximum Likelihood (ML) technique for MUD, while the latter scenarios employ dynamic power control and MUD based on SIC and ML. To our best knowledge, combining different chaos-based PLS techniques and NOMA strategies as used in this paper to address the highlighted challenges is the first of its kind and required critical system design and analysis.
- A key-space analysis of proposed sNOMA schemes is presented to demonstrate the strong confidentiality against brute-force attacks from unauthorized receivers. The realized massive key-space at the physical layer is configured based on the critical characteristics of chaotic signals in addition to the key system parameters. Moreover, a BER-based security gap analysis is presented to provide feasible evaluation of the employed chaotic channel coding-based PLS. The BER performance is optimized based on the allocated users' powers through designed algorithms over constrained total received power and target error rate.
- The effectiveness of sNOMA designs is validated through analysis and intensive simulations compared with the reference systems. For realistic assessment, the actual performance is evaluated by isolating the well-known gains of OMA schemes such as OFDMA [5], [25], and MIMO [20], [21], [22]. The achieved

outcomes using different scenarios are demonstrated with a tradeoff between the target BER, connectivity, security level, and complexity.
- The major research challenges and practical issues for sNOMA technology based on chaotic signals are discussed and followed by some potential avenues to extend the state-of-the-art for future wireless networks.

C. PAPER ORGANIZATION AND NOTATIONS

The rest of this paper is organized as follows: Section II presents a brief technical background on the employment of chaotic signals in chaotic communication networks. Section III demonstrates the generalized system design of sNOMA, including the mathematical signal model, chaotic code formation methods, and key-space analysis. The proposed CD-sNOMA, PD-sNOMA, and hybrid CPD-sNOMA schemes are provided in Section IV. Numerical results and security evaluation are given in Section V. Section VI presents the practical considerations and future research directions for sNOMA technology. Finally, Section VII concludes the paper.

Notations: Bold-face uppercase and lowercase letters denote matrices and vectors, respectively. Plain lowercase letters stand for scalars. $\mathcal{C}^{m\times u}$ denotes complex $m\times u$ matrix while $\mathcal{R}^{m\times u}$ is for real $m\times u$ matrix. Superscript $[\cdot]^{\mathrm{T}}$ stands for transposition. $\|\cdot\|$ stands for the Euclidean vector norm while $|\cdot|$ denote the determinant for matrices and magnitude for vectors.

II. CHAOTIC COMMUNICATION NETWORKS

Chaotic signals are commonly used for different modulation schemes in CBSCs such as CSK and DCSK [32], [33], [34], [35], [36], [45], [46]. These signals can be generated using very simple software or hardware circuits that demonstrate nonlinear dynamics such as Chua chaotic system (CCS), Lorenz chaotic system (LCS), and Henon chaotic system (HCS) [32], [45]. The mathematical models of these systems can be solved to find the chaotic sequences using many programs tools such as MATLAB [32].

For CCS, the typical double scroll attractor can be generated using the following three-dimensional ordinary differential equations of the chaotic circuit [32], [34]:

$$\begin{aligned}\dot{x} &= \big[G(y-x)/C_1\big] - \big[g(x)/C_1\big]\\ \dot{y} &= \big[G(x-y)/C_2\big] + \big[z/C_2\big]\\ \dot{z} &= -y/L\end{aligned} \tag{1}$$

where x is the voltage (state) of capacitor $C_1 = 1/9$, y denotes the voltage across capacitor $C_2 = 1$, z is the current of inductor $L = 1/7$, $G = 0.7$ stands for the conductance, and $g(x) = m_0x+(m_1-m_0)(|x+B_p|-|x-B_p|)/2$ represents the characteristic function of utilized nonlinear resistor with chaotic parameters as $m_0 = -0.5$, $m_1 = -0.8$ and $B_p = 1$. By simulation, (1) can be solved to find the chaotic states (x, y, and z) with vast sensitivity to ICs of 10^{-16}/state.

On the other hand, LCS is described mathematically by the following ordinary differential equations [45]:

$$\begin{aligned}\dot{x} &= \sigma(y-x)\\ \dot{y} &= rx - y - xz\\ \dot{z} &= xy - bz\end{aligned} \tag{2}$$

where x, y, and z represent the states (dimensions) of LCS with chaotic circuit parameters as $\sigma = 10$, $r = 28$, and $b = 8/3$. This model can be solved to find the chaotic signals x, y, and z with sensitivity to ICs of 10^{-18}, 10^{-15}, and 10^{-18}, respectively.

For the discrete-time HCS, the following two-dimensional difference equations can be used to generate the chaotic attractor for time instance n [26]:

$$\begin{aligned}x(n+1) &= y(n) + 1 - ax^2(n)\\ y(n+1) &= bx(n)\end{aligned} \tag{3}$$

where x and y stands for the states of HCS with chaotic parameters as $a = 1.4$ and $b = 0.3$. The dynamical model (3) can be solved to find the chaotic signals (x and y) with sensitivity to ICs of 10^{-15}/state.

The employment of chaotic signals in CBSCs will result in an encrypted information message with robust privacy. At the receiving side, data detection is impossible without prior knowledge of the accurate system parameters such as the ICs, chaotic control elements, the number of chaotic states ($\mathcal{D}$), chaotic sequence length ($\mathcal{L}$), and code length (β). Therefore, potential brute-force attacks from unauthorized receivers cannot detect the transmitted signals owing to exhaustive computations (more than 2^{100}) for breaking the massive key-space of combined system parameters [27], [28], [29]. Thus, CBSCs provide an efficient chaotic PLS advantage. In this case, only allowed receivers with the accurate system parameters will be able to decode the transmitted signals correctly. Consequently, chaotic modulation techniques can take the place of the standard encryption/decryption algorithms which are used to provide ULS at the cost of increased complexity [5], [24], [25], [26], [27], [28], [29]. Besides, chaotic PLS techniques can be integrated with the encryption-based schemes (ULS) to significantly extend the overall security of future wireless networks [4].

III. SYSTEM DESIGN OF sNOMA

Consider a generalized sNOMA system of K randomly deployed single-antenna users in a single-cell cellular network. The supported users are communicating simultaneously with a single-antenna BS over wireless fading channels, as shown in Fig. 1. Synchronized chaotic signals, in a drive-response fashion [32], are adopted at the transmitters and BS for CSK, respectively. For CSK, different chaotic systems such as CCS, LCS, and HCS are used for the generation of spreading codes. Based on the adopted transmission strategy, the BS employs ML or joint ML and SIC techniques for MUD. Complete channel state information (CSI) is assumed at the receiver through the channel estimation

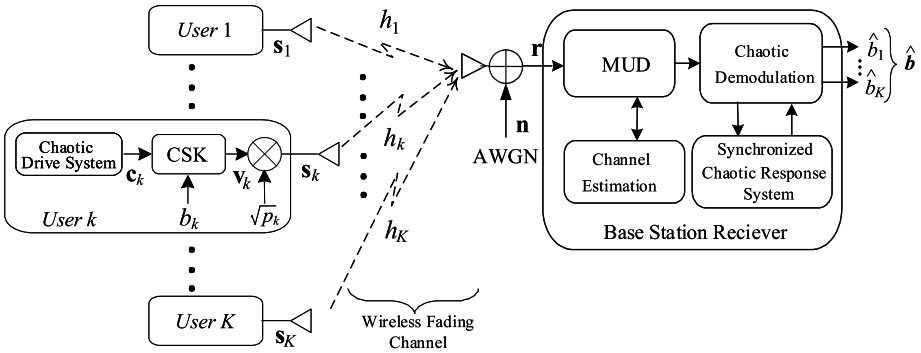

FIGURE 1. System design of sNOMA over wireless fading channel.

unit. The eavesdropper (unauthorized receiver) is assumed to be aware of the CSI and sNOMA scheme but employs incorrect secret keys due to imperfect ICs. Note that the adopted design of sNOMA in its basic form is vital to separate the well-known gains of possible integrated OMA like OFDMA [5], [25] and MIMO [20], [21], [22]. This approach has the effect of providing a realistic assessment of the actual system performance.

A. SIGNAL MODEL

At the transmit side, the digital information data of user k is mapped into binary bits $b_k \in \{+1, -1\}_{k=1}^{K}$ and modulated using CSK with a specific chaotic code $\mathbf{c}_k \in \mathcal{R}^{1\times\beta}$ of length β chips (much less than $\mathcal{L}$) as

$$\mathbf{v}_k = b_k\mathbf{c}_k = b_k\big[c_{k,1}\ \cdots\ c_{k,\beta}\big] = \big[v_{k,1}\ \cdots\ v_{k,\beta}\big] \tag{4}$$

where $c_{k,i}$ is the i^{th} chip of $\mathbf{c}_k$ assuming the bit duration T_b as β times the chip duration T_c (i.e., $T_b = \beta T_c$), $v_{k,i}$ is the i^{th} chip of modulated signal vector $\mathbf{v}_k \in \mathcal{R}^{1\times\beta}$ of user k with normalized power, and represented as

$$v_{k,i} = \begin{cases} +c_{k,i}; \text{ for bit ``1''} \\ -c_{k,i}; \text{ for bit ``}-1\text{''}. \end{cases} \tag{5}$$

Thus, the transmitted signal vector $\mathbf{s}_k \in \mathcal{R}^{1\times\beta}$ of user k with average power p_k can be written as

$$\mathbf{s}_k = \sqrt{p_k}\,\mathbf{v}_k = \big[s_{k,1}\ \cdots\ s_{k,\beta}\big]. \tag{6}$$

The received signal model of sNOMA can be written as

$$\mathbf{r} = \sum_{k=1}^{K} h_k\mathbf{s}_k + \mathbf{n} = \mathbf{h}\mathbf{S} + \mathbf{n} \tag{7}$$

where $\mathbf{r} = [r_1\ \cdots\ r_\beta] \in \mathcal{C}^{1\times\beta}$ is the received signal vector, $\mathbf{n} = [n_1\ \cdots\ n_\beta] \in \mathcal{C}^{1\times\beta}$ is i.i.d. AWGN vector of zero-mean and σ_n^2 variance elements, $\mathbf{S} = [\mathbf{s}_1, \cdots, \mathbf{s}_k]^{\mathrm{T}} \in \mathcal{R}^{K\times\beta}$ is the overall signal matrix, $\mathbf{h} = [h_1\ \cdots\ h_k] \in \mathcal{C}^{1\times K}$ is the K-user channel vector, h_k is the composite propagation channel of user k due to the large-scale path loss and small-scale fading given by the Rician model as [26]

$$h_k = \frac{1}{\sqrt{\xi_k}}\left[\sqrt{\frac{\mathcal{K}}{\mathcal{K}+1}}\bar{h}_k + \sqrt{\frac{1}{\mathcal{K}+1}}\check{h}_k\right] \tag{8}$$

where $\bar{h}_k$ is a complex-valued deterministic coefficient that accounts for the LoS component, $\check{h}_k$ denotes the scattered fading channel coefficient of zero-mean and unit-variance which assumed to be fixed over the entire bit duration T_b, $\mathcal{K}$ is the Rician factor defined as the power ratio between the LoS and scattered components, and $\xi_k = \ell_k^{\vartheta}$ is the large-scale path loss of user k which varies slowly according to the distance ℓ_k from the BS and path loss exponent ϑ.

By adopting the channel model in (8) and varying the Rician factor $\mathcal{K}$, different small-scale fading environments can be configured. For instance, a Rayleigh fading of rich scattering can be found when $\mathcal{K} = 0$. This represents a none LoS (NLoS) wireless fading channel. On the other hand, a completely deterministic channel (i.e., AWGN channel with strong LoS) can be configured when $\mathcal{K} \to \infty$.

B. CHAOTIC CODE FORMATION

For sNOMA with desired chaotic PLS and practical complexity, numerous code formation methods (i.e., $\mathbf{c}_k; k = 1, \ldots, K$ of $\beta \ll \mathcal{L}$) can be used for CSK. In particular, we consider the following techniques and demonstrate their features. The information security of these methods critically depends on the system parameters represented by $\mathcal{D}, \beta, \mathcal{L}, K$, and ICs. Note that the chaotic sequences are susceptible to ICs (for any state of utilized nonlinear dynamical system), making the task of signal prediction ultra-high complicated. For example, LCS has a sensitivity to ICs of about 10^{-18}, 10^{-15} and 10^{-18} for x, y, and z states, respectively while HCS has a sensitivity of 10^{-15} for each state. This sensitivity has a direct impact on enlarging the key-space significantly.

Case 1: All connected users employ a similar $\mathcal{D}$-state chaotic drive system with the same ICs. The users' codes are formed using the same state (e.g., the x-dimension of CCS) but from different samples of length β, i.e., different intervals. In this case, low complexity is achieved at the BS since one circuit is needed for the chaotic response system. The number of served users (K) depends mainly on the target BER (ε_T).

Case 2: All supported users utilize a similar $\mathcal{D}$-state chaotic system with the same ICs, but the users' codes are formed from different states (e.g., x, y, and z in LCS). As

in Case 1, the BS complexity is low due to the need for one chaotic system. The maximum number of supported users is limited by the number of states ($\mathcal{D}$). For instance, LCS can support up to $K = 3$ users compared with 2 users for HCS.

Case 3: Users employ the same state from a similar $\mathcal{D}$-state chaotic system, but the users' codes are formed based on different ICs. In this case, the hardware complexity at the BS is low, also due to one chaotic circuit requirement. Besides, the number of connected users is limited by the desired ε_T.

Case 4: The served users utilize different chaotic systems, and the users' codes are configured from any state (e.g., x, y, and z in CCS). The receiver complexity is relatively high due to the need for K chaotic units. Besides, the maximum number of allowed users (K) is limited by the number of chaotic response systems implemented at the BS.

C. KEY-SPACE OF CHAOTIC PLS

The immunity and robustness of the proposed sNOMA system against potential computationally-exhaustive attacks (brute-force) can be evaluated effectively based on the order of achieved key-space. The designed system has a set of important parameters that can be employed as combined secret keys $\mathcal{S} = \{K, \beta, \mathcal{L}, \mathcal{D}, \text{ICs}\}$. For instance, CCS can utilize any set of ICs $\{x_0, y_0, z_0\}$ with 10^{-16} precision/state to attain about $10^{3\times16} = 10^{48}$ key-space. The key-space of LCS and HCS are found as 10^{51} and 10^{30}, respectively. Besides, each of the K-served users may use different chaotic codes of length β from any of the $\mathcal{D}$-states which further enlarge the key-space by more than $K \times \beta \times \mathcal{L} \times \mathcal{D}$ times (e.g., $3 \times 50 \times 10^4 \times 3 = 4.5 \times 10^6$). Thus when CCS is used, the achieved key-space for chaotic PLS will be of order $\mathcal{O}(10^6 \times 10^{48} = 10^{54}) \approx \mathcal{O}(2^{179})$. This space is significantly larger than the sufficient limit of 2^{100} to resist powerful attacks, as suggested in [29]. For more convenience, the important notations for utilized variables in sNOMA schemes are listed in Table 1.

TABLE 1. Notations of utilized variables in sNOMA schemes.

Notation	Description
$\mathcal{D}$	Number of chaotic states
$\mathcal{L}$	Chaotic sequence length
β	Chaotic code length
K	Number of sNOMA users
$\mathbf{c}_k$	Chaotic code of k^{th} user with β chips
$\mathbf{v}_k$	Modulated signal vector of k^{th} user
$\mathbf{s}_k$	Transmitted signal vector of k^{th} user
h_k	Composite fading channel of k^{th} user
ξ_k	Large-scale path loss of k^{th} user
ℓ_k	Distance between the BS and k^{th} user
ϑ	Path loss exponent
$\mathcal{K}$	Rician factor
$\mathbf{r}$ and $\mathbf{n}$	Received signal and noise vectors at the BS
$\mathcal{S}$	Set of combined secret key parameters
x_0, y_0, z_0	ICs of the chaotic states x, y, and z, respectively
p_k	Transmit signal power of k^{th} user
$\mathcal{P}$	Total received power at the BS
$\mathcal{P}_{min}$	Minimum limit of $\mathcal{P}$
$\mathcal{P}_{max}$	Maximum limit of $\mathcal{P}$
$\mathcal{P}_k$	Received power from k^{th} user
α_k	Power allocation factor of k^{th} user
Ω	Number of elements in the signal matrix $\mathbb{S}$
Ψ	Number of elements in the signal matrix $\mathbb{A}$
Φ	Number of elements in the signal matrix $\mathbb{B}$
Υ	Set of sorted users based on their path losses
δ	Parameter of SIC power difference condition
M and Q	Number of users in $G_{\mathcal{A}}$ and $G_{\mathcal{B}}$, respectively
$\mathcal{P}_{G_{\mathcal{A}}}$ and $\mathcal{P}_{G_{\mathcal{B}}}$	Received powers from $G_{\mathcal{A}}$ and $G_{\mathcal{B}}$, respectively
$\alpha_{\mathcal{A}}$ and $\alpha_{\mathcal{B}}$	Power allocations of $G_{\mathcal{A}}$ and $G_{\mathcal{B}}$, respectively
ε_T	Target BER
$\triangle$	Division steps for parameters α_k
μ	Division steps for $\mathcal{P}$

IV. PROPOSED SNOMA SCHEMES

In this section, sNOMA schemes are designed for the served users by exploiting the BS's power control unit. Based on CD principles, PD principles, or both, we present CD-sNOMA, PD-sNOMA, and hybrid CPD-sNOMA designs with the adopted optimal power control algorithms and MUD techniques. These schemes can be integrated with a compatible fashion with the existing OMA methods to enhance connectivity significantly. For insightful vision, Fig. 2 illustrates the basic configurations of sNOMA over possible N-dimension OMA $\{d_n\}_{n=1}^{N}$ where up to K users $\{u_k\}_{k=1}^{K}$ can be accommodated for each orthogonal dimension, allowing a massive increase in the system connectivity up to KN users.

With the assumption that the served users are sorted in ascending order in set $\Upsilon = [1, 2, \ldots, K]$ based on their path loss conditions, $\xi_1 < \xi_2 < \cdots < \xi_K$, the power control for proposed schemes can be maintained during every symbol duration based on the users' channel gains (where u_1 is the strongest user and u_K is the weakest user). This can be achieved through the total received power condition ($\mathcal{P}$) at the BS as

$$\mathcal{P} = \sum_{k=1}^{K} \mathcal{P}_k = \sum_{k=1}^{K} \alpha_k \mathcal{P} = \sum_{k=1}^{K} p_k |h_k|^2 \tag{9}$$

where $\mathcal{P}_{min} \leq \mathcal{P} \leq \mathcal{P}_{max}$ denotes the range of $\mathcal{P}$ with the allowed minimum and maximum limits for specific network performance, $\mathcal{P}_k$ is the received power from k^{th} user, $0 < \alpha_k < 1$ is the power allocation factor for u_k with

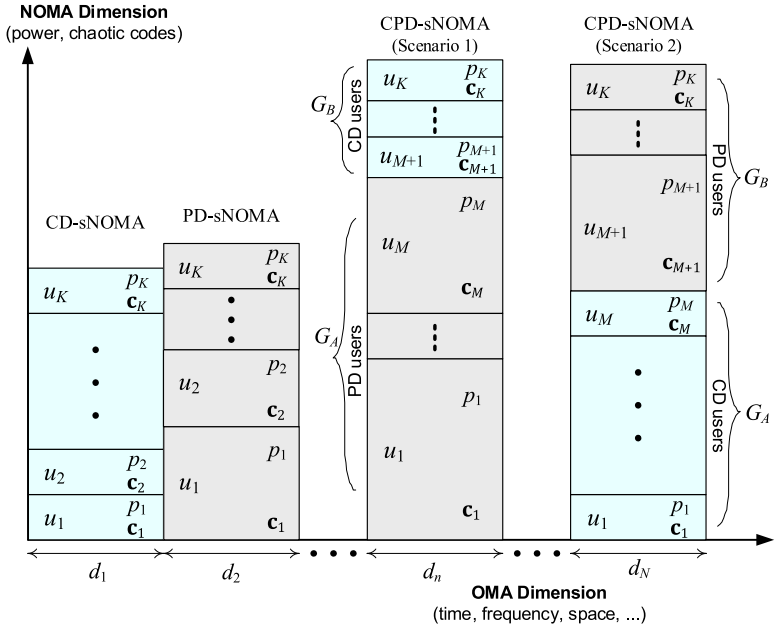

FIGURE 2. Configurations of designed *K*-user sNOMA schemes over *N*-dimensional OMA network to support up to *KN* users.

$\sum_{k=1}^{K} \alpha_k = 1$. Hence, the transmit power of u_k is given by

$$p_k = \frac{\alpha_k \mathcal{P}}{|\, h_k \,|^2}; \quad k = 1, \ldots, K. \tag{10}$$

Considering the BER-based security gap metric, the error performance of proposed sNOMA schemes with vital key-space $\mathcal{S}$ is optimized based on $\{\alpha_k\}_{k=1}^{K}$ parameters through designed power control algorithms. This can be realized by minimizing the BER of weakest user ($BER_{u_K} \leq \varepsilon_T$) to enlarge the gap with that of unauthorized device using the following optimization problem

$$\begin{aligned} &\min_{\mathcal{S};\mathcal{P};\{\alpha_k\}_{k=1}^{K}} \quad BER_{u_K}. \\ &\text{subject to} \quad (9) \text{ and } BER_{u_k} \leq \varepsilon_T, \forall k. \end{aligned} \tag{11}$$

Consequently, the adopted optimization approach will guarantee the security gap for the other users $(u_1, \ldots, u_{K-1})$ of better channel gains owing to attained $BER_{u_k} \leq \varepsilon_T$; $k = 1, \ldots, K-1$. For each channel realization, the proposed system converges to the optimal solution $\{\alpha_k^*\}_{k=1}^{K}$ over $\triangle$ division steps with the considered $\mathcal{P}$ of μ increment step size. This will be used to obtain the optimized error performance $(BER_{u_k}; \forall k)$.

A. CD-SNOMA

In this technique, the information signals of served users $(u_1, \ldots, u_K)$ in Υ are multiplexed in the CD with equal power allocation (EPA) strategy $\{\alpha_k = 1/K\}_{k=1}^{K}$. By adopting EPA, the received signals from all users over their associated channels of different gains will have equal powers $(\mathcal{P}_1 = \mathcal{P}_2 = \cdots = \mathcal{P}_K)$ as in the conventional OMA techniques [22]. This approach is important to minimize the inter-user interference with fair and uniform user performance [2], [3], [9]. At the BS receiver, MUD is carried out jointly using ML method which minimizes the error probability based on the minimum distance criterion between the received signal and all possible signal combinations over the associated channel. At the channel input, there is a set of $\Omega = 2^K$ probable arrangements for transmitted signal matrix as $\mathbb{S} = \{\mathbf{S}^{(1)}, \ldots, \mathbf{S}^{(i)}, \ldots, \mathbf{S}^{(\Omega)}\}$, where $\mathbf{S}^{(i)} = [\mathbf{s}_1^{(i)}, \ldots, \mathbf{s}_K^{(i)}]^{\mathrm{T}}$, and $\mathbf{s}_k^{(i)}$ is the i^{th} likely transmitted signal from user k. Therefore, the transmitted signals can be estimated at the receiver with complexity order of $\mathcal{O}[2^K]$ as

$$\hat{\mathbf{S}} = \left[\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_K\right]^{\mathrm{T}} = \arg \min_{\mathbf{S}^{(i)} \in \mathbb{S}} = \|\mathbf{r} - \mathbf{h}\mathbf{S}^{(i)}\|^2. \tag{12}$$

The output of estimated users' data can be found by remapping $[\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_K]^{\mathrm{T}}$ into $\hat{\mathbf{b}} = [\hat{b}_1 \ \cdots \ \hat{b}_K]^{\mathrm{T}} \in \mathcal{R}^{K \times 1}$.

The considered receiver design of CD-sNOMA is shown in Fig. 3 (a) while the pseudocode of EPA scheme is presented in Algorithm 1. The optimal power control parameters $\{\alpha_k^*\}_{k=1}^{K}$ that fulfil the optimization problem (11) will be used to find the error performance $(BER_{u_k}; \forall k)$ based on

Algorithm 1 EPA Scheme for CD-sNOMA

Input: $\mathcal{S}, \mathcal{P}_{min}, \mathcal{P}_{max}, \mu, \delta, \sigma_n^2, \varepsilon_T$, and $h_k; \forall k$.

1: Define the set of users as $\Upsilon = [1, 2, \ldots, K]$, sorted ascendingly based on $\xi_1 < \xi_2 < \cdots < \xi_K$.
2: Find: $\{\alpha_k = 1/K\}_{k=1}^{K}$.
3: Set $\mathcal{P} = \mathcal{P}_{min} - \mu$ and $BER_{u_K} = 1$.
4: **while** $BER_{u_K} > \varepsilon_T$ and $\mathcal{P} \leq \mathcal{P}_{max}$ **do**
5: Update $\mathcal{P} = \mathcal{P} + \mu$.
6: Obtain: $\{\mathcal{P}_k\}_{k=1}^{K}$ using (10) which satisfy (9).
7: Calculate: $BER_{u_k}; \forall k$ for (11) based on (12).
8: **end while**

Output: $\{\alpha_k^* = \alpha_k\}_{k=1}^{K}$ and $BER_{u_k}; \forall k$.

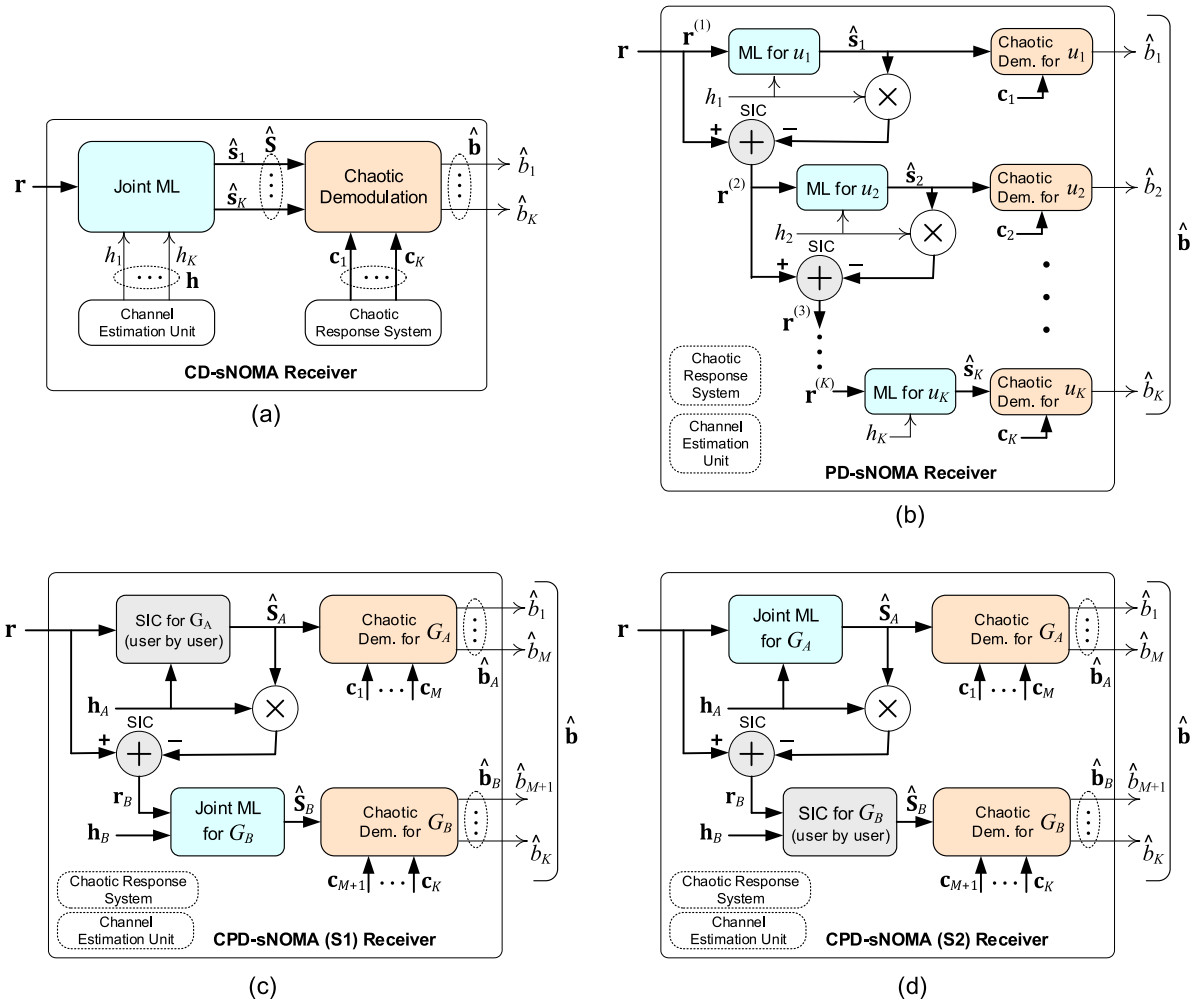

FIGURE 3. Receiver design for: (a) CD-sNOMA; (b) PD-sNOMA; (c) CPD-sNOMA (S1); and (d) CPD-sNOMA (S2).

the designed receiver and μ increment step for $\mathcal{P}$ condition. This procedure is updated when the users' channels $(h_k; \forall k)$ are changed.

B. PD-sNOMA

In this approach, the power difference between received signals from any two successive users in Υ (i.e., strong and weak users) is vital to handle the channel interference and carry out efficient MUD based on SIC [3], [12]. So, the received powers $\{\mathcal{P}_k\}_{k=1}^{K}$ are controlled through dynamic power control (DPC) strategy based on $\sum_{k=1}^{K} \alpha_k = 1$. For successful signal detection with the assumption of $\mathcal{P}_1 > \mathcal{P}_2 > \cdots > \mathcal{P}_K$ to minimize the power consumption of far users, the received powers from any two successive users must satisfy the power difference condition as [2], [3], [12]

$$\left(\mathcal{P}_k - \sum_{i=k+1}^{K} \mathcal{P}_i\right) \geq \delta \mathcal{P}_k; \quad k = 1, \ldots, K-1 \tag{13}$$

where $\delta < 1$ is a design parameter to warrant the signal estimation for target BER (ε_T). Thus, MUD can be carried out using SIC of $K-1$ stages and chaos demodulation as shown in Fig. 3 (b). The first stage of SIC is performed by estimating the signal of the strongest user $\hat{\mathbf{s}}_1$ with high reliability from the received vector $\mathbf{r}^{(1)} = \mathbf{r}$ considering the other users as background noise. This operation is performed based on the minimum Euclidean distance (ML) and given by:

$$\hat{\mathbf{s}}_1 = \arg\min_{\mathbf{s}_1 \in \mathbf{S}} \|\mathbf{r}^{(1)} - h_1 \mathbf{s}_1\|^2. \tag{14}$$

The output of the first stage is then demodulated as $\hat{b}_1$.

For the second stage, the contribution of $\hat{\mathbf{s}}_1$ will be removed from $\mathbf{r}^{(1)}$ to find the input $\mathbf{r}^{(2)} = \mathbf{r}^{(1)} - h_1 \hat{\mathbf{s}}_1$. The later is used to estimate the signal of user 2 as $\hat{\mathbf{s}}_2$ which will be demodulated to $\hat{b}_2$. Thus, the general signal estimation model for k^{th} user is given by

$$\hat{\mathbf{s}}_k = \arg\min_{\mathbf{s}_k \in \mathbf{S}} \|\mathbf{r}^{(k)} - h_k \mathbf{s}_k\|^2; k = 1, \ldots, K \tag{15}$$

where

$$\mathbf{r}^{(k)} = \begin{cases} \mathbf{r}; & \text{for } k = 1 \\ \mathbf{r}^{(k-1)} - h_{k-1} \hat{\mathbf{s}}_{k-1}; & \text{for } k = 2, \ldots, K \end{cases} \tag{16}$$

Algorithm 2 DPC Scheme for PD-sNOMA

Input: $\mathcal{S}, \mathcal{P}_{min}, \mathcal{P}_{max}\triangle, \mu, \delta, \sigma_n^2, \varepsilon_T$, and $h_k; \forall k$.

Define the set of users as $\Upsilon = [1, 2, \ldots, K]$, sorted ascendingly based on $\xi_1 < \xi_2 < \cdots < \xi_K$.
Find: $\tau = 1/2\triangle$.
Set $\mathcal{P} = \mathcal{P}_{min} - \mu$ and $BER_{u_K} = 1$.
while $BER_{u_K} > \varepsilon_T$ and $\mathcal{P} \leq \mathcal{P}_{max}$ **do**
  Update $\mathcal{P} = \mathcal{P} + \mu$.
  set $\alpha_1 = 0.5$ and $BER_{u_k}(0) = 1; \forall k$
  for $n = 1$ to $\triangle$ **do**
    Update $\alpha_1 = \alpha_1 + \tau$.
    Find: $\{\alpha_k\}_{k=2}^{K}$ based on $\sum_{k=1}^{K} \alpha_k = 1$ and (13).
    Find: $\{p_k\}_{k=1}^{K}$ using (10) which satisfy (9).
    Calculate: $BER_{u_k}(n); \forall k$ based on (14)-(16).
    if $BER_{u_K}(n) \leq BER_{u_K}(n-1)$ **then**
      Update $\{\alpha_k^* = \alpha_k(n^*)\}_{k=1}^{K}$ and $BER_{u_k} = BER_{u_k}(n^*); \forall k$.
    else
      Update $BER_{u_k} = BER_{u_k}(n-1); \forall k$.
    end if
  end for
end while

Output: $\{\alpha_k^*\}_{k=1}^{K}$ and $BER_{u_k}; \forall k$.

and the output of k^{th} stage will be demodulated as $\hat{b}_k \in \hat{\mathbf{b}} = [\hat{b}_1 \cdots \hat{b}_K]$. Note that u_K (i.e., weakest user) in the last SIC stage will enjoy interference-free since the contributions from other users are removed in the previous stages apart from possible error propagation. However, it will have the largest BER among other users owing to the smallest allocated power. The complexity of adopted receiver includes $(K-1)$ SIC stages and ML search of order $\mathcal{O}[2K]$ which is less than that of the optimal joint ML detection.

The pseudocode of DPC scheme for PD-sNOMA is shown in Algorithm 2. Over each channel realization, the optimal power parameters $\{\alpha_k^*\}_{k=1}^{K}$ that fulfil the problem (11) over $\triangle$ division steps will be used to obtain the error performance $(BER_{u_k}; \forall k)$ based on the designed receiver and $\mathcal{P}$ of μ increment step size. This procedure is updated dynamically once the users' channels $(h_k; \forall k)$ are changed.

C. HYBRID CPD-SNOMA

Based on the non-orthogonal CD and PD dimensions, different hybrid CPD-sNOMA schemes can be designed. To clarify the principles of these integrated techniques, we consider without loss of generality two groups of total K users from the set Υ. Based on the users' channel gains, the first group denoted as $G_{\mathcal{A}} = [1, 2, \ldots, M]$ includes M strongest users from Υ, i.e., $\{u_k\}_{k=1}^{M}$, while the second group $G_{\mathcal{B}} = [1, 2, \ldots, Q]$ is configured from the rest $Q = K - M$ users $\{u_k\}_{k=M+1}^{K}$. Two schemes are studied in the following scenarios by serving the allowed users in each group through CD or PD principles while PD is used for the separation between these groups and manage the inter-group interference (see Fig. 2). For the later, group power control parameters $\alpha_{\mathcal{A}}$ and $\alpha_{\mathcal{B}}$ are utilized for $G_{\mathcal{A}}$ and $G_{\mathcal{B}}$, respectively with $\alpha_{\mathcal{A}} + \alpha_{\mathcal{B}} = 1$. The signal estimation is performed at the BS receiver through integrated SIC and ML techniques as shown in Fig. 3 (c) and (d).

1) SCENARIO 1 (S1)

In this scenario, PD is used for $G_{\mathcal{A}}$ users with DPC strategy $(\alpha_{\mathcal{A}} = \sum_{k=1}^{M} \alpha_k)$ while EPA $(\alpha_{\mathcal{B}} = \sum_{k=M+1}^{K} \alpha_k)$ is employed as $\alpha_k = \alpha_{\mathcal{B}}/Q; k = M+1, \ldots, K$ for CD users in $G_{\mathcal{B}}$. The total received power condition is preserved as

$$\mathcal{P} = \underbrace{\sum_{k=1}^{M} p_k |\, h_k \,|^2}_{\mathcal{P}_{G_{\mathcal{A}}}} + \underbrace{\sum_{k=M+1}^{K} p_k |\, h_k \,|^2}_{\mathcal{P}_{G_{\mathcal{B}}}} \tag{17}$$

where $\mathcal{P}_{G_{\mathcal{A}}}$ and $\mathcal{P}_{G_{\mathcal{B}}}$ are the received powers from $G_{\mathcal{A}}$ and $G_{\mathcal{B}}$ users, respectively. To efficiently control the inter-group interference and for group SIC, the power difference between designed groups must be satisfied as

$$\left[\mathcal{P}_{G_{\mathcal{A}}} - \mathcal{P}_{G_{\mathcal{B}}}\right] \geq \delta \mathcal{P}_{G_{\mathcal{A}}}. \tag{18}$$

Assuming $\mathcal{P}_1 > \mathcal{P}_2 > \cdots > \mathcal{P}_M$ for accommodated users in $G_{\mathcal{A}}$, the received powers from any two successive users must satisfy (13) to manage the intra-group interference (with the parameter K replaced by M). In this case, the minimum user's received power from $G_{\mathcal{A}}$ should be greater than $\mathcal{P}_{G_{\mathcal{B}}}$ (i.e., $[\mathcal{P}_M - \mathcal{P}_{G_{\mathcal{B}}}] \geq \delta \mathcal{P}_M$).

According to the power control conditions, the decoding process at the receiver can take place in two steps as shown in Fig. 3 (c). In the first step, SIC is applied to estimate $G_{\mathcal{A}}$ signals $\hat{\mathbf{S}}_{\mathcal{A}} = [\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_M]^{\mathrm{T}} \in \mathcal{R}^{M \times \beta}$ using $M-1$ SIC stages based on (14)-(16) with K replaced by M and the matrix $\mathbf{S}$ is changed to $\mathbf{S}_{\mathcal{A}} = [\mathbf{s}_1, \ldots, \mathbf{s}_M]^{\mathrm{T}}$. These signals are used for the chaotic demodulator to find the estimated data of $G_{\mathcal{A}}$ users as $\hat{\mathbf{b}}_{\mathcal{A}} = [\hat{b}_1 \cdots \hat{b}_M]^{\mathrm{T}} \in \mathcal{R}^{M \times 1}$.

In the second step and to estimate $G_{\mathcal{B}}$ signals, the contribution of $\hat{\mathbf{S}}_{\mathcal{A}}$ will be subtracted from $\mathbf{r}$ using group SIC stage to find the input $\mathbf{r}_{\mathcal{B}} \in \mathcal{C}^{1 \times \beta}$ for joint ML as

$$\mathbf{r}_{\mathcal{B}} = \mathbf{r} - \mathbf{h}_{\mathcal{A}} \hat{\mathbf{S}}_{\mathcal{A}}, \tag{19}$$

where $\mathbf{h}_{\mathcal{A}} = [h_1 \cdots h_M] \in \mathcal{C}^{1 \times M}$ is the channel vector of $G_{\mathcal{A}}$ users. Note that in this case, there is a set of $\Phi = 2^{\mathcal{Q}}$ possible transmitted signal matrices to be considered at the multiple access channel input as $\mathbb{B} = \{\mathbf{S}_{\mathcal{B}}^{(1)}, \ldots, \mathbf{S}_{\mathcal{B}}^{(\Phi)}\}$, where $\mathbf{S}_{\mathcal{B}}^{(i)} = [\mathbf{s}_{M+1}^{(i)}, \ldots, \mathbf{s}_K^{(i)}]^{\mathrm{T}} \in \mathcal{R}^{\mathcal{Q} \times \beta}$, and $\mathbf{s}_k^{(i)}$ is the i^{th} probable transmitted signal from user k in $G_{\mathcal{B}}$. Therefore, the transmitted signals from $G_{\mathcal{B}}$ users can be found as:

$$\hat{\mathbf{S}}_{\mathcal{B}} = \left[\hat{\mathbf{s}}_{M+1}, \ldots, \hat{\mathbf{s}}_K\right]^{\mathrm{T}} = \arg \min_{\mathbf{S}_{\mathcal{B}}^{(i)} \in \mathbb{B}} \|\mathbf{r}_{\mathcal{B}} - \mathbf{h}_{\mathcal{B}} \mathbf{S}_{\mathcal{B}}^{(i)}\|^2, \tag{20}$$

where $\mathbf{h}_{\mathcal{B}} = [h_{M+1} \cdots h_K] \in \mathcal{C}^{1 \times \mathcal{Q}}$ is the channel vector of $G_{\mathcal{B}}$ users. The output of (20) can be used to demodulate the users' data of $G_{\mathcal{B}}$ as $\hat{\mathbf{b}}_{\mathcal{B}} = [\hat{b}_{M+1} \cdots \hat{b}_K]^{\mathrm{T}} \in \mathcal{R}^{\mathcal{Q} \times 1}$. The receiver complexity in this scenario consist of total M SIC stages and ML search efforts of order $\mathcal{O}[2M + 2^{\mathcal{Q}}]$ which is also less than the joint ML detection.

Algorithm 3 Power Control for CPD-sNOMA (S1)

Input: $\mathcal{S}, M, Q, \mathcal{P}_{min}, \mathcal{P}_{max}, \triangle, \mu, \delta, \sigma_n^2, \varepsilon_T$, and h_k; $\forall k$.

Define the set of users as $\Upsilon = [1, 2, \ldots, K]$, sorted ascendingly based on $\xi_1 < \xi_2 < \cdots < \xi_K$.
Form $G_{\mathcal{A}} = [1, \ldots, M]$ from the first M elements in Υ.
Form $G_{\mathcal{B}} = [1, \ldots, Q]$ from the last Q elements in Υ.
Find: $\tau = 1/2\triangle$.
Set $\mathcal{P} = \mathcal{P}_{min} - \mu$ and $BER_{u_K} = 1$.
while $BER_{u_K} > \varepsilon_T$ and $\mathcal{P} \leq \mathcal{P}_{max}$ **do**
  Update $\mathcal{P} = \mathcal{P} + \mu$ and set $\alpha_{\mathcal{A}} = 0.5$.
  for $i = 1$ to $\triangle$ **do**
    Update $\alpha_{\mathcal{A}} = \alpha_{\mathcal{A}} + \tau$ and $\alpha_{\mathcal{B}} = 1 - \alpha_{\mathcal{A}}$.
    Set $\alpha_1 = \alpha_{\mathcal{A}}/2$ and $BER_{u_k}(0) = 1$; $\forall k$.
    for $n = 1$ to $\triangle$ **do**
      Update $\alpha_1 = \alpha_1 + \tau$.
      Find: $\{\alpha_k\}_{k=2}^{M}$ based on $\sum_{k=1}^{K} \alpha_k = 1, \alpha_{\mathcal{A}}$, (13), and (18).
      Find: $\alpha_k = \alpha_{\mathcal{B}}/Q; k = M+1, \ldots, K$.
      Find: $\{p_k\}_{k=1}^{K}$ using (10) which satisfy (9).
      Find: $BER_{u_k}(n); k = 1, \ldots, M$ using (14)-(16).
      Find: $BER_{u_k}(n); k = M+1, \ldots, K$ using (17)-(20).
      if $BER_{u_K}(n) \leq BER_{u_K}(n-1)$ **then**
        Update $\{\alpha_k^* = \alpha_k(n^*)\}_{k=1}^{K}$ and $BER_{u_k} = BER_{u_k}(n^*)$; $\forall k$.
        Update $\alpha_{\mathcal{A}}^* = \alpha_{\mathcal{A}}$ and $\alpha_{\mathcal{B}}^* = 1 - \alpha_{\mathcal{A}}^*$
      else
        Update $BER_{u_k} = BER_{u_k}(n-1)$; $\forall k$.
      end if
    end for
  end for
end while

Output: $\alpha_{\mathcal{A}}^*, \alpha_{\mathcal{B}}^*, \{\alpha_k^*\}_{k=1}^{K}$ and BER_{u_k}; $\forall k$.

The pseudocode of power control scheme for CPD-sNOMA (S1) is shown in Algorithm 3. Over each channel realization, the optimal power parameters $\alpha_{\mathcal{A}}^*, \alpha_{\mathcal{B}}^*$, and $\{\alpha_k^*\}_{k=1}^{K}$ that fulfil (11) will be used to obtain the error rate ($BER_{u_k}; \forall k$) based on the considered receiver design and received power conditions.

2) SCENARIO 2 (S2)

The users of $G_{\mathcal{A}}$ are served in this scenario by employing CD approach with EPA ($\alpha_{\mathcal{A}} = \sum_{k=1}^{M} \alpha_k$) as $\alpha_k = \alpha_{\mathcal{A}}/M; k = 1, \ldots, M$ while the PD users in $G_{\mathcal{B}}$ are supported with DPC as $\alpha_{\mathcal{B}} = \sum_{k=M+1}^{K} \alpha_k$. As in S1, the important conditions (17) and (18) must be satisfied to realize effective inter-group interference management and group SIC.

Considering the power control conditions for configured groups, the decoding process at the receiver is carried out in two steps as shown in Fig. 3 (d). In the first step, joint ML is applied to estimate $G_{\mathcal{A}}$ signals from $\mathbf{r}$ assuming $G_{\mathcal{B}}$ signals as background noise. In this case, there is a set of $\Psi = 2^M$ possible signal matrices at the channel input as $\mathbb{A} = \{\mathbf{S}_{\mathcal{A}}^{(1)}, \ldots, \mathbf{S}_{\mathcal{A}}^{(\Psi)}\}$, where $\mathbf{S}_{\mathcal{A}}^{(i)} = [\mathbf{s}_1^{(i)}, \ldots, \mathbf{s}_M^{(i)}]^{\mathrm{T}} \in \mathcal{R}^{M \times \beta}$, and $\mathbf{s}_k^{(i)}$ is the i^{th} probable transmitted signal vector from user k in $G_{\mathcal{A}}$. Thus, the transmitted $G_{\mathcal{A}}$ signals can be estimated as

$$\hat{\mathbf{S}}_{\mathcal{A}} = \left[\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_M\right]^{\mathrm{T}} = \arg \min_{\mathbf{S}_{\mathcal{A}}^{(i)} \in \mathbb{A}} \left\|\mathbf{r} - \mathbf{h}_{\mathcal{A}} \mathbf{S}_{\mathcal{A}}^{(i)}\right\|^2 \quad (21)$$

Algorithm 4 Power Control for CPD-sNOMA (S2)

Input: $\mathcal{S}, M, Q, \mathcal{P}_{min}, \mathcal{P}_{max}, \triangle, \mu, \delta, \sigma_n^2, \varepsilon_T$, and h_k; $\forall k$.

Define the set of users as $\Upsilon = [1, 2, \ldots, K]$, sorted ascendingly based on $\xi_1 < \xi_2 < \cdots < \xi_K$.
Form $G_{\mathcal{A}} = [1, \ldots, M]$ from the first M elements in Υ.
Form $G_{\mathcal{B}} = [1, \ldots, Q]$ from the last Q elements in Υ.
Find: $\tau = 1/2\triangle$.
Set $\mathcal{P} = \mathcal{P}_{min} - \mu$ and $BER_{u_K} = 1$.
while $BER_{u_K} > \varepsilon_T$ and $\mathcal{P} \leq \mathcal{P}_{max}$ **do**
  Update $\mathcal{P} = \mathcal{P} + \mu$ and set $\alpha_{\mathcal{A}} = 0.5$.
  for $i = 1$ to $\triangle$ **do**
    Update $\alpha_{\mathcal{A}} = \alpha_{\mathcal{A}} + \tau$ and $\alpha_{\mathcal{B}} = 1 - \alpha_{\mathcal{A}}$.
    Set $\alpha_{M+1} = \alpha_{\mathcal{B}}/2$ and $BER_{u_k}(0) = 1$; $\forall k$.
    for $n = 1$ to $\triangle$ **do**
      Find: $\alpha_k = \alpha_{\mathcal{A}}/M; k = 1, \ldots, M$.
      Update $\alpha_{M+1} = \alpha_{M+1} + \tau$.
      Find: $\{\alpha_k\}_{k=M+2}^{K}$ based on $\sum_{k=1}^{K} \alpha_k = 1, \alpha_{\mathcal{B}}$, (13), and (18).
      Find: $\{p_k\}_{k=1}^{K}$ using (10) which satisfy (9).
      Find: $BER_{u_k}(n); k = 1, \ldots, M$ based on (17), (18), and (21).
      Find: $BER_{u_k}(n); k = M+1, \ldots, K$ based on (14)-(16), and (19).
      if $BER_{u_K}(n) \leq BER_{u_K}(n-1)$ **then**
        Update $\{\alpha_k^* = \alpha_k(n^*)\}_{k=1}^{K}$ and $BER_{u_k} = BER_{u_k}(n^*)$; $\forall k$.
        Update $\alpha_{\mathcal{A}}^* = \alpha_{\mathcal{A}}$ and $\alpha_{\mathcal{B}}^* = 1 - \alpha_{\mathcal{A}}^*$
      else
        Update $BER_{u_k} = BER_{u_k}(n-1)$; $\forall k$.
      end if
    end for
  end for
end while

Output: $\alpha_{\mathcal{A}}^*, \alpha_{\mathcal{B}}^*, \{\alpha_k^*\}_{k=1}^{K}$ and BER_{u_k}; $\forall k$.

where $\mathbf{h}_{\mathcal{A}} = [h_1 \cdots h_M] \in \mathcal{C}^{1 \times M}$ is the channel vector of $G_{\mathcal{A}}$ users. The output of (21) can be used to find the users' data of $G_{\mathcal{A}}$ as $\hat{\mathbf{b}}_{\mathcal{A}} = [\hat{b}_1 \cdots \hat{b}_M]^{\mathrm{T}}$.

To estimate the $G_{\mathcal{B}}$ signals in the second step, the contribution of $\hat{\mathbf{S}}_{\mathcal{A}}$ will be subtracted from $\mathbf{r}$ using group SIC to find the input signal $\mathbf{r}_{\mathcal{B}} \in \mathcal{C}^{1 \times \beta}$ as in (19). Assuming $\mathcal{P}_{M+1} > \mathcal{P}_{M+2} > \cdots > \mathcal{P}_K$ for accommodated users in $G_{\mathcal{B}}$, the received powers from any two successive users must satisfy (13) to control the intra-group interference with the user index as $k = M+1, \ldots, K-1$. Consequently, user SIC can be applied to find $\hat{\mathbf{S}}_{\mathcal{B}}$ signals using $Q-1$ stages based on (14)-(16) with the user index as $k = M+1, \ldots, K$ and the matrix $\mathbf{S}$ is changed to $\mathbf{S}_{\mathcal{B}}$. These signals are used at the demodulator to find $\hat{\mathbf{b}}_{\mathcal{B}}$. The total complexity of the designed receiver incorporates Q SIC stages and ML search of order $\mathcal{O}[2^M + 2Q]$ which is also affordable compared with the optimal joint ML technique. The pseudocode of power control strategy for CPD-sNOMA (S2) is shown in Algorithm 4. The optimal power parameters $\alpha_{\mathcal{A}}^*, \alpha_{\mathcal{B}}^*$ and $\{\alpha_k^*\}_{k=1}^{K}$ that fulfil (11) over each channel realization will be used to obtain the error rate ($BER_{u_k}; \forall k$) based on the designed receiver and received power constraints.

In Table 2, complexity comparisons between the proposed K-user sNOMA schemes are presented in terms of the power

TABLE 2. Complexity of designed K-user sNOMA schemes.

sNOMA Scheme	Power Control Requirement	Receiver Complexity	
		ML Search Efforts	SIC Stages
CD-sNOMA	EPA (K users)	$\mathcal{O}\left[2^K\right]$	N/A
PD-sNOMA	DPA (K users)	$\mathcal{O}\left[2K\right]$	$K-1$
CPD-sNOMA (S1)	DPC (M users) EPA (Q users)	$\mathcal{O}\left[2M+2^Q\right]$	M
CPD-sNOMA (S2)	EPA (M users) DPC (Q users)	$\mathcal{O}\left[2Q+2^M\right]$	Q

control requirements, the order of ML search efforts, and the number of implemented SIC stages. Note that all of the proposed schemes include the same channel estimation units and chaotic drive/response systems.

V. RESULTS AND SECURITY EVALUATIONS

In this section, numerical simulations are conducted using MATLAB to demonstrate the performance of proposed sNOMA schemes in terms of BER, the security gap between authorized and unauthorized receivers, and user connectivity. For the latter, the K-user sNOMA system represents K-fold user connectivity over the same OMA dimension. The impact of power allocation factors, code length, and key mismatch on the BER is studied. A key-space analysis is also provided to show the enhanced resistance of designed techniques against brute-force attacks from illegal receivers. The considered system parameters are: a single cellular cell of 500 m radius; $K = 3 \rightarrow 8$; 10 m $\leq \ell_k \leq$ 500 m, $\forall k$; $\vartheta = 3.8$; $\mathcal{L} = 10^4$; $\beta = 50$ (unless otherwise stated); $\mathcal{P}_{min} = 1$; $\mathcal{P}_{max} = K$; $\triangle = 10^2$; $\mu = 0.1$; $\delta = 0.5$; and $\varepsilon_T = 10^{-3}$. The chaotic codes are formed using CCS for Case 1 - Case 3 while CCS, LCS, and HCS are used for Case 4. The ICs for chaotic drive and response systems are: $\{x_0 = 0.15264, y_0 = -0.02281, z_0 = 0.38127\}$, $\{x_0 = 0.0, y_0 = 1.0, z_0 = 0.0\}$, and $\{x_0 = 0.0, y_0 = 0.0\}$ for CCS, LCS, HCS, respectively. The authorized receiver employs correct secret keys of perfect ICs while the illegal device is assumed to use incorrect keys due to imperfect ICs of about 10^{-15} accuracy. The BER outcomes are averaged over 10^6 channel realizations and compared for fairness with the reference K-user sOMA (based on OFDMA) and binary phase-shift keying NOMA (BPSK-NOMA) systems. Note that the general modulation schemes such as MPSK can be used in the proposed sNOMA designs, but require an additional number of chaotic codes/user for CSK.

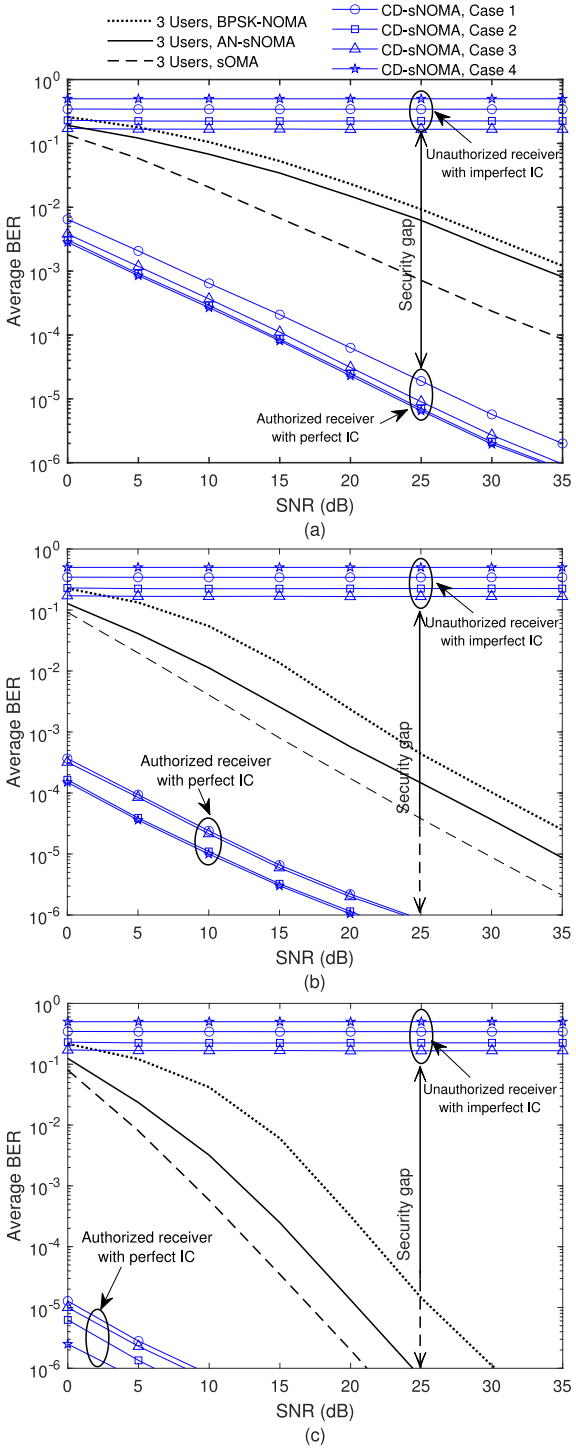

FIGURE 4. Average BER of 3-user CD-sNOMA using different Rician factors, code formations (Case 1 - Case 4), and $\beta = 50$ compared with the reference systems. (a) $\mathcal{K} = 0$; (b) $\mathcal{K} = 5$; (c) $\mathcal{K} = 10$.

A. BER PERFORMANCE AND SECURITY GAP

In Figs. 4(a)-(c), the BER results of 3-user CD-sNOMA are shown as a function of signal-to-noise ratio (SNR) using different Rician factors. Using EPA algorithm with $\alpha_1 = \alpha_2 = \alpha_3 = 1/3$, the results are compared with the reference systems and those achieved by the unauthorized receiver. It can be seen that the BER results of the authorized receiver, for all code formation scenarios (Case 1 - Case 4) and Rician factors, demonstrate uniform user performance and outperform the reference systems significantly due to CD diversity. On the other hand, the BERs of unauthorized receiver demonstrates a clear error-floor (about $0.1 \sim 0.5$)

over the entire range of SNRs owing to an ultra-tiny mismatch in ICs. The transmitted messages can be recovered correctly only when the precision of utilized ICs in the chaotic response system is less than 10^{-16}. In this case, the BERs will be similar to that achieved by the intended receiver. Consequently, a significant BER based security gap is achieved and increases remarkably as $\mathcal{K}$ increased from $\mathcal{K} = 0$ (NLoS channel) to $\mathcal{K} = 10$ ($\sim$AWGN channel). Note that Case 4 achieves robust BERs and the largest key-space compared with the other cases due to the utilized codes from three different chaotic systems with enhanced non-orthogonal sequences. This enables valuable tradeoffs between target BER, complexity, and desired PLS. For instance, it shows a SNR gain of 4 dB at BER of 10^{-3} compared with that of Case 1 (outperforms 3-user sOMA by 18.5 dB). The key-space $\mathcal{S} = \{K, \beta, \mathcal{L}, \mathcal{D}, \text{ICs}\}$ can be computed approximately as $10^6 \times 10^{48} = 10^{54}$ for Case 1 - Case 3 while Case 4 provides $10^6 \times 10^{48} \times 10^{51} \times 10^{30} = 10^{135}$ of ultra-high protection at cost of additional complexity.

Fig. 5 demonstrates the BERs of 3-user PD-sNOMA as a function of SNR using Case 1 for the spreading codes and different Rician factors. In this scenario, the optimal power parameters are found through Algorithm 2 as $\alpha_1 = 0.7$, $\alpha_2 = 0.21$, and $\alpha_3 = 0.09$. From the presented results in Figs. 5 (a)-(c), it can be seen that the authorized receiver achieves significant performance gains for the connected users compared with the reference 3-user BPSK-NOMA due to the additional code diversity. For instance, at target BER of 10^{-3} when $\mathcal{K} = 0$, user 1 (strongest user) outperforms user 2 and user 3 (weakest user) by 4.2 dB and 5.2 dB, respectively based on the highest allocated power. Though, robust BERs are realized also for users 2 and 3 through SIC diversity regardless of their small allowed powers. The average BER for $\mathcal{K} = 5$ is shown to achieve a considerable gain of about 3.3 dB compared with the reference 3-user sOMA, though it is less than that of CD-sNOMA in Fig. 4 (a). This can be seen also in terms of the achieved security gap which increases considerably as $\mathcal{K}$ increased. On the other hand, the BERs of the illegal receiver demonstrates a serious error-floor (~ 0.5) over the entire range of SNRs due to the critical mismatch in ICs. Moreover, the power parameter can be used to further enhance the combined secret key-space as $\mathcal{S} = \{K, \beta, \mathcal{L}, \mathcal{D}, \alpha, \text{ICs}\}$. For example, the continuous range of power parameters using $\Delta = 10^2$ division steps will increase the key-space of Case 1 to $10^2 \times 10^{54} = 10^{56}$.

In Figs. 6 and 7, the BERs of 3-user CPD-sNOMA (S1) and (S2) are shown as a function of SNR, respectively using different Rician factors. In these scenarios, Case 1 is used for the code formation to provide 10^{56} key-space. For S1 scenario, user grouping is performed by allocating the strongest user (user 1) in $G_{\mathcal{A}}$ while users 2 and 3 are grouped in $G_{\mathcal{B}}$. The optimized power parameters are found through Algorithm 3 as $\alpha_{\mathcal{A}} = \alpha_1 = 0.8$, $\alpha_{\mathcal{B}} = 0.2$, and $\alpha_2 = \alpha_3 = 0.1$. As can be seen from Figs. 6 (a)-(c), the authorized receiver for S1 provides the best BER for user 1, as expected, due to the largest allocated power compared

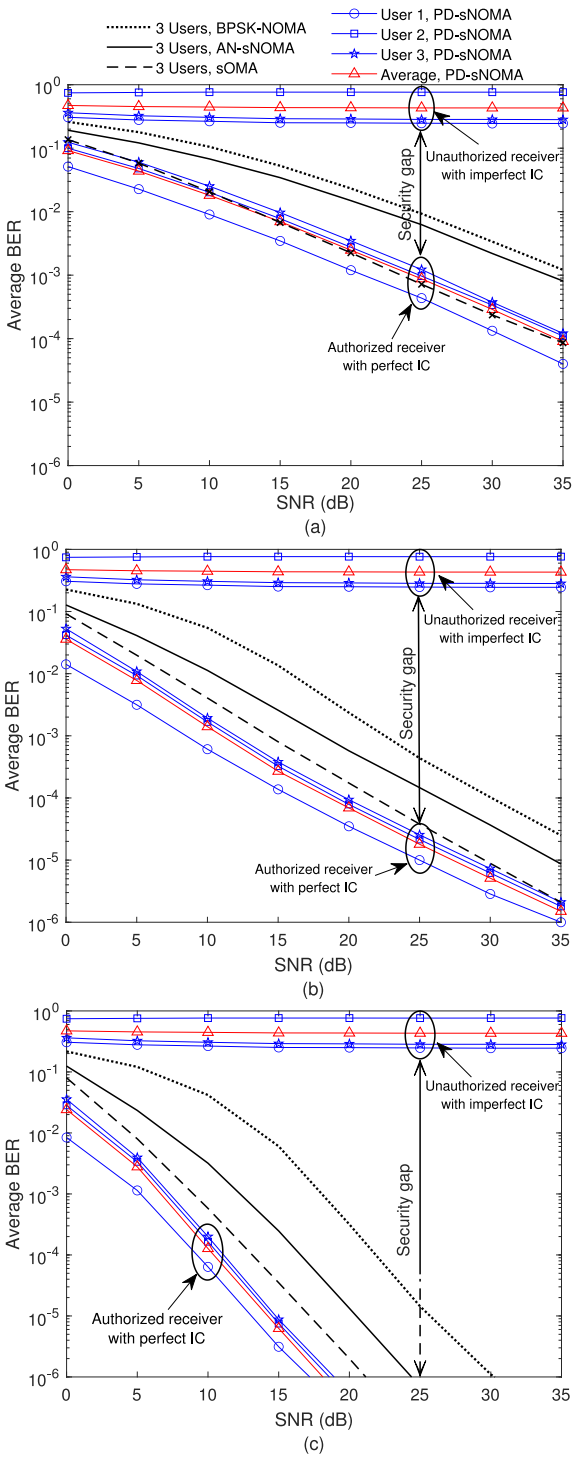

FIGURE 5. Average BER of 3-user PD-sNOMA using different Rician factors, Case 1 for the chaotic codes, and $\beta = 50$ compared with the reference systems. (a) $\mathcal{K} = 0$; (b) $\mathcal{K} = 5$; (c) $\mathcal{K} = 10$.

with the other users. At target BER of 10^{-3} when $\mathcal{K} = 5$, the SNR gain of user 1 is about 7 dB compared with the average performance of $G_{\mathcal{B}}$ users. Besides, the average BER of all served users demonstrate a significant gain of 4.6 dB compared with the reference 3-user sOMA. For S2, $G_{\mathcal{A}}$ includes users 1 and 2 of highest channel gains while $G_{\mathcal{B}}$ is

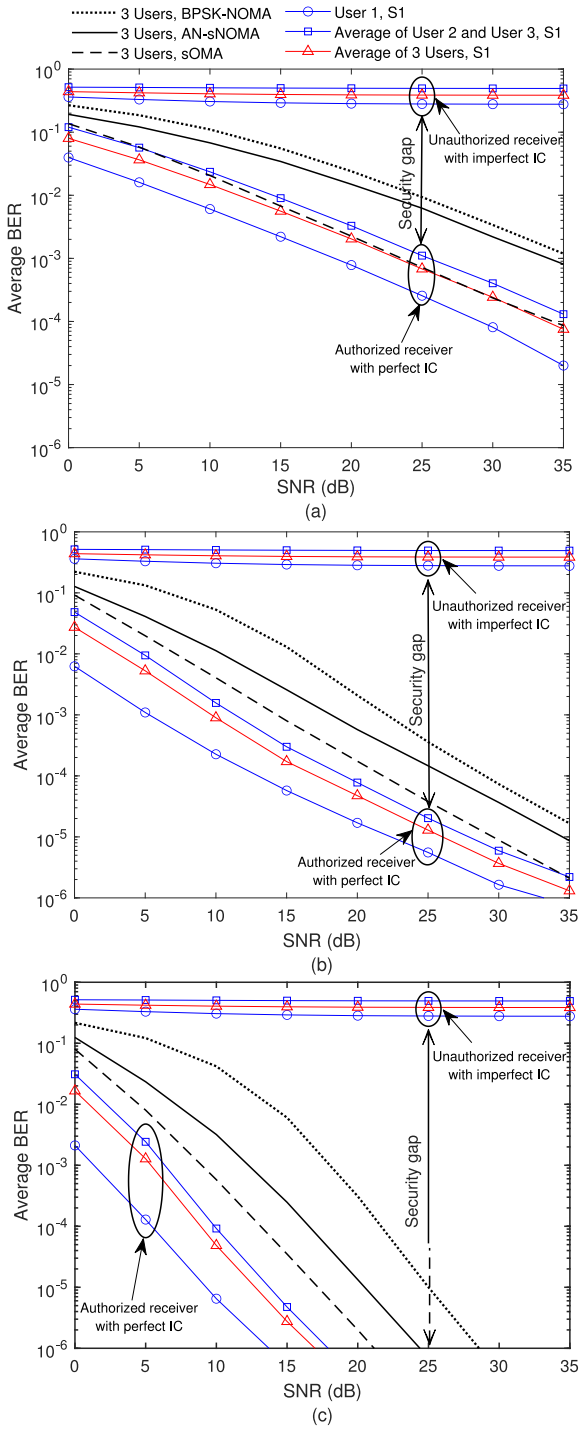

FIGURE 6. Average BER of 3-user CPD-sNOMA (S1) using different Rician factors, Case 1 for the chaotic codes, and $\beta = 50$ compared with the reference systems. (a) $\mathcal{K} = 0$; (b) $\mathcal{K} = 5$; (c) $\mathcal{K} = 10$.

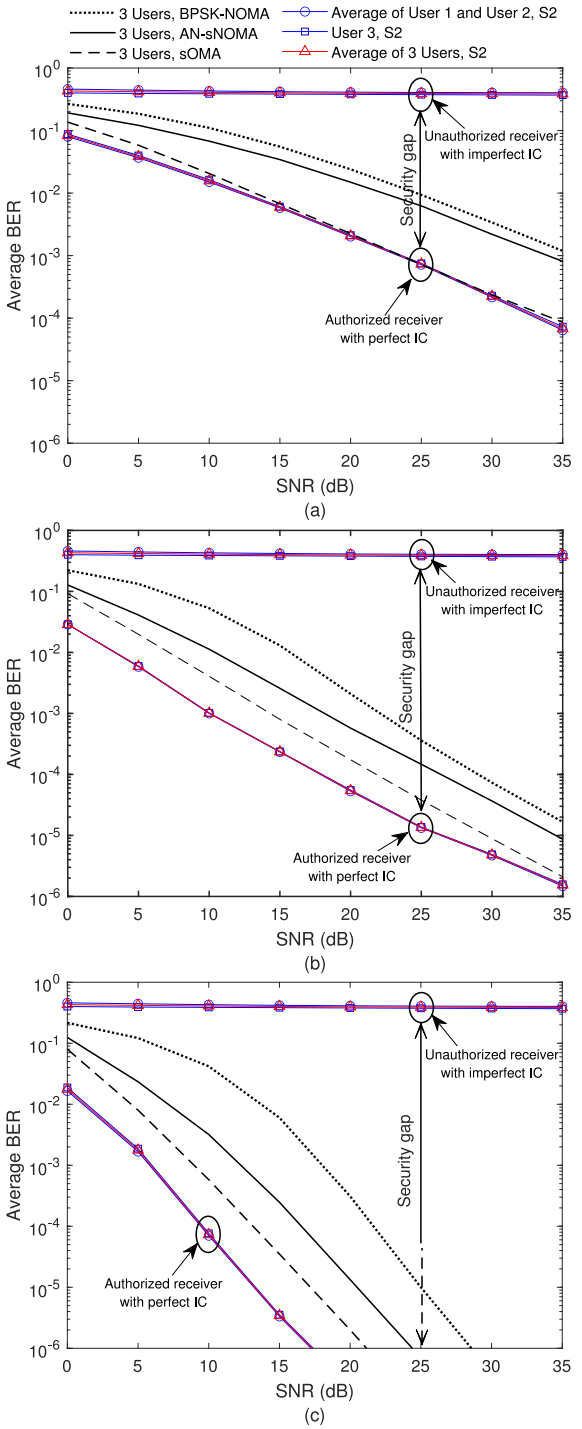

FIGURE 7. Average BER of 3-user CPD-sNOMA (S2) using different Rician factors, Case 1 for the chaotic codes, and $\beta = 50$ compared with the reference systems. (a) $\mathcal{K} = 0$; (b) $\mathcal{K} = 5$; (c) $\mathcal{K} = 10$.

used to accommodate the weakest user (user3). The optimal power control parameters are obtained using Algorithm 4 as $\alpha_{\mathcal{A}} = 0.8$, $\alpha_{\mathcal{B}} = 0.2$, $\alpha_1 = \alpha_2 = 0.4$, and $\alpha_3 = 0.2$. In this scenario, the authorized receiver provides fair BERs among served users for all $\mathcal{K}$ values as shown in Figs. 7 (a)-(c). This result is due to the use of a joint ML receiver for $G_{\mathcal{A}}$. Moreover, the average BER for the case of $\mathcal{K} = 5$ in Fig. 7 (a) shows a SNR gain of about 4.2 dB at BER of 10^{-3} compared with the reference 3-user sOMA. Note that the BER results of the illegal receiver in both scenarios (S1 and S2) exhibit a significant error-floor (~ 0.5) over the entire range of SNRs due to inaccurate secret keys. Besides,

TABLE 3. Summary of the performance results of 3-user sNOMA schemes using $\beta = 50$. The SNR gains are calculated for $\mathcal{K} = 5$ at average BER of 10^{-3} compared with the reference sOMA system.

sNOMA Scheme	Key-Space	SNR gain (dB)
CD-sNOMA	$\mathcal{O}\left[2^{179}\right]$	20.3
PD-sNOMA	$\mathcal{O}\left[2^{186}\right]$	3.3
CPD-sNOMA (S1)	$\mathcal{O}\left[2^{186}\right]$	4.6
CPD-sNOMA (S2)	$\mathcal{O}\left[2^{186}\right]$	4.2

the security gap of both scenarios is approximately the same and increases significantly as $\mathcal{K}$ increased. These gaps are slightly better than that achieved by the PD-sNOMA due to the additional CD diversity in one of the designed groups (i.e., $G_{\mathcal{A}}$ or $G_{\mathcal{B}}$).

In Table 3, a summary of the key performance results of 3-user sNOMA schemes is presented. It includes the realized key-space for chaotic PLS when Case 1 is used for the generation of chaotic codes. Furthermore, the achieved SNR gains at average BER target of 10^{-3} when $\mathcal{K} = 5$ are presented compared with the reference 3-user sOMA system. It can be seen that CD-sNOMA of 20.3 dB gain outperforms the other schemes significantly with uniform user performance. However, this scheme requires a joint ML receiver of high complexity and EPA that has drawbacks of power consumption at the user terminals with near-far concerns [2]. The hybrid CPD-sNOMA (S2) also offers user-fairness in terms of the error rate with an important SNR gain of 4.2 dB. The huge key-space of each design is very important to attain the required PLS against brute-force attacks. For instance, a key-space of order $\mathcal{O}(2^{179})$ is achieved using CD-sNOMA while the other sNOMA schemes provide about $\mathcal{O}(10^{56}) \approx \mathcal{O}(2^{186})$. These are sufficient to combat the most powerful attacks of 2^{100} search capabilities recommended by [29]. For the current fastest computing speed of about $415.53 \times 10^{15}/sec$, the eavesdropper needs more than 7×10^{38} years to obtain the correct keys of designed sNOMA schemes and detect the transmitted signals successfully.

B. IMPACT OF POWER FACTORS AND CODE LENGTH

To show the impact of power allocation factors on the performance of sNOMA schemes, Fig. 8 demonstrates the average BERs of 3-user PD-sNOMA and CPD-sNOMA schemes as a function of α for two SNR values (20 dB and 30 dB) and two Rician factors ($\mathcal{K} = 0$ and 5). The parameter $\alpha = \alpha_1$ is used for PD-sNOMA while $\alpha = \alpha_{\mathcal{A}}$ is considered for CPD-sNOMA scenarios (S1 and S2) The chaotic codes are generated using Case 1 with $\beta = 50$. It can be seen that the intended receivers achieve nearly stable performance owing to the utilized codes which provide an extra dimension for signal detection even for insufficient power difference among users. Overall, the best BERs in Figs. 8 (a) and (b) are noticed to be around $\alpha = 0.7$ for PD-sNOMA and $\alpha = 0.8$ for S1 and S2 schemes which

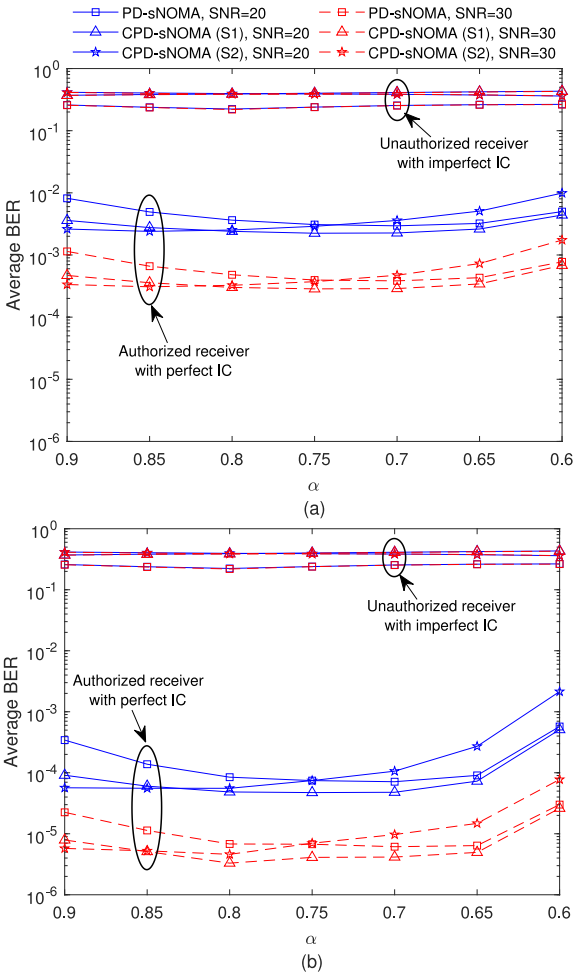

FIGURE 8. Average BER of 3-user sNOMA schemes as a function of α using $\beta = 50$. (a) $\mathcal{K} = 0$; (b) $\mathcal{K} = 5$.

coincide with the achieved results in Figs 5–7. These values validated the designed power control algorithms for optimal performance with largest security gap.

In Fig. 9, the average BERs of 3-user sNOMA schemes are shown as a function of β and for two SNRs (20 dB and 30 dB) and two Rician factors ($\mathcal{K} = 0$ and 5). The power control parameters are obtained as in Figs. 4–7 using the designed Algorithms 1-4, respectively. For CD-sNOMA with EPA scheme, the increase of code length β has a direct impact on improving the average BER and also PLS at the cost of additional receiver complexity. The other schemes show a slight improvement in the BER since the signal estimation depends mainly on the SIC process and hence the error-propagation effects. Note that the increase of code length β has no effects on the link data rate degradation compared with the OMA schemes as long as the chip duration condition is satisfied (i.e., $T_b = \beta T_c$).

Form Figs. 8 and 9, It can be seen that the unauthorized receiver with imperfect ICs shows a serious error-floor (close to 0.5) over the entire ranges of α and β. The achieved outcomes are based on a very-tiny mismatch

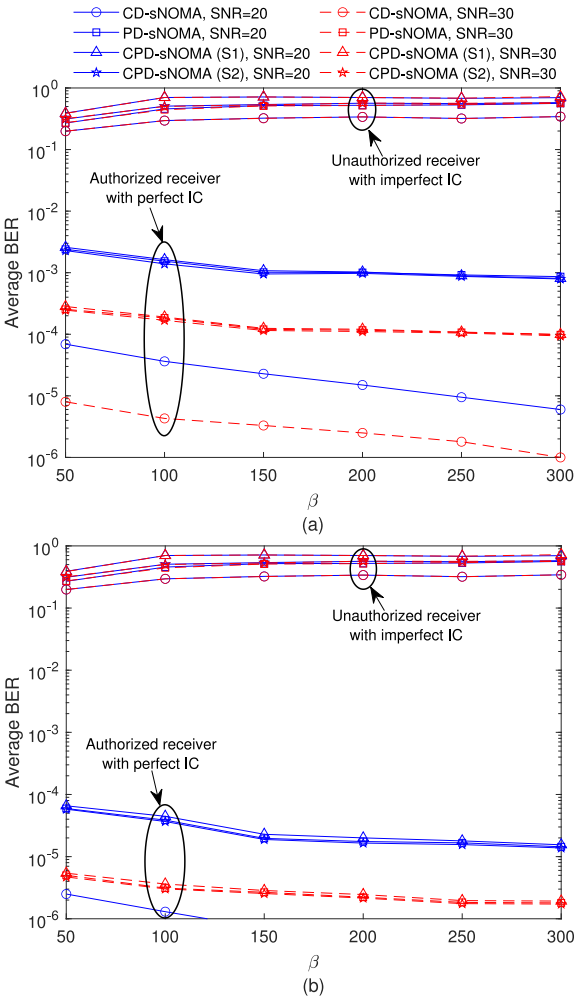

FIGURE 9. Average BER of 3-user sNOMA schemes as a function of β. (a) $\mathcal{K} = 0$; (b) $\mathcal{K} = 5$.

in the ICs of 10^{-15}. Therefore, the proposed sNOMA schemes with suitable system parameters enable robust error performance with cost-effective security against potential attacks.

C. USER CONNECTIVITY

To study the impact of user connectivity on the performance of sNOMA schemes, Fig. 10 shows the average BERs as a function of K for two SNRs (10 dB and 20 dB) and different Rician factors. The spreading codes are formed using Case 1 with $\beta = 50$, while the power allocation parameters for each K-user system are optimized based on Algorithms 1-4. From the presented results and considering a target BER of 10^{-3}, it can be seen that CD-sNOMA provides the highest number of connected users with trivial performance loss as K increased. For instance, up to $K = 8$ users can be served reliably for the case of ($\mathcal{K} = 0$ (i.e., NLoS) and SNR of 10 dB, and increases considerably as the SNR and/or $\mathcal{K}$ (i.e., LoS) values increased by employing low cross-correlation codes. Nevertheless, this will increase the decoder complexity to $\mathcal{O}[2K]$ as shown in Table 2. On the other hand, when $\mathcal{K} = 10$ and SNR of 20 dB are considered, PD-sNOMA and CPD-sNOMA scenarios of low complexity receivers can reliably support only up to $K = 4$ users due to SIC based error propagation. This results in a valuable tradeoff between user connectivity and BER performance. Summary of the achieved user connectivity results are shown in Table 4.

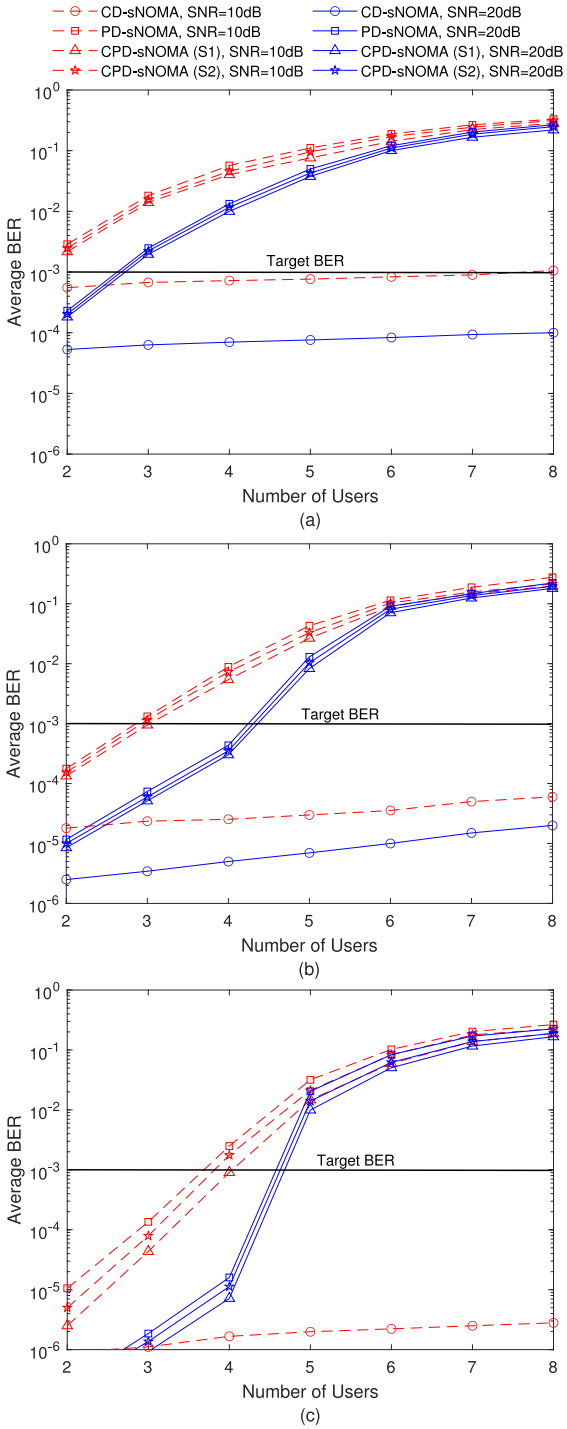

FIGURE 10. Average BER of sNOMA schemes as a function of the number of connected users k using $\beta = 50$. (a) $\mathcal{K} = 0$; (b) $\mathcal{K} = 5$; (c) $\mathcal{K} = 10$.

TABLE 4. Summary of the achieved user connectivity of sNOMA schemes at average BER of 10^{-3} using $\beta = 50$ and SNR of 20 dB.

sNOMA-Scheme	Number of Connected Users (K)		
	$\mathcal{K} = 0$	$\mathcal{K} = 5$	$\mathcal{K} = 10$
CD-sNOMA	> 8	> 8	> 8
PD-sNOMA	2	4	4
CPD-sNOMA (S1)	2	4	4
CPD-sNOMA (S2)	2	4	4

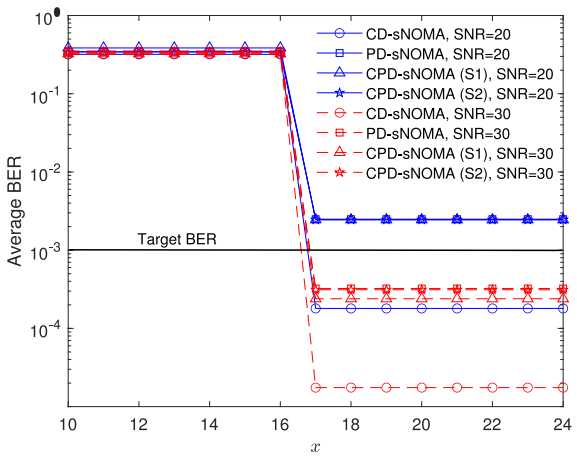

FIGURE 11. Average BER of 3-user sNOMA schemes as a function of sensitivity to ICs (10^{-x}) using $\beta = 50$ and Rician factor of $\mathcal{K} = 0$.

D. IMPACT OF KEY MISMATCH

The key mismatch between transmit and receiving sides is a very important security metric that reflects the ability of an eavesdropper to guess the correct system parameter through exhaustive search [4], [27], [28], [29]. Therefore, the impact of this issue on the average BER of sNOMA schemes is investigated in Fig. 11 as a function of sensitivity to the utilized ICs (10^{-x}). Note that the ICs of employed chaotic systems represent the most critical elements of the key-space $\mathcal{S} = \{K, \beta, \mathcal{L}, \mathcal{D}, \text{ICs}\}$. Two SNR values (20 dB and 30 dB) are considered for a 3-user system with Rician factor of $\mathcal{K} = 0$, Case 1 for code formation using CCS, $\beta = 50$. The power control parameters are similar to those obtained in Figs. 4–7 for PD-sNOMA, CD-sNOMA, and CPD-sNOMA (S1 and S2), respectively. From the obtained results, it can be seen that the estimated signals of all designs exhibit severe error-floor (close to 0.5) even for an extremely high level of 10^{-16} sensitivity. Assuming a target BER of 10^{-3}, PD-sNOMA and CPD-sNOMA (S1 and S2) also can not achieve reliable links for higher sensitivity levels and nearly-high SNR of 20 dB due to SIC based error propagations. This validates the robustness and security of proposed sNOMA schemes with ultra-high key-space (see Table 3) against the most powerful attacks.

VI. PRACTICAL CONSIDERATIONS AND FUTURE DIRECTIONS

A. PRACTICAL CONSIDERATIONS

The practical implementations of sNOMA schemes are based on the integration of CBSC and NOMA technologies. Therefore, the practical concerns of these two approaches will be reflected in the overall system design and other new considerations. The most important considerations are highlighted in the following.

Chaos Synchronization: Maintaining chaos synchronization is one of the critical issues in developing sNOMA designs that employ coherent MUDs for transmitted chaotic signals. In general, there are two approaches to achieve the required synchronization between transmitter and receiver. The first one requires the regeneration of the same chaotic signal used at the transmitter with the same ICs. This method is not preferable since any small change in the ICs will lead to producing different chaotic signals and then a high possibility of link failure. For the second method, the chaotic signals are generated and stored in both the transmitter and receiver. So, the problem of high sensitivity to IC can be mitigated at the cost of feedback overhead and additional memory requirements [35]. Many updates in the field of chaos synchronization such as the methods in [32] can also be extended for practical sNOMA applications.

Chaotic Circuit Design: Energy-efficient chaotic circuit designs are required to attain the critical constraints for green communications [2], [8], [15] with desired information security [4]. Note that the hardware complexity is responsible for about $50-80\%$ of the power consumption at the BS [3]. The available circuits for chaos generation in many well-known publications like [32] and [35] can be further improved to achieve this important target.

Error propagation: This is another serious issue when SIC is used for MUD in sNOMA systems. It is evident that once a user/group is decoded erroneously, this error will propagate to the following stages, which has a direct impact to degrade the error rate. In this context, using chaotic codes with considerable lengths can compensate for the effect of error propagation at the cost of additional MUD complexity. Therefore, proper designs that consider the tradeoff between these factors should be investigated [5].

Integration of sNOMA with OMA: When the sNOMA schemes are integrated with OMA techniques, efficient and low complexity user-grouping and power control algorithms are needed to satisfy the target QoS and other important issues such as channel capacity maximization and user-fairness. This requires an accurate estimation of CSI which is necessary for MUD at the same time [1], [8], [12], [15]. Signaling overhead should be considered due to its direct relation in degrading the actual data rate. Low complexity MUD techniques are very important to reduce the processing time and consumed power for green communications [3].

B. FUTURE DIRECTIONS

In this section, we highlight some possible research directions that could extend the state-of-the-art of sNOMA designs for future applications and wireless networks.

First, uplink sNOMA communication is investigated in this paper due to: (*i*) the majority of available research works in this field have considered the downlink channel such as [5], [19], [20], [21]; and (*ii*) uplink sNOMA design and analysis is more challenging than the downlink counterpart from the perspective of both the authorized BS and eavesdropper owing to the need for multiuser CSI rather than a single-user channel. As an important extension to this work, a unified framework of uplink-downlink chaos-based sNOMA could be considered with extensive analysis and evaluation.

Second, we recognize the extension of designed sNOMA schemes with OMA approaches such as massive MIMO [2] and OFDMA [8] to be an interesting topic to enhance user connectivity and spectral efficiency significantly. This goal would require studies on the optimal/suboptimal resource allocation and user-grouping strategies to satisfy the QoS, network targets, and user-fairness [8], [9], [10], [26]. The trade-offs between system performance, MUD and computational complexity, overhead requirements, and desired level of PLS seem all topics that required further investigation [2], [3].

As a third research direction, we propose the analysis of the impact of imperfect CSI [1], [8], [15], hardware impairments, and SIC error [5] on the performance and robustness of sNOMA systems that need to be investigated.

Finally, implementation and field tests of such solutions would also be required to establish this approach's practicalities and to assess the performance and capabilities of sNOMA systems in real-time applications towards the potential adoption in beyond 5G networks.

VII. CONCLUSION

In this paper, a set of efficient uplink sNOMA designs have been presented over realistic fading channels by exploiting the advantages of chaos-based PLS and extended connectivity of NOMA approaches. In the CD-sNOMA scheme, an EPA strategy has been used for the transmitted signals. The received signals were detected then using a joint ML receiver. On the other hand, DPC algorithms have been considered for signal transmission in PD-sNOMA and CPD-sNOMA scenarios. The receiver designs for these schemes are based on integrated SIC and ML techniques. Different chaotic code formation approaches have been considered to provide robust chaotic PLS. The achieved BER results and security gap using optimized power allocation factors validated the effectiveness of proposed schemes compared with the reference systems. Moreover, a very large key-space of the order of $\mathcal{O}(2^{186})$ is obtained to resist powerful brute-force attacks. Valuable tradeoffs can be analyzed between achieved BERs, the number of supported users, the security gap, and the overall system complexity. Some important considerations on the feasible implementation and future research directions for sNOMA were also highlighted. The interesting outcomes of error performance, connectivity, and robust PLS may also lead to extending the paradigm with OMA schemes for covert wireless networks.

REFERENCES

[1] B. Makki, K. Chitti, A. Behravan, and M.-S. Alouini, "A survey of NOMA: Current status and open research challenges,"*IEEE Open J. Commun. Soc.*, vol. 1, pp. 179–189, 2020.

[2] W. Al-Hussaibi and F. Ali, "Efficient user clustering, receive antenna selection, and power allocation algorithms for massive MIMO-NOMA systems," *IEEE Access*, vol. 7, pp. 31865–31882, 2019.

[3] W. Al-Hussaibi and F. Ali, "Performance-complexity tradeoffs of MIMO-NOMA receivers towards green wireless networks,"in *Proc. 30th IEEE PIMRC*, 2019, pp. 654–659.

[4] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[5] N. Horiike, E. Okamoto, and T. Yamamoto, "A downlink non-orthogonal multiple access schemes having physical layer security," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 205, pp. 1–11, Aug. 2018.

[6] Z. Ding, R. Schober, and H. V. Poor, "Unveiling the importance of SIC in NOMA systems—Part 1: State of the art and recent findings," *IEEE Trans. Commun. Lett.*, vol. 24, no. 11, pp. 2373–2377, Nov. 2020.

[7] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[8] Y. Xu, G. Gui, H. Gacanin, and F. Adachi, "A survey on resource allocation for 5G heterogeneous networks: Current research, future trends, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 668–695, 2nd Quart., 2021.

[9] W. Al-Hussaibi, "Optimal cluster formation and power control for high connectivity wireless MIMO-NOMA applications,"*Electron. Lett.*, vol. 55, no. 20, pp. 1110–1112, Oct. 2019.

[10] Y. Xu, Z. Qin, G. Gui, H. Gacanin, H. Sari, and F. Adachi, "Energy efficiency maximization in NOMA enabled backscatter communications with QoS guarantee," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 353–357, Feb. 2021.

[11] L. Lv, Q. Wu, Z. Li, Z. Ding, N. Al-Dhahir, and J. Chen, "Covert communication in intelligent reflecting surface-assisted NOMA systems: Design, analysis, and optimization," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1735–1750, Mar. 2022.

[12] S. Islam, N. Avazov, O. Dobre, and K. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges,"*IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, 2n Quart., 2017.

[13] S. Sharma, K. Deka, V. Bhatia, and A. Gupta, "Joint power-domain and SCMA-based NOMA system for downlink in 5G and beyond,"*IEEE Commun. Lett.*, vol. 23, no. 6, pp. 971–974, Jun. 2019.

[14] L. Lv, H. Jiang, Z. Ding, and L. Yang, "Secrecy-enhancing design for cooperative downlink and uplink NOMA with an untrusted relay," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1698–1715, Mar. 2020.

[15] Y. Xu, R. Q. Hu, and G. Li, "Robust energy-efficient maximization for cognitive NOMA networks under channel uncertainties," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8318–8330, Sep. 2020.

[16] B. Di, L. Song, Y. Li, and G. Y. Li, "TCM-NOMA: Joint multi-user codeword design and detection in trellis-coded modulation-based NOMA for beyond 5G," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 766–780, Jun. 2019.

[17] X. Chen, Z. Zhang, C. Zhong, R. Jia, and D. Ng, "Fully non-orthogonal communication for massive access," *IEEE Trans. Commun.*, vol. 66, no. 4, pp. 1717–1731, Apr. 2018.

[18] A. Maatouk, E. Caliskan, M. Koca, M. Assaad, G. Gui, and H. Sari, "Frequency-domain NOMA with two sets of orthogonal signal waveforms," *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 906–909, May 2018.

[19] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[20] X. Chen, Z. Zhang, C. Zhong, D. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 788–801, Apr. 2018.
[21] K. Xiao, L. Gong, and M. Kadoch, "Opportunistic multicast NOMA with security concerns in a 5G massive MIMO systems," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 91–95, Mar. 2018.
[22] G. Gomez, F. Marten-Vega, F. Lopez-Martinez, Y. Liu, and M. Elkashlan, "Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70422–70435, 2019.
[23] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the security enhancement of uplink NOMA systems with jammer selection," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5747–5763, Sep. 2020.
[24] E. Okamoto, N. Horiike, and T. Yamamoto, "Sparse chaos code multiple access scheme achieving larger capacity and physical layer security," in *Proc. 20th WPMC*, Dec. 2017, pp. 604–610.
[25] Y. Masuda, E. Okamoto, K. Ito, and T. Yamamoto, "An uplink non-orthogonal multiple access scheme having physical layer security based on chaos modulation," in *Proc. ICOIN*, Kuala Lumpur, Malaysia, Jan. 2019, pp. 136–140.
[26] I. Almusawi, W. Al-Hussaibi, and F. Ali, "Chaos-based physical layer security in NOMA networks over Rician fading channels," in *Proc. IEEE ICC*, 2021, pp. 1–6.
[27] A. Elfiqi, H. Khallaf, S. Hegazy, A. Elsonbaty, H. Shalaby, and S. Obayya, "Chaotic polarization-assisted L DPSK-MPPM modulation for free-space optical communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 9, pp. 4225–4237, Sep. 2019.
[28] M. Bi et al., "A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON," *IEEE Photon. J.* vol. 9, no. 1, pp. 1–10, Feb. 2017.
[29] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo, "A novel chaos-based symmetric image encryption using bit-pair level process," *IEEE Access*, vol. 7, pp. 99470–99480, 2019.
[30] A. Tayebi, S. Berber, and A. Swain, "Security enhancement of fix chaotic-DSSS in WSNs," *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 816–818, Apr. 2018.
[31] H.-P. Ren, M. Baptista, and C. Grebogi, "Wireless communication with chaos," *Phys. Rev. Lett.*, vol. 110, no. 18, p. 5, Apr. 2013.
[32] W. Al-Hussaibi, "Effect of filtering on the synchronization and performance of chaos-based secure communication over Rayleigh fading channel," *Commun. Nonlinear Sci. Numer. Simulat.*, vol. 26, nos. 1–3, pp. 87–97, Sep. 2015.
[33] W. M. Tam, F. C. M. Lau, C. K. Tse, and M. M. Yip, "An approach to calculating the bit-error rate of a coherent chaos-shift-keying digital communication system under a noisy multiuser environment," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 2, pp. 210–223, Feb. 2002.
[34] I. Almusawi, W. Al-Hussaibi, Y. Tahir, and F. Ali, "Chaos-based secure power-domain NOMA for wireless applications," in *Proc. 23rd WPMC*, Okayama, Japan, Oct. 2020, pp. 1–6.
[35] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," *IEEE Access*, vol. 4, pp. 2621–2648, 2016.
[36] W. M. Tam, F. C. M. Lau, and C. K. Tse, "A multiple access scheme for chaos-based digital communication systems utilizing transmitted reference," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 9, pp. 1868–1878, Sep. 2004.
[37] W. Tam, F. Lau, and C. Tse, "Analysis of bit error rates for multiple access CSK and DCSK communication systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 50, no. 5, pp. 702–707, May 2003.
[38] T. Yang and L. Chua, "Chaotic digital code-division multiple access (CDMA) communication systems," *Int. J. Bifurcat. Chaos*, Vol. 7, no. 12, pp. 2789–2805, 1997.
[39] Y. Lau, J. Jusak, and Z. M. Hussain, "Blind adaptive multi-user detection for chaos CDMA communication," in *Proc. TENCON*, 2005, pp. 1–5.
[40] J. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, 2017.
[41] J. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1191–1194, May 2017.
[42] Y. Hwang and H. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: Analysis and design," *IEEE Trans. Signal Process.*, vol. 52, no. 9, pp. 2637–2649, Sep. 2004.
[43] R. M. Christopher and D. K. Borah, "Physical layer security for weak user in MISO NOMA using directional modulation (NOMAD)," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 956–960, May 2020.
[44] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 532–540, 2011.
[45] I. Almusawi, W. Al-Hussaibi, and Y. Tahir, "Chaos-based NOMA for secure wireless communications over Rayleigh fading channels," in *Proc. IMDC-SDSP*, 2020, pp. 1–12.
[46] H. M. Furqan, M. S. J. Solaija, H. Türkmen, and H. Arslan, "Wireless communication, sensing, and REM: A security perspective," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 287–321, 2021.
[47] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "New physical layer key generation dimensions: Subcarrier indices/positions-based key generation," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 59–63, Jan. 2021.
[48] N. Ishikawa, J. M. Hamamreh, E. Okamoto, C. Xu, and L. Xiao, "Artificially time-varying differential MIMO for achieving practical physical layer security," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2180–2194, 2021.
[49] E. Soujeri, G. Kaddoum, and M. Herceg, "Design of an initial condition-index chaos shift keying modulation,"*Electron. Lett.*, vol. 54 no. 7 pp. 447–449, Apr. 2018.

ISRAA M. AL-MUSAWI (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from BETC, Southern Technical University, Iraq, in 2016 and 2020, respectively, where she is currently a Researcher of Communication Engineering. Her research interests include wireless and mobile networks, 5G and beyond, chaos-based communications, physical layer security, non-orthogonal multiple access systems, and wireless-powered communication networks.

WALID A. AL-HUSSAIBI (Senior Member, IEEE) received the B.Sc. degree in electronics and communications from the University of Basrah, Iraq, in 1991, the M.Sc. degree in electronics and communications from the Jordan University of Science and Technology, Jordan, in 2000, and the Ph.D. degree in wireless and mobile communications from Sussex University, U.K., in 2011. In 2012, he joined the Southern Technical University, Iraq, as a Faculty Member, where he is currently a Professor with the Department of EET, BETC. His research interests include multiple access techniques, wireless and mobile networks, massive MIMO, NOMA schemes, multiuser MIMO-NOMA, chaotic communications, channel capacity, 5G and beyond, and wireless-powered communications.

FALAH H. ALI (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from Cardiff University in 1984 and 1986, respectively, and the Ph.D. degree from the University of Warwick in 1992. He is a Professor of Communications Engineering with the University of Sussex. Prior to his current post he was a Reader in Digital Communications, and a Senior Lecturer and a Lecturer in Electronics Engineering with Cardiff University. From 1992 to 1994, he was a Postdoctoral Research Associate with Lancaster University. He has published over 120 papers and has served on several international conferences' technical programme committees. His current research interests include 5G/6G mobile and wireless communication systems. He is a Fellow of the IET.