An Uplink Secure CB-NOMA with SIC Receiver for Wireless Applications

Israa M. Al-Musawi‡, Walid A. Al-Hussaibi*, Yaseen Tahir†, and Falah H. Ali†
†Faculty of Graduated studies, Southern Technical University (STU), Basrah, Iraq
‡Basrah Technical Institute, STU, Basrah, Iraq
§Basrah Technical Engineering Collage, STU, Basrah, Iraq
*University of Sussex, Brighton, BN19QT, UK

Abstract. The nonorthogonal multiple access (NOMA) techniques are considered one of the main methods to realize the goals of 5G mobile and wireless systems such as link communication reliability and high user connectivity. Yet, when the amount of simultaneously connected users increases, many concerns will arise regarding the users’ data security. Various chaotic systems in the communication field have been presented to mitigate the data security concerns offering a cost-efficient technique to provide physical layer security. This work presents an uplink secure chaos-based NOMA (SCB-NOMA) system by exploiting the power domain. For signal modulation at the transmitters’ node, chaos shift keying is used, with controlled transmit power to satisfy the receiver conditions. For multiuser detection, the receiver side employs successive interference cancellation with chaotic demodulation. The efficiency of designed SCB-NOMA is demonstrated by considering different power control factors, system scenarios, and chaotic sequence length compared with different reference systems. It is shown that the efficient selection of the power allocation parameter has a direct effect on the bit error rate (BER) performance. Meanwhile, when the amount of power difference for the successive interference cancellation process is not adequate, the chaotic codes maintain the desired data security and enable robust BER performance for connected users. Besides, the correlation between the utilized chaotic codes has more impact on BER regardless of the considered sequence length.

1. Introduction

The huge digital revolution in information technology worldwide has led to a massive increase in smart mobile phones/tablets/laptops, unmanned aerial vehicles (UAV), wireless sensors, and Internet of things (IoT) devices. Consequently, the new communication systems are predicted to fulfil the increasing burdens for wireless services with requirements of high user connectivity, ultra-reliability, low-latency, robust data security, low complexity, and affordable implementation cost [1]-[4]. In particular, the nonorthogonal multiple access (NOMA) concept based upon code-domain and/or power-domain has been considered as one of the essential techniques to achieve the core objectives of the fifth-generation (5G) of mobile and radio communications. NOMA technique mostly based on code-domain or the power-domain, can surpass the classical orthogonal multiple access methods by terms of channel capacity and the number of connected users without a substantial loss in the error performance [5]-[8].
Nonorthogonal spreading codes are used in the code-domain NOMA (CD NOMA) systems to separate the users’ data. Meanwhile, in the power-domain NOMA (PD NOMA) the users are assigned varied power levels according to the channel gains value [1]. In the downlink channel, more transmit power is assigned to the users with weak channel gains compared to the strong users. Then at the receiving node, successive interference cancellation (SIC) technique may be employed to separate the signals of the transmitting users. Contrarily for the uplink channel, the weak users may utilize s small power amount for transmitting which will prolong the life duration of the users’ batteries and meet the strong user power variance condition for an effective multiuser detection (MUD) based on SIC process [6].

Another essential point, the simultaneous communication for connected users in NOMA designs might cause security issues for the users’ data. To eliminate this challenge, in the literature various chaos-based secure communication (CBSC) schemes were studied to present robust and affordable physical layer security (PLS) solutions for mobile communications [8]-[10]. Those CBSC schemes are developed through making use of the appealing features of chaotic signals such as the unpredictability, broadband spectrum, the high sensitiveness for initial conditions (ICs), simple generation by using low-priced electronics, and high resistance to interference and jamming [11], [12]. The information messages in CBSCs are typically concealed by the employed chaotic signal and transmitted over the wireless channel environment to the destination node. For coherent detection, chaos synchronization between transmitting and receiving ends is essential to restore the transmitted messages [13], [14]. But this requirement is not needed in the non-coherent receivers where data recovery can be achieved by observing the received signal features [15], [16].

In the earlier years, many CBSC systems have been studied for multiuser communications by investing the chaotic signals wideband features [8]-[10], [13], [16], [17]. In [9], a grant-free sparse chaotic code multiple access system was proposed to extend the channel capacity by employing chaotic signals with unlike ICs in CD NOMA. Differential CSK (DCSK) and chaos shift keying (CSK) modulation techniques are employed also for multiple access channels in [13] and [16], respectively. The performance of the previously mentioned multiple-access systems is evaluated over the Gaussian channel environment to demonstrate their applicability. In [10], an uplink PD NOMA is integrated with chaotic-coding and multiple-input multiple-output (MIMO) channels to enhance the security, connectivity, and capacity. Nevertheless, an increasing complexity at the decoding process is the cost of such a scheme. In [8], a downlink channel with power-domain chaos-based MIMO-NOMA and improved security qualities is investigated. However, in [8] and [10] the integration of MIMO and the methods of orthogonal frequency division multiplexing (OFDM) may have the effect to exaggerate the performance of chaos-based security.

This paper presents an uplink system design for secure chaos-based NOMA (SCB-NOMA) by exploiting the power dimension over the wireless communication channel. The connected users will use CSK modulation to realize PLS while an efficient power control is employed in PD NOMA for the multiple-access channel. For MUD at the receiving node, SIC with chaotic demodulation is applied. To confirm the efficiency of SCB-NOMA system, simulations for the bit-error-rate (BER) are given and compared with a single and multiuser reference systems. Moreover, the orthogonal multiple access scheme gains such as OFDM and MIMO of the works [8] and [10] are isolated. The accomplished results using diverse power control factors, system operating scenarios, and chaotic sequence length are much appealing and reveal many valuable tradeoffs between the required BER performance, level of security, complexity, and user connectivity.

The remaining parts of this paper are arranged as follows. In Section II, a technical background on chaotic signals generation and the security of chaotic communications are presented. SCB-NOMA system model, signal model, power allocation, and the receiver design are given in Section III. Section IV demonstrates the BER simulation results. At last, Section V will conclude this paper.
2. Technical Background on Chaos-Based Secure Communications

2.1. Chaotic Signals Generation
Chaotic signals are typically employed in CBSC schemes for various signal modulation techniques such as chaos parameter modulation (CPM), chaos on-off keying (COOK), chaotic masking (CM), and CSK. The employed chaotic signals are generated by utilizing a simple electronic circuit that reveals nonlinear dynamical behaviours like the double-scroll attractor \cite{12, 14}. The nonlinear dynamics of this attractor are described by the below set of equations.

\[
\begin{align*}
\dot{x} &= \frac{G(y - x)}{C_1} - \frac{g(x)}{C_1} \\
\dot{y} &= \frac{G(x - y)}{C_2} + \frac{z}{C_2} \\
\dot{z} &= -\frac{y}{L}
\end{align*}
\]

where \( g(x) = m_0 x + (m_1 - m_0)(|x + B_P| - |x - B_P|)/2 \), and the used parameters for the chaotic behaviour are \( C_1 = 1/9, C_2 = 1, G = 0.7, L = 1/7, m_0 = -0.5, m_1 = -0.8, \) and \( B_P = 1 \). Many computer programs (such as MATLAB) can be used to solve the mathematical model (1) to find the chaotic signals \( x, y, \) and \( z \). A demonstration for the generated time waveform signals of \( (x, y, \text{and } z) \) states is illustrated in Figure 1, where the figure shows clearly the sensitivity to ICs using two different sets of considered values.

2.2. Chaotic Communications Security
The usage of chaotic signals for concealing the users’ messages will form an encrypted signal. To carry out the decoding process at the receiving node, a previous knowing of the utilized parameters is needed, such as the involved code, chaotic parameters, power control parameter of the transmitted signal, and the ICs. As a result, any potential attackers will be unable to detect and demodulate the

![Figure 1](image_url)

Figure 1. Generated time waveforms of the double-scroll attractor states using different sets of ICs. (a) \( x \), (b) \( y \), and (c) \( z \) states.
transmitted signals easily. Consequently, chaotic signals in CBSC will provide PLS since only the receiver with the exact system parameters can correctly demodulate the signal. Hence, the classical highly-complexed encryption and decryption methods may be replaced by chaotic modulations. In the classical methods, the encryption protocols offer upper-layer security (ULS) with a rather high implementation complexity [4], [8]-[10].

The protocols used in the ULS are classically used in conventional wireless systems, yet under certain situations, it may have serious troubles. For example, the ULS protocols in 5G enormous connectivity may become complicated, expensive, and might cause an environmental hazard owing to the large power consumption amounts. The reason behind this high consumption of power is because of a two way verification requirement as well as the increasing signal processing quantity required at the base station (BS) [4].

3. System Model of SCB-NOMA
Consider a general SCB-NOMA system with $K$ single-antenna users simultaneously communicating through a wireless communication channel with a single-antenna BS receiver as illustrated in Figure 2. The transmitter and receiver use chaotic systems with drive-response synchronization for the signal CSK modulation/demodulation technique [14], respectively, and for chaotic codes generation, the dynamical system (1) is used. For MUD at the BS, SIC and chaotic demodulation techniques are employed considering a Gaussian channel model. Note that the adopted SCB-NOMA design in its basic configuration is very essential to isolated the known gains of fading environment and other integrated orthogonal multiple access schemes like OFDM and MIMO [8], [10], which will allow a benchmark performance outcome.

3.1. The Signal Model
For the transmitting node, user $k$ messages are mapped into binary bits $b_k \in \{-1,1\}^K$ followed by CSK modulation using a certain chaotic code $c_k \in \mathbb{R}^1 \times \beta$ of length $\beta$ chips as

$$v_k = b_k c_k = b_k [c_{k,1}, \ldots, c_{k,\beta}] = [v_{k,1}, \ldots, v_{k,\beta}]$$

where $c_{k,i}$ is the $i^{th}$ chip of the chaotic code $c_k$ for user $k$, $v_{k,i}$ is the $i^{th}$ chip of the modulated data vector $v_k \in \mathbb{R}^1 \times \beta$ of user $k$ considering normalized power, and it is assumed that the bit duration $T_b$ is $\beta$ times the chip duration $T_c$ (i.e. $T_b = \beta T_c$).

Based on the utilized user’s chaotic code $c_k$; $k = 1, \ldots, K$, the $i^{th}$ chip of $v_k$ is given as

$$v_{k,i} = \begin{cases} +c_{k,i} & \text{for bit} \text{“}1\text{”} \\ -c_{k,i} & \text{for bit} \text{“} -1 \text{”} \end{cases}$$

![Figure 2. System model of SCB-NOMA](image-url)
So, user $k$ transmitted signal vector is $s_k \in \mathbb{R}^{1 \times \beta}$ with a mean power $p_k$ may be presented as

$$s_k = \sqrt{p_k} v_k = [s_{k,1} \ldots s_{k,\beta}].$$

(4)

The model of SCB-NOMA received signal can be written as

$$r = \sum_{k=1}^{K} s_k + n = S + n$$

(5)

where $r = [r_1 \ldots r_\beta] \in \mathbb{C}^{1 \times \beta}$ is the vector of the received signal, $S = [s_1 \ldots s_K]^T \in \mathbb{R}^{K \times \beta}$ is the total transmitted signal, $[\cdot]^T$ presents transpose operation, and $n = [n_1 \ldots n_\beta] \in \mathbb{C}^{1 \times \beta}$ is i.i.d. AWGN vector of zero-mean and $\sigma_n^2$-variance.

3.2. Power Control

For SCB-NOMA with PD technique, the power variance among any two consecutive users received signals (i.e. weak and strong users) is significant for managing the interference, and perform an effective MUD based on SIC [6]. Consequently, at the BS, the received powers from connected users $\{\mathcal{P}_k\}_{k=1}^K$ are efficiently controlled employing the next power allocation constraint

$$\mathcal{P} = \sum_{k=1}^{K} \alpha_k \mathcal{P}_k = \sum_{k=1}^{K} p_k$$

(6)

where $0 < \alpha_k < 1$ is the factor for the power control of the $k^{th}$ user with $\sum_{k=1}^{K} \alpha_k = 1$, and $\mathcal{P}_k$ presents user $k$ received power whose transmit power $p_k$ may be given as

$$p_k = \alpha_k \mathcal{P} ; \; k = 1, \ldots, K.$$  

(7)

It is assumed that the users are in descending order such that $\mathcal{P}_1 > \mathcal{P}_2 > \cdots > \mathcal{P}_K$, therefore any two consecutive users received powers should meet the SIC power variance as

$$\left(\mathcal{P}_k - \sum_{l=k+1}^{K} \mathcal{P}_l\right) \geq \delta \mathcal{P}_k ; \; k = 1, \ldots, K - 1$$

(8)

where the target error rate designed parameter is $\delta < 1$.

3.3. SIC Receiver

MUD is performed at the BS using SIC receiver of one stage for every user (i.e. $K$ stages) and chaotic demodulation. The users’ signals are arranged descendingly according to their received power levels from the strong user to the weak one.

Presuming $\mathcal{P}_1 > \mathcal{P}_2 > \cdots > \mathcal{P}_K$, in the first SIC stage, the strongest user $\hat{s}_1$ is estimated from the received signal $r^{(1)} = r$ with high reliability while treating other users as a noise in the background. This process is achieved according to the criteria of minimum Euclidean distance and given by

$$\hat{s}_1 = \arg \min_{s_1 \in \mathbb{S}} || r^{(1)} - s_1 ||^2$$

(9)

where $||.||$ stands for the Euclidean norm. Then, the first SIC output is demodulated to find $\hat{b}_1$. 

5
For the next SIC stage, $\hat{b}_1$ is reconstructed to eliminate its influence from $r^{(1)}$ and to find $r^{(2)}$ the new input vector. Then, $r^{(2)}$ is utilized for user 2 signal estimation as $\hat{s}_1$ which will be demodulated to $\hat{b}_2$. Accordingly, the general form for signal estimation of the $k^{th}$ user can be given as

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

and the SIC $k^{th}$ stage outcome is demodulated as $\hat{b}_k \in \hat{b} = [\hat{b}_1 \ldots \hat{b}_K]$. Note that at SIC last stage, user $K$ will have a free interference operation due to the removal of other users' contributions in the previous stages. Nevertheless, it will own the smallest error performance amongst users due to the small amount of allocated power.

4. Simulation Results

Numerical simulations in this section are performed using MATLAB to show the performance of the considered SCB-NOMA system with many tradeoffs between error rate and system security. The utilized parameters are: $K = 2$ and 3 users; normalized power constraint $P$; and a power allocation factor $\alpha = \alpha_1$. The BER results are averaged over $10^6$ channels and compared with single-user and multiuser binary phase-shift keying (BPSK) reference schemes.

Figure 3 shows the BER performance for a 2-user system as a function of signal-to-noise ratio (SNR) with $\beta = 50$ and $\alpha = 0.8$. The employed power control parameters for this scenario are $\alpha_1 = 0.8, \alpha_2 = 0.2, \text{and}\, \delta = 0.75$. As it is shown, the BERs of all users outperform the references over all SNR ranges due to the diversity of chaotic codes and insignificant multiple access interference from the weak user (i.e. user 2). Moreover, user 1 (i.e. the strong user) achieves a gain of about 1 dB at BER target of $10^{-3}$ compared with user 2. Note that the diversity improvement isverified by simulations and the theoretical proof is out of the scope of this paper.

For the SCB-NOMA system of 3-users, Figure 4 shows the BER results as SNR function considering $\alpha = 0.8$ and $\beta = 50$. In this scenario the employed power control parameters are $\alpha_1 = 0.8, \alpha_2 = 0.16, \alpha_3 = 0.04, \text{and}\, \delta = 0.75$. The BER performance of all users also still the best compared with the 3 users BPSK reference despite higher multiple access interference. For example, at BER of $10^{-2}$ the SNR gains for users 1, 2, and user 3 are 6.5 dB, 2 dB, and 1 dB, respectively. User

![Figure 3](image-url)  
**Figure 3.** Average BER performance SCB-NOMA 2-user system with $\beta = 50$ and $\alpha = 0.8$.  

![Figure 4](image-url)  
**Figure 4.** Average BER performance SCB-NOMA 3-user system with $\beta = 50$ and $\alpha = 0.8$.  

1 (i.e. the strongest) realizes the best performance owing to the larger value of assigned power in comparison to user 3 (i.e. the weakest). Still, robust performance is also realized for user 3 owing to the diversity of SIC despite the small amount of total power.

In Figure 5, the BER performance of SCB-NOMA is illustrated as a function for the power control factor $\alpha$ for 2 and 3 user system with $\beta = 50$ while considering two values for SNR of 5 dB and 7 dB. It is shown that the 2-user scheme BER performance is better than the scenario of 3-user for both SNRs and over the whole $\alpha$ range because of the smaller multiple access interference as expected. Moreover, the best performance is achieved approximately at power parameters of $\alpha = 0.8$ and $\alpha = \ldots$
0.75 for 2 user and 3 user scenarios, respectively. The employed chaotic sequences can be seen clearly to provide an extra dimension for signal detection (code-domain) when the power difference between users is insufficient.

Figure 6 demonstrates the average BER of SCB-NOMA scheme with 3-user as a function of the chaotic code length $\beta$ with $\alpha = 0.8$ while considering multiple SNRs from 3 dB to 7 dB. Although the increase in the length of the chaotic code has a direct effect on PLS (at cost of extra complexity), it cannot warrant BER improvement due to the inherent correlation among utilized nonorthogonal chaotic codes. For example, the best error performance is achieved for the considered scenario at $\beta = 150$. Consequently, the proposed SCB-NOMA system with the appropriate selection of power control parameter, and spreading chaotic code length may offer a robust error performance with cost-efficient data security.

5. Conclusion
An efficient uplink design for SCB-NOMA has been given by employing the benefits PLS in chaos-based communications and PD NOMA large connectivity. The served users transmit their signals using CSK modulation and power control technique meanwhile SIC with chaotic demodulation are used for MUD at the BS receiver. The efficiency of the designed SCB-NOMA system is confirmed by BER simulations, by utilizing different $\alpha$ and $\beta$ values, and by comparing the results with single and multiuser reference systems. Moreover, many tradeoffs can be achieved between the required BER performance, desired security level, number of connected users, and system complexity. The interesting outcomes of the robustness of BER performance over a large $\alpha$ and $\beta$ ranges can be seen as an interesting integration of PD NOMA and CD NOMA approaches. This might lead to the extension of this paradigm with the important orthogonal multiple access techniques for future secure communications.

References
[1] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, “A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 10, pp. 2181-2195, 2017.
[2] W. Al-Hussaibi, “A generalised antenna correlation model for accurate performance evaluation of 2D massive MIMO communication systems,” *Australian Journal of Electrical and Electronics Engineering*, vol. 17, no. 4, pp. 269-277, Dec. 2020.

[3] W. Al-Hussaibi, and F. Ali, “Group Layer MU-MIMO for 5G Wireless Systems,” *Telecommunication Systems*, vol. 70, no. 4, pp. 525-540, Apr. 2019.

[4] 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 Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679-695, 2018.

[5] M. Vaezi, G. A. Aruma Baduge, Y. Liu, A. Arafa, F. Fang, and Z. Ding, “Interplay Between NOMA and Other Emerging Technologies: A Survey,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 4, pp. 900-919, 2019.

[6] N. Ye, H. Han, L. Zhao, and A.-h. Wang, “Uplink Nonorthogonal Multiple Access Technologies Toward 5G: A Survey,” *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1-26, 2018/06/12, 2018.

[7] W. Al-Hussaibi, “Optimal Cluster Formation and Power Control for High Connectivity Wireless MIMO-NOMA Applications,” *Electronics Letters*, vol. 55, no. 20, pp. 1110-1112, Oct. 2019.

[8] N. Horiike, H. Kitagawa, E. Okamoto, and T. Yamamoto, “Chaos MIMO-based downlink non-orthogonal multiple access scheme with physical layer security,” in *Proc. 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-7, 2018.

[9] E. Okamoto, N. Horiike, and T. Yamamoto, “Large-Scale Grant-Free Sparse Chaos Code Multiple Access Scheme for 5G IoT,” *Proc. 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pp. 1-5, 2018.

[10] Y. Masuda, E. Okamoto, and T. Yamamoto, “Low complexity decoding of downlink chaos NOMA scheme with physical layer security,” in *Proc. IEEE 17th Annual Consumer Commun. & Networking Conf. (CCNC)*, Las Vegas, USA, pp. 1–6, 2020.

[11] S. Hayes, C. Grebogi, and E. Ott, “Communicating with chaos,” *Phys. Rev. Lett.*, vol. 70, no. 20, pp. 3031-3034, May 17, 1993.

[12] W. Al-Hussaibi, “Filtering Effects on the Synchronization and Error Performance of Promising Wireless Chaos-Based Communications,” *Wireless Networks*, vol. 21, no. 6, pp. 1957-1967, Aug. 2015.

[13] W. M. Tam, F. C. M. Lau, C. K. Tse, and A. J. Lawrance, “Exact Analytical Bit Error Rates for Multiple Access Chaos-Based Communication Systems,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 51, no. 9, pp. 473-481, 2004.

[14] W. Al-Hussaibi, “Impact of Filtering Chaotic Signals on Secure Wireless Communication Systems Based Chua's Circuit,” *Proc. IIT'13*, Al Ain, Abu Dhabi, UAE, 6 Pages, 17-19 March 2013.

[15] K. Murali, Y. Haiyang, V. Varadan, and H. Leung, “Secure communication using a chaos based signal encryption scheme,” *IEEE Transactions on Consumer Electronics*, vol. 47, no. 4, pp. 709-714, 2001.

[16] W. M. Tam, F. C. M. Lau, and C. K. Tse, “Analysis of bit error rates for multiple access CSK and DCSK communication systems,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 5, pp. 702-707, 2003.

[17] I. Al-Musawi, W. Al-Hussaibi, Y. H. Tahir, and F. Ali, “Chaos-Based Secure Power-Domain NOMA for Wireless Applications,” *Proc. 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Okayama, Japan, pp. 1-6, 2020.