Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6615767, 8 pages
https://doi.org/10.1155/2021/6615767

Research Article

Secure OFDM-Based NOMA for Machine-to-Machine Communication

Shafiq U. Rahman,[1] **Amber Sultan**,[1] **Roobaea Alroobaea**,[2] **Muhammad Talha**,[3] **Syed B. Hussain**,[1] **and Muhammad A. Raza**[4]

[1]*Department of Electronics and Electrical Systems, The University of Lahore, Pakistan*
[2]*Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[3]*Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia*
[4]*Department of Information Technology, Bahauddin Zakariya University, Multan 60000, Pakistan*

Correspondence should be addressed to Syed B. Hussain; baqar.hussain@es.uol.edu.pk

Received 26 November 2020; Revised 13 December 2020; Accepted 6 May 2021; Published 19 May 2021

Academic Editor: Mohammed El-Hajjar

Machine-to-machine communication (M2M) has obtained increasing interest in recent years. However, its enhancement and broadcasting characteristics produced a new security challenge. We have suggested a novel dynamic Quadrature Amplitude Modulation (QAM) scheme for a totally elastic and dynamic mapping of user data by using chaos. This paper analyses physical layer security methods in Orthogonal Frequency Division Multiplexing-based Nonorthogonal Multiple Access (OFDM-NOMA) and introduces a secure data transmission mechanism created by dynamic QAM. The security robustness given by the suggested encryption scheme is assessed, where an overall keyspace of $\sim 10^{163}$ is achieved, which is sufficient to provide security against exhaustive attacks. The result of the scheme is verified through MATLAB simulation, where the bit error rate performance of our proposed scheme is compared with an unencrypted OFDM signal, and the performance of our proposed scheme is analyzed for an illegal user. The suggested dynamic mapping fulfills the fundamental obligations of cryptography for data security. Moreover, it enhances the level of security in OFDM-NOMA.

1. Introduction

Among the top technological trends of the world, one of the most promising applications is M2M communications. The widespread application of M2M communication boosts their use in various fields. In M2M communication, various intelligent devices are associated with wired or wireless connections to implement Internet of Things (IoT) generation networks. These devices interface with one another without direct human intervention. IoT can be an initiative to open novel job opportunities, such as environmental monitoring, smart grids, health care, intelligent transport systems, building automation, and smart houses [1]. Since the data in M2M communication is intercommunicated through an open channel, the security of those data which contain sensitive information is a major concern. M2M communication is incredibly defenseless against attackers for a few reasons. Initially, its parts regularly invest a greater part of their energy unattended; what is more, in this way, it is easy to attack them physically. Secondly, most of the communications are done remotely, which makes eavesdropping very simple during downlink transmission [2]. In [3], an anonymous authentication hybrid encryption scheme is discussed and the Advanced Encryption Standard (AES) scheme is implemented for the confidentiality and authenticity of the multidomain of M2M communication. The scheme has achieved mutual authentication for inter- and intradomain communication in the absence of the identity of M2M devices. The presented scheme can protect small data such as text; however, is not suitable for large data encryption. Recently, work

has been done on corporate chaos with encryption. Chaos is a part of mathematics that reviews the behavior of a dynamic framework that is very sensitive to the initial condition, randomness, and unpredictability. In [4], the authors suggested a private nonorthogonal multiple-access visible-light communication system encryption based on nonlinear dynamical systems. The encryption scheme assures privacy among all legal users against attackers during communication. A recent scheme has deployed a two-level encryption mechanism that encrypts the data of multiusers using different keys [5]. A chaotic NOMA scheme for downlink transmission is given in [6]. In [7], a four-dimensional (4D) encryption is utilized to improve the secrecy of OFDM Passive Optic Network (OFDM-PON). 4D-hyperchaotic mapping is utilized to produce four masking factors to get ultra-high-confidentiality encryption in four various dimensions [8]. In [9], encryption techniques are used in the physical layer based on frequency induction for OFDM signals to enhance the security against any present attackers. In [10], the authors have proposed determining a real-time secured transmission system with a chaos-based encryption scheme deployed in the physical layer of the OFDM-PON. In the encryption procedure, field-programmable gate array boards are used at the optical line terminal (OLT) and optical network unit (ONU), utilizing hyperdigital chaos. The scheme provides optimum security and has a large keyspace. However, according to [11], the encryption algorithms based on a single round permutation diffusion are capable of resisting the chosen plain text attack. Thus, a multifold and efficient substitution-permutation-based encryption scheme is necessitated for the encryption application in the physical layer of the OFDM, which provides better security to the data communication.

Moreover, all mentioned schemes have considered a conventional mapping criteria for the underlying modulation scheme. For the traditional QAM mapping procedure, all OFDM information symbol points are static on the constellation diagram. According to this fixed mapping rule, the cipher information can only inhabit the constellation's exact position. Alone, scrambling the constellation points among those fixed locations cannot provide strong security defense. This scrambled data can be used later for statistical analysis, and thus, the security of the data can be compromised. In [12], the authors tried to hide the underlying constellation by chaotic insertion of pilots to increase the security of the OFDM-PON system based on a chaotic system. However, with blind channel estimation, the channel can be estimated and useful data can be extracted as the characteristics of the constellation would be revealed. Therefore, to assure user data security with statistical analysis, it is required to make symbol mapping dynamic.

This manuscript has introduced a novel encryption scheme for physical layer security in OFDM-NOMA. The proposed scheme is based on a dynamic system that is capable of multimedia data and text data encryption. The proposed scheme aims at mapping QAM symbols anywhere independently and dynamically onto the complex plane. The dynamic mapping of QAM does not let the mapping be static, and thus, the user data is not compromised by statistical analysis. The scheme executes the two-dimensional Zaslavsky map to generate chaotic sequences using the initial conditions and parameters. As the first step of encryption, the scheme uses the obtained chaotic sequences to permute the QAM symbols. XOR encryption is performed on the permuted QAM symbol to produce uniformness in the encrypted data that ensures the scheme's resistance against histogram attacks. The last step of our multifold encryption is distributing the encrypted QAM symbols on the complex plane independently. The independent mapping of QAM symbols consequently improves the scheme's resistance to correlation attacks. The proposed scheme achieves a keyspace of up to $\sim 10^{163}$, and as a result, it enhances the security level of the OFDM encryption scheme.

2. Methodology

In this section, we have discussed the proposed encryption scheme that is being deployed in the physical layer of OFDM-NOMA. In OFDM-NOMA, the proposed encryption scheme chaotically encrypts the data before the transmission and then sends the data through an insecure network. The scheme uses the chaotic output values to randomize user data and map it dynamically onto the dimensions of a higher QAM.

Figure 1 illustrates the proposed dynamic mapping of QAM in comparison with the conventional static QAM mapping. Figure 1(a) shows the 16-QAM static mapping, where every QAM symbol has a fixed position in the constellation plane. In Figure 1(b), we have demonstrated how the position of the QAM symbol will be changed chaotically, such that the QAM symbols will be mapped anywhere in the constellation plane. Figure 1(c) shows the resultant noisy constellation after incorporating chaos to map a QAM symbol dynamically.

In our suggested scheme, multifold chaotic encryption is achieved through the two-dimensional (2D) Zaslavsky chaos [13]:

$$\begin{aligned} x_n + 1 &= x_{n+}\nu(1 + \mu y_n) + \epsilon\nu\mu[\cos(2\pi x_n) \bmod 1], \\ y_n + 1 &= e^{-r}[y_n + \epsilon \cos(2\pi x_n)], \\ \mu &= \frac{1 - e^{-r}}{\tau}. \end{aligned} \tag{1}$$

In the above equation, x_n and y_n are the input samples to the chaotic map. The symbols ν and μ denote the controlling parameters that are used to control the chaotic behaviors, and for $n = 0$, the values of x_n and y_n are the initial conditions. The encryption scheme will be used for three operations: permutation, XOR operation, and constellation shifting [14]. Let D be user data of dimension $M \times N$. Then, the detailed procedure of the encryption process of data D is discussed in equations ((2)), equations ((3)), equations ((4)), equations ((5)), equations ((6)), and equations ((7)).

Figure 2 shows the block diagram of the proposed scheme. Since user data can be extremely correlated, therefore, initially, the proposed encryption scheme permutes the plain data. The scheme uses the chaotic map for the selection of the new position. At the beginning, the permutation step iterates the chaos map $2 \times M \times N$ times. Let x_i and y_i be the obtained iterated sequences, where the elements of

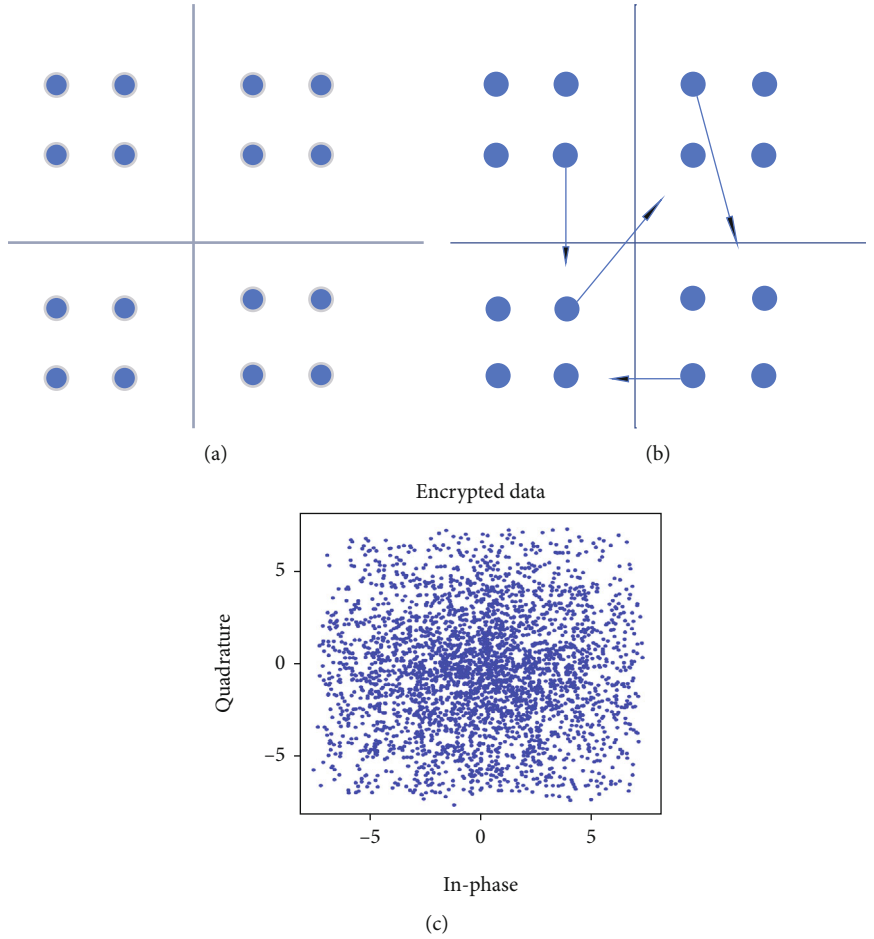

Figure 1: (a) Conventional 16 QAM. (b) Dynamic 16 QAM. (c) Resultant dynamically shifted 16 QAM.

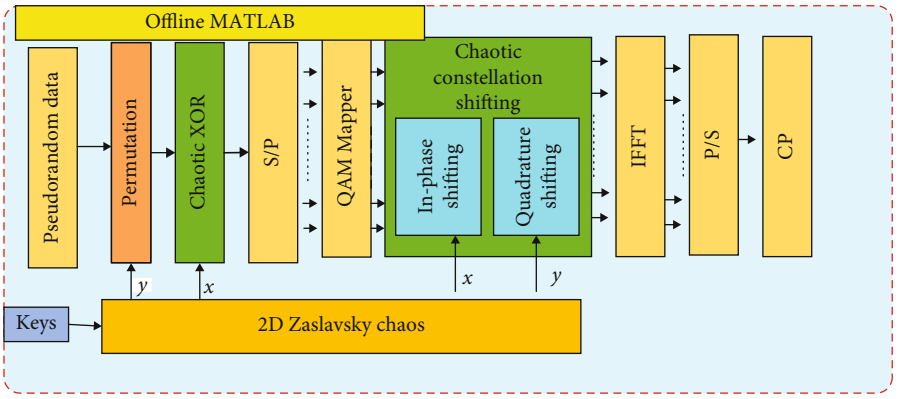

Figure 2: Block diagram of the proposed chaotic encryption scheme.

the sequences x_i and y_i belong to the close interval $[-2, 2]$. In the next step, we convert them into integer values using the following equations:

$$x_i' = \text{floor}\left(x_i \times 10^{15} \bmod M\right), \tag{2}$$

$$y_i' = \text{floor}\left(y_i \times 10^{15} \bmod N\right). \tag{3}$$

Equation (2) and equation (3) are used to transform the data from interval $[-2, 2]$ into the sets $\{0, 1, 2, 3, \cdots .M\}$ and $\{0, 1, 2, 3, \cdots, N\}$. Accordingly, in the new sequences x_i' and y_i', the elements occur randomly in the range between 0 and $M \times N$. Subsequently, we use the obtained random integer sequence and permute the data matrix D by using the equation given as follows:

$$D'(i, j) = D\left(x_i' + 1, y_i' + 1\right), \tag{4}$$

where $D(i, j)$ denote the pixel position of the original data matrix placed at the position ith row and jth column, and D' denote the permuted matrix. Consequently, one can get the permuted data.

As shown in Figure 2, the XOR operation is then used to increase the randomness in the ciphered data. The XOR operation scheme generates a sequence of random numbers through a chaotic map. Therefore, the order of the sequence is the same as the order of the data matrix. The obtained sequence is then XORed with the permuted data. The mathematical representation is given as follows:

$$C(i, j) = D'(i, j) \bigoplus S(i, j), \tag{5}$$

where $C(i, j)$ denote the data of the new data, and $S(i, j)$ denote the elements of the generated sequence. After the XOR operation, one can get the new data matrix C of the required ciphered data.

In Figure 2, the in-phase and quadrature shifting blocks show our proposed scheme. To permit an elastic mapping, we have utilized chaos for constellation shifting. The chaotic sequences x and y are used to shift the in-phase and quadrature parts of the QAM symbol as follows:

$$I_x = -2 + 4 * [\text{mod}\ (\text{abs}(y), \text{floor}(\text{abs}(y)))], \tag{6}$$

$$Q_y = -2 + 4 * [\text{mod}\ (\text{abs}(y), \text{floor}(\text{abs}(y)))], \tag{7}$$

where x and y are the chaos output value. The mod is used for the remainder, and abs is used to convert the negative value of x and y to a positive value. The floor function is utilized to round the number downward. Using equation (6) and equation (7), the in-phase I_x and quadrature-phase Q_y will give the value between $[-2, 2]$.

The encrypted data is converted into serial data after performing IFFT. This serial data is then appended with a cyclic prefix of length 1/16 of the OFDM symbol. Table 1 shows a detail of the parameters used during the offline MATLAB simulation.

As the proposed scheme is a symmetric encryption scheme, the decryption will be done by performing the reverse of all processes at the receiver side. However, for performing channel estimation with the help of pilots, a zero-forcing algorithm is used. The legal receiver would use the same initial keys to generate the chaotic sequence used by the sender and thus decrypt the received data. Moreover, due to the multifold and independent mapping of each QAM symbol, chaos reconstruction is not possible. The initial keys can be shared between the legal users wirelessly based on [15] or over an optical channel based on [16].

3. Results and Discussion

The possibility of the suggested encryption scheme is proven through simulation analysis. Figure 3 illustrates the simulation results after sending encrypted 16-QAM OFDM information. 64 subcarriers have contemplated conveying 16-QAM information. To get information from the channel, the pilots are added to the data. Then, the data is transmitted in parallel, and after performing IFFT, the ciphered information is passed from a parallel to a serial. A cyclic prefix of 1/16 length of the OFDM symbol is then attached. These ciphered signals are then transmitted over an AWGN channel with SNR ranging from 10 dB to 30 dB. The data encoding is carried out using MATLAB programs. Two types of users are contemplated at the receiving side in this simulation (i.e., User-1 and User-2). User-1 is considered the legitimate user with information about the preshared keys, while User-2 is considered the illegitimate user with no information about the preshared keys. The illegitimate user will get the same ciphered OFDM signal as that obtained by the legitimate user. However, the legitimate user will be able to demap the noisy constellation into a regular 16-QAM constellation with the help of the preshared keys. For an illegitimate user, even after blind channel estimation, the constellation will still reveal no information. In our simulation results, we have compared our proposed scheme with an unencrypted OFDM signal; the resulting BER curve is shown in Figure 3. Our proposed scheme maps the constellation points anywhere in the complex plane, i.e., the point can be located away from or near the origin, based on the output of the chaos. As long as the new location remains near the origin, there would be no power penalty; however, when the new QAM symbol is far from the origin of the complex plane, more power is required to transmit it. Therefore, when compared with an unencrypted OFDM signal, our proposed signal incurs a power penalty. As shown in Figure 3, the BER performance of our proposed scheme shows a power penalty of ~0.7 dB compared to an unencrypted OFDM signal at BER 10^{-3}. The power penalty can be reduced by allowing the dynamic mapping within the dimensions of the conventional 16 QAM. The BER curve for User-2 shows that an illegal user cannot receive any useful information at any SNR.

In the simulation results of Figure 4, we have compared encrypted signals with unencrypted OFDM signals. A decoded OFDM signal shows better execution when contrasted with encrypted signals. Figure 4 shows the simulation results after sending encrypted 64-QAM OFDM information. The power penalty at BER 10^{-4} is approximately the same for 16 QAM and 64 QAM. Therefore, our proposed scheme can be used

Table 1: Parameters used in simulation.

Parameters	Value
Subcarriers	64
Symbols	50
Pilots	4
Cyclic prefix	16
SNR	10-30
x_n	0.14
y_n	0.15
V	4
E	2.3
R	3
U	$1 - \exp(-r)/2$

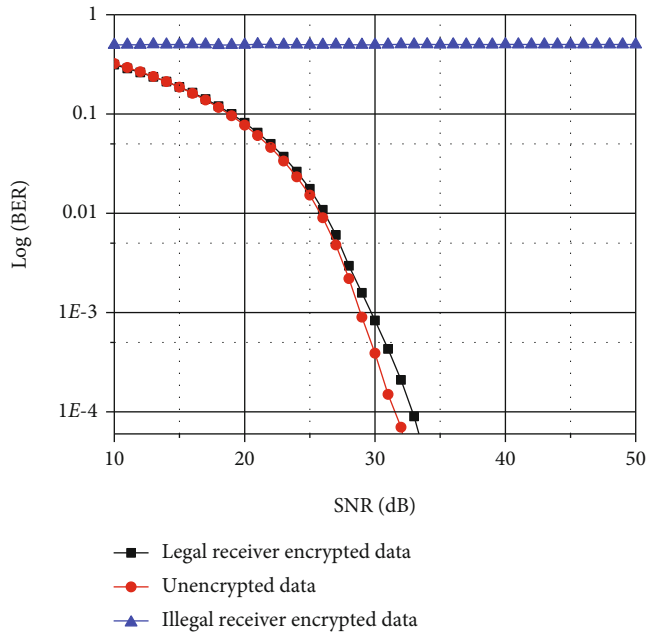

Figure 3: BER performance for encrypted 16 QAM.

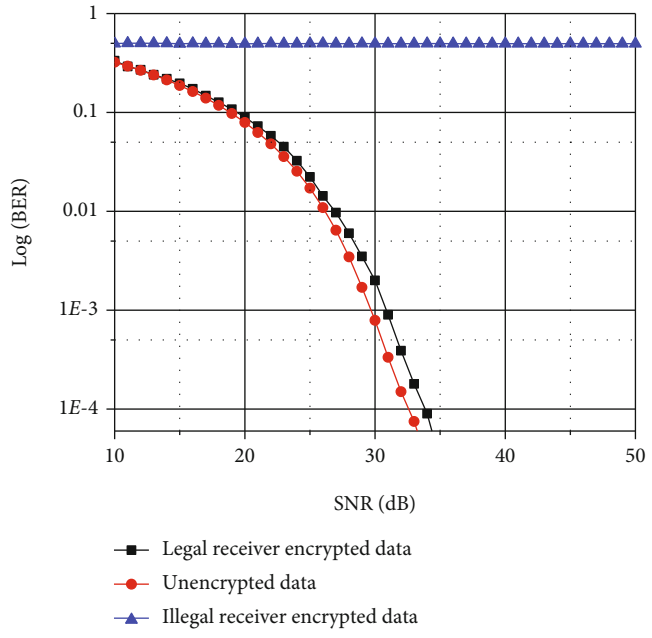

Figure 4: BER performance of encrypted 64 QAM.

for a higher dimension QAM as well. The BER is calculated after iterating the simulation model 50 times and taking the average of bit error values for all SNRs.

The sensitivity of the 2D chaotic system used in our suggested scheme is depicted in Figure 5. It is seen that with a little change, i.e., at the 10^{-15} position, in one input's initial value, the resultant output structure is completely different. Therefore, with the usage of 2D chaos to perform encryption, the confidentiality is improved. Moreover, this sensitivity of the 2D chaos system will alone provide a key space of 10^{-30}.

To examine the impact of the suggested chaotic constellation shifting plan, we decipher the obtained signals for all possible cases, where either the entire or different chaotic orders are unknown. Figure 6 illustrates the related BER analysis. We can see that in all these feasible cases, an illegal user is not able to recover the cipher data (i.e., BER ~ 0.5). The constellations, along with the encrypted data received by an illegitimate user with one identified shifting parameter, are exhibited as insets in Figure 6. With one known chaotic order, the suggested encryption scheme still hides the data

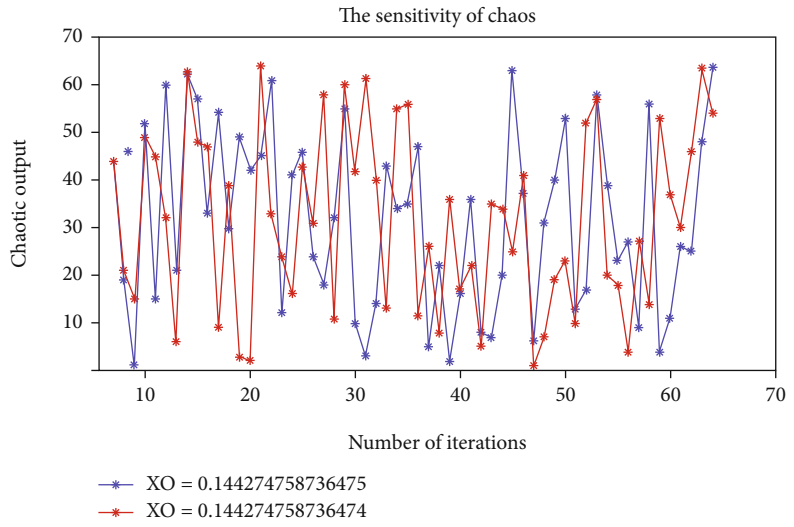

Figure 5: 2D chaos sensitivity diagram.

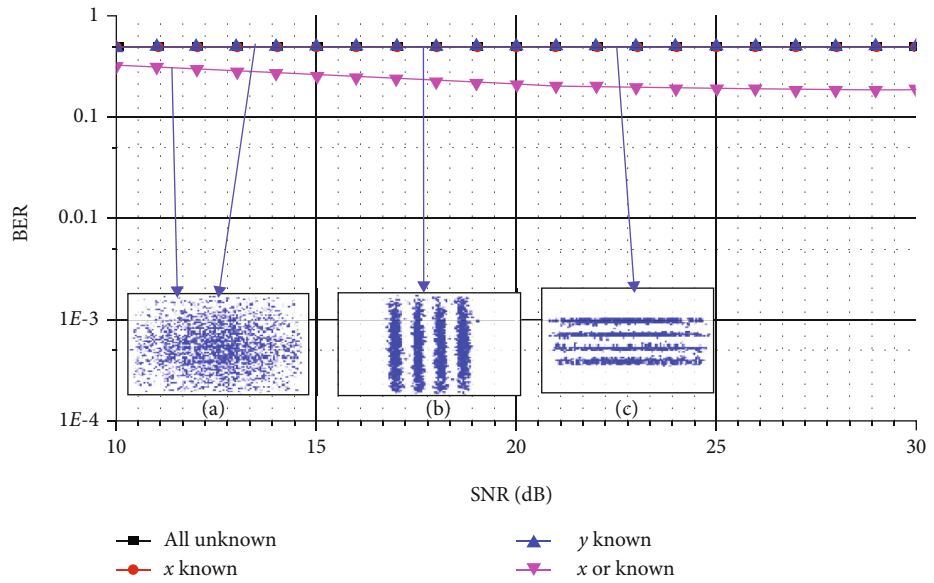

Figure 6: BER for illegal users.

successfully from an illegitimate user. As a result, it can be expressed that the suggested chaotic encryption scheme does not bargain the physical layer confidentiality of the information under all potential causes. Furthermore, finding the privacy key by relating unencrypted text with the cipher text will be challenging due to the multifold and autonomous QAM constellation shifting. Figure 6(a) shows that if the illegal user does not know about the chaotic sequence of mapping or only knows about the chaotic sequence of XOR operations, in both situations, they will receive a noisy constellation. If the illegal user knows only about the x-axis chaotic sequence, they will receive the constellation shown in Figure 6(b). If the illegal user knows about the chaotic y-axis sequence, they will only be able to demap the symbol mapping along the y-axis and thus receive the constellation as shown in Figure 6(c). Thus, it can be concluded that our proposed scheme provides efficient security even if the illegal user knows any one of the initial values.

To further evaluate our proposed scheme, we have transmitted an image. Figures 7(a) and 7(b) show the unencrypted image and its histogram, respectively, whereas Figures 7(c) and 7(d) show the encrypted image and its histogram, respectively. It can be seen that the encrypted image does not reveal any information about the real image. Moreover, the histogram of the encrypted image is almost uniform. Therefore, any attack on the histogram to reveal information about the image will not be successful. Therefore, the proposed scheme provides good image encryption as well.

The strength of the suggested chaotic encryption scheme can be assessed by determining the set of all keys used during encryption and decryption. The keyspace of the suggested scheme is quantitatively evaluated as follows. The chaotic

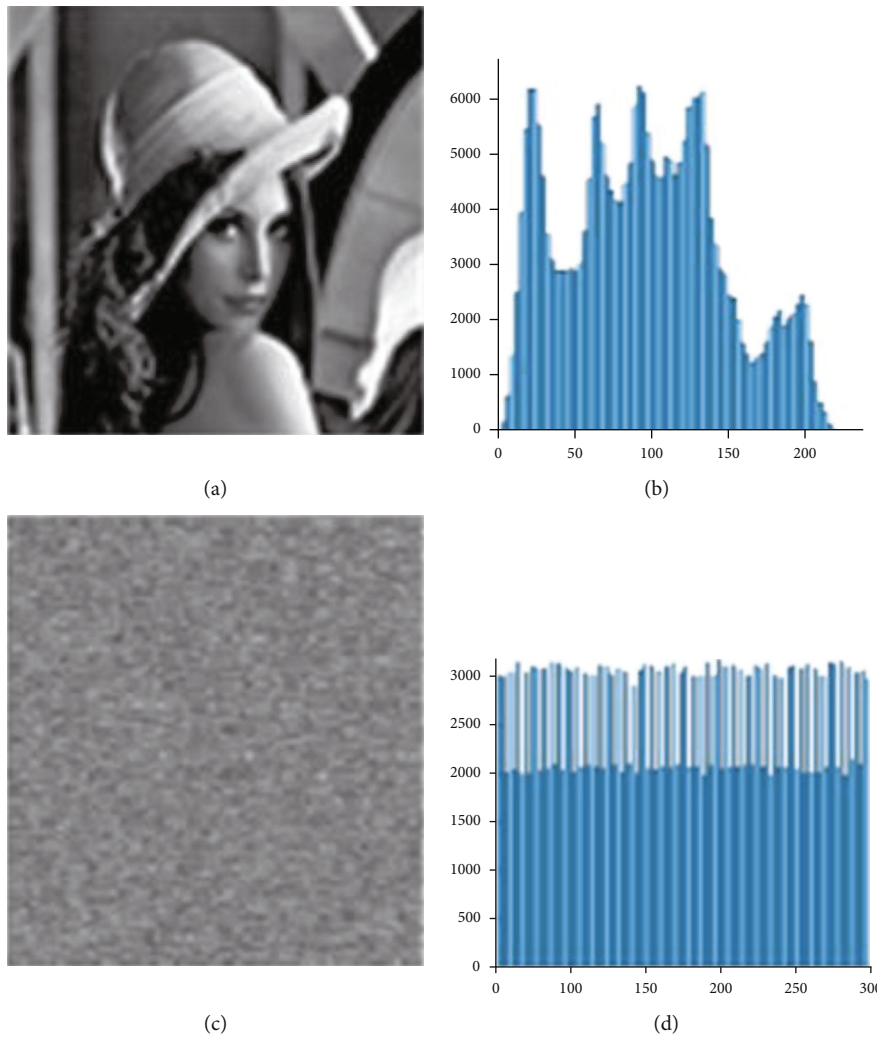

Figure 7: (a) Unencrypted transmitted image; (b) histogram of unencrypted transmitted image; (c) encrypted transmitted image; (d) histogram of encrypted transmitted image.

XOR gives a 2^{mN} keyspace, where m symbolizes the order of the QAM mapper used in the scheme, and N indicates the length of the OFDM symbol. The quadrature shifting and in-phase parameters generate $r \times 10^k \times 10^k$ keyspaces, where r is a binary number and k is the decimal position considered by (3) and (4), respectively. Consequently, the general formula to evaluate the approximate number of keyspaces is equal to $r \times 10^k \times 10^k \times 2^{mN}$. Since a total of 64 subcarriers are utilized in the suggested encryption scheme, a 16-QAM modulation is used and every single subcarrier is characterized by 4 bits. Therefore, when the chaotic XOR sequence is complete, this generates a keyspace approximately equal to 2^{256}. The chaotic parameters I and Q comprise two values before the fractional element and the digit number during constellation shifting considered on the tiny part. For clarity, we measured up to 4 positions of the decimal point; therefore, it will produce an extra keyspace of $10^4 \times 10^4 \times 2$. Similarly, when the chaotic permutation sequence is completed, this also generates a keyspace of 2^{256}. Besides, the constellation is affected because of the expansion and deduction of the moving parameters, so it boosts the order of the keyspace up to $10^4 \times 10^4 \times 2^{256} \times 2^{256} \times 4 \times 2$ ($\sim 10^{163}$). The resultant values guarantee the strength of the proposed scheme against the brute force attack.

4. Conclusion

In this paper, we exhibit a novel scheme for OFDM-based NOMA physical layer security, where we apply the confused constellation moving to multifold OFDM information encryption. Simulation results reveal that, because of the execution of constellation shifting, an elastic constellation with dynamic in-phase and quadrature shifted dimensions is accomplished. The corresponding noisy constellation successfully encodes the OFDM information with chaotic scrambling. The security robustness given by the suggested encryption scheme is assessed, where an overall keyspace of $\sim 10^{163}$ is achieved. The proposed scheme can be used to provide security to both uplink and downlink data transmission. The possibility of the scheme is certified through the

simulation, where the bit error rate performance of our proposed scheme shows a power penalty of ~0.7 dB in comparison with an unencrypted OFDM signal. However, in the presence of high noise, the power penalty would increase. The simulation results illustrate that the suggested scheme can be a good candidate for the upcoming secure OFDM-NOMA.

Data Availability

Data can be taken any time through email correspondence.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors are grateful to the Taif University Researchers Supporting Project (number TURSP-2020/36), Taif University, Taif, Saudi Arabia. The authors are also grateful to the Deanship of Scientific Research and King Saud University for funding this research work.

References

[1] W. Zhan and L. Dai, "Massive random access of machine-to-machine communications in LTE networks: throughput optimization with a finite data transmission rate," *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 5749–5763, 2019.

[2] F. Hussain, L. Ferdouse, A. Anpalagan, L. Karim, and I. Woungang, "Security threats in M2M networks: a survey with case study," *Computer Systems Science and Engineering*, vol. 270, 2016.

[3] Y. Qiu, M. Ma, and S. Chen, "An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems," *Computer Networks*, vol. 129, pp. 306–318, 2017.

[4] Y. Yang, C. Chen, W. Zhang et al., "Secure and private NOMA VLC using OFDM with two-level chaotic encryption," *Optics Express*, vol. 26, no. 26, pp. 34031–34042, 2018.

[5] J. S. Khan, W. Boulila, J. Ahmad et al., "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020.

[6] N. Horiike, E. Okamoto, and T. Yamamoto, "A downlink non-orthogonal multiple access scheme having physical layer security," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, 2018.

[7] J. Zhao, B. Liu, Y. Mao et al., "High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization," *Optics Express*, vol. 28, no. 14, pp. 21236–21246, 2020.

[8] F. M. Almansour, R. Alroobaea, and A. S. Ghiduk, "An empirical comparison of the efficiency and effectiveness of genetic algorithms and adaptive random techniques in data-flow testing," *IEEE Access*, vol. 8, pp. 12884–12896, 2020.

[9] M. Jacovic, K. Juretus, N. Kandasamy, I. Savidis, and K. R. Dandekar, "Physical layer encryption for wireless OFDM communication systems," *Journal of Hardware and Systems Security*, vol. 4, no. 3, pp. 230–245, 2020.

[10] J. Zong, A. A. Hajomer, L. Zhang, W. Hu, and X. Yang, "Real-time secure optical OFDM transmission with chaotic data encryption," *Optics Communications*, vol. 473, 2020.

[11] J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 22787–22808, 2018.

[12] Q. Chen, M. Bi, X. Fu et al., "Security scheme in IMDD-OFDM-PON system with the chaotic pilot interval and scrambling," *Optics Communications*, vol. 407, pp. 285–289, 2018.

[13] R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map," *Information Security Journal: A Global Perspective*, vol. 25, no. 4-6, pp. 162–179, 2016.

[14] A. Alsufyani, R. Alroobaea, and A. Ahmed, "Detection of single-trial EEG of the neural correlates of familiar faces recognition using machine-learning algorithms," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, pp. 2855–2860, 2019.

[15] X. Yu, X. Zhou, C. Xu, L. Wang, D. Shen, and H. Zhou, "A NOMA-based quantum key distribution system over Poisson atmospheric channels," in *IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Waikoloa, HI, USA, 2019.

[16] Y. Wu, Y. Yu, Y. Hu, Y. Sun, T. Wang, and Q. Zhang, "Channel-based dynamic key generation for physical layer security in OFDM-PON systems," *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–9, 2021.