

# Low complexity physical layer security approach for 5G internet of things

Kiran Vinayak Shanbhag<sup>1,2</sup>, Dayakshini Sathish<sup>2</sup>

<sup>1</sup>Department of Electronics and Communication Engineering, Anjuman Institute of Technology and Management, Bhatkal, India

<sup>2</sup>Department of Electronics and Communication Engineering, St Joseph Engineering College, Mangalore, India

## Article Info

### Article history:

Received Feb 22, 2022

Revised Dec 23, 2022

Accepted Dec 28, 2022

### Keywords:

Encryption

Internet of things

Orthogonal frequency division multiple access

Physical layer security

Subcarrier diversity

## ABSTRACT

Fifth-generation (5G) massive machine-type communication (mMTC) is expected to support the cellular adaptation of internet of things (IoT) applications for massive connectivity. Due to the massive access nature, IoT is prone to high interception probability and the use of conventional cryptographic techniques in these scenarios is not practical considering the limited computational capabilities of the IoT devices and their power budget. This calls for a lightweight physical layer security scheme which will provide security without much computational overhead and/or strengthen the existing security measures. Here a shift based physical layer security approach is proposed which will provide a low complexity security without much changes in baseline orthogonal frequency division multiple access (OFDMA) architecture as per the low power requirements of IoT by systematically rearranging the subcarriers. While the scheme is compatible with most fast Fourier transform (FFT) based waveform contenders which are being proposed in 5G especially in mMTC and ultra-reliable low latency communication (URLLC), it can also add an additional layer of security at physical layer to enhanced mobile broadband (eMBB).

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Kiran Vinayak Shanbhag

Department of Electronics and Communication Engineering, Anjuman Institute of Technology and Management

Bhatkal, Karnataka, 581 320, India

Email: shanbhagkiranv@anjuman.edu.in

## 1. INTRODUCTION

Fifth generation (5G) networks support three major application scenarios. While enhanced mobile broadband (eMBB) is all about supporting high bandwidth applications on computationally capable devices, the scenario is completely different in the other two [1]. Massive machine-type communications (mMTC) mainly aims at large-scale machine communication scenarios in the internet of things (IoT) where a very large number of mMTC devices may connect to a base station (BS) carrying out not so bandwidth extensive applications such as sensing, metering, and monitoring, focusing mainly on energy efficiency [2]. Ultra-reliable and low-latency communications (URLLC) meanwhile covers scenarios involving autonomous vehicles, industrial automation, remote surgery and similar services, which require millisecond level end-to-end delay and reliability guarantee.

Current higher layer cryptographic approaches are a concern for IoT applications featured in mMTC as the devices are expected to be low power consuming, possess limited storage and relatively limited computing capabilities. Hence, the complicated encryption/decryption algorithms or protocols cannot be applied. Moreover the complex encryption techniques may even worsen the latency in URLLC applications [3], [4]. Also, there is vulnerability of the lower layers being subjected to many passive and active attacks.

Security countermeasures from the physical layer are lightweight, offer protection to the wireless transmission and therefore are advantageous over conventional upper layer encryption-based security primitives [5], [6]. Here we propose a novel shift based physical layer security (PLS) method compatible with fast Fourier transform (FFT) based multicarrier modulation (MCM) techniques which can secure IoT communication and/or add additional layer of security to schemes that employ security at higher layers. It does so with the least complexity and further exploits the subcarrier diversity adding to the performance gain.

## 2. BACKGROUND AND MOTIVATION

This section is divided into 5 topics. Section 2.1 discusses the relevant areas where orthogonal frequency-division multiplexing (OFDM) based PLS schemes may find need, compatibility and suitability. Section 2.2 surveys the approaches in the context so far and its renewed interest owing to current 5G scenario. Section 2.3 lists the merit of shift-based security approach against the scrambling/interleaving approaches in terms of speed, complexity and robustness. Section 2.4 discusses the possible exploitation of subcarrier diversity. Section 2.5 lists the overall contributions of this study.

### 2.1. Orthogonal frequency-division multiplexing based multicarrier modulation schemes

OFDM encodes a single high bandwidth frequency selective data into several low bandwidth frequency flat channels, modulating overlapping but orthogonal carriers, thus providing robust fading resilience. The ease of implementation of the FFT algorithm on the receiver side, inverse FFT (IFFT) on the sender side [7], [8] makes it a preferred contender over other fading resilient techniques. It was initially employed in wireless local area network (LAN) IEEE 802.11a. Then its multiple access version orthogonal frequency division multiple access (OFDMA), was part of 3GPP long term evolution (LTE). The latest wireless LAN standard IEEE 802.11ax employs OFDMA. Narrow band IoT (NB-IoT), a specialized LTE based technology meant for IoT too employs OFDM [9]. It still continues to be the preferred carrier for 5G eMBB along with its single carrier version single-carrier FDMA (SC-FDMA) for low peak-to-average power ratio (PAPR) uplink transmission. What is more interesting is the fact that even the non-orthogonal multiple access (NOMA) schemes being proposed for 5G mMTC and URLLC, which have low latency, massive connectivity as the primary requirement, involve OFDM like IFFT, FFT operations at transmitter and receiver respectively. These schemes include sparse code multiple access (SCMA), interleave division multiple access (IDMA), and resource spread multiple access (RSMA) [10]. Hence OFDM based security scheme, which occur at the physical layer itself, should be broadly applicable to most MCM based multiple access schemes, be it orthogonal or non-orthogonal.

### 2.2. Approaches so far

Ever since the need for PLS is felt, several approaches have been proposed, ranging from securing OFDM based physical layer in wireless Ethernet IEEE 802.11a to the current NOMA schemes for 5G mMTC. Though traditional approaches for PLS mostly include beamforming with directional antennas towards desired source, exploiting the knowledge of channel state information (CSI), and introducing artificial noise against eavesdropper [11] this paper confines its study to the techniques involving OFDM based transceivers with multicarrier nature. But most of these methods are suitable for eMBB applications due to the complexity involved whereas for IoT applications, they may not be suitable. In [12] an approach to encrypt the data during OFDM modulation, by multiplying the quadrature amplitude modulation (QAM) symbols by a generalized key stream sequence before the IFFT stage, was proposed in year 2010. Several other studies [13], [14] proposed the encryption after the IFFT stage of OFDM. Most of these schemes were meant for securing mainly wireless data transmission and power line communication, without much emphasis on power budget and computational complexity. The application scenarios during the period did not really necessitate the widespread adaption of such schemes for cellular communication as conventional higher layer security schemes like advanced encryption standard (AES) were considered much robust. Moreover, OFDM was not part of cellular communication before LTE. But the introduction of massive connectivity applications like IoT with constraints on the nodes, the need for lightweight PLS has once again garnered attention [15] since the prohibitory nature of computational capabilities of sensor nodes does not allow the use of traditional encryption approaches. Several possibilities have been proposed in the direction but the compatibility of OFDM based security schemes with diverse application scenarios in 5G is making the researchers rethink on the possibility. The approaches have included several methods ranging from scrambling/interleaving the IFFT coefficients [16], [17], changing the FFT size in pseudorandom manner and even changing the cyclic prefix along with FFT size in physical layer. Secure obfuscating of the interleaver stage and obfuscating the constellation mapping stage of OFDM pipeline are proposed respectively in references [18], [19].

### 2.3. Shift vs. interleaving/scrambling based PLS

Latency is another factor which plays a major role and has several application scenarios in URLLC. Several studies have highlighted the impact of conventional encryption on latency. In [20] a need for a lightweight security algorithm for IoT keeping in mind the low latency communication is emphasized. Study [21] mentions the need to optimize PLS as a means to reduce the delays in authentication since even the hardware based secure scramblers/interleavers in physical layer, either adds to power consumption or delays. As a solution, the use of random rotations instead of interleaving is proposed in this study which is something new which has not been tried yet by any researchers. The method will have less complexity as the effort in generating large number of random address pointers is replaced by only a single initial secure address, followed by just pointer increments. This results in relatively low complexity hardware, low power consumption and reduced delays in the process as per IoT device requirements.

### 2.4. Exploitation of subcarrier diversity

Due to the diverse nature of the channel each of the frequency subcarriers after IFFT stage in OFDM, experience different channel conditions and few are likely to suffer deep fades [22]. Assuming situations where channel conditions seldom change, a few of the subcarriers might still be repeatedly subjected to fading over a time duration lasting several symbols or subframes, burdening the error control coding stage and further increase of FFT points may not be a possibility due to standardization. Just like the way interleavers would tackle burst errors in incoming data, rearrangements of coefficients after IFFT stage would make sure that fades are distributed throughout spectrum to nullify the fading effect. Several schemes have been proposed which tend to improve the performance of OFDM based multicarrier by utilizing this diversity feature among the subcarriers by periodic systematic interleaving/rearrangement of subcarrier data at slot, frame level [23], [24].

### 2.5. Contributions of the paper

Based on the issues discussed in above sections, a PLS scheme is proposed here. The approach is suitable for IoT applications and is compatible with a variety of MCM waveform contenders. The scheme is relatively simple and can mitigate deep channel fades. Listed below are the contributions of the paper:

- a. Proposal of a novel low complexity PLS approach for IoT scenarios which is compatible with most of the IFFT/FFT based physical layer waveform contenders for 5G and beyond.
- b. Proposal for the use of pseudorandom rotations as means of security as opposed to all earlier scramble/interleaving approaches with several robustness and computational advantages.
- c. Demonstration of the ability of the scheme to securely transmit data and frequency diversity utilization advantage in channel scenarios experiencing different fades among the subcarriers with bit error rate (BER) performance improvement.

## 3. PROPOSED SCHEME

Here we present a simple, yet effective PLS scheme which employs pseudorandom rotate or circular shift operations instead of interleaving/scrambling the subcarrier coefficients after the IFFT stage of multicarrier modulation based scheme like OFDM, making it unintelligible for the unauthorized receivers. The rotate operations can be computationally simpler yet secure enough so that an authorized receiver with knowledge of exact sequence of shift counts along with the initial shift value can receive the data. The rotations, when carried at a rate higher than channel frequency response variations, can also provide channel frequency diversity increasing the BER performance. The intention of the paper is to suggest this rotation based security approach with diversity advantage, which is compatible with multicarrier modulation schemes which are part of existing and futuristic physical layer. The possibility of employing such scheme as a standalone security scheme, especially for multimedia data such as audio and images is also to be explored as they usually involve either a FFT or discrete cosine transform (DCT) operation. Given the not so stringent compatibility requirement with existing hardware, and with the uniqueness in pseudonoise (PN) sequence polynomial, the initial shift count and the size of FFT, the scheme can secure the multimedia data in transit.

### 3.1. Subcarrier frequency diversity

Consider a scenario where a channel has a frequency response which is non uniform throughout the region with few subcarrier frequencies experiencing deep fades. Depicted in Figure 1, is the different low bandwidth subcarriers after IFFT stage, shown along with their respective channel gains at different instants of time. It is assumed that the channel will remain stationary for a period spanning several symbols. As we can see at time instant  $t_1$  subcarrier  $X_4$  experiences deep fade but at the same time subcarrier  $X_0$  is not. At instant  $t_2$ , when we circularly shift the entire subcarrier spectra by factor 4, assuming a relatively slowly

varying channel, subcarrier  $X_4$  experiences no fade but  $X_0$  does. Thus, the diversity is utilized to minimize effect of fading on only a particular set of subcarriers; by averaging the impact. This diversity scheme can be made secure by making sure that only authorized receivers know the sequence with which shifts are carried out at different time instants, at the transmitter. A linear feedback shift register (LFSR) with unique polynomial arrangement can be used to generate unique shift factors that are pseudorandom in nature at transmitter, making the data unintelligible for unauthorized receivers without the knowledge of the LFSR arrangement, more importantly, the initial shift count or the 'seed' [25]. This information i.e., the polynomial along with the initial seed can be used as the 'key' to secure the transmission at physical layer. The same thing holds good for interleaving too but the simple shift operation can provide the necessary diversity. The complex randomization of entire sequence as in interleaving is a necessity to avoid burst errors in time domain before IFFT stage but here only shifts are sufficient. While there have been several studies which have utilized a secure scrambling and interleaving of coefficients, both before and after the IFFT stage as part of PLS, we propose secure shifts as an alternative, particularly to interleaving, for the reasons discussed in next subsection.

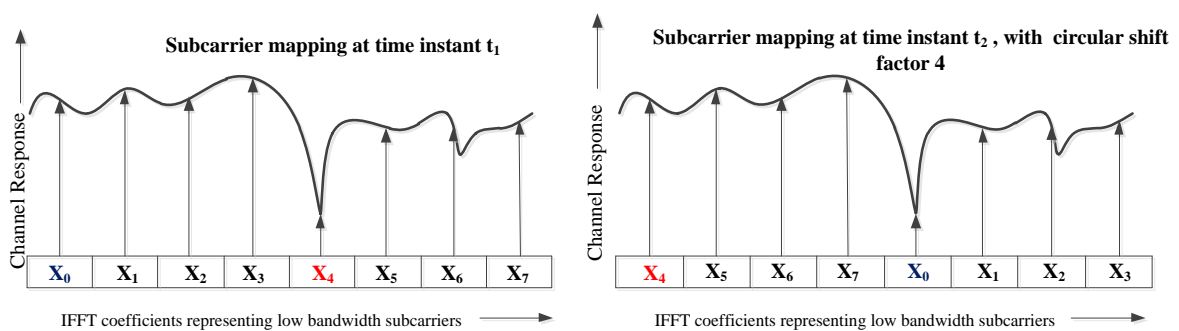


Figure 1. Illustration of channel response and its effect on subcarrier mapping. As we can see at time instant  $t_1$  subcarrier  $X_4$  experiences deep fade but  $X_0$  does not. At  $t_2$ , with coefficient shift, it is vice versa

### 3.2. Shift vs. interleaving vs. scrambling

As compared to shifts, interleaving and scrambling operations are fairly complex. The interleaving process usually involves specialized arithmetic logic unit (ALU) for address pointer generation based on lookup table, along with memory requirement for temporary storage [26]. Scrambling, on the other hand involves mathematical computations. These factors either adds to latency if micro program-based approach is used or consumes additional power if hardware-based approach is used. Both these are against the requirements for limited capability IoT devices. Hence the approach to rotate the subcarrier indices is suggested in this paper. The method is also called as circular shift. While it manages to frequently randomize the subcarrier locations to provide diversity, it does not need a complicated hardware as interleaver/scrambler. An interleaving process involves mapping the values from a unique source location to unique destination location, with each destination address being generated on the fly. But a rotate instruction simply needs an increment by factor one to generate address of subsequent locations, once the initial shift count i.e., seed is obtained. Exception case would be a modulus operation in case the index exceeds maximum value. Figure 2 compares interleaving with circular shift. From robustness point of view too, the shift method in fact is much better. In secure interleaving, the choice of polynomials is limited as register arrangement size is fixed to interleave/scramble entire coefficient set and choosing any lower value results in a part of subcarrier coefficient arrangement unchanged. Whereas in shifting, any size of LFSR lesser or even more than  $N$  will shift entire register coefficients, increasing the possible combinations drastically making it difficult for eavesdroppers. Say for a register of size  $N$  to be interleaved, there can only be an  $N$  bit interleaver polynomial, leaving the attacker of guessing the initial seed along with few standard polynomials of same width. But for shift, the possibilities are far more.

### 3.3. Pseudorandom number generator

To avoid unauthorized decoding, shift sequence needs to be pseudorandom in nature. An PN sequence with polynomial  $x^8 + x^6 + x^5 + x^4 + 1$  is shown in Figure 3 and it is few shift factors with initial value '10000000' i.e. 128 are 128, 198, 11, 255, 132, 242, 85, 7 and so on [27]. This 8-bit LFSR has a period length of 255. In general, an ' $N$ ' bit LFSR arrangement with properly chosen polynomials can produce almost random like sequence with period  $2^N - 1$ . Larger size PN sequence generator with higher order also

means a large period after which the shift factors repeat, making it more secure. For the shift factor greater than  $2^N$ , modulo  $2^N$  value can be used which will lie value within the range, giving more options in choosing the sequence generator polynomials with higher orders and the initial values adding to the security aspects.

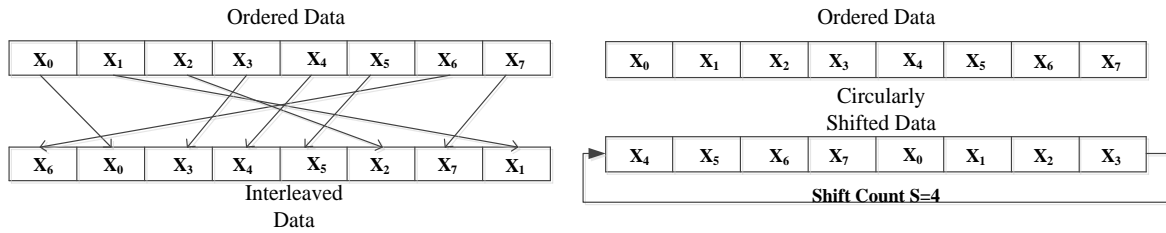


Figure 2. Illustration of interleaver and circular shifter operation

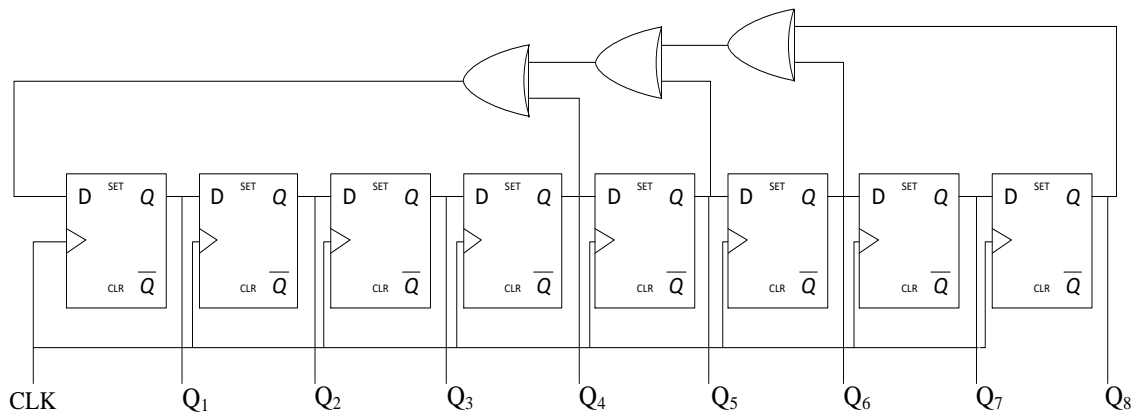


Figure 3. An 8-bit PN sequence based random shift factor generator with polynomial  $x^8 + x^6 + x^5 + x^4 + 1$

#### 4. METHOD

In the proposed scheme, the coefficients obtained after the IFFT stage i.e., are securely rotated or circularly shifted. Figure 4 shows two of the possible ways it can be done in the case of 5G NR with normal cyclic prefix, *numerology* = 1, in which a subframe has 2 slots in it [28]. Each slot in turn contains 14 OFDM symbols. In first case the IFFT coefficients are being shifted in frequency, once every OFDM symbol. For 2<sup>nd</sup> symbol, the coefficients are shifted by factor 2 and for 3<sup>rd</sup> symbol; the coefficients are shifted by factor 8 and so on. In second case, the coefficients are shifted only once per slot. For slot 3, all 14 symbols are shifted by factor 8 and for slot 4; all symbols are shifted by factor 6. In both cases, one can observe the diverse subcarrier channel characteristics experienced over time by the symbols as indicated by different colors. The other possibilities may include performing the shifts once every subframe also depending on the required robustness and channel conditions. Owing to the similar numerology in case of OFDMA/SC-FDMA in LTE/5G, the scheme can be easily adapted under different scenarios. The authorized receiver is assumed to have exact knowledge of the LFSR used at transmitter along with the initial seed and will introduce a shift in opposite direction at the receiver just before the FFT stage to recover original data by generating the exact shift sequence.

Figure 5 shows the implementation of the proposed scheme as applied to a baseline OFDM block [29] for simulation purpose. Except for the circular shifter block along with sequence generator indicated by shaded ones, rest of the blocks pertain to a simple QAM based 1,024-point OFDM with cyclic prefix. The shaded block in the transmitter after the IFFT stage is a circular shifter which rotates all the IFFT coefficients by factor ‘S’, which is generated by a PN sequence generator. The shifting may happen once every symbol or subframe or frame-based agreement between authorized entities. At receiver, the same PN sequence generator used, with same initial seed but the shifting in opposite direction to restore the coefficient arrangement before FFT operation. All 1,024 subcarriers are used as data subcarriers for the simulation purpose. The simulations were carried out on a sample image data and a random binary data set using MATLAB. 4 QAM modulation was used here along with 1,024-point IFFT with cyclic prefix length of 72.

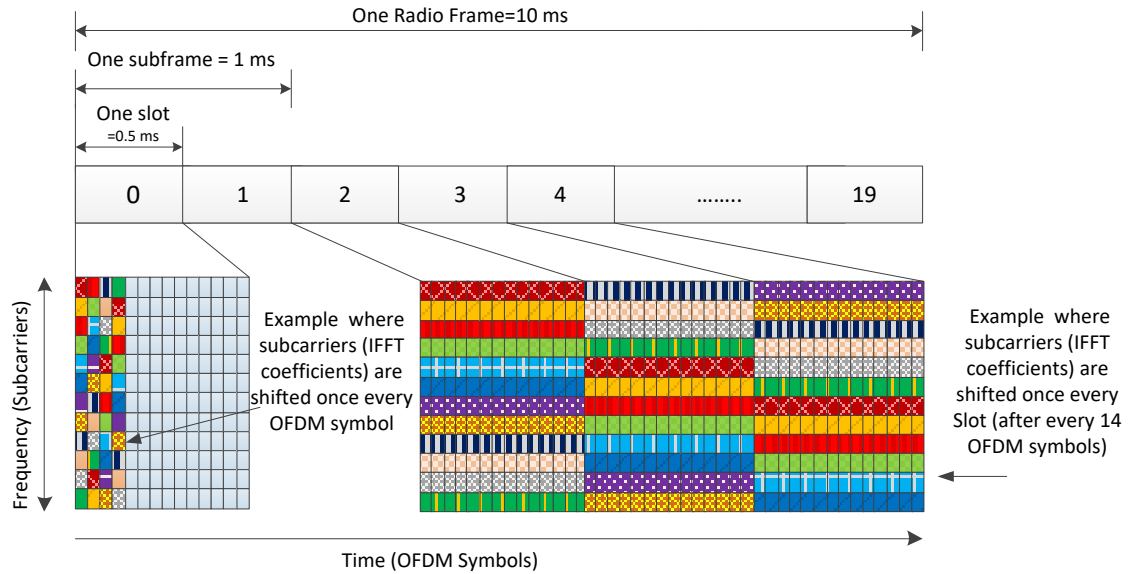


Figure 4. A subcarrier shifting arrangement in the case of 5G NR. While the coefficients are shifted once every symbol in slot 0 vertically along frequency axis, they are shifted once every slot in case of slots 2, 3, 4

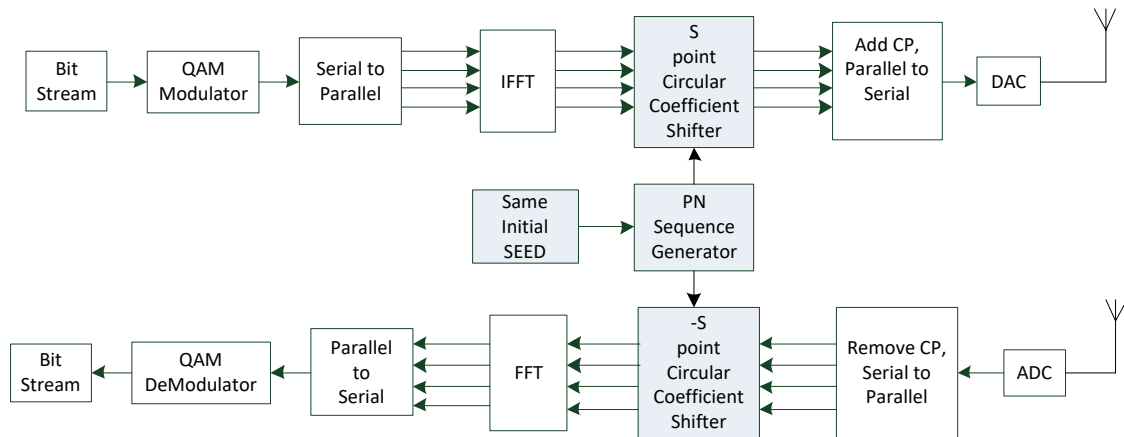


Figure 5. Scheme showing generalized OFDM based transmission/reception with proposed PLS scheme

**5. RESULTS AND DISCUSSION**

First, a  $256 \times 256$  greyscale Lena image as shown in Figure 6(a) was converted into one dimensional symbol stream by combining 2 bits to be suitable for 4-QAM and broken into chunks of 1,024 and fed to the IFFT block. A shift factor generator based on PN sequence polynomial as earlier mentioned in section 3.3 was used to perform circular shift once every OFDM symbol, resulting in the encrypted image as shown in Figure 6(b). At receiver, same circular shifter was used but with shifts in opposite direction and knowledge of initial seed was assumed to recover the image as in Figure 6(c).

The results exhibit the ability of the method to secure the data as well as the intact recovery as observed in all three images. No noise addition was done as the simulation block lacked error control mechanism. An experimental bit error rate (BER) performance comparison was carried between the baseline OFDM scheme and the proposed scheme in presence of additive white gaussian noise (AWGN) for different signal to noise ratios (SNR) to assess any possible impact of the secure shifting process on recovered data. AWGN channel along with a 3 path Rayleigh fading and Doppler spread  $fd$  was assumed.

Figure 7(a) shows the BER performance comparison curves of both the systems. There is not much difference in performance when  $fd$  value was low, as both the curves almost overlapped for  $fd=0.001$ . But when  $fd$  was changed to 0.05, it was found that there is a gain in BER performance at higher signal to noise ratios as indicated in the Figure 7(b). While the proposed scheme performed at par with baseline OFDM in

former case, it outperformed in the latter scheme when fading was worse by utilizing the diversity advantage. The analytical justification for the gain attained it to be explored further. These encouraging results make the proposed scheme i.e., including a pseudorandom subcarrier shifting module in most of the IFFT/FFT based schemes a necessary enhancement in most OFDM based architecture, to not only achieve an additional layer of security at physical layer but also a means of achieving better BER performance gain in poor channel scenarios.

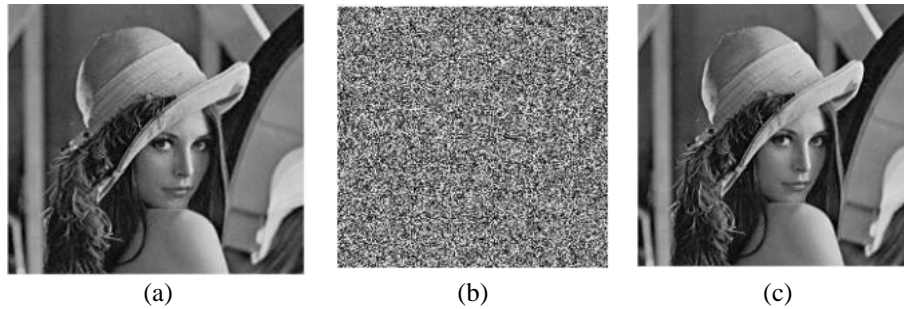


Figure 6. Demonstration of the encryption and the recovery of original image after decryption (a) original  $256 \times 256$  grey scale image of lena.bmp, (b) the encrypted image, and (c) decrypted image

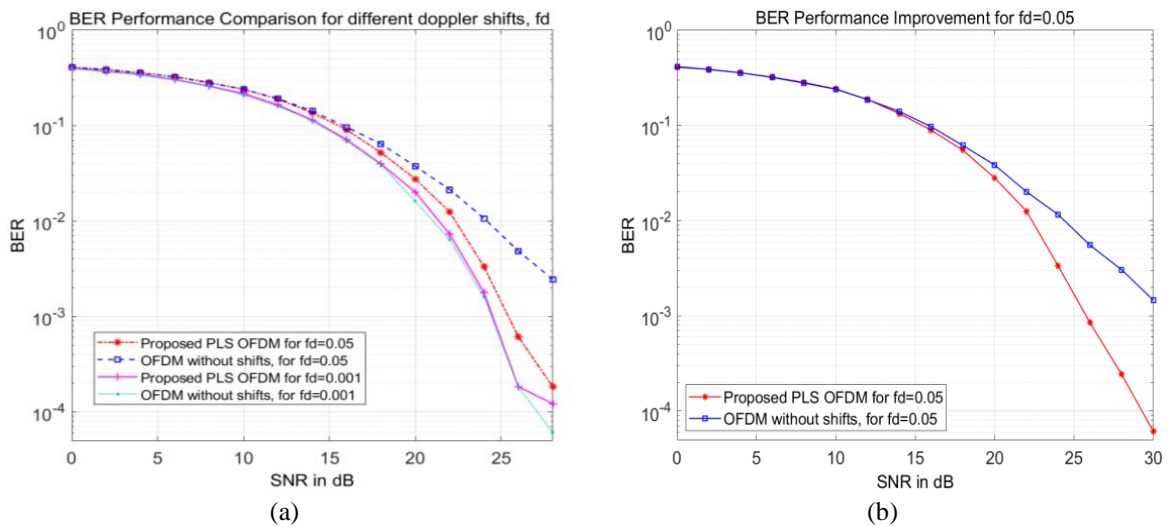


Figure 7. Demonstration of subcarrier diversity advantage of the scheme by BER performance comparison (a) BER comparison of the proposed scheme with baseline OFDM at two different Doppler shifts and (b) Improved BER performance at higher Doppler shift of  $fd=0.05$  as compared to similar results at  $fd=0.001$

Overall, in this study, the focus has been on securing the transit data by shifting the IFFT coefficients in pseudorandom manner instead of the scrambling/interleaving approach that too with minimum changes to existing multicarrier transceiver architecture, especially for IoT devices with low power, low computational capability and achieving diversity gain in the process. In below subsections some unique features of the scheme are discussed. These include the robustness, flexibility and the versatility of the scheme for different application areas.

### 5.1. Robustness against brute force attack

The exact LFSR polynomial along with seed value forms the secret key here. For any intentional attacker, the task would be two-fold. First would be guessing the length of the LFSR along with polynomial arrangement which can be any number/any of the standard combinations as stated earlier, only limited by hardware and power budget of device. Remember, as rotate operations are being used,  $N$  can be as large as possible unlike scrambling/interleaving case where LFSR size is bound to match data segment size. Second

would be acquiring the seed, which can be any number from  $2^N - 1$  combinations. Overall, the complexity of the permutations would be of the order  $\geq 2^N - 1!$  which is relatively much larger than most PLS schemes proposed so far. Table 1 summarizes the complexity. An additional complexity would involve guessing the frequency with which the shifts are being applied, be it once every symbol, every slot or subframe in fixed or in a random manner based on another polynomial with another seed value in the time domain.

### 5.2. Comparative computational complexity

As mere shift operations are used, the computational complexity will only be limited to incrementing pointer addresses once initial seed is decided. This is relatively simple as compared to the scrambling or interleaving based schemes. While scrambling schemes require one or more stages of XOR operation, interleaving based schemes require complex address generation units at both transmitter and receiver or at least a look up table for all possible combinations.

Table 1. Comparative polynomial and seed permutations, along with computational overhead

Randomizing scheme for N coefficients	Generator polynomial permutations	Initial seed permutations	Computational overhead
Scrambling	$2^N - 1$	$2^N - 1$	EX-OR operations
Interleaving	$2^N - 1$	$2^N - 1$	Random address generation
Circular Shift	$\geq 2^N - 1!$	$\geq 2^N - 1!$	Address increments/occasional modulus operations

### 5.3. Flexibility of the application to different platforms

As cited earlier most of the modulation schemes, be it OMA or NOMA, are IFFT/FFT based and this scheme can be readily applied to most of these cellular schemes with minimum changes to the architecture [30]. This is true even for latest broadband wireless enterprise networks like Wi-Fi 6 [31] which uses OFDMA. It can add an additional security at physical layer for most of bandwidth extensive schemes in eMBB. It can also be considered as a standalone security scheme in edge cameras for privacy protection, for multimedia applications as they involve either DFT or discrete cosine transform (DCT) in preliminary processing stage [32], [33]. While the encryption involves the need for additional transform calculation overhead at transmitter/receiver, the brute force attack will also be equally complicated as it now involves size of FFT as additional key. The trial and error for attacker would now involve trying out all possible FFT sizes adding to the complexity.

### 5.4. The technique as a standalone diversity scheme

The circular subcarrier shift approach can be used as diversity scheme alone in physical uplink shared channel (PUSCH) as similar approaches have been proposed involving rearrangement of coefficients but applied to resource blocks (RB) as a whole mostly [34], as a means of diversity. But this scheme can provide more flexibility in terms of hop intervals and frequency range as compared to the latter. The shift intervals can be either once per symbol or slot or subframe based on the available channel state information in time domain and either at coefficient level or RB level in frequency domain, while being secure in the process.

## 6. CONCLUSION





In this paper we proposed a novel shift based PLS scheme with diversity advantage, especially for low power, low capacity IoT devices employing FFT based multicarrier modulation schemes. It was done by circularly shifting the coefficients with pseudorandom shift counts after IFFT operation. The unique shift sequence along with the initial seed would serve as the secure key. The computational/robustness advantages provided by the shifting approach as opposed to scrambling/interleaving approaches were summarized. The simulations demonstrated the scheme's potential in terms of security and also the BER performance improvement in case of fading channels. The compatibility of the scheme with most of the FFT based MCM contenders presently being proposed for 5G mMTC, URLLC and beyond makes it more attractive. As against most of the PLS approaches proposed so far, the shift-based obfuscation approach is relatively lighter and might find further attention among the researcher community provoking further analytical study on the robustness and diversity aspects of the scheme. Not only for IoT, but the method can also add an additional layer of security/diversity at the physical layer to most cellular and enterprise communication schemes employing security at higher layers. The scheme can also be considered for securing most of the multimedia or surveillance data, as they typically involve some sort of FFT or DCT operation in processing stages, so as to increase robustness against attacks.







## REFERENCES

- [1] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A survey on 5G usage scenarios and traffic models," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 905–929, 2020, doi: 10.1109/COMST.2020.2971781.
- [2] C. Feng and H.-M. Wang, "Secure short-packet communications at the physical layer for 5G and beyond," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 96–102, Sep. 2021, doi: 10.1109/MCOMSTD.121.2100028.
- [3] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018, doi: 10.1109/ACCESS.2017.2779146.
- [4] S. Wang, W. Li, and J. Lei, "Physical-layer encryption in massive MIMO systems with spatial modulation," *China Communications*, vol. 15, no. 10, pp. 159–171, Oct. 2018, doi: 10.1109/CC.2018.8485478.
- [5] E. Jorswieck, L. Lai, W.-K. Ma, H. V. Poor, W. Saad, and A. L. Swindlehurst, "Guest editorial: signal processing for wireless physical layer security," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1657–1659, Sep. 2013, doi: 10.1109/JSAC.2013.130901.
- [6] Y. M. Al-Moliki, M. T. Alresheedi, Y. Al-Harhi, and A. H. Alqahtani, "Robust lightweight-channel-independent OFDM-based encryption method for VLC-IoT networks," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4661–4676, Mar. 2022, doi: 10.1109/JIOT.2021.3107395.
- [7] A. Goldsmith, *Wireless communications*. Cambridge University Press, 2005.
- [8] A. Ghosh, J. Zhang, J. G. Andrews, and R. Muhamed, *Fundamentals of LTE*. Pearson Education, 2010.
- [9] S. Popli, R. K. Jha, and S. Jain, "A survey on energy efficient narrowband internet of things (NB-IoT): architecture, application and challenges," *IEEE Access*, vol. 7, pp. 16739–16776, 2019, doi: 10.1109/ACCESS.2018.2881533.
- [10] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, pp. 2294–2323, 2018, doi: 10.1109/COMST.2018.2835558.
- [11] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019, doi: 10.1109/JIOT.2019.2927379.
- [12] D. Dzung, "Data encryption on the physical layer of a data transmission system," Google Patents, 2010.
- [13] A. Al-Dweik and C. Y. Yeun, "Chaotic cryptography for OFDM based communications systems," Google Patents, 2014.
- [14] F. Huo and G. Gong, "A new efficient physical layer OFDM encryption scheme," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, Apr. 2014, pp. 1024–1032, doi: 10.1109/INFOCOM.2014.6848032.
- [15] J. Zhang, T. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the internet of things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, Aug. 2017, doi: 10.3390/e19080420.
- [16] M. M. Banat, J. Bas, and A. A. Dowhuszko, "Improved physical-layer security for OFDM using data-based subcarrier scrambling," in *2021 IEEE Globecom Workshops (GC Wkshps)*, 2021, pp. 1–6, doi: 10.1109/GCWkshps52748.2021.9682170.
- [17] A. Alsadi and S. Mohan, "A new frequency hopping scheme to secure the physical layer in the internet of things (IoT)," in *2020 Wireless Telecommunications Symposium (WTS)*, Apr. 2020, pp. 1–8, doi: 10.1109/WTS48268.2020.9198722.
- [18] J. Chacko *et al.*, "Securing wireless communication via hardware-based packet obfuscation," *Journal of Hardware and Systems Security*, vol. 3, no. 3, pp. 261–272, Sep. 2019, doi: 10.1007/s41635-019-00070-0.
- [19] I. Bang and T. Kim, "Secure modulation based on constellation mapping obfuscation in OFDM based TDD systems," *IEEE Access*, vol. 8, pp. 197644–197653, 2020, doi: 10.1109/ACCESS.2020.3034633.
- [20] Q. Qi, X. Chen, C. Zhong, and Z. Zhang, "Physical layer security for massive access in cellular internet of things," *Science China Information Sciences*, vol. 63, no. 2, Feb. 2020, doi: 10.1007/s11432-019-2650-4.
- [21] L. Sun and Q. Du, "A review of physical layer security techniques for internet of things: challenges and solutions," *Entropy*, vol. 20, no. 10, Sep. 2018, doi: 10.3390/e20100730.
- [22] S. C. Yang, *OFDMA system analysis and design*. Artech House, 2010.
- [23] Y. Ida and T. Matsumoto, "Interleaved Block subcarrier allocation and power combination for frequency symbol spreading multiuser diversity OFDMA," *EURASIP Journal on Wireless Communications and Networking*, no. 1, Dec. 2022, doi: 10.1186/s13638-022-02131-5.
- [24] J. K. Ahn, N. Y. Yu, Y. W. Yun, K. J. Kim, and H. W. Park, "Frequency hopping pattern and method for transmitting uplink signals using the same," Google Patents, 2014.
- [25] M. Luby, *Pseudorandomness and cryptographic applications*. Princeton University Press, 1996.
- [26] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128–143, Feb. 2006, doi: 10.1109/TMC.2006.16.
- [27] W. J. Hurd, "Efficient generation of statistically good pseudonoise by linearly interconnected shift registers," *IEEE Transactions on Computers*, vol. C-23, no. 2, pp. 146–152, Feb. 1974, doi: 10.1109/T-C.1974.223877.
- [28] 3GPP TS 38.211, "NR; Physical channels and modulation," 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, 2017.
- [29] T. Poornima, K. Dhinesh, and R. Sudhakar, "Waveform candidates for 5G mobile communications," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT)*, May 2017, pp. 856–860, doi: 10.1109/RTEICT.2017.8256719.
- [30] Y. Yuan *et al.*, "Non-orthogonal transmission technology in LTE evolution," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 68–74, Jul. 2016, doi: 10.1109/MCOM.2016.7509381.
- [31] S. Avallone, P. Imputato, G. Redieteb, C. Ghosh, and S. Roy, "Will OFDMA improve the performance of 802.11 Wi-Fi networks?," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 100–107, Jun. 2021, doi: 10.1109/MWC.001.2000332.
- [32] A. H. Fitwi, Y. Chen, and S. Zhu, "Enforcing privacy preservation on edge cameras using lightweight video frame scrambling," *IEEE Transactions on Services Computing*, p. 1, 2021, doi: 10.1109/TSC.2021.3135352.
- [33] A. Fitwi, Y. Chen, and S. Zhu, "Lightweight frame scrambling mechanisms for end-to-end privacy in edge smart surveillance," *IET Smart Cities*, vol. 4, no. 1, pp. 17–35, Mar. 2022, doi: 10.1049/smc2.12019.
- [34] T.-K. Le, U. Salim, and F. Kaltenberger, "An overview of physical layer design for ultra-reliable low-latency communications in 3GPP releases 15, 16, and 17," *IEEE Access*, vol. 9, pp. 433–444, 2021, doi: 10.1109/ACCESS.2020.3046773.

**BIOGRAPHIES OF AUTHORS**

**Kiran Vinayak Shanbhag**     received his BE degree in Electronics and Communication Engineering from Anjuman Institute of Technology and Management, Bhatkal, Karnataka, India in 2005 and received his MTech degree in Communication Engineering from National Institute of Technology Karnataka, Surathkal, India in 2010. He is currently pursuing Ph.D. in Department of Electronics and Communication Engineering at St Joseph Engineering College, Mangaluru, India. His research interests include digital signal processing for communication, multicarrier modulation schemes, and MIMO radar. He has 4 journal papers and 4 conference papers to his credit. Currently he is assistant professor at Department of Electronics and Communication Engineering, Anjuman Institute of Technology and Management, Bhatkal, Karnataka, India. He can be contacted at email: shanbhagkiranv@anjuman.edu.in.



**Dayakshini Sathish**     obtained her BE Degree from Mangalore University, MTech from Visvesvaraya Technological University (VTU) and Ph.D. from Manipal Academy of Higher Education (MAHE) Manipal. She has got nearly 24 years of teaching/research experience in the field of Electronics and Communication Engineering and is currently working as Professor and Head at the Department of Electronics and Communication Engineering, SJEC Mangaluru. Her areas of interest include biomedical signal and image processing, machine learning, deep learning, and communication systems. She has published ten research articles in reputed international journals. She has attended various international conferences abroad and in India. She is a regular reviewer of reputed international journals published by IEEE, Elsevier, Springer, and Wiley Publishers. She can be contacted at email: dayakshini@sjec.ac.in.