IJASRM

International Journal of Advanced Scientific Research and Management, Volume 6 Issue2, Feb 2021

www.ijasrm.com

ISSN 2455-6378

A SimpleEncryption Approach to 5G Multicarrier Based Waveform Utilizing Subcarrier Frequency Diversity with Improved BER Performance

Kiran V Shanbhag[1] and Savitha H M[2]

[1] Dept of Electronics and Communication
Anjuman Institute Technology and Management
Bhatkal, Karnataka, India-581 320

[2]Department of Electronics and Communication
St Joseph Engineering College, Mangaluru, India-575028

Abstract

The security in 5G Internet of Things (IoT) is considerably different as the low power constraints and complexity features of many IoT devices are limiting the use of conventional cryptographic techniques. The fast Fourier transform (FFT) based multicarriers like orthogonal frequency division multiple access (OFDMA) and the similar non orthogonal counterparts are the preferred waveforms in 5G due to their resilience to fading and ease of implementation. Here a scheme to chaotically rearrange the frequency subcarriers is proposed which will not only provide a relatively simple physical layer security (PLS) with minute changes in existing OFDM based transceiver as per the low complexity, low power requirements of IoT but also improve the bit error rate (BER) performance by utilizing the diverse nature of the channel. The scheme provides an alternate approach to conventional higher layer security, by doing so at physical layer which will be suitable for most FFT based waveforms which have been proposed in 5G especially narrow band IoT (NB IoT) , massive machine-type communication (mMTC) and ultra-reliable low latency communicationis (URLLC).maintain uniformity in the final print version of the journal. Both form and content of the paper has to be as per these guidelines else your paper will not be published even though its content has been accepted.

Keywords:*5G, massive machine-type communication, physical layer security, NB IoT, encryption*

1. Introduction

5G network is expected to support massive user connections and exponentially increasing wireless services, which makes network security unprecedentedly important. 5G networks support three major applications, namely enhanced mobile broadband (eMBB), massive machine-type communications (mMTC) and ultra-reliable and low-latency communications (URLLC)[1]. Current network transmission security technologies rely heavily on the cryptographic approaches at the upper layer of the protocol stack, which may be afforded by eMBB but are not suitable for Internet-of-Things (IoT) applications featured by machine-type communications (mMTC) as the devices are low power, limited storage, possess relatively limited computing capabilities and complicated encryption/decryption algorithms or protocols cannot be applied. PLS often requires relatively simple signal processing operations, which translates into minor additional overheads [2].

Conventionally, the security algorithms and protocols are deployed at upper layers of protocol stack and this poses challenges in applying these approaches in IoT. IoT devices include a range of devices from high end smartphones to low-cost, low energy and lightweight computing embedded devices. While its afforded by smartphones, most of the low-cost devices which are likely to find applications in various 5G IoT scenarios cannot afford the additional silicon area, power consumption, and even the code space needed to perform the expensive mathematical calculations of cryptographic methodologies [3][4]. Conventional upper layer-based cryptography also leaves the transmission vulnerable to many passive and active attacks. Moving the encryption to the physical layer can protect the entire physical layer packet and thus the wireless connection is secured from many passive and active attacks. Security countermeasures from the physical layer are lightweight and offer

https://doi.org/10.36282/IJASRM/6.2.2021.1787

protection to the wireless transmission, and therefore are advantageous over conventional upper layer encryption-based security primitives. PLS schemes often require relatively simple signal processing operations, which translate into minor additional overheads [5].

Orthogonal frequency-division multiplexing (OFDM) is a method of encoding digital data on multiple carrier frequencies. Here a large number of closely spaced orthogonal sub-carrier signals are used to carry data. The orthogonality allows for efficient modulator and demodulator implementation using the FFT algorithm on the receiver side, and inverse FFT on the sender side [6][7]. This article presents a simple yet effective PLS scheme which systematically rearranges the subcarriers ie coefficients of the inverse fast Fourier transform (IFFT) stage of multicarrier modulation scheme like OFDM making it unintelligible for the unauthorized receivers. The rearrangement which, when changed at a rate higher than channel frequency response, provides channel frequency diversity increasing the BER performance.While the legacy cyclic prefix orthogonal frequency division multiple access (CP-OFDMA) is retained as the preferred multiple access scheme for 5G enhanced mobile broadband (eMBB), multiple access schemes being proposed for massive machine type communication (mMTC) are also OFDM based multicarriers, except for not retaining the orthogonality[8]. Hence scheme is a likely contender for lightweight encryption approaches in 5G due to its simplicity, advantages and compatibility with existing architecture. Section 2 details the proposed scheme by explaining the possible exploitation of diversity among OFDM subcarriers to improve BER performance and the means of achieving physical layer security. Section 3 gives the simulation results and finally section 4 concludes the article along with future research directions

2. Proposed Scheme

Though several schemes have been proposed to improve the performance of OFDM, very few have tried to exploit the diversity among the subcarriers [9]. Here one such scheme has been proposed where the frequency diversity gain is achieved by using a subcarrier mapper which pseudo randomlydistributes

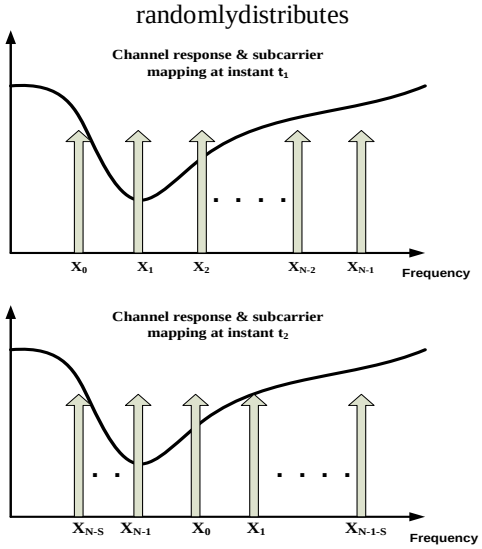


Fig. 1 Illustration of channel response and its effect on subcarrier mapping. As we can see at time instant t_1 subcarrier X_1 experiences deep fade but X_{N-1} does not. At t_2, it's vice versa

a user's subcarriers across the band. Such a distribution not only offers frequency diversity since the subcarriers would experience diverse fades but also if only legitimate users have the knowledge of the arrangement, the scheme can act as an encryption scheme . Frequency diversity advantage afforded by distributed subcarriers is well suited for those users experiencing slowly time varying channels because mobile user experiences different multipath fadings at different time instants, if subcarriers are suitably mapped. The Fig.1 illustrates an example scenario where the subcarriers are experiencing different fades in a non-uniform fading channel, at different time instants. Assuming a fairly slow time varying channel, say if the subcarriers are circularly shifted by a factor S , and the subcarriers will now experience different part of the channel. As we can see at time instant t_1 subcarrier X_1 experiences deep fade but at the same time X_{N-1} isn't. Now at instant t_2, assuming a relatively slowly varying channel, subcarrier X_1 now experiences no fade but X_{N-1} does, thus we can utilize the diversity to minimize effect of fading on a particular set of subcarriers.

Now what makes the scheme attractive is the way the subcarrier shifting/ mapping is carried out to achieve diversity. One of the approaches would be, the subcarriers can be rearranged or interleaved in a pseudorandom manner so as to achieve security, but the process may be complex. The other approach is, all the subcarriers can be simply circularly shifted, the shift factor being decided by a PN sequence generator. The latter scheme would need only an additional shifter to perform the task and is very robust in the sense that only authorized user with exact knowledge of the particular PN sequence generator and the initial seed i.e. starting shift factor can decode the data, thus achieving security.

IJASRM
International Journal of Advanced Scientific Research and Management, Volume 6 Issue2, Feb 2021
www.ijasrm.com
ISSN 2455-6378

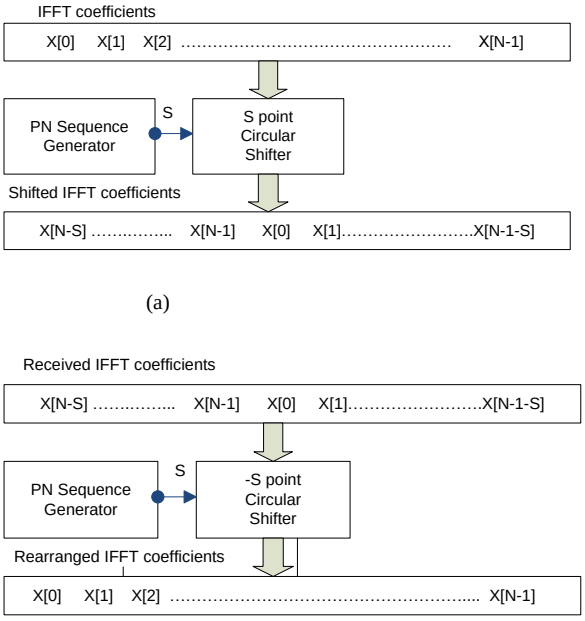


Fig. 2 The detailed description of encryption /decryption block (a) S point IFFT Co-efficient shift or encryption (b) Rearrangement of coefficients or decryption

Fig.2a shows the scheme for scrambling the data by circularly shifting the individual N IFFT coefficients by S points , where the value of S is generated by a PN sequence generator. The sequence generator can be either a simple PN sequence generator for accidental security threats or it can be one of the cryptographically secure pseudo-random number generator (CSPRNG) [10][11].
Fig.2b shows the rearrangement of IFFT coefficients by reverse shifting the coefficients using the same PN sequence generator at decoder thus decrypting the data. An example random shift factor generator based on PN sequence with polynomial x8+x6+x5+x4+1 is as shown in fig.3 and first few shift factors with initial value '10000000' i.e. 128 are as listed in table.1.

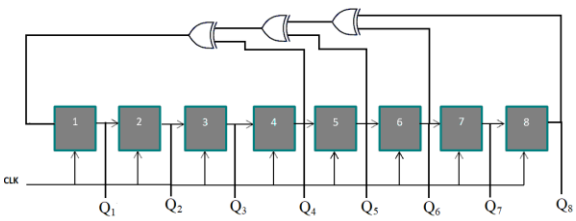


Fig. 3 An example 8 bit PN sequence based random shift factor generator with primitive polynomial $x^8+x^6+x^5+x^4+1$

While conventional scrambling approach with rearrangement of coefficients needs the generator size to be equal of more than that of coefficient dimension, the shifting approach has the freedom of choosing the shift factor generator size, and still be equally robust. If, the shift factor so generated is

Table-1: The first few shift factors generated by the PN sequence generator with polynomial x8+x6+x5+x4+1 with seed '10000000' ie 128

Clock Pulse	Q_8	Q_7	Q_6	Q_5	Q_4	Q_3	Q_2	Q_1	Shift Factor 'S'
1	1	0	0	0	0	0	0	0	128
2	1	1	0	0	0	1	1	0	198
3	0	0	0	0	1	0	1	1	11
4	1	1	1	1	1	1	1	1	255
5	1	0	0	0	0	1	0	0	132
6	1	1	1	1	0	0	1	0	242
7	0	1	0	1	0	1	0	1	85
8	0	0	0	0	0	1	1	1	7
.	.	.	.	.	.	.	.	.	…
.	.	.	.	.	.	.	.	.	…

greater than 2^N, modulo 2^N operation can be performed to get a new value within the range, thus giving more options in choosing the sequence generator, the initial values adding to the security aspects. As the shift is circular or modular in nature, a shift value greater than 2^N will not affect the performance but it increases the possible number of initial values which makes it difficult for the attackers. Larger size PN sequence generator also means a large period after which the shift factors repeat, making it more secure.

Here, in this article, the focus is on the possibility of scrambling the data by shifting the IFFT coefficients to achieve security with minimum changes to existing multicarrier transmitter architecture and with less complexity, especially for IoT applications, achieving diversity gain in the process. The detailed study on the robustness of the encryption capabilities of the scheme along with performance comparison with most of the existing schemes is not carried out.

3. Simulation and Results

The fig.4.(a) and fig.4.(b) show the implementation of the proposed diversity cum encryption scheme as applied to a generalized OFDM block[12]. Though OFDM is not being used directly , most of the 5G waveform contenders like OFDMA, filter bank multicarrier (FBMC), universal filtered multicarrier (UFMC) and even few non orthogonal multicarriers typically contain an IFFT block at transmitter and an FFT block in receiver, where we intend to introduce the pseudorandom shifts. Except for the encryption/decryption block, rest of the blocks pertain to a simple BPSK based N point OFDM with cyclic prefix. The circular shifter block along with the PN sequence generator carries out the task of

IJASRM
International Journal of Advanced Scientific Research and Management, Volume 6 Issue2, Feb 2021
www.ijasrm.com
ISSN 2455-6378

encryption.

Original Data:
'The sea of tears becomes crowded with other animals andbirds that have been swept away by the rising waters.Alice and the other animals convene on the bank and thequestion among them is how to get dry again. The mousegives them a very dry lecture on William the Conqueror.'
Encrypted Data:
;bBi%tP^5%SRLqMa*z-x#gpUbq|]1Y6&<V1Mm|3QY□&wK =[KD31Tjb'^yYg%L-a*hK#i$Q4p`x\|kAuZ^&2a=2](g7}_a]ORh GJX[aIj#B5%M)./N{y&>qgd!f<khHI`FJ,Afqf9J\"<;_C-{2dPRA Z;!E^.HB\|uC&_eX$Ap`DE"/{(/-N#?9\=Xc4M<gVVOg□ch;~ z'_,hjwB;8l]m+tC\8gi
Decrypted Data:
'The sea of tears becomes crowded with other animals and birds that have been swept away by the rising waters. Alice and the other animals convene on the bank and the question among them is how to get dry again. The mouse gives them a very dry lecture on William the Conqueror.'

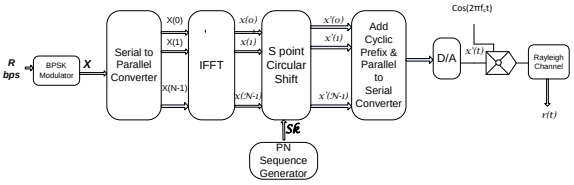


Fig. 4(a) Scheme showing OFDM transmission with Encryption

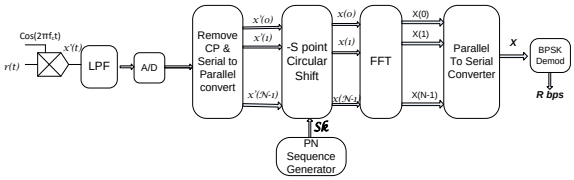
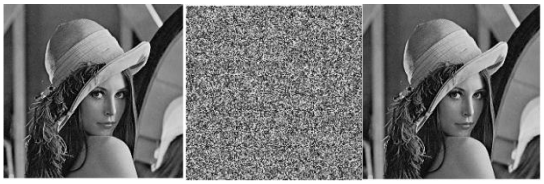


Fig. 4 (b) Scheme showing OFDM reception with Decryption

The proposed system was tested on a sample text and an image data on Matlab and the results have been summarized in this section. BPSK modulation was used here. 1024 point IFFT & FFT were used. The data , both text and grey scale image image were first converted into binary form and broken into chunks of 1024 bits and fed to the block. A 10 bit PN sequence generator wasused to generate the shift factor to perform circular shift. At receiver, circular shift in opposite direction with same generator and same initial seed was used. The results have been encouraging as both the text and the image were not intelligible without the authorized key, as shown Table 2 in case of text and Fig.5 in case of a grey scale image.



(a) (b) (c)

Fig. 5 (a) Original grey scale image of lena.bmp (b) The encrypted image (c) Decrypted image

A bit error rate (BER) performance curve of the proposed security scheme was plotted in comparison with conventional OFDM scheme without using the subcarrier diversity to demonstrate the diversity gai. A frequency selective Rayleigh faded channel with AWGN was considered for the BER performance simulation. The results have been encouraging as a relative BER performance improvement was observed in the system, as shown in the Figs. 6&7.

Fig.6 is the simulation result got for a Rayleigh channel with maximum Doppler shift, fd=0.05, with 4 delay paths. The performance gain at higher SNRs is clearly visible as the BER curve deviates from

Table 2. Original sample text data compared with the encrypted data derived through simulation

normal OFDM and decays quickly. The system performs similar to conventional OFDM when the fading effect is very low, which is apparent in Fig.7 where fd=0.001 is employed and no performance difference was found. The results indicate that as the fading increases, the said system performs relatively better due to the diversity advantage. It shows the ability of the scheme not only to provide security but also the ability of the scheme to be even considered in fading scenarios as a standalone feature even without taking the security aspects into consideration.

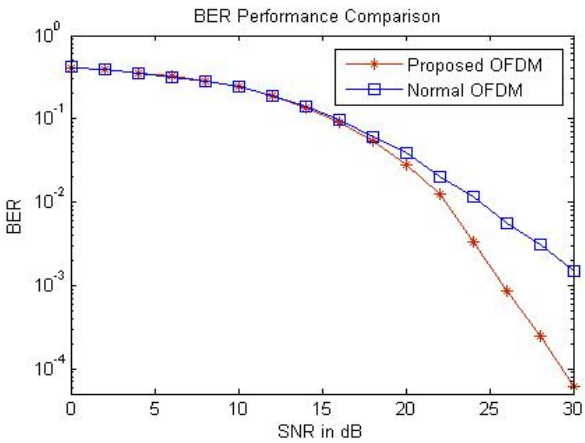


Fig. 6 BER vs SNR curves comparing the performance of the proposed scheme with a conventional OFDM scheme without employing the diversity.

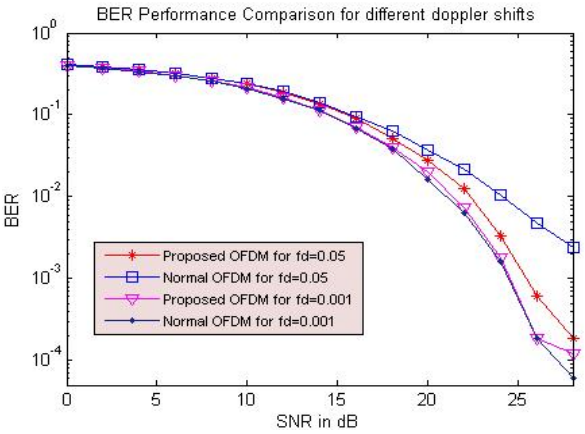


Fig.7 BER performance comparison at two different Doppler shifts, 'fd'. showing better performance even at higher Doppler shifts.

4. Conclusions

A novel PLS scheme to perform encryption in FFT based 5G multiple access waveforms was proposed by carrying the simulation study on basic OFDM block. The simulations have revealed the ability of the scheme to perform simple encryption as required by the low power, low complexity IoT devices and also to provide better BER performance by utilizing diversity among IFFT coefficients, by using minimum side information like the nature of sequence generator used and the initial shift count. Though the exhaustive study on the robustness of the scheme is not conducted, the paper presents a possibility in the direction as compared to complex higher layer security approaches, meanwhile providing diversity gain. The scheme also benefits from the fact that only small architectural changes are needed in the existing OFDM architecture with a shifting block inserted achieving both encryption and diversity. The scheme can also be considered as a generalized approach to encryption of data kind of data, in frequency domain by utilizing efficient FFT structures instead of time domain. The detailed study on the exact nature of the PN sequence generator to be used and the analysis of its robustness against attack is to be conducted in future.

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," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 905-929, Secondquarter 2020, doi: 10.1109/COMST.2020.2971781.

[2] S. Wang, W. Li and J. Lei, "Physical-layer encryption in massive MIMO systems with spatial modulation," in China Communications, vol. 15, no. 10, pp. 159-171, Oct. 2018, doi: 10.1109/CC.2018.8485478.

[3] Hao Yang, HaiyunLuo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in mobile ad hoc networks: challenges and solutions," in IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004, doi: 10.1109/MWC.2004.1269716.

[4] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," in IEEE Transactions on Mobile Computing, vol. 5, no. 2, pp. 128-143, Feb. 2006, doi: 10.1109/TMC.2006.16.

[5] Zhang J, Duong TQ, Woods R, Marshall A. "Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview". Entropy. 2017; 19(8):420. https://doi.org/10.3390/e19080420

[6] A. Goldsmith, 'Wireless Communications', Cambridge University Press, Cambridge, UK, 2006

[7] ArunabhaGhosh, Jan Zhang, Jefferey Andrews, Riaz Mohammed, 'Fundamentals of LTE', Prentice Hall, Communications Engg. and Emerging Technologies. 2011

[8] Y. Yuan et al., "Non-orthogonal transmission technology in LTE evolution," in IEEE Communications Magazine, vol. 54, no. 7, pp. 68-74, July 2016

[9] Samuel C. Yang, 'OFDMA System Design and Analysis', Artech House Library, Norwood, 2010

[10] Michael Luby, 'Pseudorandomness and Cryptographic Applications', Princeton University Press, 1996.

[11] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638.

[12] Proakis, John G, and MasoudSalehi. 'Digital Communications'. Boston: McGraw-Hill, 2008. Print.