FBMC + Security – A New Candidate for 5G

Avila Jayapalan, Prem Savarinathan, Madhumitha Munusamy, Thenmozhi Karuppasamy

Abstract: ***Recent researches and discussions stress the need for waveforms with better spectral efficiency which could be obtained by Orthogonal Frequency Division Multiplexing (OFDM). OFDM supports multicarrier communication and is capable of mitigating Inter Symbol Interference. Hence there is no need of equalizer at the receiving side. Human life has become easy and comfortable due to the rapid of wireless technology. At the same time there is an increase in the number of malicious users and the threat created by them for secure data transmission is noteworthy. Hence this work aims at to provide a solution which could solve the above discussed issues. Filter banks with multicarrier communication systems has gained popularity because of its capability to overcome the spectral leakage. Hence filter banks are placed instead of cyclic prefix. Near perfect reconstruction filter has been utilized to reduce the leakage. Further, Secure data transmission is accomplished by means of authentication tag. Pseudo Noise (PN) sequence named XOROSHIRO has been generated and appended with the information to be transmitted. At the receiving end only the information with authentication tag is accepted and the rest are omitted. FBMC system together with the authentication tag improves the spectral efficiency and also ensures safe and successful communication.***

Keywords **:** ***Authentication, FBMC, OFDM, PN sequence, XOROSHIRO128+.***

I. INTRODUCTION

Wireless Communication is the potent and flash developing technological area in the communication field, transmitting information from one point to the other, without having access to any medium like cables, wire or any physical medium. With the convenient wireless network, the transmitter and receiver can be placed anywhere between meters to thousand kilometers [1].

With the medium to be open air lot of noise sources arise and degrade the quality of the signal. The situation becomes worse with multipath propagation. Hence a system to overrule the interferences like Intercarrier Interference (ICI) and Inter symbol Interference (ISI) is needed. There are many systems which can provide a better transmission in immune way and Orthogonal Frequency- Division Multiplexing (OFDM) is one among them [2].

Orthogonal Frequency Division Multiplexing (OFDM) is a modulation technique in which data streams whose rate is higher are split into data streams of lower rate and then transmitted over various multiplexed orthogonal carriers. The conventional OFDM transmitter includes an encoder, modulator, interleaver, guard band, cyclic prefix and the FFT method which represents the digital implementation of the multicarrier modulation and the receiver executes the inverse operation of the transmitter [3].

The spectral leakage caused due to the subcarrier filters is the main drawback of OFDM. This causes interference with unsynchronized signals. OFDM transmits redundant bits known as Cyclic Prefix (CP) which are meant for the cancellation of ISI. This CP in turn decreases the overall spectral efficiency and the bandwidth consumption also increases. Filter bank provides a solution for the above discussed issues.

In addition, nowadays, the term secure data transmission gains popularity because of the breaching that has been caused by the intruders. Huge amount of money has been wasted due to hacking. Keeping this aspect in mind this work focusses on authenticated data via FBMC based system. Authentication is achieved by XORing the information with the tag generated. The tag is generated using Pseudo Noise (PN) sequence generator.

To the best of our knowledge FBMC with secure data transmission has not been discussed earlier. The remaining sections are organized as follows. Section 2 deals with the proposed methodology. Section discusses the results and section four concludes the work.

II. PROPOSED METHODOLOGY

A Tag generation

Pseudorandom (PN) generator specifically XOROSHIRO128+ is used to generate the tag. It is chosen because it is difficult to break the algorithm because of it large period without major system crash. It can generate sequences of $2^{32-}1$ integers or 2^{128}-1 integers depending on the type. It takes the next random number by repeatedly performing XOR and Bit-shift operations within the sequence. Xorshift has been widely used due to its relatively fast speed and simple code configuration [10]. As the name suggests, xoroshiro128+ generates a random number through a single xor, a single shift, and double rotate operations, respectively with high entropy having the period of 2^{128}-1. It generates two initial seed values and generates 64 consecutive random numbers.

Manuscript published on January 30, 2020.
* Correspondence Author

Avila Jayapalan*, Assistant Professor in the Department of ECE in SASTRA Deemed University, Thanjavur.

Prem Savarinathan, Assistant Professor-III in SASTRA Deemed University, Thanjavur

Madhumitha Munusamy, M.Tech(Communication System) in SASTRA Deemed to be University, Thanjavur

Thenmozhi Karuppasamy, Dean of School of Electrical and Electronics Engineering in SASTRA Deemed University, Thanjavur.

However, the random number may be biased if the given seed values are deficient because xoroshiro128+ generates random numbers in deterministic ways using xor, rotate, and shift operations [4]. The algorithm is as follows

Step 1: Set the seed values s[0], s[1] and the parameters a, b, c and n . Here is the number of random numbers.

Step 2: Add the seed values, the added values are considered to be the first random number

Step 3: Previous seed values s[0] and s[1] are xored and stored in s1.

Step 4: New seed value s[1] is determined by left rotating s1 by the value of c.

Step 5: Left rotate previous seed value s[0] by the value of a, then it is XORed with s1 , hold the value in s0.

Step 6: New seed value s[0] is determined by XORing s0 with left shifted s1 by the value of b.

Step 7: Add the new seed values which is the second random number

Step 8: The process will continue till n is less than 64.

Sample

for seed = {s1 = 0000, s0 = 0001} and a=14, b=2, c=7

0001 1010 1809 0A87 9BD9 3CAA 3502 8840 3D24 7287 71F5 90AC A818 B4C1 2CE3 CC58 B31D DF3D B7A4 A2E3 3B2E 2C20 BFFF AFE9 5B9A 3BB8 35F4 921C 6A2D CD9A A217 207F 6269 0201 12A2 AE16 D719 4AE8 984B 0C52 743C 1DF1 BCC6 DBA0 746C 34C9 07FF 3643 C642 BBC0 594E AA85 701A D05A F3AE A328 695A 67EE 93C6 C140 4964 F5E1 FC57 5E24

B Proposed Block Diagram

The block of OFDM system with filter banks is shown in figure 2. The authentication tag which is generated using the above discussed algorithm is XORed with the information. In the transmitter side after XORing the authentication tag with the information it is passed through channel coder. Convolution encoder with the rate $\frac{1}{2}$ and constraint length K=3. The output of convolutional encoder is interleaved and then modulated. The data is modulated using various modulation techniques like QAM, QPSK etc [5,6]. The modulated data is then fed to serial to parallel converter bock where it is transformed into parallel data. Then it is passed into IFFT block. The modulated data undergoes IFFT or IDFT for which cyclic prefix is removed and filter banks are added. The OFDM signal is then up sampled and then passed through Additive White Gaussian Noise (AWGN) channel. At the receiving end, reverse process is carried out to get back the original data.

C Filter Bank

Near Perfect Reconstruction (NPR) filter is inserted by eliminating the cyclic prefix and guard band in the OFDM system. Nyquist pulse shaping is performed before transmitting the OFDM symbol or transmitting the data at higher rate than the symbol rate. Synthesis and Analysis filter bank is placed at the end of transmitter and front of the receiver respectively. NPR prototype filter can be designed by directly optimizing the coefficients of the impulse response. Here three factors K, N, and L decide the impulse response coefficients of the filter for the desired frequency response. The factor K is called as Overlapping factor. It is nothing but the number of multicarrier symbols that overlap in time domain. The sub channels are denoted by N which is generally N=256. L is the Number of taps per Channel. The Synthesis filter based on these parameters with the decent coefficients and inverse is done in the Analysis filter. Therefore, Spectral efficiency, Bandwidth, and frequency response are improved [7,8].

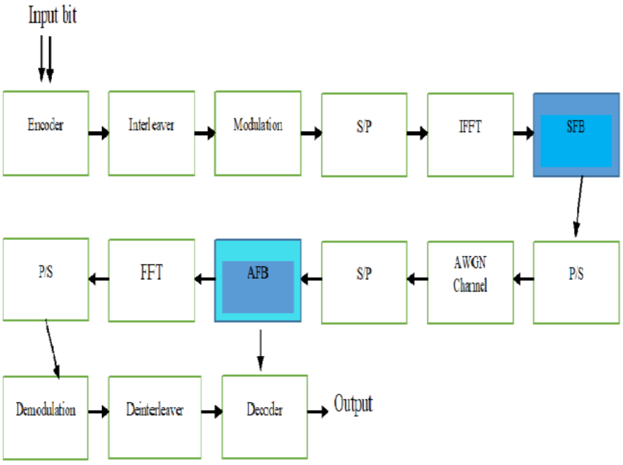

Fig. 1. OFDM with NPR filter

III. RESULTS AND DISCUSSION

Figure 2 shows the Bit Error Rate (BER) versus Signal to Noise Ratio (SNR) graph plotted between the OFDM system and the one with Filter bank. From the figure it is evident that FBMC gives better performance due to reduced spectral leakage when compared to conventional OFDM. For BER of 10^{-4} FBMC offers SNR of 9dB whereas for OFDM system it is 18dB.

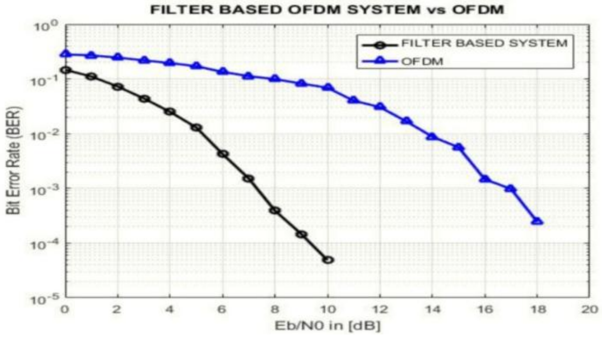

Fig. 2. Comparison between OFDM and FBMC

Figure 3 shows the BER versus SNR plotted for various values of Fast Four Transform (FFT) size. The graph has been plotted for FFT values of 256, 512 and 1024. It is clear that FFT size 1024 offers better result than FFT size of 256. With increase in the size of the transform the bin size increases. Increase in bin size improves the spectral resolution.

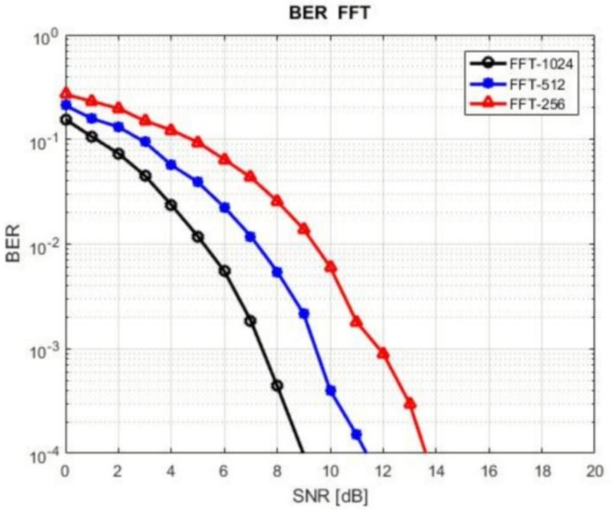

Fig.3. Various FFT Size

Figure 4 is the BER curve plotted between the two modulation schemes Quadrature Amplitude Modulation (QAM) and Quadrature Phase shift Keying (QPSK). It is clear that QPSK offers better result than QAM because the distance between the signal points is high is QPSK when compared to QAM. As the separation increases it is less sensitive to noise and the error reduces.

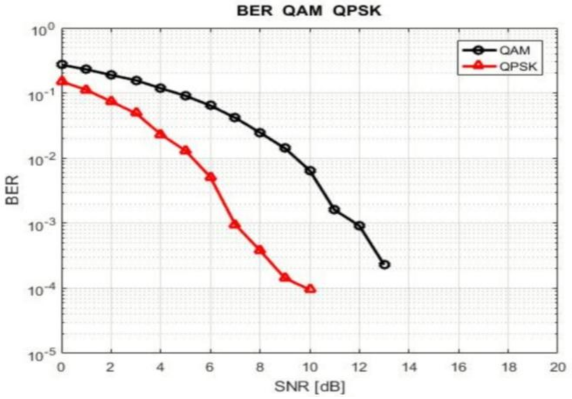

Fig. 4. comparison between QAM and QPSK

Figure 5 is the graph plotted between SNR and BER for various K values of the filter. From the figure it is clear that with increase K values the performance also increases. For K=11.4 the SNR is 8dB whereas for K=8 it is around 13dB.

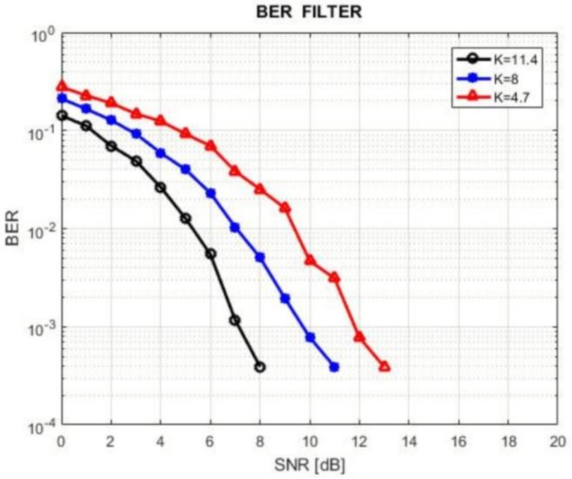

Fig. 5. Various K values

Figure 6 gives the BER versus SNR graph plotted for QAM modulation. It is plotted for M value of 32 bit, 64 bit and 128 bit. 32 QAM offers better than 128 QAM. As the M values increases more bits could be accommodated in a symbol and hence the data rate increases. At the same time the distance between the signal points come closer to each other and they become very sensitive to noise. This in turn increases the error. Hence it a tradeoff between the choice of M value.

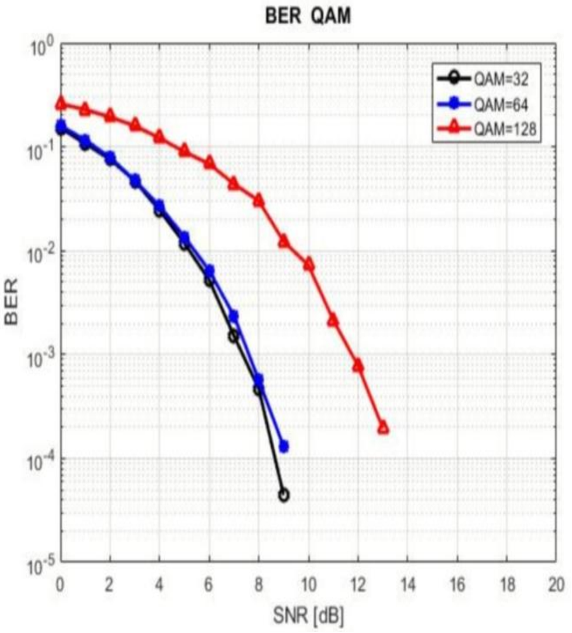

Fig. 6. QAM Modulation

Figure 7 shows the BER versus SNR graph plotted with and without the inclusion of authentication tag. The performance does not degrade with the inclusion of authentication tag. The tag is XORed with the information and hence no extra bandwidth is required to transmit it.

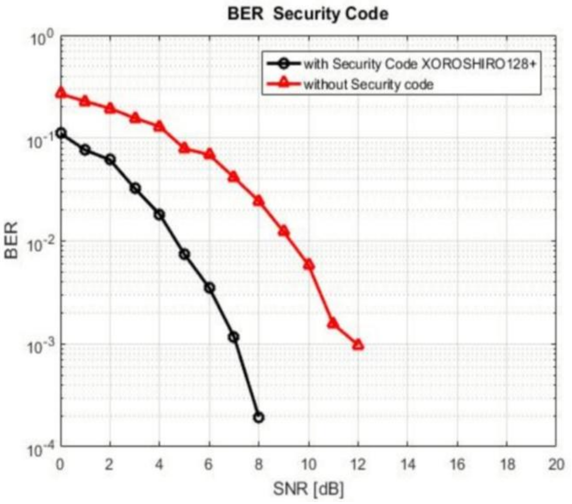

Fig. 7. With and without tag

Retrieval Number: E5711018520/2020©BEIESP
DOI:10.35940/ijrte.E5711.018520
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. CONCLUSION

This work focused on reducing the spectral leakage of conventional OFDM system with the aid of filter banks. Simulated proved that the performance of FBMC system is superior to conventional OFDM system. In addition, PN sequence- based authentication tag has been appended with the information to ensure secure data transfer. This integration of FBMC and authentication tag supported successful data transmission in the wireless environment.

REFERENCES

1. Avila.J, Prem.S, Sneha.R, Thenmozhi.K, “Mitigating Physical Layer Attack in Cognitive Radio – A New Approach,” International Conference on Computer Communication and Informatics, pp.1-4, 2018.
2. Manushree Bhardwaj, Arun Gangwar and Devendra Soni, A Review on OFDM: Concept, Scope & its Applications, IOSR Journal of Mechanical and Civil Engineering, Vol.1, No.1, pp.7-11,2012.
3. Taewon Hwang, Chenyang Yang, Gang Wu, Shaoqian Li and Geoffrey Ye Li,” OFDM and Its Wireless Applications: A Survey,” IEEE Transactions on Vehicular Technology, Vol.58, No.4,pp.1673-, 2009.
4. Nakjun Choi, Jeeun Lee, Kwangio Kim ”Fault Injection, Simple Power Analysis and Power Glitch Attacks against FPGA-implemented Xoroshiro128+”, Symposium on Cryptography and Information Security, pp.1-8, 2019.
5. Sanjeev, K. and S. Swati,”Error probability of different modulation schemes for OFDM based WLAN standard IEEE 802.11a,” International Journal of Engineering,Vol. 4,pp. 262-267,2010.
6. R. Mohamad, R. Mahmud and R. A. Awang, "Prototype of Quadrature Amplitude Modulation (QAM) baseband modem for a digital baseband signal processor," *2011 IEEE International RF & Microwave Conference*, Seremban, Negeri Sembilan, 2011, pp. 407-411.
7. Er.A.S.Kang, P.Renu Vig “Performance Analysis of Near Perfect Reconstruction Filter Bank in Cognitive Radio Environment,” International Journal *of* Advanced Networking and Applications,*Vol.8, pp.3070-3083,2016.*
8. J. Wen, J. Hua, F. Li, D. Wang and J. Li, "Design of FBMC waveform by exploiting a NPR prototype filter," *Advances in Wireless and Optical Communications (RTUWO)*, pp. 156-161,2017.

AUTHORS PROFILE

Avila Jayapalan received her B.E (ECE) from the V.M.K.V college of Engineering and M.Tech (Communication Engineering) from Vellore Institute Of Technology and Ph.D. from SASTRA Deemed University. Currently she is working as Senior Assistant Professor in the Department of ECE in SASTRA Deemed University, Thanjavur. She has teaching experience of 16 years and she has published 35 Research articles in National & International journals. Her research area includes Wireless communication and Cognitive radio

Prem Savarinathan received his B.E. degree from Mokambigai college of engineering and M.Tech. from Vellore Institute of Technology, Vellore. He is working as Assistant Professor-III in SASTRA Deemed University, Thanjavur Currently he is pursuing his Ph.D. He has teaching experience of 16 years and has published many articles in National & international journals.

Madhumitha Munusamy reveived her B.E(ECE) from Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Thiruvarur. She Currently doing my M.Tech(Communication System) in SASTRA Deemed to be University, Thanjavur. Her research area includes wireless communication.

K. Thenmozhi received her B.E (ECE) and M.E (Communication system) degree from Regional Engineering college (NIT) Tiruchirappalli and Ph.D. from SASTRA Deemed University, Thanjavur. Currently she is working as Dean of School of Electrical and Electronics Engineering in SASTRA Deemed University, Thanjavur. She has a teaching experience of 23 years. Her current research area includes Wireless communication, Steganography and Information Theory and Coding. She has supervised more than 100 UG projects, 10 Master Students and Supervising 4 Ph.D. Scholars. So far she has published 97 Research articles in National & International journals conferences. She received EDI award from the broadcast Engineering Society for the year 2007.