I.J. Wireless and Microwave Technologies, **2021, 5, 26-34**
Published Online October 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.05.04

Interference Mitigation in Wireless Communication – A Tutorial on Spread Spectrum Technology

Cosmas Kemdirim Agubor, Akinyinka Olukunle Akande, Reginald Opara
Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria.
Email: cosmas.agubor@futo.edu.ng

Received: 19 July 2021; Accepted: 20 August 2021; Published: 08 October 2021

Abstract: This paper focuses on Spread Spectrum technique and its interference mitigation feature as applied in wireless communication. With spread spectrum technology it is possible to implement the transmission of multiple signals over wider ranges of spectrum without resulting to interference from other signals transmitted over the same frequencies. It does this by rejecting any received signal that does not carry the proper code. Interference rejection, one of the several features of spread spectrum technology is a difficult concept to understand. It is therefore proper to x-ray this topic in a less complex manner so that it can be well understood by those who are not mathematically grounded. In view of this a further simplified approach in presenting this subject is necessary. A tutorial approach is used to simplify this subject for better understanding and how this feature is used in Code Division Multiple Access (CDMA) systems. To show how multipath interference rejection is achieved in CDMA systems simple equations and schematics were used. The discussions cover the method of code recognition at the receiver which serves as a technique for interference mitigation. The paper helps to understand the theory of code recognition in Spread Spectrum, and thus provides answer to the question on how does interference mitigation or rejection in spread spectrum works?

Index Terms: Bandwidth; CDMA; code; pseudo-noise; spread spectrum.

1. Introduction

The transmission of signals is generally made possible by one form of modulation scheme or the other. Narrow band modulation schemes is one of such form used in the past in which all of the power in a transmitted signal is made to occupy a very narrow segment of the frequency bandwidth. Transmission using this method becomes vulnerable to signal interference. An interfering frequency that is same or very close to the transmitted frequency can cause interference to the level of rendering the transmitted frequency noisy, distorted, unintelligible and unrecoverable. Amplitude modulation (AM) is a typical example of a narrowband modulation scheme. This method allows the amplitude of the carrier to vary in sympathy with the information or modulating signal to be transmitted. Thus the amplitude of the carrier is made stronger or weaker in response to the modulating signal. AM signals are capable of travelling long distances. The reason for this is because of the large amount of power the AM signal is associated with. The signal attenuates gradually with distance.

Another form of modulation which is very popular especially in sound broadcasting is frequency modulation (FM). In this method the frequency of the carrier signal is varied in accordance with the modulating or information signal to be transmitted. In communication, two basic techniques may be used for efficient transmission of signals. One technique is to use high power over narrow band of frequency (eg AM) and the other is to allow the spreading of low power density over a larger band of frequencies. This second method is an example of Spread Spectrum (SS) modulation.

In SS technique, a spreading operation is performed in which the bandwidth of the baseband signal that carries the intelligence is intentionally spread over a larger signal bandwidth. This is done by injecting a signal with higher frequency containing a spread-spectrum code called pseudo noise (PN) codes somewhere in the transmitter chain before transmitting [1]. This method of utilizing a larger amount of bandwidth brings about its ability to be immune to a variety of interference. The technique allows a trade-off of bandwidth for lower transmitter power [2]. To recover the signal back to its original bandwidth a dispreading operation is performed at the receiver. The dispreading operation is performed at the receiver chain by applying the same PN code. The spreading and dispreading techniques make SS a

system with high confidentiality and security compared to other modulation methods. These techniques form the major area of discussion in this paper.

Signal interference in wireless communication systems is known to negatively affect the overall quality of service (QoS) of the network. Signal interference can be intentional or unintentional. The technique adopted by SS technology gives it the ability to withstand both intentional and unintentional interference. These interference mitigation technique uses various techniques [3-5]. In [3], the technique that is based on least-mean-square was used. The method of estimating and suppressing narrowband interference pseudo-noise SS digital communication was used in [4]. A filtering approach capable of suppressing arbitrary jamming interference signals was documented in [5]. In their documentations of these methods mathematical modellings were made use of that appeared complex and difficult to understand especially by those who are not conversant with the subject. A more understanding and simplified discussion is necessary to show how these techniques from a general point of view can achieve interference suppression or mitigation.

The major objective of this paper is to present an overview and in a simple form on how interference mitigation feature of SS in wireless communication is accomplished and how it can be used in wireless communication such as code division multiple access (CDMA) system. The presentation is void of complex and difficult mathematical expressions. Spread spectrum as a transmission technique has been treated in details in several technical literature. In most cases the discussions found on this subject in related literature have complex mathematical expressions that may be difficult to comprehend.

Thus, a very simple and easy-to-understand mathematical approach has been adopted in this work to show how SS signals are immune to interference from other signals. The ability to add clarity and simplicity to the understanding of this subject which elsewhere has been treated in a more complex form is the main contribution of this paper. The remaining part of the paper is arranged as follows: section 2 is a brief literature review of some other modulation techniques used in wireless communication, section 3 covers methodology. Section 4 deals with interference mitigation and section 5 is the conclusion.

2. Literature Review

There are other procedures in use to ensure effective communication in terms of efficient spectrum utilization or mobility and security requirements. Cognitive radio (CR) is one technique suitable for spectrum management. This system is widely in use and has been found suitable in spectrum sensing, spectrum migration and spectrum sharing [6, 7]. The operation and application of CR have been elaborately discussed in [8].

Orthogonal Frequency-Division Multiplexing (OFDM) is another transmission technique adopted in today's advance wireless networks. In OFDM the bandwidth to be transmitted is divided into a number of orthogonal and non-overlapping subcarriers which are used to transmit in parallel the required bits or symbols [9, 10]. For future 5G wireless communication new modulation techniques have been proposed. These are Generalized Frequency Division Multiplexing (GFDM), filtered – Orthogonal Frequency-Division Multiplexing (f-OFDM) and Universal Filtered Multi-Carrier (UFMC) [11, 12].

Traditionally, wireless networks whose transmission medium is electromagnetic wave is faced with security challenges unlike cable communication. Different methods have been implemented in tackling security issues for each modulation technique. For SS systems some of its positive aspects have been widely published in several scholarly articles such as signal holding (lower power density, pseudo noise) non-interference with conventional and other SS systems, secure communication (privacy), code division multiple access (CDMA) and rejection or protection from intentional interference (jamming). In [13, 14], its resistance to interference and anti-jamming (AJ) properties were elaborately discussed. In the filtering technique in [6], their approach was based on a filter bank which applies different filters in parallel and dynamically selects the best filter according to the output state of the demodulator.

Unlike other systems it is only SS that sacrifices bandwidth for low transmission power, confidentiality and security [2]. Although OFDM and other advance modulation techniques have found good use in today's wireless networks like the 4G LTE, SS due to its security-friendly features will remain one of the most widely and commonly used modulation scheme for wireless transmission. Its low probability of intercept (LPI) and anti-jam (AJ) features have made it a major subject of research in contemporary communication engineering [1, 2]. Another form of achieving interference mitigation in SS was proposed in [15], where bandwidth hopping spread spectrum (BHSS) technique was used as a means of improving jamming resistance in wireless communication.

The above literature, sums up to one basic and important fact and that is SS technology is used to suppresses or combat interfering signals and by so doing the system is secured or prevented from intended or unintended attacks. The various methods by which this feature is achieved can be obtained in the reviewed literature. In this paper we have made effort to generally present the concept of interference mitigation by using simple mathematical expressions in place of the more complex expressions as found in the above related literature. In doing so, no new technique is proposed rather the focus is on providing the answer to the question on how does interference mitigation in spread spectrum works ?

It is in line with this that this study is done in which its very attractive feature of interference rejection (multi-path interference rejection) and its application in CDMA communication systems are presented.

3. Research Methods

The study was carried out by performing a review of scholarly works that are related to the topic. This was done to collect important and related information that can be helpful in presenting the topic in a more simplified form for better comprehension. Simple mathematical expressions and schematics were then formulated to replace the more difficult mathematical expressions that were used in the reviewed literature. More insight was obtained from the theory of the topic under study.

3.1 Theory of Spread Spectrum

As the name implies, SS technology propagates its signal over a wideband of the spectrum. The conventional propagation model is to transmit the signal with a discernible amplitude peak as shown in Fig 1. The SS transmission method differs by spreading the signal over a broad area as illustrated in Fig 2. This action results in compressing of the bandwidth.

.

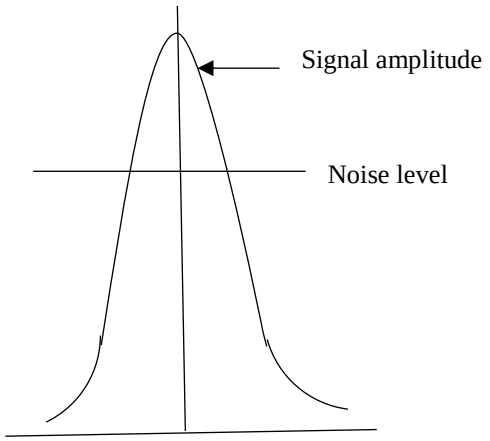

Fig. 1. Conventional signal

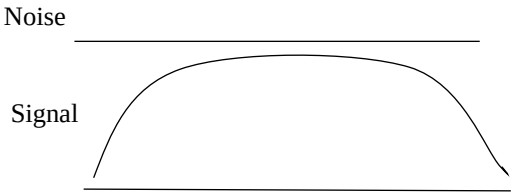

Fig. 2. Signal spread across broad area

Fig 2 shows how the baseband signal is intentionally made to spread over a larger bandwidth. This is achieved by introducing a higher frequency signal during the spreading process. This action allows the transmitted signal energy to spread over or occupy a wider bandwidth thus making the signal to appear as noise. As a result the SS now has a wider bandwidth compared to that of the original signal.

The relationship between larger bandwidth resulting from the spreading operation and that of the original signal is termed processing gain (PG). The PG is the ratio in dB between the spread baseband B_{sp} and the original information signal B_{info} which typically runs from 10dB to 60dB [1]. That is

$$G_p = \frac{B_{sp}}{B_{info}} \tag{1}$$

A simple expression obtained in [14] shows the relationship between the signal bandwidth *B*, channel capacity *C* and noise *N*. This is given by

$$C = Blog_2(1 + \frac{S}{N}) \tag{2}$$

In the above expression, *C* is the communication channel and *B* is the bandwidth which in this case is the element to be sacrificed in favor of low transmission power [16]. $\frac{S}{N}$ is the signal-to-noise ratio and expresses the effect of environmental conditions and other forms of interference as the signal propagates through the channel. For SS

application and as in Figure 2, $\frac{S}{N}$ is usually low due to the fact that the signal power density can be below the noise level [17].

Assume $\frac{S}{N}$ is unity, in this case both signal and noise power levels are the same. Then (2) now becomes

$$C = Blog_2(1+1) = Blog_2 2 = B \tag{3}$$

Equation (3) indicates that for a given $\frac{S}{N}$ in the channel and to send error-free information, it is required to perform the signal-spreading operation by increasing the bandwidth of the transmitted signal.

3.2 Types of SS

Two basic types SS exist, frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). The difference between both of them arises from the point of system code injection. A simple block diagram of a FHSS is illustrated in Fig.3 with serial binary data as its input into a frequency shift keying (FSK) modulator. The pseudo-noise (PN) generator is a driven by a clock circuit. The output generated by the PN generator is a serial pattern binary data (1 and 0) that changes randomly. The nature of the randomness makes the serial output appear wideband and noise-like [1]. In FHSS systems the signal from the transmitter end is made to hop periodically on a specific set of frequencies as illustrated in Figure 4. This set of frequencies is regarded as the spreading code [18], and must be known by the receiver to enable interception and recovery of the transmitted message. With N channels and each having bandwidth W, the bandwidth B of an FHSS system may be defined by:

$$B = WxN \text{ Hz} \tag{4}$$

The period of time T_b the transmitted signal spends on each hop is referred to as the dwell time which is usually 400ms [19].

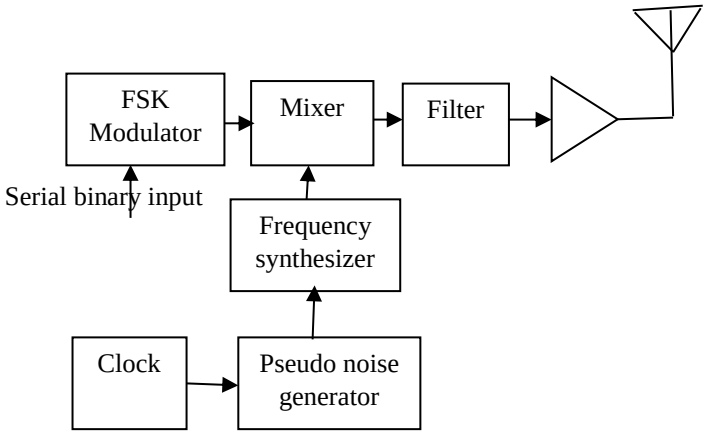

Fig. 3. Block diagram of FHSS transmitter

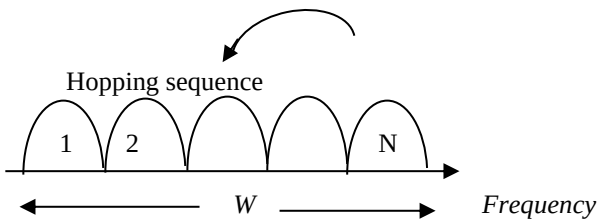

Fig. 4. FHSS Signal bandwidth

In a DSSS technique, the system employs a high speed code sequence which together with the transmitted information modulate the RF carrier. The block diagram in Fig. 5 illustrates a typical DSSS transmitter. A serial binary data with rate R_s (symbol rate) is applied to an X-OR gate.

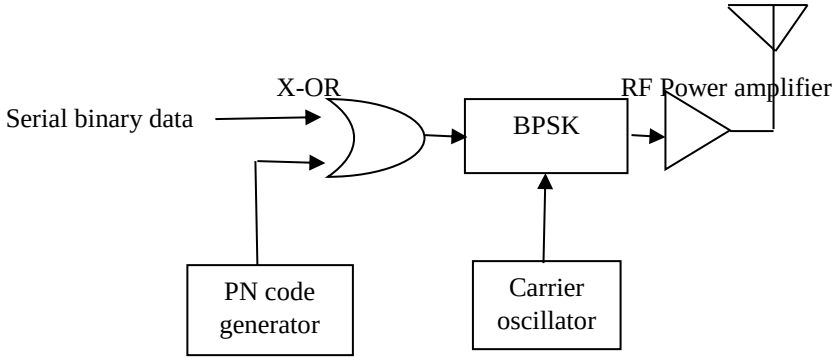

Fig. 5. Block diagram of a DSSS transmitter

The PN generator produces codes of bits at a rate R_c (chipping rate) such that, $R_c > R_s$. The binary output of the gate is fed to the binary phase shift keying (BPSK) modulator which is used to switch the phase of the RF between 0° and 180°. The result is that the complete signal takes up a large part of the spectrum resulting to a spread signal with a higher bandwidth of up to 2.4 GHz [18].

4. Interference Mitigation Feature

In DSSS, the carrier signal used for modulation is a random sequence signal with positive and negative pulses which is repeated at a very high rate [20]. Spreading the signal occurs when the original signal is multiplied with this high rate carrier signal. The transmitter uses a BPSK modulation as shown in Fig. 6.

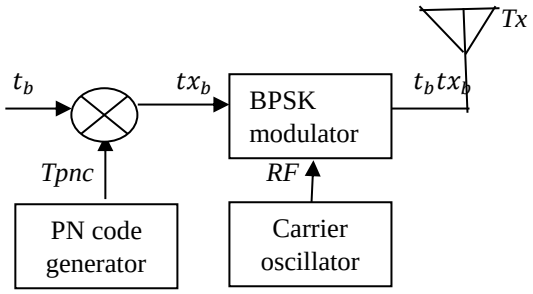

Fig 6 Block diagram of a DSSS transmitter

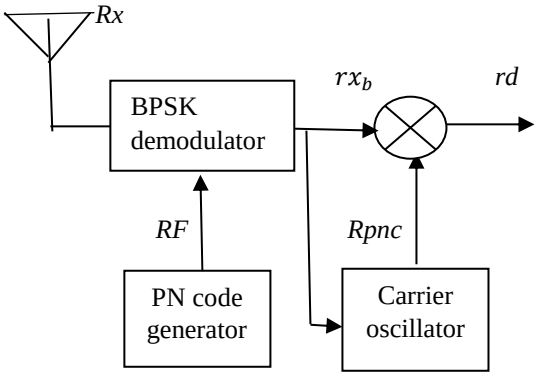

Fig. 7. Block diagram of DSSS receiver

Spreading takes place when the binary data t_b is multiplied with PN code at the transmitterT_{pnc}. This results to the transmitted baseband tx_b which is now the input of the BPSK modulator. That is

$$t_b . T_{pnc} = tx_b \tag{5}$$

Dispreading takes place as illustrated in Fig. 7. For dispreading at the receiver the PN should be known, i.e.

$$T_{pnc} = R_{pnc} \tag{6}$$

Therefore the output binary data is recovered by multiplying the received baseband from the BPSK demodulator with the receiver PN code, i.e.

$$rx_b . R_{pnc} = r_d \tag{7}$$

No dispreading at the receiver if

$$T_{pnc} \neq R_{pnc} \tag{8}$$

Dispreading at the receiver can only occur and the original information recovered if the PN code of the transmitter is known by the receiver.

For spreading at the transmitter, consider a PN code with sequence as shown:

$$T_{pnc} = +1 + 1 + 1 + 1 + 1 - 1 - 1 + 1 - 1 - 1 - 1 \tag{9}$$

$$\sum T_{pnc} = +1 \tag{10}$$

For synchronization the PN code is multiplied with itself

$$T_{pnc} . T_{pnc} = 1x1 = +1 \tag{11}$$

For dispreading T_{pnc} must synchronize with R_{pnc} at the receiver, such that

$$T_{pnc} = R_{pnc} \tag{12}$$

Therefore

$$T_{pnc} . R_{pnc} = 1 . 1 = +1 \tag{13}$$

Autocorrelation allows for proper synchronization and code recognition by the receiver. This results to

$$t_b = rd \tag{14}$$

At the receiver, if PN code takes the sequence different from that shown in (9), such as

$$R_{pnc} = +1 + 1 + 1 - 1 + 1 - 1 + 1 - 1 - 1 - 1 - 1 \tag{15}$$

Then

$$\sum R_{pnc} = -1 \tag{16}$$

Therefore

$$T_{pnc} . R_{pnc} = 1 . (-1) = -1 \tag{17}$$

Since in (13), $T_{pnc} \neq R_{pnc}$ the receiver will not be able to reproduce the original information. The transmitted PN code in (9) is different from the received PN code in (16). The original transmitted signal is shielded or protected from an interfering signal. This demonstrates the anti-jamming feature of SS making it a secure means of communications.

Spread spectrum finds application in CDMA (code division multiple access) systems which can also be termed spread spectrum multiple access (SSMA) [21]. A CDMA is a multi-user system as shown in Fig. 8.

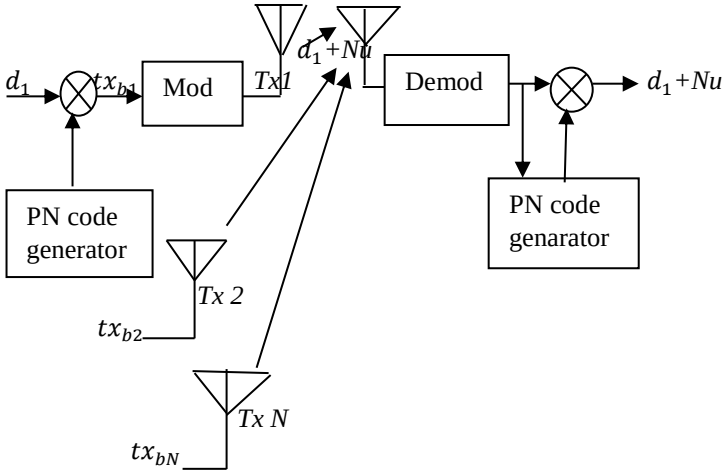

Fig. 8. CDMA system showing multi-user one receiver

The transmitted baseband tx_{b1} is a product of the input data d_1 and the transmitter PN code $Tpnc_1$ i.e

$$d_1.Tpnc_1 = tx_{b1} \tag{18}$$

The received data rx_b should be the transmitted data, i.e.

$$rx_b = tx_{b1} = d_1.Tpnc_1 \tag{19}$$

A receiver is exposed to a number of *N* transmitters. The received signal can be given by

$$rx_b = \sum_{i=1}^{N} d.Tpnc \tag{20}$$

$$rx_b = d_1.Tpnc_1 + d_2.Tpnc_2 + \cdots + d_N.Tpnc_N \tag{21}$$

Apart from user 1 all other signals cannot be dispread because of the difference in PN codes. Signals with different codes will appear noisy at receiver 1. The output at the receiver is then the sum of the data d_1 and the rejected signals appearing as noise *Nu*, i.e.

$$Output = d_1 + Nu \tag{22}$$

This demonstrates how in CDMA systems, a particular receiver which is exposed to other several transmitted signals is only able to decode the transmitted signal which it is synchronized to, without any effect from the uncorrelated signals. This feature code identification makes systems using spread spectrum technology to be immune to interfering signals.

5. Conclusions

This paper has presented an overview on the principle of spread spectrum technology and how secured digital communication can be achieved by using this technology. A review on the different methods of achieving interference suppression in spread spectrum technology was done which formed the backbone of the discussion. Interference mitigation or suppression is one important feature using this technology. The discussion was on how to simplify this concept for better understanding. In doing so the work used simple mathematical and schematics to better explain the subject. The secure nature of SS is widely used in different fields. One area of application is in mobile wireless communication especially in code division multiple access systems. In this paper we also extended the discussion to show how the method of achieving secured communication and preventing interference in CDMA communication systems can be implemented. CDMA is a multiple access method which works by allocating each user a sequence (code) that makes the user identifiable to the receiving antenna. This is known as code identification or autocorrelation. Using this technique the paper was able to demonstrate mathematically and schematically how each user in the midst of other users or interferers can be secured from their interfering signals as long as the main user's PN code differs from that of the interferers.

It is believed that this paper has been able to add clarity to the subject of interference in wireless communication system and how it can be mitigated or suppressed by adopting spread spectrum technology.

References

[1] Computing and Communications, (2008), 1036-1041. doi:10.1109/HPCC.2008.21.
[2] Abdelazeem R, Suliman, H, Bilal K.H. & Elemam I. (2018), Review Paper on Cognitive Radio Networks, Journal of Electrical & Electronic Systems, 7 (1), 1-3. DOI: 10.4172/2332-0796.1000252
[3] Milstein L. (1998), Interference Rejection in Spread Spectrum Communications, Proc of the IEEE, 76(6), 657-671.
[4] Ketchum J. and Proakis J.G. (1982) Adaptive Algorithms for Estimating and Suppressing Narrowband Interference in PN Spread Spectrum Systems, IEEE Trans. on Commun., Com-30, 913-924.
[5] Giustiniano D., Schalch M., Liechti M and Lenders V. (2018), Interference Suppression in Bandwidth Hopping Spread Spectrum Communications, in Proc. of 11th ACM Conference in Wireless and Mobile Networks, 134-143.
[6] Singh S. & Singh, H (2015), Review Paper on OFDM- Concepts and Applications, International Journal of Engineering Development and Research, 3(3), 1-4.
[7] Barakabitze A.A. & Ali, M.A. (2015), Behavior and Techniques for Improving Performance of OFDM Systems for Wireless communications, International Journal of Advanced Research in Computer and Communication Engineering, 4 (1), 237-245, DOI 10.17148/IJARCCE.2015.4152
[8] Getachew, H, Dereje, G., Molla M. & Fante, K.A. (2018), Comparative Study of Modulation Techniques for 5G Networks, International Conference on Advances of Science and Technology ICAST, 503-518.
[9] Rani P.N. & Rani, C.S. (2016), The 5G modulation technique, IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), DOI: 10.1109/ICCIC.2016.7919714
[10] Dixon, R.L. (1994), Spread Spectrum Systems with commercial applications, John Willey & Sons,
[11] R.L.Pickholtz, D.L. Schiling and Melstein L.B. (1990),"Spread Spectrum goes commercial," *IEEE Spectrum*
[12] Ding, Q. (2010) A Story of Wireless Communication, Posts and Telecom Press.
[13] J. Proakis J. & Salehi, M (2007), Digital Communications, McGraw-Hill Education,
[14] Navpreet, K., Inderdeep, K.A. and Renu V.(201), Analysis of Spread Spectrum Techniques in Cognitive Radio Networks, International Journal of Applied Engineering Research, 11(8), 5641-5645.
[15] Liechti M., Lenders V. and Guistiniano D, (2015) Jamming Mitigation by Randomizing Bandwidth Hopping, Proc. of the 11th Conference on Emerging Networking Experiments and Technologies, 1-13.
[16] https://www.semtech.com/images/promo/FCCPart15 regulations_Semtech.pdf
[17] Zoran, S. & Burns, J. (2000), Performance Comparison of Frequency Flopping and Direct Sequence Spread Spectrum Systems in the 2.4 GHz range. Personal, Indoor and Mobile Radio Communications, The 11th IEEE International Symposium vol. 1,
[18] Frezen, L.E. (2003), Principle of Electronic Communication Systems, 2nd ed edition,
[19] Glencoe:Mc GrawHill.Dixon R.L. (1994), Spread Spectrum Systems with Commercial Applications, John Willey & Sons.
[20] Pickholtz R.L., Schiling D.L.& Melstein L.B. (1990), Spread Spectrum goes commercial, IEEE Spectrum
[21] Ding Q. (2010). A Story of Wireless Communication, Posts and Telecom Press.

Authors' Profiles

Cosmas Kemdirim Agubor has obtained B.Eng, M.Eng and PhD degrees. He is a registered member of the Nigerian Society of Engineers (NSE) and the Council for the Regulation of Engineering in Nigeria (COREN). He was an Engineer with the Nigerian Telecommunications Limited (NITEL) and rose to the rank of an Assistant Manager. He is now a lecturer in the Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Imo State, Nigeria. His research area is in wireless communication with special interest in Antenna systems and diversity

Akande Olukunle Akande obtained his B. Tech (2008) in Electronic and Electrical Engineering from Ladoke Akintola University of Technology Ogbomoso in 2008. M. Eng in Communication Engineering in 2013 and a PhD in Communication Engineering in 2019 from University of Ilorin and LAUTECH, Ogbomoso, respectively. He is presently a Lecturer II at Federal University of Technology Owerri. His research interests include Mobile Wireless Communications and Resource Management in Cognitive Radio networks. He is a member of the Nigerian Society of Engineers (NSE) and Council for the Regulation of Engineering in Nigeria (COREN)

Chinedu Reginald Opara is a Lecturer in Electrical and Electronic Engineering in the Federal University of Technology Owerri. He holds a Master Degree and presently doing his PhD in Electrical and Electronic Engineering. His research interest is in 5G networks and Smart Technology

How to cite this paper: Cosmas Kemdirim Agubor, Akinyinka Olukunle Akande, Reginald Opara, "Interference Mitigation in Wireless Communication – A Tutorial on Spread Spectrum Technology", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.5, pp. 26-34, 2021.DOI: 10.5815/ijwmt.2021.05.04

