Covenant Journal of Informatics & Communication Technology. Vol. 11, No. 2, Dec., 2023

ISSN: *print* 2354 – 3566 *electronics* 2354 – 3507 DOI:

An Open Access Journal Available Online

Concept of Cryptographic Operations Based on Code Division Multiple Access

Akhigbe-mudu Thursday Ehis

Department of Computer Security. Faculty of Applied Sciences and Engineering,

African Institute of Science Administration and Commercial Studies Lome-Togo

(akhigbe-mudut@iaec-university.tg)

Received: 03.08.2023, Accepted:15.11.2023,Publication:December2023

Abstract-It is a given that numerous users connect to a single satellite transponder on a daily basis in order to communicate while discussing any satellite-based technology. As a result, they must all share the resources that are available without compromising the privacy of one another. Thus, the multiple access strategy is employed to achieve this. This paper focuses on code division multiple access, which does not require time slots or frequency slots to be shared across numerous users. The primary source of communication problems is multipath fading; and if the signal undergoes any multipath fading, then the total signal may be distorted. This work presents improved correlation features of the current Walsh code through one simple yet powerful algorithm. Here, a simulation-based method is used to evaluate performance. Utilizing power delay profiles in several mobile radio propagation channels, measurement-based channel models for indoor, outdoor, suburban, and urban environments are derived. The number of taps and tap gains are then estimated using statistics on the path loss characteristics. Since the source, output is known it is compared with a delayed version of the decision device output to obtain an empirical basis for the error rate. The suggested code's performance is then compared to a few existing orthogonal and semi- orthogonal codes using a variety of performance criteria, and the conclusion is that this proposal is superior.

Keywords: Bit Error Rates, Code Division Multiple Access, Cryptography, Modulation, Signal Noise Ratio.

1.0 Introduction

As the data exchange in electronic way is rapidly increasing, it is also equally important to protect the confidentiality of data from unauthorized access. The breaches in security affect user's privacy and reputation. Text, images, audio, video, and other types of data can all be transmitted. Every form of data has unique characteristics, and several methods are employed to prevent unwanted access to private data photos. Hence, encryption of data is done to confirm security in open networks such as the internet where the multimedia applications are ever growing (kaushal et al., 2016). The study of secure communication methods when facing an opponent is known as cryptography. It addresses issues with key distribution, authentication, and encryption, to mention a few. With a picture-obscuring technology, image encryption makes images more secure by making the original image harder to read. Image encryption has been used in a variety of fields, including internet communication, telemedicine, medical science, multimedia systems, and military communication. In general, textual data differs from visuals. The concept behind image encryption is to think of a 2D picture as a 1D data stream that can be encrypted using any text-based cryptosystem. We refer to this strategy as the nave approach. This paragraph provides a basic understanding of cryptographic function and an overview of the cryptographic services.

1.1 Cryptography

The study and application of data manipulation techniques for information concealing and authentication is known as cryptography. The idea of cryptographic services is to protect data privacy, uphold data integrity, verify communication between parties, and stop parties from denying they ever sent a message. Cryptography is a very old field of study. Building strong schemes to thwart malicious efforts to cause these schemes to depart from their intended functionality is its main focus (Theresa et al., 2023). For ages, cryptographic systems, strategies, and mechanisms have been developed to protect our data. These days, it's important to safeguard against information disclosure and make sure that unauthorized parties can't access the communications being transferred. Strong techniques must be developed as precautions due to the simultaneous growth of cryptography and cryptanalysis. Data security is crucial when using both cryptographic algorithms and authentication techniques. This research aimed to provide a security framework using cellular automata. First, utilizing Code Division Multiple Access (CDA), an authentication test based on interactive proofs with zero knowledge was created. These are linked with a 2-D cellular automaton stream cipher. These instruments were chosen because of their computational and mathematical characteristics (Konoori et al., 2020).

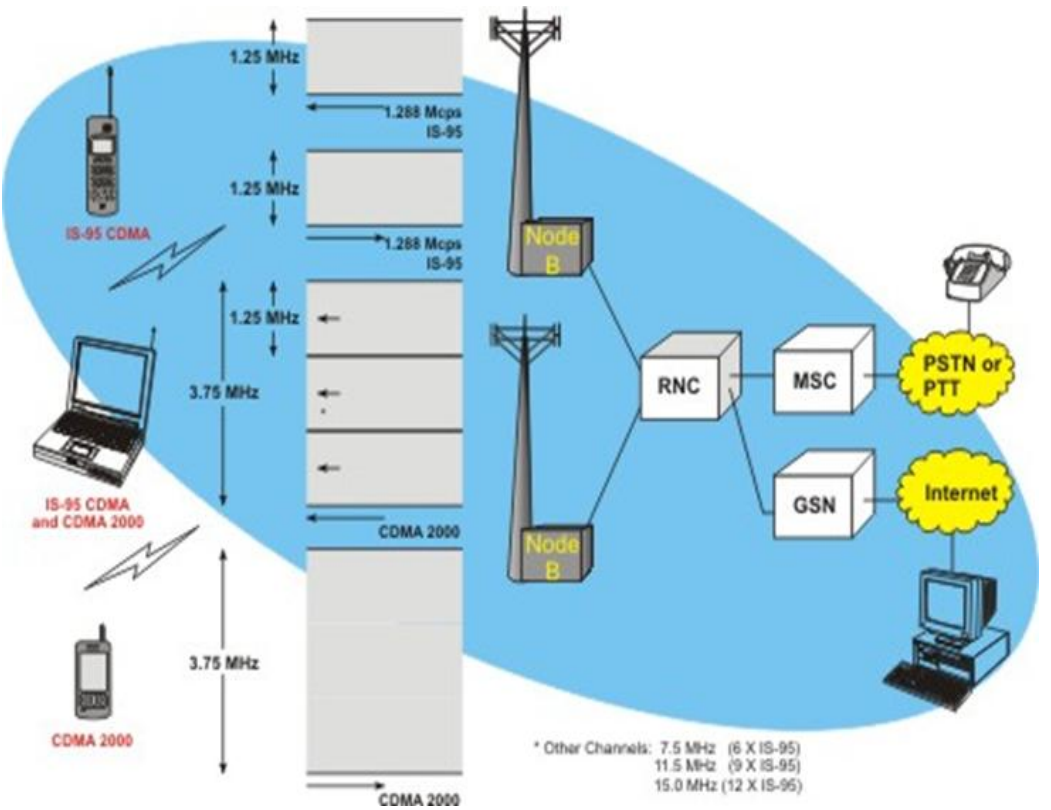


Figure 1: CDMA 2000 Radio System

An overview of a CDMA2000 radio system is presented in Figure 1. The device kinds that can be utilized with the CDMA2000 technology are depicted in this diagram. These include mobile phones that are compatible with CDMA (IS-95) and CDMA2000 multiple bandwidth radios. Typically, CDMA2000 mobile phones can function as both CDMA2000 and IS-95 CDMA mobile radios. Additionally, this diagram demonstrates how standard 1.25 MHz wide IS-95 channels can be mixed and combined into 3.75 MHz CDMA2000 channels via the CDMA2000 technology (Lubke et al., 2020).

1.2.1 Direct Sequencing Spectrum

The DSS-CDMA operating principle is as follows: two or more signals with the same bandwidth are disseminated independently using an orthogonal code that is unique to each user. The signal is merged and sent over the communication channel (Nobilet et al., 2002). In this case, the transmission energy will not change, but the bandwidth used will. The orthogonal code replica is used at the receiving end to de-spread the signals. The block diagram for DS-CDMA signal transmission and reception is displayed in f

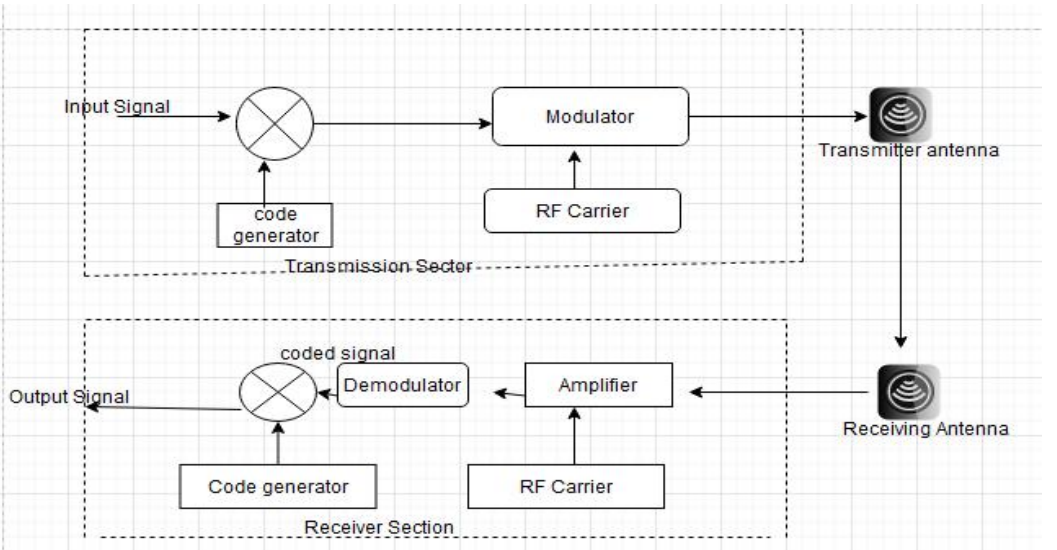


Figure 2: Principle of operation DSS-Spectrum.

The pseudorandom code generator first creates a distinct spreading code for transmission. It multiplies this random code sequence by the input data stream that the user truly wishes to send. A unique PN code will be generated for every user who is willing to broadcast over that channel in order to distribute the bit sequence. In this case, the product will only equal 1 if the data and code bits are both the same, that is, 0 or 1. If not, the product will be zero. First, the received signal is amplified to increase its level now of reception. The signal is then demodulated using a radio-frequency carrier. In this case, the sequence that was obtained looks like noise. Nevertheless, the code replica that the pseudo code generator generates multiplies the data stream that is acquired during demodulation (Mouhammed et al., 2015. The PN code created at the transmitting end and the receiving end for every single user must match in order to recover the original data stream (i.e., to de-spread). After multiplication with the de-spreading code, original data is retrieved by the receiving station. Suppose $a_1(t)$ data is multiplied with $c_1(t)$ code to produce $b_1(t)=a_1(t)+c_1(t)$ as output. Similarly, $a_2(t)$ and $c_2(t)$ gives $b_2(t)=a_2(t)+c_2(t)$ as output. The received signal will be:

$$R(t)=\sum b_1(t)+b_2(t) \qquad (1)$$

For this reason, the data must be multiplied by each user's unique code in order to obtain the true information. In this manner, simultaneous signal transmission over a channel is possible with direct spreading.

1.2.2 Spread Spectrum Concept

Spread-spectrum transmission involves the signal using more bandwidth than is necessary to transmit the data. This is achieved by using a code that is separate from the data, and the receiver uses a synchronized reception with the code to de-spread the data and recover it later (fig 3). Straight-Sequence Spread spectrum systems combine their input data with a fast spreading sequence before sending out a wideband signal. To retrieve the original data, the spreading sequence is separately created at the receiver and combined with the incoming wideband signal. Unexpectedly, in 1948, Shannon's formula was discovered a fundamental tradeoff between transmission rate, bandwidth, and signal-to-noise ratio. Hartley's rule is inexact while Shannon's formula is characteristic of the additive white Gaussian noise channel (Olivier and Jose, 2014);

Applying the Shanon formula:

$$C = B\log_2\left(1+\frac{P}{N}\right) bits/\sec \qquad (2)$$

Where,

C is Channel capacity, b/s

B is the signal bandwidth, Hz

P is the average signal power, W

N is the average noise power,

Examples

Here are two examples of the use of Shannon's Theorem.

Modem

For a typical telephone line with a signal-to-noise ratio of 30dB and an audio bandwidth of 3kHz, we get a maximum data rate of:

C = 3000 * log2 (1001) which is a little less than 30 kbps.

1.2.3 Satellite TV Channel

For a satellite TV channel with a signal-to noise ratio of 20 dB and a video bandwidth of 10MHz, we get a maximum data rate of:

C=10000000 * log2 (101) which is about 66 Mbps.

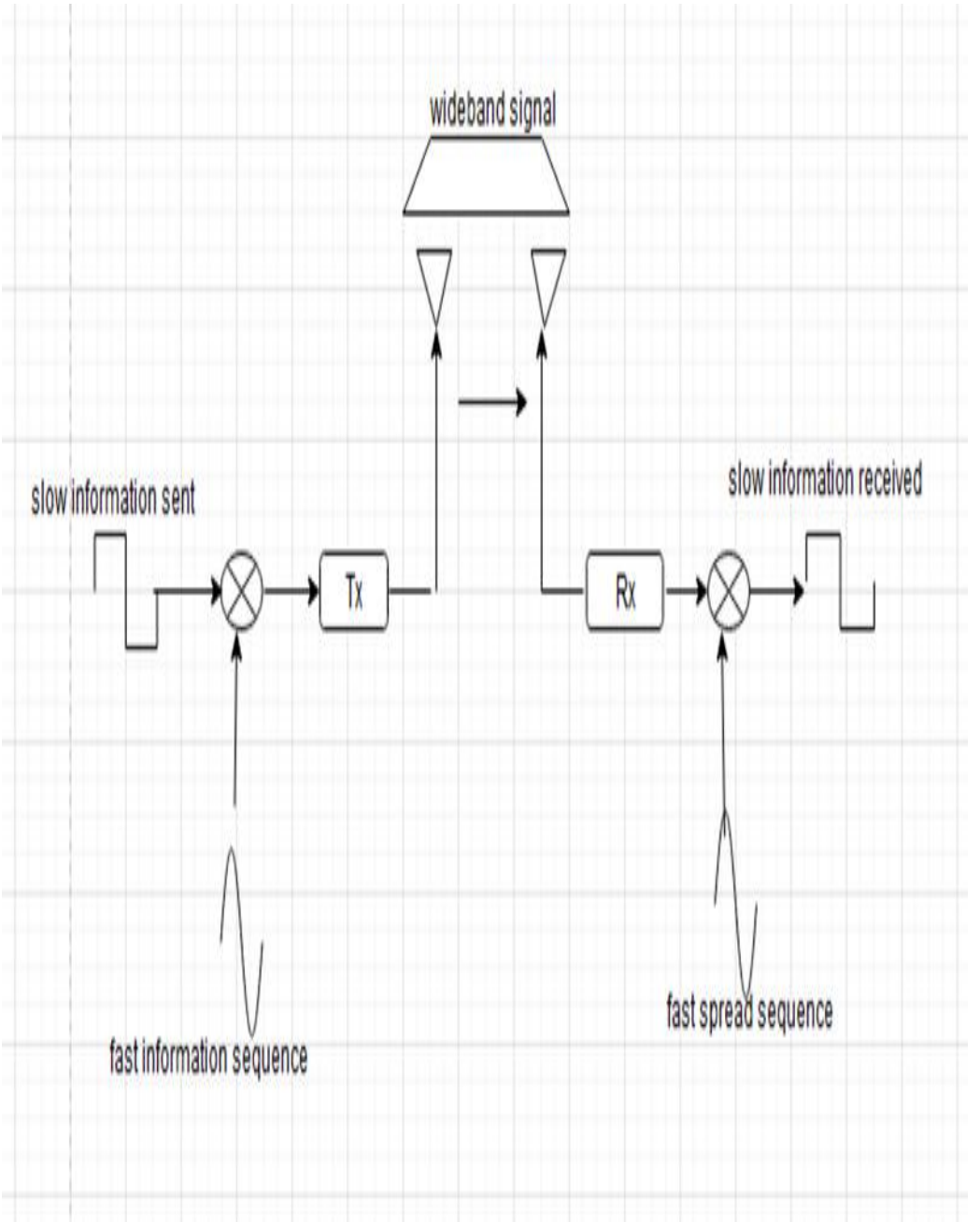


Figure 3: Spread Spectrum Concept.

1.2.3.1 Global System for Mobile (GSM)

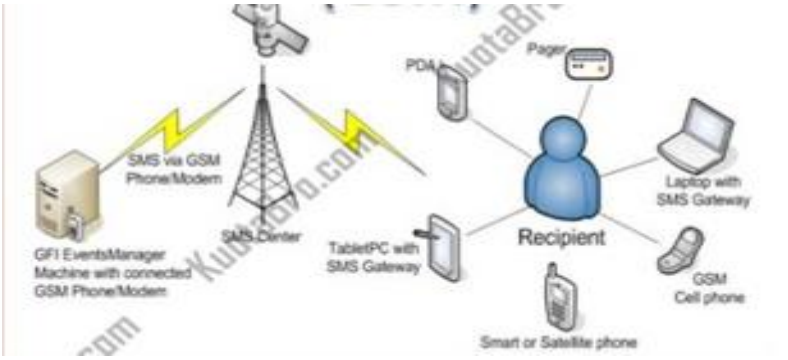


Figure 4: Shows RF Signal Processes

This diagram illustrates how a mobile phone system can employ open loop RF power regulation to maintain a consistent RF signal strength from the mobile phone to the base station, regardless of the distance between the mobile phone and the base station. Figure 4 illustrates how feedback from the mobile phone's reception component regulates the coarse (open loop) RF amplifier adjustment. The radio signal strength received from the base station is continuously measured by the mobile phone to calculate the signal strength loss between the base station and mobile phone. This diagram illustrates how the received signal strength drops when a mobile phone gets farther from the base station (Akito & Yusuke 2022). The mobile phone lowers the amplification of its own RF signal output when the received signal strength is higher; on the other hand, it increases the amplification of its own RF signal output when the received signal level is lower. As a result, regardless of the mobile phone's distance, the signal that the base station receives from it stays about at the same power level. Still, two approaches are commonly employed:

The first step is to gauge the signal's strength as it enters the antenna. Usually, dBm is used to report these values. Since the transmission line and regulated impedance antenna are the source of this, knowing the RMS voltage or current is sufficient. For example, let us say we measure the RMS voltage to be 2mV, and we have a 50-ohm antenna system. Then:

$$P = E^2_{RMS} / R \quad \text{P} = \left(0.002^2\right) / 50\Omega$$

$$= 8.10^{-8} w$$ This is converted to decibels relative to 1mW, dBm :

$$L_{dBm} = 10\log\left(\frac{p}{0.001}\right)$$

$$= 10\log\left(\frac{8.10^{-8}}{0.001}\right) = 10\log\left(8.10^{-8}\right)$$

$= -40.97$ Hence, the signal strength is about (-41 dBm)

It does estimate distances between Routers, based on the RSS (received signal strength) indoors. It is fully aware that only one will get rough estimates. For that, one has to study some radio propagation models like the ITU model for indoor attenuation which defines path loss as:

$$L = 20\log_{10} f + N\log_{10} d + p_f(n) - 28$$

3

Where,

"L" = the total path loss. Unit: (dB).

"f" = Frequency of transmission. Unit: (MHz).

"d" = Distance. Unit: metre (m)

"N" = The distance power loss coefficient.

"n" = Number of floors between the transmitter and receiver.

"P"f(n) = the floor loss penetration factor.

so to get the distance, the formula below is required:

$$d = f\frac{(-20)}{N}10\frac{L - P_f(n) + 28}{N} \qquad 4$$

$$S = \frac{P * G}{4 * \pi * R^2} \qquad 5$$

Where,

S = power Density

P = power input to antenna

G = power gain of antenna

R = distance to the center of radiation of antenna

1.3 Statement of the Problem

With the rising need for digital wireless communication systems, it is crucial to accurately anticipate both the average and instantaneous bit error rate (BER) in multipath channels. These Predictions make it possible to identify appropriate coding strategies, modulation schemes, and receiver implementations for the operational situations. Nevertheless, when many system and channel parameters are involved (such as signal noise ratio (SNR), data rate, impulse noise, and mobile speed), these predictions become quite challenging. The adjustment of these parameters is further complicated by the time-varying nature of mobile radio channels. Code Division Multiple Access (CDMA), a digital cellular technology, to enable numerous users to share the same frequency band at the same time uses spread spectrum technology. To disperse the user's signal throughout the whole band, each user is given a special code. We refer to this procedure as "spreading" the signal (Kolashi 2007). This reduces the number of users that may be served in a particular region but permits numerous users to share the same frequency band.

Moreover, CDMA's capacity may be constrained by other signals' increased susceptibility to interference. The primary source of communication problems is multipath fading. Local scatterers at nearby homes, buildings, and trees reflecting a transmitted wave in many paths mostly cause some interference. In conventional CDMA, only one carrier signal is modulated and thus if the signal undergoes any multipath fading, then the total signal may be distorted.

2.0 Background / Related Work

A variety of techniques, including elliptic curves (Kaushal et al., 2016), evolutionary algorithms (Fan & Xiang 2001), chaotic maps (Khatri and Tharani 2015), and cellular automata, are used to build cryptography. The last approach discussed is the one put forth in this research. It involves using a subset of dynamic systems that have been successfully and primarily utilized to build robust cryptosystems by utilizing both their dynamical and random characteristics. Cellular automata are used in certain cryptography applications. For example, an evolutionary computation method was presented (Rahmati & Vakili 2009) to create a quick and safe block cipher that uses non-uniform second-order cellular automata. Using the special characteristics of an image, image encryption approaches seek to safeguard the image's content more effectively and securely than traditional cryptographic techniques. A splitting cellular two-dimensional model for picture encryption automaton was proposed (Yang et al., 2001). This model is adaptable to photos with varying color depths and shares the same topology as a digital image. In order to encourage the development of sophisticated image encryption systems that provide enhanced versatility and security, this chapter discusses and summarizes a variety of image encryption techniques. An effective and essential method of safeguarding secret and classified photos is image encryption. The security of picture encryption techniques, such as AES, DES, or chaotic series type, has decreased due to advancements in computer processing power (Win et al., 2015). Consequently, those authors (Wang & Wang 1994) introduced a novel hybrid image encryption technique that uses logistic sine system (LSS) in conjunction with two-dimensional cellular automata and a finite-state machine-based DNA rule generator to safeguard secret and imperative images. Other authors (Pivanjali et al., 2017) provided an authenticated image encryption algorithm based on cellular automata. Image encryption reviewed in this passage plays a paramount part to guarantee classified transmission and capacity of images over the web. In a similar vein, cellular automata were used to develop a unique image encryption technique based on permutation–diffusion architecture. Similarly, Songchart & Hsiao (1995) put up a novel approach for image encryption that relies on the combination of chaos with reversible cellular automata (RCA). That approach made use of periodic boundary reversible cellular automata and an interweaving logistic map with complex behavior. Another picture encryption method was put forth in (Reza & Michael, 2019), and it made use of a unique class of periodic boundary cellular automata with unity attractors. Moreover, there are other uses, such a chaotic

encryption technique that functions as a pseudo-random generator (PRNG) that is built on "Life-like" cellular automata. A framework for non-uniform cellular automata is proposed in (Gutowski et al., 1999). Creating a security framework for cellular automata is the goal of this work. Using an NP-complete issue as a shared secret, an authentication test based on zero-knowledge interactive proofs is created as the initial stage. Then, as both are basic formal models for large and chaotic systems and because all the cells synchronously update their states by applying a local rule, a stream cipher created with cellular automata (CA) must be connected to it (Theresa et al., 2023). Unlike certain encryption methods like DES, AES, RC4, and VEST, our algorithm provides an authentication service that needs to be authorized before a key and the ability to encrypt or decode a file can be obtained.

2.1 CODE DIVISION MULTIPLE ACCESS

Code Division Multiple Access is referred to as CDMA. It is a technique for channel access that many radio communication technologies employ (Gorricho & Paradells 1996). It is an illustration of multiple access and digital cellular technology. Typically, mobile communication is the usage for it. A single communication channel can support multiple transmitters sending data simultaneously thanks to multiple access. Users in this system are issued distinct CDMA codes, and they have full access to the bandwidth during the entire session. Since it transmits across the whole frequency range and does not impose any frequency range restrictions on the user, it maximizes the utilization of available bandwidth. As a result, multiple users can share a frequency band using CDMA without causing excessive interference to one another. It serves as a means of access in numerous mobile phone standards.

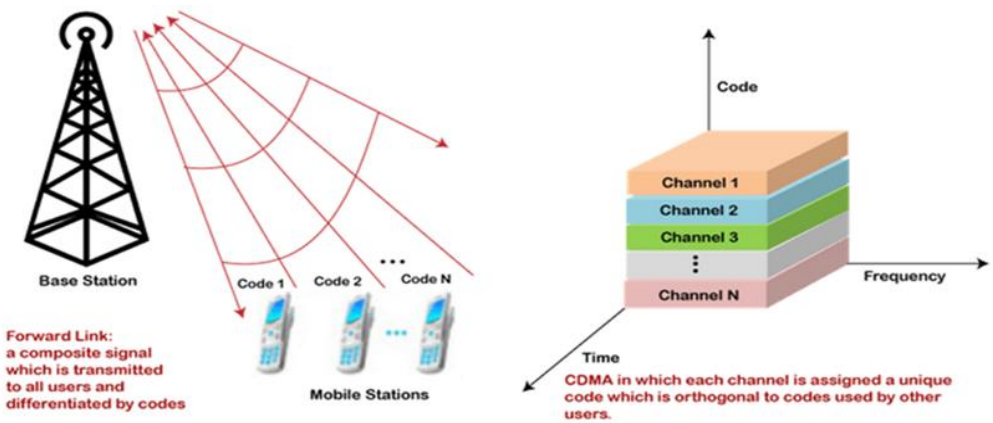


Figure 5: Shows CDMA operative.

A single direct sequence spread spectrum communication channel can have multiple channels, as seen in figure 5. Three distinct code patterns are utilized as communication routes in this example. A direct sequence spread spectrum system can create a mask, as seen in this picture, for each conversation when a receiver utilizes the reference code, allowing only information that falls within the mask to be communicated or received.

2.2 Multiple Access

It is a given that numerous users connect to a single satellite transponder on a daily basis in order to communicate while discussing any satellite-based technology. As a result, they must all share the resources that are available without compromising the privacy of one another's data. Thus, the multiple access strategy is employed to achieve this. Transmitting data from several transmitters over a single communication channel is known as multiple access. Multiple access can be implemented primarily in three ways, which are as follows: Frequency Division Multiple Access (FDMA): To enable simultaneous transmission, several frequency bands are made available to the users that are prepared to send. (TDMA) Time Division Multiple Access (Guenach & Steendam 20007).

In this case, several times are allotted to the many users in order to access the total channel bandwidth. Code Division Multiple Access (CDMA): This method assigns independent, unique codes to each user. This allows for the encoding of data and the simultaneous transmission of several users by making use of the entire channel bandwidth. This section focuses on code division multiple access, which does not require time slots or frequency slots to be shared across numerous users, in contrast to TDMA and FDMA. The data is aggregated and sent over the channel by assigning each user a unique code. At the other end, the receiving stations utilize the corresponding codes that were used by the transmitting stations to get the actual message signal of each user.

3.0 Methodology

Code division multiple access (CDMA), one of the most widely used wireless access methods, is used in current generation mobile communication systems. Over the past several decades, the design has garnered a great deal of interest from researchers. Its code family is typically divided into parts that are strictly orthogonal and non-orthogonal (near orthogonal), respectively. These members have demonstrated their use in synchronous (downlink) and asynchronous (uplink) systems (see fig 6). Walsh code is thought to be the most beneficial spreading code for synchronous applications. Nevertheless, Walsh code performs noticeably worse in asynchronous environments. As a result, several codes have been put out in an effort to address the limitations of the Walsh code. This work presents a novel attempt to improve the correlation features of the current Walsh code through one simple yet powerful algorithm. Since the proposed code of length "N" was created from code sets of length "N/4," the code generation process is recursive. The suggested code's performance was then compared to a few existing orthogonal and semi-orthogonal codes using a variety of

performance criteria, and the conclusion was that our proposal was superior.

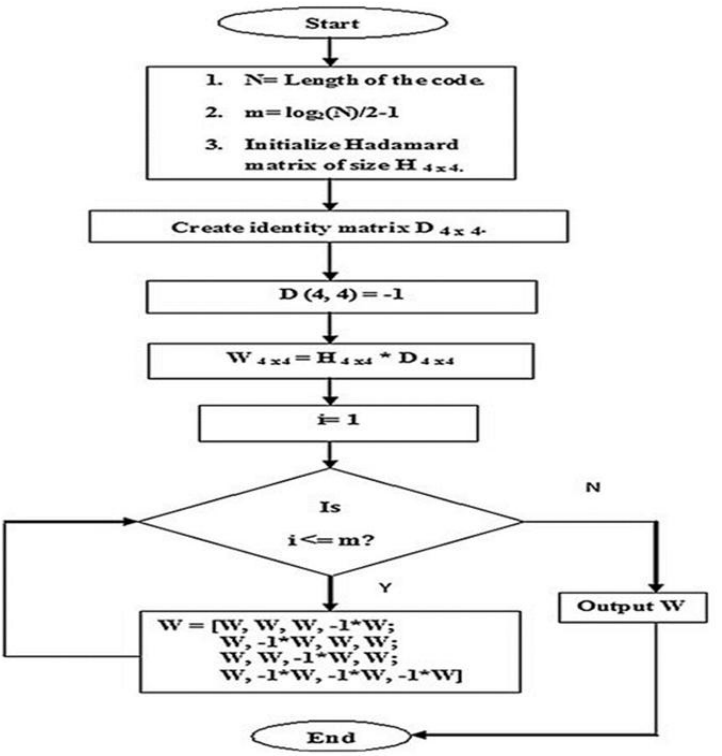


Figure 6: Flow-chart of the proposed algorithm

3.1 Python source code of CDMA:-

Import numpy as np

Print ("***\n CDMA \n***\n Enter the data bits")

D1 = int (input("Enter the D1 bit"))

D2 = int (input ("enter the D2 bit"))

D3 = int (input ("Enter the D3 bit"))

D4 = int (input ("Enter the D4 bit"))

C1 = [1, 1, 1, 1]

C2 = [1, -1, 1, -1,]

C3 = [1, 1, -1, -1]

C4 = [1, -1, -1, 1]

RC = [ ]

R1 = np.multiply (C1. D1)

R2 = np.multiply (C2. D2)

R3 = np.multiply (C3 .D3(

R4 = np. Multiply (C4 .D4)

Resultant_channel = R1+R2+R3+R4 ;

Print (“Resultant channel”, resultant_channel)

Channel = int (input(“Enter digits as C1 =1, C2 = 2, C3 = 3, C4 = 4) \n Enter the station to listen;”))

If channel = = 1;

RC = C1

El if channel = = 2;

RC = C2

El if channel = = 3;

RC = C3

El if channel = = 4;

RC = C4

Inner product = np.multiply (resultant_channel, RC0

Print (“inner product”, inner product)

Res 1 = sum (inner_ product)

Data = res 1\n (inner_productprint)

Print (“data bit that was sent”, data)

3.1.1 Evaluation

Now, consider an example to understand signal transmission and reception through CDMA (figure 7a).

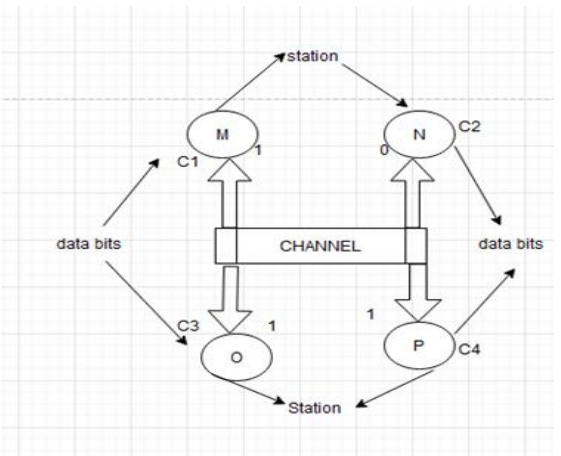


Figure 7a: CDMA Signal Transmission and Reception.

Assume that 1, 0, 1, 1 is being transmitted separately by stations M, N, O, and P. Furthermore, every single one of them has a distinct code sequence (C1, C2, C3, C4) with orthogonal codes. We will employ polar signaling to represent data bits and code bits; therefore, Binary 0 will be represented as -1 and Binary 1 as +1 (or 1). As a result, (1, -1, 1, 1) will be the data vector, or (M, N, O, P).

3.1.2 Parameter for choosing codes:

Any two stations' codes multiplied together must result in a total of zero resulting bits. It should be noted that the first bit of another sequence when determining the product of two data sequences always multiplies the first bit of one sequence. The second bit with the second bit, and so forth. Let us assume that C1*C4 = (1, 1, -1, -1).(1, –1, –1) = (1, –1, –1, 1)

When all four resultant bits are added together, we will obtain 0. Codes are therefore orthogonal in nature. The total number of stations must be indicated by the sum of the results received when a code sequence is multiplied by itself. Assume that C2*C2 equals (1, -1, -1, 1). 1, 1, 1, 1, = (1, -1, -1, 1) Thus, 1+1+1+1 will result in 4. Confirming, that four stations are transmitting simultaneously.

Transmission: As we previously explained, in order to implement DS-CDMA, data bits must first be multiplied independently by their corresponding codes. As a result, the product of the code bit and the data bit is as shown in figure 7b. Now, over the channel, the bits will be transmitted combinedly.

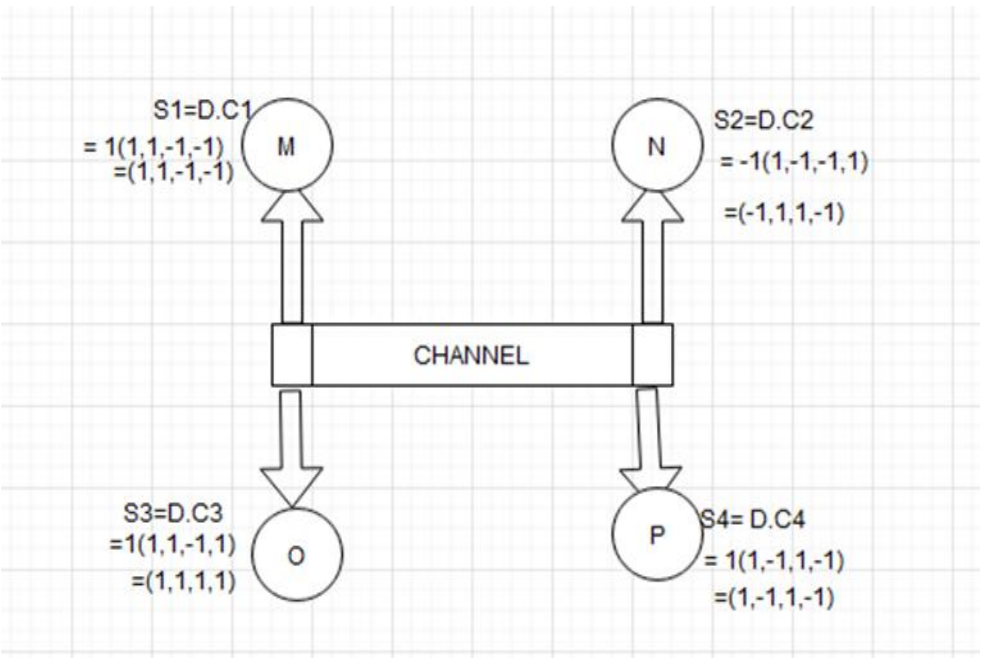


Figure 7b: transmission result of data bit sequence

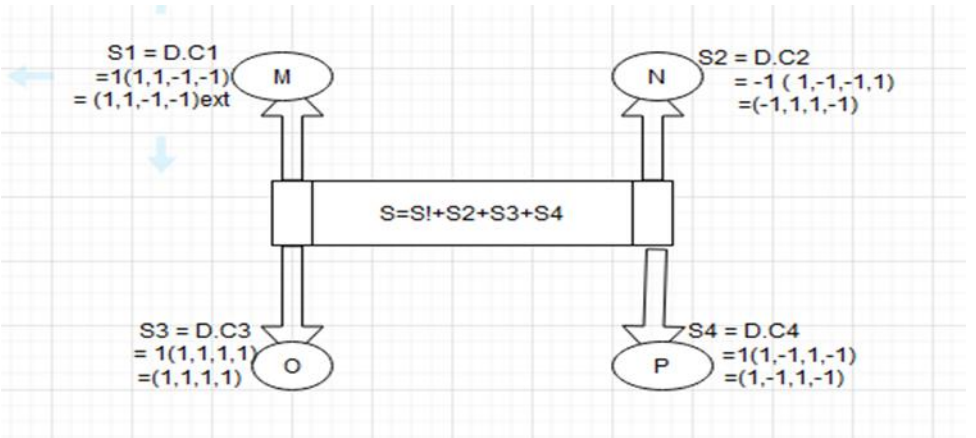


Figure 7c: Bit transmission in sequence

The complete bit sequence to be transmitted will be produced by adding the bits according to their positional sequence: see figure 7d and 7e respectively.

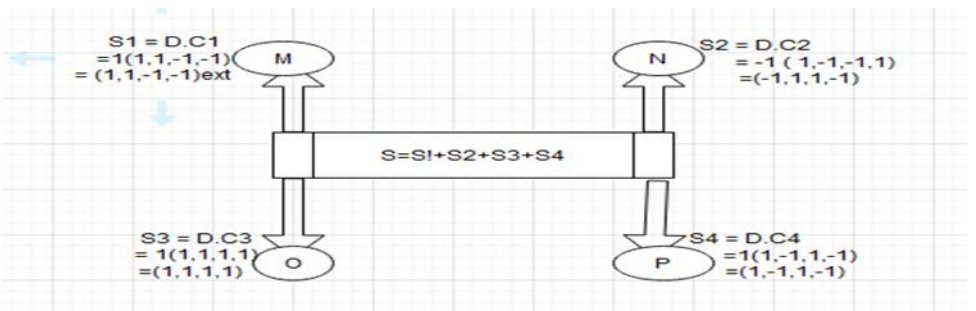


Figure 7 d: Complete bit sequences transmission

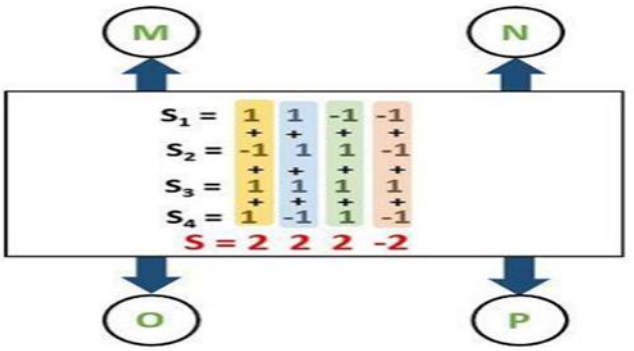
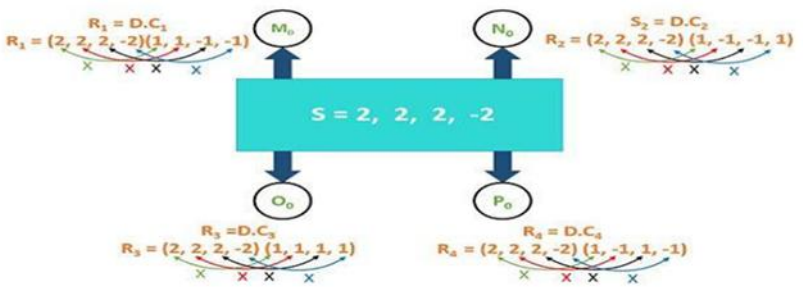


Figure 7e: Complete bit sequence transmission

2, 2, 2, -2 will be the sequence that is sent over the channel. The recipient will receive the aforementioned sequence. Now, each receiving station needs to know the code sequence of the corresponding sending station in order to extract the actual information from this received (coded form) data. Here, the received bit sequence is multiplied by the corresponding code stream for each receiver to obtain the original data sequence (see figure 7f).



R_1 = (2, 2, -2, 2)

R_2 = (2, -2, -2, -2)

R_3 = (2, 2, 2, -2)

R_4 = (2, -2, 2, 2)

Figure 7 f: Confirmation of the original data bit sequence.

Hence , by summing every bit of the sequence and dividing it with total number of transmitting stations, will result in the originally transmitted data bit. So calculating for each receiving station, will result in the following:

$R_1 =$ (2+2-2+2) / number of stations $= \frac{4}{4} = 1$

$R_2 = \left[-2+2-2-2\right] / number.of.stations =$

$R_3 = \left[2+2+2-2\right] / number.of.stations = \frac{4}{4}$

$\left[2-2+2+2\right] / number.of.stations = \frac{4}{4} = 1$

In accordance to polar signaling, 1 denotes binary 0ne and -1 denotes binary 0. Therefore, the data bits received at each receiving station will be (1,0, 1 , 1)

3.2 .0 Simulation Model

Two critical parameters that affect any communication system's performance are the signal-to-noise ratio (SNR) and the total bit error rate (BER) of the cumulative signal distortions. For the simulated communication system model, these factors are estimated using functional descriptions

3.2.1 Estimating BER

Regarding a digital communication system, the behavior of the system that causes errors is the pertinent performance metric. There are numerous ways to categorize this behavior. The scenario in which a system transmits symbols and the bit error rate (BER) is the average production of errors in an infinitely long sequence is the most frequently examined (4). This is a description of one of the simulation-based methods for BER estimation.

Monte Carlo Simulation

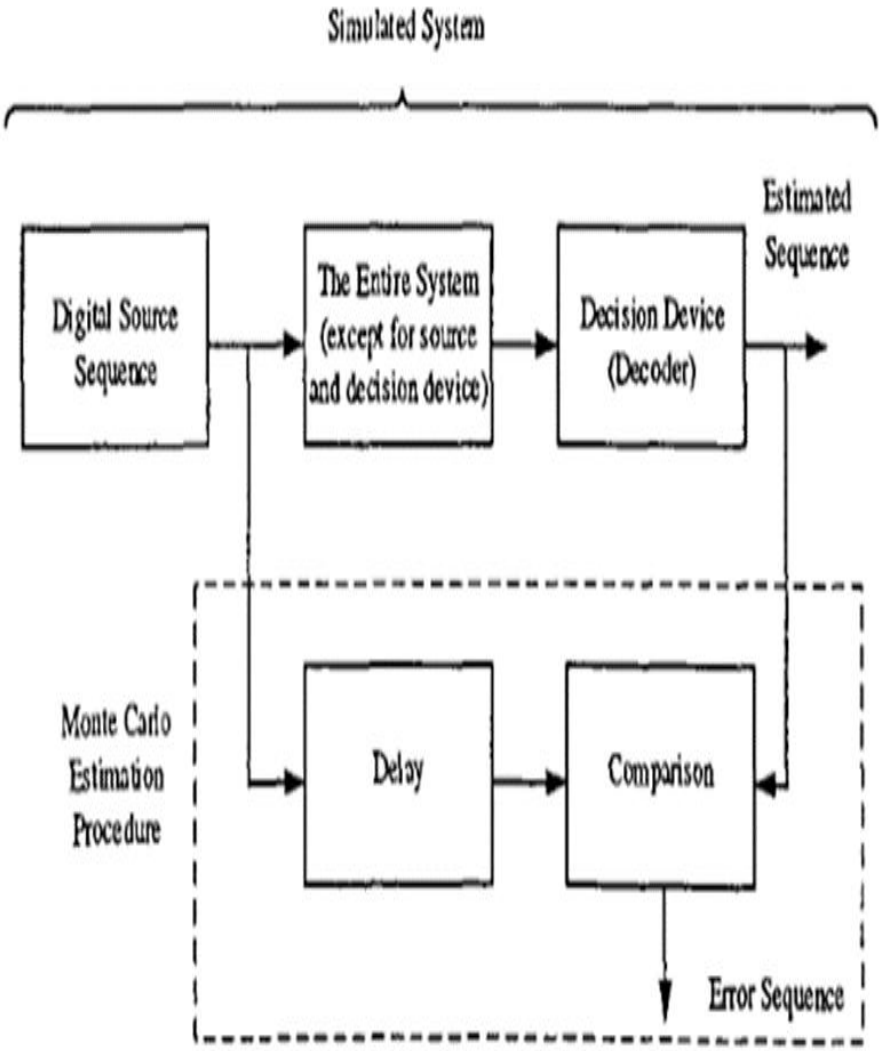


Figure 8: System Simulation Mode

The process of implementing a series of Bernoulli trials in which the number of "successes" (errors) is divided by the total number of trials is known as Monte Carlo. As seen in fig. 8, this approach makes no assumptions about the system or the input processes. An empirical foundation for the error rate is obtained by comparing the known source output with a delayed version of the decision device output. Given the assumption of perfect carrier and symbol synchronization, knowledge of this relative delay is implied. One way to write the BER is as

$$b = \int_{v \in D_0} f_v(v)\, dv \qquad 6$$

Where f_v is the pdf of sampled zeros at sampling epoch τ, D_0 is the region of v that corresponds to an error. An error indicator function can be defined such that:

$$H(v) = \begin{cases} 1, v \in D_0 \\ 0, v \notin D_0 \end{cases} \qquad 7$$

And equation (6) can be rewritten as

$$b = \int_{-\infty}^{\infty} H(v) f_v(v) dv \qquad 8$$

Which is equivalent to :

$$b = E\left[H(v)\right] \qquad 9$$

Where E is the expectation operator, since a natural estimator $\hat{b}$ of the expectation is the sample mean, it can be expressed as

$$\hat{b} = \frac{1}{N_0} \sum_{i \in I_0} H(v_i) \qquad 10$$

Where $v_i \hat{=} v(t_i)$ is the sequence of symbol spaced samples of the decision voltage, I_0 is an integer set that contains all i such that t_i corresponds to a sampling a zero and N_0 is the number of elements in the set. Hence $H(v_i)$ acts as an error detector, the summation is an error counter and $\frac{1}{N_0}$ is the normalizing factor. Assuming all symbols have the same probability of occurrence, equation (100 can be extended to apply irrespective of the symbol, namely:

$$\hat{b} = \frac{n(N)}{N} \qquad 11$$

Where N is the total number of symbols processed and n is the total number of errors observed. As $N \to \infty$, $\hat{b}$ converges to b by the law of large numbers. $H(v_i)$ is implemented using an XOR gate since the transmitted alphabet consists of $\{0,1\}$. The summation and normalization are done on the MATLAB workspace after the simulation run is completed. Thus equation (11) is implemented as the BER estimator block.

3.2. 2 SIMULATION RESULT

Bit error rate in a communication system is the ratio of number of error bits and total number of bits transmitted during a specific period. It is the likely- hood that a single error bit occur within received bits, independent of rate of transmission (Khatri & Tharani 2015).There are many ways to reducing BER. At first, considered most commonly channel that is AWGN(Additive White Gaussian Noise) channel. As shown in the graph (fig 9), that is Eb/No increases as BER decreases.

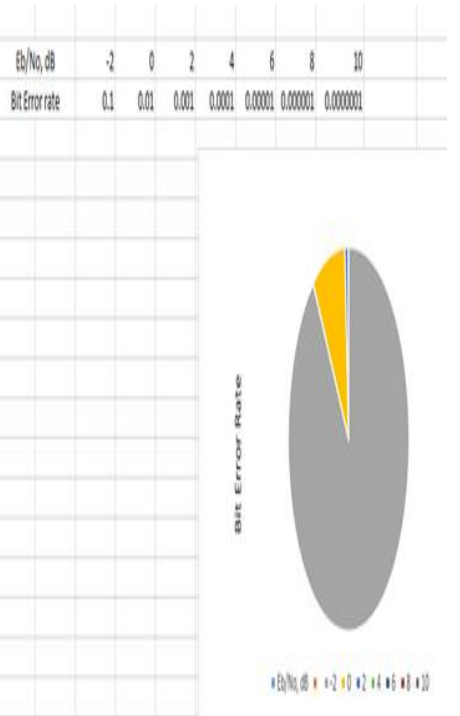


Figure 9: Graph of BER Performance

The fading caused by many broadcast signal echoes arriving at the receiver via various pathways is what sets apart a multipath channel. Intersymbol interference from time-delayed echoes can lead to mistakes in digital systems when they overlap. However, the application of channel equalization and diversity (RAKE receiver) techniques can enhance the system's performance. The number of pathways and average (or rms) delay spreads from the power delay profiles in Figure 9 were estimated, and the signal and noise components were distinguished using a noise threshold of -94 dBm or 35 dB below the strongest component. By itself, the delay spreads don't offer very accurate metrics for system assessment. Therefore, statistics regarding the number of paths and their latency are more valuable. The design of hardware and software simulators, such as diversity combining receivers, is then based on these findings

4. Conclusion

As the demand for digital wireless communication systems grows, the accurate prediction of average and instantaneous BER in multi path channels becomes increasingly important. These predictions enable the determination of acceptable modulation methods, coding techniques and receiver implementations in the operating environments. Depending on the degree of speech activity, a high number of users can be accommodated in one radio channel using the CDMA direct sequence spread spectrum approach, which is included here [2]. In a time-dispersive radio propagation channel, this property allows resolution of multipath components and offers immunity against jamming signals [3]. Here, a simulation-based method is used to evaluate performance. Utilizing power delay profiles in several mobile radio propagation channels, measurement-based channel models for indoor, outdoor, suburban, and urban environments are derived. The number of taps and tap gains are then estimated using statistics on the path loss characteristics. Utilizing a simulated system model, the effectiveness of a sophisticated CDMA-based mobile communication system is assessed. Local scatterers such nearby homes, buildings, and trees reflecting a transmitted wave in many paths mostly bring it on interferences. The channel is referred to be a Rayleigh fading environment if there are no direct waves present in addition to the reflected waves; otherwise, it is considered a Rician fading environment.

Reference

A. K. Khatri and L. Tharani (2015):", "An approach to compare the developments in performance of multicarrier CDMA system," *International Conference on Computing, Communication & Automation*, Greater Noida, India, 2015, pp. 1226-1231,

https://doi.org/10.1109/CCAA.2015.7148601

Akito Chiba and Yusuke Sunaga (2022):"RF signal estimation utilizing low-frequency beat signal due to harmonics of phase-modulation light wave". *Proceedings of the 2022 Conference on Lasers and Electro-Optics Pacific Rim Technical Digest Series (Optica Publishing Group*, 2022), paper P_CTh6_05 • https://doi.org/10.1364/CLEOPR.2022.P_CTh6_05

Debolina Chakraborty1 • Milan Kumar Tarafder1 •Abhijit Chandra (2016): "A New Walsh-Like Near Orthogonal (WNO) Sequence for Asynchronous CDMA System", Wireless Pers Commun (2016) 88:711–729 https://10.1007/s11277-016-3197-9

FAN Ping-yi;XIA Xiang-gen (2001) A New Multi-Rate Detection Algorithm for IS-95A CDMA System[J]. ACTA ELECTONICA SINICA, 2001, 29(4): 471-474

G. Gutowski, L. Jalloul, E. Golovin, M. Nakhjiri, N. Yousef and P. DeClerck (1999), "Simulation results of CDMA location finding systems," 1999 IEEE 49th Vehicular Technology Conference

(Cat. No.99CH36363), Houston, TX, USA, 1999, pp. 2124-2128 vol.3, doi: 10.1109/VETEC.1999.778426.
https://doi.org/10.4236/ijcns.2015.87027

J. -L. Gorricho and J. Paradells (1996)" "Evaluation of the soft handover benefits on CDMA systems," Proceedings of ICUPC - 5th International Conference on Universal Personal Communications, Cambridge, MA, USA, 1996, pp. 305-309 vol.1,
https://doi.org/10.1109/ICUPC.1996.557901

Kaushal T. Kevadia, Archana M. Nayak, Kaushik S. Patel, Brijesh U. Patel (2016):" A Literature Survey on Image Encryption". 2016 IJSRSET | Volume 2 | Issue 6 [(2) 6: 741-746]

Kolahi, S.S. (2007). Analysis of results in simulation and modelling of CDMA systems. Proceedings of the 12th IEEE Symposium on Computers and Communications (ISCC'07). 679-684. https://doi.org/10.1109/ISCC.2007.4381482

Kordnoori Shirin, Mostafaei, Hamidreza, kordnoori , Shaghayegh, Ostadrahimi, Mohammadmohsen (2020):" Evaluating The CDMA System Using Hidden markov and Semi Hidden markov models". The Journal of Technology and Science; Surabaya Vol.31, Issue 3, dec 2020): 295-308, https://doi.org/10.12962/j20882033.v31i3.7016

M. Guenach and H. Steendam (2007):" Performance Evaluation and Parameter Optomization of MC-CDMA " in IEEE Transactions on Vernacular Technology, vol. 56, N. 3. Pp. 1165-1175. May 2007. https://doi.org/10.1109/TVT2007 895605

M. Lübke, J. Fuchs, V. Shatov, A. Dubey, R. Weigel and F. Lurz (2020), "Simulation Environment of a Communication System Using CDMA at 77 GHz," 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 1946-1951,
https://doi.org/10.1109/IWCMC48107.2020.9148403

M. Rahmati and V. T. Vakili (2009) "STBC CDMA System Simulation in MIMO Channels with Correlative Model," 2009 International Conference on Computational Intelligence, Modelling and Simulation, Brno, Czech Republic, 2009, pp. 43-47, https://doi.org/10.1109/CSSim.2009.50

Mouhamed Fadel Diagana, Serigne Bira Gueye (2015):" Modeling and Simulation of CDMA Codes in Scilab". International Journal of Communications, Network and System Sciences > Vol.8 No.7, July 2015

Nobilet, S., Hélard, J., & Mottier, D. (2002). Spreading sequences for uplink and downlink MC-CDMA systems: PAPR and MAI minimization. Eur. Trans. Telecomm., 13, 465-474.

Olivier Rioul and José Carlos Magossi (2014):"On Shannon's Formula and Hartley's Rule: Beyond the Mathematical Coincidence". Proceedings of the MaxEnt 2014 Conference on Bayesian Inference and Maximum Entropy Methods in Science and Engineering. Entropy 2014, 16(9), 4892-4910; https://doi.org/10.3390/e16094892

Priyanjali, K.S., & Ramanjaneyulu, B.S. (2017). Performance of MC-CDMA system with various orthogonal spreading codes in multipath Rayleigh fading

channel. 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 309-312. https://10.1109/ICSTM.2017.8089175 Corpus ID: 35555519

Reza Zekavat; R. Michael Buehrer (2019):"Fundamentals of Received Signal Strength-Based Position Location," in Handbook of Position Location: Theory, Practice, and Advances, IEEE, 2019, pp.369-404, https://doiorg/10.1002/9781119434610.ch11

Songchar Jiang and M. . -T. T. Hsiao (1995): "Performance evaluation of a receiver-based handshake protocol for CDMA networks," in IEEE Transactions on Communications, vol. 43, no. 6, pp. 2127-2138, June 1995, https://doi.org/10.1109/26.387454

Theresa Olubukola Omodunbi, Ayomide S. Akindutire, Tolulope Moyosore Awoyelu, Rhoda N. Ikono, Ishaya P. Gambo (2023): "Integrating Asymmetric Cryptographic Digital Wallet for Online Services in Nigeria", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.15, No.3, pp. 29-40, 2023. https://doi.org/10.5815/ijieeb.2023.03.03

Wang, SW., Wang, I. (1994). Simulation Results on CDMA Forward Link System Capacity. In: Holtzman, J.M., Goodman, D.J. (eds) Wireless and Mobile Communications. The Springer International Series in Engineering and Computer Science, vol 277. Springer, Boston, MA. https://doi.org/10.1007/978-1-4615-2716-9_10

Win ZeyarKyaw, Su Su Yi Mon, Hla Myo Tun (2015):" Modelling and Simulation of Multicarrier Code Division Multiple Access (CDMA) System using RAKE receiver". International Journal of Emerging Engineering Research and Technology Volume 3, Issue 6, June 2015, PP 72-77

YANG Guang;YANG Da-cheng;LI Lu;GUO Jin-jun (2001). The System Level Simulation of Wideband CDMA Mobile Communication System [J]. ACTA ELECTONICA SINICA, 2001, 29(4): 464-470

Graphical Abstract file