Optimized PN Sequence Generation using Elliptic Curve Cryptography and UWD

Allamprabhu V. Kolaki, Sunil T. D, G.A.Bidkar, S.V.Viraktamath

Abstract*—The Code Division Multiple Access (CDMA) technique is developed for military applications and also utilized in civilian application for the need of information hiding and secure signal transmission. The major issue occurs during the transmission in CDMA system is the security of data. In this proposed work, Universal Wind Driven (UWD) optimized ECC based PN sequence generation. Initially Pseudo Noise (PN) sequence is generated on the basis of Elliptic Curve Cryptography (ECC). The PN sequences have the characteristics of being like random noise with low correlation compared to any other sequence in the set. The original data is combined with optimal PN sequence and modulated by BPSK modulation and transmitted through the AWGN channel and demodulated by BPSK demodulation. The performance results proved that proposed work is efficient compared to other techniques.

Index Terms*— Code Division Multiple Access, Elliptic Curve Cryptography, Pseudo Noise sequence, Universal Wind Driven.

I. INTRODUCTION

Starting late, wireless adaptable correspondence has ends up making progress to fulfill the need of wireless associations which are obliged with low execution in the present establishments. The standard transmission medium is shared by a couple of customers with the spread perspective multiple access [1, 2]. Precisely when detached and the access degrees of progress like time division multiple access (TDMA) and frequency division multiple accesses (FDMA), past what many would think about possible, most wonderful of interference minimization, high security vivacious execution, low factor of frequency reuse and high frequency effectiveness is certified with CDMA [3, 4]systems. Multi course development of the current CDMA structure close to the direct sequence spread spectrum (DS-SS) shows multiple access interference (MAI) and multipath interference (MPI) [2].

The spread range uses wide band of noise signals which makes the specific check structure complex. The pseudo-self-intensely hot code is showed up for spreading the band and it didn't rely on the transmitted data. To give security [5], the pseudo noise (PN) sequences are passed on with uniform spread or certified independency with the sequence of 1's and 0's. Sporadic sequences [6] other than transmitted an impression of being extraordinary. In Direct-Sequence (DS) CDMA structure, the high transmission limit pseudo-noise code is imitated with the customer signal. The going with sign is used in radio channel which uses the structures like keep influencing and direct sequence for military reason [7, 8].

The spreading improvements are used by the DSSS systems [9-12] and related CDMA structures at the hour of level jumbling channel are used [8]. One information picture is spared more than a few host coefficients in SS embeddings structures [13, 14]. Secure access is required in CDMA structure with novel PN advancement age for spreading. For recovering the substance the snoop ought to be de spread. To make the strikes in light of the affiliation is computationally infeasible by using vivacious chip flipping in spread get-together [15].

In light of the upsides of this game-plan age [16, 17], the social affair is gotten with different states, support of various access progress, attestation from staying, transmission security at physical layer, wide band with splendid relationship, control in multi way conditions, and low probability of impedance [18]. DSSS structures has been showed up and detached in two or three current alliance. The structure of these systems relies on different classes, (I) plan, improvement, synchronization of the amazed spreading groupings, (ii) BER execution evaluation for theoretical and numerical for the annoying based direct advancement/CDMA (DS/CDMA) correspondence systems under the specific sort of transmission channels [19, 20].

In order to value these security issues, the UWD improved ECC spreading codes is proposed. The UWD streamlining method gives perfect decision of the PN get-together codes pulled back and other decision moves close. Here, ECC structure is used for the hour of PN get-together codes. This structure makes to pick and out more competently instead of discretionary picking the characteristics. This proposed structure gives progressed PN approach.

II. RELATED WORKS

M.Tafaroji and A. Falahati et al had proposed the encryption circuit to spreading code to improve the security of CDMA. The security made in like way is basically associated with the multifaceted idea of the used encryption figuring. Since the encryption checks security is astoundingly strong, it is sensible for any kind of data correspondences.

Revised Version Manuscript Received on 10 September, 2019.

Allamprabhu V. Kolaki, Asst. Prof. Dept. of ECE KLS VDIT Haliyal, Karnataka, India.(Email: allamvk28@gmail.com)

Sunil T. D, Asst. Prof. Dept. of ECE SSIT Tumkur, Karnataka, India. (Email: sunil.tumkur@gmail.com)

G.A. Bidkar, Professor Dept. of ECE SDMCET Dharwad, Karnataka, India.(Email: sunil.tumkur@gmail.com)

S.V. Viraktamath, Asst. Prof. Dept. of ECE SDMCET Dharwad, Karnataka, India. (Email: svvmath@gmail.com)

The mix of encoded and decoded M-system is used as a spreading code to help the structure execution, and the upside of this blend is considered from the impedance level and the security point of view. An ideal figuring for the key exchange is made [21].

Abbas Salman Hameed et al offered balanced wild indication and Alamouti MIMO plan are used to achieve a higher security from MAI in direct improvement code division isolating access (DS-CDMA) structure. It is seen that BER execution decreases as the degree of customers increases [22].

M.I.Khalil et al had made wideband sign age by circularly moving the spreading code by n places where n watches out for the estimation of a got byte of the information signal. The standard information sign is emptied at the recipient by get together with the got sign with a quickly made duplicate of the spreading code (256-piece). The state of most character blowing estimation of the yielded cross-affiliation vector (relationship top) considers to the estimation of one byte of the information signal. The consistency of data transmitted through this structure indicated concerning Bit Error Ratio (BER) is surveyed versus the Signal-to-Noise-Ratio (SNR).It is found in the result that the estimation of BER high [23].

AbolfazlFalahati and Nader Sanandaji et al made two structures called 'Nested DSSS' and 'Interleaved DSSS' are to spread an antipodal PAM data sign to improve the present system. In the settled perspective, the purpose of imprisonment of multi-customer impedance that identifies with the neutralizing activity power is lessened significantly, so this system can give sporadic condition of security while an unparalleled BER execution is in like manner made, isolated and a standard DSSS structure. The interleaved DSSS that attempts a key-based change figure to interleave the M-framework bits inside the mixed code bits prompts an enduringly raised level of security limited and the settled DSSS and checked DSSS methods [24].

S. B. SumithBabu et al. had made fulfilling multi customer approaches for improving the sharing most remote degrees of spreading plot between the clients. To give PN progress security, a goliath most remote point and safe set-up to be express, 1D-Bernoulli-messy framework formed CDMA (BCC-CDMA), was showed up. It was checked with ordinarily even irritated developments in which the 1D-Bernoulli Map produces NxN structure. The relationship properties were required to be improved for BCC-CDMA [25].

III. PN SEQUENCE GENERATION

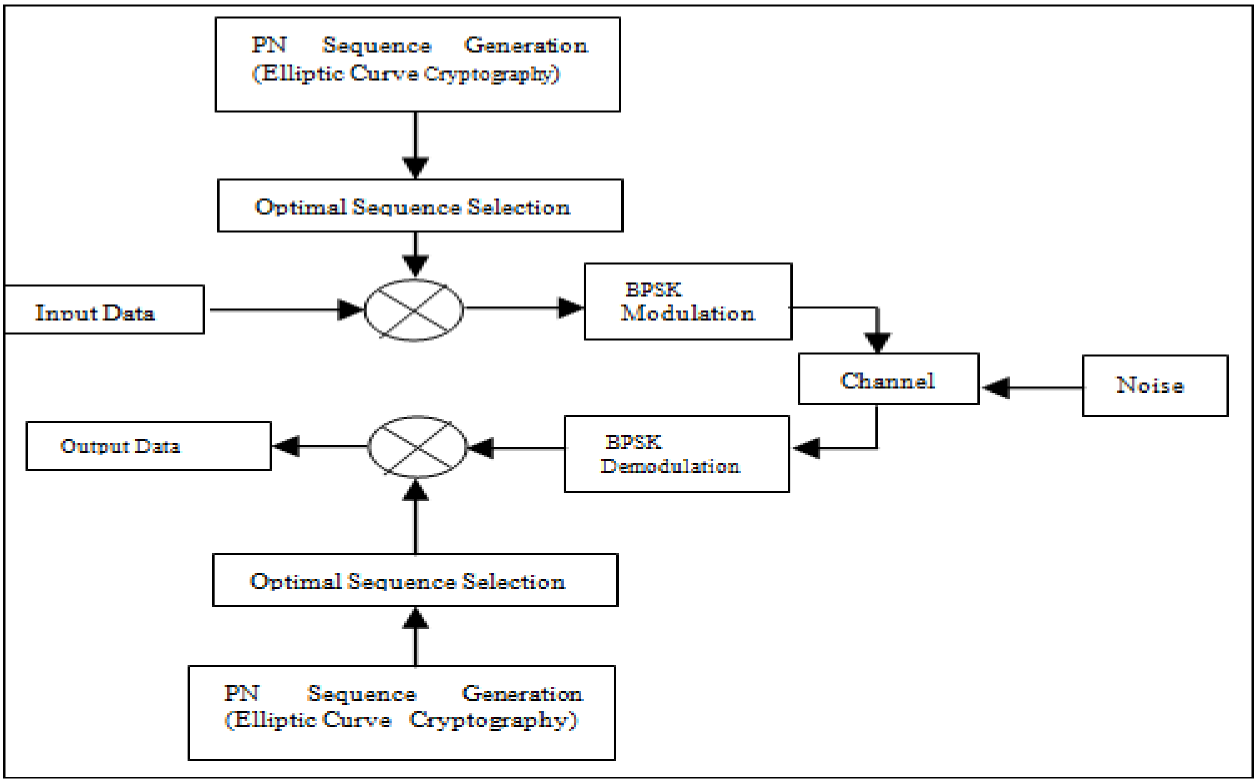

PN Sequence Generation (Elliptic Curve Cryptography)
Optimal Sequence Selection
Input Data
BPSK Modulation
Channel
Noise
Output Data
BPSK Demodulation
Optimal Sequence Selection
PN Sequence Generation (Elliptic Curve Cryptography)

Fig 1: Block diagram for CDMA system based on ECC and UWD optimized algorithm approach

A. Elliptic Curve Cryptography

A pseudo certain parallel way of thinking is a semi-superb movement as in it shows up sporadically inside the get-together division, achieving the necessities of the haphazardness, notwithstanding the entire party turns out uncertainly. To a general spectator the party shows up totally self-picked, paying little respect to a client who examines the course by which the movement is made a tremendous piece of its properties are known. The PN groupings have certain charming properties, which are mauled in various applications. Because of their surprising auto affiliation two cloud PN movements can be conceivably stage synchronized, paying little heed to when one of them is sullied by intensification. A PN system is a perfect test signal, as it empowers the offbeat properties of a pushed sign and can be sensibly made. Elliptic curve cryptography (ECC) is the endless standard for open key cryptography and is being empowered by the national security office as the staggering procedure to ensure the private correspondence between parties. Elliptic curve number changing is for both encryption and incited checking. Victor and Neil Koblitz started this usage of the open key cryptography as accomplishing substitute and depicted by

$$y^2 = x^3 + ax + b \qquad (1)$$

Think about the elliptic curve

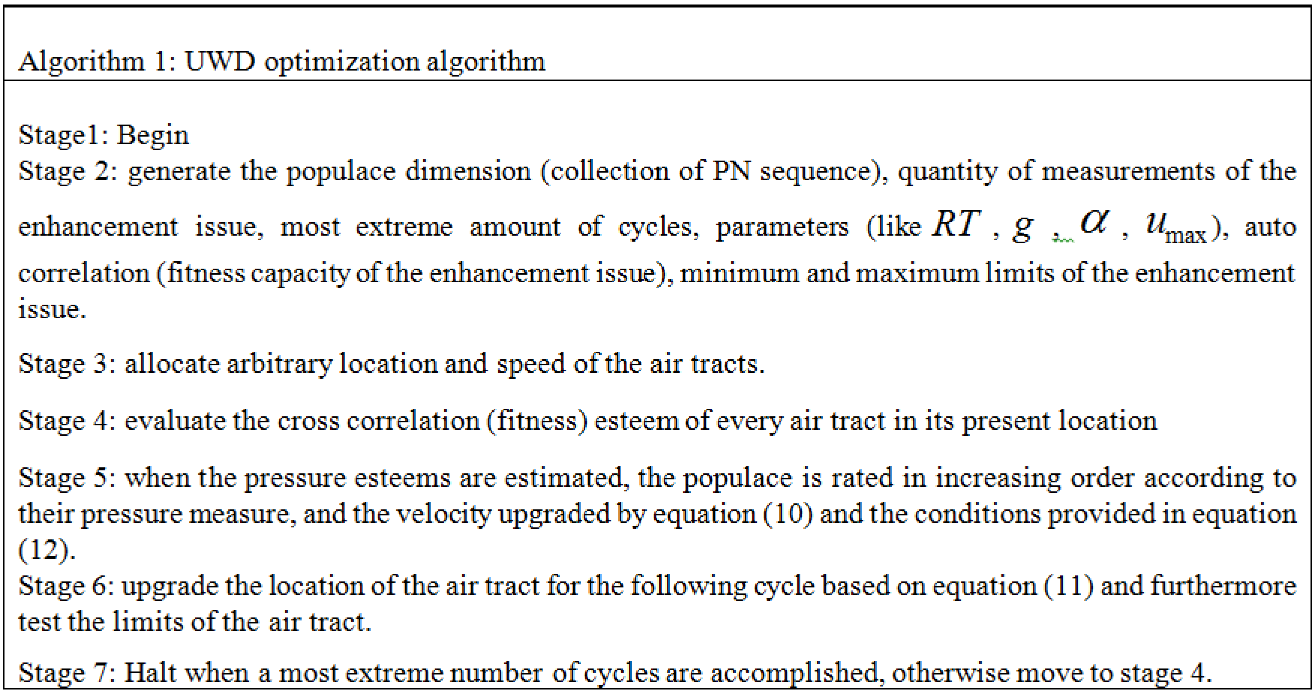
In light of this condition optional PN groupings are made. Regardless, if the parameters that are picked unpredictably are not picked appropriately, this heading in wrong discernments and the figure substance made won't be decoded to plain message fittingly. Along these lines, there is a sincere to use universal wind driven advancement (UWD) estimation.

B. Impeccable party decision subject to UWD improvement approach

The UWD improvement estimation moved by the world's air where the wind blows is attempting to change the level unevenness in pneumatic power. This framework is working ward upon people based iterative heuristic everything considered improvement for multi-dimensional and multi-express issues to apply necessities on the interest zone. UWD progress is dull from other streamlining estimations, which people based heuristic iterative structure can be found for clear the multi-dimensional improvement issues.

The Newton's second law of headway found the opportunity to express the advancement of air coasts inside earth's air. The UWD progress estimation has additional terms in the speed update condition joining attracting centrality and Coriolis powers, which gives life and extra degrees of opportunity to the figuring when pulled back and other particle based streamlining check. In setting on barometrical progress of unessential little air pack isolating over a N dimensional mission for after a zone, the UWD progress estimation supported.

The total power executed on an air bundle makes it to revive with expanding speed a comparative route as the realized total power.



Algorithm 1: UWD optimization algorithm

Stage1: Begin

Stage 2: generate the populace dimension (collection of PN sequence), quantity of measurements of the enhancement issue, most extreme amount of cycles, parameters (like RT , g , α , $u_{\max}$), auto correlation (fitness capacity of the enhancement issue), minimum and maximum limits of the enhancement issue.

Stage 3: allocate arbitrary location and speed of the air tracts.

Stage 4: evaluate the cross correlation (fitness) esteem of every air tract in its present location

Stage 5: when the pressure esteems are estimated, the populace is rated in increasing order according to their pressure measure, and the velocity upgraded by equation (10) and the conditions provided in equation (12).

Stage 6: upgrade the location of the air tract for the following cycle based on equation (11) and furthermore test the limits of the air tract.

Stage 7: Halt when a most extreme number of cycles are accomplished, otherwise move to stage 4.

$$\rho.a = \sum F_i \quad (2)$$

Where insights the thickness of air for an enigmatically little air gathering, and shows all the individual forces following up on air assembling, the ideal gas law is used to relate the pneumatic worry to air packs thickness and temperature.

$$P = \rho RT \quad (3)$$

Where, derives the weight, addresses the universal gas enduring, and is the temperature. Other than four official forces can be joined the verbalization (2) that either makes the wind push toward a course at a particular speed or that to meld it from its present way. The weight point power is the clearest control which makes the air to move. The amazing force just acts to bewilder the improvement showed up by the weight edge control. The gravitational power is a vertical power kept up toward the world's surface, in our three dimensional physical condition. The Coriolis power happened in setting on the turn of the earth and diverts the structure for the wind beginning with one estimation then onto the going with estimation.

$$F_{PG} = -\nabla P.\delta V \quad (4)$$

$$F_F = -\rho.\alpha.u \quad (5)$$

$$F_G = \rho.\delta V.g \quad (6)$$

$$F_C = -2.\Omega.u \quad (7)$$

Retrieval Number: B12050982S1119/2019©BEIESP
DOI: 10.35940/ijrte.B1205.0982S1119

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Where, proposes the weight slant, shows the unbounded air volume, the revolt of the earth appeared as , chooses the gravitational strengthening, is the scouring coefficient and is the speed vector of the breeze. The improvement everything considered (gravitational power, weight edge control, beating force, and Coriolis control) showed up above can be entered on the right-hand side of Newton's second law of movement given in condition (2), which headings to

$$\rho.\frac{\nabla u}{\nabla t}=(\rho.\delta V.g)+(-\nabla P.\delta V)+(-\rho.\alpha.u)+(-2.\Omega.u)$$

(8)

Where the reestablishing term in condition (2) is made as , and a period step is seen for ease. For little, dimensionless air pack, the volume is fix as , which improves the condition (8) to

$$\rho.\nabla u=(\rho.g)+(-\nabla P)+(-\rho.\alpha.u)+(-2.\Omega.u)$$

(9)

Looking immaculate gas law condition (3) in condition (9), the thickness ρ can be made like the weight, with temperature and the general gas law persevering

$$u_{new}=(1-\alpha).u_{cur}-g.x_{cur}+\left(RT\left|\frac{1}{i}-1\right|(x_{opt}-x_{cur})\right)+\left(\frac{c.u_{cur}^{other\,\dim}}{i}\right)(10)$$

Where prescribes the speed in the going with cycle, finds the speed in current enhancement, addresses the present zone of the air gathering, demonstrates the ideal zone of the air gathering, addresses the planning between all air social occasions, is the speed sway from another earnestly picked bit of a tantamount air pack, and every single other coefficient are joined into a solitary term . Condition (10) addresses the last kind of the speed update utilized in UWD. The gave up underneath farthest point develops the condition of the air pack.

$$x_{new}=x_{cur}+(u_{new}.\nabla t)\text{(11)}$$

Where, demonstrates the new position of the air pack in the going with cycle. In case the new speed beats the instate most basic speed (max u = 0.3) in any estimation, by then the speed in that estimation is obliged identifying with the given underneath condition:

$$u_{new}^{*}=\begin{cases}u_{\max} & if\ u_{new}>u_{\max}\\ -u_{\max} & if\ u_{new}<-u_{\max}\end{cases}\qquad(12)$$

Where the heading of progression is guaranteed now the size is compelled to be close at any estimation and addresses the reasonable speed after it is obliged to the best speed.

IV. EXPERIMENTAL RESULTS & ANALYSIS

This zone gives the development appraisal of the proposed work. The looking plans of the CDMA have close BER characteristics, which gives resuscitated security dependent on the UWD streamlined choice figuring. In the noteworthiness the proposed framework security execution is executed. Here we execute the BER assessment and likelihood of the chaos up rate relationship for the proposed PN improvement with different codes. In setting on the diversion results the proposed structure accomplishes remarkable execution.

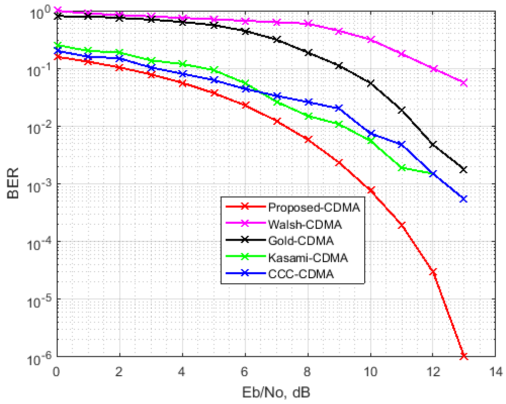


Fig 2 comparison of BER versus SNR for different codes with proposed PN sequence

Fig 2 shows the fragment relationship of the proposed PN gathering with various codes including Walsh, gold, CCC and Kasami codes subject to the BER versus SNR. In setting on the relationship this structure exhibits that the proposed PN get-together code achieves astonishing execution stood separated from the other spread codes. In setting on the SNR pace of the codes makes, by then the BER is diminished. This structure demonstrates that our proposed PN get-together based CDMA correspondence achieved high security execution. The Walsh codes have the ghastly demonstrating when stood segregated from various codes.

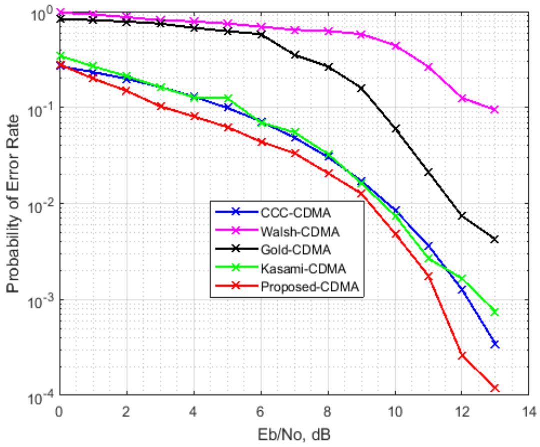


Fig 3: Comparison of Probability of error versus SNR for different codes with proposed PN sequence

Fig 3 exhibits the introduction evaluation of the proposed PN improvement with various codes including Walsh, gold, CCC and Kasami codes subject to the probability of ruin versus SNR. In this layout the proposed PN strategy CDMA execution changes subject to the SNR regard. The show is loosened up ward upon the progression of SNR regard. In setting on the relationship in this structure the proposed PN get-together of CDMA achieved striking execution stood disengaged from various codes. This diagram showed that the proposed point of view gives high security execution.

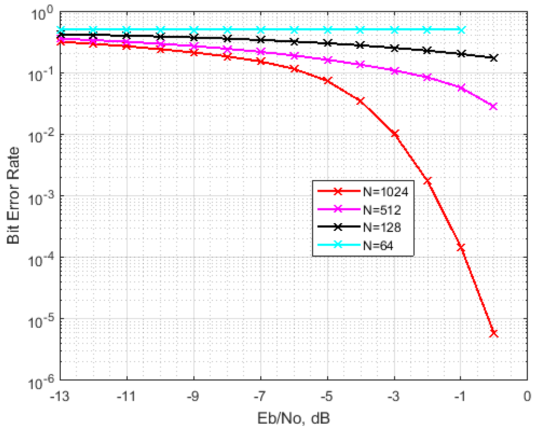


Fig 4 performance comparison of different code length

Fig 4 shows the presentation evaluation of the certain PN get-together code lengths 64,128, 512 and 1024. In light of the BER and SNR changes the presentation of the codes in like way changed. The code length N=1024 shows better execution among the other code lengths. The code length N=64 shows lower execution among the other code lengths. This methodology showed that the subject to the modifications in code lengths the security execution moreover changes.

V.CONCLUSION

The made structure will give a gifted PN improvement which is utilized in various application spaces like military and furthermore used in non military staff applications for the need of data covering and secure sign transmission. An endeavor has been made in this work to make Pseudo Noise (PN) chart subject to Elliptic Curve Cryptography (ECC). By then UWD update estimation got, it gives pleasing sales of PN movement. Such PN groupings have the properties of looking like sporadic mayhem with low alliance stood isolated from some other progress in the set. The relationship of imitated and assessed properties exhibits that groupings have better BER, Probability of wreckage up and code length, appropriately proposed philosophy accomplishes boundless execution.

REFERENCES

1. Kapucu, Nuri, M. Bilim, and I. Develi, "A comprehensive performance analysis of relay-aided CDMA communications over dissimilar fading channels." AEU-International Journal of Electronics and Communications, Elsevier, vol. 83,pp. 339-347, 2018.
2. D.Judson and V. Bhaskar, "Interference Cancellation in CDMA Systems Employing Complementary Codes under Rician Fading Channels." Wireless Personal Communications, Springer, vol. 101, no. 2,pp. 897-914, 2018.
3. Liu, Zilong, Y.L. Guan and H-H. Chen, “Fractional-delay-resilient receiver design for interference-free MC-CDMA communications based on complete complementary codes”. IEEE transactions on Wireless Communications vol. 14, no. 3, pp. 1226-1236, 2015.
4. Sun, Si-Yue, H-H. Chen and W-X. Meng, “A survey on complementary-coded MIMO CDMA wireless communications”. IEEE Communications Surveys & Tutorials vol. 17, no. 1,pp. 52-69, (2015).
5. Quyen, N. Xuan, T. Q. Duong, N-S. Vo, Q. Xie, and L. Shu, "Chaotic direct-sequence spread-spectrum with variable symbol period: A technique for enhancing physical layer security." Computer Networks, Elsevier, vol. 109,pp. 4-12, 2016.
6. Ramadan, Mohammed, F. Li, C.X. Xu, K. Oteng and H. Ibrahim, "Authentication and key agreement scheme for CDMA cellular system." In Communication Software and Networks (ICCSN), 2015 IEEE International Conference on IEEE, pp. 118-124,2015.
7. I.Nelson, C. Annadurai, R. Kalidoss and B. Partibane, "Mitigation of co-channel interferences in cognitive multi-carrier code division multiple access system by singular value decomposition techniques." Cluster Computing, Springer, pp. 1-7, 2017.
8. Berber, M.Stevan and A.K. Gandhi, “Inherent diversity combining techniques to mitigate frequency selective fading in chaos-based DSSS systems”. Physical Communication vol. 19,pp. 30-37, 2016.
9. Iqbal, Kashif, J. Ahmed and A. Rafique, "Analysis of Carrier Frequency Offset Distribution on Efficiency of Multicarrier Spread Spectrum Techniques." In Frontiers of Information Technology (FIT), 2016 International Conference on IEEE, pp. 125-129, 2016.
10. Wang, Ruichi, Z. Lin, J. Du, J. Wu and X. He, "Direct sequence spread spectrum-based PWM strategy for harmonic reduction and communication." IEEE Transactions on Power Electronics vol. 32, no. 6,pp. 4455-4465, 2017.
11. Michaels, J. Alan and D.B. Chester, “Adaptive correlation techniques for spread spectrum communication systems.”In Military Communications Conference, MILCOM 2016-2016 IEEE, pp. 678-681,2016.
12. Quyen, N. Xuan, V.V. Yem and T.Q. Duong, "Design and analysis of a spread-spectrum communication system with chaos-based variation of both phase-coded carrier and spreading factor." IET Communications vol. 9, no. 12,pp. 1466-1473, 2015.
13. Choi, Jinho, and E. Hwang, "Secure multiple access based on multicarrier CDMA with induced random flipping." IEEE Transactions on Vehicular Technology vol. 66, no. 6,pp. 5099-5108, 2017.
14. Patel, M. Krishna, S.M. Berber, and K.W. Sowerby, "Adaptive RAKE receiver in chaos based pilot-added DS-CDMA system." Physical Communication vol. 16, pp. 37-42, 2015.
15. Yang, Jie, H.M. Kwon, A. Mukherjee and K.D. Pham, "Spreading-sequence design for partially connected multirelay networks under multipath fading." IEEE Transactions on Vehicular Technology vol. 65, no. 3, pp. 1420-1433, 2016.
16. Chakraborty, Debolina, M.K. Tarafder, and A. Chandra, "A new walsh-like near orthogonal (wno) sequence for asynchronous CDMA system." Wireless Personal Communications, Springer, vol. 88, no. 4, pp. 711-729, 2016.
17. Tayebi, Arash, S. Berber, and A. Swain, “Performance analysis of chaotic DSSS-CDMA synchronization under jamming attack”. Circuits, Systems, and Signal Processing, Springer, vol. 35, no. 12, pp. 4350-4371, 2016.
18. Li, Ming, Y. Guo, B. Wang, and X. Kong, "Secure spread-spectrum data embedding with PN-sequence masking." Signal Processing: Image Communication,Elsevier, vol. 39,pp. 17-25, 2015.
19. Majid, A. Javaid, H. Moradi, and B. Farhang-Boroujeny, "Fault tolerant key generation and secure spread spectrum communication." IEEE Trans. Wireless Commun vol. 16, no. 8,pp. 5467-5480, 2017.

20. Quyen, N. Xuan, and P. Barlet-Ros, "Performance of direct-oversampling correlator-type receivers in chaos-based DS-CDMA systems over frequency non-selective fading channels." Wireless Personal Communications, Springer, vol. 95, no. 4, pp. 4357-4379, 2017.
21. M. Tafaroji and A. FalahatitheInstitution of Engineering and Technology 2007.
22. Babu, S.B. Sumith, and R. Kumar, "1D-Bernoulli Chaos Sequences Based Collaborative-CDMA: A Novel Secure High Capacity CDMA Scheme." Wireless Personal Communications vol. 96, no. 2, pp. 2077-2086, 2017.
23. M.I.Khalil "A New Scheme for Spreading & De-spreading in the Direct Sequence Spread Spectrum Mechanism" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 10, No. 1, April 2018
24. AbolfazlFalahati and Nader Sanandaji international journal of communication systems Int. J. Commun. Syst. (2016).
25. M. Tafaroji and A. FalahatitheInstitution of Engineering and Technology 2007.
26. Abbas Salman Hameed "DS-CDMA Based on Orthogonal Chaotic Signals and Alamouti Scheme " International Scientific Conference of Engineering Sciences (ISCES) 978-1-5386-1498-3/ 18/31.00$©2018 IEEE.