MULTI USER DETECTOR IN CDMA USING ELLIPTIC CURVE CRYPTOGRAPHY

M. Ranga Rao[1] and Dr. B. Prabhakara Rao[2]

[1]Research Scholar, Dept. of ECE , JNTU, Kakinada, India.
mrraovid@gmail.com
[2]Director of Evaluation, JNTU, Kakinada, India.

ABSTRACT:

Code division multiple access (CDMA) is used in various radio communication techniques due to its advantages. In CDMA one of the most important processes is multi user detection (MUD). There are numerous methods for MUD in CDMA, but in most of the methods, they identify the exact user but the interference signal is high. One of the methods used for MUD in CDM A is elliptic curve cryptography (ECC). Normally, the multi user detector in CDMA using elliptic curve cryptography is performed by using one prime field. In ECC method the exact user is identified and also interference signal reduces comparing with other techniques. To reduce the interference signal to very low, here propose a new technique for MUD in CDMA using ECC. The proposed technique uses multiple prime numbers for key generation. By generating key using different prime numbers using ECC, the bit error rate was very low. The results shows the performance of the proposed for reduce in bit error rate for MUD in CDMA.

KEYWORDS:

CDMA, MUD, elliptic curve cryptography, key generation, encoding

1. INTRODUCTION

The code-division multiple-access (CDMA) networks have seen a quick progress throughout the world in recent years [5]. Optical CDMA schemes enables multiple users to access the network asynchronously and concurrently such that this scheme have attracted much interest mainly in the area of fiber-optic networks [1] [18]. By selecting mutually orthogonal signature waveforms for all users, the multiple access interference (MAI) can be avoided. However an MAI occurs due to the impossibility of protecting orthogonality among received signature waveforms in a mobile environment [11]. OFDM (orthogonal frequency division multiplexing) and CDMA that perform transition are the synthesis of two radio access techniques which is represented by a multicarrier code division multiple access (MC-CDMA) [4]. The MC-CDMA is well-liked for broadband transmission amongst the various multiple-access schemes [2].

Since multiple users in a CDMA system are transmitting to the base station at the same time, the CDMA technology selected for the 3G (third generation) mobile phone networks uses the diversity in the radio channel in order to enhance the performance and enables improved spectral efficacy and a simple base station placement than the 2G (second generation) systems [3] [4].

DOI : 10.5121/vlsic.2012.3105

Generally, CDMA system functions on the principle of code multiplexing and a new scheme called W-CDMA has been proposed, which is an advanced version of CDMA that acts as an applicant for future land mobile networks. The detection techniques of W-CDMA usually called as multi-user detection is significantly different from the traditional schemes [6]. Due to the non-orthogonal spreading of sequences from all users, the MAI occurs in code division multiple access system. A superior detection strategy used to detect multiple users, which exploits the additional structure of the MAI instead of considering the noise [11]. To alleviate the effect of MAI to various degrees, several multi-user detection techniques have been proposed [7].

The signals of multiple users are detected concurrently by using multi-user detection scheme in the detection stage [8]. For direct-detection optical CDMA, many types of multi-user detectors have been proposed in the literature [9, 10]. The maximum likelihood (ML) detector, the decorrelating detector, the minimum-mean-square-error (MMSE) detector, the decision feedback detector and the successive or parallel interference cancellation schemes are included in several well-known methods [17]. Even though a formulation of the optimal multi-user detector for an optical system has been performed, the computational complexity of this algorithm significantly limits the number of users [9]. Due to the coefficients the performance of a linear multi-user detector relies on the chip pulse waveform but it is independent of the time delay [12]. The performance of receiver and the capacity of the CDMA systems can be improved significantly by using the multi-user detection schemes. Many recent investigations has been made in the topic of multi-user detection schemes and their performances in space-time coded CDMA systems with multiple transmit antennas [13] [14] [15]. The facts of all users have been utilized by the linear multi-user detection (MUD) methods for improving the performance of the system [16].

There are different techniques are used for MUD in CDMA, but in most of the techniques Interference is high. To reduce the interference signal, here proposed a new technique using elliptic curve cryptography. The rest of the paper is organized as follows. Section 2 reviews the related works briefly and section 3 details the proposed technique with sufficient mathematical models and illustrations. Section 4 discusses implementation results and Section 5 concludes the paper.

2. RECENT RELATED RESEARCHES: A REVIEW

Some of the recent research works related to MUD in CDMA are discussed below.

Eduard Calvo *et al.* [19] have proposed a MUD algorithm for joint data detection and a cyclic coordinate descent technique based channel estimation, in order to establish less complexity versions of the Maximum-Likelihood (ML) detector for highly distorted underwater channels. Channel responses have been estimated by using the available data symbols and this estimation is further applied for refining the symbol estimates. Adaptive estimation has been carried out by employing a minimum mean square error as the overall optimization criteria. The array processing gain essential for several underwater acoustic channels has been provided by the receiver employed in a multichannel configuration. The intricacy of the detection algorithm has been linear in the received number of elements but it does not rely on the modulation level of the transmitted signals. An excellent result has been obtained when analyzing the algorithm using the valid data acquired over a 2-km shallow water channel in a 20-kHz band.

Dongning Guo *et al*. [20] have proposed a new CDMA model with sparse spreading sequences, which allows near-optimal multi-user detection by using Belief Propagation (BP) with low intricacy. Their scheme has been partially motivated by capacity-approaching Low-Density Parity- Check (LDPC) codes and the success of iterative decoding methods. Particularly in large system, the detection based on BP is optimal under several practical conditions and it is a unique benefit of sparsely spread CDMA systems. Also, from the perspective of an individual user, it has shown that the CDMA channel is asymptotically similar to a scalar Gaussian channel with some degradation in the signal-to-noise ratio (SNR). Here, the fixed-point equation has been used for determining the degradation factor, also called as the multi-user efficiency. They have applied the results to a large class of sparse, semi-regular CDMA systems with random input and power distribution. For the systems of moderate size, the theoretical findings have been maintained by the numerical results and it further exhibit the request of sparse spreading in useful applications.

Jyh-Horng Wen *et al*. [21] have proposed a Particle Swarm Optimization (PSO) algorithm based direct-sequence code-division multiple-access systems (DS-CDMA) for multiuser detector. By considering both global and local exploration ML, their proposed system has used heuristics in order to function possibly around computational intractability. Computer simulation has proved that their proposed detector provides near-optimal performance with significantly reduced computation complexity than the existing sub-optimum detectors.

Zhilu Wu *et al.* [22] have proposed a hybrid approach with Ant Colony Optimization (ACO) and Code Filtering System (CFS) for DS-CDMA multi-user detection. In order to make the judgment of the codes of users, the method of Lagrange multipliers in CFS has been applied to set the threshold. The hybrid detector performs much better than the ACO multi-user detector, because it not only filters the most part of the wrong codes from the output of the ACO multi-user detector but also reduce the iteration numbers in the process of hunting the solution. Simulation results have proved that the hybrid detector has superior performance in reducing bit-error rate and decreasing the computational intricacy than that of the ACO multi-user detector and also it is too close to the performance of the optimum multi-user detector. Simultaneously, the data processing rate has been increased as well as the real-time performance of the systems has also been improved, by the hybrid detector because it's computational complexity is only 20.7% compared to the complexity of ACO.

Angeline *et al.* [23] have discussed that multiple input and multiple output (MIMO) is a method used to increase data rate considerably with multiple antennas at both the transmitter and receiver. The benefit of random fading and multipath delay spread has been used by the MIMO. In order to obtain effective MIMO systems, it has to perform reliably in interference restricted environment. CDMA systems are designed to function in an interference free environment therefore it has been used in recent cellular systems. The system transmission rate over the conventional CDMA system has been further enhanced by the combination of both MIMO and CDMA. Multi-user MIMO CDMA systems has been considered in which each user has multiple transmit antennas, and diverse transmit antennas of the same user have used the same spreading code. The signals containing Gaussian noise have been identified by using the techniques such as matched filter and decorrelating detector. Due to largely impulsive phenomenon, the ambient noise recognized through experimental measurements is certainly non-Gaussian in several wireless systems. The occurrence of such impulsive ambient noise can considerably degrade the performance of several MUDs. An mestimation based technique has been used for combating MAI and impulsive noise in CDMA communication systems. They have shown that the m-

estimation method has superior performance under non-Gaussian noise compared to that of the performance of other detection methods.

Morra *et al*. [24] have proposed and analyzed the performance of a particle swarm optimization algorithm based MUD detector called particle swarm (PS-MUD). The PS–MUD has presented extremely interesting results surpassing the decorrelator detector and the matched filter detector. Besides being naturally near-far resistant, the capacity resulting from it has been greater than that of the decorrelating detector. Lastly, PS–MUD has remarkably less computational complexity compared to OMUD; especially it is insignificant when compared to that of OMUD for large numbers of users.

Gao *et al* [25] have proposed a new simple quantum shuffled frog leapin (QSFL) utilizing algorithm for the application of an optimal robust decorrelating detector (optimal-RDEC) MUD in MC-CDMA systems. This new and uncomplicated QSFL algorithm is used for solving optimization problems. QSFL-RDEC has been proved to be a successful algorithm for robust multi-user detection by simulation results genetic algorithm (GA)-RDEC, PSO-RDEC and genetic quantum algorithm (GQA)-RDEC have been surpassed by it in low computational complexity and it could realize almost optimal performance. Certainly QSFL would become more attractive and realistic for diverse signals processing application due to the improvements in parallel hardware. The vision of utilizing a lowcomplexity robust MUD for MC-CDMA system of impulse noise would be realized by the QSFLRDEC approach. In their future research, they decided to develop robust multi-user detectors in STBC-MC-CDMA system and ultra wide band radio system by employing QSFL.

3. MUD FOR CDMA USING ECC

MUD is commonly used in CDMA to receive the signal with reduce in interference signal. In CDMA numerous users will transmit their signals with different codes and in the receiver side using the code they transmitted we obtain the required signal. During transmission the signal from transmitter to receiver noise added in the transmitted signal. So that we didn't receive the exact signal send from the transmitter. To reduce the interference in the transmitted signal MUD is used in receiver side. There are different techniques are used for MUD in CDMA, among them elliptic curve cryptography is commonly used. In elliptic curve cryptography the inference signal is reduced based on the prime field. Normally one prime field is used to reduce the interference signal, it will reduce the interference signal, but in order to reduce the interference signal even more here proposed a new method MUD using CDMA using multi prime field. The process takes place in the proposed method is explained briefly in the below sections. Initially we see about the transmitter operation of CDMA.

3.1 Signal transmitting process

The signal transmitting process takes place in the proposed method is shown in figure 1.

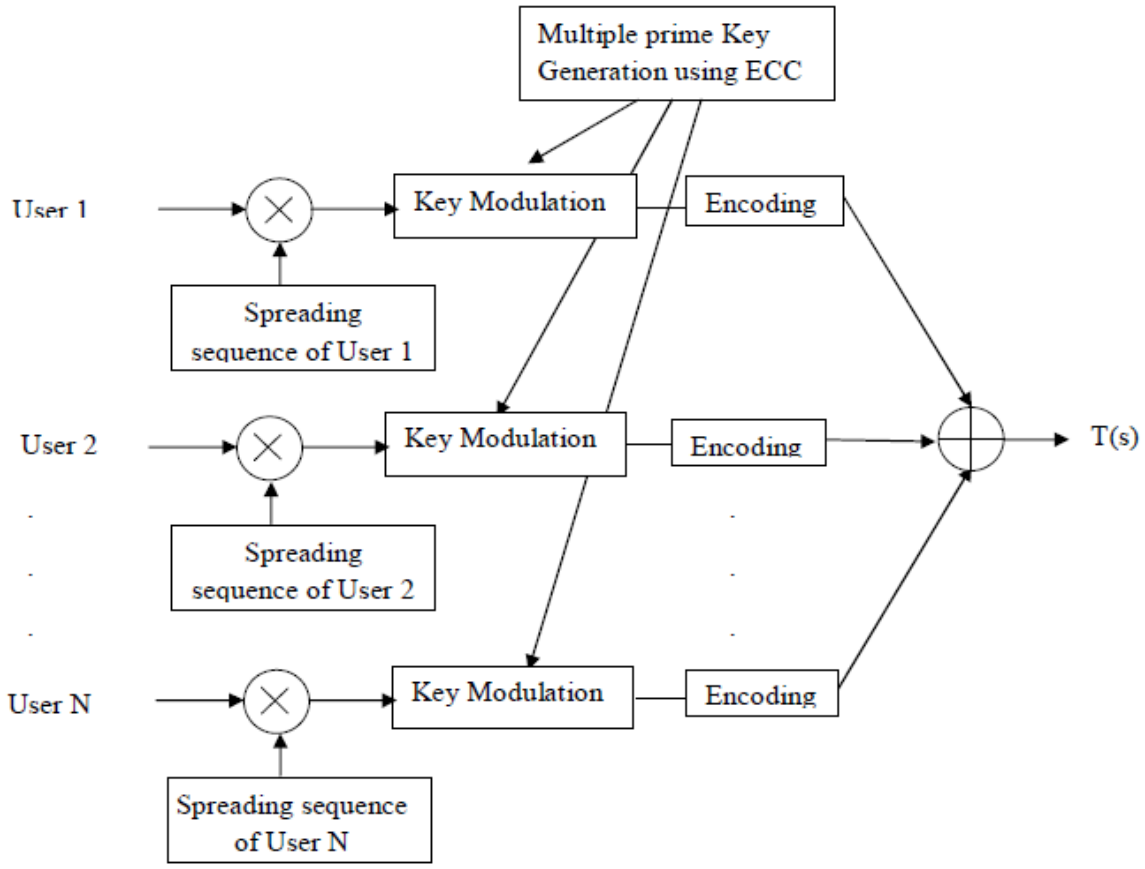

Figure 1: Signal transmitting process takes place in proposed method.

The figure 1 shows the signal transmitting process takes place in the proposed method. Here the R users are transmitting signals and before transmitting signals, there are certain process takes place. The process takes place before transmitting the signals are modulation, key generation and encoding.

Initially different user will send signal with different code in a single channel. To transmit the signal first the modulation process is applied to the each signal individually. After completion of modulation process the next step process is key generation. Key generation is one of the most important processes in communication system, because using this key, the signals are received in the receiver side. In the proposed method key is generated for each signals using elliptic curve cryptography

3.1.1. Generation of key in transmitter side

Key generation plays a major role in MUD in CDMA to reduce the interference signal. Normally there are two types of key generation process. They are

- Private key
- Public key

After generating public and private key, the public key is send to the signal required by the user. The public key is used to identify the exact signal transmitted by the user. In the proposed method both public and private keys are generated using elliptic curve cryptography.

3.1.2. Elliptic curve cryptography to generate private and public keys

Elliptic curve cryptography is used here to reduce the interference and noise present in the signal and also for receiving the correct signal. There are two different types of finite fields in elliptic curve cryptography. They are

i. Binary field
ii. Prime field

We use prime field in the proposed method. The standard form of elliptic curve is as follows.

$$y^2 \bmod \mathrm{p} = x^3 + ax + b \bmod \mathrm{p} \qquad (1)$$

In elliptic curve cryptography the mathematical operation is entirely different. The general mathematical operation takes place in elliptic curve cryptography is explained briefly in [26].

The public and private keys are generated based on the prime number using elliptic curve cryptography. In the proposed method instead of generating one prime number, here we generated multiple prime numbers to reduce the interference signal to very low. The steps for key generation using elliptic curve cryptography are as follows.

Step 1: Select a point $\mathrm{X(a, b)}$ on the elliptic curve.

Step 2: Select multiple prime numbers $p_1, p_2, \ldots p_n$; where n is the number of prime numbers selected and integer values for x and y.

Step 3: Select one point in the curve $\mathrm{X}_1 = (\mathrm{a}_i, b_i)$.

Step 4: Select m value which is a random integer value.

Step 5: Calculate X_2 using the formula

$$\mathrm{X}_2 = (a_j, b_j) = m * X_1 \qquad (2)$$

Step 6: Use X_1 and X_2 as public key and m as private key.

After completion of key generation, the next step is to filter the signals and combine all the signals in to one signal and transmitted to the receiver. After key generation the public key is sent to the user who requires the corresponding signal and then encoding operation is performed for the transmitting signal.

3.1.3. Encoding signal using ECC

In the encoding operation the signal transmitted is converted into a different form, so that except the user no other person can get the desired signal. The process take place during encoding operation is as follows:

Step 1: Select k value in plain text P , which is a random integer value.
Step 2: Calculate ciphertext value using the equation given below.

$$C_i = k * X_1 \quad (3)$$

$$C_j = (a_{pi}, b_{pi}) + k * X_2 \quad (4)$$

Step 3: Generate a unique matrix from X
Step 4: Take unique elements present in the X matrix and calculate the sum of the unique elements i.e. d .
Step 5: Find the nearest square value of the sum value and take square root of the nearest square value i.e. f .
Step 6: Create a new matrix D with size $f \times f$ using the equation given below.

$$D_{(i*N+j)} >> \begin{cases} X(0,0); if\ i = 0, j = 0 \\ X(i,j);\ if\ R(i,j) \notin D \end{cases} \quad (5)$$

After completion of encoding operation, the encoded signal is transmitted. Next we discuss about the receiver operation that takes place in MUD.

3.2. Receiving signals using proposed method

In the receiver side, the transmitted signal is received by the user based on the need. The user requesting signal is first decoded and the correct signal transmitted by the user is obtained. Then, the received signal is filtered to reduce the noise and interference and the process that takes place in the receiver are shown in the figure given below.

The figure 2 shows the operation that takes place in the CDMA of the receiver. Next we discuss about the system model of receiver.

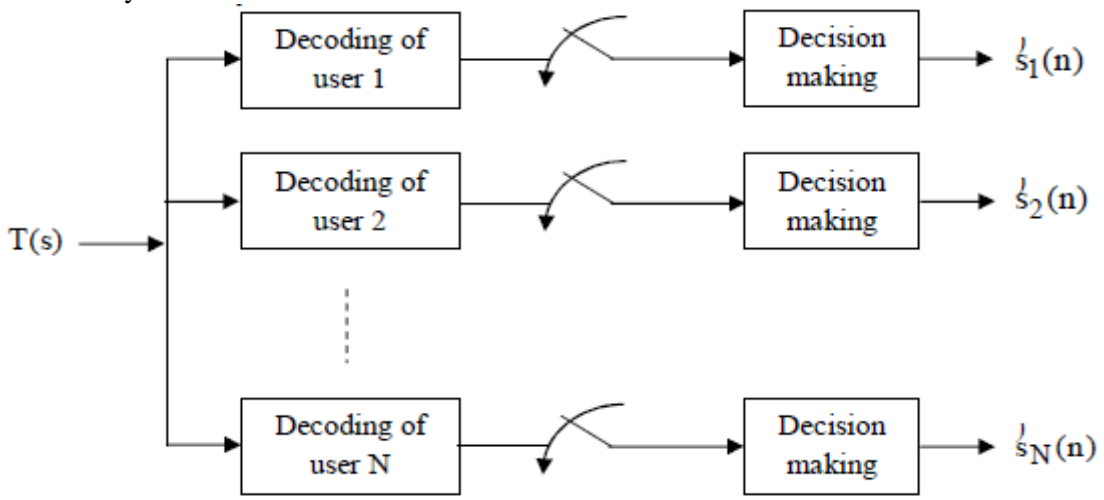

Figure 2: Receiver operation in CDMA

3.2.1. Receiver system model

In the transmitter side different signals sent by different users are combined together and transmitted and in the receiver side the signal required for each receiver is extracted from the

combined signal. Let us consider N users are present in the receiver side for receiving signals. The signal received at the receiver side is shown in the equation given below.

$$T_{ECC}(s) = \sum_{m=1}^{N} A_m . d_m . s_m(s) + g(s) \quad (6)$$

where, s_m is the signature waveform of the N^{th} user. The formula to calculate signature waveform is as follows,

$$s_m(s) = \sum_{m=0}^{30} b_m . P_T(s - m.C_i) \quad (7)$$

where, T is the bit period, C_i is the chip interval, d_m is the input bit of the N^{th} user, A_m is the received amplitude of the N^{th} user, is the additive white Gaussian noise.

The ECC cross-correlation of the signature sequences is

$$\rho_{ij} = \sum_{m=1}^{L} s_i(m).s_j(m) \quad (8)$$

where, L is the length of the signature sequence.

The ECC cross-correlation matrix is defined as follows,

$$X = \{\rho_{ij}\}$$

$$\text{i.e., } X = \begin{bmatrix} \rho_{11} & \rho_{12} \cdots\cdots \rho_{1N} \\ \rho_{21} & \rho_{22} \cdots\cdots \rho_{2N} \\ . & \\ . & \\ \rho_{M1} & \rho_{M2} \cdots\cdots \rho_{NN} \end{bmatrix} \quad (9)$$

After receiving the signal, the signal is demodulated to obtain the desired signal to the user. Now we discuss about the decoding operation that takes place in the received signal using ECC.

3.2.2. Decoding using ECC

In the decoding the received signal is decoded using the private key to obtain the exact signal send by the user. The process takes place to identify the exact signal send by the user is as follows.

Step 1: Calculate P using the private key g, after receiving the ciphertext C_i and C_j as follows,

$$(a_{pi}, b_{pi}) = C_j - (g * C_i) \quad (10)$$

Step 2: Read the characters from the coordinates (a_{pi}, b_{pi}).

After decoding the received signal, we obtain the original transmitted signal. The next step after decoding operation is filtering. In the filtering process noise present in the signal are reduced to obtain the exact signal.

4. RESULT AND DISCUSSIONS

The proposed technique was implemented in MATLAB 7.10 A and the proposed method is tested for 10 users transmitting and receiving at a time. The performance of the proposed method is identified from the bit error rate vs signal to noise ratio plot. The performance of proposed method is compared with decorrelating detector, blind MUD and MMSE linear detector. Initially we see about the BER vs SNR graph for decorrelating detector.

4.1. Decorrelating detector with different prime numbers

The BER vs SNR graph obtained using the proposed method is compared with decorrelating detector. Here, using one prime number three different conditions are computed. Here we added two different noises in the proposed method key and the results are analyzed and also the proposed method without noise also computed. The graph obtained for different prime numbers are as follows.

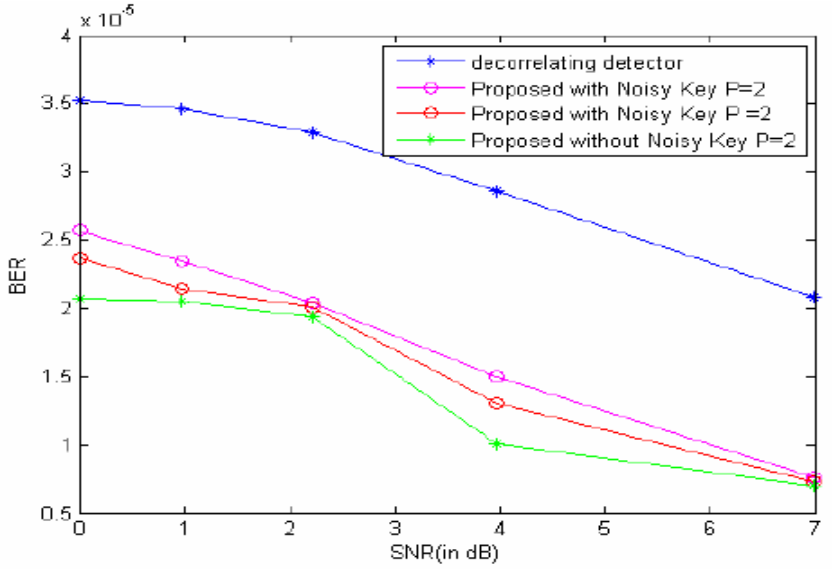

Figure 3: BER vs SNR graph between proposed method and decorrelating detector with prime number 2.

From figure 3 it is clear that for decorrelating detector the BER value is from 3.5 X 10^{-5} to 2.1 X 10^{-5} for different SNR values. For the same SNR values the BER for proposed method with noisy key is from 2.6 X 10^{-5} to 0.75 X 10^{-5} and 2.4 X 10^{-5} to 0.7 X 10^{-5} . For proposed method without noisy key the BER value is 2.1 X 10^{-5} to 0.65 X 10^{-5} . From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

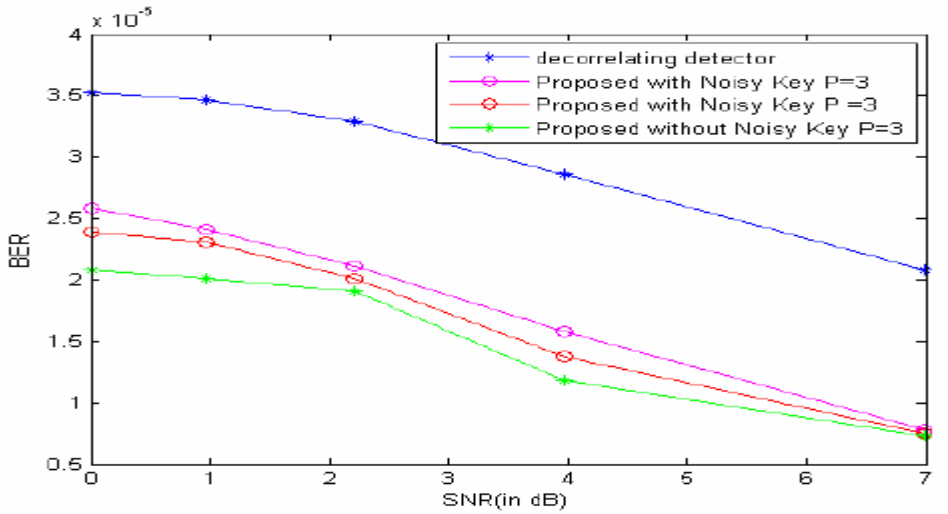

Figure 4: BER vs SNR graph between proposed method and decorrelating detector with prime number 3.

From figure 4 it is clear that for decorrelating detector the BER value is from 3.5 X 10^{-5} to 2.1 X 10^{-5} for different SNR values. For the same SNR values the BER for proposed method with noisy key is from 2.55 X 10^{-5} to 0.75 X 10^{-5} and 2.4 X 10^{-5} to 0.7 X 10^{-5}. For proposed method without noisy key the BER value is 2.1 X 10^{-5} to 0.7 X 10^{-5}. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

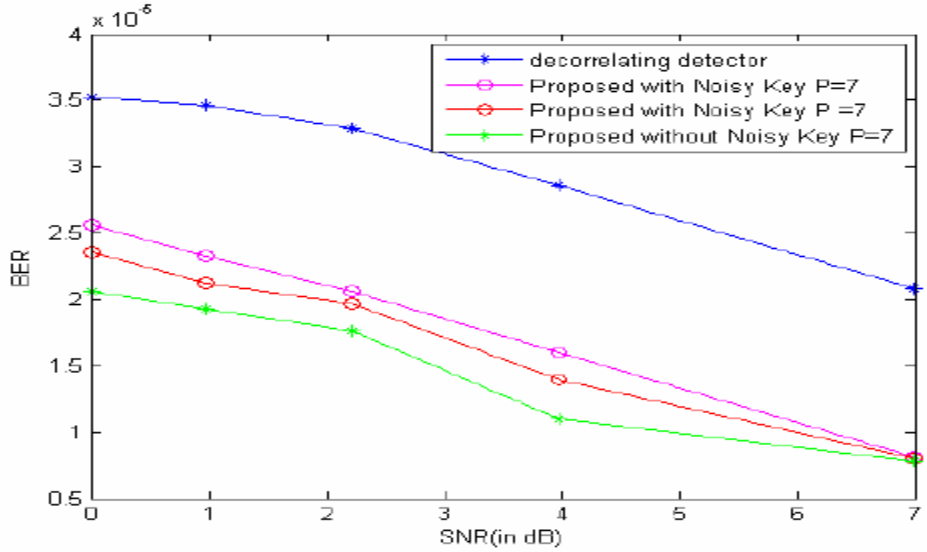

Figure 5: BER vs SNR graph between proposed method and decorrelating detector with prime number 7.

From figure 5 it is clear that for decorrelating detector the BER value is from 3.5 X 10^{-5} to 2.1 X 10^{-5} for different SNR values. For the same SNR values the BER for proposed method with noisy key is from 2.51 X 10^{-5} to 0.8 X 10^{-5} and 2.35 X 10^{-5} to 0.75 X 10^{-5}. For proposed method without noisy key the BER value is 2.1 X 10^{-5} to 0.7 X 10^{-5}. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

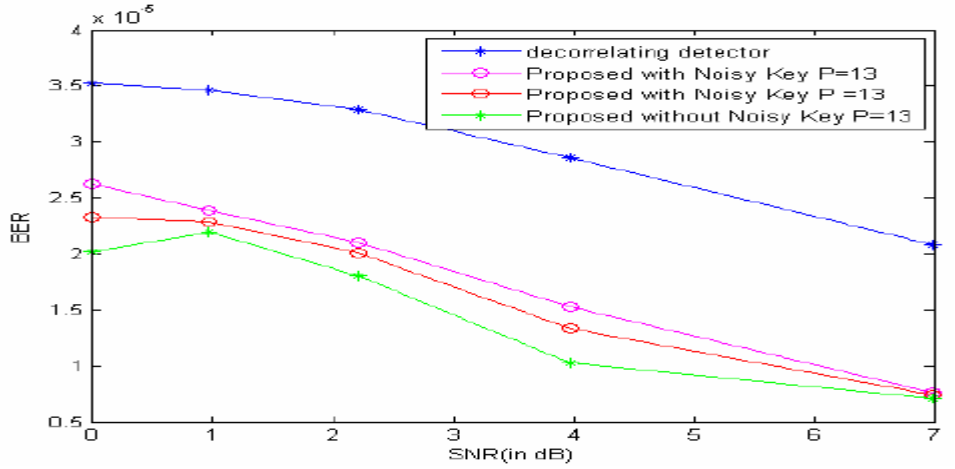

Figure 6: BER vs SNR graph between proposed method and decorrelating detector with prime number 13.

From figure 6 it is clear that for decorrelating detector the BER value is from 3.5 X 10^{-5} to 2.1 X 10^{-5} for different SNR values. For the same SNR values the BER for proposed method with noisy key is from 2.65 X 10^{-5} to 0.7 X 10^{-5} and 2.3 X 10^{-5} to 0.7 X 10^{-5}. For proposed method without noisy key the BER value is 2.0 X 10^{-5} to 0.65 X 10^{-5}. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

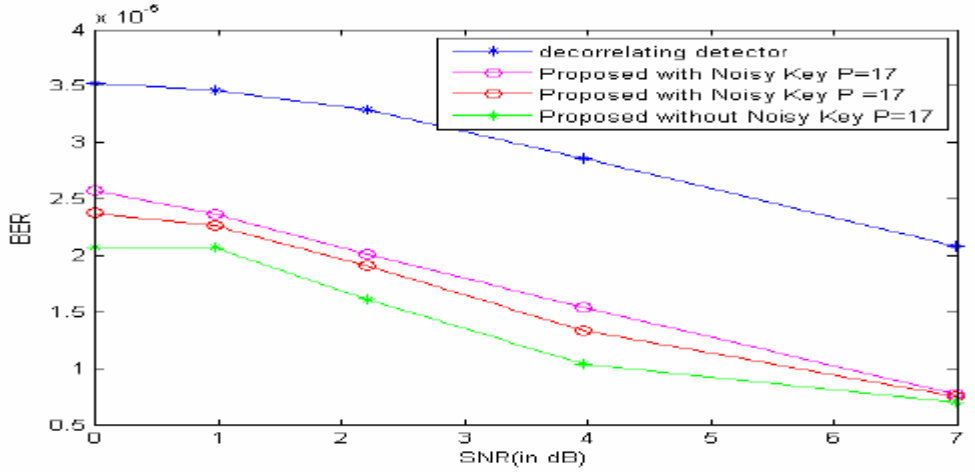

Figure 7: BER vs SNR graph between proposed method and decorrelating detector with prime number 17.

From figure 7 it is clear that for decorrelating detector the BER value is from 3.51 X 10^{-5} to 2.1 X 10^{-5} for different SNR values. For the same SNR values the BER for proposed method with noisy key is from 2.55 X 10^{-5} to 0.75 X 10^{-5} and 2.4 X 10^{-5} to 0.75 X 10^{-5}. For proposed method without noisy key the BER value is 2.1 X 10^{-5} to 0.65 X 10^{-5}. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used. Next the performance using MMSE method is analyzed.

4.2. MMSE method with different prime numbers

The BER vs SNR graph obtained using the proposed method is compared with MMSE method. Here, using one prime number three different conditions are computed. Here we added two different noises in the proposed method key and the results are analyzed and also the proposed method without noise also computed. The graph obtained for different prime numbers are as follows.

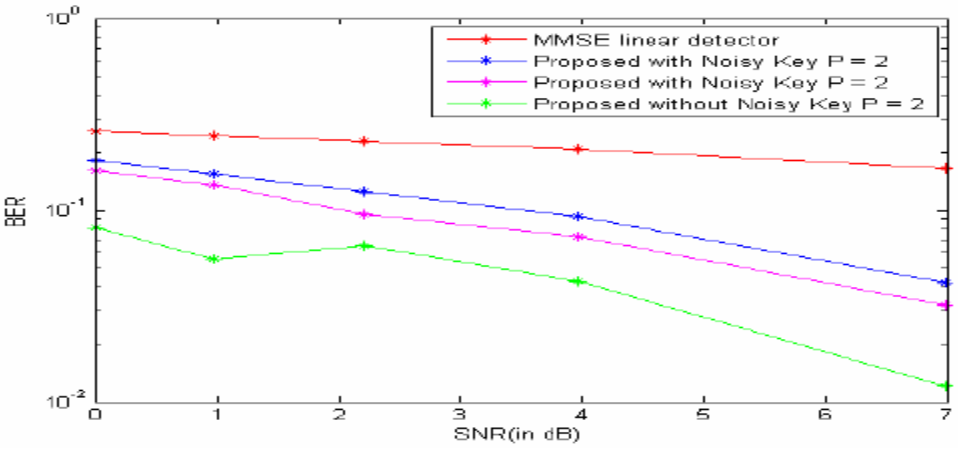

Figure 8: BER vs SNR graph between proposed method and MMSE method with prime number 2.

From figure 8 it is clear that for MMSE linear detector the BER value is from $10^{-0.75}$ to $10^{-0.9}$ for different SNR values. For the same SNR values the BER for proposed method with noisy key is from $10^{-0.85}$ to $10^{-1.6}$ and $10^{-0.9}$ to $10^{-1.78}$. For proposed method without noisy key the BER value is $10^{-1.2}$ to $10^{-1.9}$. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

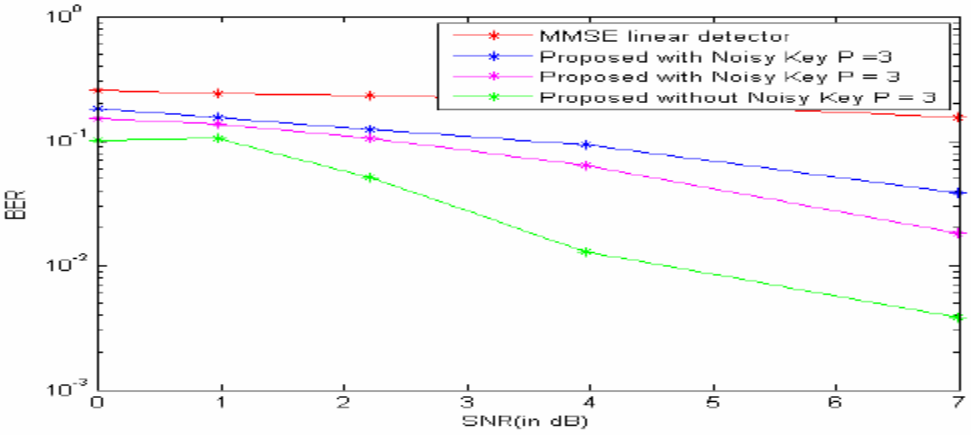

Figure 9: BER vs SNR graph between proposed method and MMSE method with prime number 3.

From figure 9 it is clear that for MMSE linear detector the BER value is from $10^{-0.6}$ to $10^{-0.75}$ for different SNR values. For the same SNR values the BER for proposed method with noisy key is from $10^{-0.8}$ to $10^{-1.6}$ and $10^{-0.9}$ to $10^{-1.9}$. For proposed method without noisy key the BER value is

10^{-1} to $10^{-2.6}$. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

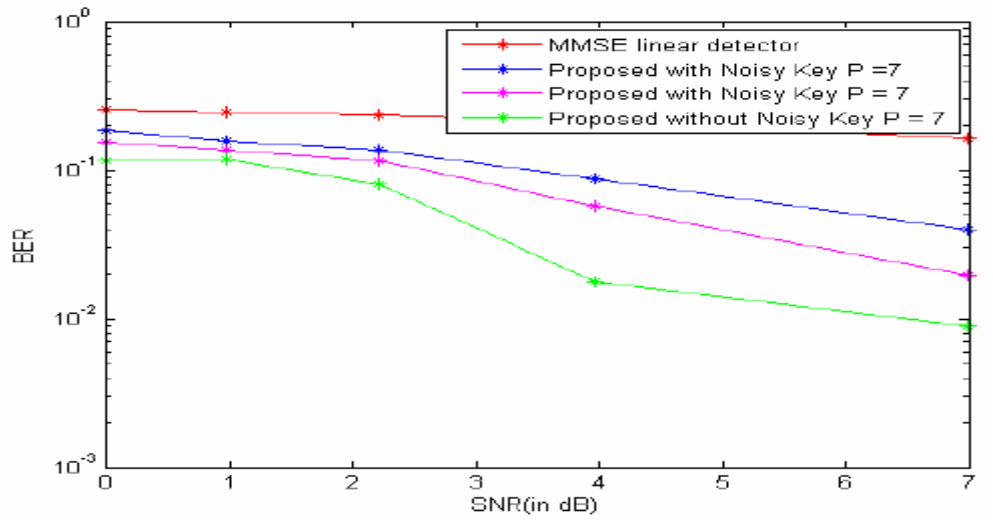

Figure 10: BER vs SNR graph between proposed method and MMSE method with prime number 7.

From figure 10 it is clear that for MMSE linear detector the BER value is from $10^{-0.6}$ to $10^{-0.85}$ for different SNR values. For the same SNR values the BER for proposed method with noisy key is from $10^{-0.9}$ to $10^{-1.7}$ and $10^{-0.95}$ to $10^{-1.9}$. For proposed method without noisy key the BER value is $10^{-0.98}$ to $10^{-2.1}$. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

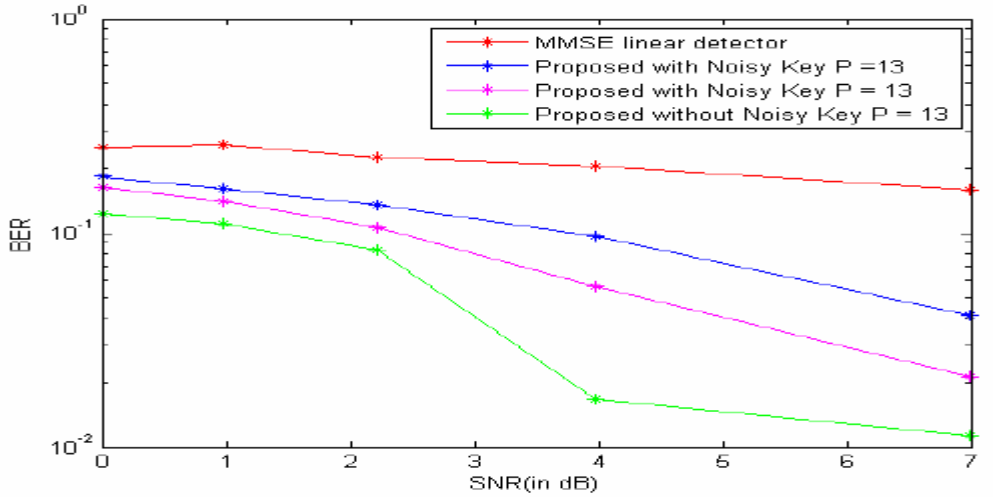

Figure 11: BER vs SNR graph between proposed method and MMSE method with prime number 13.

From figure 11 it is clear that for MMSE linear detector the BER value is from $10^{-0.6}$ to $10^{-0.8}$ for different SNR values. For the same SNR values the BER for proposed method with noisy key is from $10^{-0.9}$ to $10^{-1.6}$ and $10^{-0.95}$ to $10^{-1.9.}$ For proposed method without noisy key the BER value is $10^{-0.95}$ to $10^{-1.9}$. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

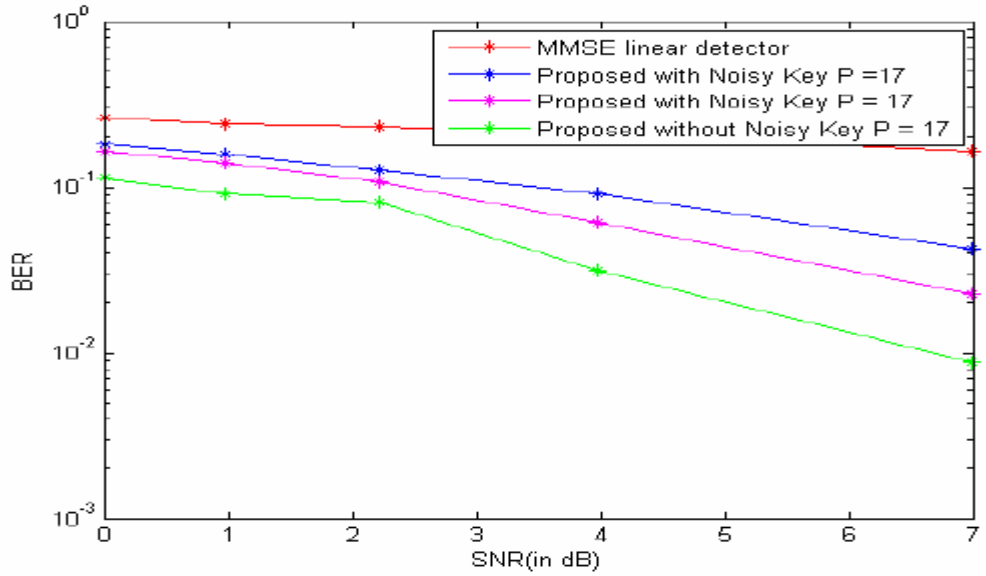

Figure 12: BER vs SNR graph between proposed method and MMSE method with prime number 17.

From figure 12 it is clear that for MMSE linear detector the BER value is from $10^{-0.6}$ to $10^{-0.8}$ for different SNR values. For the same SNR values the BER for proposed method with noisy key is from $10^{-0.92}$ to $10^{-1.5}$ and $10^{-0.95}$ to $10^{-1.8}$. For proposed method without noisy key the BER value is $10^{-0.98}$ to $10^{-2.1}$. From the above result it is clear that the proposed method is better than the decorrelating detector even if noisy key is used.

Next we see about the performance using Blind MUD method.

4.3. Blind MUD method with different μ values

The BER vs SNR graph obtained using the proposed method is compared with Blind MUD method. Here, using one prime number three different conditions are computed. Here we added two different noises in the proposed method key and the results are analyzed and also the proposed method without noise also computed. The graph obtained is as follows.

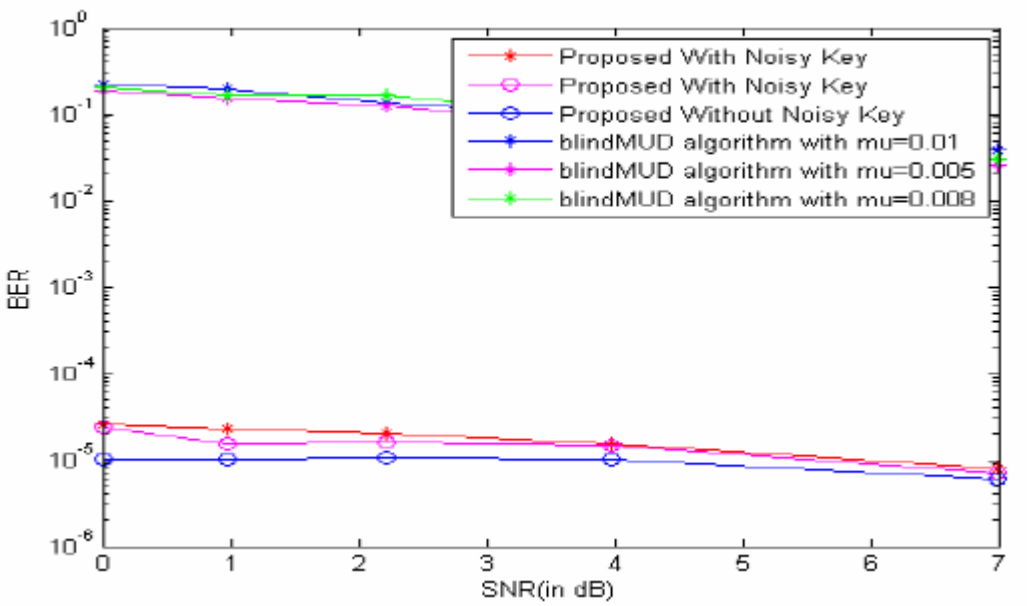

Figure 13: BER vs SNR graph between proposed method and Blind MUD method with different μ values.

Figure 13 shows the BER vs SNR graph between proposed method and Blind MUD method with different μvalues. From the above figure it is clear that the proposed method is better than the blind MUD method for μ = 0.010.005,0.008. From the above results, it is clear that the proposed method reduces the BER value to very low and even if noise is added in the key the proposed method is better. If there is no noise in the generated key, the BER value reduces to very low value.

From the above results, it is clear that the proposed method is better than decorrelating detector, blind MUD and MMSE linear detector, even if noise is added in the key.

5. CONCLUSION

In this paper, elliptic curve cryptography is used for MUD in CDMA and the proposed technique is implemented in MATLAB 7.10 B. In the proposed method multiple prime numbers is used for key generation. By using multiple prime numbers in key generation the interference signal was very low, so that exact signal is obtained for the receiver. The proposed elliptic curve cryptography method is tested for two users and the bit error rate obtained from our method is very low when compared with other techniques. The proposed method is tested using different prime numbers and also by adding noise in the key and the results obtained is analyzed. The results obtained from the proposed technique are compared with decorrelating detector, blind MUD and MMSE linear detector. From the comparison results it is evident that the proposed method is better than other methods.

REFERENCES

[1] Tomoaki Ohtsuki and Joseph M. Kahn, "BER Performance of Turbo-Coded PPM CDMA Systems on Optical Fiber", Journal of Light wave Technology, Vol. 18, No. 12, pp. 1776-1784, December 2000.

[2] Rensheng Wang, Hongbin Li and Tao Li, "Robust Multi-user Detection for Multicarrier CDMA Systems", IEEE Journal on Selected Areas In Communications, Vol. 24, No. 3, pp. 673-683, March 2006.

[3] Michiel P. Lotter and Pieter van Rooyen, "Modeling Spatial Aspects of Cellular CDMA/SDMA Systems", IEEE Communications Letters, Vol. 3, No. 5, pp. 128-131, May 1999.

[4] McCormick and Al-Susam, "Multicarrier CDMA for Future Generation Mobile Communication", Journal of Electronics & Communication Engineering, Vol. 14, No. 2, pp. 52-60, April 2002.

[5] Phuoc Tran Gia, Nikhil Jain and Kenji Leibnitz, "Code Division Multiple Access wireless network planning considering clustered spatial customer traffic", In Proceedings of 8th International Telecommunication Network Planning Symposium, Sorrento, Italy, pp. 1-14, October 1998

[6] Halil Tanyer Eyyuboglu, "MATLAB simulation of multi-user detection in CDMA", World Academy of Science, Engineering and Technology, Vol. 3, No. 8, pp. 31-34, 2005

[7] Dongning Guo and Sergio Verdu, "Decoupling of CDMA Multi-user Detection via the Replica Method", Fortyfirst Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, pp. 1124-1133, 2003

[8] Yoshiyuki Kabashima, "A CDMA multi-user detection algorithm on the basis of belief propagation", Journal of Physics A: Mathematical and Theoretical, Vol. 36, No. 43, pp. 11111-11121, 2003

[9] Verdu, "Multiple-access channels with point-process observations: Optimum demodulation," IEEE Transactions on Information Theory, Vol. 32, No. 5, pp. 642–651, September 1986

[10] Brandt-Pearce and Aazhang, "Multi-user detection for optical code division multiple access systems," IEEE Transactions on Communications, Vol. 42, No. 234, pp. 1801-1810, April 1994

[11] Peng Hui Tan and Lars K. Rasmussen, "Multi-user Detection in CDMA—A Comparison of Relaxations, Exact, and Heuristic Search Methods", IEEE Transactions on Wireless Communications, Vol. 3, No. 5, pp. 1802-1809, September 2004

[12] Laura Cottatellucci, Merouane Debbah and Ralf R. Muller, "Linear Multi-user Detection for Asynchronous CDMA Systems: Chip Pulse Design and Time Delay Distribution", In Proceedings of IEEE Information Theory Workshop, Punta del Este, Uruguay, pp. 293-297, 2006

[13] Sharma and Chockalingam, "Performance Analysis of Maximum-Likelihood Multi-user Detection in Space-Time Coded CDMA ", In Proceedings of IEEE Conference on Vehicular Technology, Vol. 3, pp. 1664-1668, 2004

[14] Huang, Viswanathan and Foschini, "Multiple antennas in cellular CDMA systems: Transmission, detection, and spectral efficiency," IEEE Transactions on Wireless Communications, Vol. 1, No. 3, pp. 383-392, July 2002

[15] Reynolds, Wang, and Poor, "Blind adaptive space-time multi-user detection with multiple transmitter and receiver antennas," IEEE Transactions on Signal Processing, Vol. 50, No. 6, pp. 1261-1276, June 2002

[16] Heli Vaataja, Markku Juntti and Pauli Kuosmanen, "Performance of Multi-user Detection in TDCDMA Uplink", In Proceedings of Conference on European Signal Processing, Tampere, Finland, Vol. 1, 2000

[17] Wan-Jen Huang, Peter Hong, and Jay Kuo, "Relay-Assisted Decorrelating Multi-user Detector (RADMUD) for Cooperative CDMA Networks", IEEE Journal on Selected Areas in Communications, Vol. 26, No. 3, pp. 550-560, April 2008

[18] Ohtsuki, Kaneko and Kahn, "Performance analysis of linear binary block coded optical PPM CDMA systems with soft-decision decoding", In Proceedings of IEEE Conference on Global Telecommunications, San Francisco, CA , USA, Vol. 2, pp. 1196-1200, 2000

[19] Eduard Calvo and Milica Stojanovic, "Efficient Channel-Estimation-Based Multiuser Detection for Underwater CDMA Systems", IEEE Journal of Oceanic Engineering, Vol. 33, No. 4, pp. 502-512, October 2008

[20] Dongning Guo and Chih-Chun Wang, "Multiuser Detection of Sparsely Spread CDMA", IEEE Journal on Selected Areas In Communications, Vol. 26, No. 3, pp. 421-431, April 2008
[21] Jyh-Horng Wen, Chuan-Wang Chang and Ho-Lung Hung, "Particle Swarm Optimization for Multiuser Asynchronous CDMA Detector in Multipath Fading Channel", Journal of WSEAS Transactions on Computers, Vol. 7, No. 7, pp. 909-918, July 2008
[22] Zhilu Wu, Yunsheng Kuang, Nan Zhao and Yaqin Zhao, "A Hybrid CDMA Multiuser Detector with Ant Colony Optimization and Code Filtering System", Journal of Information Technology, Vol. 9, No. 4, pp. 818-824, 2010
[23] Angeline and Lenty Stuwart, "Multiuser Detection for MIMO CDMA Systems", International Journal of Computer Applications, Vol. 4, No. 6, pp. 11-17, July 2010.
[24] H. H. El Morra, A. U. Sheikh, and A. Zerguine, "Optimum Multiuser Detection in Cdma using Particle Swarm Algorithm", The Arabian Journal for Science and Engineering, Vol. 34, pp:197-202, April 2009.
[25] Hongyuan GAO, Ming DIAO and Xuemei YU, "Robust MC-CDMA Multiuser Detection Based on Quantum Shuffled Frog Leaping", Journal of Computational Information Systems, Vol.6, No.10, pp: 3309-3318, 2010.
[26] M. Ranga Rao and B. Prabhakara Rao, "A Hybrid Multi-User Detector for CDMA Systems", CiiT International Journal of Wireless Communication, Dec 2011.

Authors

Mr. M. Ranga Rao received his M.Tech. in digital electronics and communication systems from JNTU college of engineering, Anathapur, in 2003. He is currently pursuing the Ph.D degree with the department of ECE, JNTU, Kakinada, India. He is presently working as senior faculty member in department of electronics and communication engineering, PSCMR college of engineering and technology, Vijayawada, India.

Dr. B. Prabhakara Rao received his B.Tech and M.Tech. in electronics & communication engineering from S.V. University, Tirupathi, India in 1978 and 1982 and Ph.D degree from IISc, Bangalore, India in 1995. He is an expert in Signal Processing & Communications. He is currently Director of Evaluation, JNT University, Kakinada. He has more than 28 years of experience in teaching and 20 years of R & D. He produced 5 PhD's and guiding 25 PhD scholars. He held different positions in his career like Head of the Department, Vice Principal, in JNTU College of Engineering and Director (Institute of Science & Technology) in the Newly Established JNT University from 2003 to 2010. He published more than 95 technical papers in national and International journals and conferences.