iaes
Institute of Advanced Engineering and Science

Secured data transmission in a V-Blast encoded MIMO MCCDMA wireless communication system

Mousumi Haque*, Most. Farjana Sharmin* and Shaikh Enayet Ullah**
* Department of Information and Communication Engineering, Rajshahi University, Rajshahi-6205, Bangladesh
** Department of Applied Physics and Electronic Engineering, Rajshahi University, Rajshahi-6205, Bangladesh

Article Info

Article history:

Received Oct 21th, 2012
Revised Jan 4th, 2013
Accepted Feb 15th, 2013

Keyword:

MIMO MCCDMA
V-BLAST encoding
Vigenere Cipher and RSA cryptographic algorithm,
Bit Error rate (BER)
AWGN and Raleigh fading channels

ABSTRACT

In this paper, a comprehensive performance evaluative study has been made on a V-Blast encoded MIMO MCCDMA wireless communication system on encrypted synthetically generated binary data transmissionusing Minimum Mean Square Error (MMSE) and Zero- Forcing (ZF) Linear channel equalization schemes. The 4G compatible system deploys two channel encoding schemes (1/2-rated Convolutional and CRC) under BPSK, DPSK, QPSK and QAM digital modulations. In the present simulated system, synthetically generated binary data transmission has been secured with concatenated implementation of Vigenere Cipher and RSA cryptographic algorithm. It is anticipated from the numerical results that the BPSK modulation outperforms as compared to DPSK, QPSK and QAM modulation schemes in MMSE channel equalization and V-BLAST based 1/2-rated Convolutional channel Encoded MIMO MCCDMA schemes under AWGN channels. For ZF channel equalization and CRC channel coding, the system shows identical performance. For both cases, QPSK digital modulation shows worst performance. It is noticeable from the present study that the ZF with ½-rated Convolution coding scheme is superior as compared to MMSE with CRC coding scheme for BPSK digital modulation.

Corresponding Author:

Mousumi Haque
Department of Information and Communication Engineering
Rajshahi University, Rajshahi-6205, BANGLADESH
Email:mishiape@yahoo.com

1. INTRODUCTION

The MC-CDMA is a hybrid transmission technique employing an amalgam of Code Division Multiple Access (CDMA) and Orthogonal Frequency Division Multiplexing (OFDM) and is expected to combine the benefits of pure CDMA and OFDM techniques. The MC-CDMA is an attractive choice for high speed wireless communication as it mitigates the problem of inters symbol interference (ISI) with exploitation of frequency diversity. It supports multiple users with high speed data communications.

The CDMA technique is widely used in current Third Generation (3G) wireless communication systems(W-CDMA-Wideband Code Division Multiple Access, UMTS-Universal Mobile Telecommunications etc) presenting a wide range higher data rate supported services such as voice/video/data (IP Television, video on demand, video conferencing, tele-medicine)[1],[2]. In spectrally efficient multiplexing scheme based MC-CDMA radio interface technique, data symbol of each individual is transmitted over multiple sub-carriers of an Orthogonal Frequency Division Multiplexing (OFDM) signal [3],[4].Through the use of orthogonal spreading codes, multiple data symbols share common subcarriers and their signals remain separable at the receiver.With suitable selections of spreading codes, the frequency diversity created by multipath propagation in the communications channel is exploited to improve the bit error rate (BER) over standard OFDM [5].

As the use of multiple antennas at both the transmit and receive ends(MIMO) has become one of the most important paradigms for the deployment of existing and emerging wireless communications systems, an effort has been made to exploit maximum multiplexing gain under implementation of V-BLAST scheme in MIMO transmission. The Vertical Bell Labs Layered Space-Time (V-BLAST) scheme was proposed in [6] for providing a multiplexing gain, viz. such scheme provides an increase of a specific user's effective bandwidth efficiency without the need for any increase in the transmitted power or in the system's bandwidth. Additionally, a MIMO scheme combining the benefits of V-BLAST and STBC was proposed in [7] and referred as a Double Space- Time Transmit Diversity (D-STTD). The D-STTD benefits from the diversity gain of the STBC and the multiplexing gain of the V-BLAST arrangement.

In 2011, Joshi, et.al., conducted simulation based study on performance evaluation of V-BLAST encoded MIMO wireless communication system with implementation of Maximum Likelihood (ML), Zero Forcing (ZF), Minimum Mean-Square Error (MMSE), and Successive Interference Cancellation (SIC) channel equalization(signal detection) schemes[8]. The present work has been extended to implement various channel equalization and channel coding schemes in 4G compatible MC CDMA MIMO system.

2. MATHEMATICAL MODEL

In our presently considered secured V-BLAST scheme implementation based MIMO (4× 4) MCCDMA Wireless communication system, Vigenere Cipher and RSA cryptographic algorithms and two channel equalization

2.1 V-Blast Scheme

In such a spatial multiplexing/demultiplexing scheme, the preprocessed digitally modulated complex symbols are mapped vertically onto successive columns of the transmission array viz. in encoding stage, a single complex signal stream is multiplexed inspace over multiple antennas. In decoding stage, the spatially multiplexed complex signals from multiple antennas are demultiplexed to produce a single complex signal stream [9].

2.2. Cryptographic Algorithm

The fundamental objective of cryptography is to enable two concerned persons to communicate over an insecure channel in such a way that an opponent cannot understand what is being said. This channel could be a telephone line or computer network. The information that one person wants to send to another, which we call "plaintext," can be English text, numerical data, or anything at all — its structure is completely arbitrary. The person encrypts the plaintext, using a predetermined key and sends the resulting ciphertext over the channel. No other person, upon seeing the ciphertext in the channel by eavesdropping, cannot determine what the plaintext was; but the concerned person who knows the encryption key, can decrypt the ciphertext and reconstruct the plaintext. In the present study, two cryptosystems such as Vigenere Cipher and RSA have been used.

Vigenere Cipher is a well-known mono alphabetic Cipher. In other mono alphabetic cryptosystems (Shift Cipher and the Substitution Cipher) once a key is chosen, each alphabetic character is mapped to a unique alphabetic character. The Vigenere Cipher is named after Blaise de Vigenere, who lived in the sixteenth century. The Vigenere Cipher encrypts *m* alphabetic characters at a time: each plaintext element is equivalent to *m* alphabetic characters. The whole plaintext is grouped and each group consists of m elements. To each group, the plaintext elements are converted to residues modulo 26 with adding a key consisted of m number of integer values to encrypt. In the paper, such Key has been represented with key word as:
K=[1 2 3 4 5 6 7 8].

To decrypt, we can use the same keyword, but we would subtract it modulo 26 instead of adding. In a Vigenere Cipher having keyword length *m*, an alphabetic character can be mapped to one of *m* possible alphabetic characters (assuming that the keyword contains *m* distinct characters). Such a cryptosystem is called polyalphabetic[10].

The RSA (Rivest-Shamir-Adleman) was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman. This RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n 1 for n less than 1024. It makes use of an expression with exponentials .Plaintext is encrypted in blocks and each block size must be less than or equal to log2(n). In RSA, Encryption and Decryption are of the following form, for some plaintext block M and ciphertext block C:

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n \qquad (1)$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e, n} and a private key of PU = {d, n}. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met up in consideration of two chosen prime numbers, p,q [11].

$ed\equiv 1 \bmod \varphi(n)$ and $d\equiv e^{1} \bmod \varphi(n)$ (2)

where, $n = pq$ and $\varphi(n) = (p- 1)(q -1)$

2.3 Channel Equalization

The received complex signal $y\in€^{4\times L}$ in terms of transmitted complex signal $s\in€^{4\times L}$, complex channel matrix $H\in€^{4\times 4}$ and additive white Gaussian noise $n\in€^{4\times L}$(L implies the total number of symbols transmitted from each antenna)can be written as

$$y=Hs+n \quad (3)$$

In Zero-Forcing (ZF) linear Channel Equalization (signal detection) scheme, the reconstructed transmitted complex signal $\hat{s}$ can be written as

$$\hat{s}=(H^{H}H)^{-1}H^{H}y \quad (4)$$

The ZF detection may give rise to noise enhancement, since:

$$\hat{s}=(H^{H}H)^{-1}H^{H}(Hs+n)=s+(H^{H}H)^{-1}H^{H}n \quad (5)$$

In Minimum mean square error (MMSE) linear signal detection(channel Equalization)scheme, the reconstructed transmitted complex signal $\hat{s}$ can be written as

$$\hat{s}=(H^{H}H+\sigma^{2}I)^{-1}H^{H}y \quad (6)$$

where, σ^{2} is the variance of the noise. At higher SNR, the term $\sigma^{2}I$ becomes negligible and the asymptotic performance is the same as ZF[9].

3. SYSTEM MODEL

A simulated single -user 4x 4 spatially multiplexed MCCDMA wireless communication system as depicted in Figure 1 utilizes two channel coding, linear channel equalization schemes and a 1024-tone OFDM. In such a communication system, the synthetically generated binary data is encrypted two times using Vigenere Cipher and RSA cryptographic algorithm. The doubly encrypted data are converted into binary bits and channel encoded using ½-rated Convolutional encoding or CRC scheme and interleaved for minimization of burst errors.

The interleaved bits are digitally modulated using various types of digital modulations such as Binary Phase Shift Keying (BPSK), Differential Phase Shift Keying (DPSK), Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude modulation (QAM). The number of digitally modulated symbols is increased eight times in copying section(as the processing gain of the Walsh Hadamard codes is eight).and subsequently multiplied with Walsh Hadamard codes. The Walsh–Hadamard coded digitally modulated symbols are fed into Vertical Bell Labs Layered Space-Time (V-BLAST) encoder.

In encoding stage, a single complex signal stream is multiplexed in space over multiple antennas [9]. The output of Vertical Bell Labs Layered Space-Time (V-BLAST) encoder are sent up into four serial to parallel converter. The serial to parallelly(S/P) converted complex data symbols are fed into each of the four OFDM modulator with 1024 sub carriers which performs an IFFT on each OFDM block of length 1024 followed by a parallel –to- serial conversion. A cyclic prefix(CP) of length L_{cp} (0.1*1024) containing a copy of the last L_{cp} samples of the parallel –to- serial converted output of the 1024-point IFFT is then prepended. The CP is essentially a guard interval which serves to eliminate interference between OFDM symbols. However, the resulting OFDM symbols of length 1024+ Lcp are lunched from the four transmitting antenna.

In receiving section, all the transmitted signals are detected with linear signal detection schemes and the detected signals are subsequently sent up to the serial to parallel(S/P) converter and fed into OFDM demodulator which performs FFT operation on each OFDM block. The FFT operated OFDM blocked signal are processed with cyclic prefix removing scheme and are undergone from parallel to serial conversion and are fed into Vertical Bell Labs Layered Space-Time (V-BLAST) decoder. Its output is multiplied with Walsh–Hadamard codes. The complex symbols are digitally demodulated, decopied, deinterleaved and channel decoded to recover the transmitted binary data [12], [13].

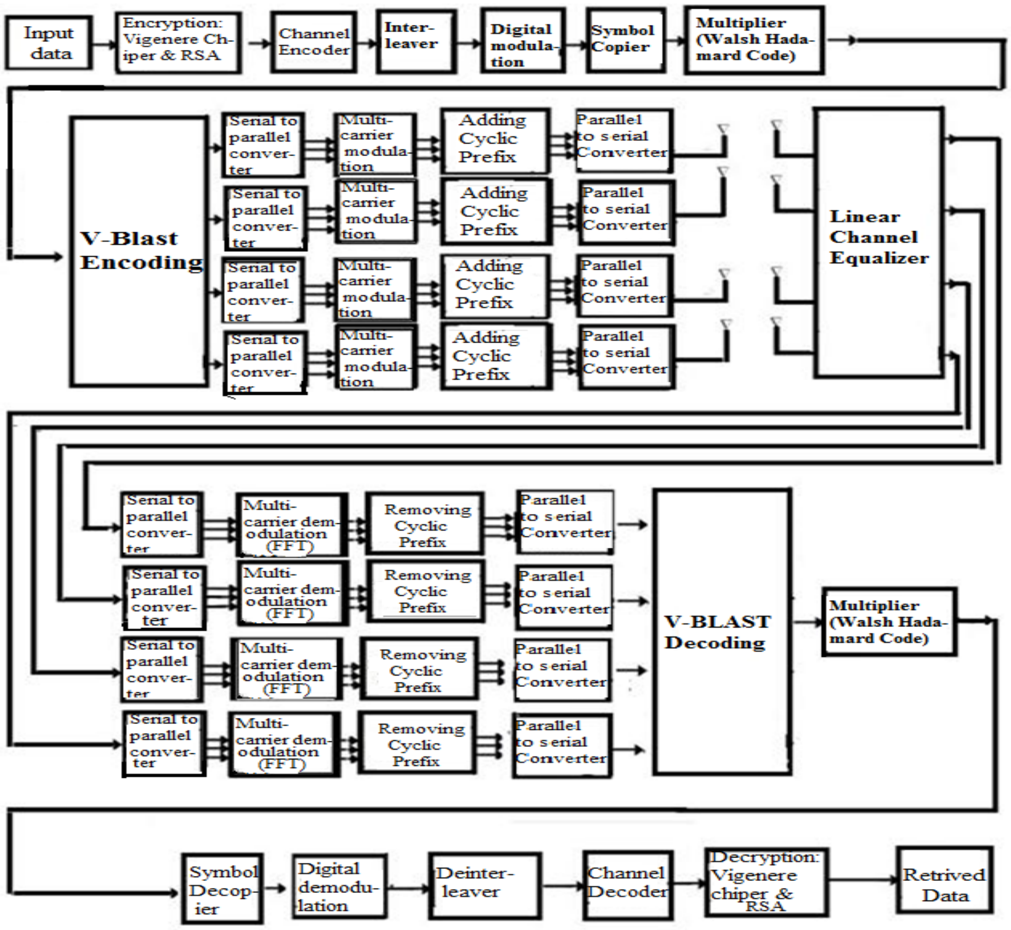
Input data
Encryption: Vigenere Chiper & RSA
Channel Encoder
Inter-leaver
Digital modulation
Symbol Copier
Multiplier (Walsh Hadamard Code)
V-Blast Encoding
Serial to parallel converter
Multi-carrier modulation
Adding Cyclic Prefix
Parallel to serial Converter
Serial to parallel converter
Multi-carrier modulation
Adding Cyclic Prefix
Parallel to serial Converter
Serial to parallel converter
Multi-carrier modulation
Adding Cyclic Prefix
Parallel to serial Converter
Serial to parallel converter
Multi-carrier modulation
Adding Cyclic Prefix
Parallel to serial Converter
Linear Channel Equalizer
Serial to parallel converter
Multi-carrier demodulation (FFT)
Removing Cyclic Prefix
Parallel to serial Converter
Serial to parallel converter
Multi-carrier demodulation (FFT)
Removing Cyclic Prefix
Parallel to serial Converter
Serial to parallel converter
Multi-carrier demodulation (FFT)
Removing Cyclic Prefix
Parallel to serial Converter
Serial to parallel converter
Multi-carrier demodulation (FFT)
Removing Cyclic Prefix
Parallel to serial Converter
V-BLAST Decoding
Multiplier (Walsh Hadamard Code)
Symbol Decopier
Digital demodulation
Deinter-leaver
Channel Decoder
Decryption: Vigenere chiper & RSA
Retrived Data

Figure 1. Block diagram of a V-Blast encoded MIMO MCCDMA wireless communication system

4. PARAMETERS FOR SIMULATION SETUP

The present study has been conducted with consideration of parameters presented in Table1.

Table 1. Summary of the simulated model parameters

Parameter	Values
Synthetically generated binary data (bits)	1024
Channel Coding	½-rated Convolutional and CRC Channel Encoding
Modulation	BPSK,DPSK,QPSK and QAM
Cryptographic algorithm	Vigenere Cipher and RSA
Linear Channel Equalization Scheme	Minimum Mean Square Error (MMSE) and Zero- Forcing (ZF)
Antenna configuration	4 × 4
Channel	AWGN and Rayleigh
Signal to noise ratio, SNR	0 to10 dB

5. RESULT AND DISCUSSION

In this section, it has been tried to present some simulation results with Matlab based on the parameters given in Table 1. The study is aimed at the verification of our theoretical claims on the BER performance of the V-BLAST encoded MIMO MCCDMA system under implementation of linear channel equalizers at different SNR values.The SNR is defined as symbol energy per transmit antenna versus noise power spectral density. It is assumed that the channel state information (CSI) is available at the receiver and the fading process is approximately constant during whole period of transmitted signals. The outcome of the present work illustrated in Figure 2 through Figure 6 is clearly indicative of system performance comparison in terms of Bit error rate (BER) for different SNR values.

In Figure 2for ZF channel equalization and Convolution channel coding schemes, it is observable that the system shows quite satisfactory performance for BPSK modulation at low SNR value area upto 4dB.Over a large examined SNR values, the system provides well defined and acceptable BER performance in BPSK modulation. It is observed that the BPSK modulation outperforms as compared to DPSK, QPSK and QAM modulation schemes. The performance of MCCDMA system is improved by 10.5817 dB in BPSK as compared to QPSK digital modulation at 3dB SNR.

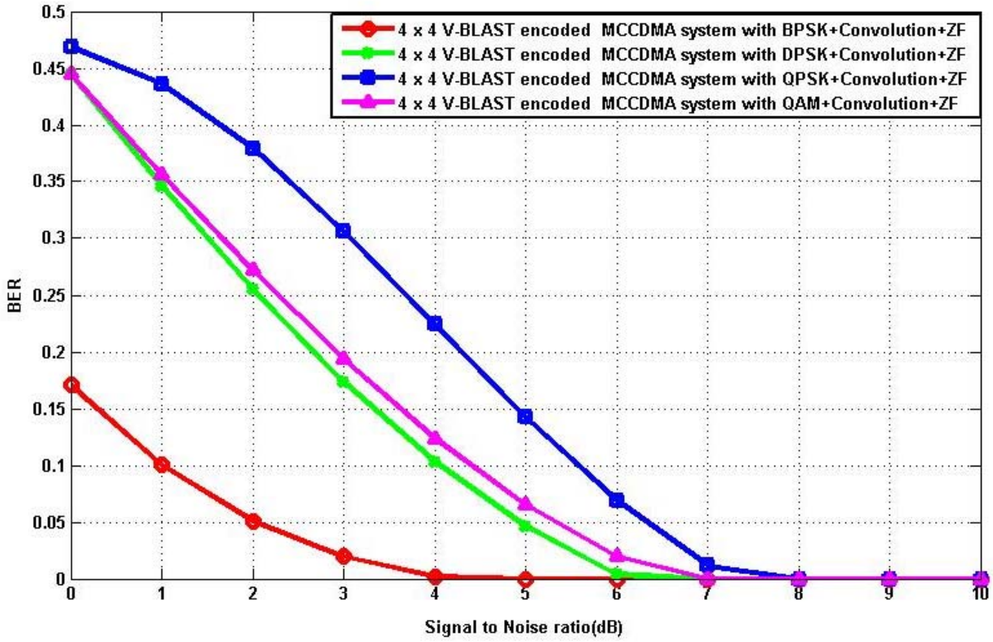

Figure 2. BER performance comparison of MIMO MCCDMA system with implementation of different digital modulation scheme under Convolution channel coding and ZF channel equalization scheme

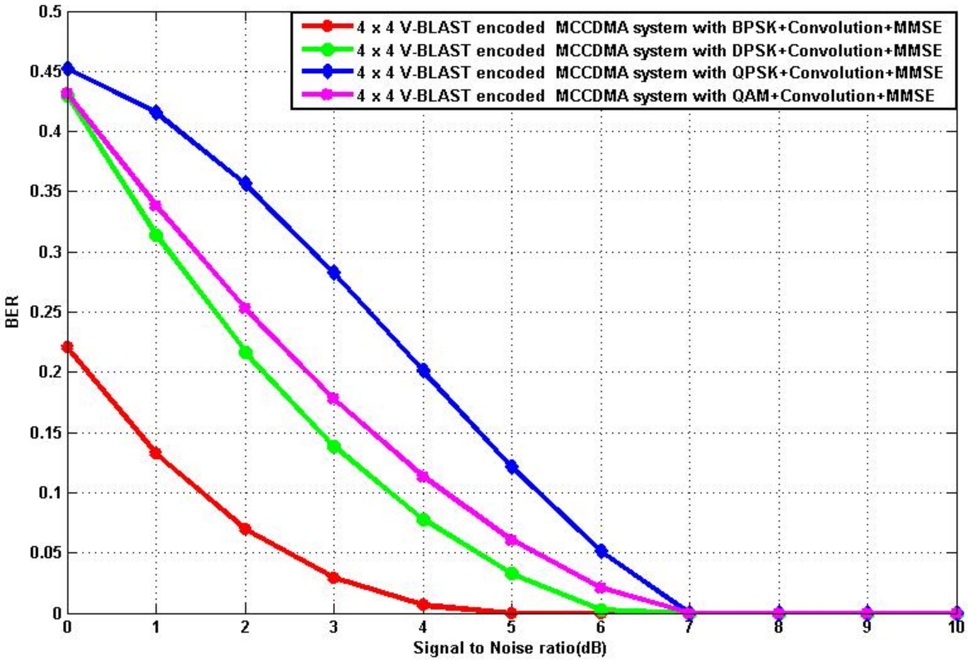

Figure 3. BER performance comparison of MIMO MCCDMA system with implementation of different digital modulation scheme under Convolution channel coding and MMSE channel equalization scheme

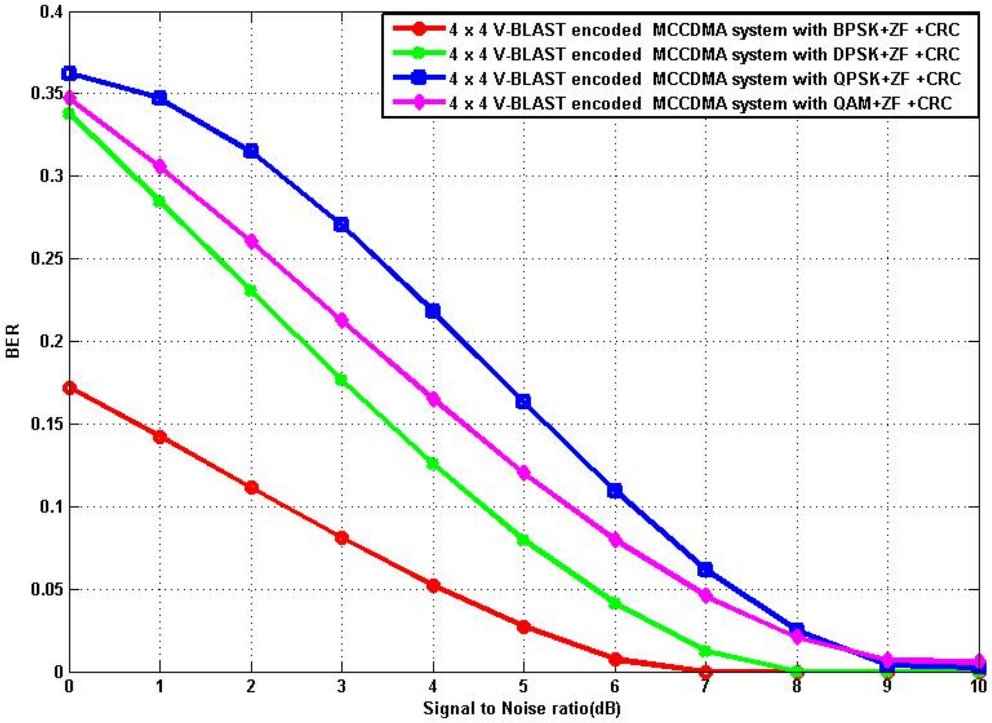

Figure 4. BER performance comparison of MIMO MCCDMA system with implementation of different digital modulation scheme under CRC channel coding and ZF channel equalization scheme

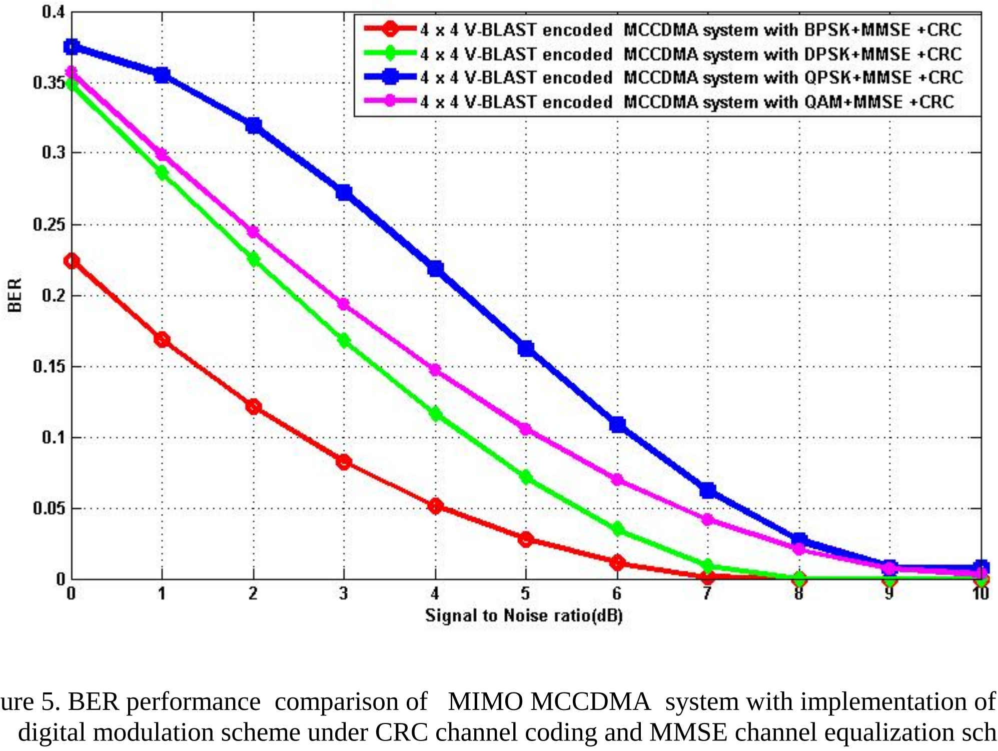

Figure 5. BER performance comparison of MIMO MCCDMA system with implementation of different digital modulation scheme under CRC channel coding and MMSE channel equalization scheme

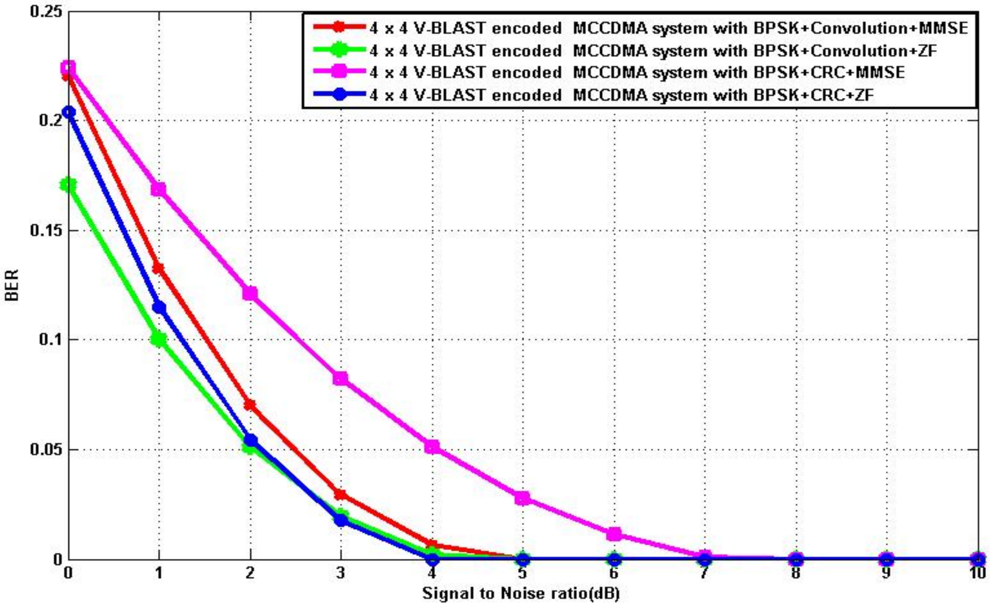

Figure 6. BER performance comparison of MIMO MCCDMA system with implementation of different channel coding and channel equalization schemes under BPSK digital modulation

In Figure 3 for MMSE with Convolution the BER values are 0.1387, 0.0293, 0.2821 and 0.1778 in BPSK, DPSK, QAM and QPSK digital modulation at a typically assumed SNR value of 3 dB viz. the V-BLAST encoded MIMO MCCDMA system shows better performance for BPSK and worst performance for QPSK. Meanwhile, Figure 4 for ZF channel equalization and CRC channel coding schemes, the present system shows almost identical performance for BPSK, DPSK, QAM and QPSK digital modulation over a large SNR value area. The BER values for a typical SNR value of 3dB are 0.0880 and 0.2302 in case of BPSK and QPSK digital modulation viz. the V-BLAST encoded MIMO MCCDMA system achieves an appreciable gain of 2.6159dB.

Figure 5 shows BER performance comparison of V-BLAST encoded MIMO MCCDMA system with implementation of different digital modulation scheme under CRC channel coding and MMSE channel equalization scheme. In Figure 5, the BER values for a typical SNR value of 3dB are 0.0678 and 0.2059 in case of BPSK and QPSK digital modulation viz the presently considered system performance is improved by 3.036 dB in BPSK as compared to QPSK digital modulation.

Additionally in Figure 6, it is keenly observed with 2dB SNR value consideration that the system performance with implemented ZF and Convolutional coding scheme is superior by approximately 2.3838 dB as compared to MMSE with CRC coding scheme for BPSK digital modulation

6. CONCLUSION

In our present study, we have tried to show performance of a FEC encoded 4 x 4 spatially multiplexed MIMO MCCDMA wireless communication system adopting various digital modulations and linear channel equalization schemes. A range of system performance results highlights the impact of a simplified digital modulation, channel equalization (signal detection) and channel coding techniques. In the context of system performance, it can be concluded that the implementation of BPSK digital modulation technique with Minimum Mean Square Error (MMSE) channel equalization in V-Blast with Convolutionally channel Encoded MIMO MCCDMA wireless communication system provides satisfactory performance in retrieving synthetically generated binary data in a hostile fading channel environment

REFERENCES

[1] Pallavi, P. and Dutta, P,"Muti-Carrier CDMA overview with BPSK modulation in Rayleigh channel", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 4, pp.464-469, 2010
[2] Cornelia-IonelaBadoi, Neeli Prasad ,Victor Croitoru , Ramjee Prasad," 5G Based on Cognitive Radio" , Wireless Pers Communications, vol.57, pp.441-464, 2011
[3] Savo Glisic,"Advanced Wireless Communications 4G Technologies" , John Wiley and Sons Ltd, England,2004
[4] M. McCloud," Analysis and design of short block OFDM spreading matrices for use on multipath fading channels", IEEE Trans. Commun.,vol. 53, no. 4, pp. 656-665, 2005

[5] M. Furudate, H. Ishikawa, and T. Suzuki," Evaluation of MC-CDMA with frequency interleaving technique in frequency selective fading channel", IEICE Trans. Commun., vol. E88-B, no. 2, pp. 443-451, 2005

[6] P.W. Wolniansky, G.J. Foschini, G.D. Golden and R.A. Valenzuela,"VBLAST: an architecture for realizing veryhigh data rates over the rich scattering wireless channel, International Symposium on Signals,Systems and Electronics", (Pisa), pp. 295–300,1998

[7] E.N. Onggosanusi, A.G. Dabak and T.A. Schmidl," High rate space time block coded scheme: performance and improvement in correlated fading channels", IEEE Wireless Communications and Networking Conference, vol. 1, pp. 194–199,2002

[8] Joshi, S.A.; Rukmini, T.S.; Mahesh, H.M." Error rate analysis of the V-BLAST MIMO channels using interference cancellation detectors, 2011", IEEE Wireless Communications and Networking Conference , pp. 614 - 618, 2011

[9] Alain Sibille, Claude Oestges and Alberto Zanella,,"MIMO From Theory to Implementation", Elsevier Inc., United Kingdom, 2011

[10] Douglas R. Stinson: Cryptography, "Theory and Practice", CRC Press, CRC Press LLC, USA

[11] William Stallings, 2005: Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall Publisher, 1995

[12] Goldsmith, Andrea"Wireless Communications", First Edition, Cambridge University Press, United Kingdom, 2005

[13] L. J. Cimini, Jr."Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing", IEEE Trans. Commun., vol. COM-33, pp. 665–675. 1985

BIOGRAPHY OF AUTHORS

Mousumi Haque joined as a lecturer in the Department of Information and Communication Engineering, Faculty of Engineering, University of Rajshahi, Rajshahi, Bangladesh in 2012. She received her B.Sc. (Hons) and M.Sc. degree from the Department of Applied Physics and Electronic Engineering, University of Rajshahi, Bangladesh in 2010 and 2011 respectively. During her post graduate study in the Department of Applied Physics and Electronic Engineering, She completed a research work on FEC encoded SISO MCCDMA wireless communication system. Her research interests include advanced wireless communications with special emphasis on MCCDMA, MIMO OFDM/OFDMA radio interface technologies.

Most. Farjana Sharmin received her Bachelor of Science (B.Sc) Honoursand M.ScDegree in Information and Communication Engineering from Rajshahi University in 2011 and 2012 respectively .Her main research interests include Space Time Block Coding, MISO/MIMO-OFDM, 4G compatible MC-CDMA radio interface technology.

Shaikh Enayet Ullah is a Professor of the Department of Applied Physics and Electronic Engineering, Faculty of Engineering, University of Rajshahi, Bangladesh. He received his B.Sc (Hons) and M.Sc degree both in Applied Physics and Electronics from University of Rajshahi in 1983 and 1985 respectively. He received his Ph.D degree in Physics from Jahangirnagar University, Bangladesh in 2000.He has earned US equivalent Bachelors and Master's degree in Physics and Electronics and Ph.D degree in Physics from a regionally accredited institution of USA from New York based World Education Services on the basis of his previously received degrees and academic activities (Teaching and Research), in 2003. He worked as a Professor and Chairman (on deputation) in the Department of Information and Communication Engineering, University of Rajshahi from 2009 to 2012. He has published more than 60 articles in multidisciplinary fields. His main research interests include Cooperative communications, MIMO-OFDM, WiMAX, Cognitive radio and LTE radio interface technologies.