SECURE TEXT MESSAGE TRANSMISSION IN MCCDMA WIRELESS COMMUNICATION SYSTEM WITH IMPLEMENTATION OF STBC AND MIMO BEAMFORMING SCHEMES

Mousumi Haque[1], Shaikh Enayet Ullah[2] and Joarder Jafor Sadique[2]

mishiape@yahoo.com , enayet67@yahoo.com and joarderjafor@yahoo.com

[1]Department of Information and Communication Engineering
Rajshahi University, Rajshahi-6205, Bangladesh
[2]Department of Applied Physics and Electronic Engineering
Rajshahi University, Rajshahi-6205, Bangladesh

ABSTRACT

In this paper, an effort has been made to elucidate BER performance of a secured MIMO MCCDMA wireless communication system. The simulated system under present study implements Space time block coding(STBC) and MIMO Beamforming schemes with three channel encoding schemes(1/2-rated Convolutional and CRC and BCH) and four digital modulations(BPSK,DPSK QPSK and QAM). In this system, transmission of text data has been secured with concatenated implementation of Vigenere Cipher and RSA cryptographic algorithm. It is anticipated from the numerical results that the STBC and MIMO Beamforming scheme adopted MCCDMA system with 1/2-rated Convolutional channel encoding technique outperforms in BPSK digital modulation under AWGN and Raleigh fading channels. In higher Signal to Noise ratio(SNR) values, the simulated system shows comparatively worst performance under CRC channel coding and DPSK, QPSK and QAM digital modulation schemes. It is also noticeable of system performance deterioration with lower SNR values

KEYWORDS:, *MIMO Beamforming , Cryptographic algorithm, MIMO MCCDMA, Bit Error rate , AWGN and Raleigh fading channels*

1.INTRODUCTION

With innovative technological development in wireless communications, it is known that the 4G LTE mobile phone networks have been deployed commercially in many countries of the world. To develop future generation robust MIMO communication systems for ensuring crystal clear voice conversation, live video transmission and high speed internet connectivity, a considerable amount of research is being going on worldwide to materialize the ever increasing wish of mankind using the constrained resources.

The MC-CDMA, a hybrid transmission technique is originated from an amalgamation of Code Division Multiple Access (CDMA) and Orthogonal Frequency Division Multiplexing (OFDM) and it exploits the benefits of pure CDMA and OFDM techniques. In high speed wireless

DOI : 10.5121/ijmnct.2013.3102

communication ,the MC-CDMA is considered as an attractive choice mitigating the problem of inter symbol interference (ISI) with exploitation of frequency diversity. The MC-CDMA radio interface technology supports multiple users with high speed data communications. It has not yet implemented in 4G network. In current Third Generation (3G) wireless communication systems(W-CDMA-Wideband Code Division Multiple Access, UMTS-Universal Mobile Telecommunications etc), the CDMA technique is widely used for providing high data rate supported services such as voice/video/data (IP Television, video on demand, video conferencing, tele-medicine)**[1,2].** In 2012, Lu zhang et.al, performed performance evaluative study of MIMO Beamforming and STBC when co-channel interferes use arbitrary MIMO modes **[3].** With implementation of STBC and MIMO Beamforming techniques, the present study is linked with secured data transmission in MCCDMA wireless communication system.

2. MATHEMATICAL MODEL

In my presently considered secured STBC and Beamforming based multi antenna supported MCCDMA wireless communication system, two cryptographic algorithms(Vigenere Cipher and RSA) and three channel coding schemes have been used. A brief description of Cryptographic algorithm and Diversity techniques is given below:

2.1 CRYPTOGRAPHIC ALGORITHM

The implementation of cryptographic algorithm(s)/technique(s) is fundamentally related to enable two concerned persons to communicate with each other over an insecure and hostile channel in such a way that an opponent cannot understand what is being communicated. The information that one person wants to send to another called plaintext which can be in English text, numerical data and other form. Using a predetermined key, the person encrypts the plaintext to send the resulting ciphertext over the channel. No other unauthorized person, upon seeing the ciphertext in the channel by eavesdropping, cannot determine the real feature of the plaintext. The concerned person knowing the encryption key, can decrypt the ciphertext and reconstruct the plaintext.

2.1.1 VIGENERE CIPHER

The Vigenere Cipher named after Blaise de Vigenere is a well-known monoalphabetic Cipher. In other monoalphabetic 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 encrypts *m* alphabetic characters at a time and 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. The Vigenere Cipher is a polyalphabetic cryptosystem 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) **[4,5].**

2.1.2 RSA

Ron Rivest, Adi Shamir, and Len Adleman developed RSA (Rivest-Shamir-Adleman) in 1977. This RSA cryptographic scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and 2^{1024}. This cryptographic scheme makes use of an expression with exponentials. The plaintext is encrypted in blocks and each block having a binary value less than a typical number n viz. each block size must be less than or equal to $\log_2(n)$. In RSA, encryption and decryption are of the following form for some plaintext block M and ciphertext block C:

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

In RSA scheme, 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 **[6].**

$$ed \equiv 1 \bmod \varphi(n) \text{ and } d \equiv e^1 \bmod \varphi(n) \quad (2)$$
where, $n = pq$ and $\varphi(n) = (p-1)(q-1)$

2.2 Diversity

The idea of diversity is very simple and intuitive. In communication terms, if multiple and independent routes called diversity branches are provided for the same information, the probability that the information is lost due to fading is much reduced, since it would require all branches to fade simultaneously. If the branches are indeed independent then the error probability is reduced according to the number of branches. If n number of branches is used to transmit the same information, n will be the diversity order. In space diversity MIMO system, the diversity branches are provided by spatially separated antennas **[7]**

2.2.1 MIMO Beamforming

MIMO(Multi-input multi-output) techniques utilizing multiple antennas at the transmitter and/or receiver have emerged as a milestone of modern wireless communications due to their potential for achieving higher link reliability and data rates.

We assume a general antenna configuration of 2×2 for a single user MIMO beamforming downlink transmission(Base Station to mobile station.) . At each transmitted symbol period, the baseband received signal vector

$r \in \mathbb{C}^{2\times 1}$ can be modeled as
$r = H_0 w_0 s_0 + n$

where $H_0 \in \mathbb{C}^{2\times 2}$ is the channel matrix over the desired link and it is assumed to be perfectly known by the Base station; n is the additive which white Gaussian noise and $_0$ is the transmitted symbol from base station; and $w_0 \in \mathbb{C}^{2\times 1}$ is the precoding unitary vector for MIMO

Beamforming transmission. On Singular value decomposition(SVD) of H_0, we get, $H_0 = U\Sigma V^H$, where, $U \in \mathbb{C}^{2\times2}$ and $V \in \mathbb{C}^{2\times2}$ are the left and right unitary matrices respectively;

$\Sigma \in \mathbb{C}^{2\times2}$ is a rectangular diagonal matrix with two non negative real singular values (λ_1 and λ_2, $\lambda_1 > \lambda_2$). For the largest singular value λ_1, the corresponding column vector in U and corresponding column vector in V are denoted by u_1 $\mathbb{C}^{2\times1}$ and v_1 $\mathbb{C}^{2\times1}$ respectively. The precoding unitary vector $w_0 = \sqrt{2}v_1$. At the receiving end, the transmitted symbol s_0 is recovered through left multiplying received signal vector r by u_1^H **[3].**

3. SYSTEM MODEL

A simulated single -user multi antenna supported MCCDMA wireless communication system as illustrated in Figure 1 adopts MIMO Beamforming(Transmit and Receive), channel coding, and various digital modulation schemes with a 1024-tone OFDM. In such a simulated wireless system, the text message is encrypted doubly using Vigenere Cipher and RSA cryptographic algorithms. The encrypted data are converted into binary bits and channel encoded using individual implementation of ½-rated Convolutional , CRC and BCH schemes and interleaved for minimization of burst errors. The interleaved bits are digitally modulated using 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 for an assigned processing gain value of eight and subsequently multiplied with Walsh Hadamard codes. The Walsh–Hadamard coded and digitally modulated symbols are fed into Space time block encoder for processing with implemented philosophy of Alamouti's G_2 Space time block coding scheme **[8, 9].** The output of the STBC encoder is sent up into two serial to parallel(S/P) converter. The S/P converted complex data symbols are fed into each of the two OFDM modulator with 1024 sub carriers which performs an IFFT on each OFDM block of length 1024 followed by a parallel-to-serial(P/S) conversion. The output of the parallel-to-serial conversion are sent up into two multiplier with beamforming transmit weights.

All the transmitted signals in receiving section are detected by multiplier with beamforming receiver weights and the detected signals are subsequently sent up to the 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 P/S conversion and are fed into STBC decoder. The decoded output is multiplied with Walsh–Hadamard codes .The complex symbols are digitally demodulated, decopied, deinterleaved, channel decoded and eventually undergone through double decryption process to recover the transmitted text message**[10,11].**

Fi

Figure 1. Block diagram of a secured STBC and MIMO Beamforming scheme implemented MCCDMA wireless communication system

4. RESULTS AND DISCUSSION

In this section, computer simulations using MATLAB have been performed to evaluate the BER performance of a 2x2 multi antenna supported and STBC and MIMO Beamforming schemes implemented MC-CDMA wireless communication system based on the parameters presented in Table 1.

Table 1. Summary of the simulated model parameters

Parameter	Values
Text message(bits)	1024
Channel Coding	½-rated Convolutional and CRC and BCH Channel Encoding
Modulation	BPSK,DPSK,QPSK and QAM
Cryptographic algorithm	Vigenere Cipher and RSA
Diversity technique	MIMO Beamforming and STBC
Antenna configuration	2 × 2
Channel	AWGN and Rayleigh
Signal to noise ratio, SNR	0 to10 dB

The present study is mainly directed towards critical BER performance evaluation of the MIMO MCCDMA system under various considerable schemes. The SNR has been defined as symbol energy per transmit antenna versus noise power spectral density. The graphical illustrations presented in Figure 2 through Figure 5 are clearly indicative of system performance comparison in terms of Bit error rate(BER) for different SNR values.

In Figure 2 with CRC channel coding scheme, it is observable that the system shows quite satisfactory performance for BPSK modulation at low SNR value. Over a significant d SNR values, the system provides well defined and acceptable BER performance in BPSK modulation. It is observed that the system outperforms in BPSK modulation as compared to DPSK, QPSK and QAM modulation schemes. The estimated BER values are 0.0732 and 0.2666 in BPSK and QPSK digital modulation at 3dB SNR value viz. the performance of the MIMO MCCDMA system is improved by 5.61 dB.

In Figure 3, the BER performance are compared under the setting with ½ rated Convolution channel coding scheme. The estimated BER values are 0.0142, 0.1475, 0.1514 and 0.2705 in case of BPSK, DPSK, QAM and QPSK digital modulations at a typically assumed SNR value of 3dB viz. the system shows better performance in BPSK and worst performance in QPSK with a 12.80 dB system performance improvement.

In Figure 4 with BCH channel coding scheme, we can see that the performance loss is due to increase in modulation order with imperfect recovery of carrier frequency and phase in QPSK digital modulation as compared to BPSK. At a typically assumed SNR value of 2 dB, the estimated BER values are 0.0168 and 0.2988 in case of BPSK and QPSK digital modulations viz. the simulated system achieves an appreciable gain of 12.50dB.

In Figure 5, the performance gap of the system with different channel coding schemes is noticeable. At low SNR value of 2dB, the estimated BER values are 0.0255 and 0.1303 in case of BCH and CRC channel coding schemes under BPSK digital modulation which is indicative of system performance improvement by 7.08 dB

.

Additionally in Figure 6, the original, encrypted and retrieved text messages at 0dB, 1dB, 2dB, 4dB, 6dB, 8dB and 10dB SNR values have been presented under implementation of BPSK digital modulation and BCH channel coding schemes. It is keenly observed that the system shows quite satisfactory performance in retrieving text message at a quite low SNR value of 4dB.

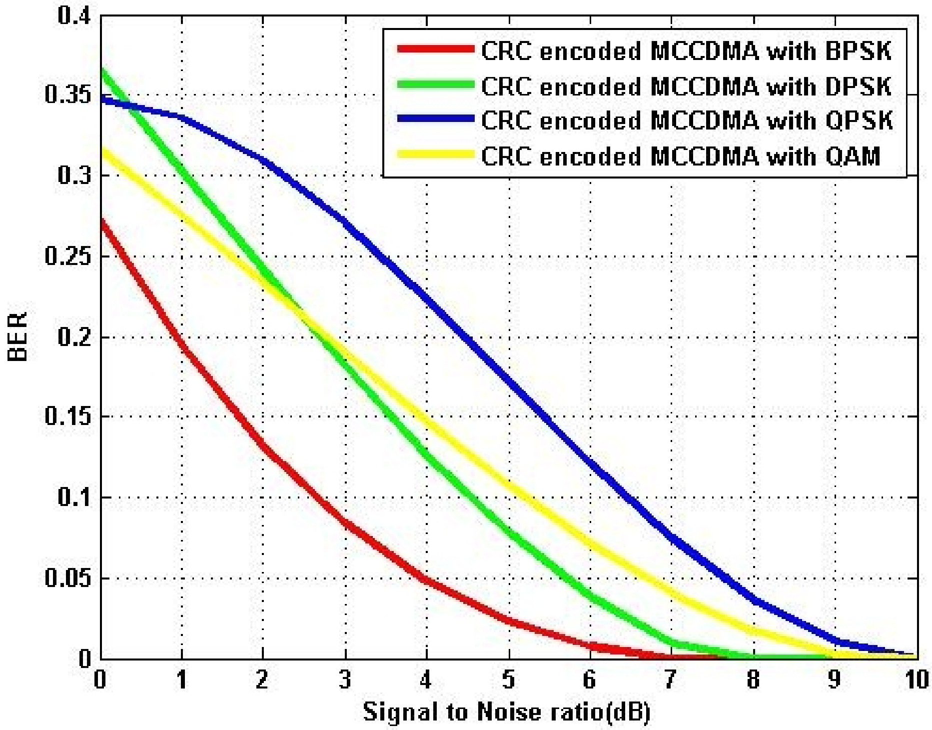

Figure 2. BER performance of a secured STBC and MIMO Beamforming scheme adopted MCCDMA wireless communication system under implementation of CRC channel coding and different digital modulation schemes

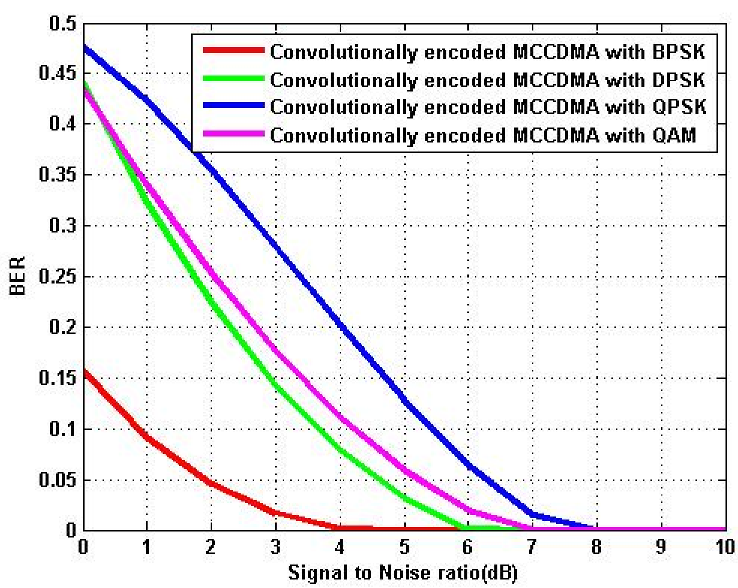

Figure 3. BER performance of a secured STBC and MIMO Beamforming scheme adopted MCCDMA wireless communication system under implementation of Convolutional channel coding and different digital modulation schemes

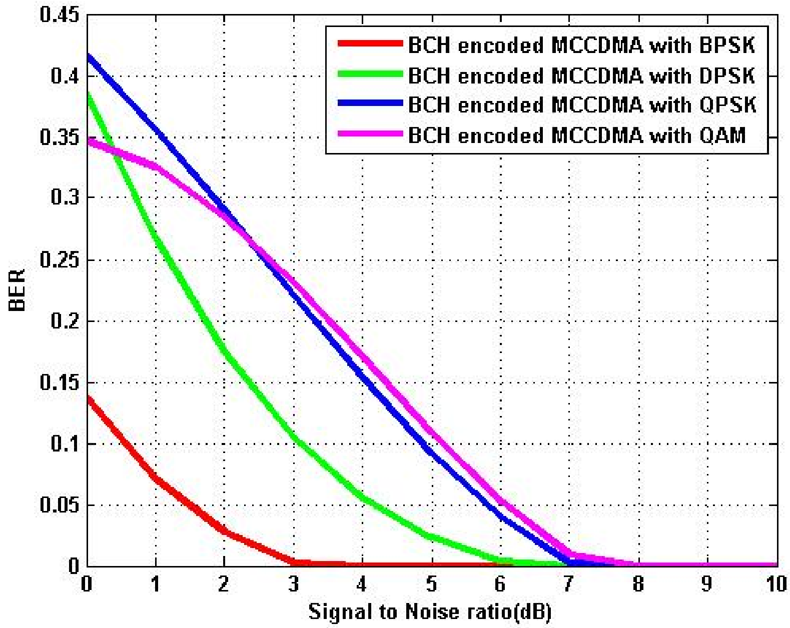

Figure 4. BER performance of a secured STBC and MIMO Beamforming scheme adopted MCCDMA wireless communication system under implementation of BCH channel coding and different digital modulation schemes

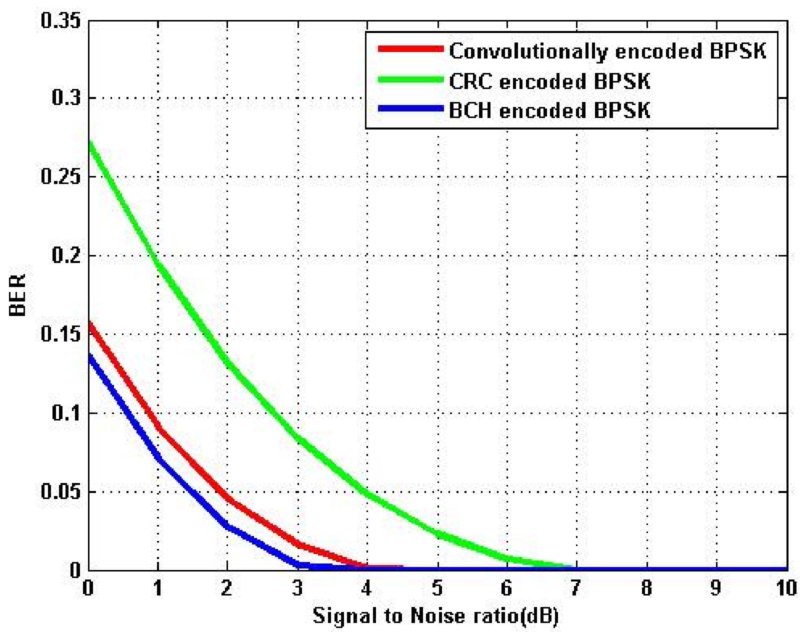

Figure 5. BER performance comparison of a secured STBC and MIMO Beamforming scheme adopted MCCDMA wireless communication system under implementation of different channel coding and BPSK digital modulation schemes

In 30th Oct.2012,a UK based Mobile operator EE first lunched 4G LTE mobile phone network in United Kingdom over its 11 cities

(a)Original text message

k9D 5"C(| b fY,D-
|&iitggE1ui gDGuJXiu uEkl' tvW Pv hh fN(M
EI~t ,JCi vC CgD " G D G&\v vhh 09vh: uF GzKWW& p
KWJ"(

(b) Encrypted text message

h& 3 t% hE.2 Y.,a!UK a`O\ MJb.lM opira jr WG(f.rstX u/dkeS
G=LTE= mvile peon n-twork in Unit* %x ng @O voN i% w1o c tiss

(c) Retrieved text message at 0dB

IgB4Y(:MOc_f2&1=WN UKwbMaes8 oCilA!fpTPator^EE {Ur&4%l&lah%d
vs 9 g7mo i)h Y@o*eHnetJor2oin\ _: e Kilhdo %ok*iHGos,1I ci4 eE

(d) Retrieved text message at 1dB

In 3hth Oct.]A1. a UK b ed M4 &l* t HratoC%E cfirst unchfS 4 NTE
m@bilV p:jne n6tBork sn U itedN/ingdofX4le| itst1l -i i<sD

(e) Retrieved text message at 2dB

In 30th Oct.2012,a UK based Mobile operator EE first lunched 4G LTE mobile phone network in United Kingdom over its 11 cities

(f) Retrieved text message at 4dB

In 30th Oct.2012,a UK based Mobile operator EE first lunched 4G LTE mobile phone network in United Kingdom over its 11 cities

(g) Retrieved text message at 6dB

In 30th Oct.2012,a UK based Mobile operator EE first lunched 4G LTE mobile phone network in United Kingdom over its 11 cities

(h) Retrieved text message at 8dB

In 30th Oct.2012,a UK based Mobile operator EE first lunched 4G LTE mobile phone network in United Kingdom over its 11 cities

(i) Retrieved text message at 10dB

Figure 6. Transmitted, Encrypted and Retrieved text messages in a secured STBC and MIMO Beamforming scheme adopted MCCDMA wireless communication system. Red marks indicate noise contamination

5. CONCLUSION

In our present study, we have studied the performance of 2 x 2 spatially multiplexed MIMO MCCDMA wireless communication system with implementation of STBC and MIMO Beamforming schemes adopting various digital modulations and channel coding schemes. A range of system performance results highlights the impact of a simplified digital modulation, and channel coding techniques. In the context of system performance, it can be concluded that the implementation of BPSK digital modulation technique with BCH channel Encoded MIMO MCCDMA wireless communication system provides satisfactory performance in retrieving the transmitted text message 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, NeeliPrasad ,VictorCroitoru and Ramjee Prasad , "5G Based on Cognitive Radio," Wireless Personal Communications, vol.57, pp.441-464, 2011

[3] Lu Zhang, Yongzhao Li, Leonard J. Cimini," Statistical Performance Analysis for MIMO Beamforming and STBC when Co-Channel Interferers Use Arbitrary MIMO Modes" IEEE Transactions on Communications, vol. 60, no. 10, pp. 2926 – 2937, 2012

[4] Douglas R. Stinson" Cryptography: Theory and Practice", CRC Press, CRC Press LLC, USA, 1995

[5] Mousumi Haque'' Secure text message transmission in a 4G compatible MIMO MCCDMA system with combined implementation of Vigenere Cipher and RSA cryptographic algorithm'', International Journal of Information Technology Convergence and Services (IJITCS) vol.2, no.5, pp.9-18, 2012

[6] William Stallings" Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall Publisher, 2005

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

[8] John . G. Proakis and Masoud Salehi" Digital Communications", Fifth Edition, McGraw Hill Company Inc., New York, USA, 2001

[9] Siavash M. Alamouti" A Simple Transmit Diversity Technique For Wireless Communications",IEEE Journal on Select areas in Communications, vol.16, no.8, pp.1451-1458, 1998

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

[11] 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

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.

Shaikh Enayet Ullah is a Professor of the Department of Applied Physics and Electronic Engineering, Faculty of Engineering, University of Rajshahi, 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.

Joarder Jafor Sadique received his B.Sc. (Hons.) degree in Applied Physics and Electronic Engineering department from University of Rajshahi, Bangladesh in 2010. During his post graduate study, he has completed a research work on MIMO SC-FDMA Wireless Communication System. His research interest includes Channel Equalization, Radio Interface technologies (OFDMA and SC-FDMA) and Antenna Diversity.