Secure text message transmission in a 4G compatible MIMO MCCDMA system with combined implementation of Vigenere Cipher and RSA cryptographic algorithm

Mousumi Haque[1]

[1]Department of Information and Communication Engineering
Rajshahi University, Rajshahi-6205, BANGLADESH

mishiape@yahoo.com

ABSTRACT

In this paper, a comprehensive performance evaluative study has been made on a secured MIMO MCCDMA wireless communication system with implementation of 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, a text message transmission has been secured with concatenated implementation of Vigenere Cipher and RSA cryptographic algorithm. It is anticipated from the numerical results that with MMSE channel equalization and 1/2-rated Convolutional channel Encoding schemes, the MIMO MCCDMA system outperforms in BPSK digital modulation under AWGN and Raleigh fading channels. In CRC channel coding, the system shows comparatively worst performance in higher Signal to Noise ratio(SNR) values under DPSK, QPSK and QAM digital modulations. It has been observed from the present study that the system performance deteriorates with increase in noise power as compared to signal power.

KEYWORDS

MIMO MCCDMA, ZF, MMSE, Vigenere Cipher and RSA cryptographic algorithm, Bit Error rate(BER), AWGN and Raleigh fading channels.

1. INTRODUCTION

Orthogonal Frequency-Division Multiplexing (OFDM) has emerged as a successful air-interface multicarrier digital modulation technique advocated by many European standards, such as Digital Audio Broadcasting (DAB), Digital Video Broadcasting for Terrestrial television (DVB-T), Digital Video Broadcasting for Handheld terminals (DVB-H) , Wireless Local Area Networks (WLANs) and Broadband Radio Access Networks (BRANs). In perspective of wired environments, the OFDM transmission techniques known as Discrete Multi-Tone (DMT) are employed in theAmerican National Standards Institute’s (ANSI’s) Asymmetric Digital Subscriber Line (ADSL), High-bit-rate Digital Subscriber Line (HDSL) and Very-high-speed Digital Subscriber Line (VDSL) standards as well as in the European

DOI : 10.5121/ijitcs.2012.2502

Telecommunication Standard Institute's (ETSI's) VDSL applications**[1]**. 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 inter 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)**[2,3].** In 2012, Sarkar et.al, performed performance evaluative study ofFEC encoded MC-CDMA wireless communication system with adaptation of various signals detection and two-layer spreading schemes**[4].** In the present study, secured data transmission has been ensured with implementation of cryptographic algorithm.

2. MATHEMATICAL MODEL

In my presently considered secured **2 x 2** spatially multiplexed MIMO MCCDMA wireless communication system, Vigenere Cipher and RSA cryptographic algorithms and two channel equalization schemes have been used. A brief description is given below.

2.1. 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.

VigenereCipher 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 VigenereCipher 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**[5].**

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:

$C = M^{e} \bmod n$

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

(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 **[6].**	

ed1 mod (n) and de^{1} mod (n) (2)

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

2.2. Channel Equalization

The received complex signal $y\text{€}^{2\times L}$ in terms of transmitted complex signal $s\text{€}^{2\times L}$, complex channel matrix $H\text{€}^{2\times 2}$ and additive white Gaussian noise $n\text{€}^{2\times L}$(**L** implies the total number of symbols transmitted from each antenna)can be written as

y=Hs+n (3)

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

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

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**[7].**

3. SYSTEM MODEL

.A simulated single -user 2 x 2 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 text message 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/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 Hadamardcodes.The Walsh–Hadamard coded digitally modulated symbols are fed into Space time block encoder for processing

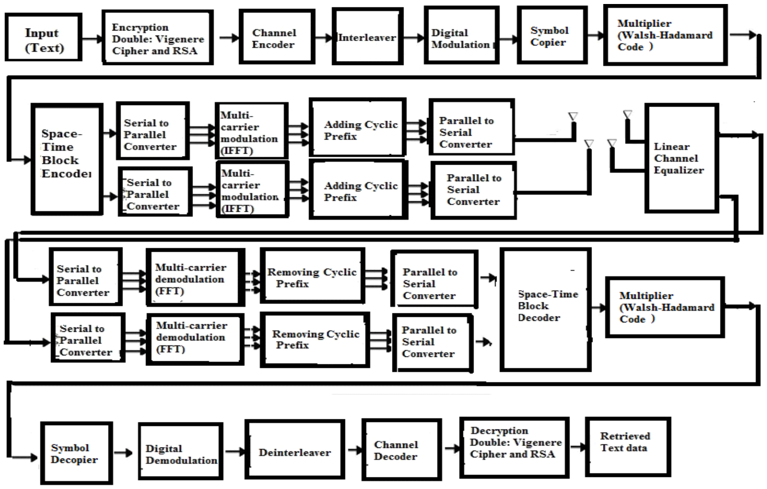
Input (Text)
Encryption Double: Vigenere Cipher and RSA
Channel Encoder
Interleaver
Digital Modulation
Symbol Copier
Multiplier (Walsh-Hadamard Code)
Space-Time Block Encoder
Serial to Parallel Converter
Multi-carrier modulation (IFFT)
Adding Cyclic Prefix
Parallel to Serial Converter
Serial to Parallel Converter
Multi-carrier modulation (IFFT)
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
Space-Time Block Decoder
Multiplier (Walsh-Hadamard Code)
Symbol Decopier
Digital Demodulation
Deinterleaver
Channel Decoder
Decryption Double: Vigenere Cipher and RSA
Retrieved Text data

Figure 1: Block diagram of a MIMO MCCDMA wireless communication system

with implemented philosophy of Alamouti's G_2 Space time block coding scheme**[8,9].**The output of theSpace time block encoder are sent up into two serial to parallel converter. The serial to parallelly(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 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 two 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 Space time block decoder. Its output is multiplied with Walsh–Hadamard codes .The complex symbols are digitally demodulated ,decopied , deinterleaved and channel decoded to recover the transmitted text message**[10,11].**

4. RESULT AND DISCUSSION

In this section, It has been tried to present some simulation results with Matlabbased on the parameters given in Table 1 . The study is aimed at the verification of my theoretical claims on the BER performance of the 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 4 is clearly indicative of system performance comparison in terms of Bit error rate(BER) for different SNR values. In all cases, it is remarkable that the system performance is non discriminativeat high SNR values as the noise contribution is insignificant in MMSE as compared to ZF. In Figure 2for QPSK modulation, it is observable that the system shows quite satisfactory performance in MMSE and CRC channel coding schemes at low SNR value area upto 3dB.Over a large examined SNR values, the system provides well defined and acceptable BER performance in MMSE and Convolutional coding schemes. At a reasonably considered 5% BER value, the implemented MMSE with Convolutional coding scheme is superior by approximately 1.6 dB as compared to ZF with CRC coding scheme. In Figure 3 for QAM modulation, no remarkable change in BER values is noticeable in case of MMSE with CRC and ZF with CRC. The BER values are 0.1539 and0.2096in MMSE with Convolutional coding and ZF with CRC at a typically assumed SNR value of 3 dB viz. the MIMO MCCDMA system achieves an inappreciable gain of 1.34 dB .In Figure 4 for DPSK, the present system shows almost identical performance withboth MMSE and ZF implementation with Convolutionalchannel coding scheme over a large SNR value area. In case of CRC, a slightly improved performance is observed in MMSE as compared to ZF. At low SNR value upto 1.5 dB, the system provides improved performance in CRC relative to Convolutional channel coding. In Figure 5 for BPSK, the system shows well defined response in MMSE and Convolutional channel coding.The BER values are 0.0153and 0.0807in MMSE with Convolutional coding and ZF with CRC at a typically assumed SNR value of 3 dB viz. the MIMO MCCDMA system achieves an appreciable gain of 7.22dB. Additionally, it is keenly observed that the implemented MMSE with Convolutional coding scheme is superior by approximately 2.2 dB as compared to ZF with CRC coding scheme at a typically considered 5% BER value.In Figure 6, the transmitted and retrieved text messages at 0dB, 2dB, 4dB and 6dB have been presented under implementation of BPSK, MMSE and Convolutional channel coding schemes. The estimated BER values at 0dB, 2dB, 4dB and 6dB are 0.1348, 0.0547, 0.0059 and 0.0 respectively.

Table 1: Summary of the simulated model parameters

Text message(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	2 × 2
Channel	AWGN and Rayleigh
Signal to noise ratio, SNR	0 to10 dB

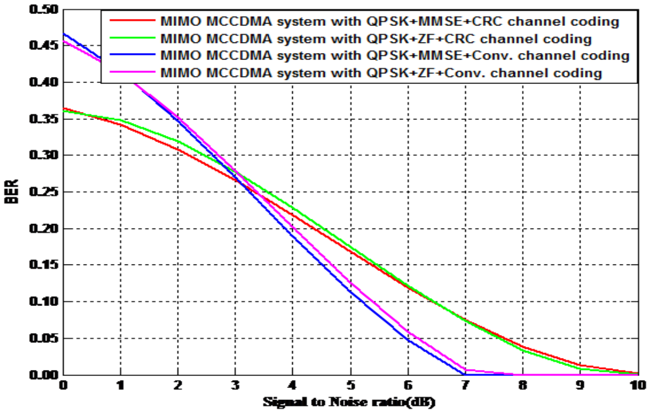

Figure 2 : BER performance comparison of MIMO MCCDMA system with implementation of different channel coding and channel equalization schemes under QPSK digital modulation

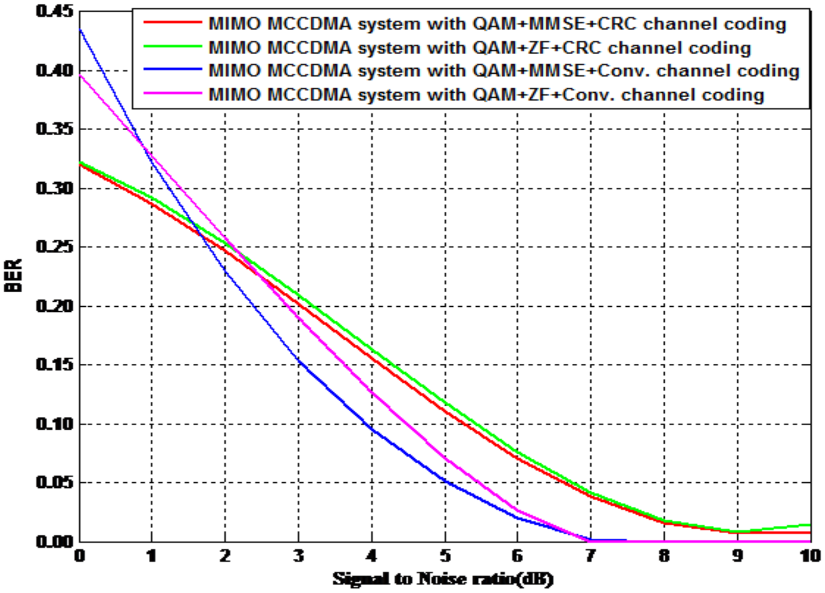

Figure 3 : BER performance comparison of MIMO MCCDMA system with implementation of different channel coding and channel equalization schemes under QAM digital modulation

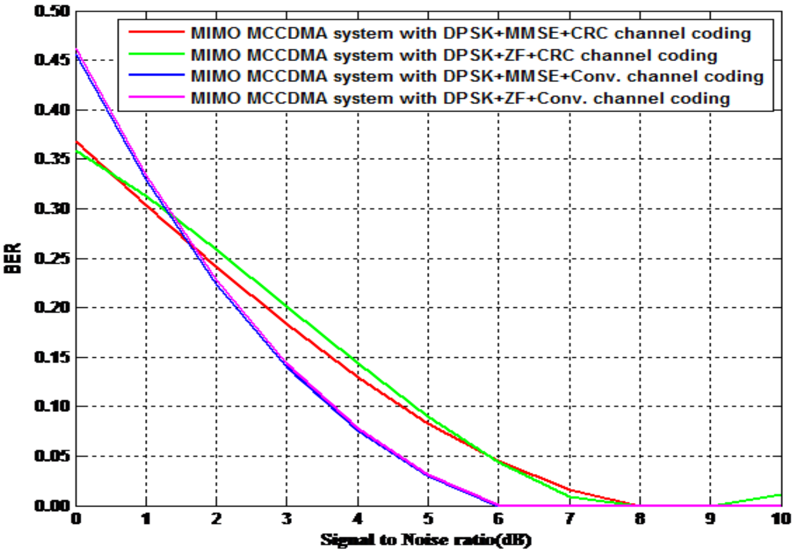

Figure 4 : BER performance comparison of MIMO MCCDMA system with implementation of different channel coding and channel equalization schemes under DPSK digital modulation

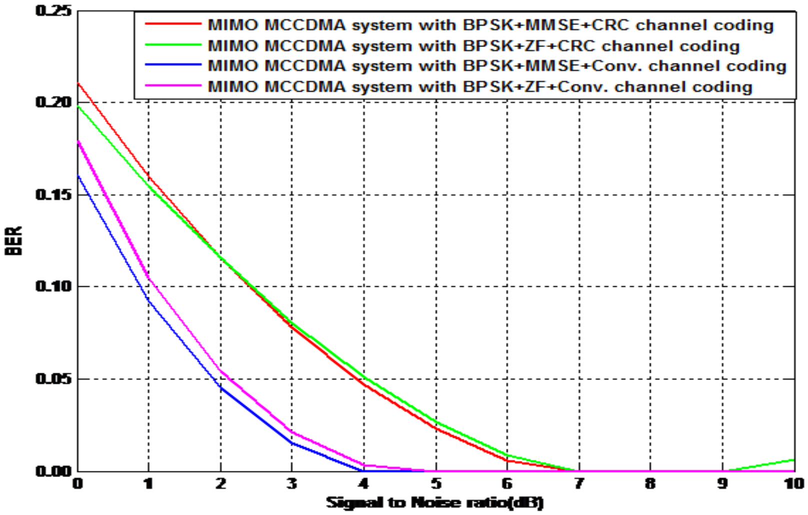

Figure 5 : BER performance comparison of MIMO MCCDMA system with implementation of different channel coding and channel equalization schemes
under BPSK digital modulation

Text message transmission in a multi user MIMO MCCDMA wireless Communication system using RSA cryptographic algorithm.

- **Original text message**

Text dessageu9ra@<g%ssio/HinkabhY&iuserMMO MCCDMKo"c1Eless Communicatiopsytem\A)p RS crypWo#u8 hictalg*rith

(b) Retrieved text message at 0dB

Text mesfgetrapsmissin in a multi u'er M M□ MCCDMA w+rless Communication system using RSA cryptographic algorithm.1?Tv

(c) Retrieved text message at 2dB

Text message transmission in a multi user MIMO CCDMA wireless Communication syste- using RSA cryptographic algorithm.

(d) Retrieved text message at 4dB

(e) Retrieved text message at 6dB

Figure 6 : Transmitted and Retrieved text messages.

Red marks indicate noise contamination

5. CONCLUSIONS

In my present study, I have studied the performance of a FEC encoded 2 x 2 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 techniquewithMinimum Mean Square Error(MMSE)channel equalization in Convolutionally channel Encoded MIMO MCCDMA wireless communication system provides satisfactory performance in retrieving the transmitted text message in a hostile fading channel environment.

ACKNOWLEDGEMENT

The author would like to express her gratefulness to Dr. ShaikhEnayetUllah, Ex. Professor and Chairman, Department of Information and Communication Engineering, Rajshahi University, Rajshahi, Bangladesh for critical reviewing the manuscript

REFERENCES

[1]. LajosHanzo, Yosef (Jos) Akhtman , Li Wang and Ming Jiang(2011)" MIMO-OFDM for LTE, Wi-Fi and WiMAX," John Wiley and Sons Ltd, United Kingdom.

[2]. Pallavi, P. and Dutta, P(2010)" 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.

[3]. Cornelia-IonelaBadoi, NeeliPrasad ,VictorCroitoru , Ramjee Prasad (2011)"5G Based on Cognitive Radio" Wireless Pers Communications, Vol.57, pp.441-464.

[4] SohagSarker, FarhanaEnam, Md. GolamRashed and ShaikhEnayetUllah(2012)" Performance Analysis of Two-Layer Spreading scheme based FEC encoded MC–CDMA wireless communication system under implementation of various signal detection schemes", Journal of Emerging Trends in Computing and Information Sciences, vol 3, No.4, pp 554-560, Canada

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

[6] William Stallings(2005)" Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall Publisher
[7] Alain Sibille, Claude Oestges and Alberto Zanella(2011)"MIMO From Theory to Implementation", Elsevier Inc., United Kingdom

[8] John . G. Proakisand MasoudSalehi(2001)" Digital Communications", Fifth Edition, McGraw Hill Company Inc., New York, USA

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

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

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

BIOGRAPHY OF AUTHOR

MousumiHaque 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.