SECURED TEXT MESSAGE TRANSMISSION IN PRE -CHANNEL EQUALIZATION BASED MIMO- OFDM SYSTEM WITH IMPLEMENTATION OF CONCATENATED ECB AND CFB CRYPTOGRAPHIC ALGORITHM

Laila Naznin[1],Shahrina Sultana[1], M. Golam Rashed[1] and Shaikh Enayet Ullah[2]

[1]Department of Information and Communication Engineering,
University of Rajshahi, Rajshahi, Bangladesh
{lipy_ice,im.sultana}@yhaoo.com,golamrashed@ru.ac.bd

[2]Department of Applied Physics and Electronic Engineering,
Rajshahi University, Rajshahi, Bangladesh
enayet67@yhaoo.com

ABSTRACT

In this paper, we made a comprehensive performance evaluative study of a secured MIMO Orthogonal Frequency-Division Multiplexing wireless communication system with implementation of two pre channel equalization techniques such as Pre-Minimum Mean Square Error (Pre-MMSE) and Pre-Zero Forcing(Pre-ZF) under QPSK and QAM digital modulations. The simulated system deploys three channel coding techniques(1/2-rated Convolutional, CRC and BCH). In the present simulated system, text message transmission has been secured with concatenated implementation of Electronic Codebook (ECB) and Cipher Feedback(CFB) cryptographic algorithm. It is remarked from simulation results that the MIMO OFDM system outperforms with pre-ZF channel equalization,QAM digital modulation and BCH channel coding schemes under fading channels(AWGN and Raleigh).In Pre-MMSE/pre-ZF channel equalization scheme, the system shows comparatively worst performance in convolutional channel coding scheme with QAM/QPSK digital modulation. With increase in noise power as compared to signal power, the system is found to have shown performance deterioration.

KEYWORDS

MIMO-OFDM, Pre-MMSE, Pre-ZF, ECB and CFB cryptographic algorithm, Bit Error rate(BER), AWGN and Raleigh fading channels.

1. INTRODUCTION

Higher data rate supported MIMO technique has become one of the most important paradigms for the deployment of existing and emerging wireless communications systems. The MIMO systems are capable of showing reliable performance as compared to 3G network based communication systems(Universal Mobile Telecommunications System (UMTS) and the High-Speed Downlink Packet Access (HSDPA)).With implementation of MIMO techniques, MIMOOFDM systems have shown increased capacity, coverage and achievable reliability. In many European standards such as Broadband RadioAccess Networks (BRANs),Wireless Local Area Networks (WLANs), Digital Video Broadcasting for Handheld terminals (DVB-H),Digital Video Broadcasting for Terrestrial television (DVB-T) and Digital Audio Broadcasting (DAB), the OFDM has been advocated. High-speed cellular and WLAN standards (i.e., 4G cellular includingWiMAXand LTE, and 802.11a,g,n) have migrated to OFDM, which offers higher spectral efficiency and performance With MIMO signal processing and wider band channels, it becomes possible to increase peak bit rates to the range of 100 Mb/s in both LTE

DOI : 10.5121/ijnsa.2012.4514

andWiMAXsystems. The MIMO based OFDM technologies have been used in WLAN systems to achieve significantly higher bit rates.The 802.11nstandard has a peak bit rate of 300 Mb/s using OFDM with higher order adaptive modulation and MIMO along with multiple channel techniques [1-3].

2. MATHEMATICAL MODEL

In our presently considered secured spatially multiplexed MIMO OFDM wireless communication system, various Pre channel equalization schemes, Electronic Codebook(ECB) and Cipher Feedback(CFB) cryptographic algorithms have been used. A brief description is given below.

2.1. Pre-Channel Equalization

In pre channel equalization scheme, pre equalization is represented by a pre-equalizer weight matrix in complex form($w \in C^{2\times 2}$) and the precoded digitally modulated complex symbol vector ($x \in C^{2\times L}$) can be expressed as

$$x = W\tilde{x} \tag{1}$$

where, L is the length of complex symbol transmitted in each channel, $\tilde{x}$ is the original symbol vector for transmission. In case of zero-forcing (ZF) equalization employment, the corresponding weight matrix (assuming that the channel matrix H issquare) is given as

$$W_{ZF} = \beta H^{-1} \tag{2}$$

whereβ is a constant to meet the total transmitted power constraint after pre-equalization and it is given with two transmitting antenna(N_T=2) as

$$\beta = \sqrt{\frac{N_T}{Tr(H^{-1}(H^{-1})^H)}} \tag{3}$$

To compensate for the effect of amplification by a factor of β at the transmitter, the received signal must be divided by b via automatic gain control (AGC) at the receiver, The received signal y is given by

$$\begin{aligned} y &= \frac{1}{\beta}(HW_{ZF}\tilde{x} + z) \\ &= \frac{1}{\beta}(H\beta H^{-1}\tilde{x} + z) \\ &= \tilde{x} + \frac{1}{\beta}z \\ &= \tilde{x} + \tilde{z} \end{aligned} \tag{4}$$

Other than ZF pre-equalization, MMSE pre-equalization can also be used. In this case, theweight matrix is given as

$$\begin{aligned} W_{MMSE} = \beta \times \underset{w}{\arg\min}\ E\{\|\beta^{-1}(HW\tilde{x} + z) - \tilde{x}\|^2\} \\ = \beta \times H^H(HH^H + \frac{\sigma_z^2}{\sigma_{\tilde{x}}^2}I)^{-1} \end{aligned} \tag{5}$$

Where, the constant β is used again to meet up the total transmitted power constraintafter pre-equalization. It isattributed to the fact that the receiver-side equalization suffers from noise enhancement in thecourse of equalization[4].

2.2. Cryptographic algorithm

Cryptography is synonymous with encryption and used exclusively on providing confidentiality of messages. With the advancement of information technology, agreat emphasis has been given to provide confidentiality, integrity and authentication for secured data transmission. Under Symmetric Key Cryptography, both stream ciphers and block ciphers have been categorized with encrypted data processing of one digit (bit or byte) at a time and fixed-length groups of bits respectively. [6].

In 1977, National Bureau of Standards adopted an acceptable and widely used encryption scheme based on the Data Encryption Standard (DES). The DES scheme is essentially a block cipher technique thatuses certainnumber ofbit blocks. In ElectronicCodebook (ECB) block cipher cryptographic scheme, we have divided the whole message into several blocks of each size 64 bits.Each blockof plaintext is encrypted using the same key of size 64 bits.In Cipher-Feedback (CFB) cryptographic scheme, theinput(whole plaintext)is processed segment wise with64 bitsat a time. Each segmented encrypted plaintext is used as input to produce a pseudorandom output which is processed to undergo XORing operation with segmented plaintext for production of next unit of segmented ciphertext[7].

3. COMMUNICATION SYSTEM MODEL

A simulated single -user 2 × 2 spatially multiplexed MIMO OFDM wireless communication system as depicted in Figure 1 utilizes two pre channel equalization schemes.In such a communication system, the text message is encrypted doubly with concatenation of Electronic Codebook (ECB) and Cipher Feedback (CFB) cryptographic algorithm. The encrypted text message is channel encoded using each of the three channel coding scheme (½-rated convolutional, CRC an BCH) and interleaved for minimization of burst errors. The interleaved bits are digitally modulated using two types of digital modulations such as Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude (QAM**) [8,9].** The complex digitally modulated symbols are spatially multiplexed using Alamouti's space –time block coding (STBC), an efficient transmit diversity scheme [10]**.** The outputs of the Space- time block encoder are sent up into two serial to parallel converter. The serial to parallely (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 Lcp (0.1*1024) containing a copy of the last Lcp 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.

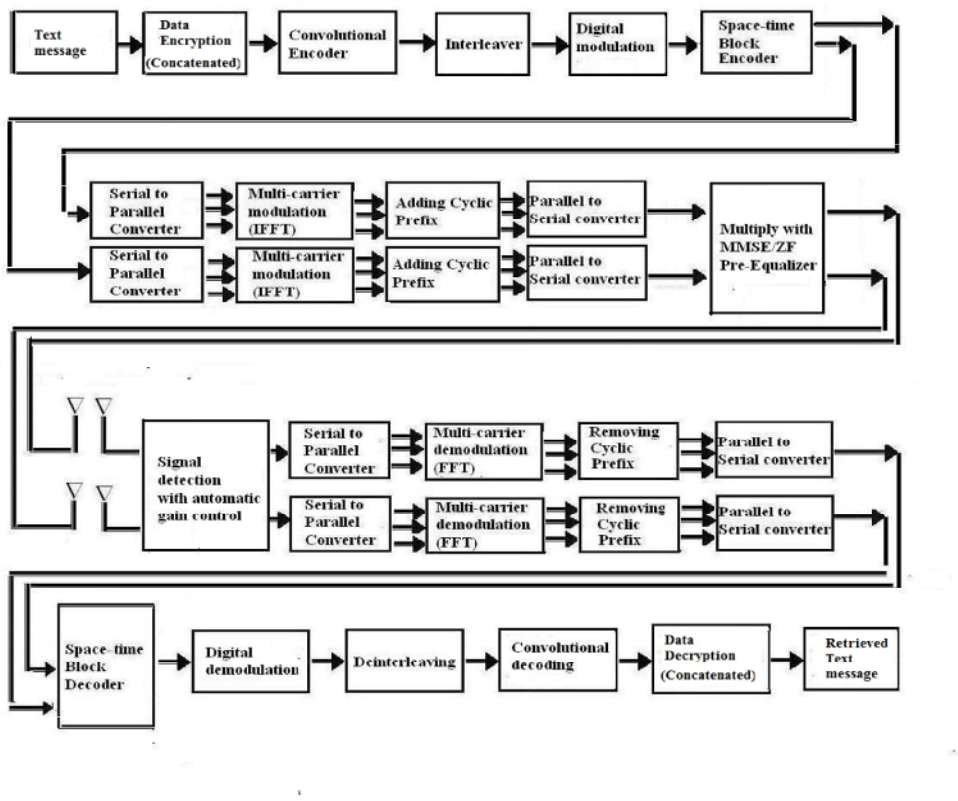

Figure 1: Block diagram of a Pre-Channel Equalization based secured MIMO OFDM wireless communication system.

However, the resulting OFDM symbols of length 1024+ Lcp are weighted with pre equalization channel coefficients prior to lunching from the two transmitting antenna. In case of post channel equalization, no pre-channel equalization operation is performed.However, in receiving section, the signals are detected and passed through automatic gain controlling section to compensate the effect of amplification at the transmitter. 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 in complex symbols are digitally demodulated, deinterleaved, channel decoded and decrypted doubly to recover the transmitted text message.

4. RESULT AND DISCUSSION

The present simulation based study has been made for MIMO OFDM wireless communication system in consideration with various parameters presented in Table 1.

Table 1: Summary of the simulated model parameters

Text message(Converted into bits)	1024
Channel Coding	½-rated Convolutional, CRC and BCH Channel Encoding
Modulation	QPSK and QAM
No of OFDM sub-carriers	1024
Cryptographic algorithm	Electronic Codebook(ECB) and Cipher Feedback(CFB)
Channel Equalization Scheme	Pre-Mean Square error (Pre-MMSE) and Pre-Zero-Forcing (Pre-ZF)
CP length	103 symbols
Channel	AWGN and Rayleigh
Signal to noise ratio, SNR	0 to10 dB

We have conducted computer simulations to observe the impact of pre and post channel equalization schemes on the BER performance of the secured MIMO OFDM wireless communication system based on the parameters given in Table 1. It is assumed that the channel state information (CSI) is available at the transmitter side and the fading process is approximately constant during one OFDM block length.

The graphical illustrations presented in Figure 2 through Figure 5 show system performance comparison with implementation of pre-MMSE and pre-ZF based Channel equalization schemes under QPSK and QAM digital modulations. In all cases, it is noticeable that Pre-ZF based channel equalization with BCH channel coding schemes improves the system performance. In Figure 2, it is observable that the system performance is well discriminable less than three different channel coding schemes. For a typically assumed SNR value of 2 dB, the BER values are 0.4609 and 0.2485 in case of Convolutional and BCH channel coding schemes under QPSK and Pre-MMSE and viz., the system achieves a gain of 2.68 dB in BCH as compared to ½-rated Convolutional. The system shows well defined performance over a large examined SNR values under the situation of three channel coding schemes and QAM and Pre-MMSE (Figure 3). At a SNR value of 2 dB, the system performance is improved by 3.15dB for BER values of 0.1673 and 0.3454 in case of BCH as compared to ½-rated Convolutional.

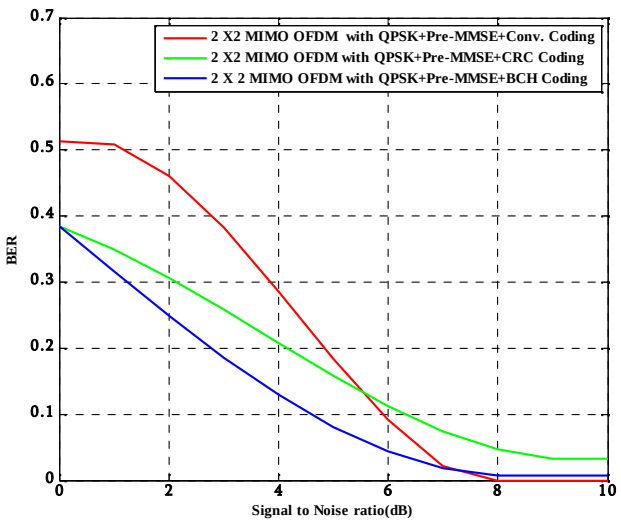

Figure 2 : BER Performance of a secured MIMO OFDM wireless communication with implementation of different Channel coding, Pre-MMSE channel equalization and QPSK digital modulation schemes.

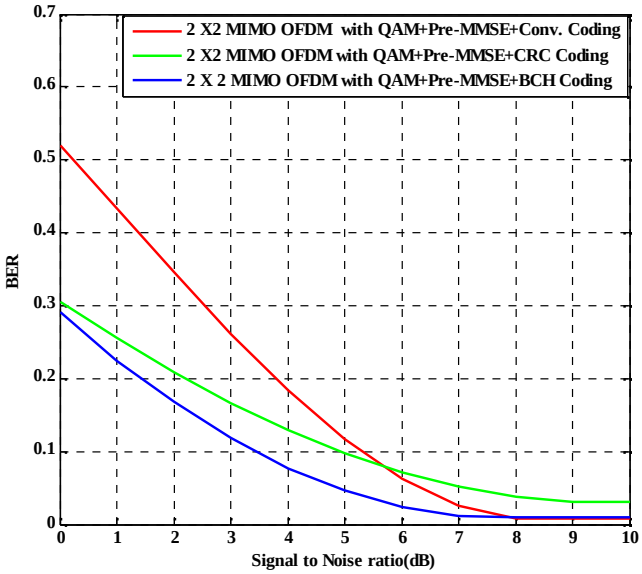

Figure 3 : BER Performance of a secured MIMO OFDM wireless communication with implementation of different Channel coding, Pre-MMSE channel equalization and QAM digital modulation schemes.

In Figure 4, and Figure 5, it is observable that the rate of system performance improvement with increase in SNR values. is comparatively higher in Convolutional coding as compared to CRC and BCH. In Figure 4 and Figure 5, the system performance improvement is found to have values of 2.76dB (BERs: 0.2363 and 0.4461) and 3.40dB(BERs: 0.1565 and 0.3425) at a typically assumed SNR value of 2 dB in case of most satisfactory and worst system performance.

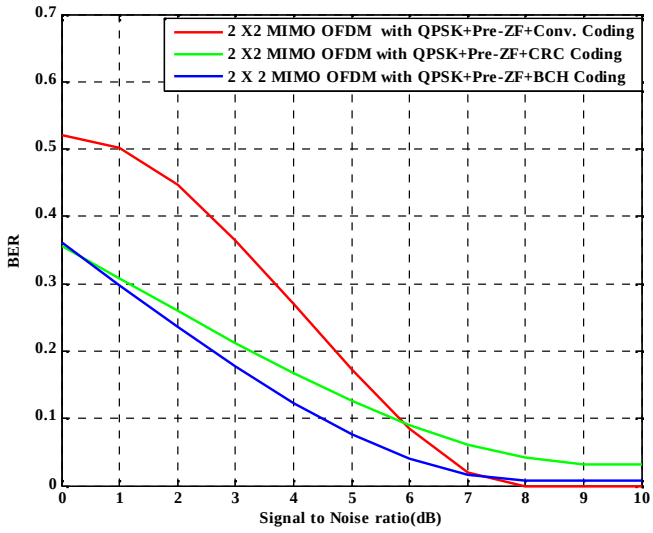

Figure 4 : BER Performance of a secured MIMO OFDM wireless communication with implementation of different Channel coding, Pre-ZF channel equalization and QPSK digital modulation schemes.

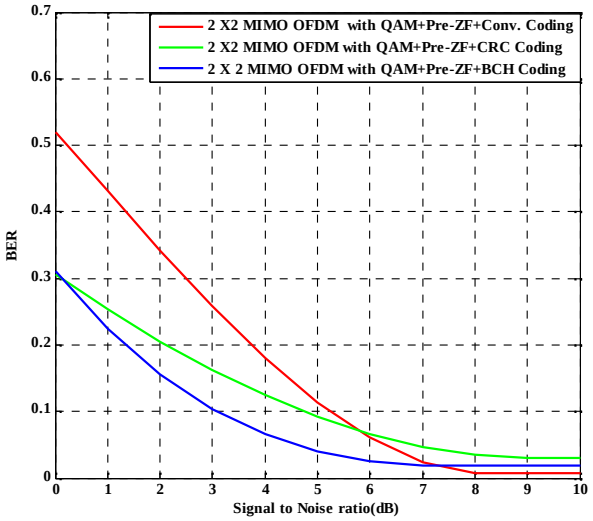

Figure 5 : BER Performance of a secured MIMO OFDM wireless communication with implementation of different Channel coding, Pre-ZF channel equalization and QAM digital modulation schemes.

In Figure 6, a BER comparison has been made for the system in identical channel coding and different digital modulation and pre-channel equalization schemes. It is remarkable that over a significant SNR value area, the system shows quite satisfactory performance in QAM, Pre-ZF and BCH schemes. Under identical implementation of channel coding(BCH) scheme, the system shows worst performance in QPSK and Pre-MMSE. A system performance improvement of 2.01 dB is achieved at SNR value of 2dB in QAM, Pre-ZF and BCH schemes as compared to QAM, Pre-MMSE and BCH(BERs: 0.1565 and 0.2485).

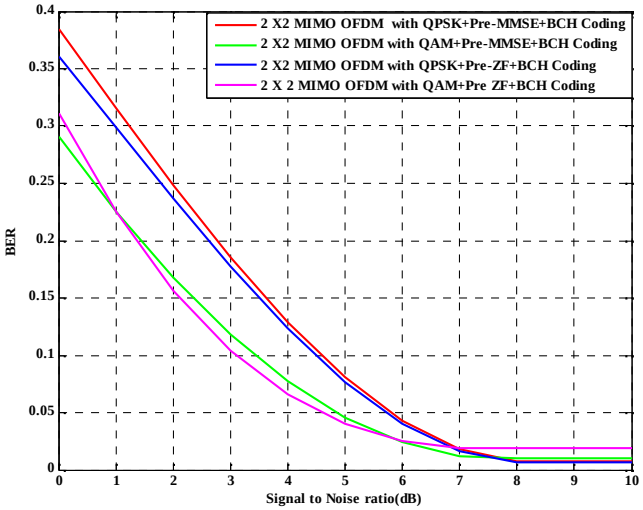

Figure 6: BER Performance Comparison of the MIMO OFDM wireless communication system for different Pre channel equalization and digital modulation schemes under BCH channel coding scheme.

In Figure 7, the transmitted, doubly encrypted and retrieved text messages at 4dB and 6dB have been presented under implementation of QAM, Pre-ZF and BCH channel coding schemes. The estimated BER values are found to have values of 0.0166 and 0.000.

Multiple-input multiple-output systems have attracted considerable attention due to the linear growth of the system capacity.

(a)

_Íjz¶9ãx ¼Bù_Á¨ùN£|×óù >nq½a ydy(_ôj?¬ sùêüß) b É6õ19êxß 7ÙA¢ Ïj • u&êZ yQØÀa_jò°,êZßIV+ $#`?o ð×B\·

(b)

Multiple-input multipLeoõôx}ô óystems have attracted considerable attention due to the linear growth of the system0s1`!cmpy.

(c)

Multiple-input multiple-output systems have attracted considerable attention due to the linear growth of the system capacity.

(d)

Figure 7 : Presented text message in various forms in a MIMO OFDM wireless communication system , (a) Transmitted, (b) Doubly Encrypted (c) Retrieved message at 4 dB(d) Retrieved message at 6 dB. Red marks indicate noise contamination.

5. CONCLUSIONS

In this paper, we made a comprehensive study to enhance be performance for MIMO OFDM wireless communication system. The simulation results, which are based on MATLAB show that under implementation of Pre-ZF channel equalization with BCH channel coding scheme the simulated system with QAM digital modulation has a better performance compared to other channel equalization, channel coding and digital modulation schemes. The results presented can be taken into consideration to propose a robust and reliable multi antenna supported OFDM wireless communication system.

REFERENCES

[1] LajosHanzo, YosefAkhtman, Li Wang and Ming Jiang, (2011)" MIMO-OFDM for LTE, Wi-Fi and WiMAX , Coherent versus Non-coherent and Cooperative Turbo-transceivers", John Wiley and Sons, Ltd, United Kingdom.

[2] DipankarRaychaudhuriand Narayan B. Mandayam ,(2012) " Frontiers of Wireless and Mobile Communications" , Proceedings of the IEEE vol. 100, no. 4, pp. 828-840.

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

[4] Yong Soo Cho, Jaekwon Kim, Won Young Yang, Chung G. Kang, (2010) "MIMO-OFDM Wireless Communications with MATLAB", John Wiley and Sons (Asia) Pte Limited, Singapore.

[5] Lin BaiandJinho Choi, (2012) "Low Complexity MIMO Detection", Springer Science and Business Media, LLC ,New York, USA

[6] Alan Holt and Chi-Yu Huang, (2010) "802.11 Wireless Networks Security and Analysis", Springer-Verlag London Limited, New York.

[7] William Stallings, (2005)"Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall Publisher.

[8] Theodore S Rappaport,(2001)"Wireless Communications: Principles and Practice," Second Edition, Prentice Hall, Upper Saddle River, New Jersey, USA

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

[10] 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

Bibliography

LailaNaznin joined as a Lecturer in the Department of Information and Communication Engineering, Faculty of Engineering, University of Rajshahi, Rajshahi, Bangladesh in 2006. She received her B.Sc. (Hons) and M.Sc. degree from the Department of Applied Physics and Electronic Engineering, University of Rajshahi, Bangladesh in 1999 and 2000 respectively. She is now working as an Assistant Professor of the Department of Information and Communication Engineering, University of Rajshahi. Her research interests include advanced wireless communications with special emphasis on MIMO OFDM/OFDMA and MCCDMA radio interface technologies.

Shahrina Sultana is a postgraduate student of the Department of Information and Communication Engineering, Faculty of Engineering, University of Rajshahi, Rajshahi ,Bangladesh. She received her B.Sc. (Hons) degree in Information and Communication Engineering from university of Rajshahi in 2011.During her undergraduate study, Ms. Sultana completed a project work on Performance evaluative study of a Mobile WiMAX wireless Communication system under supervision of Dr.ShaikhEnayetUllah, Ex. Professor and Chairman, Department of Information and Communication Engineering, University of Rajshahi.Her main research interests include Channel Equalization, Space Time Block Coding, MISO/MIMO-OFDM and 4G compatible MC-CDMA radio interface technology.

Md. GolamRashed is a Lecturer of the Department of Information and Communication Engineering, Faculty of Engineering, University of Rajshahi, Rajshahi, Bangladesh. He received his B.Sc. (Hons) and M.Sc. degree from the Department of Information and Communication Engineering, University of Rajshahi, Bangladesh in 2006 and 2007 respectively. He worked as a Lecturer of the Department of Electronics and Telecommunication Engineering, Prime University, Dhaka, Bangladesh in 2010-2011. In 2009, he was awarded a research fellowship under the Ministry of Science, Information and Communication Technology, People's Republic of Bangladesh and conducted research work in Wireless Sensor Networking . His research interests include advanced wireless communication, Ad-hoc networking. He has a significant number of publications in international referred journals.

ShaikhEnayetUllah 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 55 articles in multidisciplinary fields. His main research interests include Cooperative communications, MIMO-OFDM, WiMAX, Cognitive radio and LTE radio interface technologies.