# Encrypted Data Transmission in a Multiuser MIMO OFDMA Wireless Communication System with Implementation of Pre-RSNA Cryptographic Algorithm

Tanjina Afrin and Shaikh Enayet Ullah

*Department of Applied Physics and Electronic Engineering*
*Rajshahi University*
*Rajshahi-6205, Bangladesh*
*ta.tinni@yahoo.com, enayet67@yahoo.com*

***Abstract***

*This paper incorporates a comprehensive BER simulation study undertaken on the effectiveness of a multi-user MIMO OFDMA wireless communication system on encrypted data transmission. The channel encoded and spatially multiplexed multi-user MIMO OFDMA system under investigation implements Pre-RSNA cryptographic algorithm. The simulated system deploys three linear signal detection schemes (Equalizers) such as Minimum Mean Square Error (MMSE), Zero Forcing (ZF) and Q-Less QR decomposition under BPSK, DPSK, QPSK and QAM digital modulations. It is anticipated from computer simulation tests with synthetic data transmission that the multi antenna supported OFDMA wireless communication system outperforms in Zero Forcing (ZF) channel equalization scheme with BPSK digital modulation and shows comparatively worst performance in Q-Less QR channel equalization scheme.*

***Keywords:*** *MIMO-OFDMA, Pre-RSNA, Signal detection scheme, Bit error rate, AWGN and Rayleigh Fading channel*

## 1. Introduction

The OFDMA is one of the most useful approaches in the mobile cellular system. The OFDMA system assigns a subset of subcarriers (not all subcarriers in each OFDM symbol) to each user, where the number of subcarriers for a specific user can be adaptively varied in each frame. The OFDMA based cellular system suffers from inter-cell interference at the cell boundary in specific situation of fully frequency channel utilization. In such undesirable situation, the performance of the OFDMA cellular system at the cell boundary can be improved with consideration of the concept of fractional frequency reuse (FFR). The OFDMA is used in scalable IEEE 802.16 standard based Wireless MAN network. The scalable OFDMA (S-OFDMA) architecture supports a wide range of bandwidth, which spans from 1.25 to 20MHz combined with fixed subcarrier spacing for both fixed and portable/mobile uses. WiMAX technology is based on the S-OFDMA air interface designed for achieving high spectral efficiency and data rates [1, 2].

Multiple Input Multiple Output (MIMO) technologies are nowadays being used in the major cellular and wireless standards such as LTE, and the IEEE 802.11 family. Basically all cellular systems or Wireless Local Area Networks (WLANs) can be seen as multi-user systems. The LTE and LTE-Advanced represent the recent efforts of the 3rd Generation Partnership Project (3GPP) to define the evolution of cellular communications beyond 3rd Generation (3G) CDMA-based technology, The LTE advanced system employs MIMO-

OFDMA in the downlink and Single Carrier Frequency Division Multiple Access (SC-FDMA) in the uplink. The MIMO-OFDM systems can achieve high data-rates, are robust to the effects of multipath fading and have low complexity equalizer implementations. OFDMA-based multiple access results in a high degree of orthogonality between the signals at the receiver associated with different users within the cell [3, 4].

## 2. Mathematical Model

In our presently considered spatially multiplexed MIMO OFDMA wireless communication system, pre-RSNA algorithm, convolutional coding and various signal detection schemes have been implemented. A brief description is given below.

### 2.1. Pre-RSNA

Pre-RSNA algorithms originated from WEP which first appeared in the 802.11b amendment. WEP was introduced for the purpose of providing confidentiality, integrity and authentication. The RC4 stream cipher from RSA Security Inc. is used for confidentiality (encryption). A 32-bit cyclic redundancy check (CRC) is used for data integrity. WEP, and shared key authentication methods are still in wide-spread use.

An integrity check value (ICV) is computed for each frame (M). The ICV is a 32-bit CRC and thus a plaintext frame M yields ICV =$CRC_{32}$ (M). The ICV is appended to a plaintext packet M to form P = M|ICV (where | denotes concatenation). A key stream is generated using a pseudo-random number generator (PRNG) from the WEP key $K_{WEP}$ and a 24-bit initialization vector (IV). A new IV is used for each frame (though IVs are reused every $24^2$ frames). The IV is prepended to K to form a per-frame key, K =IV|$K_{WEP}$. P is then encrypted using the RC4 cipher. The cipher text message C is derived by XOR ing the per-frame key K with P:

C =P $\oplus$K **[5].**

### 2.2. Spatially Multiplexed MIMO System

Spatially multiplexed MIMO (SM-MIMO) systems can transmit data at a higher speed than a MIMO systems using antenna diversity technique. Spatial de-multiplexing or signal detection at the receiver side is a challenging task for SM-MIMO system. In a typically assumed $N_R \times N_T$ MIMO system, let us consider that H denotes a channel matrix with it (**j,i**)th entry $h_{ij}$ for the channel gain between the ith transmit antenna and the jth receive antenna, **j=1,2, . . . . . ,**$N_R$and **i=1,2, . . . . . ,**$N_T$**.** The spatially-multiplexed user data and the corresponding received signals are represented by $x = [x_1, x_2, \ldots, x_{N_T}]^T$ and $y = [y_1, y_2, \ldots, y_{N_R}]^T$, respectively, where $x_i$ and $y_j$ denote the transmit signal from the ith transmit antenna and the received signal at the jth receive antenna, respectively. Let $z_j$ denote the white Gaussian noise with a variance of $\sigma_z^2$ at the jth receive antenna and $h_i$ denotes the ith column vector of the channel matrix **H**. Now the $N_R \times N_T$MIMO system is represented as

$$y = Hx + z$$

$$= h_1x_1 + h_2x_2 + \ldots\ldots + h_{N_T}x_{N_T} + z \qquad \textbf{(1)}$$

Where,$z = [z_1, z_2, \ldots\ldots, z_{N_R}]^T$.

### 2.3. Signal Detection Schemes

The Zero Forcing technique nullifies the interference by the following weight matrix:

$$W_{ZF} = (H^H H)^{-1} H^H \quad (2)$$

where $(.)^H$ denotes the Hermitian transpose operation. In other words, it inverts the effect of channel as

$$\tilde{x}_{ZF} = W_{ZF} y$$
$$= x + (H^H H)^{-1} H^H z \quad (3)$$

In order to maximize the post-detection signal-to-interference plus noise ratio(SNR), the MMSE weight matrix is given as

$$W_{MMSE} = (H^H H + \sigma_z^2 I)^{-1} H^H \quad (4)$$

and the detected desired signal from the transmitting antenna is given by**[6]**

$$\tilde{x}_{MMSE} = W_{MMSE} y$$

With Q-less QR Decomposition scheme, the detected desired signal $\tilde{\mathbf{x}}$ from the transmitting antenna can be found based on the least squares approximate solution to $\tilde{\mathbf{H}} * \tilde{\mathbf{x}} = \tilde{\mathbf{y}}$ where, $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{y}}$ are the channel matrix and received signal respectively. From $\tilde{\mathbf{H}}$ channel matrix, an upper triangular matrix $\tilde{\mathbf{R}}$ of the same dimension as $\tilde{\mathbf{H}}$ is estimated and using the following steps, the detected desired signal $\tilde{\mathbf{x}}$ is computed [7].

$$\tilde{\mathbf{x}} = \tilde{\mathbf{R}} \setminus (\tilde{\mathbf{R}}^{\mathbf{H}} \setminus (\tilde{\mathbf{H}}^{\mathbf{H}} * \tilde{\mathbf{y}}))$$
$$\tilde{\mathbf{r}} = \tilde{\mathbf{y}} - \tilde{\mathbf{H}} * \tilde{\mathbf{x}}$$
$$\tilde{\mathbf{e}} = \tilde{\mathbf{R}} \setminus (\tilde{\mathbf{R}}^{\mathbf{H}} \setminus (\tilde{\mathbf{H}}^{\mathbf{H}} * \tilde{\mathbf{r}}))$$
$$\tilde{\mathbf{x}} = \tilde{\mathbf{x}} + \tilde{\mathbf{e}} \quad (5)$$

## 3. Communication System Model

A simulated multi -user 2 x 2 spatially multiplexed and FEC encoded OFDMA wireless communication system is depicted in Figure 1. In such a communication system, four users are simultaneously transmitting their data in the form of text message/synthetically generated binary bit stream. Primarily, the input data of each user is processed for encryption with a robust pre-RSNA encryption algorithm. The encrypted data are converted into binary bits and

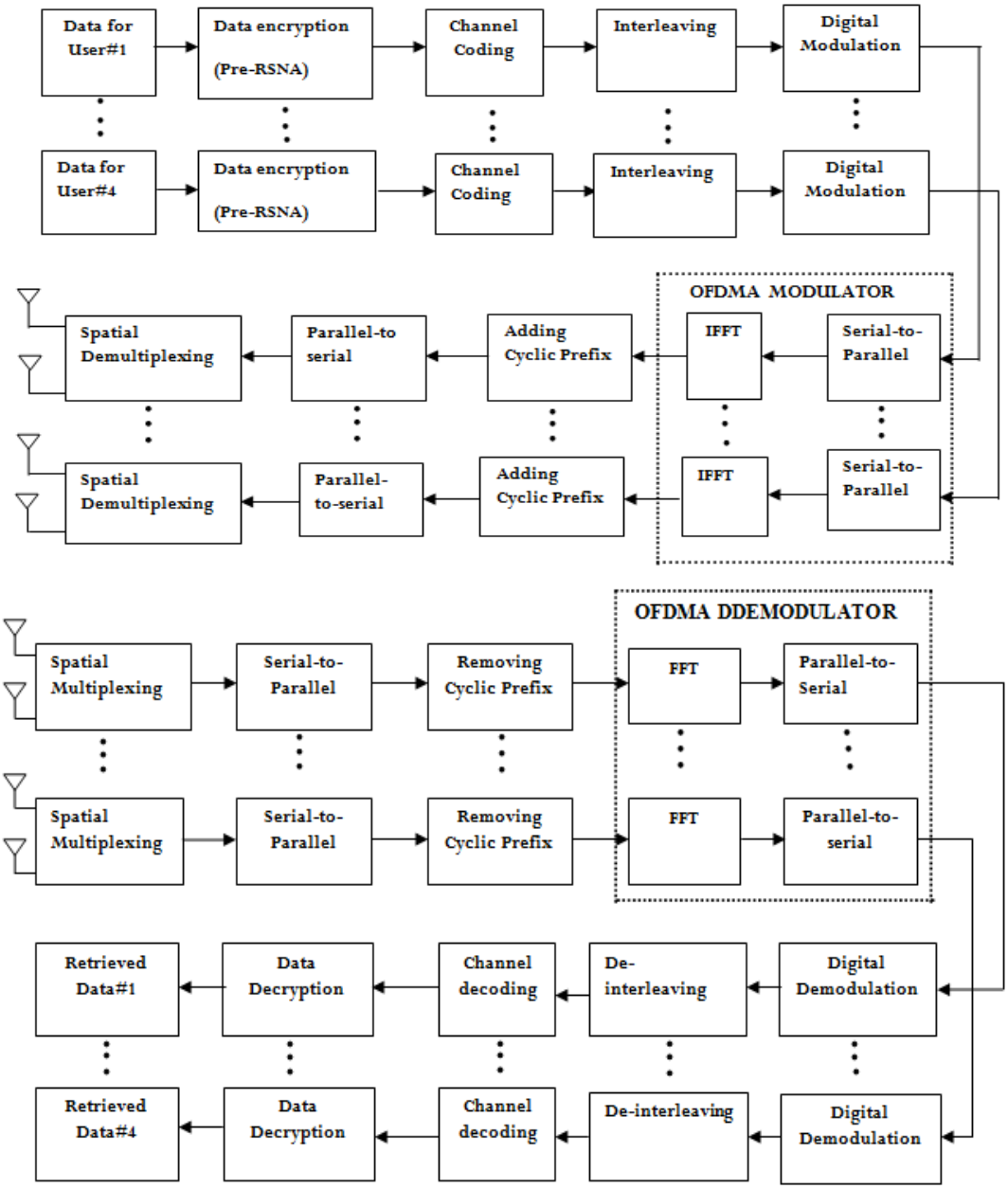


**Figure 1. Block Diagram of a Multi User MIMO OFDMA Wireless Communication System**

channel encoded using ½-rated convolutionally encoding schemes and interleaved for minimization of burst errors. The interleaved and channel encoded bits are digitally modulated using BPSK, DPSK, QAM and QPSK [8]. In each OFDMA section assigned for each user, the interleaved digitally modulated symbols are serial to parallelly converted and fed into IFFT section where modulation is performed utilizing all subcarriers in a OFDM block on TDMA basis viz. each OFDM block for a time slot is assigned to a single user subsequently. The modulated complex symbols are cyclically prefixed for minimizing inter symbol interference (ISI). It is then converted from parallel to serial and multiplexed

spatially. The spatially demultiplexed complex signals are transmitted from each of the two transmitting antennas. In receiving section, the transmitted signals are detected using channel equalization schemes. The detected signal for each user is passed through spatial multiplexer and its output is serial to parallely converted with removal of cyclic prefixing. The processed signals are now sent to FFT section where demodulation occurs resulting in production of an output which is parallel to serially converted and processed for digital demodulation, deinterleaving and channel decoding. The processed signal is sent up for performing decryption operation. Eventually, the transmitted text message / synthetic binary bit stream of each user is retrieved.

## 4. Results and Discussion

In this section, results of computer simulations using Matlab for the 2 ×2 multi user MIMO OFDMA wireless communication system have been presented. The study is based on considering the parameters presented in Table 1 and availability of channel state information (CSI) at the transmitter side and the fading process is approximately constant during each transmitted signal. The graphical illustrations of Figure 2 through Figure 4 confirm that system outperforms in low order digital modulation, BPSK. In Figure 2, it is noticeable that the system shows worst performance in QPSK with MMSE signal detection technique. For a typically assumed SNR value of 3 dB, the BER values are 0.0889 and 0.4286 in case of BPSK and QPSK viz. the system performance is improved by 6.83 dB. In Figure 2, it is also seen that at 10% BER, the simulated system achieves

**Table 1. Summary of the Simulated Model Parameters**

| Parameters | Types |
|---|---|
| Input Data | synthetically generated binary bits |
| Modulation | BPSK,DPSK,QPSK and QAM |
| SNR | 0-10 dB |
| Signal detector(Equalizer) | ZF, MMSE and Q-Less QR decomposition |
| Channel | AWGN and Rayleigh fading |
| Cryptographic algorithm | Pre-RSNA |
| Antenna Configuration(each user) | 2 x 2 |

A SNR gain of 5.2dB in BPSK as compared to QPSK. In Figure 3, the system shows worst performance in QAM with Q-Less QR Detection aided signal detection technique. For a SNR value of 3dB, the BER values for BPSK and QAM are 0.2201 and 0.4846 respectively which is indicative of system performance improvement by 3.42 dB. In Figure 3, it is also observable that at low SNR value region, the system shows non appreciable change in BER performance for DPSK and QAM digital modulations. In Figure 4, it has been found at 3dB SNR value that the estimated BER values are 0.0054 and 0.2591 in case of BPSK and QPSK with a system performance improvement of 16.81 dB under ZF signal detection technique. In Figure 5, it is noticeable that at 0 dB SNR value viz. at the critical situation when signal power and noise power are identical, the transmitted bits are not properly retrieved. In Figure 6, it is found that at a comparatively favorable situation with 6dB SNR value, the transmitted bits are fairly retrieved. In Figure 7, estimated power spectral density of the binary data in transmitted, encrypted and retrieved form for the user #1 has been presented merely to get a comprehensive idea on processing operation performed in the simulated system. It is also observable from the Figure 7 that the graphical illustrations presented in case of transmitted and retrieved binary data at 6dB SNR value are highly resemblance to each other. On the other hand, the encrypted form is quite different.

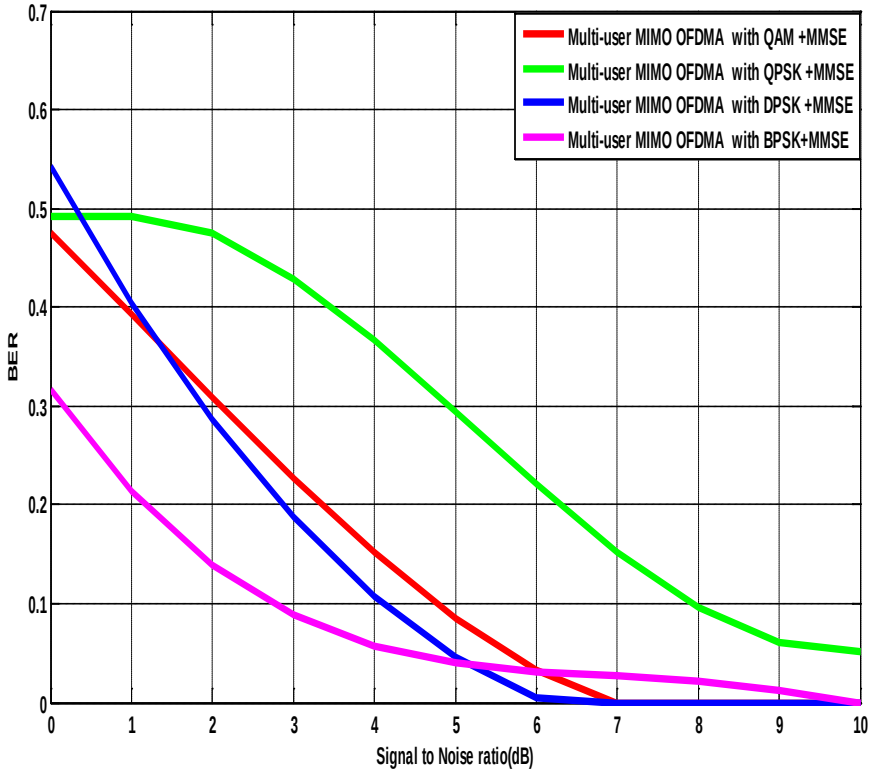


**Figure 2: BER Performance Comparison of Multiuser MIMO OFDMA Wireless Communication System with MMSE Channel Equalization and Various Digital Modulation Schemes**

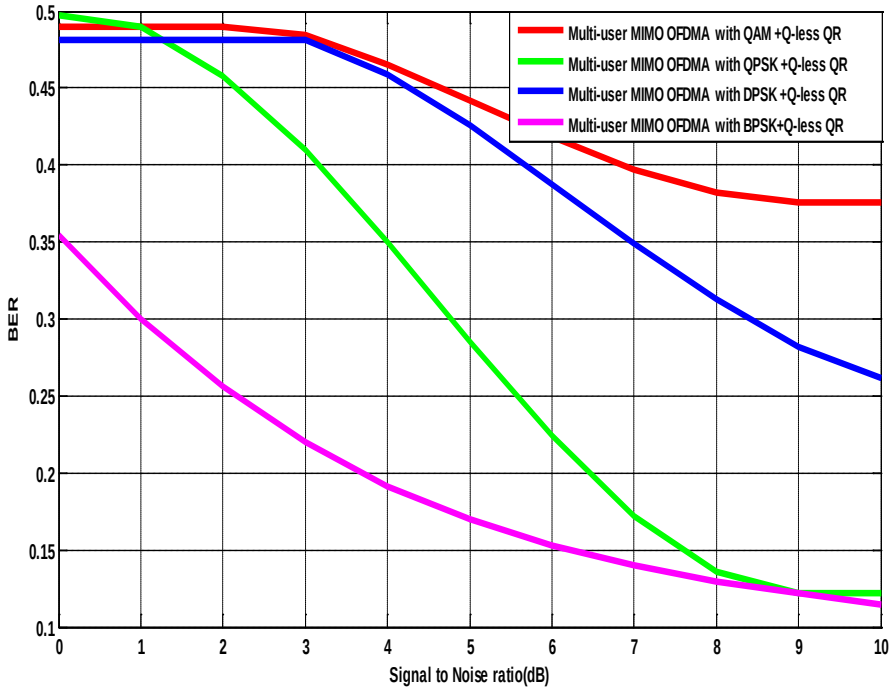


**Figure 3. BER Performance Comparison of Multiuser MIMO OFDMA Wireless Communication System with Q-Less QR Decomposition Aided Channel Equalization and Various Digital Modulation Schemes**

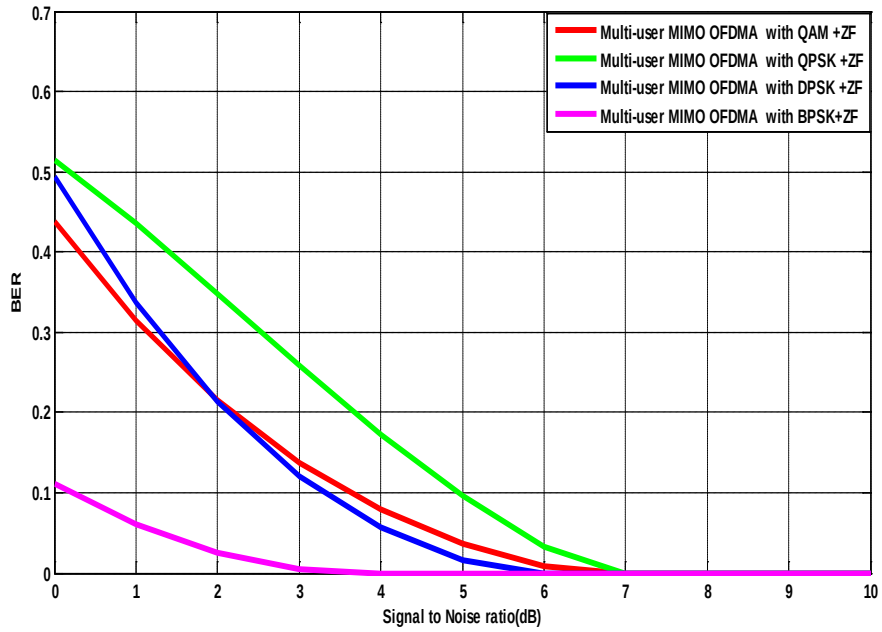


**Figure 4: BER Performance Comparison of Multiuser MIMO OFDMA Wireless Communication System with ZF Channel Equalization and Various Digital Modulation Schemes**

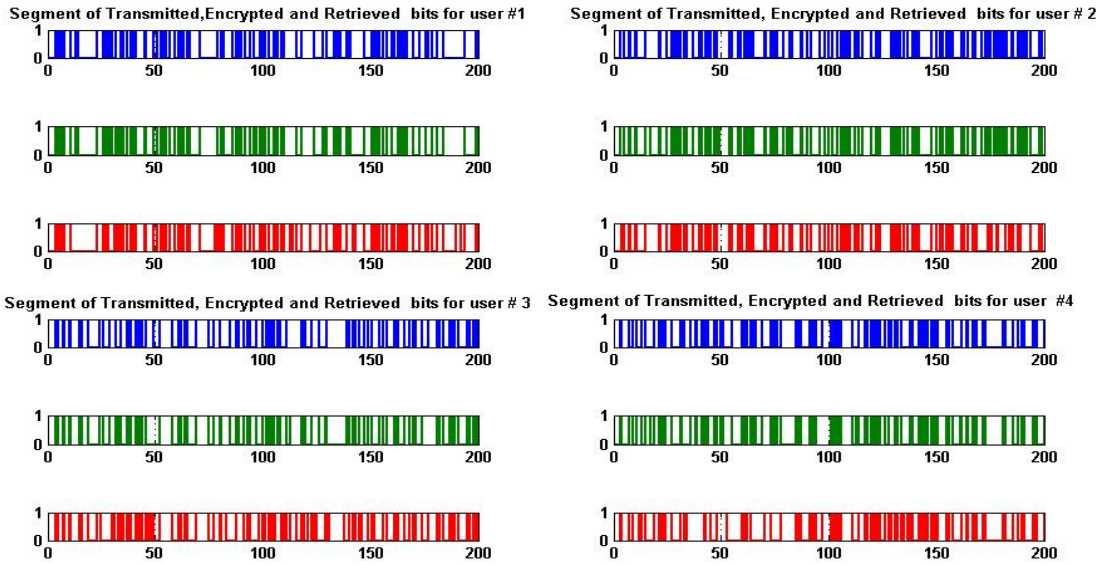


**Figure 5. Transmitted(Blue), Encrypted(Green) and Retrieved(Red) Binary Data at 0 dB SNR in multiuser MIMO OFDMA Wireless Communication System using Zero-forcing Channel Equalization and BPSK Digital Modulation Schemes**

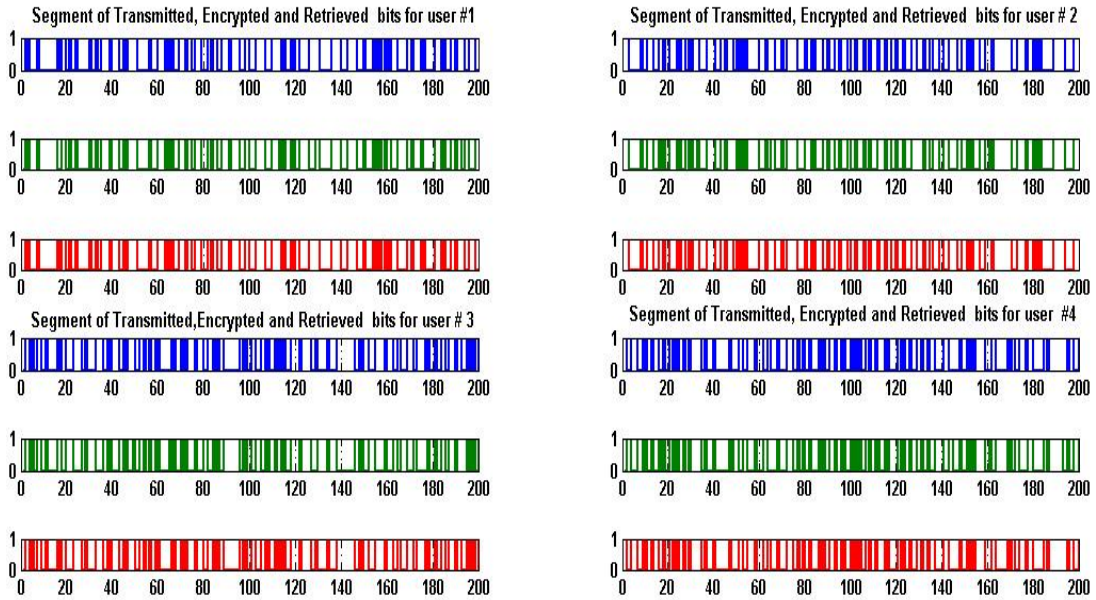


**Figure 6. Transmitted (Blue), Encrypted(Green) and Retrieved(Red) Binary Data at 6 dB SNR in Multiuser MIMO OFDMA Wireless Communication System using Zero-forcing Channel Equalization and BPSK Digital Modulation Schemes**

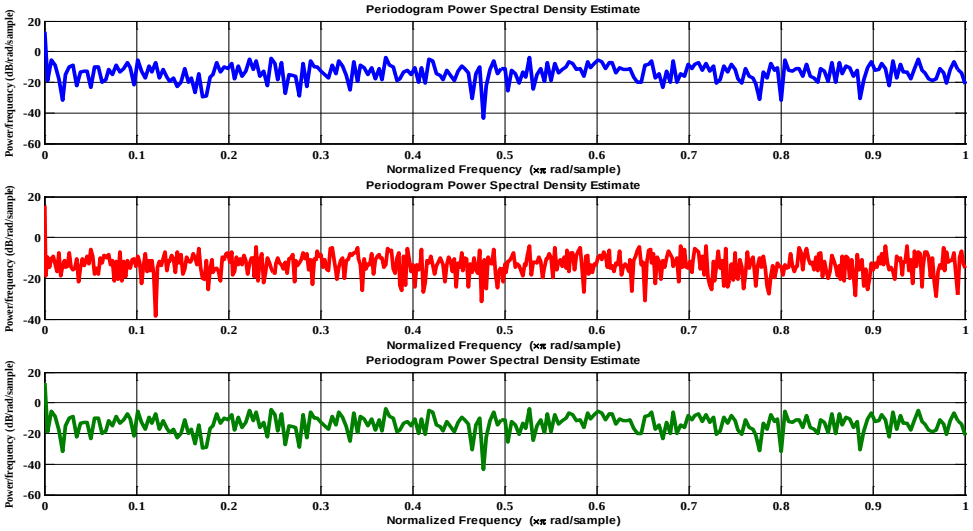


**Figure 7. Estimated Power Spectral Density of Transmitted(blue), Encrypted(Red) and Retrieved(Blue) Binary Data at 6dB SNR for user #1**

## 5. Conclusion

In this paper an effort has been taken to make performance evaluative study of a multiuser MIMO OFDMA wireless communication system under various channel equalization and digital modulation schemes. From the simulated results, it can be concluded that the convolutionally encoded multiuser MIMO OFDMA wireless communication system provides quite satisfactory performance under Zero Forcing channel equalization and low order digital modulation BPSK. The OFDMA has been adopted in the downlink communication for 4G LTE-Advanced system. It is expected that such OFDMA radio interface technology would be effectively implemented in multi antenna supported future generation wireless communication system

## References

[1] Y. Soo Cho, J. Kim, W. Young Yang and C. G. Kang, "MIMO-OFDM Wireless Communications with Matlab", John Wiley and Sons (Asia) Pte Limited, Singapore, **(2010)**.

[2] L. Hanzo, Y. (Jos) Akhtman, L. Wang and M. Jiang, "MIMO-OFDM for LTE, Wi-Fi and WiMAX", John Wiley and Sons Ltd, United Kingdom, **(2011)**.

[3] G. de la Roche, A. Alay´on Glazunov and B. Allen, "LTE-advanced and next generation wireless networks Channel modelling and propagation", John Wiley and Sons, Limited publishing Company, United Kingdom, **(2013)**.

[4] A. Sibille, C. Oestges and A. Zanella, "MIMO From Theory to Implementation", Elsevier Inc., United Kingdom, **(2011)**.

[5] A. Holt and C.-Y. Huang, "802.11 Wireless Networks Security and Analysis", Springer-Verlag London Limited, New York, **(2010)**.

[6] Y. Soo Cho, J. Kim, W. Young Yang and C. G. Kang, "MIMO-OFDM Wireless Communications with Matlab", John Wiley and Sons (Asia) Pte Limited, Singapore, **(2010)**.

[7] S. T. Karris, "Numerical Analysis Using MATLAB and Spreadsheets", Second Edition, Orchard Publications, California, USA, **(2004)**.

[8] T. S. Rappaport, "Wireless communications: Principles and Practices", Second Edition, Prentice Hall Inc., New Jersey, USA, **(2004)**.

# Authors

**Tanjina Afrin** received her B.Sc. (Hons.) and M.Sc. degree both in Applied Physics and Electronic Engineering department from University of Rajshahi, Bangladesh in 2010 and 2011 respectively. During her post graduate study, she has completed a research work on multi user MIMO OFDMA Wireless Communication System. Her research interest includes Channel Equalization, MIMO technology, Radio Interface technologies (OFDM, MCCDMA and LTE).

**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.