Secure Color Image Transmission in a Downlink JP-COMP Based MIMO-OFDM Wireless Communication System

Joarder Jafor Sadique¹ and Shaikh Enayet Ullah²

1. Department of Electronics and Telecommunication Engineering, Begum Rokeya University, Rangpur 5400, Bangladesh
2. Department of Applied Physics and Electronic Engineering, Rajshahi University, Rajshahi 6205, Bangladesh

Corresponding author: Joarder Jafor Sadique (joarderjafor@yahoo.com)

Abstract: In this paper, we made a comprehensive BER (bit error rate) performance simulative study on secure color image transmission in a joint processing-coordinated multipoint aided MIMO-OFDM (multiple input multiple output-orthogonal frequency division multiplexing) wireless communication system. The multi antenna supported system under investigation implements Block cipher encryption aided and ½-rated Convolutional channel encoding; MMSE (minimum mean square error) and ZF-SIC (zero forcing-successive interference cancellation) signal detection (Equalizers) schemes under QAM (quadrature amplitude modulation), QPSK (quadrature phase shift keying) and DQPSK (differential quadrature phase shift keying) digital modulations. Based on the simulation result with MATLAB, it is quite noticeable that the simulated system is highly robust in retrieving transmitted color image under Rayleigh fading channel in QAM digital modulation and ZF-SIC channel equalization technique with Block cipher encryption based channel coding scheme.

Key words: CoMP (coordinated multiple point transmission and reception), channel coding, linear signal detection technique, BER (bit error rate), AWGN (additive white gaussian noise) and Rayleigh fading channels.

1. Introduction

With the aim of fully implementing the concept of “anywhere” and “anytime well as to support new and emergent services, LTE-Advanced (long term evolution) was initially specified in release 10 of 3GPP and improved in its release 11 and 12 to meet up key user requirements in perspective of increasing throughputs and bandwidths, enhanced spectrum efficiency, lower delays, and network capacity. The LTE-advanced consists of a 4G (fourth-generation cellular system), being expected to be fully implemented in this year 2014. It aims to support peak data rates in the range of 100 Mbps for vehicular mobility to 1 Gbps for nomadic access (in both indoor and outdoor environments). 4G aims to support current and emergent multimedia services, such as social networks and gaming, mobile TV, HDTV (high-definition television), DVB (digital video broadcast), MMS (multimedia messaging service), or video chat, using the all-over IP concept and with improved QoS (quality of service). The LTE comprises an air interface based on OFDMA (orthogonal frequency division multiple access) in the downlink and SC-FDMA (single carrier-frequency division multiple access) in the uplink. This allows a spectral efficiency improvement by a factor of 2-4, as compared to the HSPA (high-speed packet access), making use of new spectrum, different transmission bandwidths from 1.4 MHz up to 20 MHz, along with MIMO (multiple-input-multiple-output) systems and the all-over IP architecture [1].

In multiuser MIMO communication systems, wireless
Secure Color Image Transmission in a Downlink JP-COMP Based MIMO-OFDM Wireless Communication System

resources like spectrum and power are shared to enable communication between centralized communication terminals (e.g., BSs, access points, etc.) and multiple user terminals (e.g., phones, laptops). Additionally, several access techniques such as FDMA (frequency division multiple access), TDMA (time division multiple access), CDMA (code division multiple access), and OFDMA (orthogonal frequency division multiple access) are being used in such systems [2]. With development of physical layer techniques, the data rates of mobile communication services have increased by about 100 times every 6-7 years and it is predicted that in 2020, the required data rate will be as large as 100-1000 times, the currently served data rate. Due to the recent breakthrough in transmission technologies with consideration of constraints of traditional cellular systems in terms of transmit power, complicacy in frequency of handover in high speed mobile environment (350 km/h) and cell edge effect for transmission frequencies higher than 2 GHz, cellular communications have entered the era of cooperative communications. In Cooperative communication system, various types of cooperative schemes such as relay, DAS (distributed antenna system), multicellular coordination, group cell, CoMP (coordinated multiple point) transmission and reception are used [3].

The present work focuses on the performance evaluative study of multi antenna supported system under implementation of coordinated multiple point transmission and reception and orthogonal frequency division multiplexing schemes. A scenario of downlink coordinated multiple point transmission is presented in Fig. 1.

The structure of this paper is arranged as follows: Section 2 will provide a comprehensive idea on various signal processing schemes such as image encryption, Block cipher encryption aided channel coding for redundant bit addition, multicarrier modulation and transmitted signal detection; In Section 3, we analyzed performance of a simulated JP-COMP based wireless communication system under scenario of various implemented channel coding, low order digital modulation and signal detection schemes; Finally, conclusions are given in Section 4.

2. Signal Processing

We assume that a RGB color image, D contains 96 \times 96 \times 3 array of color pixels with pixel values in the range [0, 255] and D_{red}, D_{green} and D_{blue} are the three 96 \times 96 sized color image components. Another synthetically generated 96 \times 96 \times 3 sized matrix, K is used as a key and its three 96 \times 96 sized matrix components are K_{red}, K_{green} and K_{blue}, respectively. Each element of matrix component has value in the range [0, 255]. Each pixel of the color image component is represented by 8 binary bits. A diffusion operation is performed to produce cipher image C with components as

\[
\begin{align*}
    C_{\text{red}} &= D_{\text{red}} \oplus K_{\text{red}} \\
    C_{\text{green}} &= D_{\text{green}} \oplus K_{\text{green}} \\
    C_{\text{blue}} &= D_{\text{blue}} \oplus K_{\text{blue}}
\end{align*}
\]

where \( \oplus \) is the bit level XOR operation between each pixel and element of color image and matrix components. To retrieve the transmitted color image D,
Secure Color Image Transmission in a Downlink JP-COMP Based MIMO-OFDM Wireless Communication System

reverse diffusion operation is performed to decrypt the color images with components as [4]

\[
\begin{align*}
D_{\text{rretrieved}} &= C_{\text{red}} \oplus K_{\text{red}} \\
D_{\text{gretrieved}} &= C_{\text{green}} \oplus K_{\text{green}} \\
D_{\text{bretrieved}} &= C_{\text{blue}} \oplus K_{\text{blue}}
\end{align*}
\]  

(2)

In transmitter side, the number of generated binary bit from encrypted color image is 221184. The binary data sequence S is channel encoded using \( \frac{1}{2} \)-rated convolutional coding/BCECC (block cipher encryption based channel coding). The BCECC system is shown in Fig. 2. In BCECC scheme, a symmetric block cipher process a data blocks of 256 bits at a time using a secret cryptographic key of 256 bits. The input source binary data are framed into 256 bit block wise and processed in two channels. In one channel, data block is merely channel encoded using \( \frac{1}{2} \)-rated convolutional encoder. In another channel, data block is encrypted using symmetric block cipher and fed into another \( \frac{1}{2} \)-rated convolutional encoder. The output of both channel encoder are demultiplexed to produce Block cipher encrypted Channel encoded binary data [5, 6]. The channel encoded binary data \( D_{\text{FEC}} \) is interleaved and mapped into digitally modulated symbol sequence \( X \) [7]. The symbol sequences \( X \) are spatially demultiplexed into four complex data streams \( X_1, X_2, X_3 \) and \( X_4 \). The data of each stream is rearranged into blocks with each block containing \( N = 2048 \) number of digitally modulated complex data symbols prior to cyclic prefixing for ISI (intersymbol interference) reduction. If \( NN \) being the identical number of blocks processed in each of the four transmitting antenna section and the blockwise complex symbols \( S_{kk,mm}(n), n = 0, 1, 2, 3 \ldots N-1 \) are processed in OFDM modulation process using \( N \) number of sub-carriers used for inverse fast fourier transformation, the time domain OFDM signal can be written as

\[
x_{kk,mm}(t) = \frac{1}{N} \sum_{n=0}^{N-1} S_{kk,mm}(n)e^{j2\pi fn/N} 
\]

(3)

where, \( kk \) and \( mm \) are the transmitting antenna and block identifiers respectively; \( kk = 1, 2, 3, 4 \) and \( mm = 1, 2, 3, \ldots NN \). \( T_{\text{ofdm}} = NT_{\text{data}} \) is the OFDM symbol duration and \( T_{\text{data}} \) is the data symbol duration. The sampled sequence of the complex envelope \( x_{kk,mm}(t) \) of an OFDM symbol presented in Eq. (3) with rate \( 1/T_{\text{data}} \) can be written as

\[
x_{kk,mm}(w) = \frac{1}{N} \sum_{n=0}^{N-1} S_{kk,mm}(n)e^{j2\pi nw/N} \quad w = 0, 1, 2, 3 \ldots N-1
\]

(4)

We assume that the OFDM symbol duration \( T_{\text{ofdm}} \) is large as compared to the duration of the impulse response of the MIMO channel \( \tau_{\text{max}} \). In order to make significant reduction of ISI, a guard interval of duration \( T_{\text{cyclic}} \geq \tau_{\text{max}} \) is inserted between adjacent OFDM symbols. The guard interval \( T_{\text{cyclic}} = 205T_{\text{data}} \) is a cyclic extension of each OFDM symbol, which is obtained by extending the duration of an OFDM symbol to

\[
T_{\text{ofdm}}' = T_{\text{cyclic}} + T_{\text{data}}
\]

(5)

If \( L_g = 205 \) is the discrete length of the of the guard interval, the sampled sequence with cyclically extended guard interval can be written as

\[
x_{kk,mm}(w)=\frac{1}{N} \sum_{n=0}^{N-1} S_{kk,mm}(n)e^{j2\pi nw/N} \quad w = -L_g \ldots N-1
\]

(6)

Fig. 2 Block cipher encryption based channel coding system.
In perspective of signal model presented in Eq. (6) and its applicability for all blocks of signals transmitted from all antennas, we can write the transmitted signal vector $X_s$ in terms of its four signal vector components $X_{11}, X_{22}, X_{33}$ and $X_{44}$ transmitted simultaneously from each of the seven macro base stations as:

$$X_s = \begin{bmatrix}
X_{11}(w) & X_{12}(w) & \ldots & X_{1,NN-1}(w) & X_{1,NN}(w) \\
X_{21}(w) & X_{22}(w) & \ldots & X_{2,NN-1}(w) & X_{2,NN}(w) \\
X_{31}(w) & X_{32}(w) & \ldots & X_{3,NN-1}(w) & X_{3,NN}(w) \\
X_{41}(w) & X_{42}(w) & \ldots & X_{4,NN-1}(w) & X_{4,NN}(w)
\end{bmatrix}$$

(7)

If $H_1, H_2 \ldots H_7$ are considered to be the $4 \times 4$ channel matrices for the base stations to the user unit and $n_1, n_2 \ldots n_7$ are the corresponding zero mean circularly symmetric complex Gaussian noises, we can write, the received signal at the user unit as:

$$Y = (H_1 + H_2 + H_3 + H_4 + H_5 + H_6 + H_7) X_s + (n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7)$$

(8)

Eq. (8) can be written in terms of equivalent channel matrix $H$ and Equivalent noise $N$ as:

$$Y = HX_s + N$$

(9)

With implementation of channel equalization techniques, the transmitted signal is recovered/detected using the following relation:

$$\hat{X}_s^{\text{detected}} = WY$$

(10)

In Eq. (10), first $L_g$ samples of each element of the four rows are induced with ISI and these $L_g$ samples are removed from each cyclically extended OFDM block before multi-carrier demodulation with exploitation of fast fourier transformation [8].

3. Results and Discussion

In this section, we have presented a series of simulation results to illustrate the significant impact of system performance in terms of BER in JP-CoMP (joint processing coordinate multiple point transmission and reception). We have investigated BER performance of the downlink JP-CoMP based MIMO-OFDM wireless communication system with simulation parameters tabulated in Table 1.

It is quite noticeable that the BER curves depicted in Figs. 3-6 are clearly indicative of showing distinguishable difference between system performance under various channel equalization and digital modulation schemes. In Fig. 3, it is observable that the JP-CoMP based convolutionally encoded system exhibits better BER (bit error rate) performance with deployment of MMSE channel equalization in QAM digital modulation as compared to QPSK and DQPSK. At 5% BER, the convolutionally encoded JP-CoMP based system with QAM achieves SNR gain of 1.10 dB and 3.6 dB respectively as compared to QPSK and DQPSK. At low SNR value region, noise enhancement effect is significant causing reduction of system performance. In Fig. 4, it is seen that the BER values with ZF-SIC channel equalization in case of identical signal and noise power for QAM and DQPSK are 0.2370 and 0.4980 respectively which implies a system performance enhancement by 3.22 dB. In Fig. 5, it is quite obvious that the Block cipher encryption based channel encoded system with implemented MMSE shows satisfactory performance in QAM as compared to DQPSK and QPSK. At 5% bit error rate, this JP-CoMP based MIMO-OFDM system with QAM achieves SNR gain of 1 dB and 3.4 dB respectively as compared to QPSK and DQPSK. It is clearly indicative that the system outperforms in QAM digital modulation. In Fig. 6, the estimated BERs are 0.0210 and 0.0841 in case of QAM and DQPSK at SNR value of 0 to 10 dB.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Summary of the simulated model parameters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data type</td>
<td>Color image (96 × 96 × 3 pixels)</td>
</tr>
<tr>
<td>Antenna configuration</td>
<td>4-by-4</td>
</tr>
<tr>
<td>Channel coding/decoding</td>
<td>½-rated Convolutional and block cipher encryption based channel coding</td>
</tr>
<tr>
<td>Data modulation</td>
<td>QPSK, DQPSK and QAM</td>
</tr>
<tr>
<td>IFFT/FFT size</td>
<td>2048</td>
</tr>
<tr>
<td>CP length</td>
<td>205</td>
</tr>
<tr>
<td>Channel equalization scheme</td>
<td>MMSE, ZF-SIC</td>
</tr>
<tr>
<td>Channel</td>
<td>AWGN and Rayleigh fading</td>
</tr>
<tr>
<td>Signal to noise ratio, SN</td>
<td>0 to 10 dB</td>
</tr>
</tbody>
</table>
Secure Color Image Transmission in a Downlink JP-COMP Based MIMO-OFDM Wireless Communication System

Fig. 3 BER performance of downlink JP-COMP based convolutionally encoded MIMO-OFDM wireless communication system with adaptation of MMSE channel equalization and different digital modulation schemes.

Fig. 4 BER performance of downlink JP-COMP based convolutionally encoded MIMO-OFDM wireless communication system with adaptation of ZF-SIC channel equalization and different digital modulation schemes.

of 5 dB for the Block cipher encryption based channel encoded system with ZF-SIC which ratify a system performance improvement of 6.03 dB. At 5% bit error rate, the Block cipher encryption channel encoded JP-CoMP based MIMO-OFDM system with QAM achieves SNR gain of 1 dB and 3.4 dB respectively as compared to QPSK and DQPSK under implemented ZF-SIC channel equalization scheme. In Fig. 7, it has been confirmed that the encrypted image is highly uncorrelated with the original image. At a comparatively low SNR value of 6 dB, the retrieved image has a great similarity with the original transmitted image.

4. Conclusions

We have shown theoretically that the JP-COMP aided MIMO-OFDM wireless communication system can be effectively used for data transmission. We have explored that such JP-COMP aided and multi antenna supported multicarrier simulated system shows enhanced
Secure Color Image Transmission in a Downlink JP-COMP Based MIMO-OFDM Wireless Communication System

Fig. 7 Transmitted, Encrypted and Retrieved Color images in downlink JP-COMP based MIMO-OFDM wireless communication system under scenario of adapting block cipher encryption aided channel coding, ZF-SIC channel equalization and QAM digital modulation schemes.

and robust performance using Block Cipher Encryption aided channel encoder and ZF-SIC receiver. We found an interesting result from this study that the system shows degraded performance under implementation of convolutional channel coding. In perspective of low order digital modulation, QAM is preferable as compared to QPSK and DQPSK digital modulations.

References