Encrypted message transmission in a QO-STBC encoded MISO wireless Communication system under implementation of low complexity ML decoding algorithm

Md. Golam Rashed
Dept. of Information and Communication Engineering, University of Rajshahi, Rajshahi-6205, Bangladesh.

Shaikh Enayet Ullah
Dept. of Applied Physics and Electronics Engineering. University of Rajshahi, Rajshahi-6205, Bangladesh.

Most. Farjana Sharmin
Dept. of Information and Communication Engineering, University of Rajshahi, Rajshahi-6205, Bangladesh.

ABSTRACT

In this paper, we made a comprehensive BER simulation study of a quasi- orthogonal space time block encoded (QO-STBC) multiple-input single output(MISO) system. The communication system under investigation has incorporated four digital modulations (QPSK, QAM, 16PSK and 16QAM) over an Additative White Gaussian Noise (AWGN) and Raleigh fading channels for three transmit and one receive antennas. In its FEC channel coding section, three schemes such as Cyclic, Reed-Solomon and ½-rated convolutionally encoding have been used. Under implementation of merely low complexity ML decoding based channel estimation and RSA cryptographic encoding /decoding algorithms, it is observable from conducted simulation test on encrypted text message transmission that the communication system with QAM digital modulation and ½-rated convolutionally encoding techniques is highly effective to combat inherent interferences under Raleigh fading and additive white Gaussian noise (AWGN) channels. It is also noticeable from the study that the retrieving performance of the communication system degrades with the lowering of the signal to noise ratio (SNR) and increasing in order of modulation.

Keywords

Quasi-orthogonal space time block codes (QO-STBCs), ML decoding, Channel Coding, Bit Error rate, Data Encryption/Decryption.

1. INTRODUCTION

Data Security using cryptography has emerged as a topic of significant interest in both academic and industry circles. In data and telecommunications, cryptography is necessary when communicating over any untrusted network particularly Internet. In recent year, a significant amount of research is being going on to enrich network security through development of Asymmetric key algorithm [1].

In asymmetric key cryptography, also called Public Key cryptography, two different keys (which forms a key pair) are used. One key is used for encryption and only the other corresponding key must be used for decryption. No other key can decrypt the message, not even the original (i.e. the first) key used for encryption. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else. RSA is a well-known public-key cryptography algorithm. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography [2]

In wireless communications, one main challenge is the transmission over channels that experience time-variant multipath fading . Such detrimental effects in wireless fading channels can be combated

using space –time block coding (STBC), an efficient transmit diversity scheme with exploitation of the diversity advantage of multi-antenna systems[3,4].Orthogonal space time block codes (OSTBCs) achieve full transmit diversity with a low (linear) maximum-likelihood (ML) decoding complexity . In case of multi-input multi-output (MIMO) communication systems with more than two transmit antennas, full-diversity rate-one O-STBCs do not exist. To overcome the low-rate constraints of OSTBCs, Quasi-orthogonal space time block codes (QO-STBCs) for four and three transmit antennas have been proposed which not achieve full diversity and have a substantially higher ML decoding complexity than the OSTBCs[5].In this present study , a low-complexity sub optimal ML decoder for coherent quasi-orthogonal space time block codes with three transmit antennas and RSA block cipher scheme based data encryption/decryption algorithm have been used. A brief description of these data processing schemes are outlined below.

2. MATHEMATICAL MODEL

2.1 RSA Algorithm

A cryptographic algorithm 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 21024. 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::

$C = M^e \bmod n$

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

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[10].

2.2 Low Complexity ML Decoding

In this section, the low-complexity sub optimal ML decoding scheme proposed by Samer J. Alabed and et.al in 2011 has been reviewed[5], In a MISO wireless communication system with three transmit and one receive antennas and assumed flat block fading channel with block length of T, the input-output relation can be expressed as:

$$R = XH + N \qquad \text{……………………………….(1)}$$

and the QO-STBC for three transmitting antenna can be written to derive low-complexity decoding scheme as:

$$\mathbf{X} = \begin{bmatrix} x_1 & x_2 & 0 \\ -x_2^* & x_1^* & 0 \\ 0 & x_3 & x_4 \\ 0 & -x_4^* & x_3^* \end{bmatrix} \qquad \text{…………}$$

………….(2)

where $(.)^*$ denotes the complex conjugate and x_i are the transmitted digitally modulated signals that depend on s_i. The diversity order of two can be achieved if $x_i = s_i (i = 1,2,3,4);$ To achieve full diversity, the following mapping can be used [7].

$$x_1 = s_1 + \hat{s}_3, \quad x_2 = s_2 + \hat{s}_4.$$
$$x_3 = s_1 - \hat{s}_3, \quad x_4 = s_2 + \hat{s}_4 \qquad \text{………………(3)}$$

Where $\hat{s}_3 \triangleq s_3 e^{j\emptyset}, \hat{s}_4 \triangleq s_4 e^{j\emptyset}$ and $\emptyset$ is the rotation angle that is selected as in [7].

Using (2) and (3), (1) can be divided into two equations as

$$r_1 = X_1 h_1 + n_1 \qquad \text{and}$$
$$r_2 = X_2 h_2 + n_2 \qquad \text{……………….(4)}$$

Where

$$r_1 \triangleq \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}. h_1 \triangleq \begin{bmatrix} h_1 \\ h_2 \end{bmatrix}. n_1 \triangleq \begin{bmatrix} n_1 \\ n_2 \end{bmatrix},$$

$$X_1 \triangleq \begin{bmatrix} s_1 + \hat{s}_3 & s_2 + \hat{s}_4 \\ -(s_2 + \hat{s}_4)^* & (s_1 + \hat{s}_3)^* \end{bmatrix},$$

$$r_2 \triangleq \begin{bmatrix} r_3 \\ r_4 \end{bmatrix}. h_2 \triangleq \begin{bmatrix} h_2 \\ h_3 \end{bmatrix}. n_2 \triangleq \begin{bmatrix} n_3 \\ n_4 \end{bmatrix},$$

$$X_2 \triangleq \begin{bmatrix} s_1 - \hat{s}_3 & s_2 - \hat{s}_4 \\ -(s_2 - \hat{s}_4)^* & (s_1 - \hat{s}_3)^* \end{bmatrix}.$$

2.3 2.3 The coherent QO-STBC

Using (4) and assuming the perfect CSI at the receiver, the coherent ML decoder of (2) can be written as

$$\min_{s_1,s_2,\hat{s}_3,\hat{s}_4} \|R - XH\|^2 = \min_{s_1,s_2,\hat{s}_3,\hat{s}_4} \|r_1 - X_1 h_1\|^2 +$$
$$\min_{s_1,s_2,\hat{s}_3,\hat{s}_4} \|r_2 - X_2 h_2\|^2 \qquad \text{……………………….(5)}$$

Where $\|.\|$ stand for the frobenious norm. Expanding the first and second term at the right hand side of (5). We obtain

$$\|r_1 - X_1 h_1\|^2 = (|s_1 + \hat{s}_3|^2 + |s_2 + \hat{s}_4|^2)(|h_1|^2 + |h_2|^2)$$
$$-2R_e\{(h_1 r_1^* + h_2^* r_2)(s_1 + \hat{s}_3)\}$$
$$-2R_e\{(h_2 r_1^* + h_1^* r_2)(s_2 + \hat{s}_4)\} + c_1 \quad \text{…(6)}$$

$$\|r_2 - X_2 h_2\|^2 = (|s_1 - \hat{s}_3|^2 + |s_2 - \hat{s}_4|^2)(|h_2|^2 + |h_3|^2)$$
$$-2R_e\{(h_2 r_3^* + h_3^* r_4)(s_1 - \hat{s}_3)\}$$
$$-2R_e\{(h_3 r_3^* - h_2^* r_4)(s_2 - \hat{s}_4)\} + c_4 \quad \text{………..(7)}$$

Respectively, where c_1 and c_2 are constant terms that do not depend on the symbols and $R_e\{.\}$ Denotes the real part. Using (6) and (7) in (5), we note that s_1 and $\hat{s}_3$ can be denoted independently of s_2 and $\hat{s}_4$. Therefore, (5) can be rewritten as

$$\min_{s_1,s_2,\hat{s}_3,\hat{s}_4} \|R - XH\|^2 = \min_{s_1,\hat{s}_3,} f_{13}(s_1,\hat{s}_3) + \min_{s_2,\hat{s}_4,} f_{24}(s_2,\hat{s}_4)$$

……………………..(8)

Where $f_{13}(s_1,\hat{s}_3) = |s_1 + \hat{s}_3|^2 \, (|h_1|^2 + |h_2|^2)$

$$+|s_1 - \hat{s}_3|^2 \, (|h_2|^2 + |h_3|^2)$$
$$-2R_e\{(h_1 r_1^* + h_2^* r_2)(s_1 + \hat{s}_3)\}$$

$$-(h_2 r_3^* - h_3^* r_4)(s_1 - \hat{s}_3) \text{........(9)}$$

$$\begin{aligned} f_{24}(s_2,\hat{s}_4) = {} & |s_2+\hat{s}_4|^2\,(|h_1|^2+|h_2|^2) \\ & +|s_2-\hat{s}_4|^2\,(|h_2|^2+|h_3|^2) \\ & -2R_e\{(h_2 r_1^* - h_1^* r_2)(s_2+\hat{s}_4)\} \\ & -(h_3 r_3^* - h_2^* r_4)(s_2-\hat{s}_4) \text{.......(10)} \end{aligned}$$

and the subscripts of the functions denote the unknown symbols used in their respective arguments. As the pairs $(s_1,\hat{s}_3)$ and $(s_2,\hat{s}_4)$ can be detected independently of each other. We can use a pair-wise complex symbol decoder instead of the full ML decoder. However, such decoding can be still prohibitively expensive when the signal constellation size is high. Using developed suboptimal decoder for s_1 and $\hat{s}_3$, the decoding procedure for s_2 and $\hat{s}_4$ follows similar steps. We can express $f_{13}(s_1,\hat{s}_3)$ in Equation (9) as :

$$\begin{aligned} f_{13}(s_1,\hat{s}_3) = {} & |s_1|^2(|h_1|^2+2|h_2|^2+|h_3|^2) \\ & -2R_e\{(h_1 r_1^* + h_2^* r_2 + h_2 r_3^* + h_3^* r_4)s_1\} \\ & +|\hat{s}_3|^2(|h_1|^2+2|h_2|^2+|h_3|^2) \\ & -2R_e\{(h_1 r_1^* + h_2^* r_2 - h_2 r_3^* - h_3^* r_1)\hat{s}_3\} \\ & +2(|h_1|^2-|h_3|^2)R_e\{s_1\hat{s}_3^*\} \text{......................(11)} \end{aligned}$$

If the decoder knows s_3, then (11) can be reduced to

$$\begin{aligned} f_1(s_1,\hat{s}_3) = {} & |s_1|^2(|h_1|^2+2|h_2|^2+|h_3|^2) \\ & -2R_e\{(h_1 r_1^* + h_2^* r_2 + h_2 r_3^* + h_3^* r_4)s_1\} \\ & +2(|h_1|^2-|h_3|^2)R_e\{s_1\hat{s}_3^*\} \text{...............(12)} \end{aligned}$$

To detect s_1, similarly, if the decoder knows s_1, then we can reduce (11) to

$$\begin{aligned} f_3(s_1,\hat{s}_3) = {} & |\hat{s}_3|^2(|h_1|^2+2|h_2|^2+|h_3|^2) \\ & -2R_e\{(h_1 r_1^* + h_2^* r_2 - h_2 r_3^* - h_3^* r_1)\hat{s}_3\} \\ & +2(|h_1|^2-|h_3|^2)R_e\{s_1\hat{s}_3^*\} \text{...............(13)} \end{aligned}$$

to detect s_3.

3. COMMUNICATION SYSTEM MODEL

A simulated single -user 3 x 1 spatially multiplexed wireless communication system as depicted in Figure 1 utilizes low complexity ML decoding scheme based Quasi-Orthogonal space-time block and o coding scheme. In such a communication system, the text message is converted into integer and subsequently encrypted using RSA encryption algorithm. The encrypted data are converted into binary bits and channel encoded using Cyclic, Reed-Solomon and ½-rated convolutionally encoding schemes and interleaved for minimization of burst errors. The interleaved bits are digitally modulated using various types of digital modulations such as Quadrature Phase Shift Keying (QPSK), Quadrature Amplitude (QAM), 16PSK and 16QAM [8,9]. The complex digitally modulated symbols are block encoded with implemented QOSTBC scheme and fed into three transmitting antennas. In receiving section, the transmitted signal is processed with ML decoding algorithm and the decoded modulated symbols are fed into Q-OSTBC decoder. Its output data are demapped, deinterleaved and channel decoded . The decoded binary data are converted into integer and decrypted with RSA decryption algorithm.. The decrypted data are converted into message.

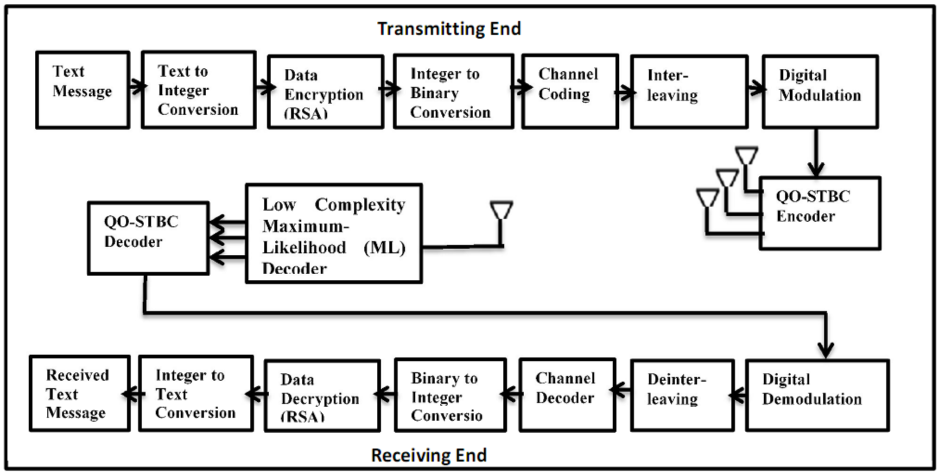

Figure 1: Block diagram of a low complexity ML decoding scheme based QO-STBC encoded MISO wireless communication system

4. RESULTS AND DISCUSSION

We have made a comprehensive BER simulation study for a single- user MISO QO-STBC encoded wireless communication system based on the parameters given in Table 1. It is assumed that the channel state information (CSI) is available at the receiver and the fading process is approximately constant during each time slot assigned for simultaneous transmission of symbols from three transmitting antennas in a Q-OSTBC codeword. The graphical illustrations presented in Figure 2 through Figure 4 show system performance comparison with implementation of various channel coding and ML signal detection schemes under different digital modulations. In Figure 2, it is noticeable that for a typically assumed SNR value of 3 dB, the BER values are 0.0012 and 0.4562 in case of QAM and 16 PSK digital modulations viz., the system achieves a substantial gain of 25.80 dB in QAM as compared to 16PSK. In Figure 3, it is observable that the system shows comparatively better performance in convolutional encoding scheme as compared to cyclic coding. Under implementation of cyclic coding, the system shows almost flat response for wide range of SNR values. For a typically assumed SNR value of 3 dB, the BER values are 0.0012 and 0.3684 in case of convolutional and cyclic channel coding schemes viz., the system achieves a substantial gain of 24.87 dB in convolutional coding as compared to Cyclic.

Figure 4 is clearly indicative of the impact of channel coding, The bit error rate in case of system performance with implemented channel and interleaving schemes and without implemented channel and interleaving schemes at a typically assumed low SNR value of 0.5 dB are 0.0178 and 0.0683 respectively. This is also a case of system performance improvement of 5.84 dB.

Table 1: Summary of the simulated model parameters

Parameters	Values
Data type	Text message
Encryption/Decryption algorithm	RSA
Antenna configuration	3-by-1
Channel Coding	½-rated Convolutional , Reed_Solomon and Cyclic
Modulation	QPSK, QAM, 16PSK and 16QAM
Signal Detection Scheme	Maximum-Likelihood
Channel	AWGN and Rayleigh
Signal to noise ratio, SNR	0 to10 dB

In Figure 5, the bit error rate at SNR value of 0dB and 5 dB are 0.0301 and 0.0007 respectively. The quality of transmitted encrypted message is improved with increase in SNR values.

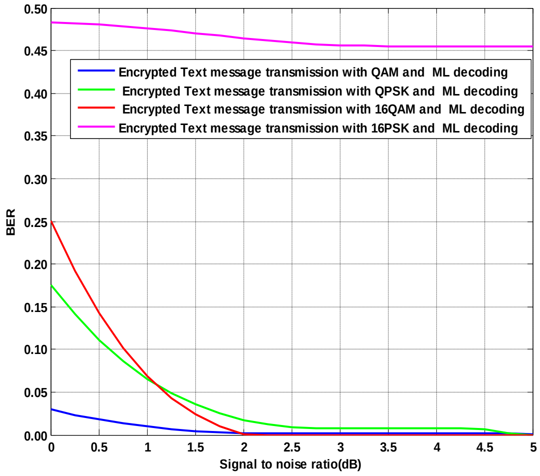

Figure 2: BER performance of the QO-STBC encoded MISO wireless communication simulated wireless communication system under implementation of low complexity ML decoding algorithm and various digital modulations.

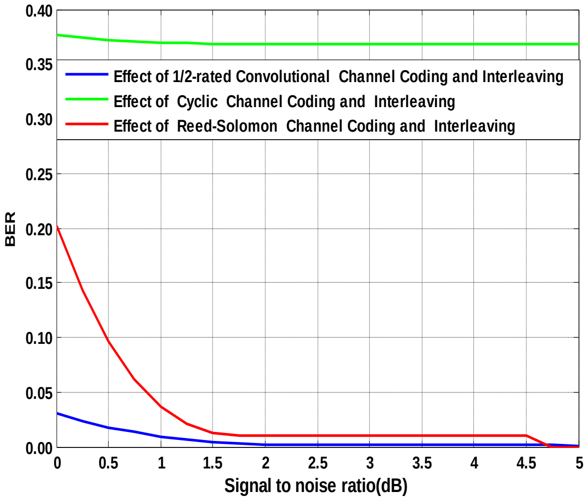

Figure 3: Effect of various types of implemented Channel coding schemes on the BER performance of low complexity ML decoding algorithm and QAM modulation based simulated wireless communication system

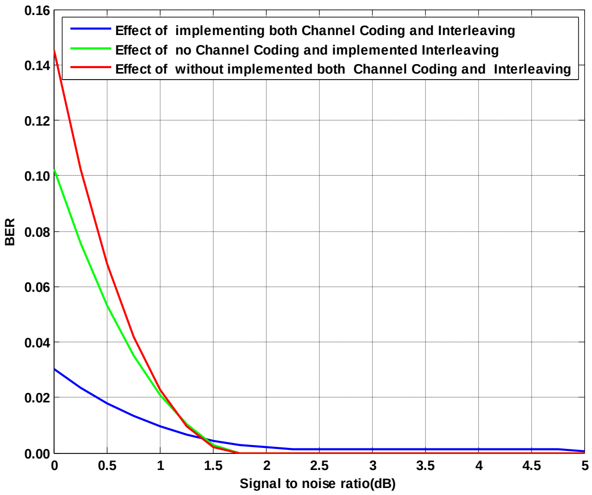

Figure 4: Effect of Channel coding and Interleaving schemes on BER performance of the simulated wireless communication system under implementation of low complexity ML decoding algorithm and QAM modulation

The use of multiple antennas at the transmitter and receiver in wireless systems, popularly known as MIMO (multiple-input multiple-output) technology, has rapidly gained in popularity over the past decade due to its powerful performance-enhancing capabilities. Communication in wireless channels is impaired predominantly by multi-path fading

(a)

2³TL□• TLwL□0J`I0TL\BJTBB\ • L\JLJ³TLJ~\B • `JJT~L\B • L~T°T`eT~L`BL`~T0T • • j¯
• M • JT • II□0\~0MLpBBL\ • Ly=yLt□0J`I0Tz`BI□JL□0J`I0T z□JI□J.LJT°³B0Mj¯³
\ • L~\I` • 0ML\`BT • L`BLII□0\~`JMLeT~LJ³TLI\ • JL • T°\ • T L • □TLJL`J • LIT~w□0Lj¯IT~w
~\B°TzTB³\B°`BL°\I\`0`J`T • C□B`°\J`BL`BL`~T0T • • L°³\BB T0 • L` • Lj¯`I\`~T • LI~
T • `B\BJ0MLML□0J`zI\J³Lw\ • `Bj¯j¯j¯j¯

(b)

The use of multiple antennas at the transmitter and receiver in wireless systems, popularly known as MIMO (multiple-input multiple-output) technology, has rapidly gained in popularity over the past decade due to its poSerful performance-enhancing capabilities. Communicaton ·n wireless channels is impaired predominantly by multi-path fading]

(c)

The use of multiple antennas at the transmitter and receiver in wireless systems, popularly known as MIMO (multiple-input multiple-output) technology, has rapidly gained in popularity over the past decade due to its powerful performance-enhancing capabilities. Communication in wireless channels is impaired predominantly by multi-path fading]

(d)

Figure 5: Transmitted , Encrypted and Retrieved message, (a) Original Transmitted Text message (b) Encrypted Text Message, (c) Retrieved Text message at 0dB, (d) Retrieved Text message at 5dB. Red mark indicates noise contamination

5. Conclusions

In this paper, an effort has been made to present simulation results under implementation of various channel encoding techniques in a single -user low complexity ML decoding scheme based Quasi-Orthogonal space-time block encoded MISO wireless communication system. A range of system performance results highlights the impact of ML detection and channel coding scheme on encrypted text message transmission. In the context of system performance, it can be concluded that the implementation of QAM digital modulation technique with deployment of ML signal detection technique provides satisfactory result for such a single -user Q-OSTBC encoded MISO wireless communication system.

6. REFERENCES

[1] Prakash Kuppuswamy and. C.Chandrasekar, 2011: Enrichment of Security through Cryptographic Public Key Algorithm based on Block Cipher, Indian Journal of Computer

Science and Engineering (IJCSE), vol. 2 ,no. 3 pp. 347-355

[2] Dhakar, Ravi Shankar Gupta, Amit Kumar Sharma, Prashant ,2012: International Conference on Advanced Computing & Communication Technologies (ACCT), pp. 426 – 429

[3] Zhongding Lei, Chau Yuen, and Francois P.S. Chin, 2011: Quasi-Orthogonal Space-Time Block Codes for Two Transmit Antennas and Three Time Slots, IEEE Transactions on Wireless Communications, vol. 10, no. 6,pp.1983-1991

[4] Xiaoyong Guo , 2010: A Simple Construction of Full-Rate Quasi-Orthogonal Space-Time Block Codes for 4 and 6 Transmit Antennas, proceedings of IEEE GLOBECOM,pp.1-5

[5] Samer J. Alabed, Javier M. Paredes, and Alex B. Gershman ,2011: A Low Complexity Decoder for Quasi-Orthogonal Space Time Block Codes, Transactions on Wireless Communications, vol. 10, no. 3, pp.988-994.

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

[7] A. Wong, J.-K. Zhang, and K. M. Wong, 2008: Full diversity group decodal orthogonal linear dispersion codes for MISO flat fading channels, in Proc. ICASSP’08, Las Vegas, USA pp. 2929-2932.

[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

Authors

Md. Golam Rashed 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. He also worked as a Lecturer of the Department of Electronic and Telecommunication Engineering, University of Development alternative, Dhaka, Bangladesh in 2010. 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.

Shaikh Enayet Ullah 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 50 articles in multidisciplinary fields. His main research interests include Cooperative communications, MIMO-OFDM, WiMAX , Cognitive radio and LTE radio interface technologies.

Most. Farjana Sharmin received her Bachelor of Science B.Sc(Hons) Degree in Information and Communication Engineering from Rajshahi University in 2011. Concurrently, She is working as a M.Sc. research student in the Department of Information and Communication Engineering, University of Rajshahi. Her main research interests include Space Time Block Coding, MISO/MIMO-OFDM, 4G compatible MC-CDMA radio interface technology.