Middle-East Journal of Scientific Research 17 (4): 500-506, 2013
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2013.17.04.12079

Performance Analysis of Wireless System Intertwined with Crypto and Stego Applications

[1]M. Hemalatha, [2]V. Prithiviraj, [3]R. Karthick and [3]R. Prasanth

[1]School of Computing, SASTRA University, Thanjavur, Tamil Nadu, India
[2]Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India
[3]IBM, Bengaluru, India

Abstract: The developments in the wireless communication domain is at fast pace in the recent decades and the challenges are also arising in par with the advancements. Most important issues are the security, shortage of bandwidth in the licensed and unlicensed band and the signal interference. Many sophisticated algorithms have been proposed for traditional communication systems, but it is essential to verify their performance in a wireless scenario. Since interference is a major threat in wireless communication, the cryptographic algorithms should assure for reliability for different noise and channel characteristics. This report examines the performance of traditional cryptographic algorithm with steg image transported over a noisy wireless link with OFDM transceiver. A novel idea is proposed to strengthen the key generation for security algorithms. Performance comparison is made for QPSK and BPSK modulation schemes.

Key words: OFDM · Steganography · Bit error rate · Data embedding

INTRODUCTION

In order to avoid inter-symbol interference in single carrier communication long symbol periods are used [1]. Since symbol period is inversely proportional to data rate, presence of long symbol periods will lead to low data rate and inefficiency in communication. In Frequency Division Multiplexing (FDM), the available bandwidth is separated into sub-bands for multicarrier to transmit in parallel [2]. In FDM high data rate can be achieved, but due to lack of spacing to separate the carrier inter-carrier interference will occur.

OFDM (Orthogonal frequency division multiplexing) is the multicarrier communication scheme to solve both issues. It constructs a high data rate channel by combining large number of low rate carriers. The carriers are closely spaced and even overlapped without inter-carrier interference due to the orthogonal property of OFDM. High rate data streams are converted into numerous parallel low rate streams in order to provide high data rate. The two signals are said to be orthogonal to each other, if the integral of the product of two signals is zero over a time period T_0. Orthogonality is the key feature of OFDM. The orthogonality is defined by

$$\int_0^{T_0} \cos(2\pi aft)\cos(2\pi bft)dt = 0 \quad (a \neq b)$$

where a and b are two unequal integers; f is the fundamental frequency [3, 4].

Security is the major threat for wireless communications. If two persons need to exchange message secretly through wireless network, it is difficult in modern days as there are many techniques which captures and alter the message sent. These techniques are created by intruders to listen the private communication. One should ensure security in the network before exchanging the data. In this paper, we analyze how cryptography and steganography provide security through OFDM system when they are combined.

Corresponding Author: M. Hemalatha, School of Computing,
SASTRA University, Thanjavur, Tamil Nadu, India.

In the steganography system scenario, before the hiding process, the sender must select the appropriate message carrier. Steganography can be classified into four categories namely image steganography, video steganography, audio steganography and text steganography [5]. The image steganography algorithms can be classified into spatial domain and frequency domain. Least Significant Bit (LSB) method is mostly preferred whenever information has to hide in images. In the LSB method one bit of secret information is substituted in the 8th bit of every pixel in the cover image.LSB method works fine in the image carriers since the change in the least significant bit position will hardly cause change in the appearance of the color of that pixel [6].

The novel idea is to generate and strengthen the cipher key with the traditional encrypting algorithm e.g. RSA algorithm in a reliable manner. The attempt is made to explore the cryptographic algorithm over the wireless link with the simulated noisy channel [7].

System Description: The message to be transmitted through OFDM system is encrypted using user's key by using cryptographic algorithm [8]. The encryption algorithm we used was RC6 encryption algorithm. Then the encrypted text is embedded into the cover image. This steg image is transmitted using OFDM transmitter

$$P3 = P3 \oplus f(P4)$$

through AWGN channel [9]. After receiving the steg image, the data is retrieved from the image and decrypted to get original message. The BER is calculated between the data retrieved and the original message.

Key Generation: Our algorithm uses two keys. First key will be static which is known for both parties. Second Key is generated from three parts, where first part will be present date's Sudoku's first row [10]. Second part is difficulty of the Sudoku which is represented as alphabets [11]. Third part is current date in the format of ddmmyy. Now, both keys are XOR'ed.

STEPS IN RC6 ALGORITHM
NOTATIONS

p + q Addition of a and b modulo 2^w
p - q Subtraction of a and b modulo 2^w
p⊕q Exclusive-or of a and b(w-bit word sizes)
p x q Multiplication of a and b modulo 2^w
p<<q Rotate to the left by q
$q=\log_2 w = 5$

where w is word size which is 32,
So we rotate p to the left by 5
p>>q we rotate to the right where q can be determined as above.

Key Expansion: The sub keys are generated from the user supplied keys of length b. Padding of zero bytes to user supplied key is done to make the key to get its required length. The sub key which are generated from user supplied key are stored into array w (0..Pl-1) of size l words [12]. The generated sub keys are loaded into another array called Ks(0, ..., 2Pr + 3). The size of the array is 2Pr + 4.

Encryption Algorithm: The plaintext, which is the input, is loaded into registers called (P1, P2, P3, P4). The encryption can be done by following these steps:

- RC6 begins with two initial steps:
  - P2 and sub key Ks(0) are added
  - P4 and sub key Ks(1) are added
- Ks[2i] and Ks(2i+1) are the sub keys which are used in each and every round of i to Pr, i.e. Ks(2) and Ks(3) are used in first round.
- A round is described as:
  - The following function has been used by P2 and P4

$$G(a) = a(2a + 1) <<\log_2 w.$$

$$P1 = P1 \oplus G(P2)$$

  - The above function was left-shifted with G(P4) and sum up with Ks(2i)

$$P3 = P3 \oplus f(P4)$$

  - The above function was left-shifted with G(P2) and sum up with Ks(2i+1)
  - The parallel assignment which rotates the registers as follows:
    (P1, P2, P3, P4) = (P2, P3, P4, P1)

- Next step, which is next to last round and the last step:

- P1 and sub key Ks (2Pr + 2) are added.
- P3 and sub key Ks(2Pr + 3) are added.

Decryption Algorithm: The decryption algorithm can be done by following these steps:

- RC6 begins with two initial steps:
  - P3=P3-Ks(2Pr+3)
    P3and sub key Ks(2Pr + 3) are subtracted.
  - P1 = P1-Ks(2Pr+2)
    P1and sub key Ks(2Pr + 2) are subtracted.
  - Ks(2i) and Ks(2i+1) are the sub keys which are used in each and every round of i down to 1, i.e. Ks(21) and Ks(20) are used in first round [13].

- A round is described as:
  - The parallel assignment which rotates the registers as follows:

  (P1, P2, P3, P4) = (P4, P1, P2, P3)

$G(a) = a(2a + 1) - \log_2 w$

  - The following function has been used by P4 and P2 as in encryption
  - P3 = P3 - Ks (2i + 1)
    The above function, which right-shifts with G(P2) and then Xor'ed with G(P4).
  - P1 = P1 – Ks(2i)
    The above function, which right-shifts with G(P4) and then Xor'ed with G(P2)

- The last step in decryption:

  - P4=P4-Ks(1)
    The P4 and Ks(1) are subtracted as above.
  - P2=P2-Ks(0)
    The sub key Ks (0) and P2 are subtracted.

Steganography Using Lsb Method: Least Significant Method is simplest method for hiding data in an image. In this method, the least significant bit of each pixel of a cover image is replaced by the binary values of the secret information.LSB method works fine in the image carriers since the change in the least significant bit position will hardly cause change in the appearance of the color of that pixel [14].

Transmitter Model:

Frame Divider: OFDM symbols are divided into number of frames so that the data will be modulated frame by frame in order for received signal be in sync with the receiver [15].

DPSK Modulator: Each frame is converted from serial to parallel and the frames are differentially encoded and modulated using BPSK [16]. If the bit from the frame is b_k at any time slot t (say), then the differential encoder produce

$e_k = e_{k-1} \oplus b_k$

where $\oplus$ indicates binary or modulo-2 addition.

So e_k changes only state if b_k is 1, otherwise it will be in its previous state.

The carriers are allocated into the IFFT bins. The number of carriers are limited to ((IFFT_Size)-2)/2, since there are as many conjugate carriers as carriers [17]. One IFFT bin is reserved for DC signal and another IFFT bin is reserved for the symmetrical point at the Nyquist frequency to separate carriers and conjugate carriers. Then the IFFT of the data is taken in order to convert data

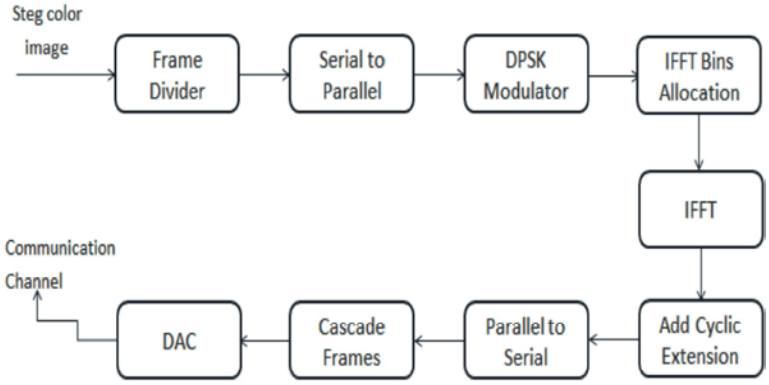

Fig. 1: Transmitter model of OFDM system

Fig. 2: Adding cyclic extensions

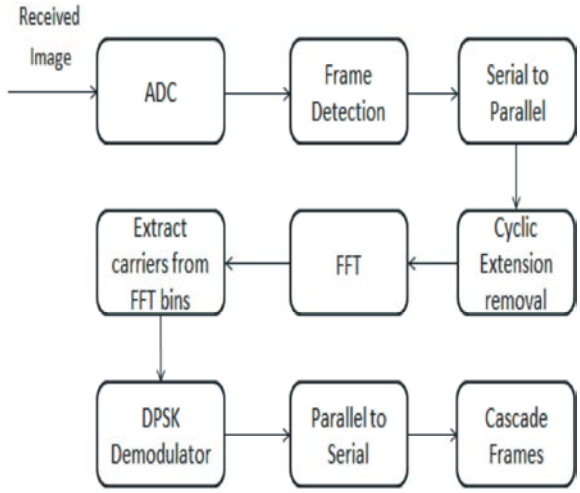

Fig. 3: Receiver model of OFDM system.

from frequency domain to time domain and then it is transmitted. Cyclic extensions are added to each symbol period in order to make Inter Symbol Interference (ISI) nearly eliminated. A 25% fraction of the cycle is taken and added to the front of the symbol period, so that the demodulator can capture the symbol period up to the length of cyclic extension with an uncertainty and still obtain the information for the entire symbol period.

Output frames from IFFT after adding cyclic extension are converted from parallel to serial and cascaded

Awgn Channel: The channel noise is modeled by adding a white Gaussian noise (AWGN) defined by [5]:

$$\sigma\, of\ AWGN\ = \sqrt{\frac{Variance of\ the\ \text{modulated}\ signal}{Linear\ SNR}}$$

Receiver Model: In order to determine the start of the signal frame, a part of the received signal is processed by the frame detector. This selected portion is sampled to a discrete signal with shorter distance and moving sum is measured. The minimum index of the sampled signal represents the approximate location for start of the frame guard. The approximate location for start of the useful signal frame is located by moving one symbol period further from this index.

After converting a frame of discrete time signal from serial to parallel, a length of 25% is discarded from every row. Thus the remaining discrete signals which has length of one symbol period lined up in parallel. Fast Fourier Transform of the resulting time signal is taken which results in the spectrum of the received signal. The columns in the location of carriers are extracted in order to retrieve the complex matrix of the received data. The received signal is demodulated to yield $e_k = \pm 1$ and then the differential decoder reverses the encoding procedure and produces:

$$b_k = e_k \oplus e_{k-1}$$

Each demodulated frame are converted from parallel to serial and cascaded to form a received image.

RESULTS AND DISCUSSION

Fig 4 shows the cover image used to embed the encrypted text. In Fig 5 the text to be encrypted is displayed. The steg image is sent through OFDM transceiver and the received image is shown in Fig 6.

Table 1: Simulation Parameters of OFDM

Parameters	Values
Source Image Size	500 x 500
IFFT size	1024
Number of carriers	400
Peak Power Clipping	5 dB
Signal-to-Noise Ratio	15 dB

Fig. 4: cover image

cryptanalysis in telecommunication system intertwined in wireless domain

Fig. 5: Text to be encrypted

Fig 6: Steg image

Fig 7: Received image

cryptanalysis in telecommunication system intert??„?–çÒ¶wX$ì-*¾ss domain

Fig 8: Decrypted text when SNR=0

cryptanalysis in telecommunication system intertwined in wireless domain

Fig 9: Decrypted text when SNR=10

Fig 10: Received image when SNR=0

Fig 11: Received image when SNR=10

Fig 12: Received image when SNR=16

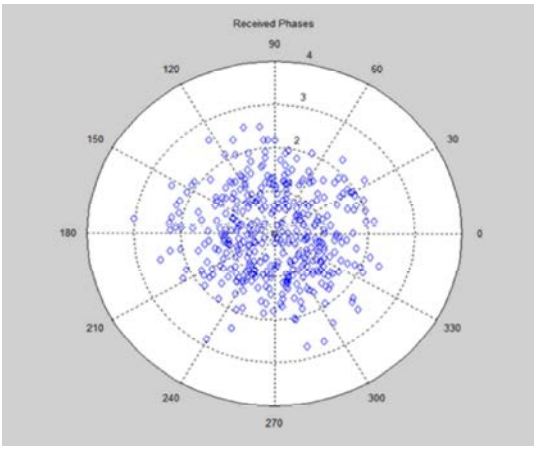

Fig 13: Phasor plot when SNR=0

Figures 10, 11, 12 witnessed the improvement in image reception when SNR is increased. This can be observed in the phasor plots for different values. Figures 13, 14, 15 show the phasor plot for BPSK scheme when employed in a OFDM transceiver.

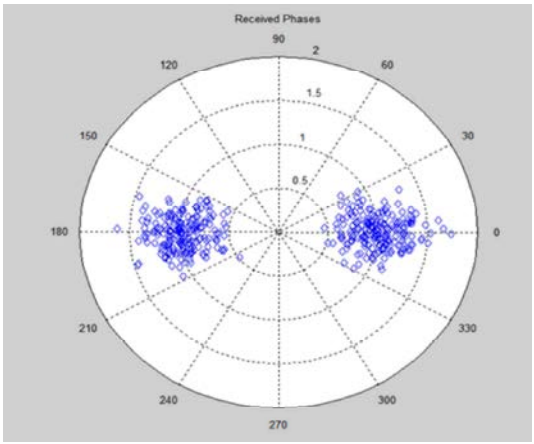

Fig 14: Phasor plot when SNR=10

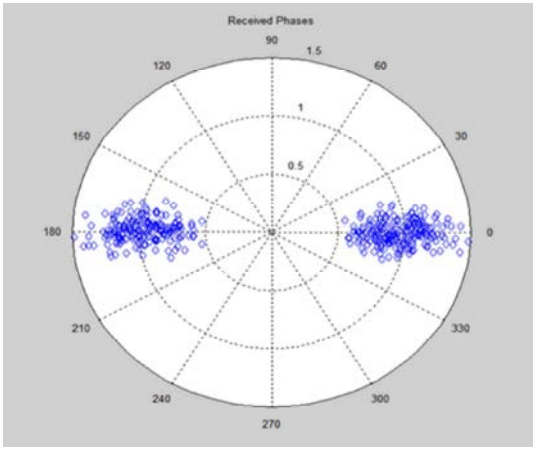

Fig 15: Phasor plot when SNR=16

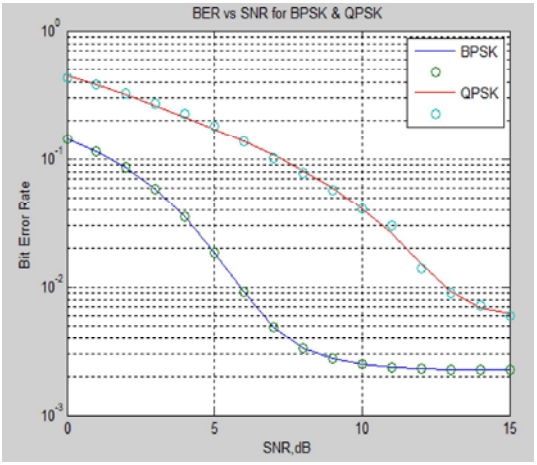

Fig 16: BER vs. SNR

Fig 16 gives the comparison between BPSK and QPSK modulation for various Eb/N_0 levels. It is observed that BPSK is good candidate only when SNR is low, otherwise QPSK performs well against noise.

CONCLUSION

This work suggests a way of testing cryptography and steganography algorithms in a wireless scenario with various channel models. This attempt intertwines the various aspects of wireless communication such as secured transmission, reliable reception and efficient bandwidth utilization through combined crypto and stego system with OFDM transceiver. Idea of strengthening the key is suggested and is demonstrated with BPSK and QPSK modulation techniques. Conventional Bit Error Rate analysis is carried out for the standard open source images. Cryptanalysis for the proposed model may be carried as future expansion and similar work can be carried out for the visual cryptographic system. The extension of this proposal may be focused on concatenated channel model to simulate real-time wireless scenario.

ACKNOWLEDMENTS

The authors want to thank Dinesh V J of SASTRA University for his time and support.

REFERENCES

1. Schulze Henrik and Christian Luders, 2005. Theory and Applications of OFDM and CDMA, John Wiley & Sons, Ltd.
2. Harold, P.E., Stern and Samy A. Mahmoud, 2004. Communication Systems: Analysis and Design, ISBN-0-13-040268-0.
3. John, R., Barry, Edward A. Lee and David G. Messerschmitt, 2003. Digital Communication, ISBN-10:0792375483.
4. Bernad Sklar, 2001. Digital Communication: Fundamentals and Applications, ISBN-10:0130847887, ISBN-13:978-0130847881
5. Paul Guanming Lin, 2010. OFDM Simulation in MATLAB, Bachelor thesis, California Polytechnic State University, June.
6. Hemalatha, M., K. Thenmozhi, V. Prithviraj D. Bharadwaj and S. Vignesh, 0000. Diversity reception in CDMA based broadband mobile systems, Proceedings of international conference wireless VITAE'09, pp: 660-664.
7. Hemalatha, M., V. Prithviraj, S. Jayalalitha and K. Thenmozhi, 2011. Diversity analysis in Wi-Fi systems, Journal of Theoretical and Applied Information Technology, 33(1): 111-117.

8. Hemalatha, M., V. Prithviraj, S. Jayalalitha and K. Thenmozhi, 2012. Diversity analysis in CDMA based broadband wireless systems, Research Journal of Applied Sciences, Engineering and Technology, 4(6): 660-663.
9. Hemalatha, M., V. Prithviraj, S. Jayalalitha and K. Thenmozhi, 0000. Space Diversity Knotted with WiMAX- Away for Undistorted and Anti-Corruptive Channel, Wireless Pers Commun DOI 10.1007/s11277-012-0987-6, Article in press.
10. Gil-HO Kim, Jong-Nam Kim and Gyeong-Yeon Cho, 0000. An improved RC6 algorithm with the same structure of encryption and decryption.
11. Atallah, M., Al-Shatnawi and Al-albayt, 2012. A New Method in Image Steganography with Improved image quality, University of Jordan, Applied Mathematics Sciences, 6(79): 3907-3915.
12. Fouad Ramia and Hunar Oadir, RC6 Implementation including Key Scheduling using FPGA.
13. Roszizti Ibrahim and Teoh Sukkuan, 2011. Steganography Algorithm to Hide Secret Message inside an Image, Computer Technology and Applications 2, Feb.25, David Publishing.
14. Vijay Kumar Sharam and Vishal Shrivastava, 2012. A Steganography Algorithm for Hiding Image in Image by improved LSB substitution by minimize detection, Journal of Theoretical and Applied Information Technology, Feb.15, 36(1): 1992-8645, E-ISSN: 1817-3195.
15. Abou-Deif, M.H., M.A. Rashed, M.A.A. Sallam, E.A.H. Mostafa and W.A. Ramadan, 2013. Characterization of Twenty Wheat Varieties by ISSR Markers, Middle-East Journal of Scientific Research, 15(2): 168-175.
16. Kabiru Jinjiri Ringim, 2013. Understanding of Account Holder in Conventional Bank Toward Islamic Banking Products, Middle-East Journal of Scientific Research, 15(2): 176-183.
17. Muhammad Azam, Sallahuddin Hassan and Khairuzzaman, 2013. Corruption, Workers Remittances, Fdi and Economic Growth in Five South and South East Asian Countries: A Panel Data Approach Middle-East Journal of Scientific Research, 15(2): 184-190.