Chaotically Modulated RSA/SHIFT Secured IFFT/FFT Based OFDM Wireless System

Sumathra T[1], Nagaraja N S[2], Shreeganesh Kedilaya B[3]

Department of E&C, Srinivas School of Engineering, Mukka, Mangalore

Abstract- **Traditional OFDM systems present some embedded features that may be exploited in order to intercept the wireless transmitted signal. However, such a possibility is not accepted in many applications where security is a very important issue. Chaotic sequences and encryption algorithms may be advantageous for secure communications. Hence in this paper we have proposed an algorithm for chaotic/RSA/shift secured IFFT/FFT based OFDM wireless system. Also we have studied the BER (Bit Error Rate) vs. SNR (Signal-to-Noise Ratio) performance in an AWGN wireless channel.**

***Key Words –RSA*, IFFT/FFT, OFDM, BER**

I. INTRODUCTION

The mobile or indoor radio channel is characterized by "multi-path reception". The signal offered to the receiver contains not only a direct line-of-sight radio wave, but also a large number of reflected radio waves. These reflected waves interfere with the direct wave, which causes significant degradation on the performance of the network. A wireless network has to be designed such a way the adverse effect of these reflections is minimized. Another critical design objective is high spectrum efficiency. The latter should ensure that the network can accommodate as many users as possible within a given frequency band.

The effects of (multi-path) radio propagation, modulation, and coding and signal processing techniques on the spectrum efficiency and performance of wireless radio networks are to be studied, in particular Orthogonal Frequency Division Multiplexing (OFDM) and related transmission methods[1,2]. OFDM is significantly less sensitive to inter-symbol interference, because a special set of signals is used to build the composite transmitted signal. The basic idea is that each bit occupies a frequency- time window ensures little or no distortion of the waveform. In practice it means that bits are transmitted in parallel over a number of frequency non-selective channels.

But the multimedia information is not secured in the wireless environment compared to that of wired environment. So, there is a need to encrypt the information and transmit over wireless medium and then receive the encrypted information from the wireless medium to recover the original information by using a decryption method. Cryptosystems have evolved from the two basic classifications: the Symmetric Key Cryptography (SKC) and the Public Key Cryptography (PKC).

Chaotic sequences are advantageous for secure communications. . In case of chaotic modulation chaotic signals are used as basis functions instead of sinusoids. Many different chaotic communications systems have been proposed: chaotic modulation, chaotic masking, chaos shift keying (CSK) and its variants, spread spectrum techniques, etc. (see [3], [4] for a review).This modulation technique shows good performance under noisy conditions, but can suffer severe degradation in channels with multipath distortion and selective fading. This problem is avoided by considering an OFDM communications system which sends the chaotically modulated signals in each subcarrier, instead of the usual PSK or QAM signals. Although a conventional modulation achieves a better performance in terms of bit error rate (BER), the proposed chaos-based scheme is advantageous in terms of secure communications: the BER of an eavesdropper without a perfect knowledge of the parameters of the chaotic system is highly deteriorated. Moreover, a class of chaotic map with a control parameter is discussed, which allows us to trade performance (i.e. BER) and security (i.e. chaotic behavior) in a natural way.

In this paper, we have combined both the symmetric key mono alphabetic shift ciphering and the public key RSA (Rivest, Shamir, and Adleman) ciphering which is combined with the future generation multimedia wireless systems of IFFT/FFT based OFDM. We have considered the merits of both SKC and PKC and eliminated the demerits of both SKC and PKC. This technique is able to encrypt/decrypt the text, audio and image signals (multimedia) in less time and at the same time it is very hard for the hackers to get the information which is being transmitted in the wireless medium [5,6]. Further in this paper, to increase the security we propose an efficient cryptosystem by using chaotic modulation based on the symbolic sequence associated to the chaotic map and backward iteration

The organization of our paper is as follows: Section II discusses about the encryption and decryption system, Section

III talks about the Walsh Hadamard Spreading code, section IV discusses about the wireless AWGN channel, Section V describes the chaotic communication system, Section VI briefs about the OFDM transmitter and receiver, Section VII discusses about the algorithm for the proposed work, Section VIII and IX discusses about some results and finally Section X concludes this paper.

II. ENCRYPTION AND DECRYPTION SYSTEM

The basic idea of our proposed cryptosystem is using the combination of both RSA and Shift cipher algorithms. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

The shift ciphering is a symmetric key cryptography algorithm using a shared key for both encryption (the cipher alphabet is the plain alphabet rotated left or right by some number of positions) and decryption and here the ASCII characters are substituted as numbers from 0 to 127 and they are shifted according to a key and the shifted numbers are transmitted and at the receiver the original numbers are obtained again by shifting using a key which is shared along with the transmitter key.

The advantages of PKC are: (1) removes the restriction of a shared symmetric key between two parties (2) reduces the number of keys required and very hard to break the code and the disadvantages of the PKC are: (1) it is more complex and used for short messages (2) the authentication of the user's public key [5]. Hence we have considered the merits of both SKC and PKC and eliminated the demerits of both SKC and PKC.

III. WALSH HADAMARD SPREAD SPECTRUM CODES

The most important purpose of the spreading codes is to help preserve orthogonality among different channels. Walsh codes are generated by applying the Hadamard transform to one by one dimensional zero matrixes repeatedly. The Hadamard transform is defined as:

$$H_1 = [1]$$
$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & \overline{H_n} \end{bmatrix}$$

This transform gives us a Hadamard matrix, H_n only for n=2i, where i is an integer. The Hadamard matrix is symmetric square-shaped matrix. Each column or row corresponds to Walsh code of length n. Every row of H_n is orthogonal to all other rows.

IV. WIRELESS AWGN CHANNEL

Since white noise is present in all communication systems, and is predominant noise source for many systems, the thermal noise characteristics of Additive, White, and Gaussian are most often used to model the noise in the detection process and in the receiver design. The channel is modeled as AWGN channel as its impairments to communication is a linear addition of wideband or white noise with a constant spectral density(expressed as watts per hertz of bandwidth) and a Gaussian distribution of amplitude. The wireless medium is a multipath fading type.

V. CHAOTIC COMMUNICATIONS SYSTEM

The structure of the whole chaotic communications system considered is shown in Fig. 1. The input bits are fed into a chaotic modulator with pre-assigned parameters *p* and *x*[*N*], which generates the baseband transmitted signal, *x*[*n*]. The main idea of the chaotic modulator [8] is to iterate backwards from a known final condition, *x*[*N*], using the input bits to construct the symbolic sequence. This chaotic sequence then passes through the channel, composed of a linear time-invariant (LTI) filter and additive white Gaussian noise (AWGN), resulting in a received signal *y*[*n*]. Finally, the chaotic demodulator tries to obtain the best estimate (i.e. the one with the minimum probability of error) of the transmitted bits using Viterbi decoding algorithm.

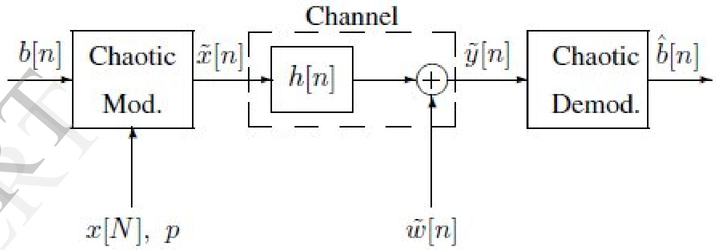

Fig. 1. Baseband chaotic communications system: modulator, channel, and demodulator.

VI. OFDM TRANSMITTER AND RECEIVER

Orthogonal frequency division multiplexing (OFDM) is a special case of multicarrier transmission, where a single data stream is transmitted over a number of lower rate subcarriers. OFDM can be seen as either a modulation technique or a multiplexing technique. One of the main reasons to use OFDM is to increase the robustness against frequency selective fading or narrowband interference. In a single carrier system, a single fade or interferer can cause the entire link to fail, but in a multicarrier system, only a small percentage of the subcarriers will be affected. Error correction coding can then be used to correct for the few erroneous subcarriers. OFDM is also spectrally efficient because the channels are overlapped and contiguous.

The OFDM modulation technique is generated through the use of complex signal processing approaches such as fast Fourier transforms (FFTs) and inverse FFTs in the transmitter and receiver sections of the radio. The block diagram of the

OFDM transmitter and receiver with chaotic modulation is shown in figure-2. In OFDM a block of N serial data symbols, each of duration Ts, is converted into a block of N parallel data symbols, each of duration T = NTs. The N parallel data symbols modulate N orthogonal sub carriers. Each bit stream obtained from the S/P converter is then modulated to a carrier. The modulated signals are then summed together before transmission on the channel.

The input bits are used to obtain the chaotic signal [8]. Then, a serial to parallel conversion is performed to generate the signal corresponding to each sub-carrier, pilots and guard symbols (zeros) are inserted, and an IFFT is performed.

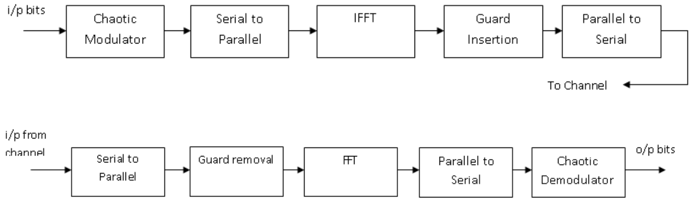

Fig-2: OFDM transmitter and receiver with chaotic modulation

VII. ALGORITHM

Step 1: Initialize all network parameters
Step 2: Generate random data and encrypt the data
Step 3: Spread the data with Walsh Hadamard code
STEP 4: chaotically modulate the signals.
Step 5: Convert the serial code stream into parallel format
Step 6: Place the chaotically modulated signals into the OFDM sub-carriers.
Step 7: Find the symbol time waveform using IFFT
Step 8: Add a Guard Period to each symbol time waveform
Step 9: Transmit the signal as frames
Step10: Channel is modeled to have Gaussian noise
Step11: Receive the signal frames
Step12: Find the spectrum of the symbols
Step13: Extract the used carriers from the symbol spectrum.
Step14: Convert the parallel code stream into serial format
Step15: Decode the signal using Viterbi decoding algorithm.
Step16: De-spread the data using the same Walsh Hadamard code
Step17: Receive data and decrypt the data
Step 18: Find BER from the received data
Step 19: Plot the results

VIII. OUTPUT USING DQPSK MODULATION

The text files (Input (Transmitter) [7], Output (Receiver) and the Cipher (Wireless Medium)) Shown below represent the results of RSA/SHIFT Secured IFFT/FFT based OFDM Wireless System with the OFDM model and with the RSA/SHIFT Secured method. The Output file was observed at SNR of 10 dB with two characters wrong but for SNR of 12 dB, the Output file was observed without a single error. The BER vs. SNR curve is plotted in Figure 3.

Input Text File:
Hello Sir,
Good Morning! How are you?
I will come at 10 AM!

Output Text File:
Hello Sir,
□ood Mor5ing! How are you?
I will come at 10 AM!

Chiper Text File:
□E□□□□□□□s□□□□□D□[□□□□□□□□
□□□□J□E□o□□□□□□□□□□□□□□□E□
J□□□□□□[□

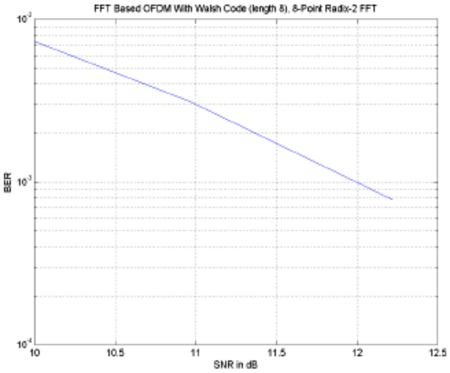

Fig- 3: BER Performance for “Text File”.

IX. OUTPUT USING CHAOTIC MODULATION

Fig. 4 shows the results [8] for the AWGN channel and four different values of *p*, with the OFDM+BPSK system used for comparison. As *p* is increased towards one the performance of the system approaches that of the conventional OFDM+BPSK modulation scheme. When *p* is decreased the BER increases, but an improvement in the level of security is achieved: since the amplitude for each symbol becomes more irregular and unpredictable, an unintended user who does not know exactly the parameters of the system will see his detection capability heavily impaired.

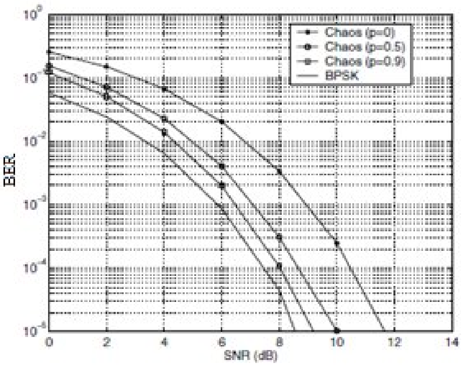

Fig. 4. BER for the OFDM system and AWGN channel.

X. CONCLUSION

It is showed in [8] that chaotically modulated signals are transmitted in the subcarriers of the OFDM system instead of conventional modulation schemes (BPSK, QAM or DQPSK), and the scheme showed considerable improvement in security. In [7] they have used RSA/SHIFT ciphering algorithm to secure the information transmitted using OFDM system, and this system is also proved secure. In our proposed scheme we have combined both chaotic modulation and RSA/SHIFT ciphering algorithm. Hence the proposed scheme is expected to give better security with little compromise in SNR Vs BER performance.

REFERENCES

1. Abiteboul, S. et al, 2000. *Data on the Web: From Relations to Semistructured Data and XML*. Morgan Kaufmann Publishers, San Francisco, USA.
2. Beck, K. and Ralph, J., 1994. Patterns Generates Architectures. *Proceedings of European Conference of Object-Oriented Programming.* Bologna, Italy, pp. 139-149.
3. M. P. Kennedy, R. Rovatti, and G. Setti, Eds., *Chaotic Electronics in Telecommunications*. CRC Press, 2000.
4. F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems*. Berlin: Springer-Verlag, 2003.
5. Bewley, William L, et al, 1983, The Origins of Spread Spectrum Communications. In IEEE Transactions on Communications, Vol. 22, No. 5, pp. 637-648.
6. Esmael H., et al, 1998, Spreading Codes for Direct Sequence CDMA and Wideband Cellular Networks. *In IEEE Communications Magazine.* Vol. 36, pp. 88-95.
7. D. Rajaveerappa,and Abdelsalam Almarimi, 2009, RSA/SHIFT secured IFFT/FFT based OFDM wireless System, proceedings of Fifth IEEE International Conference on Information Assurance and Security, pp. 208-211.
8. David Luengo and Ignacio Santamaria, 2005, Secure Communications Using OFDM with Chaotic Modulation in the Subcarriers, IEEE.