International Journal of New Technology and Research (IJNTR)
ISSN:2454-4116, Volume-3, Issue-8, August 2017 Pages 55-59

Improve Image Security Over wireless Sensor Network

Wa'il A. H. Hadi, Hayder F. Y. Hussein, Safa A. A. Abass

***Abstract*— The major weaknesses of Wireless Sensor Network is the energy consumption, because the difficult battery replacement or recharge . The energy consume can be regulator by more than one layers. In this paper goals to reduce the energy consume in the physical layer, because the most of the energy consume occurs in the physical layer. This reduce will be achieved via the use of Zigbee transceiver standard at the physical layer with the reduced complexity and lower power consumption than other system used in wireless sensor networks. Furthermore, such use will also enhance energy efficiency and bit error rate of the wireless sensor network. In this paper will apply the chaotic interleaver and chaos encryption to get best encryption (two level encryption) and reducing in time processing and enhancement simulation for bit error rate and peak signal to noise ration by transceiver image cameraman though an AWGN and Rayleigh fading channels are displayed.**

I. INTRODUCTION

In latest years, with advance of Wireless Sensor Networks and multimedia technology, multimedia data are use extra broadly in human society and most of these signals are redundant. At other side, transmission channel is always insecure and bandwidth constrained some multimedia data containing (education, politics, militaries,economies, industries,…. etc.) This is necessary by providing protection of confidentiality, integrity and availability [1].In order to protect multimedia content, an effective method of encrypting information security has been adopted in many practical applications. Most of these applications have become increasingly challenging, due to the number, of constraints such as; The limitation of storage in memory, bandwidth, and unreliable timing requirement .Then, these data usually need to be encrypted and compressed for efficient security, storage and transmission [2]. many different systems are proposed in image security as an attempt to enhance the performance of Wireless Sensor Networks.
First, the security features of the system are described by the two-level security (two-dimensional encryption). And the bit error rate performance of different systems are presented. The throughput and energy efficiency evaluation of the systems are then introduced. This has been achieved by using ZigBee transceiver protocol (at the physical layer) with and without using chaotic interleaver and chaos encryption.

Wa'il A. H. Hadi,University of Technology, Dept. of Elec. Eng. Baghdad – Iraq.
Hayder F. Y. Hussein,University of Technology, Dept. of Elec. Eng. Baghdad – Iraq
Safa A. A. Abass,University of Technology, Dept. of Elec. Eng. Baghdad – Iraq

II. ZIGBEE PACKET FORMAT

Thestructure ofZigbee Packet is shown in figure (1). Thethree parts areconsists in the header, preamble 32-bit to synchronization, start of packet delimiter 8-bits to signify end of preamble, and PHY header 8-bit to specify length of PSDU [7]

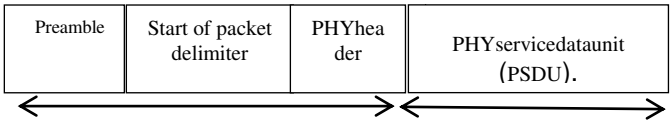


Figure 1. Format for ZigBee packet. [7]

Thelength of Payload field contains 0-127 bytes. TheusedZigbee network to detect the error retransmission technique. To create sure a successful transceiver of data, an acceptable frame delivery protocol is supported to transfer reliability is increasing[8]. The DSSS technique is using in ZigBee network for data transmission is shown in the table (1), The immunityit's increasing against interfering. The built of original bit streamit is multiplicationwitha wideband (PN) spreading code, which is created in a wideband continuous time scrambled signal. The DSSS technique immune the protection against interfering signals, it also offersthe ability to multiple access, when they were used the different spreading codes, it also provides security between transmitter and receiver. The DSSStechnique 32-chip PN sequences is also used as a technique to generated ultra wideband signals [9]. Is shown in figure (2) [10], the m(t) has a very greatly bandwidth than the input signal d(t) [11,12].

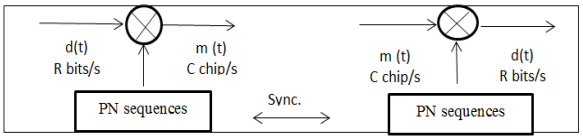


Figure 2.The DSSS technique[10]

Table I.Zigbee symbol to chip mapping [13]

ZigBee symbol	Chip value
0000	11011001110000110101001000101110
1000	11101101100111000011010100100010
0100	00101110110110011100001101010010
1100	00100010111011011001110000110101
0010	01010010001011101101100111000011
1010	00110101001000101110110011100
0110	11000011010100100010111011011001
1110	10011100001101010010001011101101
0001	10001100100101100000011101111011
1001	10111000110010010110000001110111
0101	01111011100011001001011000000111
1101	01110111101110001100100101100000
1011	00000111011110111000110010010110
1011	01100000011101111011100011001001
0111	10010110000001110111101110001100
1111	11001001011000000111011110111000

III. CHAOTIC INTERLEAVING

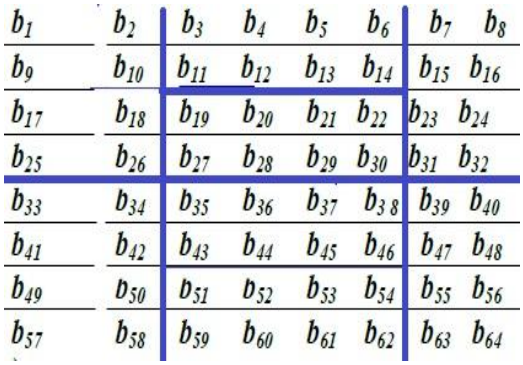
The presentedidea for chaotic interleaver by use the logistic map [14]. the Baker map is used to randomize the bits 2-D shape,. Let B (n_1,…….,n_k), indicate the discretized of map, Where thekey secret, S_{key}itis vector [n_1,……,n_k], must be known the complete numbers of the data items in one row, the S_{key} is selected to make each integer n_i divides N, And must (n_1+…… + n_k = N). Let (N_i = n_1 +…..… + n_{i-1}). The data items at the indices (r, s), is moving to the indices .

$$B(r,s) = [\frac{N}{n_i}(r - N_i) + s \bmod (\frac{N}{n_i}), \frac{n_i}{N}(s - s \bmod (\frac{N}{n_i})) + N_i]$$

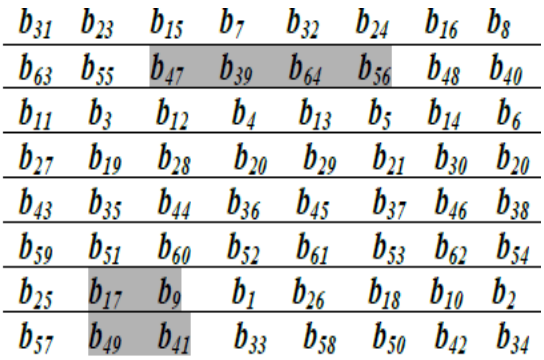
Where is $Ni \le r < N_i + n_i$, $0 \le s < N$, and N_1=0. The followsit is steps in the chaotic permutation:

1. The image cameraman is square shape N * N divided into N rectangles with width rectangle n_i and number of elements N.
2. Each rectangle from elements will be rearranged into a row in the permuted rectangle. The elements are taken first from left to right with lower elements then upper ones.
3. Within each element, the selecting procedure begins from the bottom left corner to upper elements.

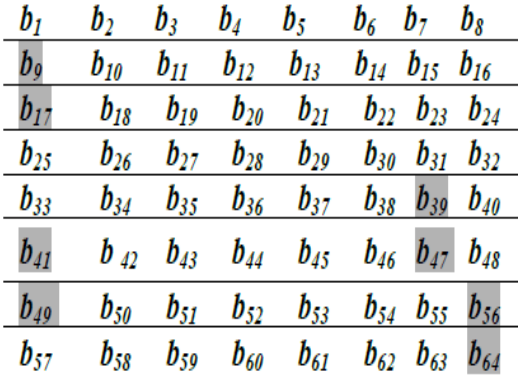
Figure (3) is shown for backer map chaotic interleaver for a 8 × 8 square matrix (i.e. N = 8). The S_{key} = [n_1, n_2, n_3] = [2, 4, 2].



(a)



(b)



(c)

Figure 3. Chaotic interleaving of an 8×8 matrix:
(a) the 8×8 matrix divided into rectangles,
(b) chaotic interleaving of the matrix,
(c) effect of error bursts after de-interleaving. [10]

IV. SCRAMBLING BY CHAOS ENCRYPTION

The map is development function that exhibitions some sort of chaotic behavior. Chaotic maps may be parameterized by a discrete-time. Discrete maps usually take the form iterated functions. Chaotic maps often occur in the study of dynamically systems [12,14]. The well-known chaotic map such as logistic map [14], which is time series map manufactured by the following equation.

$$X_{k+1} = 1 - 2X_k^2 \quad \ldots\ldots\ldots\ldots\ldots \quad (1)$$

The advantages of this design are simplicity. But the sor method may be time consumed especial in their large frame i is required $k(k-1)/2$ of comparison to sorting the samples.

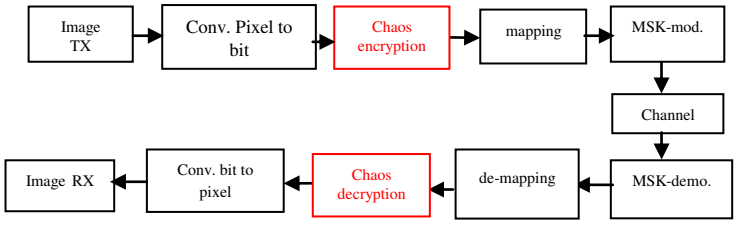


Figure 4.Block diagram of image encryption

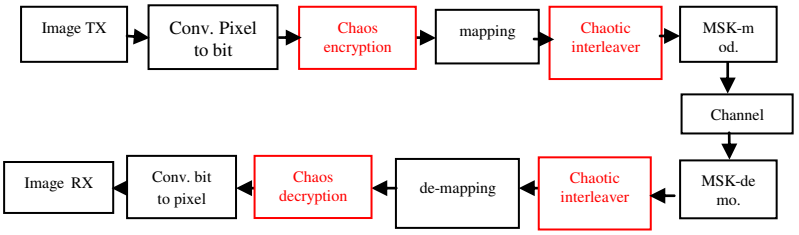


Figure 5.Block diagram of bit Chaotic Interleaver

V. PROPOSED MODIFICATIONS

The specifications of 802.15.4 Zigbee transceiver worked in 2.4 GHz. The data modulation scheme used here is DSSS technique (32-chip PN sequences) minimum shift keying (DSSS-MSK). The block diagram of 802.15.4 Zigbee transceiver system includes spreading and modulating of input bits. In the first stage, the coming encryption bits are grouped into four bits, so it denotes to a Zigbee symbol. These four bits are used to select one of the 16 orthogonal (PN) sequences to the transmitter. The PN sequences are related to each other through cyclic shifts and the successive selected PN sequences are concatenated and sent to the MSK modulator. The waveform in MSK modulation technique is nonstop in phase, hence, there are no sudden changes in waveform amplitude. The side lobes of MSK are very small. Consequently, bandpass filtering is not needed in MSK modulation to avoid interference. The medium with burst error characteristics decreases the performance of error correction and peak signal to noise ratio. This problem can be solved by using the scrambling in chaotic interleaver as shown in figure (4) and figure(5). The logistic map encryption will apply over pixel or bits because small size frame samples that not need large time to sort . And chaotic interlever will apply over the chip. The aim of using scrambling by chaotic interlever to prevent the focused burst error in one place within the received image by distributing this error along stream data and can be corrected in demoing through converted from chip to bit.

VI. SIMULATION RESULTS

The computer simulations results are presented. The importance used in a simulation, the transceiver packet if an error results in any parts will be discarded. The channel used AWGN and Rayleigh fading channel. Jake's model, assume mobile speed is 10 miles/hour, frequency carrier is 2.46GHz. The image cameraman is transmitted over an AWGN channel with SNR= 0 dB. Three scenarios are presented, no encryption image, image encryptions by chaos system and image encryptions by chaos system and apply chaotic interleaver over chips. The results used AWGN channel are shown in Figure (6) The image (c), it's have PSNR=29.69dB which is more clarify from other images because the chip scrambling by using chaotic interleaver the segmentation and distribution burst error on the stream data and can be a correction by de-mapping in using DSSS technique. Replace this experiment by transmitted image over Relight channel with SNR= 5 dB The results are shown in Figure (7).

(A)

(B)

(c)

Figure 6. Receiving image cameramanover AWGN channel at SNR= 0dB with (a) PSNR = 22.15dB, (b) PSNR = 22.48dB, and(c)PSNR = 29.69dB.

(A)

(B)

(c)

Figure 7. Receiving image cameraman over Rayleigh fading channel at SNR= 5dB with (a) PSNR = 22.51 dB, (b) PSNR= 22.68dB, (c) and(d) PSNR= 39.68dB.

The sent image cameraman in SNR values and display in the figure(6) and figure(7). The image cameraman(a) send the cameraman image in the normal case (without any encryptions and interleaver) and show the effect of the burst error on the image cameraman in badly. In image cameraman(b) will distribution the burst error in bits by chaos encryption in all the image process and this leads to clarity for cameraman image with remaining on the same values PSNR approximation. But in image cameraman(c) and the final processing apply over chip by chaotic interleaver, it is the distribution of burst error will lead to correct the error and clarity of the image dramatically with an increase in the value of PSNR.

The medium with burst error characteristics decreases the performance of error correction and so the retransmission is increased. This problem can be solved by using the Scrambling in the chip. Therefore, it has been suggested that the chaotic interleaver will be added to the transmitter of the system after spread spectrum (chip Scrambling) to improve BER, throughput, and energy efficiency performance of the systems mentioned, shown in figure(8) and figure(9).

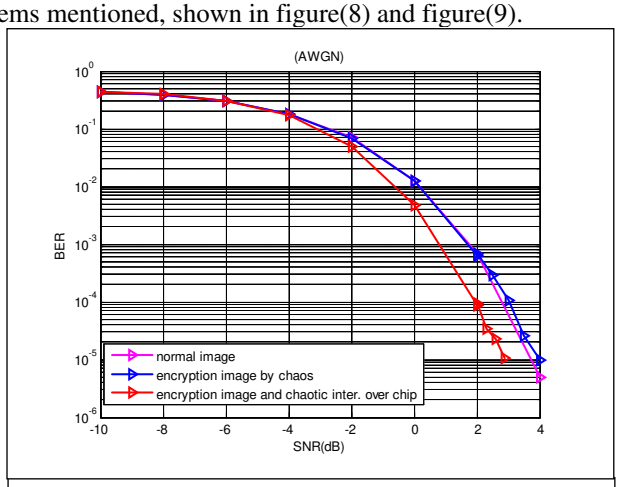


Figure 8. BER against SNR for the received cameraman image over AWGN channel.

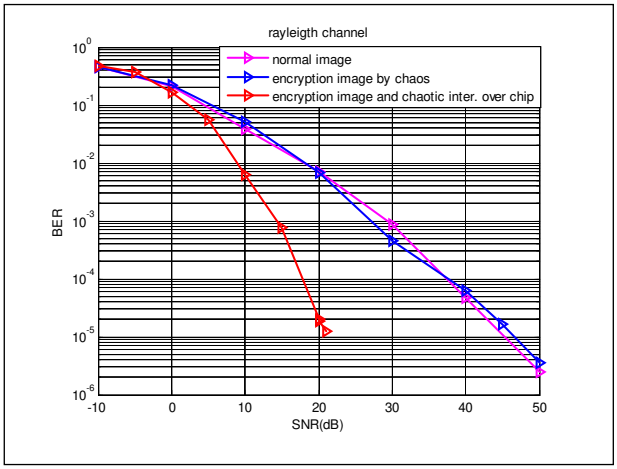


Figure 9. BER against SNR for the received cameraman image over Rayleighfading channel.

VII. . CONCLUSION

The show result in Multimedia Wireless sensor networksof the Zigbee transceiveris calculated in terms of Symbol BER and PSNR.These parameters are measured under various conditionssuch as AWGNchannel and Rayleigh fading channel.The simulation results display that the perform of Zigbee transceiver is better under AWGNchannel and Rayleigh fading channel with add chaotic interleaver applied over the chip. Also, the enhanced chaotic interleaver security level over the Zigbeetransceiver network link.

REFERENCES

[1] Salah IbrahemSowan," Steganography For Embedding Data In Digital Image",2003,M.Sc. thesis in University Putra Malaysia.
[2] Seyyed Mohammad Reza Farschi · H. Farschi," A novel chaotic approach for information hiding in image", Nonlinear Dyn , Springer Science+Business Media B.V.,2012,(IVSL)
[3] S. Vafi and T. Wysocki,“Performance of convolutional interleavers with different spacing parameters in turbo codes”, in Proc. 6th Australian Commun. Theory Worksh., Brisbane, Australia, 2005.
[4] G. Pekhteryev, Z. Sahinoglu, P. Orlik, and G. Bhatti, “Image transmissi3on over IEEE 802.15.4 and ZigBee networks”, in Proc. IEEE ISCAS, Kobe, Japan, 2005.
[5] L. Ozarow, S. Shamai, and A.D. Wyner,“Information theoretic considerations for cellar mobile radio”, IEEE Trans. Veh. Technol.,vol. 43, pp. 359–378, 1994.
[6] E. N. Farag and M. I. Elmasry, Mixed Signal VLSI Wireless Design Circuits and System. Kluwer, 1999.
[7] T. S. Rappaport, Wireless Communications. Prentice Hall, 1996.
[8] Tubaishat, M.; Madria, S. Sensor networks: an overview. IEEE Potentials 2003, (22), 20‑ 30.
[9] Y. Dong, L. Liu, C. Zhu, Y. Wang, Image Encryption Algorithm Based on Chaotic Mapping. 3rd IEEE International Conference on Computer Science and Information technology, ICCSIT, 2010.
[10] M. Salleh, S. Ibrahim and I. F. Isnin, Enhanced chaotic image encryption algorithm based on Baker's map. IEEE Conference on Circuits and Systems, Vol.2, pp.508-511, 2003.
[11] N. Lemma, J. Aprea, W. Oomen, and L. V. de Kerkhof, A Temporal Domain Audio Watermarking Technique. IEEE Transactions on Signal Processing, Vol. 51, (4), pp. 1088-1097, 2003.
[12] W. Li, X. Xue, and P. Lu, Localized Audio Watermarking Technique Robust Against Time- Scale Modification. IEEE Transactions on Multimedia, Vol. 8, (1), pp. 60-69, 2006.
[13] Li-fang He, Gang Zhang “A Chaotic Secure Communication Scheme Based on Logistic Map”, International Conference on Computer Application and System Modeling, IEEE, PP.589-591, 2010.8.
[14] J. Fridrich, “Symmetric ciphers based on two- dimensional chaotic maps,” International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, Vol. 8, No. 6, pp. 1259-1284, 1998.