Image Security Over Wireless Sensor Network

Wa'il A. H. Hadi*,Ph.D.(Asst.Prof.) Haydar F. Y. Hussein*

Abstract

To secure the multimedia information, cryptography is an active method for information Security has been utilized in some practical techniques. Most of these techniques have become widely challenging, due to a number of weaknesses such as,the limitation of storage in memory, bandwidth, and the unreliability of the timing requirement. Besides, these data usually needs to encryption and compression for efficient security, storage and transmission.

One of the major weaknesses for wireless sensor network is the energy consumption, because of the battery replacement or the difficult recharging. The energy consomption can be controlled by more than one layer in WSNs. This paper, focused on the image security with major enhancement on the energy consumption over physical layer, because most of the energy consumption occur in this layer. The reduction will be accomplished by using the Zigbee transceiver standard at the physical layer with the minimum complexity and lower power consumption than other system used in wireless sensor networks. Additionally, such use will also improve energy efficiency and bit error rate of the wireless sensor network. Also the chaos system was applied to the pixels, bits and chips. The enhancement simulation for bit error rate and peak signal to noise ratio by transceiver image cameraman through an AWGN and Rayleigh fading channels are displayed. The enhanced transmitting image by 5 dB signal to noise ratio on the Rayleigh fading channel, an improvement on the peak signal to noise ratio of the received image from 23.5 dB to 37 dB can be observed.

Keywords; Wireless sensor networks,IEEE 802.15.4, ZigBee,,Automatic repeat request (ARQ), BER.

*University of Technology

1. Introduction

In the last years, with advance of wireless sensor networks and multimedia technologies, multimedia data such as (image, audio and video) are widely used in human society and most of these signals are redundant. On the other hand, the channels are usually insecure and bandwidth constrained some multimedia data containing (politics, economies, militaries, industries, education…. etc .) This is necessary to providing protection of confidentiality, integrity and availability [1].In order to protect multimedia content, an effected method for the information security has been adopted in many practical applications. Most of these applications have become increasingly challenging, due to anumber, of constraints such as; The limitation of storage in memory, bandwidth, and the unreliability of the timing requirement. Besides, these data usually needs to encryption and compression 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 bit error rate performance of different system are presented. The throughput and energy efficiency evaluation of the system are introduced. This has been achieved by used ZigBee transceiver protocol (at the physical layer) with and without used chaos encryption .

2. Zigbeepacket format

The Zigbee Packet structure is shown in figure (1). The header consists of a three parts, 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 [3]

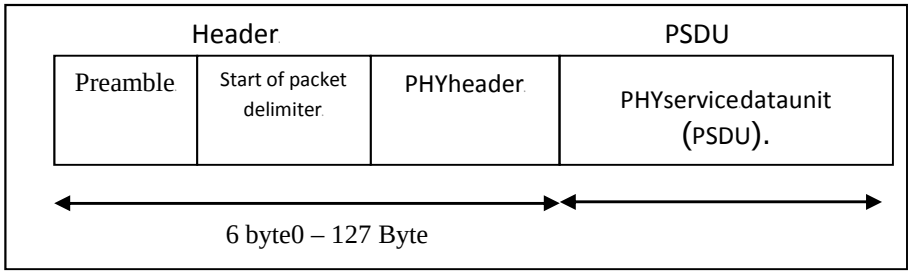


Figure 1. Formats for ZigBee packets [3].

The Payload field contains a length of 0-127 bytes. The ZigBee networks is used to detect the error retransmission technique. To make sure a successful receiver of data, an allowed frame delivery protocol is supported to increase the transfer reliability [4]. The ZigBee network uses the DSSS technique for data transmission shown in table (1), it increases the immunity against interference. The multiplication process of the original bit stream with the wideband (PN) spreading code was done to produce a wideband continuous time scrambled signal. DSSS technique improves the protection against noise signals.Also, This process offers the ability to multiple access, when they being used the some different spreading codes, it also provides security for a transceiver. DSSS 32-chip PN sequences technique is used as a technique to generate ultra wideband signals. As shown in figure (2) [5], the m(t) has a wider bandwidth than the input signal d(t) [6,7],

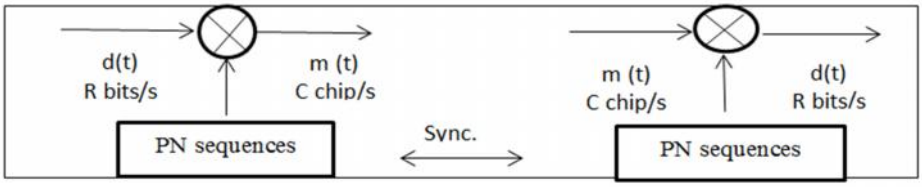


Figure 2. DSSS technique [5]

Table I. Zigbee symbol to chip mapping [8]

ZigBee symbol	Chip value
0000	11011001110000110101001000101110
1000	11101101100111000011010100100010
0100	00101110110110011100001101010010
1100	00100010111011011001110000110101
0010	01010010001011101101100111000011
1010	00110101001000101110110110011100
0110	11000011010100100010111011011001
1110	10011100001101010010001011101101
0001	10001100100101100000011101111011
1001	10111000110010010110000001110111
0101	01111011100011001001011000000111
1101	01110111011100011001001011000000
1011	00000111011110111000110010010110
1011	01100000011101111011100011001001
0111	10010110000001110111101110001100
1111	11001001011000000111011110111000

3. Scrambling by Chaos encryption

The behaviors that have association with the increase of a nonlinear physical system is chaotic which happen for certain values of system parameters. From the perspective of differential equations, the chaotic system is called the flow, and in the difference equation, called the map. The improvement of these non-static system is defined by trajectory and orbit. The course taken by a flow as time progresses is regarded as a trajectory, and a collection of points moved over a map/going on iteration [9].

Mapis a development function that exhibit as equence of chaotic behavior. Chaotic maps may be parameterized by a discrete-time. Discrete maps usually take the form of iterated functions. Chaotic maps often occur in the study of dynamically systems. The well-known chaotic map such as logistic map, which is time series map manufactured by the following equation[10].

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

4. 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 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 logistic map encryption. The aim from using scrambling 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.

4.1 Chip scrambling by chaos encryption

By using DS/SS special case in ZigBee. The income bits stream that will be divided to this 4 bits symbols and replace to 32 chip. That will permutation chip to get best security from other. The chips are permuted with the key in sender and receiver. The encryption image is obtained from the chip permutation which is transmitted to the receiver shown in figure (3).

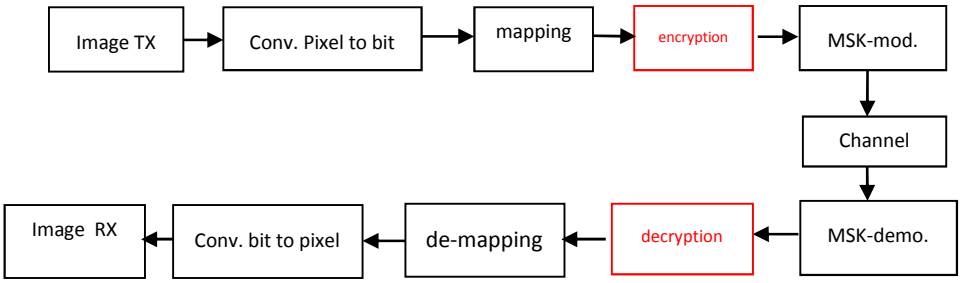


Figure 3.Block diagram of chip chaos encryption

4.2 Bits scrambling by chaos encryption

The image can be seen as a matrix of pixels, each 8 bits represented 256 gray levels. In the bit permutation, the bits in pixel are permuted with the key fixed in sender and receiver, as shown in figure (4) . The encrypted image is obtained from the bit permutation which is transmitted to the receiver through the insecure channel. At the receiver, the encrypted image is decrypted by using the same protocol.

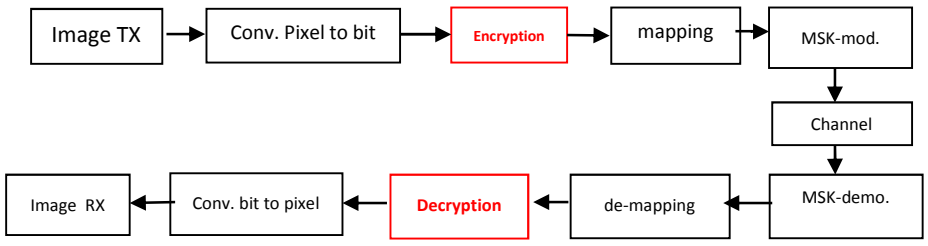


Figure 4.Block Diagram of bits chaos encryption

The encryption and decryption procedure is thesame as in the bit permutation. The only difference is that permutation bits and the pixels contain an 8-bits. Here, there will be permutation between pixels. The pixels in the image are permuted using the key selected show in figure(5) .

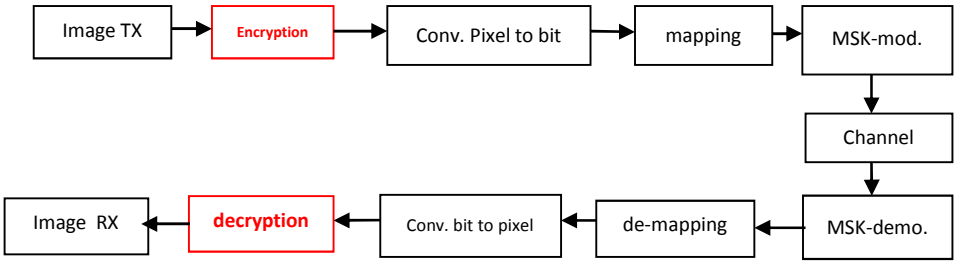


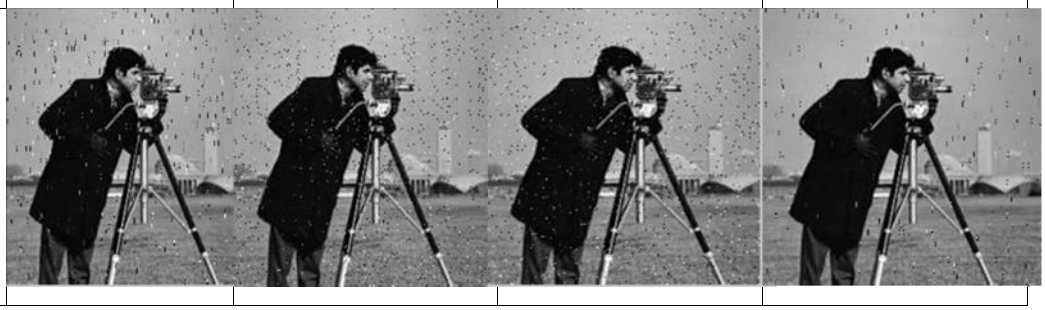
Figure 5.Block diagram of pixel chaos encryption

5. Simulation Results

The simulation result can be summarized by:

1. This Simulation results have been proposed algorithm by using Matlab Cameraman image shown in figure(6) and figure(7) over AWGN and Rayleigh fading channel.
2. Rayleigh fading channel in SNR= 5 dB by Jake's model will be used, assuming mobile velocity 10 miles/hour, frequency carrier 2.46 GHz. It has been consider in some simulation tests the image is transmitted.
3. Four scenarios are presented:
   - 3.1. At the transmitter side the cameraman image will transmitted without any encryption in the first time.
   - 3.2. Scrambling pixel by using chaos system in logestic map.
   - 3.3. Scrambling bit by using chaos system in logestic map.
   - 3.4. Apply scrambling chip by chaos system in logisticmap.
4. The resultsshown in figure (7). The chip scramling image have PSNR=36.8778dB, whichis more clarify fromother images because the chip scrambling will segmentation and distribution burst error on the stream data and can be corrected by de-mapping with DSSS.

5. By repeating the sametestson the transmitted image over AWGN Channel with SNR= 0 dB,this results are shown in figure(6).
6. It has been sent cameraman image with a number of SNR values. The image (a) send the cameraman image in normal case (without any encryptions) and appear the effect of the burst error on the received image. In the image (b) and (c), the burst error was choped and distributed by scrambling the pixels and bits in all the image size and this leads to clarify the image with approximty the same values PSNR. But in image (d) the final processing apply over chip,the burst error was choped and distributed, which is lead to correct the error and clear the image dramatically by increasing the values of PSNR.

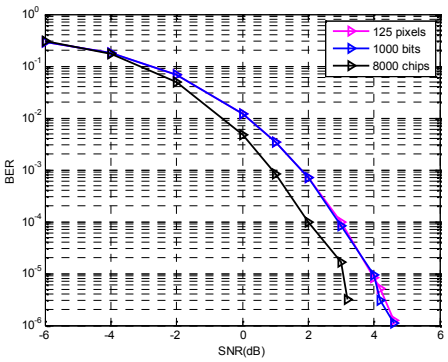
SNR	a-normal	b-pixel Scrambling	c-bits Scrambling	d-chip Scrambling
0 dB				

Figure(6) Receiving image cameraman over AWGN channel at SNR = 0dB with (a) PSNR = 23.171dB, (b) PSNR = 23.429dB, (c) PSNR = 23.678dB, and (d) PSNR = 28.087dB.

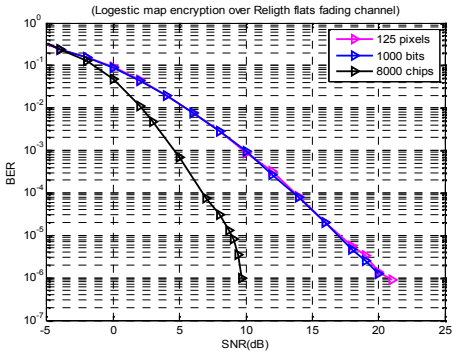
SNR	a-normal	b-pixel Scrambling	c-Bits Scrambling	d-chip Scrambling
5 dB				

Figure(7) Receiving image cameraman over Rayleigh fading channel at SNR = 5dB with (a) PSNR = 23.487 dB, (b) PSNR = 23.359dB, (c) PSNR = 23.650dB, and (d) PSNR = 36.8778dB.

7. The medium with burst error characteristics decreas the performance of error correction and increase the re-transmission process. This problem can be solved by using the scrambling in chaos system. Therefore, it has been suggested that, the logestic map encryptions will be add to the transmitter after spread spectrum (chip scrambling) to improve BER, throughput and energy efficiency performance of the systems mentioned in figure(8) and figure(9)



Figure(8) performance of chaos encryption over AWGN channel.



Figure(9) Performance of chaos encryption over Rayleigh channel.

6. Conclusion

The previous results of this work can be concluded by the following:

- The performance analyses of the Zigbee transceiver in Wireless Multimedia sensor networks is studied in terms of Symbol BER and PSNR.
- The encryption algorithme permutation built on sorted way because it's values increase or decrease in sequence (smooth change).
- Generating a vector of values,which are initially sorting either ascending or descending by one of these methods. This lead to decreas the error and decreas the re-transmission. Therefore, this improvement in performance will achieve power reduction.
- The permuting cannot combining the two advantages (security and real time) at the same time.

Reference

[1]. Salah IbrahemSowan," Steganography For Embedding Data In Digital Image",2003,M.Sc. thesis in UniversitiPutra Malaysia**.**

[2]. Seyyed Mohammad RezaFarschi · H. Farschi," A novelchaoticapproach for information hiding in image", Nonlinear Dyn , Springer Science+Business Media B.V.,2012,(IVSL)

[3]. S. Vafi and T. Wysocki,"Performance of convolutionalinterleaverswithdifferentspacingparameters in turbo codes", in Proc. 6th Australian Commun. TheoryWorksh., Brisbane, Australia, 2005, pp. 8–12.

[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 theoreticconsiderations 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]. S. Pasupathly, "Minmum Shift Keying: A Spectrally Efficient Modulation", IEEE Communication Magazine, 1979.

[9]. Edwardott "Chaos DynamicalSystems" CAMBRIDGE University, second edition, 2002

[10]. Li-fang He, Gang Zhang "A Chaotic Secure Communication SchemeBased on LogisticMap", International Conference on Computer Application and System Modeling, IEEE, PP.589-591, 2010.8

تشفير الصورة في شبكات الاستشعار اللاسلكية

حيدر فاضل ياسين* أم.د. وائل عبد الحسن هادي*

المستخلص

يعد استهلاك الطاقة في شبكات الاستشعار اللاسلكي هي النقطة الاضعف وذلك لان شبكات الاستشعار اللاسلكية محدودة الطاقة من خلال استعمالها لمصدر التيار المستمر (البطارية) والذي يكون في بعض الاحالات من الصعب اذ لم يكن من المستحيل شحن البطارية او استبدالها بسبب مواقع توزيع هذه المتحسسات . ان استهلاك الطاقة في منظومات الاستشعار اللاسلكي يمكن السيطرة عليه في عدد من الطبقات . في هذه الورقة عن طريق تشفير الصورة نعمل على تقليل استهلاك الطاقة في الطبقة المادية (physical layer) لأنها الطبقة الاكثر استهلاك للطاقة من الطبقات الاخرى. وذألك من خلال استخدام (zigbee device) مع بعض التقنيات للحصول على نظام أعلى كفاءة للطاقة ,وأقل نسبة خطأ.
استخدمت العديد من التطبيقات العملية في تشفير محتويات الوسائط المتعددة و التشفير هي الوسيلة الفعالة في أمن المعلومات المستخدمة. أصبحت معظم هذه التطبيقات صعبة على نحو متزايد، ويرجع ذلك إلى عدد من المعوقات مثل: الحد من التخزين في الذاكرة (memory) ، وعرض النطاق الترددي (bandwidth)، والتأخير في عمليات التشفير (delay). وقد تم التحقيق نظرية الفوضى على نطاق واسع وخاصة لتطوير خوارزميات تشفير الصور. في هذه الورقة سوف يتم تطبيق نظام الفوضى على الصور في بعض الطرق المختلفة للحصول على اعلى تشفير للصورة واقل خسائر في (BER) .

*الجامعة التكنولوجية