A New Chaotic Encryption Algorithm to Enhance the Security of ZigBee and Wi-Fi networks

Bassem Bakhache
LASTRE – Centre Azm pour la Recherche en Biotechnologie et ses applications, EDST, Lebanese University, Tripoli, Lebanon

Kassem Ahmad, Safwan el Assad
IREENA - Ecole polytechnique de l'Université de Nantes, Rue Christian Pauc, B.P 50609, 44306, Nantes, France

Abstract

Wi-Fi and Zigbee networks are widely deployed in wireless industrial control and monitoring applications. The security protocols used in these wireless networks rely on stream cipher to encrypt data before being transmitted. These protocols are secure but they don't respect the real-time requirement of industrial control. Chaotic systems are able to produce stream cipher with higher randomicity, which looks like stochastic noise. Based on two perturbed piecewise linear chaotic map (PWLCM), we propose a new high speed chaotic cryptographic scheme. It requires a little memory capacity, and also appears to be very secure. The proposed generator is easily realized and succeeds all the statistical tests. In this paper, we will explain briefly the design of our proposed generator and show its efficiency through encryption tests.

1. Introduction

With the development of industrial automation, there is an imminent demand to establish a secured wireless network, so the data can be exchanged reliably and wirelessly to some moving equipments for example, where cables can't be used Wi-Fi and Zigbee are widely deployed in wireless industrial control and monitoring applications. The transmission of data in a Wireless network is done by means of electromagnetic wave, so all nodes can receive these data, if they are within range of this wave. If the network is not secured, an adversary could modify and inject messages to either trigger an alarm, or worse, to suppress legitimate alarm signals. Therefore the encryption of important industrial data control should be done before transmission. Furthermore, real time data exchange is a very important criterion in industrial control systems and it is for some applications an essential requirement to be respected absolutely. Additionally, the sensors deployed in industries, like ZigBee equipments, are often devices characterized by a little memory and cannot support a complex encryption algorithm which needs high hardware configuration.

The Wi-Fi, or IEEE 802.11, was designed for local area networks such as: houses, companies, or factories networks. In fact, industries are employing more varied applications based on several variants of Wi-Fi (802.11a, 802.11b, 802.11g, etc..) which offers different data rates from 11Mb/s to more than 100 Mb/s. WEP (Wired Equivalent Privacy) was the original encryption standard for IEEE 802.11. It is very simple to implement [1] and it uses the RC4 algorithm (stream cipher). Unfortunately, the WEP has some weaknesses and it was cracked after less than three months of its design. Therefore, WEP is insufficient for ensuring data privacy; nevertheless, it is still used to ensure a minimum level of security.

Therefore, the WPA (Wi-Fi Protected Access) protocol was defined as an intermediate measure to take the place of WEP, pending the preparation of the security standard 802.11i. The WPA is based on TKIP (Temporal Key Integrity Protocol) protocol, itself based on RC4, and it was conceived to be implemented in the existing equipments. As the TKIP was developed on the same basic mechanism of WEP, flaws were discovered in this protocol, and it was cracked. The final security protocol WPA2 was designed to replace the WPA and to fulfill the mandatory requirements of the IEEE 822.11i standard. It introduces CCMP (Counter mode with Cipher block chaining Message authentication code) Protocol relying on the AES (Advanced Encryption Standard) encryption algorithm applied with the counter mode CTR. The AES is extremely robust, reliable and secure, and consequently the WPA2 remains untouchable. But unfortunately, the AES is very complex, and it needs a high power and high time consumption. For this reason the WPA2 can be implemented only on recent and powerful Wi-Fi material with new drivers and new operating systems, and does not operate on old generation equipments.

ZigBee network based on the IEEE 802.15.4 standard, targets: personal area and sensor networks. It is a low-cost, low-power, wireless mesh networking [2]. First, the low cost allows the

technology to be widely deployed in wireless control and monitoring applications. Second, the low power-usage allows longer life with smaller batteries. Third, the mesh networking provides high reliability and more extensive range.

ZigBee has a lower data rate (250 kb/s) than other digital radio standards, and it can include up to 65000 nodes per network. The 802.15.4 specification defines eight different security suites classified by the properties that they offer: no security, encryption only, authentication only, and encryption and authentication. Each category [3] that supports authentication comes in three variants depending on the size of the MAC (Message Authentication Code) that it offers. Each variant is considered a different suite and has its own name, but all the offered suites encrypt the data using the AES encryption algorithm with counter mode CTR.

Therefore, the security of Wi-Fi and ZigBee, is based on two algorithms: RC4 (for Wi-Fi), and AES-CTR (for Wi-Fi and ZigBee). The first algorithm presents vulnerabilities, then it is not very secure; the second one is highly secure but it has a very complex algorithm, time-consuming and high memory capacity, then it does not meet the real-time requirement of industrial control. On the other hand, chaotic functions show numerous interesting properties. The iterative values generated from such functions are completely random in nature, although limited between bounds. The close relationship between chaos and cryptography makes chaos as a natural candidate for secure communication. The chaotic signals possess many desirable features, such as pseudo-randomness, ergodicity and sensitivity to the initial value. All these features enable chaos based encryption to achieve better confusion and diffusion. Chaos encryption scheme was proposed [4] for ZigBee network. It relies on modified logistic maps. This scheme is secure and fast, but it is breakable because of the weak chaotic maps used. A new robust and fast chaotic algorithm must be developed for wireless network industrial control and this is the target of this paper.

This paper is organized as follows: in the next section, the encryption schemes used in Wi-Fi and ZigBee networks are investigated. These schemes are analyzed in section four. In section IV we present the chaotic cryptographic and the dynamical degradation caused by the digitization of the chaotic maps. The section five describes the proposed generator and its properties, and we explain the proposed encryption scheme. Test and analysis are presented in section six. Finally, conclusions are made in the last section.

2. Wi-Fi and ZigBee: encryption analyzing

Let us analyze how RC4 and AES-CTR work and how they are applied in their own networks.

2.1. RC4 encryption

The RC4 is the most widely-used software stream cipher. It is used in popular protocols such as: SSL (Secure Sockets Layer) and TLS (Transport Layer Security), and in several protocols like: BitTorrent protocol encryption, Microsoft Point-to-Point encryption, secure shell (optionally), oracle secure SQL, Kerberos (optionally), Remote Desktop Protocol, SASL Mechanism Digest-MD5 (optionally). It requires a shared secure key (between 5 and 16 bytes) called RC4 key. The role of RC4 [1] is simply to produce an endless series of pseudo-random bits R. The RC4 works on an array of 256 bytes to generate a pseudo random number sequence, and both encryption and decryption is performed using bits output R from the generator.

An array of 256 bytes (i.e. 2048 bits) is first initialized with the RC4 key repeated as many times as necessary to complete the table. Then, very simple operations are performed: bytes are swapped (permutation), bytes are added, and etc. the aim is to mix as much as possible the array. Finally, we get a table filled with bytes which seem completely random. Subsequently, we can continue to mix this table and to extract pseudorandom bits R progressively. The two essential points of RC4 are:

- The sequence of bits R produced by RC4 seem perfectly random.
- By using the same key RC4, we can get again exactly the same sequence of bits R provided.

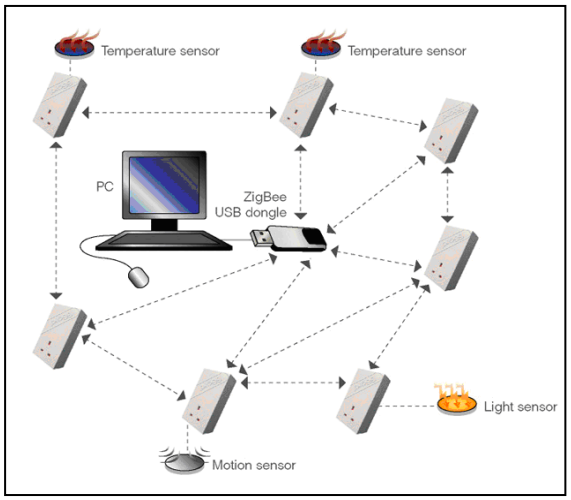


Figure 1. Zigbee network

For WEP and TKIP protocols, RC4 algorithm encrypts data as following: the random bits generated R is combined with the plaintext M using exclusive-or operation, i.e. XOR ($\oplus$). The encrypted data become $C=M \oplus R$. Having the shared RC4 key, and by generating the same random sequence R, the

receiver can decrypt the received data by the same way since XOR is a symmetric operation, and the reconstructed plaintext is M=C ⊕ R= (M ⊕ R) ⊕ R. RC4 has weaknesses [5], and it is especially vulnerable when: the beginning of the output R is not discarded, nonrandom or related keys are used, or a sequence is used twice. Some ways of using RC4 can lead to very insecure cryptosystems.

One reason for the algorithm's popularity is its simplicity. The algorithm can be memorized and quickly implemented from memory. Additionally, it is ideal for software implementations, as it requires only byte-length manipulations. RC4 is one of the fastest ciphers to be widely used for serious work. For this reason, RC4 is likely to remain the algorithm of choice for many applications and embedded systems.

2.2. AES-CTR encryption

The AES is a symmetric-key encryption standard [6] adopted by the U.S.A. government, and it is the first publicly accessible and open cipher approved by the NSA (National Security Agency) for top secret information. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES operates on blocks of data 128 bits long (16=4x4 bytes) that can be organized as a 4×4 matrix (called the state). For full encryption, the data is passed through N_e rounds (N_e = 10, 12, 14) [7]. These rounds are governed by four basic transformations: *SubByte*, *Shiftrows*, *Mixcolumns*, and *Addroundkey* transformation.

The encryption procedure consists of several steps performed iteratively (N_e times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure.

The AES is not breakable. It resists all the known types of attack and brute-force (where the cryptanalyst has to try all the possible combination until the correct key is found) remains the only solution. Some researchers have shown that the AES has weaknesses and they have proposed variants of the algorithm more secure [8] (for encryption images and for PDA communication, etc.).

To encrypt data using AES with counter mode (AES-CTR), the sender breaks the plaintext frame into 16-byte blocks $M_1 \ldots M_n \ldots$; AES ciphering is performed [3] on series of blocks called counters x_i to generate a sequence of pseudorandom number blocks $E_k(x_i)$ which is combined by XOR with the cleartext to produce the encrypted data C_i. The ciphertext is given by $C_i = M_i \oplus E_k(x_i)$.

Each 16-byte block M_i uses its own varying counter x_i. To decrypt the received data and obtain the original cleartext, the receiver computes $M_i = C_i \oplus E_k(x_i)$. Clearly, the receiver needs the counter value x_i in order to get M_i. Known as a nonce, the x_i counter, is composed of "see Fig. 2": a static flags field, the sender's physical address (address MAC Medium Access Control), and 3 separate counters: a packet number PN that identifies the packet, a key counter field, and a block counter that numbers the 16 byte blocks within the packet. The senders increment PN for each encrypted packet. The key counter is incremented when PN ever reaches its maximum value. The nonce must never repeat within the lifetime of a used key, and the role of the packet and key counters is to prevent nonce reuse. The role of the block counter is to ensure that each block will use a different nonce value; the sender does not need to include it with the packet, since the receiver can infer its value for each block.

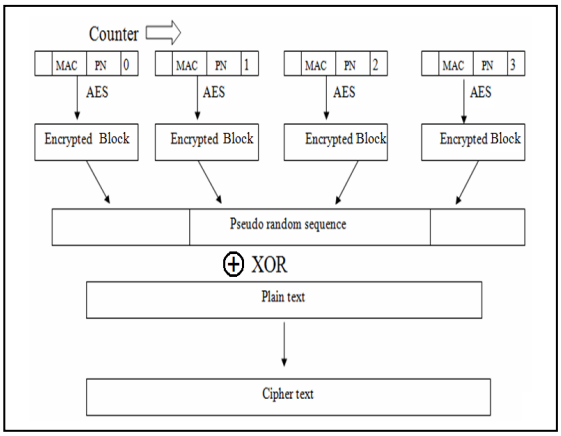


Figure 2. Data encryption with AES-CTR mode

As a nonce, the counter x_i guarantee [3] that two identical packets sent, from the same sender or not and with the same key or not and belonging to the same block or not, doesn't ever give the same results $E_k(x_i)$. So when the same counter x_i is used for two different messages M_i and M_j, the XOR of the cipher texts will be $[M_i \oplus E_k(x_i)] \oplus [M_j \oplus E_k(x_i)] = M_i \oplus M_j$. In this case, when the message M_i contains a series of zero, then $M_i \oplus M_j = M_j$, and the transmitted message loses its encryption. Thus the variation of the counter x_i (nonce) provides a high degree of security.

2.3. Analysis and proposition

The algorithm AES is not applied directly to the data (ECB mode), but to the counters (CTR mode) and the result (random sequence) is used to encrypt the plaintext (using XOR). In general, the ECB (Electronic CodeBook) mode, where the encryption algorithm is applied directly at the cleartext, i.e. $C_i = E_k(M_i)$, presents serious problems and it is not recommended at all. The disadvantage of this mode, and contrary to the CTR mode, is that identical plaintext blocks M_i are encrypted into identical ciphertext blocks C_i; thus, it does not hide data patterns well. It doesn't provide serious message

confidentiality. Among all the existing 'modes of operation' in the literature (ECB, CBC, OFB, CTR and CFB), CTR mode is widely used and it is well suited to operate on a multi-processor machine where blocks can be encrypted in parallel.

We have to notice that this mode transforms the encryption algorithm to a stream cipher whose role is only to generate random sequence number. Consequently, the AES-CTR becomes a stream cipher exactly like RC4.

In summary, the existing security protocols in Wi-Fi and ZigBee are not the ideal solution for transmitting important data in industrial control. For ZigBee network, the AES-CTR is very secure but it is complex and heavy. So, it is not fast enough to respect the real time requirement of industrial control. Additionally, it needs high hardware configuration while the ZigBee sensors are small and cheap devices characterized by small memory and designed for limited power consumption. For Wi-Fi network, the two security protocols WEP and TKIP relying on RC4 algorithm present vulnerabilities and are not reliable enough for sensitive data transmission, and the latest protocol WPA2 using AES-CTR doesn't satisfy the requirement of the real-time.

So, as the RC4 and AES-CTR role is to produce pseudo random sequence number (which is combined with the plaintext), we propose to replace them by a new simple chaotic scheme. The generated chaotic sequence has higher randomicity and looks more like stochastic noise. As non linear sequences, it is difficult to predict and analyze due to the big range of the secret key. Indeed, there are tight relationships between good random sequences and robust encryption. So, we think that the using of such chaotic structure will ensure very good data security of wireless networks considered. Therefore, a new chaotic scheme will be proposed in this paper, which has a very fast encryption speed so it can respect the real-time requirement of industrial control.

3. Chaos

3.1. Chaotic cryptographic

Chaos functions have mainly used to develop mathematical models of non linear systems. They have attracted the attention of many mathematicians owing to their extremely sensitive nature to initial conditions and their immense applicability to modeling complex problems of daily life. Chaotic functions which were first studied in the 1960's show numerous interesting properties. The sequences produced by such functions [9] has very good random and complexity. These functions have an extreme sensitiveness to initial conditions. For example, if the initial start value of a chaotic function is modified 10^{-20}, iterative numbers produced after some iterations are completely different from each other. This extreme sensitivity to initial conditions and some other interesting properties, such as pseudo-randomness, ergodicity, wide spectrum and good correlation, grant chaotic functions as a promising alternative for the conventional cryptographic algorithms. Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography.

Detailed theoretical analyzes show that chaotic functions has good cryptographic properties, and can be used to construct stream ciphers with high speed and security. Chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps which are deterministic but simple. The main advantage using chaos lies in the observation that a chaotic signal looks like noise for the unauthorized users. Moreover, generating chaotic values is often of low cost with simple iterations, which makes it suitable for the construction of stream ciphers. Therefore, cryptosystem can provide a secure and fast means for data encryption, which is crucial for data transmission in industrial control applications.

Generally speaking, chaotic stream ciphers use chaotic systems to generate pseudorandom keystream to encrypt the plaintext one by one. Many different chaotic systems have been utilized [9, 10, 11, 12, 13] to produce such keystream: 2-D Hénon attractor, logistic map and its generalized version, piecewise linear chaotic map (PWLCM), and piecewise nonlinear chaotic map, Frey map… Some researchers have analyzed the performance estimation of PRNGs (Pseudo-Random Number Generator) based on chaos. For continuous valued chaotic systems, many chaotic pseudo-random sequences have been proved to have perfect statistical properties, and other ones haven't been well enough.

3.2. Dynamical degradation

Digital chaotic generators have been proposed such as the traditional continuous chaotic maps. But they are discretized in 2^N finite space, and many researchers have found that they don't have good statistical properties and they present dynamical degradation. Such degradation threatens security of designed chaotic ciphers.

Because of the sensitivity of chaotic systems, the quantization errors which are introduced into iterations will make pseudo orbits in finite precision entirely different from the theoretical ones even after a short number of iterations. Even "trivial" changes of computer arithmetic can definitely change pseudo orbits structures. Additionally, since we work in a discrete space with 2^N elements, it is obvious that every chaotic orbit will certainly be periodic, i.e., finally go to a cycle with limited length lower than

2^N. Conceptually, there are only a small number of limit cycles for all orbits, which means the digital phase space will contrast to an attractor whose size does not exceed 2^N. Apparently, such a collapsed phase space will degrade the ergodicity of the continuous systems.

To improve the dynamical signal properties, some practical remedies have been proposed and are the following: using higher finite precision, cascading multiple chaotic systems, and randomly perturbing the chaotic systems.

3.3. Chaotic generator

The chaotic stream cipher is based on chaotic map as PRNG to encrypt the plaintext bit by bit. The produced chaotic random sequences are combined with the plaintext using XOR operation. There are very tight relationships between pseudo-random sequence and good cryptography. Consequently, the higher randomicity the chaotic sequence is, the stronger the encryption robustness will be. Therefore, to replace the RC4 and AES-CTR in the considered wireless networks, we need a high performance chaotic generator which can produce random series having a noise-like shape. And it must be very fast to meet the real time requirement of industrial control.

3.3.1. PWLCM chaotic map. The encryption speed of the chaotic stream ciphers is mainly determined by the time consuming on chaotic iterations. Consequently, the simpler the chaotic system is, the faster the encryption speed will be. PWLCM is one of the simplest chaotic systems [14], since only one or two multiplications/divisions and several additions/comparisons are needed for each digital chaotic iteration. Additionally, the PWLCM is widely used in digital chaotic ciphers because it has the following properties [15]:

- A uniform and invariant density
- Perfect dynamical properties
- An exponentially decayed correlation function
- A simple hardware and software realization and implementation.

A PWLCM is a map composed of multiple linear segments [16] and it is given by:

$$x(n) = F[x(n-1)]$$

$$= \begin{cases} x(n-1) \times \frac{1}{p} & if\ 0 \le x(n-1) < p \\ [x(n-1) - p] \times \frac{1}{0.5-p} & if\ p \le x(n-1) < 0.5 \\ F[1 - x(n-1)] & if\ 0.5 < x(n-1) < 1 \end{cases} \quad (1)$$

Where the positive control parameter p ϵ (0, 0.5) and x(i) ϵ (0, 1). Even if the continuous PWLCM have provided perfect properties, its digital version realized have dynamical properties far different from the ones described by the continuous map, and some degradation will arise. Therefore, we will use different remedies to enhance the dynamical degradation of digital PWLCM. We will mix two perturbed PWLCM together.

3.3.2. Perturbed PWLCM. There are different typical perturbation methods. A perturbation based algorithm is still suggested since it can provide better performance than other ones [16]. It can successfully improve the dynamical degradation of digital PWLCM to fulfill the requirements of digital chaotic ciphers. Indeed, the cycle length is expanded and good statistical properties are reached. Considering a PWLCM map defined by:

$$x(n) = F[x(n-1)] \quad [0,1] \quad n = 1,2,\ldots \quad (2)$$

Here, for a computing precision N, each x can be described:

$$x(n) = 0.x_1(n)x_2(n)\ldots x_i(n)\ldots x_N(n) \quad x_i(n) \quad \{0,1\} \quad /i = 1,2,\ldots N \quad (3)$$

The fundamental basis of the perturbing method is the fact that no stable cycles exist, i.e. the PWLCM output having entered a periodic cycle can be led to leave it by a perturbance, and will run away from the cycle loop.

The candidate proposed [17] for perturbing the PWLCM signal generator is the maximal length LFSR because its produced series have many advantages. The perturbing bit for every *n* clock time can be generated as following:

$$Q_{k-1}^{*}(n) =$$

$$Q_k(x) = g_0 Q_0(n) \oplus g_1 Q_1(n) \oplus \ldots g_{k-1} Q_{k-1}(n) \quad /n = 0,1,\ldots \quad (4)$$

Where g0 g1…gk-1 are the tap coefficients of the primitive polynomial generator, and Q0 Q1…Qk-1 are the initial values of register which at least one is not zero. The perturbance begins with n=0 and it occurs each Δ iterations (Δ is a positive integer), with n=l×Δ, l=1, 2… The perturbed sequence is given by the following equation:

$$x_t(n) = \begin{cases} F[x_t(n-1)] & 1 \le t \le N-k \\ F[x_t(n-1)] \oplus Q_{N-t}(n) & N-k+1 \le t \le N \end{cases} \quad (5)$$

Where F $[x_i (n)]$ represents the ith bit of F[x(n)].

The perturbance is applied on the last k bits of F[*x*(n)], "see Fig. 3".

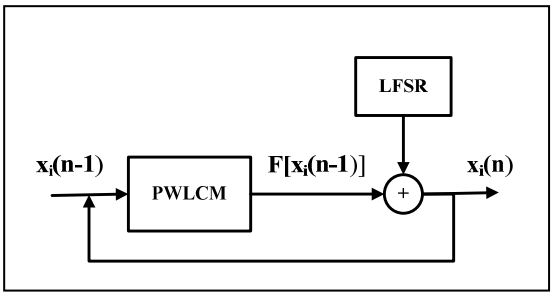


Figure 3. Perturbation technique principle

When $n \neq l \times \Delta$ there is not any perturbation, and then $x(n)=F[x(n-1)]$. This type of perturbation, can not only increase the cycle length, but can also dramatically improve the dynamical properties of PWLCM, and this greatly improves the robustness of chaotic encryption.

4. Proposed chaotic encryption algorithm

4.1. Proposed chaotic generator

Using multiple chaotic systems instead a single one may be useful to enhance the security, since mixing of multiple chaotic systems should make cryptanalysis much more difficult. It expends also the orbit cycle length. Some practical and theoretical analyses made in the literature shows that a couple of chaotic systems are enough to provide good security against information leaking from cipher text [18].

Additionally, the capability of parallel computation in hardware makes the practical implementations of digital chaos ciphers very fast. The proposed chaotic generator is the combination of two perturbed PWLCM by XOR operation (as shown in "Fig.4"). It produces a new chaotic sequence with higher random than either of them, and looks more like stochastic noise. This makes it difficult for the attackers to decrypt the ciphertext.

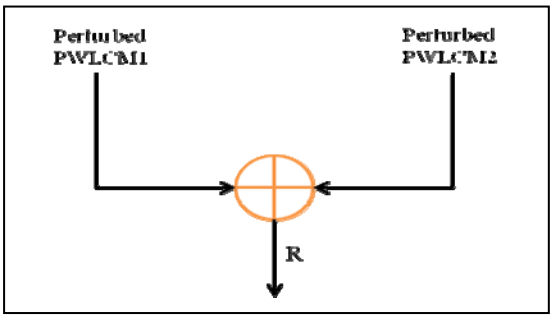


Figure 4. Proposed chaotic generator

4.2. Performances of the proposed chaotic generator

In order to verify the performances of the proposed generator some simulations have been realized. The results are presented in Figures 5, 6 and 7. The mapping, of the proposed generator, shown in "Fig. 5", indicates clearly that the produced series are random. Also, we found that the auto and cross correlation functions in "Fig. 6" and the spectrum DFT in "Fig. 7" are clearly noise-like.

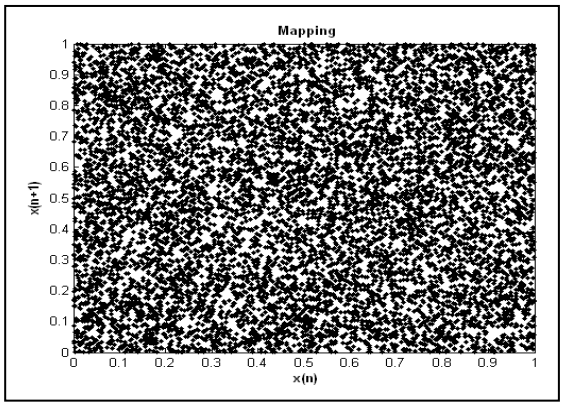


Figure 5. Mapping result

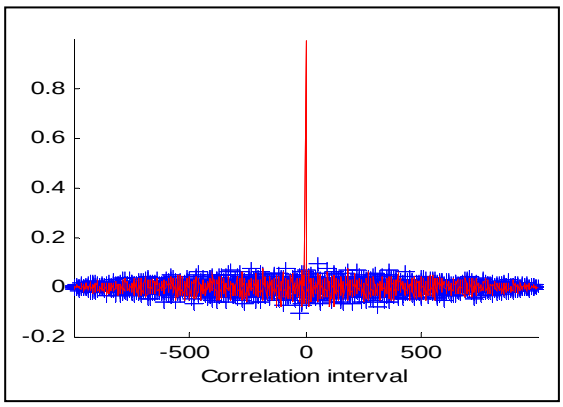


Figure 6. Auto and cross correlation functions

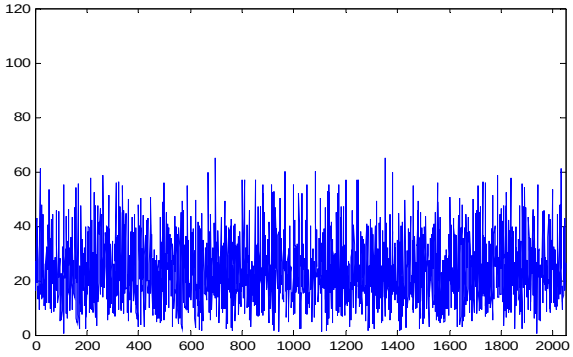


Figure 7. DFT spectrum of the proposed generator

Additionally, we have verified that the produced binary sequences pass all the NIST (National Institute of Standards and Technology) statistical tests, so they can be used in secure communication and our proposed generator can be used to encrypt data.

4.3. Proposed chaotic scheme

The stream ciphers RC4 and AES-CTR will be replaced by our proposed chaotic generator. So the random bits generated R are combined with the plaintext M using XOR operation, i.e. the encrypted data are given by C=M⊕R. with R=R1⊕ R2, where Ri is the generated sequence by the PWLCM for i=1 or 2. Having the initial conditions (The Key), the receiver can generate the same random sequences R1 and R2, and decrypts the received data by computing: M=C⊕ R1⊕ R2= (M⊕ R1 ⊕R2)⊕ R1 ⊕R2. The block diagram of cryptographic principle of our proposed chaotic system is given by "Fig. 8".

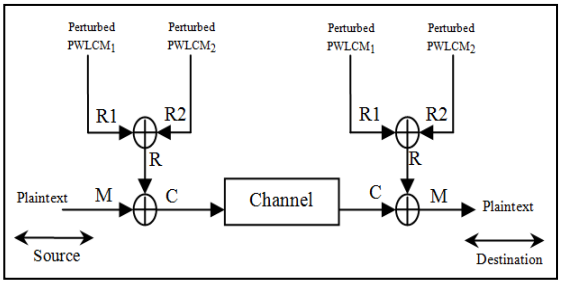


Figure 8. Proposed chaotic system

5. Tests and simulations

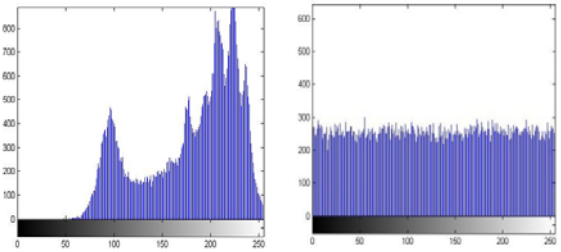
Simulation results and analysis of the proposed encryption scheme are provided in this section. As the image encryption is more difficult from text encryption due to some intrinsic properties of images such as bulky data capacity and high redundancy.

Therefore, the standard Lena image of size 512 x 512 and 256 gray levels is employed. The image is converted to a binary stream which is combined with pseudo-random binary sequence generated by the proposed chaotic generator; the corresponding ciphered image is formed.

The obtained result is shown in "Fig. 9", where 9(a) is the original image (plain image) and 9(b) is its encrypted image. By comparing these two images, there is no visual information observed in the encrypted image. It is visually indistinguishable and also having a big difference in the color repartition found in the plain image.

(a) **(b)**

Figure 9. (a) Original image (b) Encrypted image



(a) **(b)**

Figure 10. Histograms (a) of original image, and (b) of encrypted image

As shown in "Fig. 10", the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. Therefore, it does not provide any indication to employ any statistical attack on the image under consideration.

Let us now, test the proposed chaotic encryption algorithm through the calculation of some important parameters. And as RC4 is weak and it can be easily cracked, we will compare our proposed algorithm with only the AES-CTR which is still robust and secure.

5.1. Correlation coefficients

To test the correlation between horizontal, vertical or diagonal adjacent pixels of « Lena » original image and the encrypted image we calculate the Correlation coefficient. It is the measure of extent and direction of linear combination of two random variables. If two variables are closely related with stronger association, the correlation coefficient is close to the value one. On the other hand, if the coefficient is close to zero, two variables are not related and cannot predict each other. The coefficient *r* can be calculated using these formulas (6), (7), (8) and (9):

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (6)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x_i)\right)^2 \qquad (7)$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x_i)\right)\left(y_i - E(y_i)\right) \qquad (8)$$

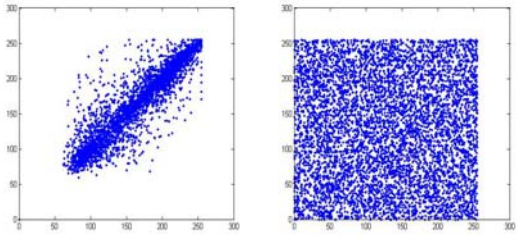
$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (9)$$

x and *y* are two adjacent pixels (horizontal, vertical, or diagonal) of the image. The results of the correlation coefficient are given in "Table 1". We can indicate that our proposed algorithm has got the best results.

Table 1. Correlation coefficients

	AES-CTR	Proposed algorithm
Horizontal Correlation	0.00235	0.000407
Vertical Correlation	0.01402	0.006686
Diagonal Correlation	0.01752	0.006096

"Fig. 11" shows the correlation distributions of two horizontally adjacent pixels in the original image and the encrypted one by the proposed algorithm.



(a) **(b)**

Figure 11. Correlation of two horizontally adjacent pixels; (a) in the original image, and (b) in the ciphered image

5.2. Test parameters: NPCR and UACI

Two criteria NPCR and UACI are used to test the change between the plain and the encrypted image. Number of Pixels Change Rate (NPCR) denotes the percentage of different pixel numbers between the original and the encrypted image. Unified Average Changing Intensity (UACI) denotes the average intensity of differences between the original and the encrypted image. Consider *C*1 *(Original image)* and *C*2 *(encrypted image)*. Let the gray-scale values of the pixels at position (i, j) are *C1* (*i*, *j*) and *C2* (*i*, *j*) of the two images *C1* and *C2* respectively. Define an array D with the same size as *C1* and *C2*. Then D (i, j) is determined by the following condition (10):

$$D(i,j) = \begin{cases} 1 & \text{if } C1(i,j) \neq C2(i,j) \\ 0 & \text{else} \end{cases} \quad (10)$$

NPCR and UACI are defined through the equations (11) and (12) respectively.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (11)$$

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|C1(i,j) - C2(i,j)|}{255} \times 100\% \quad (12)$$

Where M and N are the width and height of the considered image.

Results for these parameters are given in "Table 2".

Table 2. Comparative results in terms of the two parameters UACI and NPCR

	AES-CTR	Proposed algorithm
UACI	32.9523	32.5958
NPCR	99.6185	99.6277

We can note that the values of NPCR and UACI, for both AES-CTR and our proposed algorithm, verify that there is no resemblance between the plain and the encrypted image. We must note that the optimal values of: NPCR is 99.61 and of UACI is 33.46 [16].

5.3. NIST Statistical Tests

Among the numerous standard tests for pseudo-randomness, a convincing way to show the randomness of the produced sequences is to confront them to the NIST (National Institute of Standards and technology) statistical tests. The NIST statistical test suite [19] is a statistical package consisting of 188 tests that were developed to test the randomness of arbitrary long binary sequences produced by either hardware or software based cryptographic pseudorandom generators. These tests focus on a variety of different types of randomness that could exist in a sequence.

To verify our results, we use the above test suite to test the randomness of 100 sequences of 200,000 bits. In "Table 3" we show the results of the percentage of sequences that succeed the test. We must note that both AES-CTR and our proposed algorithm succeed these tests. But we can note clearly that the proposed method gives better results than the AES-CTR.

Table 3. NIST statistical test suite results

Tests (Results in %)	AES-CTR	Our Generator
Block Frequency	97	99
Frequency	95	99
Runs	89	99
Rank	96	100
DFT	99	100
Longest Run of ones	97	100
Non Overlapping	86	91
Overlapping	88	100
Linear Complexity	94	99
Serial	92	98
Entropy	99	99
Cumulative Sum	96	98
Random Excursions	99	100
Lempel-Ziv Complexity	93	100

5.4. Security analysis

For a secure cryptosystem, the key space should be large enough to make the brute force attack infeasible. In the proposed scheme, the key consists of: the initial values $x_1(0)$ and $x_2(0)$ of the two PWLCM maps, and their parameters p_1 and p_2, and the degree l of the two LFSR used for perturbing the chaotic maps. If N is the precision (floating-point number) that corresponds to the station's word length, so the proposed encryption method has $2^{2(2N-1)+2l}$ different combinations of the secret key. For N equal to 32, and l equal to 17 therefore, the key space is 2^{160} which satisfies the general requirement of resisting brute force attack.

As the encryption method used is a stream cipher, so it is robust against the differential and linear cryptanalysis. And as chaotic sequences have good randomicity, the statistical characterization of encrypted data is diffuse. So it is robust against statistical cryptanalysis.

6. Conclusion

A new encryption method has been proposed for Wi-Fi and ZigBee networks. It relies on a new chaotic generator formed by the combination of two perturbed PWLCM map. The proposed generator has the role of a stream cipher that produces random sequences which resembles stochastic noise. This sequence is combined with the plaintext to form the encrypted data. The proposed encryption algorithm has very good properties and succeeds all the statistical tests. We have shown also that the proposed method gives better results than the AES-CTR in terms of many measures and tests like: correlation, UACI, NPCR, and NIST statistical tests. Therefore, this encryption method is very secure and it has a high encryption speed.

Additionally, it is easily realized, it has a very large key range and it needs a low memory capacity. So, it meets the requirements of industrial control and it can replace the traditional encryption methods used in Wi-Fi and ZigBee networks.

7. References

[1] Géron. A., WIFI Déploiement et sécurité, Dunod, second edition, Paris, 2006, pp 245.

[2] Zhang, Z.Q., Yang, X.L., Zhou, Y.M., "A wireless solution for green house monitoring and control system based on ZigBee technology", *Journal of Zhejiang University Science*, 2007, Vol. 8, pp. 1584-1587.

[3] Sastry, N., Wagner, D., "Security considerations for IEEE 802.15.4 networks," in ACM Workshop on Wireless Security WiSe. PA. Philadelphia ,2004, pp. 32-42.

[4] He, Q., Qi, Q., Zhao, Y., Huang, W., Huang, Q. "The application of chaotic encryption in industrial control based on ZigBee wireless network," 2nd international symposium on systems and control in aerospace and astronautics ISSCAA (2008).

[5] Tews, E., Beck, M. "Practical attacks against WEP and WPA," Conference on wireless network security, Zurich, 2009, pp. 79-86.

[6] Buchmann, J., Introduction to cryptography, springer-verlag, second edition, 2004, pp. 157.

[7] Stinson, D., Cryptographie: Théorie et pratique, Vuilbert, second edition, Paris, 2003, pp. 64.

[8] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., Tourki, R., "A modified AES based algorithm for image encryption", *International journal of computer science and engineering*, 2007, Vol.1, No.1, pp. 70-75.

[9] Zhou, H., A design methodology of chaotic stream ciphers and the realization problems in finite precision. Ph.D. thesis, Department of Electrical Engineering, Fudan University, Shanghai, China , 1996.

[10] Parker, T.S., Chua, L.O., Practical Numerical Algorithms for Chaotic Systems. Springer, Verlag, 1989.

[11] Frey, D., "Chaotic digital encoding: an approach to secure communication," IEEE Transactions on Circuits and Systems II, Analog and Digital Signal Processing, 1993, Vol. 40, No 10, pp. 660-666.

[12] El Assad, S., Vladeanu, C., "Digital chaotic codec for DS-CDMA Communication Systems," Lebanese Science Journal. Lebanon, 2006, Vol. 7, No 2, pp. 55-71.

[13] Awad, A., El Assad, S., Wang, Q. Vladeanu, C., Bakhache, B., "Comparative study of 1-D chaotic generators for digital data encryption," International Journal of Computer Science. USA, 2008, Vol. 35, No 4, pp. 483-488.

[14] Baranovsky, A., Dames, D. "Design of One-Dimensional chaotic maps with prescribed properties", International Journal of Bifurcation and chaos. USA, 1995, Vol. 5, pp. 1585-1598.

[15] G. Chen, X. Mou and S. Li, "On the Dynamical Degradation of Digital Piecewise Linear Choatic Maps," *International Journal of Bifurcation and Chaos,* August 2005, Vol. 15, no 10, pp. 3119-3151.

[16] Shujun, Li., Analyses and New Designs of Digital Chaotic Ciphers. PhD thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University 2003.

[17] El Assad, S., Noura, H., Taralova, I., "Design and analyses of efficient chaotic generators for crypto-systems," IAENG special edition of the world congress on engineering and computer science, Advances in Electrical and Electronics Engineering, USA, 2008, vol. I, pp. 3-12.

[18] Heidari-Bateni, G., McGillem, C. D., "A chaotic direct-sequence spread-spectrum communication system," IEEE Trans. Communications, 1998, Vol. 8, No 4, pp. 647-65.

[19] J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. levrnson, M. Vangel, D.Banks, A. Heckert, J. Dray and S. Rukhin, "A Statistical Test Suite For Random and Pseudo-random Number Generators For Cryptographic Applications", NIST Special Publication 800-22, 2001.

