Encryption Algorithms to Enhance Security for ZigBee Network

J.Punitha Nicholine[*1], Dr.VE.Jayanthi[2]
[*1]*Assistant Professor, Department of Computer Science and Engg,*
[2]*Professor, Department of Electronics and communication Engg,*
[*1, 2]*PSNA College of Engineering and Technology & Dindigul-624622, Tamilnadu, India.*
[1]infantia.1@gmail.com

***Abstract* - Image encryption plays an important role in the field of information security. Due to the rapid growth of high security image transfer in multimedia application, network security becomes an important problem in communication. Encryption ensures safety data transfer in the field of communication. Modern cryptography provides important techniques for securing information and protecting multimedia data. In recent years, encryption technology has been developed and many image encryption methods have been used to protect confidential image data from unauthorized access. In this paper a brief review on image encryption techniques have been discussed in which researchers can have an idea for choosing the efficient technique and to be used in ZigBee networks.**

Keywords: Image Encryption, Decryption, ZigBee

I. INTRODUCTION

IEEE ZigBee 802.15.4 is a short-range communication standard that could be used for small distance multimedia transmissions. In fact, the ZigBee network is a wireless personal area network (WPAN), which needs a strong interleaving mechanism for protection against error bursts. This scheme depends on the chaotic Baker map [1].

ZigBee is a fairly new but promising standard for wireless networks due to its low resource requirements. As in other wireless network standards, security is an important issue and each new version of the ZigBee Specification enhances the level of the ZigBee security [2].

In Wireless Personal Area Networks (WPANs), the Zigbee protocol/IEEE 802.15.4 standard is a protocol specification for low range, less cost and low power systems [3].

The increased popularity of multimedia applications places a great demand on efficient data storage and transmission techniques. Network communication, especially over a wireless network, can easily be intercepted and must be protected from Eavesdroppers. Methods have to combine compression and encryption together to reduce the overall processing time [4].

AES 128-bit encryption algorithm in CCM* mode is secure transferred data; however, AES's secret key will be break within nearest future. Efficient public key algorithm, ECC has been mixed with AES to rescue the ZigBee wireless sensor from cipher text and replay attack. Also, the proposed protocol can parallelize the integrity function to increase system performance [5].

A chaotic map has sensitivity to a change in initial conditions and parameters, and a long-term forecast becomes impossible by the iterations of a chaotic map..The authentication protocol based on the iteration of the coupled logistic maps in a public-key cryptography [6].

ZigBee Network is used for home automation, surveillance and monitoring system. Security is essential.

Attribute-based proxy reencryption on ZigBee networks can distribute the authority to designated sensor nodes to decrypt re-encrypted ciphertext with associated attributes. We present a novel mechanism that can reduce overhead by imposing overhead to full function devices and ensure routing paths as well [7].

The adopted watermarking method implements the Singular-Value Decomposition (SVD) mathematical technique. This method is based on embedding a chaotic encrypted image in the Singular Values (SVs) of the audio signal after transforming it into a 2-D format. The objective of chaotic encryption is to enhance the level of security and resist different attacks [8].

A new robust and fast chaotic encryption algorithm RFCA is presented. This consists of a chaotic cipher composed of two perturbed maps piecewise linear chaotic map. This algorithm is, adequate for data encryption in ZigBee networks where robustness and real time are both essential [9].

II. SECURITY OF ZIGBEE NETWORK

2.1 Chaotic Interleaver Scheme

The 2-D chaotic Baker map in its discretized version is a good candidate for this purpose. After rearrangement of bits into a 2-D format, the chaotic Baker map is used to randomize the bits. The discretized Baker map is an efficient tool to randomize the items in a square matrix. Let $B(n1, \ldots, nk)$, denote the discretized map, where the vector, $[n1, \ldots nk]$, represents the secret key, *Skey*. Defining *N* as the number of

© 2014 IJAIR. ALL RIGHTS RESERVED

data items in one row, the secret key is chosen such that each integer *ni* divides *N*.

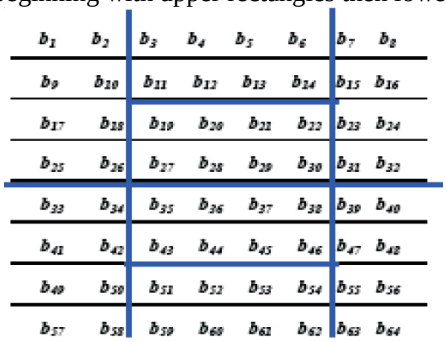
Let $N_i = n_1 + \ldots + n_{i-1}$. The data item at the indices (*r*, *s*),is moved to the indices.

$$B(r,s) = \left[\frac{N}{n_i}(r - N_i) + s \bmod \left(\frac{N}{n_i}\right), \frac{n_i}{N}\left(s - s \bmod \left(\frac{N}{n_i}\right)\right) + N_i\right] \quad (1)$$

Where $Ni \le r < Ni+ni$, $0 \le S < N$, and $N1 = 0$.I

In steps, the chaotic permutation is performed as follows:

1. An N×N square matrix is divided into N rectangles of width n_i and number of elements N.
2. The elements in each rectangle are rearranged to a row in the permuted rectangle. Rectangles are taken from left to right beginning with upper rectangles then lower ones.



(a)

(b)

(c)

Fig2.1: (a) the 8×8 matrix divided into rectangles (shaded bits are bits affected by error bursts), (b) chaotic interleaving of the matrix, (c) Effect of error bursts after de-interleaving

Figure 2.1 shows an example for chaotic interleaving of an 8 × 8 square matrix (i.e., N = 8). The secret key, Skey = [n1, n2, n3] = [2, 4, 2]. Note that, the chaotic interleaving mechanism has a better treatment to both 1-D and 2-D error bursts than the block interleaving mechanism. Errors are better distributed to bits after de-interleaving in the proposed chaotic interleaving scheme. As a result, a better peak signal to noise ratio (PSNR) of received images can be achieved with this proposed mechanism. Moreover, it adds a degree of security to the communication system. At the receiver of the ZigBee system, a chaotic de-interleaving step is performed.

2.2. Simulation Results

In this section, the computer simulation results are presented. This is a realistic assumption to simulate the real ZigBee system operation. A correlated Rayleigh fading channel is used. The assumed mobile ZigBee device velocity is 10 miles/hour, and the carrier frequency is 2.46 GHz. The Doppler spread is 36.6 Hz. Figure 2.2 gives the original cameraman image used in the experiments. It is the Matlab image and it format is tag image file format (TIF).

Figure.2.2 Original cameraman image

The image binary sequence to be transmitted is fragmented into packets. The PSNR of the received images is used as an evaluation metric in this paper. The results of this experiment are shown in Fig. 2.3 From these results, it is clear that the effect of chaotic interleaving schemes is approximately equal at low SNR values.

Figure.2.3.Received cameraman image over a correlated fading channel at SNR = 10 dB with a) PSNR = 21.5 dB.

© 2014 IJAIR. ALL RIGHTS RESERVED

III. Attribute-Based Proxy Re-encryption

3.1 ABPRE with Constant Pairing Operations

ABPRE with constant pairing operations is an enhance and To reduce the number of pairing operations, exponentiation is conducted instead of the operation. Therefore, the pairing operation is computed at once at the end. When the sender wants to send a message to recipient #1, it directly transmits the cipher text to the destination after encryption. In the case of recipient #2, the sender transmits the packet to the base node. The base node then re-encrypts the packet using recipient #2's attributes. The re-encrypted data is transmitted to recipient #2 and then the data is decrypted with the attributes of recipient #2.The detailed process of the algorithm is described in Table 3.1

TABLE 3.1 PROCESS OF ENCRYPTION AND DECRYPTION OVER A SENSOR NETWORK

S.No	To adjacent nodes	To nodes in the distance
1	Generate a packet	Generate a packet
2	Encrypt the packet with its attribute	Encrypt the packet with its attribute
3	Send the ciphertext to its destination	Send the ciphertext to its destination
4	Send the ciphertext to its destination	Send the ciphertext to its destination
5	Decrypt the ciphertext	Re-encrypt the ciphertext
6	-	Send the re-encrypted ciphertext
7	-	Decrypt the re-encrypted ciphertext

3.2. Evaluation

The attribute-based proxy re-encryption scheme has the capability of attribute encryption with specific attributes and re-encrypting the message for delegating the capability of decryption to selected users, which enables various features such as the simplicity of group key management and delegation of decryption capability. Comparing the number of keys with other schemes, ABPRE has *O* (n) complexity, but the current ZigBee system is *O* (n2) because in symmetric cryptography all users should maintain the same secret key as the others. Therefore, traditional cryptography is not suitable for ZigBee security, but the proposed method is efficient in terms of distribution and management of keys. However, ABPRE does not offer a digital signature because it uses the attributes that are not representative of the user. For practical application, a proposal is required to reduce the computation cost because the scheme claims high overhead including pairing operations. Currently pairing operations over sensor networks take about 1 second. Therefore; it is not practical if many pairing operations are needed. In traditional ABPRE, the pairing operation is conducted by a number of attributes. Therefore, it is infeasible to enable the technology over a sensor network

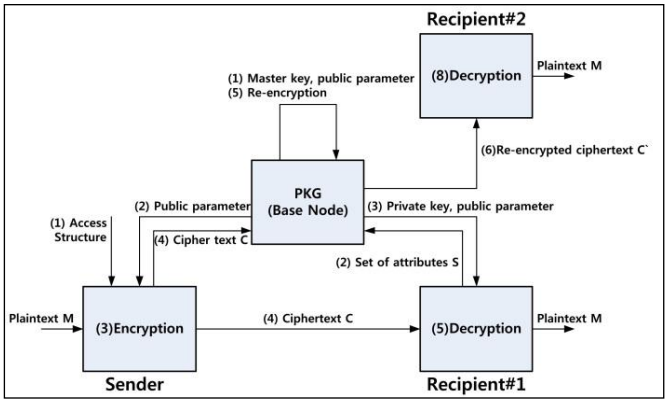


Figure.3.1 Process of encryption and decryption (PKG: private key generator).

To solve this drawback, we use a constant pairing operation based on ABPRE.The architecture of this method is shown in fig 3.1. We must compute two or three pairing operations by conducting decryption. The re-encryption is conducted by a full function node, a base node. Therefore, overhead is reduced in the leaf nodes. Table 3.1 illustrates the computational complexity of ABPRE. The leaf node needs to conduct the encryption process per each transmission. In the previous method, we had to conduct re-encryption whenever we needed to transmit data to users that were not included in first access structure of the ciphertext by the leaf node. However, in the case of the proposed method, the reencryption process imposes the overhead on the base node, a much more powerful device. Therefore, the computational costs on the leaf nodes are reduced. Even though the method provides a small number of pairing operations, it is still not a practical method for ATmega128L and MSP430 devices.

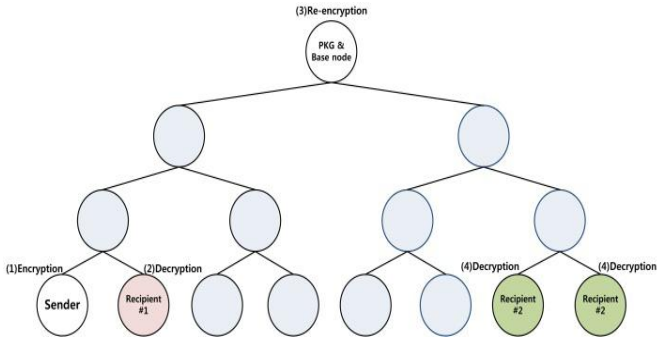


Figure.3.2. Process of encryption and decryption. PKG: private key generator.

The security strength of the proposed model is based on the user's secret key and attributes. First, if the sender's secret key is not revealed to others, the encryption and decryption process are secure, depending on the CTDH and ADBDH

© 2014 IJAIR. ALL RIGHTS RESERVED

assumption. Secondly, the re-encryption process also demands the user's secret key to allow it to proceed. Even though malicious users might obtain the user's encrypted text, they cannot generate a re-encrypted text because the encryption key is not available for malicious users.

TABLE.3.2. COMPUTATIONAL COMPLEXITY OF ABPRE

Encryption	$(n + 2)G_1 + 2G_T$
Decryption	$(3n + 2)G_1 + 2G_T + 2C_e$
Re-encryption	$3nG_1 + G_T + 2C_e$
Re-decryption	$3nG_1 + 4G_T + 3C_e$

Where, ABPRE: attribute-based proxy re-encryption.

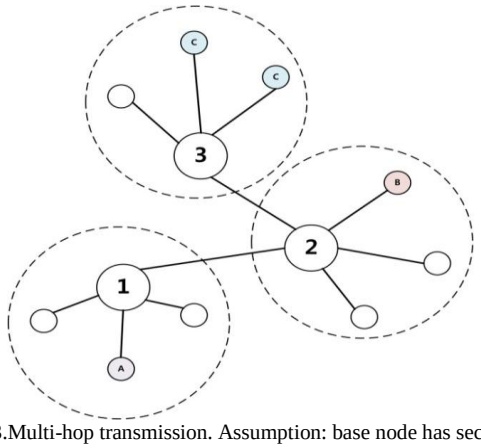


Figure.3.3.Multi-hop transmission. Assumption: base node has secret key of leaf nodes.

IV. AES AND ECC MIXED FOR ZIGBEE WIRELESS SENSOR SECURITY

AES algorithm provides confidentiality, CCM* mode is apply for integrity, and frame nonce is checked to prevent replay attack. There are three keys in ZigBee technology master key, network key, and link key. Each one of the keys has specified benefit, where link key is used for encrypting exchanged messages, network key is used to secure broadcast messages to all or group of nodes, and master key is used for transfer link key between nodes.

ZigBee technology apply CCM* mode to provide confidentiality, integrity and defense against replay attack; which is a developed version of CCM. CCM* provides ZigBee technology the ability to perform one of the following operation or both: encrypt the message with counter (CRT), and authenticate CBC-MAC the message. With this mode the maximum message size is up to 2_{64} byte. The authentication field *T* for the message with assumption that no authentication data is compute by the follow steps (authentication is shown in figure 4.1)

• Define sequence of 16-octet blocks.

• Split the message m to 16-octet blocks and then padding the last block with zeros if necessary. (If message m is empty string, then blocks will not be added in this step).

Compute:

$$X_1 = E(K_1\ B0) \quad (1)$$

$$X_{i+1} = E(K_i \times_i \oplus B_i) \text{ for } i=1,\ldots n \quad (2)$$

$$T = \text{first\_M\_bytes}(X_{i+1}) \quad (3)$$

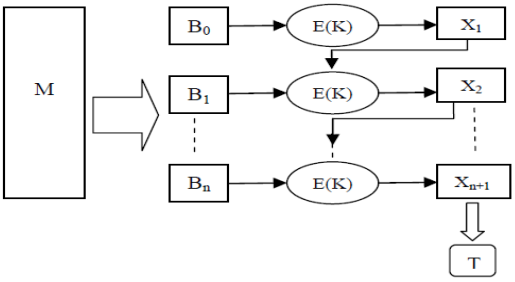


Figure.4.1. Message Authentication in CCM* Mode

Where,

T: is the authentication code, which is truncated from X_{n+1}.

K: is the block cipher key for (key size is 128 bit for AES in ZigBee technology).

M: is the size of authentication field.

E(): is the block cipher encryption function.

The Multiple key protocol is given bellow in fig 4.1

Input: k_0, r_0, Message, PK, Security_L

Output: C

Begin

Block Size=128

for i= 1 to Security_L

$k_i = ECC(k_{i-1}, PK)$

$r_i = ECC(r_{i-1}, PK)$

$K_i = f(k_i, r_{n-i+1})$

No_of_Blocks = Message/BlockSize

No_of_Blocks_in_Group = No_of_Blocks /Security_L

Count = 1

Key = K_{count}

for j =1 to No_of_Blocks

$C_j = AES(B_j, Key)$

if (j % No_of_Blocks_in_Group == 0)

then Key = $K_{count++}$

End

© 2014 IJAIR. ALL RIGHTS RESERVED

A new algorithm is implemented Using MKP protocol. In MKP, Secret key are implemented in ECC algorithm. A number of blocks in each group are computed based on message Size and security level.

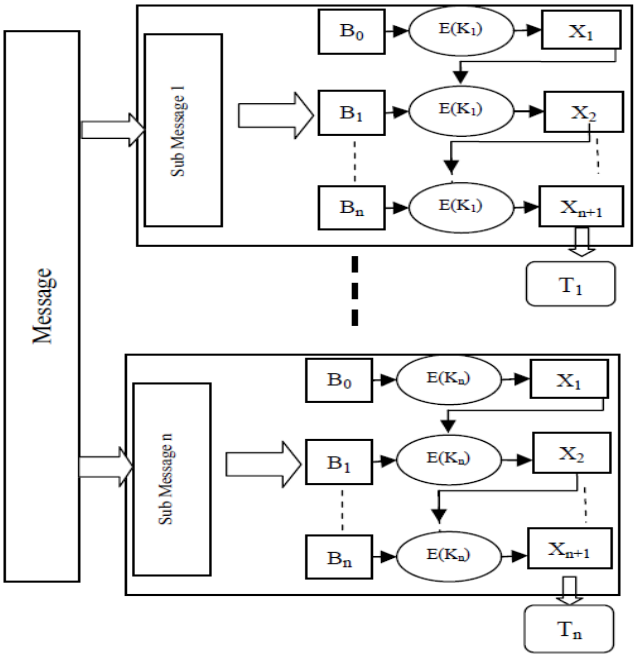


Figure 4.3 ZigBee authentication code in MKP

4.2. Benefits Of MKP For ZigBee

The MKP protocol provides multi-level security in ZigBee technology. ZigBee applications with multi-role can get multilevel of security when using MKP. The numbers of generated keys in MKP are computed by a level of security. From secrecy side, in previous protocol it used one secret key, while in MPK protocol it uses multiple-key. If the analyst needs 2keysize/2 operations to break one key in previous with time complexity O (log2 (keysize/2)).

V. Partial Encryption Based on Data Decomposition

Partial encryption of images is examined in this section. The encrypted part is more than 50% of the total size of the compressed image, and outlines of objects are revealed. We have found two classes of algorithms that are suitable for partial encryption. Both types of algorithms are suitable for low bit rate applications, and partial encryption schemes for them are proposed.

The relative size of the important part, the computational complexity, and the security of each scheme are then analyzed. The size of the important part compared with the total size of the compressed image is directly proportional to the amount of encryption and decryption time required.

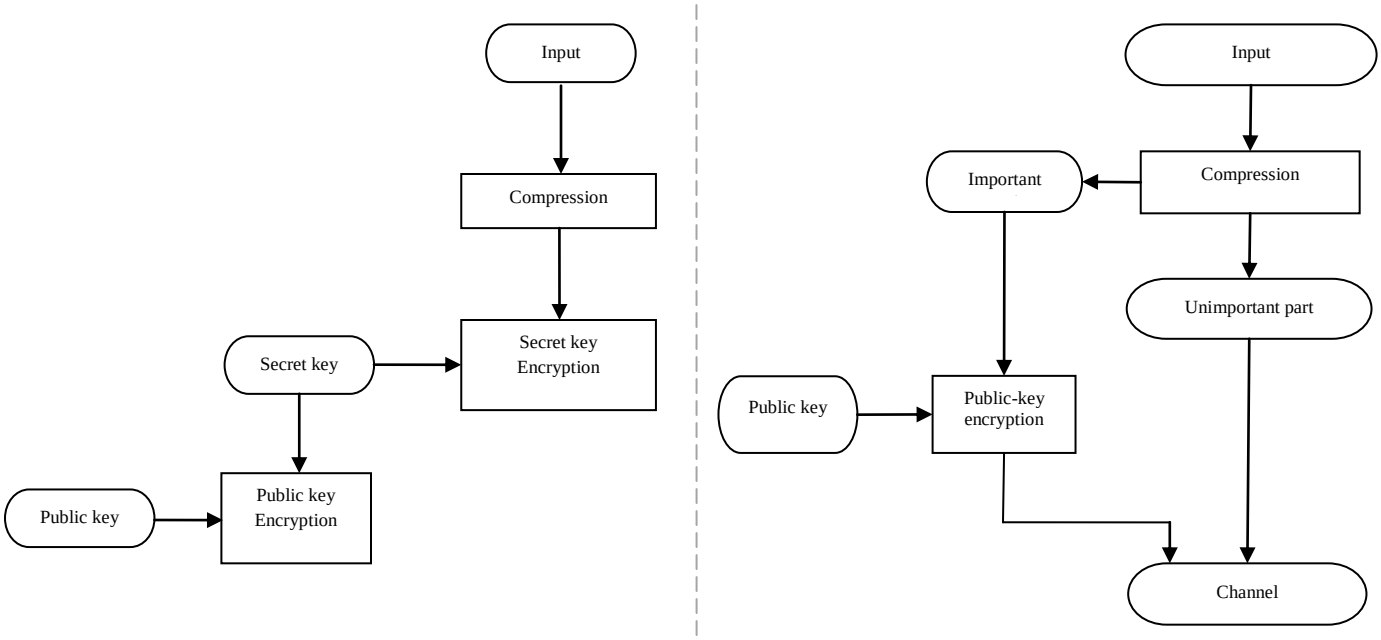
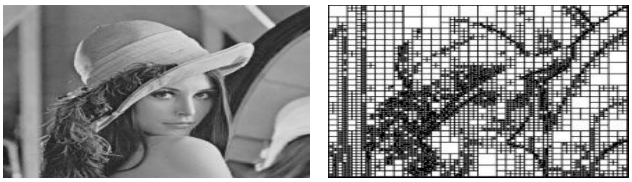


Figure.5.1.Comparison of (a) the traditional approach to secure image and video communication and (b) the proposed approach when public-key encryption can be applied directly to the important part

© 2014 IJAIR. ALL RIGHTS RESERVED

.5.1 Quadtree Compression

The quadtree partial encryption scheme can be used for both lossless compression and lossy compression. In lossless quadtree compression, each leaf value is represented by the same number of bits. In lossy compression, however, the number of bits used to represent each leaf value is different. When a block is large, it is important to accurately represent its intensity.the compression is shown in figure 5.2



(a) (b)

Fig.5.2.Quadtree decomposition of an image. (a) Original image. (b) Quadtree decomposition

5.2. Zerotrees Wavelet Compression

Wavelet compression algorithms based on zero trees generally transmit the structure of the zerotrees in addition to the significant coefficients. For example, the SPIHT compression algorithm transmits the significance of the coefficient sets that correspond to trees of coefficients. This is similar to quadtree compression as it indicates whether a set needs to be decomposed further. Instead of homogeneity, significance is the factor for deciding whether a set is partitioned. The SPIHT algorithm uses the significance information of sets to determine the tree structures, and the execution of the algorithm depends strongly on the structure of the zerotrees. The compression algorithm produces
many different types of bits:

- sign bits;
- refinement bits;
- significance of pixels;
- significance of set

The following partial encryption is extended for videos. It is shown in figure 5.3

Figure 5.3 Reconstructed images using only first K encrypted bits

VI. RC4 ALGORITHMS

The security of Wi-Fi and ZigBee, is based on two algorithms: RC4 (for Wi-Fi), and AES-CTR (for Wi-Fi and ZigBee). ZigBee is shown in figure 6.1.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. 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 is simply to produce an endless series of pseudorandom 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. 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.

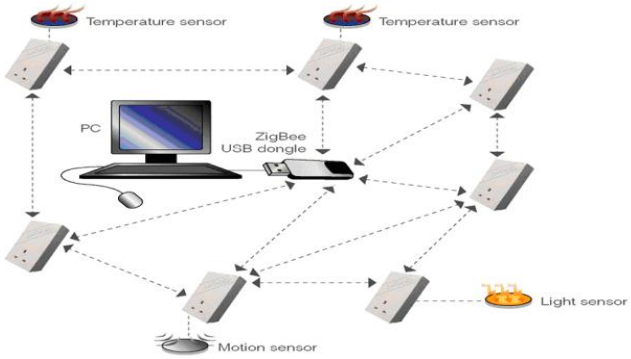


Figure. 6.1 Zigbee networks

6.1. AES-CTR encryption

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

© 2014 IJAIR. ALL RIGHTS RESERVED

(called the state). These rounds are governed by four basic transformations: SubByte, Shiftrows, Mixcolumns, and Add round key transformation To encrypt data using AES with counter mode (AES-CTR), the sender breaks the plaintext frame into 16-byte blocks M1…Mn…; AES ciphering is performed on series of blocks called counters xi\to generate a sequence of pseudorandom number blocks Ek(xi) which is combined by XOR with the cleartext to produce the encrypted data Ci. The ciphertext is given by Ci = Mi Ek(xi).Each 16-byte block Mi uses its own varying counter xi. To decrypt the received data and obtain the original cleartext, the receiver computes Mi = Ci Ek(xi). . T he 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. AES-CTR is shown in figure 6.2

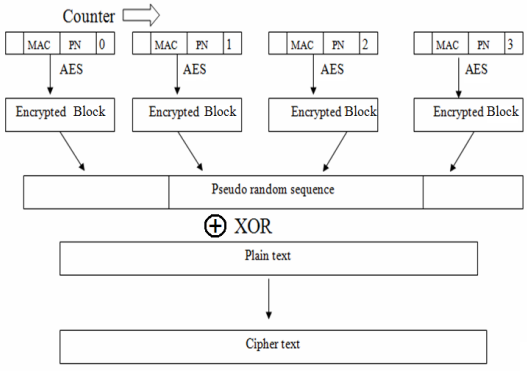


Fig 6.2 AES-CTR

6.2. Chaotic encryption algorithm using RFCA:

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 . 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.6.3"). 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.

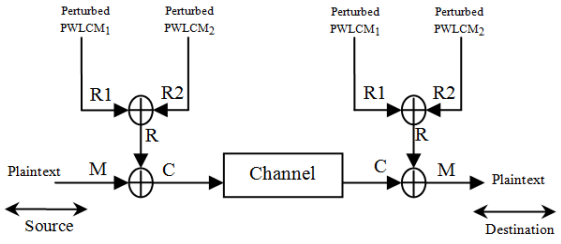


Fig 6.3 RFCA Model

6.3 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.

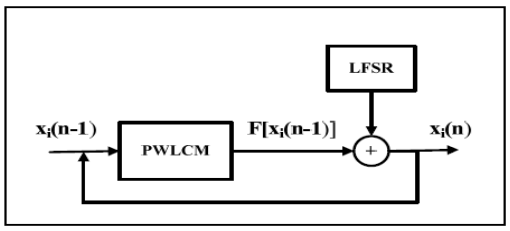


Figure 6.4 Perturbation technique principle

Additionally, the capability of parallel computation in hardware makes the practical implementations of digital chaos ciphers very fast. The chaotic generator is the combination of two perturbed PWLCM by XOR operation. 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 PWLCM (perturbation is shown in figure 6.4)map defined by:

$$x(n)= F[x(n-1)]\ [0,1]\ n = 1,2,\ldots \quad (4)$$

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

$$x(n)= 0.x_1(n)x_2(n)\ldots x_i(n)\ldots x_N(n)\ x_i(n)\ \{0,1\}$$
$$i = 1,2,\ldots N \quad (5)$$

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:

$$(n)=n = 0,1,\ldots \quad (6)$$

The mapping, of the proposed generator, shown in "Fig. 6.5", indicates clearly that the produced series are random. Also, we found that the auto and cross correlation functions in "Fig. 6.6" and the spectrum DFT in "Fig. 6.7" are clearly noise-like.

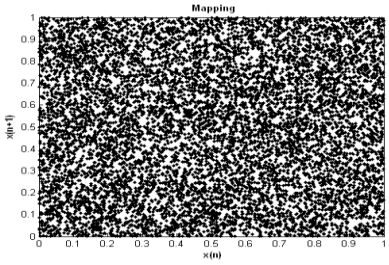


Figure 6.5 Mapping result

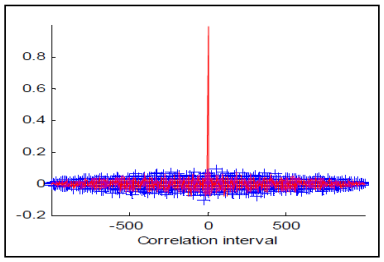


Figure.6.6 Auto cross correlation functions

© 2014 IJAIR. ALL RIGHTS RESERVED

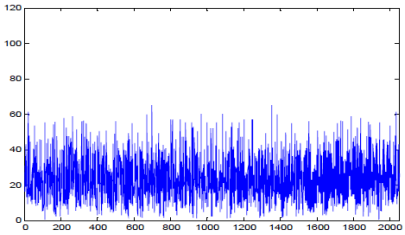


Figure.6.7. DFT spectrum of proposed Generator

6.4. Test and Results:

The obtained result is shown in "Fig 6.8", where (a) is the original image (plain image) and (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 6.8 (a) Original image (b) Encrypted image

VII. Conclusion

In this paper, familiar encryption algorithms are discussed, which is used in ZigBee networks. Along with the simulation results every algorithm has advantages and disadvantages as listed in the following table 6.1, based on their application. On this review, proper selection of encryption algorithm based on real time application is made easier on image encryption and different techniques have been discussed in which researchers can have an idea for choosing the efficient technique and to be used in ZigBee networks.

Table 6.1. Comparative Results on Various Encryption Techniques

S.NO	ENCRYPTION TECHNIQUE	ADVANTAGES	DISADVANTAGES
1.	Chaotic interleaver	1. We get a better peak signal to noise ratio (PSNR) of received images. 2. To improve the received image quality with the Security enhancing.	The proposed chaotic interleaver does not decrease the number of lost frames.
2.	Attribute-Based Proxy Re-encryption	1. The method can reduce overhead by imposing overhead to full Function devices and ensure routing paths as well. 2. Simplicity of group key management and delegation of decryption capability. 3. A proposal is required to reduce the computation cost and a constant number of pairing operations	The method does not show reasonable performance
3.	AES and ECC Mixed	AES algorithm provides confidentiality, CCM* mode is apply for integrity, and frame nonce is checked to prevent replay attack.	System has complexity and the difficulty of the is how to generate multiple keys and manage their secrecy.
4.	RC4	RC4 is simple and it is one of the fastest ciphers to be widely used for serious work .	RC4 can lead to very insecure cryptosystems.
5.	AES -CTR	AES-CTR is highly secure.	it has a very complex algorithm, time-consuming and high memory capacity, then it does not meet the real-time requirement of industrial control
6.	RFCA	A new high speed chaotic Cryptographic scheme. It requires a little memory capacity, and also appears to be very secure.	it has a very large key range and it needs a low memory capacity

© 2014 IJAIR. ALL RIGHTS RESERVED

REFERENCES

[1] M. A. M. El-Bendary, A. E. Abou-El-azm, N. A. El-Fishawy, F. Shawki, M. El-Tokhy, F. E. Abd El-Samie, and H. B. Kazemian, "An Efficient Chaotic Interleaver for Image Transmission over IEEE 802.15.4 Zigbee Network",journal of telecommunication and information technology 2/2011.

[2] Ender Y¨uksel Hanne Riis Nielson Flemming Nielson, "ZigBee-2007 Security Essentials" ,Informatics and Mathematical Modelling, Technical University of Denmark Richard Petersens Plads bldg 321, DK-2800 Kongens Lyngby, Denmark {ey,riis,nielson}@imm.dtu.dk.

[3] Hariram R M,Anjunatha S,Jitendranath Mungara,"Efficient E-mrzt Algorithm Based Tree Construction Technique for Zigbee Mobile Wireless Networks", International Journal of Smart Sensors and AdHoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-3,4, 2012.

[4] Howard Cheng and Xiaobo Li, *Senior Member* ,"Partial Encryption of Compressed Images and Videos", IEEE transactions on signal processing, VOL. 48, NO. 8, AUGUST 2000.

[5] Saif Al-alak, Zuriati Ahmed, Azizol Abdullah and Shamala Subramiam,"AES and ECC Mixed for ZigBee Wireless Sensor Security", World Academy of Science, Engineering and Technology,Vol:57 2011-09-21.

[6] Shuichi Aono†, Yoshifumi Nishio," A User Authentication Protocol Using Chaotic Maps", 2007 RISP International Workshop on Nonlinear Circuits and Signal Processing (NCSP'07) Shanghai Jiao Tong University, Shanghai, China, Mar. 3-6, 2007.

[7] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy Reencryption with delegating capabilities," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, pp. 276-286, 2009.

[8] Hwajeong Seo and Howon Kim*, Member, KIICE, " ZigBee Security Using Attribute-Based Proxy Re-encryption", J. lnf. Commun. Converg. Eng. 10(4): 343-348, Dec. 2012.

[9] Mohsen A. M. El-Bendary*a*, Atef Abou El-Azm*b*, Nawal El-Fishawy*b*, Farid Shawki*b*,Mostafa A. R. El-Tokhy*a*, Fathi E. Abd El-Samie*b*, and H. B. Kazemian "SVD Audio Watermarking: A Tool to Enhance the Security of ImageTransmission over ZigBee Networks", journal of telecommunication and information technology 4/2011.

[10]Bassem Bakhache, Kassem Ahmad, Safwan el Assad "A New Chaotic Encryption Algorithm to Enhance the Security of ZigBee and Wi-Fi" . International Journal of Intelligent Computing Research (IJICR), Volume 2, Issues 1/2/3/4, Mar/Jun/Sept/Dec 2011.

© 2014 IJAIR. ALL RIGHTS RESERVED