Research Inventy: International Journal of Engineering And Science
Vol.5, Issue 4 (April 2014), PP -84-87
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Robust Encryption Algorithm for Zigbee Communication

KSK Swamy[1], M Suresh[2], S Rakesh[3]
[1,2,3]*ECE Department, Sree Dattha Institute of Engineering & Science*

Abstract: *Zigbee Technology was developed for Wireless Personnel Area Networks (WPAN), aimed at control of military applications with high security. To provide the security in Zigbee networks cryptography technique is used. Cryptography performs encryption operation before transmitting the data. Zigbee networks use stream cipher encryption mechanism. Several new stream cipher cryptography techniques are proposed, but these stream cipher techniques have shown some drawbacks. In this paper a robust and fast stream cipher encryption technique has proposed for the Zigbee communication. The proposed work is less complex to design and robust to the Zigbee communication. The design of stream cipher algorithm is carried out using Verilog HDL and implemented using FPGA.*

Keywords: *Zigbee, Cryptography & Stream Cipher.*

I. Introduction

ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios based on an IEEE 802.15.4 standard for personal area networks. ZigBee devices are often used in mesh network form to transmit data over longer distances, passing data through intermediate devices to reach more distant ones. This allows ZigBee networks to be formed ad-hoc, with no centralized control or high-power transmitter/receiver able to reach all of the devices. Any ZigBee device can be tasked with running the network. A minimum level of security must be maintained in a network to protect it from adversaries. For example, in an unsecure industrial ZigBee network, an unauthorized user may either trigger an alarm or suppress legitimate alarm signal. To ensure the confidentiality of the exchanged data encryption must be applied before transmission [1],[2].

Cryptography plays a significantly important role in the security of data transmission. On one hand with developing computing technology implementation of sophisticated cryptographic algorithms has become feasible. The cryptographic algorithms are classified into Block cipher cryptography and Stream Cipher cryptography. The Block Cipher cryptography which usually has a relatively compact architecture than Stream Cipher cryptography is often used to encrypt/decrypt sensitive information or documents. The well known Block Cipher cryptography algorithm is AES (Advance Encryption Standard) and for Stream Cipher several papers proposed different techniques, most used stream cipher is RFCA cryptography. AES cryptography algorithm we can use as a stream cipher by running in counter (AES-CTR) mode [3].

The AES is one of the most secure, robust, and reliable algorithms. AES encrypts 128-bit blocks of data, using multiple substitution and permutation operations (block cipher). But, using it in counter mode, the AES-CTR is somehow transformed into a stream cipher because the counter is encrypted then applied to data before transmission. The AES-CTR is highly secure but it is a complex algorithm, and it requires a high memory capacity and is time consuming. Thus, this algorithm does not meet the real-time requirements for some industrial and medical applications [4]. In [5] proposed a RFCA technique for Stream cipher cryptography in place of AES-CTR to reduce the complexity and increase the robustness and faster computations. This paper is organized as follows: Section II presents RFCA encryption algorithm; section III presents proposed robust Encryption algorithm; section IV is dedicated to results and V section is for concluding the work.

II. RFCA

In this part, we present a general overview on chaos and show the digital chaotic system problems and how to solve them. Then, we describe the piecewise linear chaotic map (PWLCM) and its properties, as long as the perturbation method applied to this map.

A. Chaos and Cryptography

Chaos functions have been mainly used to develop mathematical models for nonlinear systems. Due to their extremely sensitive nature to initial conditions and many more interesting characteristics, they have attracted the attention of many mathematicians. Chaotic functions were first studied in the 1960s and have shown several remarkable properties. Sequences produced by these functions [6] are very random and complex. The main advantage using chaos lies in the shape of the chaotic signal that looks like noise for the unauthorized users. Moreover, chaotic values are often generated with simple iterations, which make chaos suitable for

designing strong and high-speed stream ciphers. Chaotic stream ciphers use chaotic generators to produce pseudorandom stream of bits to encrypt the plaintext using XOR operation.

B. Piece Wise Linear Chaotic Map (PWLCM)

The encryption speed of chaotic stream ciphers is mostly determined by the time consumed on chaotic iterations. Therefore, a simple chaotic system will lead to a faster encryption speed. PWLCM is one of the simplest chaotic systems, since only some multiplications/divisions, additions/comparisons are needed for each digital chaotic iteration. Moreover, the PWLCM is widely used because it has the following properties:

1) A uniform and invariant density;
2) An exponentially decayed correlation function;
3) A simple hardware and software realization and implementation.

A PWLCM is a map composed of multiple linear segments and it is given by,

$$x(n+1) = \begin{cases} Bx(n) + A & x(n) < 0 \\ Bx(n) - A & x(n) \geq 0 \end{cases} \quad n = 0, 1, 2, \ldots$$

Where parameters A and B are chosen to be 1 and 1.998 respectively to generate chaos. This map is extensively used for chaos generation due to its perfect properties such as uniform invariant density function; exactness, mixing and periodicity; exponentially decaying correlation function and simple realization in both hardware and software.

C. Perturbed PWLCM

Applying perturbation technique on the digital PWLCM can significantly improve its dynamical degradation, and can provide better performance for its generated sequences. Indeed, the cycle length is expanded and good statistical properties are reached.

The linear feedback shift register (LFSR) based perturbation technique was proposed [7], [8] to enhance the properties of the digital PWLCM. Considering a PWLCM map defined by

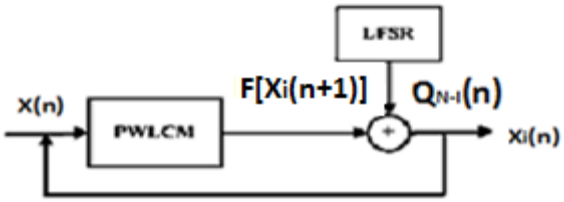

Fig 1. Perturbed PWLCM Principle

The perturbed sequence is given by the following equation:

$$X_i(n) = \begin{cases} F[X_i(n+1)] + Q_{N-i}(n), & X(n) < 0 \\ F[X_i(n+1)] + Q_{N-i}(n), & X(n) \geq 0 \end{cases}$$

D. RFCA Algorithm

Fig. 2 represents the scheme of the proposed RFCA. The results of the two perturbed PWLCM i, i = 1 or 2 (R1 and R2) are combined with a XOR operation to produce a new chaotic stream R with higher randomicity. R is then combined with the plaintext M using a XOR operation. So, the encrypted data will be given by $C = M$ xor R. Sharing the initial conditions (the keys), the receiver can generate the same random sequences R1 and R2, compute R and decrypt the received data since XOR is a symmetric operation, by computing: M=C xor R = (M xor R) xor R.

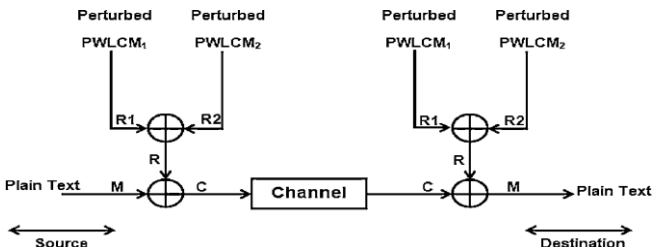

Fig 2. RFCA Scheme

III. Proposed Algorithm

Many stream cipher algorithms include RFCA uses LFSR (Linear Feed Back Shift Register) for key generation in several ways. LFSR-based generators are often hardware oriented and for a variety of them it is known how to achieve desired cryptographic properties. For software implementation, a few key stream generators have been designed which are not based on shift registers such as RC4. Based on the table-shuffling principle, the alleged RC4 stream cipher was designed by Ron Rivest. It was famous as its simple algorithm and fast speed and it was widely used in some popular protocols such as SSL (Secure Socket Layer) and TLS (Transport Layer Security) to protect internet traffic and some others such as WEP (Wired Equivalent Privacy) and Zigbee to secure wireless networks. But the algorithm is kept secret until 1994. After RC4 was released, many people began to analyze it from two aspects: one is the weakness of the KSA, and another is the weakness of the PRGA. In PRGA, the most important is the initial state the S-box, which is used to produce key stream. One of the weaknesses of the PRGA is the relations between the S-boxes in different time. Many attacks tried to resume the initial state of the PRGA and achieved good efficiency. In this paper, we focus on the weakness of PRGA and present an improved RC4 to protect the PRGA from being attacked. The relation between the states of S-boxes which was used by many attacks is destroyed by the Robust RC4.

Robust RC4:

RC4 chooses a secret key k which is called the seed, and an array S called S-box which contains N (N=2n) elements (usually N=256, n=8). RC4 also contains two algorithms: KSA and PRGA. The KSA is Key Scheduling Algorithm. In KSA, the S-box is filled from 0 to N-l, and is throwed into confusion by the secret k. The PRGA is Pseudo Random Generation Algorithm.

In PRGA, there is a public pointer i. It calculates another pointer j(j=j+S[i]) which is secret as the element S[i] is secret. Two elements in S-box are swapped by the pointers i and j. After that, another secret pointer is calculated and a secret pseudo-random word is exported. In order to distinguish the states of S-box in different loops, the states SO, SI , S2 ...S t-l, St, St+1 are defined. The two algorithms are giving as follows:

KSA Algorithm

```
for (i=0;j=0;i<=255;i++)
    j=j + S[i] + K[i]
    swap (s[i] , s[j])
```

PRGA Algorithm:

```
For (i=0;j=0;i<=255;i++)
    j=j + S[i]
     swap (s[i] , s[j])
   t=add (s[i] , s[j])
        S [t])
```

The improved RC4 chooses two secret keys kl and k2 as the seed and two S-boxes S 1 and S2 which all contain N elements from 0 to N-l. In the new algorithm, there are two pointers i and j are used.

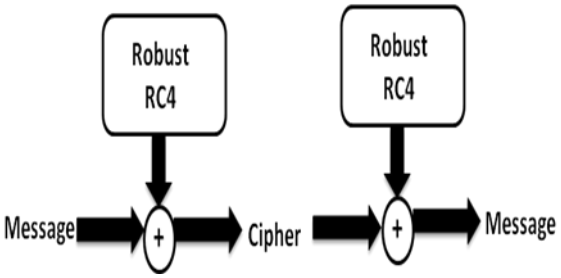

Fig 3. Proposed RC4 Schem

IV. Result Discussion

RC4 for Key Generation:

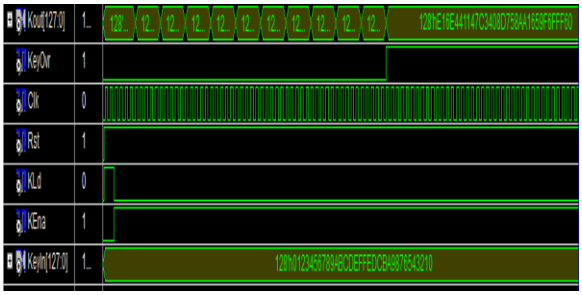

Fig 4. Key generation using RC4

Encryption:

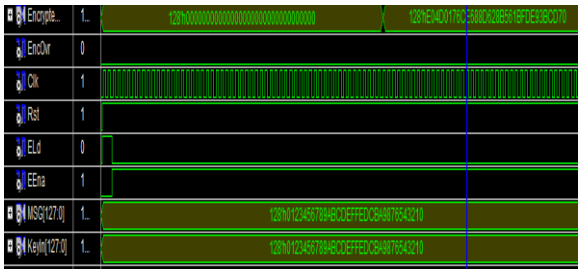

Fig 5. Encryption Algorithm

Decryption:

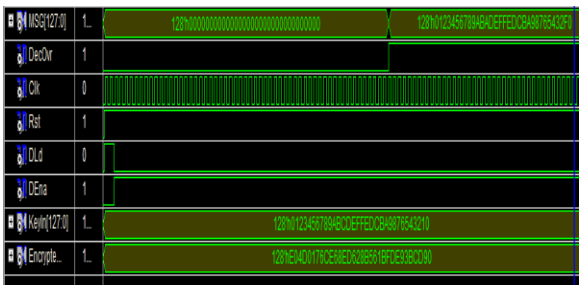

Fig 6. Decryption Algorithm

V. Conclusion

Firstly this paper introduced a Robust RC4 Stream Cipher Algorithm based on the weaknesses of the LFSR in RFCA algorithm. The new algorithm has solved the problem of hardware complexity of LFSR circuits and also improves the security in Zigbee communication protocols. The proposed new algorithm we can use in WPA (Wi-Fi Protected Access) also to protect the data transmission. The proposed algorithm is designed by using Verilog HDL and simulation and Synthesis is done by using ISE Design Suite.

References

[1]. Divya Bharathi R, "Design and simulation of ZigBee Transmitter using Verilog," volume 1 issue.3 march 2013 IJETEE.

[2]. N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proc. ACM Workshop Wireless Security WiSe*, 2004, pp. 32–42.

[3]. J. Buchmann, *Introduction to Cryptography*. Berlin, Germany: Springer,2004.

[4]. W. Puech, J. M. Rodrigues, and J. E. Develay-Morice, "Safe transfer of medical images by conjoined coding: Selective encryption by AES using the stream cipher mode OFB and JPEG compression," Ph.D. dissertation, Centre Hospitalier Univ. Montpellier, Univ. Montpellier II, Nîmes, France, 2006.

[5]. Baseem Bakhache, "Improvement of Security of a Zigbee by a new chaotic algorithm," IEEE Systems Journal 2013.

[6]. S. Li., "Analyses and new designs of digital chaotic ciphers," Ph.D. dissertation, School Electron. Inform. Eng., Xi'an Jiaotong Univ., Xi'an, China, 2003.

[7]. S. Li, X. Mou, and Y Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision," *Comput. Phys. Commun.*, vol. 153, no. 1, pp. 52–58, 2003.

[8]. S. Tao, W. Ruli, and Y. Yixun, "Perturbance based algorithm to expand cycle length of chaotic key stream," *IEEE Electron. Lett.*, vol. 34, no.