Performance Analysis of Genetic Operation Based Encryption in Wireless Sensor Networks

Suganya K [1], Keerthana L[2]
Assistant Professor[1], M.E Communication Systems[2]
Department of Electronics and Communication Engineering
Bharathiyar Institute of Engineering for Women
(kanrosesuganya185@gmail.com)[1], (keerthuloganathan@gmail.com)[2]

ABSTRACT

Wireless Sensor Networks (WSNs) have experienced a fast growth during the last few years. The continuous advancement in wireless technologies, intelligent sensors and micro-electronic-mechanical systems (MEMS) has improved the scope of presentation domains of sensor networks. The key distress in designing crypto-systems for WSNs is to preserve the trade-off among security, performance and cost. A number of security appliances have been proposed for sensor networks to deliver data confidentiality: 1) AES; 2) KATAN; 3) LED and 4) TWINE. However, these schemes consume problems, including security vulnerabilities, need for hardware constructed implementation, and higher computational involvedness. To address these restrictions, we propose a lightweight block cipher founded on chaotic map and genetic processes. The proposed cryptographic arrangement employs elliptic curve points to prove the communicating nodes and as one of the chaotic map parameters to create the pseudorandom bit sequence. This order is used in XOR, mutation, and crossover techniques in order to encrypt the data blocks.

Index terms: Light weight block cipher, Koblitz curves algorithm, Chaotic Map, Genetic Operations.

I. INTRODUCTION

WSNs intended at various industrial, medical, and military applications necessitate research in the design of secure and energy effective protocols. Specifically, the use of sensors in hazardous systems such as nuclear power plants, aircrafts, and hospitals requires effective mechanisms to ensure the authentication, confidentiality and reliability of the sensed and communicated data [1]. However, security is a challenging issue in WSNs, then sensors are usually used in hostile environments. Moreover, restricted memory and processing power, and short communiqué range of sensor nodes (SNs) present several challenges when instigating outmoded cryptographic schemes in wireless environments. WSNs thus require efficient encryption orders in terms of storage space, power ingestion, and operating speed.

The key concern in designing crypto-systems for WSNs is to preserve the trade-

off among security, performance and cost. A number of encryption algorithms for resource guarded SNs have been designed in the past few years. These algorithms may be classified into three main classifications: compact hardware oriented cryptographic outlines, conventional block ciphers, and lightweight block ciphers. Highly enhanced and squeezed block ciphers (e.g., KATAN and KTANTAN) are not freely suitable for WSNs, since the energy consumption also memory usage are in elevation [2].

On the other hand, most of the classical block ciphers accepted for WSNs are vulnerable to an integer of security attacks [5], [7]. Therefore, the contemporary research concentrations on designing secure and lightweight block ciphers. In spitefulness of the best efforts of researchers, several of these lightweight ciphers have relatively deprived performance compared to conventional cryptographic schemes. For example, the quantity of CPU cycles to encrypt one byte data in conventional cryptosystems (e.g., Tiny Encryption Algorithm (TEA) and extended TEA) is fewer than 2000, whereas the lightweight block ciphers (e.g., LED and TWINE) need about 5500 cycles [2].

To address these defects, we propose a chaotic map and genetic actions based block cipher for tiny sensor devices permitting low cost and secure data announcement between the source and the destination nodes.

II. RELATED WORKS

We critically look at a number of existing security mechanisms and their appropriateness for WSNs. Here, we provide an overview of a number of security protocols used in WSN submissions. RC5 is a flexible block cipher that has a variable block size (32, 64, or 128 bits), numeral of rounds (0-255), and key size (0-2040 bits). While RC5 is considered more suitable for WSNs, the key arranging course increases both memory and computational costs [3]. Moreover, the RC5 cipher is considered to take advantage of variable-bit rotation tutoring (e.g., ROL), which is not stayed by many embedded systems like Intel architecture [4]. Another generally used block cipher in WSN is Skipjack developed by the US National Security Agency (NSA). It expenditures an 80-bits key to code or decode 64-bit data blocks. The short key length creates Skipjack vulnerable to the in-depth key search attack [5]. A protracted version, Skipjack-X is proposed by SenSec inventers to make the cipher more secure alongside security attacks. However, it is seen that the strategy is not a apposite replacement of Skipjack in WSNs. Tiny Encryption Algorithm (TEA) is notable intended for its simple edifice and small memory requirement. It has a few weaknesses, such as being vulnerable to a related-key attack and chosen plaintext attack [6].

To exclude these feebleness, a Corrected Block TEA (XXTEA) is designed with 128-bits key. However, the past reported attack against full-round XXTEA dowries a chosen plaintext attack using 259 queries and negligible graft [7]. The Advanced Encryption System (AES) algorithm is a commonly used block cipher based on a

substitution-permutation manner and has a fixed block size of 128 bits. It activates on a 4×4 array of bytes and has a key size of 128, 192, or 256 bits. Conversely, AES seriatim on 10, 12, and 14 rounds for 128, 192, and 256-bits key respectively is still found at risk by the researchers [8].

In addition to security productions, AES is mainly not proper for WSNs due to the demand for more hardware means [9]. KATAN and KTANTAN are two block ciphers wished-for by Canniere et al. [10]. Both ciphers habit blocks of sizes 32, 48 or 64 bits in 80 bits key and iterate for 254 rounds. The central difference between KATAN and KTANTAN is the key scheduling order. The 80 bits key in KATAN is loaded into a register and is repetitively clocked, whereas in KTANTAN the key is permanent. These two encryption schemes are vulnerable to a number of security attacks. An unconfirmed differential cryptanalysis with a concrete complexity in single key sites and related key settings is existing against KATAN [11], [12]. In the same way, a meet-in-the-middle attack is suggested against KTANTAN that make progress the 80-bits secret key of the complete rounds KTANTAN (32/48/64 bits) at time complexity of 272.9, 273.8, and 274.4 [13].

Furthermore, these dualistic algorithms are expensive in relations of energy and memory feasting. LED is a lightweight block cipher that encrypts 64 bits blocks spending either 64 bits or 128 bits key with 32 or 48 rounds respectively [14].

As a replacement for of key scheduling, the key is XORed at every one four rounds in LED. This article is compensated by a larger number of rounds paralleled to the AES. A meet in the middle attack against 8 rounds of LED-64 also 16 rounds of LED-128 and the effects of differential cryptanalysis of full LED in the allied key settings are presented in [15] and [16]. Further these consequences, the LED cipher also consumes supplementary CPU cycles compared to conventional cryptographic systems. TWINE is a 64 bits block cipher that expenditures an 80 bits or 128 bits key [17].

It employs a comprehensive feistel structure with 16 branches and redoes for 36 rounds. The inside *F*-function is repeated 8 times in each round and is composed of a sub-key addition plus a single S-box. The superlative known attacks against TWINE are twofold biclique attacks on TWINE-80 and TWINE-128 with the time involvedness equal to 279.1 and 2126.8 respectively, with a data requirement for the two attacks one and the same to 260 [18].

The Simple Lightweight Encryption Scheme (SLES) stands a block cipher that uses elliptic curve operations over crucial field to generate pseudorandom bit classifications [19]. Instead of using a fixed base point for the intact epoch of a WSN, SLES regenerates a large key lake to share a fresh key at the beginning of the communication process.

This key is used as a different base opinion to generate the haphazard bit

sequence. The inadequacy of SLES is that the computational time intensifications when the range of elliptic curve limits is extended.

III. PROPOSED SYSTEM

The proposed scheme includes a number of benefits: It uses the discrete chaotic map, which supports a wider data range with less computational cost. Most of the encryption schemes use fixed chaotic map parameters to produce the random bit series, but our algorithm uses random values of *'x'* and *'y'* for every session generated in elliptic curve operations.

Projected crypto-system makes different pseudorandom bit sequences for every session and thus preserves liberated behavioral characteristics of the algorithm.

These scheme is more capable compared to Skipjack, Advanced Encryption System (AES), LED, TWINE, in addition Block Cipher based on Chaos (BCC) in terms of CPU depletion and encryption time and speed. Hence, the encryption scheme should be robust, fast, and computationally protected. The block cipher ensures all these properties. The main influences of this paper are threefold:

1) A new key establishing procedure, which reduces the implementation gap between different security mechanisms. This is accomplished by employing the same elliptic curve points for in cooperation the node-verification and pseudorandom bit sequence generation procedures.

2) A novel cryptographic scheme that integrates the remunerations of elliptic curve, discrete chaotic map, and genetic cryptography for WSN applications. This integration guarantees an adequate level of security with limited resources.

3) Robust block cipher that can be used intended for both text and image data encryption. It allows the use of the same encryption appliance in multi-mode sensors, for example, sensing various environmental phenomena as well as images.

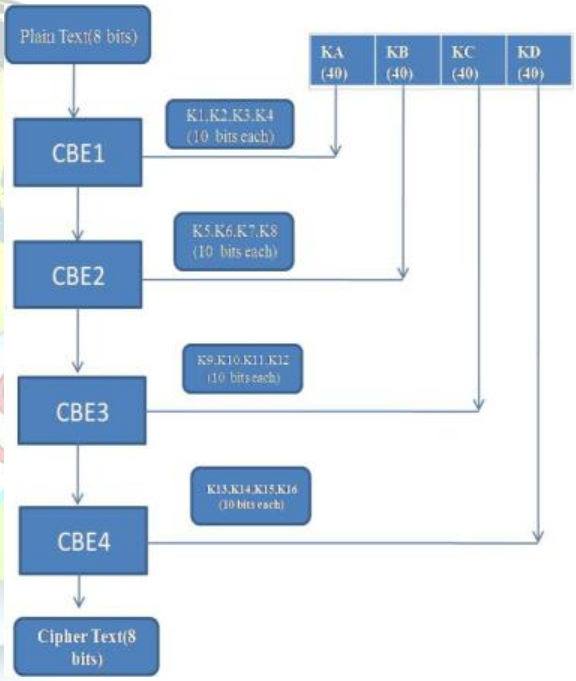


Fig 1: Light weight Koblitz curves block diagram

In our design, 4 Block Cipher (Ek1,Ek2,Ek3,Ek4) are used. Each Block Cipher has 16 bit input and produces 16 bit output. Total key length in our design is 256 bits wide. These 256 bits are divided in to 4 key sub blocks. Each key sub block has 64 bit length. Each block cipher will have 64

bit key, which again be divided in to 4 blocks (16 bit wide).

IV. Block Cipher Key Generation

Block cipher encryption depends on the use of a 10-bit key shared between sender and receiver. From this key, two 8-bit sub keys are produced for use in particular stages of the encryption and encryption algorithm.

In these the cipher, encryption algorithm is suitable for text and image encryption. From the claim point of view, it is desirable for the crypto-system to protect. Private information not single in text form but also in image form. Image data differ from text due to essential features, such as strong correspondence between adjacent pixels and high redundancy.

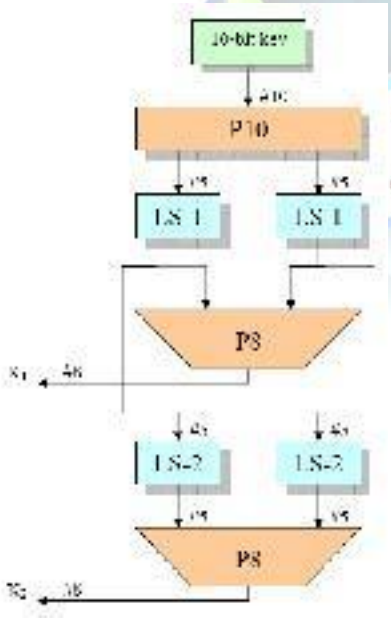


Fig2 Block Cipher Key Generation

V . PERMUTATION

First, permute the key in the following fashion. Let the 10-bit key be elected as (k1, k2,k3, k4, k5, k6, k7, k8, k9, k10). Then the permutation P10 is defined as:

P10 (k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k3, k5, k2, k7, k4, k10, k1, k9, k8, k6).

P10									
1	2	3	4	5	6	7	8	9	10
3	5	2	7	4	10	1	9	8	6

Fig 3: Permutation P10

- **Step 1:** For illustration, the key (1010000010) is permuted to (1000001100).
- **Step 2:** Divide (1000001100) into a left part 5-bit value (10000) and a right part 5-bit value (01100).
- **Step 3:** Perform a circular left shift (LS-1), or rotation, separately. The left value (10000) becomes (00001). The right value (01100) becomes (11000). Concatenate the left part (00001) and the right part (11000) into a 10-bit value (0000111000).
- **Step 4:** Pick out and permutes 8, (don't use 1 and 2), of the 10 bits according to the following rules:

P8							
6	3	7	4	8	5	10	9

Fig 4: Permutation P8

- The result is sub key k1. The value (00 00111000) becomes: k1 = (10100100).

- **Step 5:** Go back to the pair of 5-bit strings produced by the two LS-1 functions, the results of step 3, and perform a circular left shift of 2 bit points on each string. The left value (00001) becomes (00100) and the right value (11000) becomes (00011).Concatenate the left part (00100) and the right part (00011) into a 10-bit value (0010000011).

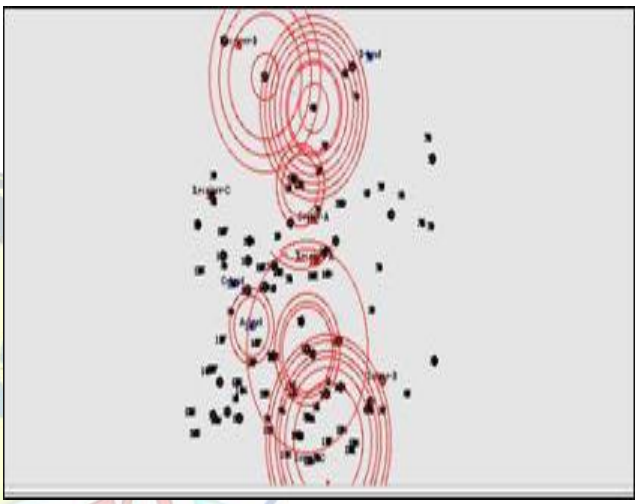
- **Step 6:** Finally, P8 is applied again to produce k2, the value of k2 = 00 10000011.

VI . CONCLUSION

The suggested cryptographic scheme employs elliptic curve points to verify the communicating nodes and as one of the chaotic map factors to engender the pseudorandom bit sequence. This sequence is used in xor, mutation, and crossover operations in order to encrypt the data blocks. We have also performed a number of statistical tests and cryptanalytic doses to appraise the security strength of the algorithm and found the cipher provably secure. This paper presents a fast, provably protected and robust block cipher for WSN applications. The cryptographic scheme incorporates the paybacks of elliptic curve maneuvers, chaotic map and genetic cryptography to provide data confidentiality.

VII. SIMULATION RESULTS

In this result, by using chaotic map and genetic operation in three hundred communicating nodes for wireless sensor network to provide security, and high information entropy.

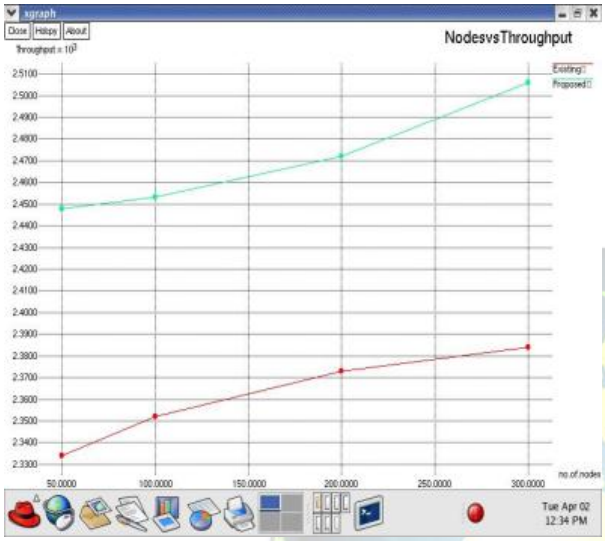


Power Consumption

Compare to existing system, the proposed algorithm provide more power consumption .The graph plotted for relationship between nodes and power consumption.

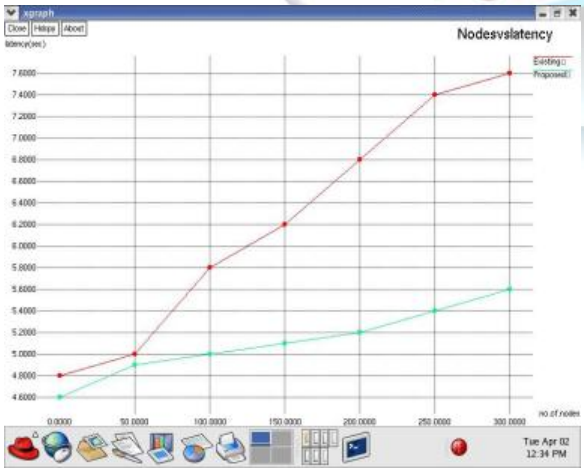
Throughput

This figure shows that the relation between the number of communication nodes and throughput.



Latency

This figure shows that the relation between the number of communication nodes and latency.



REFERENCES

[1] G. R. Sakthidharan and S. Chitra, "A survey on wireless sensor network: An application perspective," in *Proc. ICCCI*, Jan. 2012, pp. 1–5.

[2] M. Cazorla, K. Marquet, and M. Minier, "Survey and benchmark of lightweight block ciphers for WSNs," in *Proc. Int. Conf. Secur. Cryptograph.*, Jul. 2013, pp. 543–548.

[3] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. 2nd Int. Conf. SenSys*, 2004, pp. 162–175.

[4] *Intel Architecture Software Developer's Manual*, Intel Corporation, Santa Clara, CA, USA, 1997.

[5] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," *J. Cryptol.*, vol. 18, no. 4, pp. 291–311, 2005.

[6] J. Kelsey, B. Schneier, and D. Wagner, "Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA," in *Proc. 1st Int. Conf. ICICS*, 1997, pp. 233–246.

[7] E. Yarrkov. (2010). *Cryptanalysis of XXTEA*. [Online]. Available: http://eprint.iacr.org/2010/254.pdf

[8] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique cryptanalysis of the full AES," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 7073. Berlin, Germany: Springer-Verlag, 2011, pp. 344–371.

[9] T. Xiao-Jun, W. Zhu, and Z. Ke, "A novel block encryption scheme based on chaos and an S-box for wireless sensor

networks," *J. Chin. Phys. B*, vol. 21, no. 2, p. 020506, 2012.

[10] C. De Cannière, O. Dunkelman, and M. Kneževi´c, "KATAN and KTANTAN—A family of small and efficient hardware-oriented block ciphers," in *Cryptographic Hardware and Embedded Systems*, vol. 5747. Berlin, Germany: Springer-Verlag, 2009, pp. 272–288.

[11] S. Knellwolf, W. Meier, and M. Naya-Plasencia, "Conditional differential cryptanalysis of NLFSR-based cryptosystems," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 6477. Berlin, Germany: Springer-Verlag, 2010, pp. 130–145.

[12] S. Knellwolf, W. Meier, and M. Naya-Plasencia, "Conditional differential cryptanalysis of trivium and KATAN," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), vol. 7118. Berlin, Germany: Springer-Verlag, 2012, pp. 200–212.

[13] L. Wei, C. Rechberger, J. Guo, H. Wu, H. Wang, and S. Ling, "Improved meet-in-the-middle cryptanalysis of KTANTAN (Poster)," in *Information Security and Privacy* (Lecture Notes in Computer Science), vol. 6812. Berlin, Germany: Springer-Verlag, 2011, pp. 433–438.

[14] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2011, pp. 326–341.

[15] T. Isobe and K. Shibutani, "Security analysis of the lightweight block ciphers XTEA, LED and piccolo," in *Information Security and Privacy* (Lecture Notes in Computer Science), vol. 7372. Berlin, Germany: Springer-Verlag, 2012, pp. 71–86.

[16] F. Mendel, V. Rijmen, D. Toz, and K. Varici, "Differential analysis of the LED block cipher," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 7658. Berlin, Germany: Springer-Verlag, 2012, pp. 190–207.

[17] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, "TWINE: A lightweight block cipher for multiple platforms," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2012, pp. 339–354.

[18] M. Çoban, F. Karakoç, and O. Bozta¸s, "Biclique cryptanalysis of TWINE," in *Cryptology and Network Security*, vol. 7712 (LNCS). Berlin, Germany: Springer-Verlag, 2012, pp. 43–55. [Online]. Available: http://eprint.iacr.org

[19] K. Biswas, V. Muthukkumarasamy, E. Sithirasenan, and K. Singh, "A simple lightweight encryption scheme for wireless sensor networks," in *Distributed Computing and Networking* (Lecture Notes in Computer Science), vol. 8314. Berlin, Germany: Springer-Verlag, 2014, pp. 499–504.

[20] S. Chen, X. Zhong, and Z. Wu, "Chaos block cipher for wireless sensor network," *J. Sci. China Ser. F, Inf. Sci.*, vol. 51, no. 8, pp. 1055–1063, 2008.

[21] J. Yang, D. Xiao, and T. Xiang, "Cryptanalysis of a chaos block cipher for wireless sensor network," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 844–850, 2011.

[22] Y. Liu and S. Tian, "Design and statistical analysis of a new chaos block cipher for WSN," in *Proc. IEEE ICITIS*, Dec. 2010, pp. 327–330.

[23] M. Amara and A. Siad, "Elliptic curve cryptography and its applications," in *Proc. 7th Int. WOSSPA*, May 2011, pp. 247–250.

[24] NIST. (2014). *Download Documentation and Software*. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

[25] Q. Fang, Y. Liu, and X. Zhao, "A chaos-based secure cluster protocol for wireless sensor networks," *Kybernetika*, vol. 44, no. 4, pp. 522–533, 2008.