An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks

Kamanashis Biswas, Vallipuram Muthukkumarasamy, and Kalvinder Singh

***Abstract*— Over the past decade, the application domain of wireless sensor networks has expanded steadily, ranging from environmental management to industry control, and from structural health monitoring to strategic surveillance. With the proliferation of sensor networks at home, work place, and beyond, securing data in the network has become a challenge. A number of security mechanisms have been proposed for sensor networks to provide data confidentiality: 1) advanced encryption system; 2) KATAN; 3) LED; and 4) TWINE. However, these schemes have drawbacks, including security vulnerabilities, need for hardware-based implementation, and higher computational complexity. To address these limitations, we propose a lightweight block cipher based on chaotic map and genetic operations. The proposed cryptographic scheme employs elliptic curve points to verify the communicating nodes and as one of the chaotic map parameters to generate the pseudorandom bit sequence. This sequence is used in XOR, mutation, and crossover operations in order to encrypt the data blocks. The experimental results based on Mica2 sensor mote show that the proposed encryption scheme is nine times faster than the LED protocol and two times faster than the TWINE protocol. We have also performed a number of statistical tests and cryptanalytic attacks to evaluate the security strength of the algorithm and found the cipher provably secure.**

***Index Terms*— Wireless sensor network, pseudorandom bit sequence generator, data encryption, elliptic curve, chaotic map, mutation, crossover.**

I. Introduction

WIRELESS Sensor Networks (WSNs) have experienced a rapid growth during the last few years. The continuous advancement in wireless technologies, intelligent sensors and micro-electronic-mechanical systems (MEMS) has increased the scope of application domains of sensor networks. WSNs aimed at various industrial, medical, and military applications necessitate research in the design of secure and energy efficient protocols. Specially, the use of sensors in critical systems such as nuclear power plants, aircrafts, and hospitals requires effective mechanisms to ensure the authenticity, confidentiality and integrity of the sensed and transmitted data [1]. However, security is a challenging issue in WSNs, since sensors are usually deployed in hostile environments. Moreover, limited memory and processing power, and short communication range of sensor nodes (SNs) introduce several challenges when implementing traditional cryptographic schemes in wireless environments. WSNs thus require efficient encryption schemes in terms of storage space, power consumption, and operating speed.

The key issue in designing crypto-systems for WSNs is to maintain the trade-off among security, performance and cost. Several encryption algorithms for resource constrained SNs have been designed in the past few years. These algorithms may be classified into three main categories: compact hardware oriented cryptographic schemes, conventional block ciphers, and lightweight block ciphers. Highly optimized and compact block ciphers (e.g., KATAN and KTANTAN) are not readily suitable for WSNs, since the energy consumption and memory usage are high [2]. On the other hand, most of the classical block ciphers adopted for WSNs are vulnerable to a number of security attacks [5], [7]. Therefore, the current research focuses on designing secure and lightweight block ciphers. In spite of the best efforts of researchers, many of these lightweight ciphers have relatively poor performance compared to conventional cryptographic schemes. For example, the number of CPU cycles to encrypt one byte data in conventional crypto-systems (e.g., Tiny Encryption Algorithm (TEA) and extended TEA) is less than 2000, whereas the lightweight block ciphers (e.g., LED and TWINE) require about 5500 cycles [2]. To address these shortcomings, we propose a chaotic map and genetic operations based block cipher for tiny sensor devices enabling low cost and secure data communication between the source and the destination nodes.

The proposed scheme includes a number of benefits: i) it uses the discrete chaotic map, which supports a wider data range with low computational cost. Most of the encryption schemes use fixed chaotic map parameters to generate the random bit sequences, but our algorithm uses random values of *'x'* and *'y'* for every session generated by elliptic curve operations; ii) the proposed crypto-system makes different pseudorandom bit sequences for every session and thus preserves independent behavioural characteristics of the algorithm; iii) the scheme is more efficient compared to SkipJack, Advanced Encryption System (AES), LED, TWINE, and Block Cipher based on Chaos (BCC) in terms of CPU consumption and encryption time; iv) the proposed encryption algorithm is suitable for both text and image encryption. From the application point of view, it is desirable for the

Manuscript received October 14, 2014; revised November 27, 2014; accepted December 1, 2014. Date of publication December 18, 2014; date of current version March 27, 2015. The associate editor coordinating the review of this paper and approving it for publication was Dr. M. R. Yuce.

K. Biswas and V. Muthukkumarasamy are with the School of Information and Communication Technology, Griffith University, Gold Coast, QLD 4111, Australia (e-mail: kamanashis.biswas@griffithuni.edu.au; v.muthu@griffith.edu.au).

K. Singh is with the IBM Australia Development Laboratory, Gold Coast, QLD 4215, Australia, and also with Griffith University, Gold Coast, QLD 4111, Australia (e-mail: kalsingh@au.ibm.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSEN.2014.2380816

crypto-system to protect confidential information not only in text form but also in image form. Image data differ from text due to intrinsic features, such as strong correlation between adjacent pixels and high redundancy. Hence, the encryption scheme should be robust, fast, and computationally secure. Experimental results show that the proposed block cipher ensures all these properties. The main contributions of this paper are threefold:

1) a new key establishment procedure, which minimizes the implementation gap between different security mechanisms. This is achieved by employing the same elliptic curve points for both the node-verification and pseudo-random bit sequence generation processes.
2) a novel cryptographic scheme that integrates the benefits of elliptic curve, discrete chaotic map, and genetic cryptography for WSN applications. This integration ensures an adequate level of security with limited resources.
3) a robust block cipher that can be used for both text and image data encryption. It enables the use of the same encryption mechanism in multi-mode sensors, for example, sensing different environmental phenomena as well as images.

The rest of the paper is organized as follows: In Section II, we discuss the feasibility of existing security mechanisms in WSN environments. Section III provides details of the new key establishment procedure, pseudorandom bit sequence generation process and the proposed encryption scheme. A concrete security treatment and analysis is presented in Section IV. Section V and Section VI examine the security and performance analysis of our proposed protocol respectively. Finally, Section VII concludes the paper.

II. Related Works

We critically examine a number of existing security mechanisms and their suitability for WSNs. Here, we provide an overview of a number of security protocols used in WSN applications.

RC5 is a flexible block cipher that has a variable block size (32, 64, or 128 bits), number of rounds (0-255), and key size (0-2040 bits). Although RC5 is considered more suitable for WSNs, the key scheduling process increases both memory and computational costs [3]. Moreover, the RC5 cipher is designed to take advantage of variable-bit rotation instruction (e.g., ROL), which is not supported by many embedded systems like Intel architecture [4].

Another widely used block cipher in WSN is Skipjack developed by the US National Security Agency (NSA). It uses an 80-bits key to encrypt or decrypt 64-bit data blocks. The short key length makes SkipJack vulnerable to the exhaustive key search attack [5]. An extended version, SkipJack-X is proposed by SenSec designers to make the cipher more secure against security attacks. However, it is seen that the strategy is not a proper replacement of SkipJack in WSNs.

Tiny Encryption Algorithm (TEA) is notable for its simple structure and small memory requirement. It has a few weaknesses, such as being vulnerable to a related-key attack and chosen plaintext attack [6]. To eliminate these weaknesses, a Corrected Block TEA (XXTEA) is designed with 128-bits key. However, the last reported attack against full-round XXTEA presents a chosen plaintext attack using 2^{59} queries and negligible work [7].

The Advanced Encryption System (AES) algorithm is a widely used block cipher based on a substitution-permutation process and has a fixed block size of 128 bits. It operates on a 4×4 array of bytes and has a key size of 128, 192, or 256 bits. However, AES running on 10, 12, and 14 rounds for 128, 192, and 256-bits key respectively is still found vulnerable by the researchers [8]. In addition to security issues, AES is mainly not suitable for WSNs due to the demand for more hardware resources [9].

KATAN and KTANTAN are two block ciphers proposed by Canniere et al. [10]. Both ciphers use blocks of sizes 32, 48 or 64 bits under 80 bits key and iterate for 254 rounds. The main difference between KATAN and KTANTAN is the key scheduling scheme. The 80 bits key in KATAN is loaded into a register and is repeatedly clocked, whereas in KTANTAN the key is fixed. These two encryption schemes are vulnerable to a number of security attacks. A conditional differential cryptanalysis with a practical complexity in single key settings and related key settings is presented against KATAN [11], [12]. Similarly, a meet-in-the-middle attack is proposed against KTANTAN that recovers the 80-bits secret key of the full rounds KTANTAN (32/48/64 bits) at time complexity of $2^{72.9}$, $2^{73.8}$, and $2^{74.4}$ [13]. Furthermore, these two algorithms are expensive in terms of energy and memory consumption.

LED is a lightweight block cipher that encrypts 64 bits blocks using either 64 bits or 128 bits key with 32 or 48 rounds respectively [14]. Instead of key scheduling, the key is XORed at every four rounds in LED. This feature is compensated by a larger number of rounds compared to the AES. A meet-in-the-middle attack against 8 rounds of LED-64 and 16 rounds of LED-128 and the results of differential cryptanalysis of full LED in the related key settings are presented in [15] and [16]. Besides these pitfalls, the LED cipher also consumes more CPU cycles compared to conventional cryptographic schemes.

TWINE is a 64 bits block cipher that uses an 80 bits or 128 bits key [17]. It employs a generalized feistel structure with 16 branches and iterates for 36 rounds. The internal F-function is repeated 8 times in each round and is composed of a sub-key addition and a single S-box. The best known attacks against TWINE are two biclique attacks on TWINE-80 and TWINE-128 with the time complexities equal to $2^{79.1}$ and $2^{126.8}$ respectively, with a data requirement for the two attacks equal to 2^{60} [18].

The Simple Lightweight Encryption Scheme (SLES) is a block cipher that uses elliptic curve operations over prime field to generate pseudorandom bit sequences [19]. Instead of using a fixed base point for the entire lifetime of a WSN, SLES pre-generates a large key pool to share a new key at the beginning of the communication process. This key is used as a new base point to generate the random bit sequence. The limitation of SLES is that the computational time increases when the range of elliptic curve parameters is extended.

The chaos-based cryptographic scheme has been widely investigated over the past few years and a number of

chaotic block ciphers are proposed for conventional networks. However, most of these chaos-based ciphers are not suitable for WSNs, since sensor nodes are resource constrained. The chaotic maps usually generate the sequences of random floating-point numbers which are not supported by tiny sensor nodes (e.g., Mica2). To overcome this problem, a chaos block cipher with integer parameters was proposed [20]. The algorithm divides the plaintext into 8-bit blocks and then performs bit permutation. The permuted bits are encrypted in four rounds Feistel cipher using four bytes sub-keys. These sub-keys are generated by performing XOR operations with 32-bits integer chaos. Finally, the 8-bits are permuted again to generate the corresponding ciphertext. However, this chaos block cipher cannot resist differential attack because the number of rounds is too small and the calculation precision of round function is too short [21]. Moreover, the energy consumption and memory usage are also not analysed in this protocol.

Xiao-Jun et al. proposed a fast, secure, and low resource consumption algorithm based on the integer discretization of a chaotic map, the Feistel network structure and an S-box [9]. The encryption algorithm uses a block length of 32 bits, a key length of 128 bits, an initial vector of 32 bits, and 14 rounds iteration to generate 32 bits ciphertext. Experimental outcomes and analysis show that the cipher has a large key space, very good diffusion and good statistical balance. The main drawback of this protocol is that 32-bit block size is not semantically secure to resist a chosen-plaintext attack.

Another block cipher based on chaotic S-boxes and a substitution-permutation network was proposed in [22]. The encryption procedure avoids floating-point operations and multiplications in order to minimize the energy consumption. Similar to RC5, the block cipher based on chaos (BCC) supports variable word size (w), number of rounds (r), and length of the encryption key (b). Although the authors claim that BCC has good diffusion property and low energy consumption, they failed to present any security and performance analysis.

III. The Proposed Block Cipher

Our proposed block cipher is divided into three phases: a) key establishment phase, b) pseudorandom bit sequence generation phase, and c) encryption phase. Each of the phases is described in detail below.

A. Key Establishment Phase

In this phase, a secret key is randomly selected from the key pool and exchanged between sending and receiving nodes. The key establishment phase uses an elliptic curve over prime field to generate a large key pool for node-verification purpose. An elliptic curve over prime field is an algebraic expression and is defined by the following equation:

$$y^2(mod\ p) = x^3 + Ax + B(mod\ p) \tag{1}$$

where, A and B are the coefficients and the variables x and y take the values only from the finite field within the range of prime field p. Given the values of these parameters, a large number of points on the curve can be generated using basic elliptic curve operations, known as point addition and point doubling [23].

We assume that the elliptic curve parameters (i.e., prime field p, base point G (x, y), co-efficients A and B), and chaotic map parameters (i.e., m, N, μ and β) are predistributed securely among all sensor nodes in the WSN. Now, each SN generates a list of elliptic curve points referred to as key pool by using elliptic curve operations. When a node is required to send data packets, it randomly selects a secret key (x_i, y_i) from the key pool and converts it into hash code using a pre-defined hash function. Then, the hash code is shared with the destination node. The destination node retrieves the shared key by matching the received code with the hash code generated for each point of its own key pool. Upon successful retrieval of the secret key, destination node verifies the legitimacy of the source node and sends an acknowledgement. This secret key (x_i, y_i) is used in N-logistic tent map with other parameters to generate the random bit sequence.

B. Generation of Pseudorandom Bit Sequence

This phase involves the generation of pseudorandom bit sequences using chaotic functions. The security level of a discrete chaotic map depends on the properties of the random number generation scheme such as unpredictability and unlimited period. However, most of the chaotic maps involve high-precision floating point calculation to produce the sequences of random floating-point numbers which are not suitable for resource limited SNs. However, the advantage of using N-logistic tent map is that it can deal with integer parameters and thus simplifies the computation process in SNs. We have investigated the randomness of the derived binary sequence using the test code developed by the National Institute of Standards and Technology (NIST) and found that the sequence is random [24]. The following equations present the chaotic functions used to generate the pseudorandom bit sequences in our proposed encryption scheme.

$$\begin{cases} x_{n+1} = \mu x_n(N - x_n/m)/N - y_n/2 \\ y_{n+1} = \beta(N - |N - y_n|) \end{cases} \tag{2}$$

where $x \in (0, m\times\mathrm{N})$, $\mu \in [0, 4]$, $y \in (0, 2\times N)$, $\beta \in [1, 2]$, $N = 2^K$, and $m = 2^k$ with integers K and k [25]. The seed key is the set $\{x_i, y_i, m, N, \mu, \beta\}$, where, the values of m, N, μ, and β are predistributed in the sensor nodes, and the initial values of x_i and y_i are exchanged through the key establishment phase as explained earlier.

C. The Encryption Process

The overall encryption process is shown as a block diagram presented in Fig. 1 where the symbols '*M*' and '*XO*' denote mutation and crossover operation respectively. Confusion and diffusion are two general principles that guide the design of a block cipher. Confusion is achieved by obscuring the relationship between the ciphertext and the symmetric key as best as possible. On the other hand, diffusion is achieved by dissipating the redundancy of the plaintext through spreading it over the ciphertext. The proposed cryptographic scheme

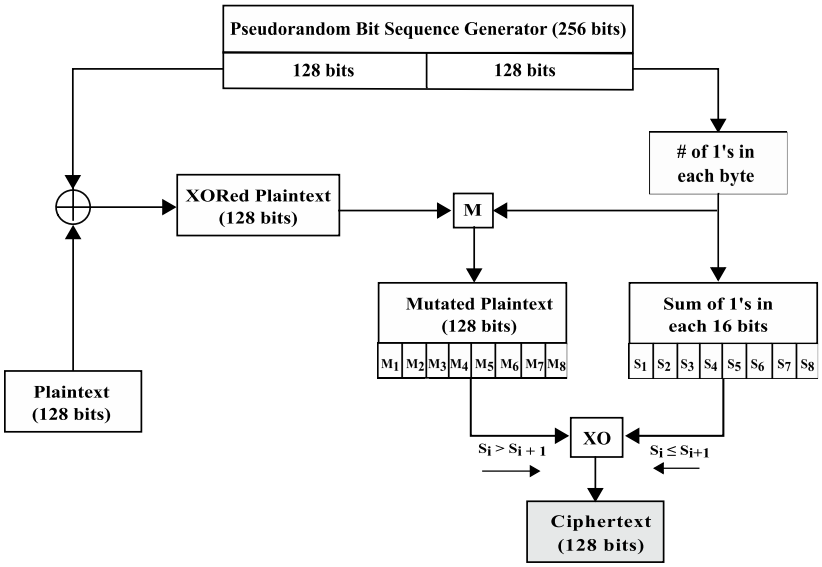

Fig. 1. The general schema of the proposed encryption process.

implements three different operations: XOR, mutation, and crossover. The additive cipher *XOR* is secure when the key-stream is as long as the plaintext. On the other hand, *mutation* is a process of flipping one or multiple bits in a given bit string. *Crossover* is a process of taking two parent bit strings and producing corresponding child bit strings by interchanging selected parts of bit strings between the parents. These two genetic operations are used in genetic algorithm to generate a new population from the existing one [26]. In our proposed encryption mechanism, the mutation and crossover genetic operations are used as tools for introducing diffusion and confusion properties in the ciphertext. The mutation process is applied to create random diversity (diffusion) in the ciphertext, whereas the crossover operation is used to change the order of the mutated text or image data (confusion). The main benefit of using genetic operations is that they introduce relatively fair diversity in the ciphertext. Below, we describe the encryption procedure with typical examples.

We first divide the pseudorandom bit sequence generated by chaotic map into 256-bit blocks, and each block is divided into two sub-blocks of 128 bits. Then, we calculate the number of 1's in each byte as well as the sum of 1's for each two consecutive bytes in the other half of the pseudorandom bit sequence. After that, we convert the plaintext into their corresponding binary codes and group them into blocks of 128-bits. This block is XORed with the first sub-block of the pseudorandom bit sequence. Then, the mutation is performed on each byte of the XORed binary codes using the total number of 1's in each byte as the starting index of the mutation process. For example, if the number of 1's in the first byte of the second sub-block of a pseudorandom bit sequence is 7, we mutate the 7^{th} and 8^{th} number bits in the first byte of the XORed plaintext. Thereafter, the crossover operation is executed on mutated plaintext as shown in the Fig. 1 to generate the ciphertext. At this step, we take four consecutive bytes from mutated plaintext and then perform crossover operations according to the number of 1's in the second sub-block of pseudorandom bit sequence. For example, in the case of B_1–B_2–B_3–B_4 being the four successive bytes of mutated binary codes. We compare the sum of 1's (*sum1*) in the first two bytes in pseudorandom bit sequence with that of the next two consecutive bytes (*sum2*). If *sum1* is greater than *sum2*, then the crossover is performed from left to right (i.e., 1 to *sum1*), otherwise it is done from right to left (i.e., 32 to *sum2*). This crossover operation is done repeatedly (e.g., B_1–B_2–B_3–B_4, B_2–B_3–B_4–B_5, ... , B_{14}–B_{15}–B_{16}–B_1) so that each byte in mutated plaintext performs the operation at least twice. The decryption process is simply the inverse of the encryption procedure.

IV. Concrete Security Evaluation

In this section, we present the formal description of the proposed cryptographic scheme, mathematical notation of indistingushability under a chosen-plaintext attack (IND-CPA), and IND-CPA security analysis.

A. Formal Description

A symmetric encryption algorithm is defined by a family of functions such as F: Keys(F) $\times$ Dom(F) $\rightarrow$ Range(F). For $K \in$ Keys(F), F_K: Dom(F) $\rightarrow$ Range(F) can be defined as $\forall x \in Dom(F)$: $F_K(x) = F(K, x)$. Thus, our proposed encryption scheme with Keys(F) $= \{0,1\}^{256}$ and Dom(F) $=$ Range(F) $= \{0,1\}^{128}$ can be expressed as, F: $\{0,1\}^{256} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ where, the mode of operation over F with a random starting point is a stateless block cipher. The encryption and decryption algorithms are presented in *Algorithm 1*. The starting point $S[0]$ is used to define a set of values on which F_K is applied to generate a "pseudorandom bit sequence" of desired length. Then, the sequence is subdivided into two parts ($P[i]^L$ and $P[i]^R$) to perform XOR($\oplus$), mutation($\bar{\mu}$) and crossover($\otimes$) operation as shown in the *Algorithm 1*.

Algorithm 1 Encryption and Decryption Algorithm

1: **Procedure** ENC_ALG $\xi_K(M)$	1: **Procedure** DEC_ALG $D_K(M)$
2: $M[1] \ldots M[n] \leftarrow M$	2: $C[1] \ldots C[n] \leftarrow C$
3: $S[0] \leftarrow \{0,1\}^l$	3: $S[0] \leftarrow \{0,1\}^l$
4: **for** $i = 1 \ldots n$ do	4: **for** $i = 1 \ldots n$ do
5: $P[i] \leftarrow F_K(S[0], i)$	5: $P[i] \leftarrow F_K(S[0], i)$
6: $CT1[i] \leftarrow P[i]^L \oplus M[i]$	6: $M1[i] \leftarrow C[i] \otimes P[i]^R$
7: $CT2[i] \leftarrow CT1[i] \bar{\mu} P[i]^R$	7: $M2[i] \leftarrow M1[i] \bar{\mu} P[i]^R$
8: $C[i] \leftarrow CT2[i] \otimes P[i]^R$	8: $M[i] \leftarrow P[i]^L \oplus M2[i]$
9: **end for**	9: **end for**
10: **return** C	10: **return** M
11. **end procedure**	11. **end procedure**

B. Indistinguishability Under Chosen-Plaintext Attack

Suppose an adversary is given a sequence of ciphertexts ($C_1 \ldots C_n$) where C_i is either an encryption of $M_{0,i}$ or $M_{1,i}$ for all $1 \leq i \leq n$. Now, the goal of the adversary is to generate the sequence of ciphertexts and guess whether $M_{0,i} \ldots M_{0,n}$ were encrypted or $M_{1,i} \ldots M_{1,n}$ were encrypted. The encryption scheme is considered secure if the adversary finds it hard to distinguish which of the two message sequences correspond to the cipher, C_i.

Let us now formalize an attack scenario. Let $\pi = (K, \xi, D)$ be a symmetric encryption scheme. An adversary 'A' is a program that has access to an oracle known as LR (left or right) oracle. 'A' can input any pair of equal-length messages and the oracle will return a ciphertext. For $K \in Key$, let $Real_K$ be the left oracle that on input M returns $C \xleftarrow{\$} \xi_K(M)$ and $Fake_K$ be the right oracle that on input M returns $C \xleftarrow{\$} \xi_K(0^{|M|})$. Now, the *ind-cpa advantage* of A, i.e, the success of the adversary in breaking the encryption scheme can be defined by the difference in probabilities of the two worlds as follows [27]:

$$Adv_{\pi\xi}^{ind-cpa}(A) = Pr[Real_{\pi\xi}^{A} \Rightarrow 1] - Pr[Fake_{\pi\xi}^{A} \Rightarrow 1] \quad (3)$$

If $Adv_{\pi\xi}^{ind-cpa}(A)$ is very small (i.e., close to zero), it indicates that 'A' is doing poorly and F resists the attacks that A is mounting. On the other hand, if $Adv_{\pi\xi}^{ind-cpa}(A)$ is large (i.e., close to one), it means that 'A' is doing well and F is not secure. The next sub-section uses the above analysis to test the security of the proposed scheme.

C. IND-CPA Security of the Encryption Scheme

Let F: $\{0,1\}^{256} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ be our proposed block cipher. Let A be an adversary that executes in time t and performs at most q queries, which means totaling at most σ n-bit blocks. Then, according to [28], there exists an adversary B, attacking the pseudorandom function (PRF) security of F such that

$$Adv_{\pi\xi}^{ind-cpa}(A) \leq Adv_{F}^{prf}(B) + \frac{0.5\sigma^2}{2^n} \quad (4)$$

Although our proposed encryption scheme is provably secure, there is a possibility that a collision may produce 'overlaps' in the pseudorandom bit sequences. We assume that the best attack against the PRF security of our proposed block cipher is a birthday attack since the attack is used to find a collision between random attack attempts. As mentioned before, F is our proposed block cipher that takes 128 bits plaintext to generate corresponding ciphertext. Suppose we want to encrypt $q = 2^{20}$ messages where each message is 2^{15} bits long, thus in total, 2^{35} bits have to be encrypted resulting in a total of 2^{28} number of blocks (σ). Let A be an adversary that cannot do better than mounting a birthday attack (B) against the block cipher F. It means that the advantage of the attack $Adv_{F}^{prf}(B) \not> \sigma^2/2^{128}$. Under this condition, the IND-CPA security of our proposed encryption scheme is: $Adv_{\pi\xi}^{ind-cpa}(A) = \sigma^2/2^{128} + 0.5\sigma^2/2^{128} = 1.5(2^{56}/2^{128}) \leq 1/2^{71}$, which is a very small number indeed. It indicates that the cipher is secure under the assumption that the best attack on the PRF security of the proposed block cipher is a birthday attack.

V. Security Analysis and Test Results

We have tested our proposed encryption scheme against various security attacks. Here, we describe some of the important security analysis results including key-space analysis, statistical analysis, differential attack analysis, information entropy analysis, known-plaintext and ciphertext-only attack analysis. The experiments are performed on two gray-level images with a size of 128 × 128 using MATLAB simulator.

A. Key-Space Analysis

Key space size is determined by the total number of different keys used in the encryption scheme. The key-space of a good encryption algorithm should be large enough to make brute-force attacks infeasible. In our proposed encryption scheme, the set of secret parameters is $\{x_i, y_i, \mu, \beta, m, N\}$, where, x_i, y_i, μ, β, m, and N are integer values, having the following range: $\{x_i, y_i, \mu, \beta, N\} \in [1, 2^{128}]$ and $m \in [1, 2^{64}]$. Therefore, the complete key-space of the proposed encryption scheme is $5.087 \times 10^{135} \approx 2^{448}$. Hence, we conclude that brute force attack is not feasible for such a large key space.

B. Statistical Analysis

We have performed several statistical analyses to test the robustness of our proposed encryption procedure. From the experiments, we have found that the encrypted information in the cipher image is nearly uniformly distributed. Here, we present the results of the histogram analysis and correlation analysis of two adjacent pixels in cipher images.

1) Histogram Analysis: An image histogram plots the pixels at each gray scale level in order to illustrate the distribution of pixels in that image. It is expected that the distribution of pixels in the cipher image should hide the redundancy of the original image and should not leak any information about the plain image or the relationship between the plain image and the cipher image. We have calculated and analysed the histograms of two encrypted images as well as original images consisting of different contents. The histograms of the plain images shown in Fig. 2(a) and 2(e) and their corresponding cipher images Fig. 2(c) and 2(g) produced by the proposed scheme are depicted in Fig. 2(b), 2(f); and 2(d), 2(h) respectively. From Fig. 2(d) and 2(h), it can be seen that the

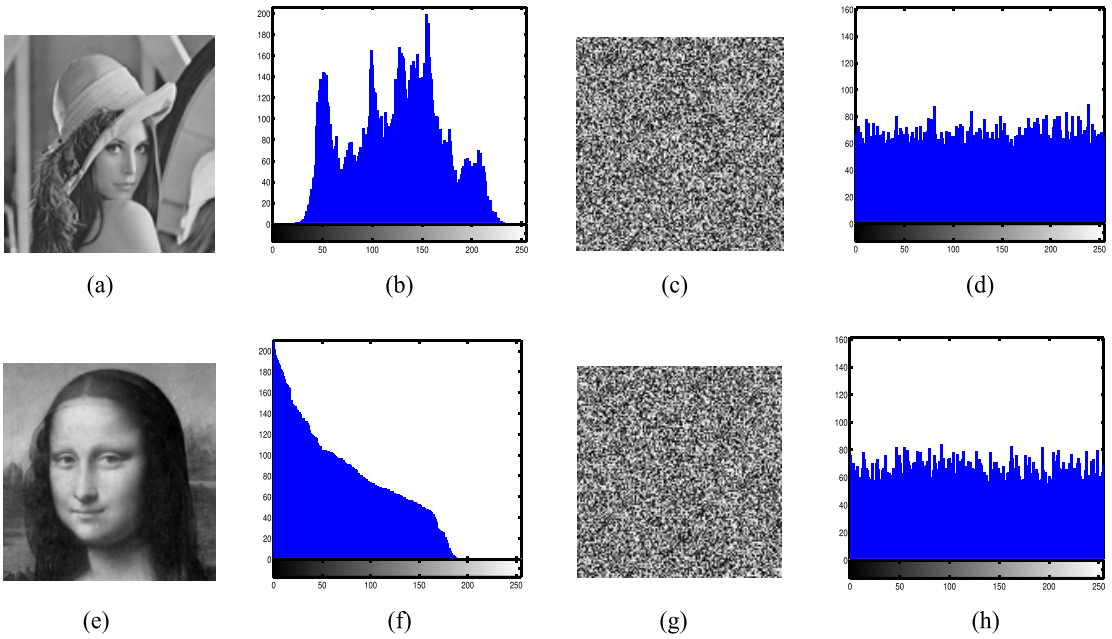

Fig. 2. Histograms of plain and cipher images: (a) Plain image Lena.png. (b) Histogram of Lena.png. (c) Cipher image Lena_enc.png. (d) Histogram of Lena_enc.png. (e) Plain image Mona.gif. (f) Histogram of Mona.gif. (g) Cipher image Mona_enc.gif. (h) Histogram of Mona_enc.gif.

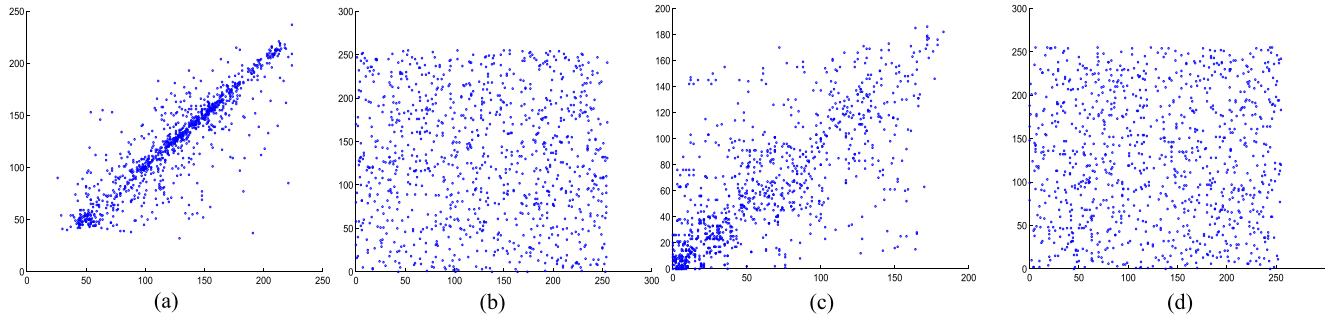

Fig. 3. Correlation of two horizontally adjacent pixels: (a) Plain image (Lena.png). (b) Cipher image (Lena_enc.png). (c) Plain image (Mona.gif). (d) Cipher image (Mona_enc.gif).

histograms of the cipher images are significantly different from that of the plain images and have a reasonably uniform distribution. It demonstrates that the proposed crypto-system can resist statistical attack well.

2) Correlation of Two Adjacent Pixels: The pixels in an ordinary image are highly correlated with their adjacent pixels either in horizontal, vertical, diagonal or anti-diagonal directions. However, a secure encryption scheme should maintain sufficiently low correlation in the adjacent pixels in the cipher image. To compare the correlations of adjacent pixels, we have calculated the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, two diagonally adjacent pixels, and two anti-diagonally adjacent pixels in the plain and cipher images respectively. We have performed the following procedure to find out the correlation between two adjacent pixels. We have randomly selected 1000 pairs of adjacent pixels from the plain image. Then, we have calculated their correlation coefficient using the following formulas:

$$cov(x, y) = E((x - E(x))(y - E(y))) \quad (5)$$

$$r_{xy} = \frac{cov(x, y)}{\sqrt{var(x)}\sqrt{var(y)}} \quad (6)$$

where x and y are gray-levels of two adjacent pixels in the image. Fig. 3(a) and Fig. 3(c) show the correlations of two horizontally adjacent pixels in the original images in Fig. 2(a) and Fig. 2(e) respectively, whereas Fig. 3(b) and Fig. 3(d) represent the correlation of two horizontally adjacent pixels in corresponding cipher images in Fig. 2(c) and Fig. 2(g) respectively. From the figures, it can be seen that the two horizontally adjacent pixels in the plain images are highly correlated but the correlation between the two adjacent pixels in the cipher images is negligible. Similar results are obtained for the vertical, diagonal, and anti-diagonal directions, and shown in Table I.

C. Differential Attack Analysis

To test the impact of a one-pixel change in the original image, two common measures are used: the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). Let C_1 and C_2 be two cipher images, whose corresponding plain images have only one pixel difference. We define the gray values of the pixels at grid *(i, j)* in C_1 and C_2 as $C_1(i, j)$ and $C_2(i, j)$, respectively. We declare a bipolar

TABLE I
CORRELATION COEFFICIENTS OF ADJACENT PIXELS

Input Images	Horizontal	Vertical	Diagonal	Anti-diagonal
Lena.png	0.8960	0.9473	0.8647	0.8907
Lena_enc.png	0.0027	0.0019	0.0070	0.0034
Mona.gif	0.7798	0.7719	0.7093	0.7343
Mona_enc.gif	0.0197	0.0356	0.0061	0.0280

TABLE II
NPCR AND UACI TEST RESULT

Input Images	NPCR	UACI
Lena_enc.png	99.676	33.462
Mona_enc.gif	99.621	33.422

array D with the same size as image C_1 or C_2. The value of $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$ as follows; if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 1$, otherwise $D(i, j) = 0$. The NPCR is defined by the following formula:

$$NPCR = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\% \tag{7}$$

where W and H are the width and height of C_1 or C_2. Similarly, the UACI is defined by the following equation:

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i, j) - C_2(i, j)|}{255}\right] \times 100\% \tag{8}$$

The NPCR calculates the percentage of different pixel numbers between the two images and the UACI calculates the average intensity of differences between the two images. To calculate the NPCR and UACI value for our proposed algorithm, we have changed one pixel value of the two plain images (Fig. 2(a) and Fig. 2(e)) and generated the corresponding cipher images. The results of the NPCR and UACI tests are shown in Table II. From the results, it can be seen that our proposed encryption scheme passes both the NPCR and UACI randomness tests.

D. Information Entropy Analysis

Information entropy presents the degrees of uncertainty in the system and can be used to analyse the indeterminateness of an encryption scheme. We can formally define the entropy, $H(m)$ of any message m as follows:

$$H(m) = \sum_{i=1}^{N} p(m_i) \times log_2 \frac{1}{p(m_i)} \tag{9}$$

where $p(m_i)$ denotes the probability of the symbol m_i and N is the total number of symbols. If the output of a cipher emits 2^n symbols, then the entropy should be n. As an example, the ideal entropy of a 256-gray scale image must be 8 since the pixel elements have 2^8 possible values. If the entropy value is less than 8, there exists a certain degree of predictability, which threatens the security of the encryption algorithm.

TABLE III
INFORMATION ENTROPY OF PLAIN AND CIPHER IMAGES

Input Images	Plain image	Cipher image
Lena	7.4102	7.9988
Mona	7.3499	7.9884

The Table III shows the entropies for both plain images and cipher images. It can be seen that the entropy values of cipher images are much closer to the expected value of 8. This means that the chance of information leakage is negligible and the proposed scheme is secure against entropy attack.

E. Known Plaintext and Ciphertext Only Attack

The known plaintext attack (KPA) is an attack based on having samples of both plaintext and corresponding ciphertext. Now, using this information, the attacker tries to find the secret key used in encryption and decryption process. However, KPA is not feasible in this encryption scheme since different plain images are encrypted using a different key stream. Hence, it is not possible to obtain useful information by encrypting any special image because the resultant cipher depends upon a random number of operations on the basis of the key stream.

The ciphertext only attack (COA) is an attack model used in cryptanalysis when the attacker has access only to a set of ciphertext. For a given set of ciphertext, if the attacker can determine corresponding plaintext then COA is successful. Suppose an adversary performs exhaustive search on the first 1024 bits of a cipher image to retrieve one-sixteenth segment of the plain image. The possible combinations will then be a number of $2^{1024} \approx 1.797 \times 10^{308}$ which indicates that the COA attack on this proposed encryption scheme is infeasible.

VI. PERFORMANCE COMPARISON

We implemented our proposed encryption scheme in MICA2 sensor mote, consists of a microprocessor (ATmega128L) operating at 7.3728 MHz, 128 KB program memory and 4 KB data memory [29]. The mote supports an event driven operating system known as TinyOS [30] and a high level programming language based on components called nesC. Moreover, we have evaluated our crypto-system in ATEMU emulator to perform high fidelity large scale sensor network emulation studies in a controlled environment. Here, we present the results of our experiments performed using both simulator TOSSIM and emulator ATEMU [31]. NIST recommended 128-bit elliptic curve domain parameters over prime field were used in our experiments to generate the key pool in the key establishment phase. However, the computational cost of key establishment phase is not considered in our experiments since this process is done only once during the setup phase. AES, non-optimized SkipJack, LED, TWINE and BCC protocols are also implemented in TinyOS environment and the results are compared with our proposed cryptographic scheme as shown in Table IV.

Operation speed indicates time complexity and is an important factor for performance evaluation. We have used ATEMU

TABLE IV
COMPARING CPU AND MEMORY USAGE

Algorithm	CPU Cycles	Time (ms)	RAM (bytes)	ROM (bytes)
SkipJack	91224	12.353	292	7218
AES	68512	9.287	324	6994
LED	589652	78.972	378	5970
TWINE	128896	17.477	384	5280
BCC	91286	12.547	976	6240
Proposed	62396	8.547	542	5326

to get the total CPU cycles required to encrypt 32 bytes data for MICA2 sensor mote. On the other hand, using TOSSIM, we have calculated the memory and total encryption time in milliseconds for SkipJack, AES, LED, TWINE, BCC and our proposed cipher. The results in the table indicate that our proposed algorithm performs better in terms of CPU elapsed time (8.547 ms) using only 62396 CPU cycles. For AES, SkipJack and BCC, the number of CPU cycles and encryption time is higher compared to our scheme, while the elapsed time and required CPU cycles are almost double for TWINE and nine times higher for LED protocol. In case of memory consumption, it can be seen that TWINE is more efficient than the other protocols. Although our algorithm uses marginally more memory compared to TWINE, it is less than that of SkipJack, AES, LED and BCC. Overall the proposed algorithm performed significantly better than other algorithms.

VII. CONCLUSION

This paper presents a fast, provably secure and robust block cipher for WSN applications. The cryptographic scheme incorporates the benefits of elliptic curve operations, chaotic map and genetic cryptography to provide data confidentiality. The proposed encryption scheme randomly selects different secret keys $(x_i,\ y_i)$ rather than fixed parameters for every session. This mechanism makes the crypto-system harder to break for adversaries. Another advantage of the proposed cryptographic scheme is the ability to encrypt both text and image data. The scheme is thus more suitable for use in multi-mode sensors. Theoretical analyses and experimental results show that the proposed block cipher is provably secure and is more resource efficient in terms of resource consumption. However, the encryption scheme has a few limitations: i) since the proposed algorithm uses blocks of plaintext (i.e., binary codes), it requires padding when the size of plaintext is smaller than the pre-defined block size; ii) the initial parameters must be pre-distributed using a secure channel or a key exchange mechanism. In our future work, we will implement the protocol for audio and video encryption. Moreover, we plan to implement it in large scale sensor networks to evaluate overall message throughput 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. Knežević, "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. Boztaş, "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.

[26] J. Kumar and S. Nirmala, "Encryption of images based on genetic algorithm—A new approach," in *Advances in Computer Science, Engineering & Applications* (Advances in Intelligent Systems and Computing), vol. 167. Berlin, Germany: Springer-Verlag, 2012, pp. 783–791.
[27] J. Black, P. Rogaway, and T. Shrimpton, "Encryption-scheme security in the presence of key-dependent messages," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), vol. 2595. Berlin, Germany: Springer-Verlag, 2003, pp. 62–75.
[28] M. Bellare, J. Kilian, and P. Rogaway, "The security of the cipher block chaining message authentication code," *J. Comput. Syst. Sci.*, vol. 61, no. 3, pp. 363–399, 2000.
[29] Crossbow Technology. *MICA2, Wireless Measurement System*. [Online]. Available: http://www.eol.ucar.edu/isf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf, accessed Nov. 20, 2014.
[30] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," *ACM SIGPLAN Notices*, vol. 35, no. 11, pp. 93–104, 2000.
[31] J. Polley, D. Blazakis, J. McGee, D. Rusk, and J. S. Baras, "ATEMU: A fine-grained sensor network simulator," in *Proc. 1st Annu. IEEE Commun. Soc. Conf. Sensor Ad Hoc Commun. Netw.*, Oct. 2004, pp. 145–152.

Kamanashis Biswas received the master's degree in security engineering from the Blekinge Institue of Technology, Karlskrona, Sweden, in 2007. He is currently pursuing the Ph.D. degree at the School of Information and Communications Technologies, Griffith University, Gold Coast, QLD, Australia. His research interests include cryptography, intrusion detection system, energy efficient and secure routing, and clustering in wireless sensor networks.

Vallipuram Muthukkumarasamy received the B.Sc.Eng. (Hons.) degree from the University of Peradeniya, Peradeniya, Sri Lanka, and the Ph.D. degree from Cambridge University, Cambridge, U.K. He is currently with the School of Information and Communications Technology, Griffith University, Gold Coast, QLD, Australia, as an Associate Professor. His current research areas include in the investigation of security issues in wireless networks, sensor networks, trust management in MANETs, key establishment protocols, and medical sensor networks. He is leading the Network Security Research Group with the Institute for Integrated and Intelligent Systems, Griffith University. He is the recipient of a number of Best Teacher Awards.

Kalvinder Singh received the Ph.D. degree from Griffith University, Gold Coast, QLD, Australia. He is currently a Researcher and Developer with the Security Division, Australia Development Laboratory, IBM. His research interests include authentication protocols, cryptography, network security, intrusion detection, sensors, and body sensors.