International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

DNA-Chaos S-Box Generation for Modified Lightweight AES Algorithm for Data Packet Protection in MANET

Muntaha A. Hatem[1], Haider K. Hoomod[2]

[1, 2]Al-Mustansiriya University, Department of Computer Science, College of Education, Baghdad, Iraq

Abstract: ***Cryptography is an effective mechanism to protect data packet confidential from passive attack in mobile wireless AdHoc network. Especially in sensitive applications like secrecy conference meetings, military applications, etc. Advance encryption standard (AES) algorithm is one of the most secure algorithms used by many protocols and encryption systems. In this paper proposed modified AES algorithm to make lightweight and more suitable to implement on MANET and AdHoc networks. One the improving AES is generating new dynamic S-Box based hybrid chaotic system and DNA for SubByte transformation. The randomness test was performed on the output of proposed algorithm. The result of the tests shows that the proposed algorithm has good randomness and reduction in encryption and decryption time of AES algorithm.***

Keywords: AdHoc network, MANET, AES, DNA, 2D-modified logistic chaotic

1. Introduction

Wireless AdHoc Networks are a new wireless networking model to mobile hosts that it inviting the attention of several researchers unlike conventional wireless networks (e.g. WLANs, cellular networks or satellite) due its provides everywhere connectivity without help any centralized infrastructure and other its features [1]. Mobile Ad-hoc Network (MANET) is a type of AdHoc networks [2] with mobile wireless nodes have great strength to be applied in critical situations like battlefields and commercial applications [3]. Communication in MANET comprises two stages, the path-discovery and the forward data packet, and both stages are porn to different of attacks [4]. These attacks classified in passive and active attacks [5]. Passive attack intercept information exchanging in order get confidentiality of data without disrupt the normal function of the network. This attack is hard to detection in network because the function of network not affected [6].

Confidentiality data packet content can be achieving by used cryptographic techniques [7]. Cryptography is play a major role in communication systems for protect digital data exchanging. Especially when exchange sensitive data over any insecure channel. Cryptography can be classed as symmetric and asymmetric cipher [8]. Symmetric key in which same key is used for encryption and decryption and asymmetric key in which different keys are used for encryption and decryptions. Symmetric key algorithms are much faster and easier to implement and generally requires less processing power when compared with asymmetric key algorithms[9]. AES algorithm is symmetric cipher and it chosen as one of the most secure techniques by the National Institute of Standards and Technology (NIST) after passing many cryptanalysis challenges, proving that it provides the required security for the foreseeable future [10].

DNA cryptography is a new promising field which has attracted researchers in recent years. Each DNA molecule has two long strands of nucleotides and each nucleotide is made of deoxyribose sugar, phosphate group and a nitrogenous base. Nitrogenous bases are A (Adenine), G (guanine), C (Cytosine) and T (Thymine). These nucleotides appear in random order in each DNA molecule [11]. DNA strands can be used to store information in terms of nucleotide bases. Thus DNA Cryptography gives the high strength of security for storing sensitive information due to the usage of nucleotides which are unique for an organism [12].

Ghada Zaibi et al. [13] proposed efficient chaotic S-Box suitable for implementation on wireless sensor nodes that we classify into two categories: S-Box based on real output of chaotic map (1D-piecewise linear chaotic map and 3D-map) and S-box based on integer outputs of chaotic maps (using discretized Lorenz map and logistic–tent map). Anchal Jain et al.[14], are proposed Symmetric image encryption algorithm based on DNA S-Box and two dimensional logistic map. The unique DNA based s-box to be used in the SubByte transformation on the DNA encoded image and then confusion is achieved by shuffling rows and columns of cipher based chaotic. Nur Hafiza Zakaria et al. [15] proposed to improvep proposed to improvement AES S-Box generation by adding one new function which are inspired from crossover and mutation process. Felicisimo V. and, Wenceslao, Jr.[16] were proposed modified AES algorithm by using multiple substitution boxes to enhance speed performance of the cipher. The first Sbox is the Rijndael S-Box that is in the original cipher structure. However, the second S-Box construct by using XOR operation and affine transformation. This S-box, which we call AES-2SBoxXOR, replaced the MixColumns step in the AES cipher rounds. K.Kalaiselvi and Anand Kumar [17] were proposed modified AES cryptosystem by using Genetic algorithm (GA) in SP-boxes and modified of AES by executing nonlinear neural network in SP network to increase the security against timing attack and minimize the computational time. Julia Juremi et al [18], proposed a new technique Determinant Rotation to modify AES S-box by implementing determinant matrix calculation in rotating the position of AES S-box to be used in the SubByte transformation.

The rest of this paper is arranged as following. Section II preliminaries are brief information of substitution box generation and some chaotic map. Section III explains the proposed modified lightweight AES, Section IV discussions the experimental results, and finally Section VI summarizes the conclusions.

2. Preliminaries

Chaotic System

Chaotic system is nonlinear system that is highly sensitive to initial value. Chaotic behavior is noting in several branches of sciences and engineering. It was used in cryptography due their properties such as sensitive to initialvalue and similarity of random behavior [19]. In the subsections below, a concise description of some chaotic systems is given.

• Logistic Map: In 1976, Robert May first offered Logistic map [20]. Logistic map is a popular and simple of one-dimension chaotic system with (initial value x_0, control parameter **r** and output x_n), as shown in the following equation (1):

$$x_{n+1} = r\ x_n \times (1 - x_n) \quad (1)$$

Where $x_0 \in (0, 1)$ denotes the initial condition and r is a constant parameter between $\in [0, 4]$.

• Two-Dimensional Logistic-Adjusted-Sine Map (2D-LSM): 2D-LASM is a nonlinear discrete-time proposed by Hua and Zhou [21] that derives from Logistic map and Sine map as given equation*:*

$$X_{n+1} = \text{Sin}\,(\pi * r\ (y_n + 3)\ (x_n - x_n^2)) \quad (2)$$
$$Y_{n+1} = \text{Sin}\,(\pi * r\ (X_{n+1} + 3)\ (y_n - x_n^2))$$

where the control parameter r ∈ [0,1].

2.2 Substitution Box generation

Substitution is a nonlinear transformation which performs confusion of bits. In the AES, nonlinear transformations are implemented S-box as matrix of (16 x 16 = 256) elements in which rows and columns are having values ranging from 0 to 15 (0 to f in hexadecimal). S-box is generating by two transformations in the Galois fields GF (2) and GF (2^8) as shown in the equation (4). The first transformation: S-box finds the multiplication inverse of the byte in the field GF(2^8) and then followed affine transformation (over GF(2)) is computed.

$$Y = Zx \oplus c \bmod M \quad \ldots\ldots\ldots (4)$$

where Z is affine matrix, x is a vector that is multiplicative inverse of element of state matrix, c is affine constant i.e. $63_{16} = 01100011_2$ is given in hexadecimaland M is irreducible polynomial x 8 + x 4 + x 3 + x + 1. The affine matrix used is shown as under

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

where *s*, *b* and *c* are 8 bit arrays. The inverse S-box is simply the S-box run in reverse. It is calculated by first calculating the inverse affine transformation of the input value, followed by the multiplicative inverse [22]3.

3. Proposed Lightweight Modified AES

In this section is proposed modified AES algorithm to reduce execution time and make faster and more lightweight for limited resource than original AES . This proposed system consist of three stage which are:proposed generation chaos keys, proposed new S-box stage and modified AES operations stage.

3.1 Generation Chaos Keys

In this stage we proposed generation chaos keys consist of two proposed (**A**) and (**B**) and named **Hybrid Chaotic System** (**HCS**). Both (**A)** and (**B)** also, consists of two stage for generate three random chaos keys by apply chaotic system. The first stage applies **2D-Logistic-Sine Chaotic Map (2D-LASM)** for take the output it as initial value for second stage to make it complex and hard to predictable. Whereas, the second stage proposed modified 1D-logistic map and convert to 2-dimensions chaotic system and named **2D-modified logistic map (2D-ML)** based on two equations with two control parameters and initial values are fed from first stage for generate three chaos keys as shown in figure (1).

$$x_{n+1} = b * x_n\ (1 - x_n)\ (1 - x_n^2)$$
$$y_{n+1} = a * y_n\ (1 - y_n)\ (1 - y_n^2) \quad (3)$$

Where the **a** and **b**∈[3.9, 6.27] are represent control parameter.

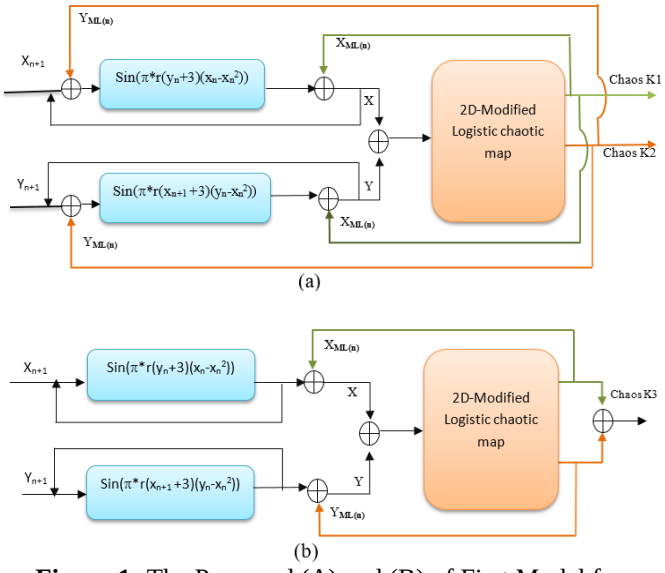

Figure 1: The Proposed (A) and (B) of First Model for Generate Chaos Keys.

The following algorithms (1) and (2) shows the method of using the 2D-Logistic-Sine (2D-LASM) and 2D-modified logistic (2D-ML) chaotic system in proposed (**A)** and **(B)** respectively of **Hybrid Chaotic System**.

Algorithm (1): Generate Chaos Keys of Proposed (A)

Input: Initial conditions X_0, Y_0.
Output: Chaos keys.
Step1: Read two initial values X_0, Y_0;
Step2: Read positive constant **r**, **a, b** as control parameters;
Step3: Read initial values for X_{ML} =0, chaos Y_{ML} =0;
Step4: Apply equations (2) of **2D-LASM** to generate two random values X,Y;
Step5: Apply XORED between X and Y and save the result z_n;
Step6: Read$X_0, Y_0$for 2D-ML ;
Step7: Truncate the last three significant digits of value $z_n$and thenconcatenating it with X_0, Y_0 and save result in t_n, v_n, $t_n = z_n||X_0$, $v_n = z_n||Y_0$;
Step8: Read t_n, v_n as initial values within range (0,1) for 2D-ML;
Step9: Apply equation (3) of 2D-ML for generate two random value $X_{ML,}$ Y_{ML};
Step10: Apply XORED between $X_{ML(n)}$ and $X_{n+1}$for feed the equation (2) of 2D-LASM and then the result XORED with $Y_{ML(n)}$ and then save result in **X**;
Step11: Apply XORED between $X_{ML(n)\ and}$ $Y_{n+1}$for feed the equation (2) of 2D-LASM and then the result XORED with $Y_{ML(n)}$ and then save result in **Y**;
Step12: Repeat steps 5-10;
Step13: Save X_{ML} and Y_{ML}, as chaosK1 and chaosK2;
Step14: End.

Algorithm (2): Generate Chaos Key of Proposed (B)

Input: Initial conditions X_0, Y_0.
Output: Chaos keys.
Step1: Read two initial values X_0, Y_0;
Step2: Read positive constant **r, a, b** as control parameters;
Step3: Read initial values for X_{ML} =0, chaos Y_{ML} =0;
Step4: Apply equations (2) of **2D-LASM** to generate two random array X,Y;
Step5: Apply XORED between X and Y and save the result z_n;
Step6: Read$X_0, Y_0$for 2D-ML ;
Step7: Truncate the last three significant digits of value $z_n$and thenconcatenating it with X_0, Y_0 and save result in t_n, $t_n = z_n||X_0$, $v_n = z_n||Y_0$;
Step8: Read t_n, v_n as initial values within range (0,1) for 2D-ML;
Step9: Apply equation (3) of 2D-ML for generate two random value $X_{ML,}$ Y_{ML};
Step10: Apply XORED between $X_{ML(n)}$ and the result X value of equation (2) of 2D-LASM and then save result in array X_{ML}
Step11: Apply XORED between $Y_{ML(n)}$ and the result Y value of equation (2) of 2D-LASM and then save result in array Y_{ML};
Step12: Repeat steps 5-11;
Step13: Apply XORED between $X_{ML\ and}$ $Y_{ML\ and}$ save the result in one matric, represent chaos k3;
Step14: End.

In this proposed to generating three chaos keys (K1, K2, and K3) only. These chaos keys it used as a secret keys to modified AES and generate new S-box.

3.2 Proposed New S-box

In this section, is proposed New S-box based rule DNA and chaotic system in order provied highly security to algorithm and ensure the randomness and complexity of S-box. The New S-box is derived from original S-box of AES as illustrate in following (3) algorithm steps:

Algorithm (3): Generate New S-Box

Input:original S-box.
Output:generate new S-box.
Step1: for each byte in original S-box;
Step2:convert hexadecimal number to binary number;
Step3:perform permutation on binary sequence by shift cycle to left based on (**chaos k3)**;
Step4: encoded every pairs of binary sequence by the rule DNA (nucleotides), A = 00, T = 01, G = 10 and C =11;
Step5: generate square DNA table by XOR operation of DNA nucleotides;
Step6: for every nucleotide in DNA sequence it is substituted with corresponding nucleotide resulting from intersection it with next nucleotide in square DNA table;
Step7: convert the resulting DNA sequence to binary number;
Step8: convert the binary number to hexadecimal number;
Step9: save the result in corresponding byte of original S-box;
Step10: end.

In step3 of algorithm (3) is implement shift cycle to right by dynamic number of shifiting depending on last significant digit of chaos K3 of proposed (b) of Hybrid chaotic keys to determine the number of shift cycle.

3.3 Proposed Modified AES

In this stage is proposed modified AES operation algorithm to reduce execution time and make faster than original AES . This proposed modified AES comprise basic opration except Mix-Column process due its consumes very long time in comparison with other operations and we compensate it with proposed Add-Shift-Cycle, proposed Add-XOR operations, and proposed hybrid chaos keys. In this proposed The **chaos K1** and **chaose K2**keys it used as secret keys to modified AES operations. Whereas, the **chaos K3**its used as a secret key for determine the number of rounds and changes its random values after each encryption or decryption process to overcome the limitation of the initial key in original AESis without change in the whole encryption operation. The following steps describe operations of state encryption in proposed algorithm.

- **Proposed New SubByte Operation:**

This operation provides substiution process by Replace every byte of state with byte of proposed New S-box.

- **Proposed New Shift-Rows Operation:**

In this operation after complet shifiting to left on last three rows of state the result is a 4 * 4 matrix XOR with **chaos K1** (128-bit) as it show in fig (2).

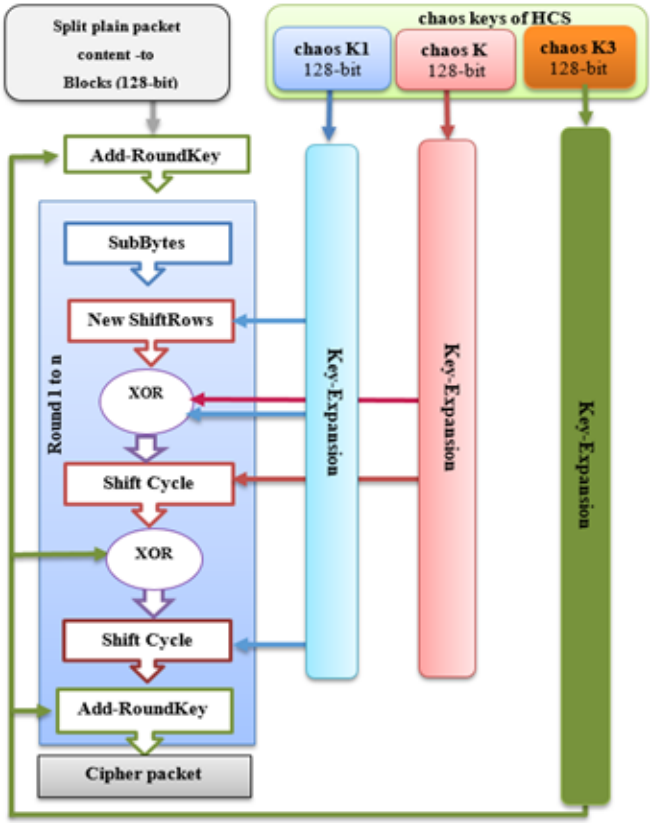

Figure 2: Flowchart Proposed Modified AES

- **Add-Round-Key Operation:**

In this process, The resulting state of roundXOR with random**chaos K3** (128 bit).

- **The Proposed Add-Two-XOR Operation:**

In this proposed operation is added two XOR operation to each round, the first XOR operation apply to the resulting state from previous process (New ShiftRow) will dual bitwise XORED with chaos keys: **chaos K1** (128-bit) and **chaos K2** respectively as shown in figure (1). The seconde XOR operation is applied on output data block from the second shift cycle with **chaos K3**. The two XOR process are done by take each column of the state will be XOR with corresponding column in the chaos keys block. The purpose of this process is to increase randomization and try to make more secure and difficult to detect by attacker.

- **The Proposed Add-Shift-Cycle Operation:**

This operation is added to each round of AES for provide permutation by shifting rows to left by dynamic number of shifiting depending on chaos keys. In this proposed of modified AES two shift cycle operation were proposed in different location in AES round. The first shift cylcle operation depend on the last signifcant digit of **chaosK2** to determine the number of shift cycle need during this round. While, the second shift cycle based on the last signifcant digit of **chaosK1**. Each **chaosK2** and **chaosK1** changing every round make th number of shift differ

3.4 Encryption/ Decryption Process Using the MAES

The algorithm (4) shows the encryption process, after source node S_n capture plain-message contents and its divided into blocks size 4*4 byte, then pass each block (state) with six chaos key have length 4*4 to lightweight modified AES.

Algorithm (4): Encryption packet data
Input: packet data.
Output: cipher packet data.
Step1: S_n capture packet data;
Step3: $S_n$split Plain-packet contents into blocks each has a size of 4 * 4 byte;
Step5: S_n Generate chaos keys by apply algorithms (1) and (2) for second mode e of modified AES algorithm;
Step6: implemented LMAES algorithm on Plain-packet contents with chaos keys to produce cipher-packet;
Step8: sent cipher-packet contents based AODV;
Step 9: end.

While, the decryption processes it done in node destination by apply the modified AES as shown in algorithm (5), but some of lightweight modified AES operations in the encryption process will remain it same such as generate six chaos keys, Add-Two-XOR and Addroundkey, whereas, many of its operations reversed for decryption process as description in following steps:

- Inverse New Sub-Bytes Operation.
- Inverse New ShiftRows process.
- The Proposed Inverse-Shift-Cycle Operation.

Algorithm (5): Decryption process
Input: Cipher-Packet contents and chaos keys.
Output: plain Packet contents.
Step1: Receive cipher Packet contents based on AODV;
Step4: Split the cipher packet conentsinto blocks every block has size (4*4) byte;
Step5: implemented LMAES algorithm)with chaos keys;
Step6: Decrypt Packet contents;
Step7: end

4. Experiment and Discussion Results

In order to test the proposed lightweight Modified AES algorithm (LMAES) in wireless enviorment, we implementation of Modified Lightweight AES algorithm to tested encryption the packets transferred in the Ad hoc and MNAET.by using different parameters of the wireless network for performance validation of the proposed system. The proposed Modified Lightweight AES algorithm that used hybrid chaotic system (2D-modified logistic chaotic system and logistic-sin map) with modified AES.

Table (1) and figur (3) show the average encryption time for original and modified AES with different iteration rounds (12, 10 ,8, and 6) for the MLAES when applied on different data size (10KB to 1000KB). the. Figure(3) shows the encryption time of the MLAES algorithm in the different rounds (8, 10, and 12), MLAES is still less than encryption time of original AES due to the reduction in AES operations. Also, we can point that the gap in encryption time increase when data increase.

Table 1: The encryption time comparison with MAES-DNA with different iteration rounds (12, 10 , 8, and 6)

Text size (KB)	Original AES (msec)	Modified AES (msec)	MLAES (msec)			
			6 rounds	8 rounds	10 rounds	12 rounds
10	5.183	4.785	1.669	2.298	3.455	4.213
25	12.057	11.234	6.554	8.563	10.132	11.765
70	28.957	21.098	11.088	13.561	16.678	19.341
100	69.309	45.781	27.509	31.908	38.775	43.086
1000	105.879	67.908	41.112	45.991	50.683	56.897

We measured the time for the proposed MLAES operations. Table (I) shows the average encryption time for the original and modified AES algorithm with different numbers of iteration rounds (6, 8,10, and 12) of LMAES with DNA. For 6 rounds of iteration, the proposed MAES algorithm is faster (140.1 msec to encrypt 10 kB), while the original AES algorithm takes 161.2 msec to encrypt the same file size. This difference was shown in all results (as shown in Figure (3)). It indicates that the proposed lightweight MAES-DNA is consistently faster than the traditional AES.

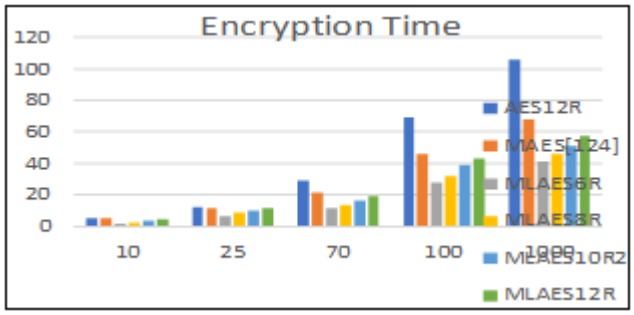

Figure 3: Encryption Time Comparison for MLAES with different Rounds

The proposed MLAES is designed with less complex functions and was tested to calculate the CPU cycles during different rounds. Figure (4) shows an example for generated s-boxes using DNA. Table (2) shows that the proposed MLAES passes all of the NIST statistical test results for the different numbers of rounds of iteration comparing with the original AES.

Table 2: The NIST statistical test results for proposed MLAES

NIST statistical tests Results Name	Original AES 10 rounds	**MLAES**		
		10 rounds	8 rounds	6 rounds
Frequency (Monobit) test	2.786	1.310	0.776	0.748
Runs test	7.677	4.456	3.789	2.987
Discrete Fourier transform	0.564	0.355	0.310	0.276
Block frequency	0.883	0.754	0.678	0.632
Longest runs test	0.567	0.314	0.298	0.256
Cumulative sums test	1.876	0.811	0.755	0.721
Serial test	6.096	1.670	1.421	0.980
Matrix rank test	1.765	0.998	0.890	0.810
Overlapping template test	0.981	0.674	0.545	0.359
Linear complexity test	1.530	1.435	1.099	0.900
Non overlapping template test	0.934	0.897	0.801	0.645
Random excursions variant test	1.065	0.603	0.589	0.511
Random excursions test	0.976	0.977	0.876	0.768

5. Conclusion

The results of MLAES show these modifications to the original AES algorithm, has increase the speed encryption process and make it more lightweight and efficient for encryption in limited resource. The removing Mix-column operation effect in randomness of AES results, but chaos keys and proposed nonlinear operation raised the randomness degree of MLAES outputs and security remains robust. The proposed modified AES algorithm is, making it more desirable for embedding in IoT devices and sensors because of its reduced power consumption. Also, the results in table (I) show that the proposed modified AES faster than the algorithm in [19].

The proposed MLAES is designed with less complex functions and was tested to calculate the CPU cycles during different rounds.

References

[1] N. Patel. "A Survey: Security Technique for On Demand Multicast Routing (SAODV)." IJIRST, National Conference on Latest Trends in Networking and Cyber Security, 2017.
[2] A. Dorri, "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET." Wireless Networks 23, no. 6 (2017): 1767-1778..
[3] P. Sharma, N. Sharma, and R Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network." International Journal of Computer Applications 41, no. 21 (2012).
[4] E. Elmahdi, S.Yoo, and K. Sharshembiev. "Securing data forwarding against blackhole attacks in mobile ad hoc networks." In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 463-467. IEEE, 2018..
[5] A. Sharma, D. Bhuriya, U. Singh, and S. Singh. "Prevention of black hole attack in AODV routing algorithm of MANET using trust based computing." (IJCSIT) International Journal of Computer Science and Information Technologies 5, no. 4 (2014): 5201-5205.
[6] N. Gupta, and S. Narayan Singh. "Wormhole Attacks In MANET." In Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference, pp. 236-239. IEEE, 2016.
[7] R. Kapur, and S. K. Khatri. "Secure data transfer in MANET using symmetric and asymmetric cryptography." In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), pp. 1-5. IEEE, 2015.
[8] K. binti Mohamed, F. H. Ali, Suriyani Ariffin, and Mohd Nazran Mohammed Pauzi. "A Review of Cryptography Based on Key Dependent S-Box in Block Cipher." Selangor Science & Technology Review (SeSTeR) 2, no. 2 (2018): 1-8.)
[9] G. Venkatesha, S. Dinesh, and M. Manjunath. "AES Based Algorithm for Image Encryption and Decryption." Perspectives in Communication,

Embedded-systems and Signal-processing-PiCES 2, no. 11 (2019): 342-345.
[10] A. Atteya, and A.H. Madian. "A hybrid Chaos-AES encryption algorithm and its impelmention based on FPGA." In 2014 IEEE 12th International New Circuits and Systems Conference (NEWCAS), pp. 217-220. IEEE, 2014.
[11] C. Thomas "Secure Symmetric Encryption Scheme Using Genetic Algorithm." International Journal of Applied Engineering Research 12, no. 21 (2017): 10828-10833.
[12] M. Poriye, and S. Upadhyaya. "Improved Security using DNA Cryptography in Wireless Sensor Networks." International Journal of Computer Applications 155, no. 13 (2016).
[13] G.Zaibi, F. Peyrard, A. Kachouri, D. Fournier-Prunaret, and M. Samet. "Efficient and secure chaotic S-Box for wireless sensor network." Security and Communication Networks 7, no. 2 (2014): 279-292.
[14] A. Jain, P. Agarwal, R. Jain, and V. Singh. "Chaotic Image Encryption Technique using S-box based on DNA Approach." International Journal of Computer Applications 92, no. 13 (2014).
[15] N.H. Zakaria, R Mahmod, N. I. Udzir, and Z. A. Zukarnain. "Ehanceing Advanced Encryption Standard (AES) S-Box Generation Using Affin Transformations." Journal of Theoretical & Applied Information Technology 72, no. 1 (2015).
[16] J. Wenceslao, V. Felicisimo "Performance efficiency of modified AES algorithm using multiple S-boxes." International Journal of New Computer Architectures and their Applications (IJNCAA) 5, no. 1 (2015): 1-9.
[17] K.Kalaiselvi, , and A. Kumar. "Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box." In 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), pp. 1-6. IEEE, 2016.
[18] J. Juremi, R Mahmod, Z. A. Zukarnain, and S. M. Yasin. "Modified AES S-Box Based on Determinant Matrix Algorithm." International Journal 7, no. 1 (2017).
[19] Z. Hua, and Y. Zhou. "One-Dimensional Nonlinear Model for Producing Chaos." IEEE Transactions on Circuits and Systems I: Regular Papers 65, no. 1 (2018): 235-246.
[20] J. Feng, J. Zhang, X. Zhu, and W. Lian. "A Novel Chaos Optimization Algorithm." Multimedia Tools and Applications, Springer, vol: 76, no:16, 2017.
[21] P. Ping, , J. Fan, , Y. Mao, and J. Gao, , "A Chaos Based Image Encryption Scheme Using Digit-Level Permutation And Block Diffusion." IEEE Access 6 (2018): 67581-67593.2018.
[22] A. Singh, P. Agarwal, and M. Chand. "Analysis of Development of Dynamic S-Box Generation." (2017).
[23] H.K. Hoomod, and A. M. Radi. "New Secure E-Mail System Based On Bio-Chaos Key Generation And Modified AES Algorithm." In Journal of Physics: Conference Series, vol. 1003, no. 1, p. 012025. IOP Publishing, 2018.

.