Low Complexity Security Algorithm for CPS / IoT Networks

R. Upadhyay, S. S. Baghel, S. Singh, A. Soni and U. R. Bhatt
Department of Electronics & Telecommunication. Institute of Engineering & Technology, Devi Ahilya University, Khandwa Road, Indore 452001, India
rupadhyay@ietdavv.edu.in

***Abstract*— Due to its noisy nature, wireless channel plays a dominant role in deciding the performance of data communication between the smart objects in the cyber-physical systems (CPS) or the internet of things (IoT). Open and heterogeneous nature of these networks makes them susceptible to vulnerable attacks. So, to keep up the confidentiality and integrity of the transmitted data against the adversaries, it should be secured before transmission. However, issues such as power efficiency, low computational complexity need to be considered when designing security algorithms for CPS/IoT networks. Traditional encryption algorithms, such as Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA) can be used for security purpose, but they do not satisfy power and complexity criteria as per CPS/IOT networks requirements. Moreover, they exhibit poor bit error ratio (BER) performance in a noisy wireless channel. This paper presents a modified security algorithm, AES-P, with X-OR mapping on AES to make them suitable for CPS/IoT applications. Simulation and analysis of the proposed algorithm showed that its power consumption and complexity are reduced as compared to traditional AES. It also performed better in the wireless channel, while maintaining the required security level satisfied by Avalanche effect.**

***Index Terms*— Advanced Encryption System; Bit Error Rate; Internet of Things Security; Physical Layer security**

I. INTRODUCTION

Cyber-physical systems or the internet of things enables the connectivity and information exchange among different smart objects & networks, such as sensors, ZigBee, and Bluetooth. It provides the sensorial and computational capability to the objects, by which they can interact or communicate with each other through the internet. In short, CPS/IoT is a network of different physical or smart objects, in which they can collect or exchange data. CPS/IoT has many advantages, such as control & automation, monitoring, and communication, but there are some resource constraints of CPS/IoT networks, such as complexity, security, processing time, power requirement [1].

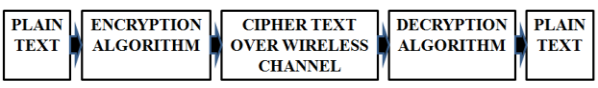

Figure 1: Model to achieve security in the wireless network.

Network Security is an essential concern in CPS/IoT networks to maintain the confidentiality and integrity of the data between the objects. Data transmission between objects in CPS/IoT communication takes place through a wireless channel, which affects the performance of the system like bit error, throughput [2][3]. Due to the open and diverse nature of CPS/IoT networks over the wireless channel, there is a possibility that the intruders present in the cloud or channel may intercept and manipulate the information. Therefore, before sending the data into CPS/IoT cloud or channel, we should secure information with the help of an encryption algorithm to avoid the effect of adversaries in the channel, as shown in Figure 1. However, most of the CPS/IoT objects have several resource constraints like limited power, low complexity, and delay [4]. The traditional security algorithms are more complex and consume more power; hence, an optimized or lightweight security algorithm is required [5] [6].

Table 1
Symmetric Cryptographic Algorithms for IoT Networks

Symmetric Algorithm	Block Size	Key Size	No of Rounds	Possible Attacks
AES [6]	128 bit	128 bit	10	Man-in-middle [9]
IDEA [9]	64 bit	128 bit	8	Key vulnerability[6]
HEIGHT[3]	64 bit	128 bit	32	Saturation attack[3]
RC5 [6]	32 bit	16 bit	20	Differential attack[6]

There are many symmetric and asymmetric cryptographic algorithms present in the literature to provide security in wireless networks, but in the context of CPS/IoT network security, most of the cryptographic algorithms are not reliable due to limited resources of CPS/IoT networks and their avalanche effect is analyzed in [7]. Table 1 and Table 2 give the comparative analysis of different cryptographic algorithms for CPS/IoT networks in terms of key size, the number of rounds, block size, power consumption, possible attacks, and speed. From the above analysis, asymmetric key cryptographic algorithms and some of the symmetric key cryptographic algorithm (HEIGHT, RC5) are not suitable for CPS/IoT security due to their complex nature. Symmetric security algorithm such as AES, IDEA can be used for CPS/IoT security, but these algorithms also consume more power due to their key size and complexity [8][9]; so, they are not suitable for communicating data over a wireless channel.

Moreover, from the literature reviewed so far, it is concluded that power efficiency and security are inversely related to each other and a complex algorithm may cause power inefficiency and delay in CPS/IoT networks; hence, a lightweight security algorithm is required for security of CPS/IoT networks. So, a modified AES algorithm, AES-P

using X-OR mapping is proposed in this paper. Performance of the proposed algorithm is compared based on computational complexity, power requirement, time delay, and randomness, with that of traditional AES approach to check its suitability for the wireless mode of data communication for CPS/IoT networks.

Table 2
Asymmetric Cryptographic Techniques for IoT Networks

Parameter	RSA [6]	Diffie Hellmen (DH) [6]
Key Length	*1024 bit*	*Key exchange*
Speed	*Average*	*Slow*
Power Consumption	*High*	*High*
Complexity	*Complex*	*Complex than RSA*

This paper is arranged as follows: Section II provides the related work about AES in literature followed by Section III, which demonstrated the working of advanced encryption. In Section IV, the proposed algorithm was described. Section V described the performance metrics. Section VI consisted of simulation results and analysis, followed by a conclusion.

II. Related Work

The basic structure of CPS/IoT network security and solutions over various security attacks were discussed in [10][11], in which AES-128 is implemented for CPS/IoT over Intel Galileo board. In [8] [12] [13], three different optimized security algorithms were proposed for IoT networks based on AES-128 encryption. Some optimized cryptographic algorithms based on AES-128 and the security attacks were described in various papers [9] [12-16]. As the main building blocks of AES are S-Box & Mix column operation, which are nonlinear transformations, they consume more power due to their complex operations. Therefore, optimization of these blocks is required to enhance the performance of AES algorithms. P. Rajshekhar [12] et al. discussed an efficient FPGA implementation of AES-128 bit with modified S-Box & Mix Column Transformation to optimize power consumption and processing time. Shilparani [16] et al. proposed hardware implementation of AES128 algorithm using Xilinx-vertex5 FPGA with X-OR based mixed column. Isha Luhach [6] et al. suggested AES 128 for IoT networks due to its less key size and block size as compared to the asymmetric cryptographic algorithm. Aylin Yener [4] discussed the effect of the wireless channel on security. The author in [17] proposed a novel approach for the design of S-Box using second-order reversible one-dimensional cellular automata RCA2 as a replacement to the classical look-up-table LUT based S-Box used in AES algorithm applied to telemedicine applications. A lightweight wave dynamic differential logic based AES was implemented for securing IoT in [18]. A low power encryption scheme was proposed by reducing the encryption cycle of AES along with LoRaWAN [19]. In [20], the author proposes an AES-dependent Hsiao (AD-Hsiao) code to improve the error correction capability followed by AES decryption for syndrome decoding and observed the Avalanche effect in secure wireless Fieldbus system. Some of the latest work on MANET based IoT system security was discussed in [21-25].

Further, the data transmission over a noisy wireless channel is vulnerable to security attacks like eavesdropping and jamming. A working wireless channel also suffers from noise effect, which degrades the performance of bit error ratio (BER) and throughput of the system. From the above study, our research is based on optimized AES 128 algorithm for IoT networks to reduce power and elapsed time and make them suitable for data transmission over a wireless channel as the performance of AES 128 over the wireless channel is poor.

III. Advanced Encryption Standard

Cryptography plays a vital role for secured CPS/IoT communication and maintains confidentiality and integrity of the data against the adversaries present in the channel, which may intercept and modify the data. It leads to data loss, confidentiality, integrity, and authenticity. Ciphers are classified into two types: Block cipher (IDEA and AES) & Bit cipher (stream cipher). AES is symmetric key block cipher cryptographic algorithms, which utilize the same key for encryption as well as for decryption and all operations are carried out by the blocks. AES is known as "Rijndael Encryption", which was developed by United States National Institute of Standard and Technology (NIST) in 2001. AES performs all operations in the form of blocks. The basic unit of operation is a byte (a combination of 8 bit). The upcoming bit sequence is firstly converted into byte sequence after which it forms a 2-dimensional array of bytes, known as State (plain text) of AES or the basic input unit of AES. It uses a fixed block size of 128-bit and three variant of keys, such as 128, 192, 256-bit keys. For 128-bit block size (fixed) and 128-bit, 192-bit and 256-bit key size, AES performs 10, 12 and 14 rounds respectively [26]. Here, AES-128-bit encryption that performs ten rounds is considered. Each round in AES performs four operations, which are as follows:

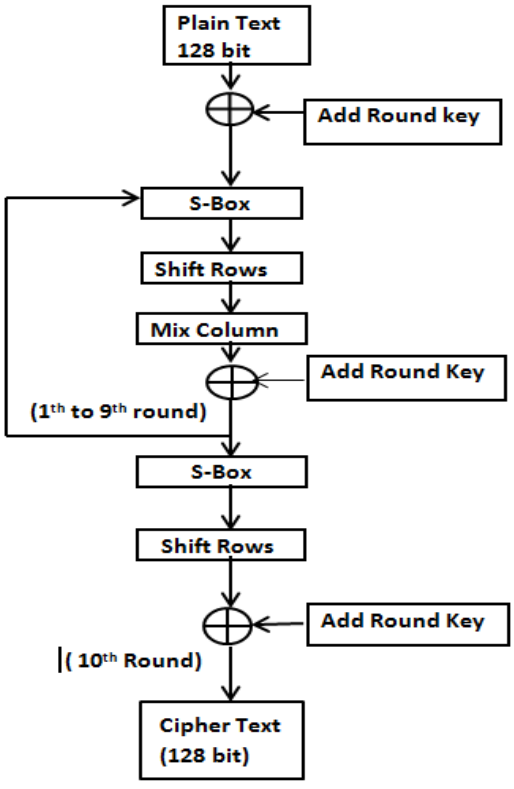

Figure 2: AES Encryption

In the first nine rounds, AES performs the following operations, i.e. four operations in each round.

- S-box substitution
- Shift rows transformation
- Mix column operation
- Addition of round key

In the last round, AES performs the following three operations.

- S-box substitution
- Shift rows transformation
- Addition of round key

After the 10th round, AES generates a ciphertext of the corresponding plain text. Figure 2 and Figure 3 show the block diagram of the encryption & decryption process of AES respectively.

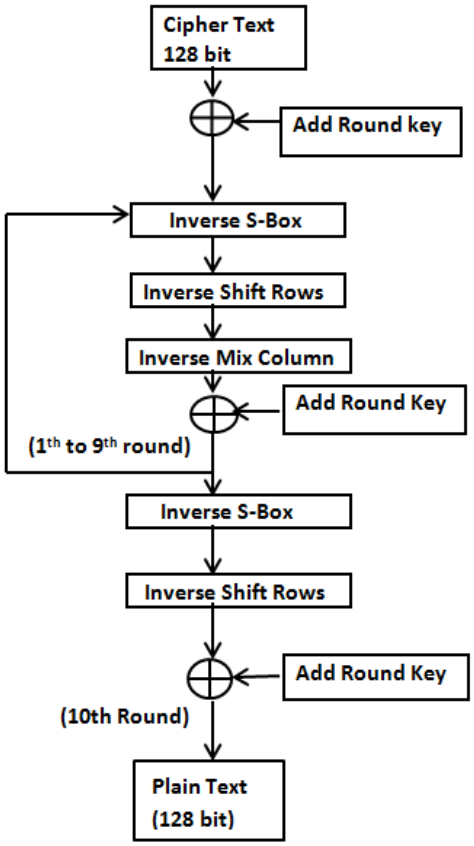

Figure 3: AES Decryption

IV. Proposed Algorithm

It is evident that the traditional AES due to its complex structure and more power consumption proves inefficient in terms of performance parameters like BER, throughput, data loss, for data transmission in CPS/IoT networks over wireless (AWGN) channel. In the proposed algorithm, the main focus is to minimize the drawbacks of traditional AES algorithm concerning data communication over the wireless channel in CPS/IoT networks by applying X-OR mapping in the encryption and decryption algorithms, which leads to improved BER, less elapsed time and reduced number of operations. Here, the aim is to secure the data stream, which is divided into n frames each of 128 bits before sending them over AWGN channel. Encryption and decryption of data using AES-P are discussed as:

A. Encryption

In traditional AES, encryption is performed on each frame but in the proposed algorithm, traditional AES is applied to the first frame only and output of that encrypted data is X-ORed with the rest of the frames to encrypt them as shown in Figure 4. It leads to relaxation in (n-1) computational complexity. If the adversary can decode the first frame, the remaining frames can be decoded. Since the decoding of (n-1) frames depends on the outcome of encrypted data of frame-1, it needs to be more secure. Therefore, one more AES encryption is performed to the first frame. So, encrypted data consists of the first frame of 128 bits encrypted twice with AES, and all remaining frames are XORed with the output of first AES encryption of frames.

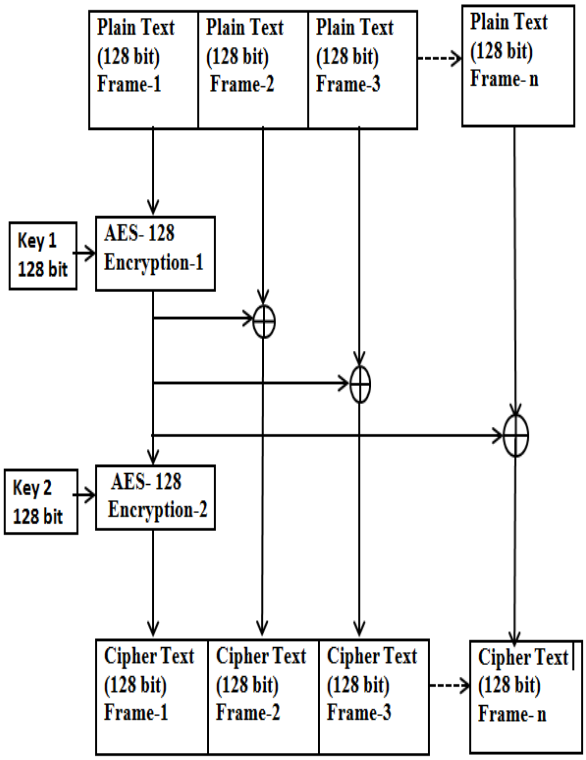

Figure 4: Encryption with X-OR mapping on AES

B. Reduction in Number of Operations

As compared to the traditional AES, the number of operations performed in the proposed approach is reduced substantially. Since, only 39 operations are required for one AES encryption, a message is divided into n number of frames of 128 bits each; hence, the total number of operations required is n*39. When considering both encoding and decoding, the total number of operations required is (n*39*2), while in the proposed approach, AES encryption is performed only twice irrespective of the number of frames and (n-1) number X-ORing of each one of the operation. When considering both for encoding and decoding, the total number of operations required is {(2AES + (n-1)X-OR)*2} i.e. {(2*39 + (n-1)*1)*2}. Hence, as compared to traditional AES, the proposed algorithm requires fewer operations making it suitable for CPS/IoT systems.

C. Decryption

Decryption is the reverse process of encryption, in which ciphertext frame-1 goes for the decryption process with the corresponding key-2, as shown in Figure 5. After decryption-2, decrypted frame-1 is X-ORed with other consecutive frames simultaneously to decrypt other frames to give plain text frame-2 to plain text frame-n. After which decrypted frame-1 again decrypted with the corresponding key-1 and it will give the plain text frame-1.

V. Performance Matrices

A. Bit Error Ratio

Bit error ratio is the percentage in which transmitted and received bits differ and can be considered as an approximate of its probability. It should be low. For the bit streams B^T and B^R of length N at transmitter and receiver respectively, it can be mathematically expressed as:

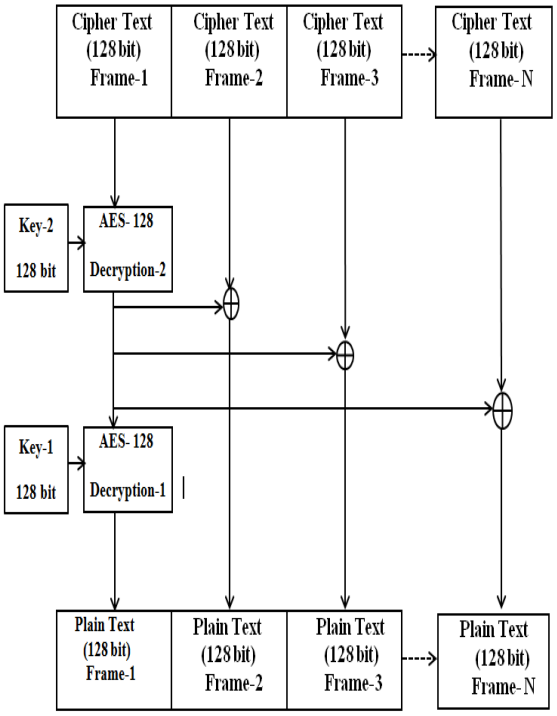

Figure 5: Decryption with X-OR mapping on AES

$$BER(\%) = \frac{\sum_{i=1}^{N} \left| B^T(i) - B^R(i) \right|}{N} * 100 \quad (1)$$

B. Average Throughput

Average throughput is another critical parameter to evaluate the performance of IoT networks. It is the measure of successfully received data bits per unit time and is expressed in bits/sec [27].

C. Complexity and Elapsed Time

The complexity of algorithms is expressed in terms of the number of arithmetic and logical operations performed and should be low for resource constraint networks, such as IoT. Elapsed time represents the time required to process an algorithm. The Elapsed time should be low to avoid delays for real-time systems like IoT.

D. Avalanche Effect

Avalanche Effect is one of the desirable attributes of various cryptographic algorithms, which help to decide their security level. Security level is decided based on the following two conditions, and an algorithm is secured if that algorithm should follow any one of the following two conditions:

1) A small change in plain text (flipping a single bit in plain text) results in a drastic change in the ciphertext (half the ciphertext bit flips) [28].

2) A small change in key results into a large number of bits change in the ciphertext [29].

In the proposed algorithm, the first condition is considered to evaluate the avalanche effects. The percentage avalanche effect can be defined as the ratio of the number of changed bit N_c in ciphertext to the total number of bits in the ciphertext N_t.

$$\%AE = N_c / N_t \quad (2)$$

E. Randomness

Randomness is one of the essential parameters in characterizing the performance of any cryptographic technique. Cipher generated by encryption should possess sufficient randomness to ensure data security from false decoding. The randomness of a bit sequence is analyzed by various statistical tests, such as Linear Span test, DieHard, Collision test, NIST statistical test suit [30] [31]. We employed the NIST randomness test suit for evaluating the randomness of the generated block cipher.

VI. Simulation Results & Analysis

Traditional AES-128 and proposed algorithm are simulated with parameters, as mentioned in Table 3 and they were analyzed using MATLAB 8.3 R2014a.

Table 3
Simulation Parameters

Parameter	Value
Key size	128 Bit
Channel type	AWGN
SNR range	0-10 dB
Modulation type	DPSK
AES mode	CTR
Number of frames processed	10, 20, 30, 50

A. BER & Transmission Power Analysis

The BER performance of proposed X-OR mapping on AES is found more efficient over the traditional AES algorithm, as shown in Figure 6. When 30 frames were considered for transmission after encryption as well as decryption by AES over a noisy channel (AWGN), most of the data bits were corrupted, and bit error ratio was found around 60%. Based on this analysis, the traditional AES algorithm is not suitable for CPS/IoT data transmission over a noisy channel. On the other hand, if the proposed algorithm was analyzed, the BER performance was significantly efficient over noisy medium for CPS/IoT networks as the lower values of BER were achieved for lower SNR environment. From the above analysis, it can be said that proposed X-OR mapping on the AES algorithm is

suitable for data transmission in networks even with the worst condition of the channel (i.e., lower SNR).

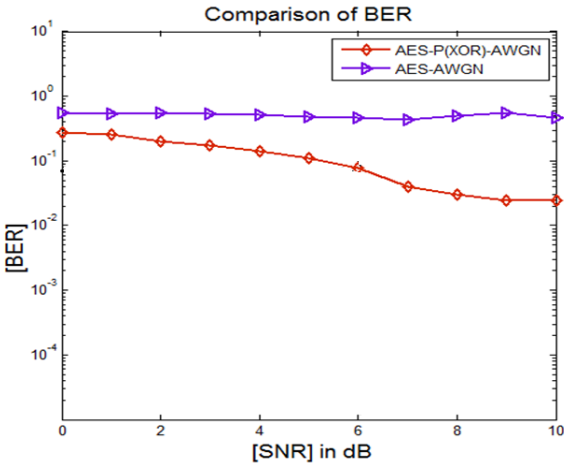

Figure 6: Reduction in Power

From the simulation results, it was clear that the power requirement in the proposed scheme is reduced significantly as compared to the traditional AES algorithm**.** At SNR of 6 dB bit error ratio achieved by AES-P algorithm was nearly 0.07 and that of traditional AES was 0.60 approximately. It

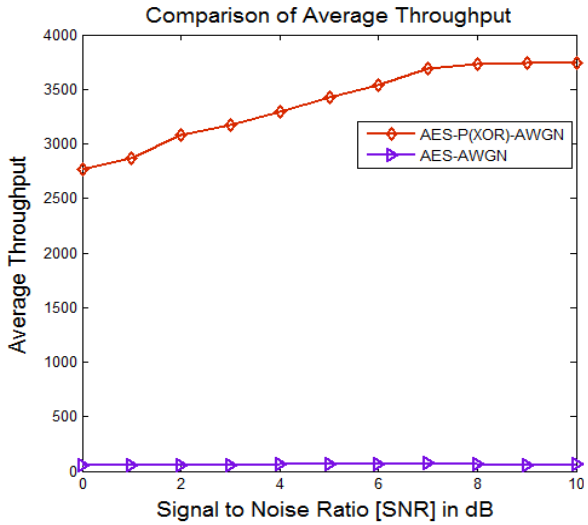

Figure 7: Average Throughput vs. SNR

can be said that the traditional AES algorithm consumes nearly 90% more transmission power than the proposed scheme to transmit the data over the AWGN channel to achieve the same BER.

B. Average Throughput:

In the present scenario, if the AES algorithm was applied to all the input frames, the throughput becomes very less, and more than 90% of the bits get corrupted or lost over AWGN channel, as shown in Figure 7. For example, at lower SNR value of 6dB with traditional AES algorithm, only 250-260 bits out of 3840 bits are received correctly, but if the input frames were encrypted with AES-P algorithm and transmitted over AWGN channel, it gives an efficient throughput, and 3400-3450 bits out of 3840 bits are received. Hence, AES-P algorithm is efficient for data transmission over AWGN channel for lower SNR values as compared to the traditional AES, which is suitable for IoT network.

C. Avalanche Effect (Security) Analysis

Table 4 shows the test of avalanche effect for the proposed algorithm. It illustrates the change in the number of bits and its percentage in the ciphertext bits corresponding to change in 1, 2 and 3 bits in plain text for the single frame of 128 bits. Its average value was around 50% which is desirable.

D. Complexity, Elapsed Time & Processing Power

Here, the elapsed time was calculated for the traditional AES algorithm and proposed an algorithm for data transmission over the wireless channel. It was observed from Table 5 that the complexity is reduced by around 77% for data of 10 frames (128 bits/frame) with the proposed approach and the percentage reduction in the complexity increases with increase in a number of data frames. Further, the elapsed time is also reduced considerably by applying the proposed scheme. From the above analysis, the complexity and elapsed time for the proposed algorithms are predominant as compared to the traditional AES. Since processing power depends on the complexity and the execution time, it also decreases on applying AES-P.

Table 4
Avalanche Effect Analysis

No of bit changed in Plain Text	No of bits changed in Cipher Text	% Avalanche effect in AES-P
1	62	48.412
2	63	50.218
3	66	51.56

Table 5
Comparison of Complexity & Elapsed Time

Parameters	n	AES	AES-P	% Reduction
Complexity (in terms of operations)	10	390*2	87*2	77%
	20	780*2	97*2	87%
	50	1950*2	127*2	93%
Elapsed Time (in seconds)	10	79.271	53.890	32%
	20	80.038	58.710	26%
	50	84.087	59.677	29%

Table 6
Test Result of Randomness Testing

S. No.	Test	AES	AES-5	AES-P
1	Frequency	0.05898	0.00175	0.07572
2	Block Frequency	0.49439	0.85138	0.28967
3	Cumulative Sums	0.53415	0.65793	0.08559
4	Cummulative Sums	0.53415	0.95583	0.73992
5	Runs	0.81654	0.35048	0.41902
6	Longest Runs	0.01791	0.05194	0.61631
7	Approximate Entropy	0.88317	0.93571	0.05194
8	Serial	0.38383	0.41902	0.93572
9	Serial	0.88317	0.13728	0.77919

E. Randomness Testing

The randomness of the block cipher generated with the traditional AES and the proposed AES-P scheme was tested using the NIST statistical test suit. Cipher consists of 100 blocks of 128 bits. The test results are shown in Table 6. We checked the randomness after all the ten rounds (AES), after five rounds (AES-5) of the standard AES algorithm, and also for the proposed AES algorithm (AES-P) and it is

concluded that the cipher generated from the proposed AES also exhibits sufficient randomness as that of that generated from its traditional counterpart (AES). Further, the randomness of AES-5 is nearly the same as that of AES-P with less number of numerical computations as compared to standard AES.

Therefore, the proposed algorithm is suitable for data transmission for CPS/IoT network due to adequate BER, good throughput, better avalanche effect, less computational complexity, less processing time, sufficient randomness and high power efficiency (transmission and processing).

VII. CONCLUSION

CPS/IoT Networks is the system of smart objects with some basic requirements, such as security, high power efficiency, and high BER performance, efficient throughput, less complexity and less elapsed time. As we have seen that the traditional AES is inefficient for CPS/IoT networks due to its limitation of data transmission over the wireless channel; so, to overcome this problem, this paper proposes a security algorithm, AES-P, using X-OR mapping on AES. Since the number of operations performed is reduced significantly in AES-P its power requirement, computational complexity and time required to process the algorithm are reduced. It is shown in the results that the computational complexity and the elapsed time is reduced significantly when applying AES-P as compared to that of traditional AES. Additionally, when encrypted data is transmitted over the AWGN channel using AES-P, BER performance improves substantially. It can be concluded that to achieve the same BER traditional AES requires considerably more transmission power as compared to the proposed approach, so the proposed approach is power efficient. Avalanche effect is also calculated and found satisfactory to test the security level of AES-P. Further, the block cipher generated by AES-P is sufficiently random. So the proposed security algorithm may be well suited for CPS/IoT systems deployed in noisy wireless channels.

REFERENCES

[1] Dhananjay, S., et al.: 'Secure Layer Based Architecture for Internet of Things' IEEE world forum on Internet of Things (WF-IoT), IEEE, 2015, pp. 1-12.

[2] Aylin, Y.: 'Wireless physical layer security: Lessons learned from information theory' Proc. of the IEEE, 2015,103 (10), pp.1814-1824.

[3] Reiter Gil: 'Wireless Connectivity for the Internet of Things.' Texas Instruments, White Paper, June 2014, pp. 1-12.

[4] Soni, A., Upadhyay, R., Jain, A.: 'Internet of Things & Wireless Physical Layer Security: A Survey,' Proc. Int. Conf. Computer Communication Networking and Internet Security, Vijayawada, November 2016, pp. 115-123

[5] Qian, X., et al.: 'Security enhancement for IoT communication Exposed to Eavesdropper with uncertain locations', IEEE Access, 2016, pp.1-12.

[6] Isha, et al.: 'Analysis of Lightweight Cryptographic Solutions for Internet of Things', Indian Journal of Science and Technology, 2016 9(28), pp-1-7.

[7] K. D. Muthavhine, M. Sumbwanyambe: 'An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect', Int. Conf. on Information & Comm. Tech., 2018

[8] Karsanbhai R, Grace, M.: 'AES Algorithm for Secured Wireless Communication', Conf. on Recent Trends in Engineering & Technology, May 2011, pp. 13-14

[9] Jia, C., et al.: "An Analysis of International Data Encryption Algorithm (IDEA) Security against Differential Cryptanalysis," Wuhan University Journal of Natural Science, 13, (6)2008, pp. 697-701

[10] Kulkarni S, et al.: ' Internet of Things (IoT) Security'. Int. Conf. on Computing for Sustainable Global Development (INDIAcom), IEEE, Feb. 2016, pp 821-824.

[11] Khan R., et al.: 'Future Internet: The Internet of Things architecture, possible applications, and key challenges'. Proc. 10th Int. Conf.. FIT, Islamabad, Dec. 2012, pp. 257-260.

[12] Rajshekhar P., Mangalam H.: 'Efficient FPGA Implementation of AES 128 Bit for IEEE 802.16e Mobile WiMax Standards', Scientific Research Publishing, Circuits and System, 2016, 7, pp. 371-380

[13] Goswami M., Kanojiya S.: 'High-Performance FPGAImplementation of AES Algorithm with 128-bit keys' Proc. of IEEE Int. Conf. Advances Computing Comm., vol 1, Himarpur, India, 2011, pp. 281-286

[14] 'DDoS Quick Guide- National Cybersecurity and communication integration', TLP: WHITE, 29 January, 2014.

[15] Mukherjee A.: 'Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality under Resource constraint'. Proc. IEEE, Oct. 2015,103, (10), pp. 1747-1761.

[16] Shilparani, et al.: 'High Performance of AES using XOR Based Mixed Column', Int. Journal of Ethics in Engineering & Management Education, May 2014, 1,(5), pp. 123-126.

[17] B. R. Gangadari and S. Rafi Ahamed, "Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications," in *Healthcare Technology Letters*, vol. 3, no. 3, pp. 177-183, 9 2016.

[18] W. Yu and S. Köse, "A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 11, pp. 2934-2944, Nov. 2017.

[19] K. Tsai, Y. Huang, F. Leu, I. You, Y. Huang and C. Tsai, "AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments," in *IEEE Access*, vol. 6, pp. 45325-45334, 2018.

[20] B. Li and Y. Pei, "Measures for error avalanche and energy avalanche effect in secure wireless fieldbus systems," in *China Communications*, vol. 16, no. 2, pp. 202-214, Feb. 2019.

[21] Alam T, Benaida M.: 'The Role of Cloud-MANET Framework in the Internet of Things (IoT)'. International Journal of Online Engineering (iJOE). 2018;14(12):97-111. DOI: https://doi.org/10.3991/ijoe.v14i12.8338

[22] Alam, Tanweer. (2018) 'A reliable framework for communication ininternet of smart devices using IEEE 802.15.4.' ARPN Journal of Engineering and Applied Sciences 13(10), 3378-3387.

[23] Alam T, Benaida M.: 'CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices.' International Journal of Interactive Mobile Technologies (iJIM). 2018 Nov 1;12(6):74-84.

[24] Alam, T., Rababah, B.: 'Convergence of MANET inCommunication among Smart Devices in IoT', International Journal ofWireless and Microwave Technologies(IJWMT), Vol.9, No.2, pp. 1-10, 2019.

[25] Alam, T.: "Blockchain and its Role in the Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp. 151-157, 2019.

[26] William Stalling: 'Cryptography and Network Security', Principle & Practices, 2012, (4th edn.), pp-289-320.

[27] Wang T., et.al: 'Empirical Network Performance Analysis on IEEE 802.11g with different Protocols and Signal to Noise Ratio', IEEE, 2005, pp. 7803-9019

[28] H. Shi, Y. Deng, Y.Guan, 'Analysis of Avalanche Effect of the AES S-box', Int. Conf. on Artificial Intelligence, Management Science and Electronic Commerce, Sep2011.

[29] Farshid, H.: 'Analysis of Avalanche Effect on Advanced Encryption Standard by using dynamic S-box depends on round key', Int. Conf. on Computational Science and Technology, May 2014, 8

[30] Ariffin, S., Yusof, N.: 'Randomness analysis on 3D-AES block cipher', Int.Conf. on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Jul 2017

[31] Soni, A.. Upadhyay, R., Kumar, A.: 'Wireless physical layer key generation with improved bit disagreement for the internet of things using moving window averaging' Physical Communication, Elsevier April 2019, pp. 249-258