Security Enhancement In 3G And 4G Networks

M.M. Prasada Reddy
Associate Professor, DIET , Hyd

Abstract: *4G, the cutting edge portable media transmission network, is the necessity for security improvement and solid correspondence. This paper introduces the plan of security improvement systems for information transmission in LTE systems utilizing TLS. Here AES is utilized for encryption. AES is improved by utilizing Chaos and Dynamic S-box. By the utilization of chaos the shift rows is made dynamic and the key space is made infinite. S-box is made dynamic and key dependant using cipher key. Complexity of the system is increased by using AES in round structures. Examination of the traditional and improved AES will be made on the premise of Performance assessment utilizing Encryption Time, Decryption Time, Overall Time, and Throughput.*

Key words: 4G; AES; S-box; Round structure; Chaos

1.Introduction :

Cryptography is the practice and investigation of strategies for secure correspondence within the sight of third parties. In the present time of data innovation, cryptography expect uncommon significance. Cryptography is presently routinely used to ensure information, which must be imparted as well as spared over long stretches, to secure electronic reserve exchanges and arranged interchanges. Current cryptographic procedures [1] depend on number theoretic or arithmetical ideas.After the arrival of 1G network right now 4G, the cutting edge versatile mobile telecommunication network, is the necessity for security upgrade and reliable correspondence. A 4G framework, notwithstanding the standard voice and different administrations of 3G, gives versatile broadband Internet access, for instance to portable PCs with remote modems, to smart phones, and to other cell phones. 4G wireless networks work totally on the TCP/IP, henceforth one might say that it is totally IP based.

A standout amongst the most effective encryption methods is Advance Encryption Standard (AES).To give end-to-end security to information transmission, Transport Layer Security (TLS) is utilized. In TLS, AES is utilized for giving confidentiality. However, since the core structure of AES itself renders a perfect, straightforward mathematical technique, it yielding the algorithm susceptible towards arithmetical based cryptanalysis attacks. Hybridization of AES with other popular algorithms like DES,ECC, RSA [2-4] etc. can enhance its strength. AES is enhanced using dynamic S-Box and Chaos concept.

Chaos is another method, which seems promising [6]. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems are being investigated using this novel technique of nonlinear dynamics [7]. The chaotic behaviour is a subtle behaviour of a nonlinear system, which apparently looks

random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes [8]. The important characteristic of chaos is its extreme sensitivity to initial conditions of the system. Enhancement of the key generation method of AES using chaos has increased more confusion and diffusion.Dynamic S-Box is produced utilizing cipher key algorithm as a part of which static S-Box is changed over to element to build the cryptographic quality of AES figure system[29]. The inverse S-box is additionally changed according to S-box.Analysis of algorithm is done on the premise of different parameters. The parameters are encryption time, decoding time, overall time, throughput,avalanche effect, CPU utilization, and memory expended.

1.1 Advance Encryption Standard

The Advanced Encryption algorithm also known as Rijndael after its inventors Vincent Rijmen and Joan Daemen. This algorithm works on 128-bit blocks and can use a key of 128, 192 or 256 bits in length. For encryption, each round consists of the four steps: Substitute bytes, Shift rows, Mix columns, and Add round key. For decryption, each round consists of the steps: Inverse sub bytes, inverse shift rows, inverse mix columns and Add round key.

1.2 AES S-box

The Rijndael S-box is a matrix (square array of numbers) utilized in the Advanced Encryption Standard (AES) cryptographic algorithm. The S-box is the substitution box which serves as a lookup table. The S-box is generated by determining the multiplicative inverse for a given number in GF (2^8)

1.3 Chaos Concept

The chaos is one kind of nonlinear movement form. It is produced by a definite system, and it relies on the initial condition, and it is unpredictable. The chaos system has several characteristics: stochastic, sensitive to initial condition, long-term unpredictability and so on. Chaos theory studies the behaviour of dynamical systems that are highly sensitive to initial conditions

2.Literature Survey

In 1991, Mark E. Bianco and Diamond Bar, workers of Hughes Software Company have enrolled a patent on Encryption System Based on Chaos Theory [14]. An encryption framework and strategy in light of the arithmetic of Chaos hypothesis, which gives security of information from unauthorized modifications and use amid its storage and transmission. In year 2001, L Kocarev has improved the work on the idea which included chaos in cryptography [10]. Research performed by Nicolas Courtois and Josef Pieprzyk demonstrated that the AES was designed as an arrangement of over defined system of Multivariate Quadratic conditions (MQ) [18]. In February 2001, G. Jakimoski, L. Kocarev demonstrates the investigation of the effect of chaos based methods with respect to block encryption ciphers. It introduces a few chaos based ciphers [15]. To overcome the drawbacks of Algebraic attacks on AES, M.B. Vishnu, S.K. Tiong, Member IEEE, M. Zaini, Member IEEE, S.P. Koh, Member IEEE, presented another calculation called Hybrid AES-DES used to secure transmission of digital motion image. In September 2008, Krishnamurthy G N and

V Rama swamy in the paper[23] made S-box key ward without changing its value and without changing the inverse S-box. The paper [5] demonstrates change of static S-box to dynamic in light of one-dimensional chaotic maps. In 2010, two professors, Jonathan Blackledge and Nikolai Ptitsyn, have given the idea of Encryption utilizing Deterministic Chaos in 2010. In this they addressed the significance of being „random", „unpredictable" and „complex "and what do these properties mean scientifically and how would they identify with bedlam. Additionally demonstrated the issues connected with outlining pseudo-irregular number generators in view of riotous systems. RaziHosseinkhani and H. Haj SeyyedJavadi produce Dynamic S-Box utilizing figure 1.Figure 1 shows the overall security system which is inclusive of all the three aspects of secure data transmission

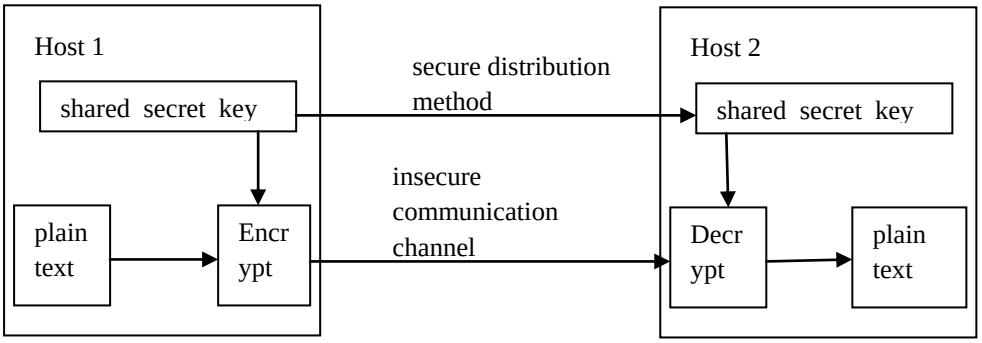

Figure 1: Proposed model

Data Encryption: Using AES-128 Bit.
Message Authentication: Using SHA-256.
Key Exchange Mechanism: Using ECDHE-384.

cipher key in AES Cipher System in 2012. They change static S-box into dynamic to increase the cryptographic strength of AES cipher system. Authors of [25] described the process of producing S-Box dynamically from cipher key and finally analyze the results and experiments. In paper [26], Julia Juremi, RamlanMahmod, SalasiahSulaiman made AES S-box key dependent to make AES stronger. Here, only the S-box is made key-dependent without changing the value. In January 2013 in [27] authors Shabaan Sahmoud, WisamElmasry and ShadiAbdulfa proposed enhancement of the security of AES against modern attacks by using variable key block cipher.

3. PROPOSED SYSTEM

3.1 Research Gaps

In this paper, improving the security of AES against modern attacks by using variable key block cipher, according to the results it seems that the algorithm is slower and has more complexity to AES. In this paper, Security improvement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm, it does not provide resistant against algebraic attacks. In this paper, AKA and Authorization Scheme For 4G Mobile Networks Based on Trusted Mobile Platform, authors explain the primary drawback in 4G security is

that its use of cryptography does not provide end-to-end security. So, for secure data, end-to-end encryption is done , e.g. Using SSL/TLS, SSH, a VPN.

3.2:Problem definition

A cryptographic system should be designed with respect to three components:

- Cipher text generation
- Key exchange
- Authenticity

This work is mainly focused on the improvement of encryption algorithm but any improvement in message authentication and key exchange is easily considerable. Further performance evaluation of selected symmetric encryption algorithms has to be done. The selected algorithms are AES, DES and DES with Feistal structure, AES with Feistal structure and Hybrid AES-DES structure. There are certain attacks on the AES algorithm such as linear, algebraic attacks hence to increase the complexity . AES is used in Feistel structure. The S-box of AES algorithm is improved by making it dynamic [30]. Further performance evaluation of selected symmetric encryption algorithms has to be done. The performance evaluation has been done based on parameters: Avalanche Effect, Throughput, CPU Usage, Encryption and Decryption Time.

3.3 Model Development

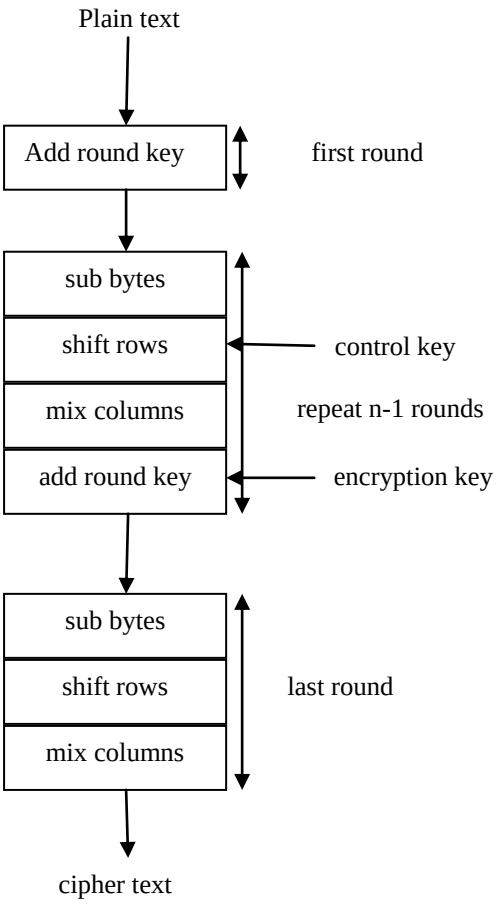

Figure 2 AES with chaos concept

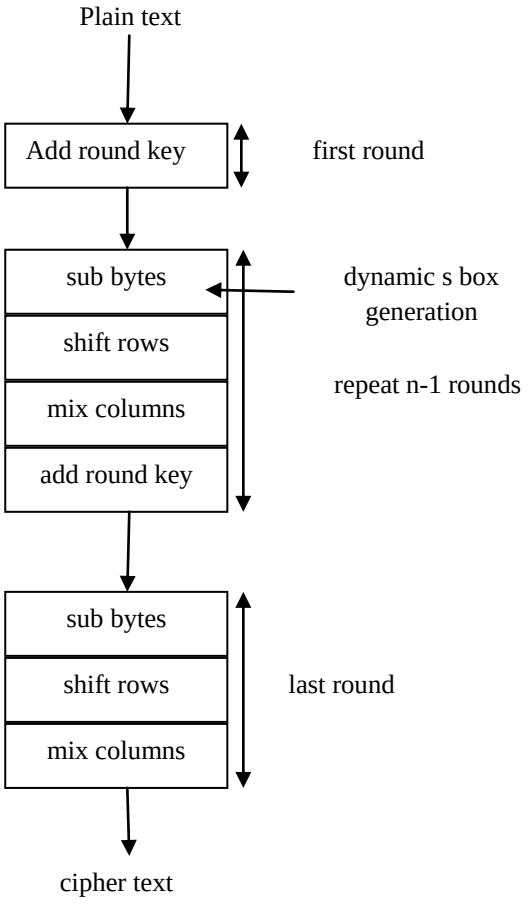

Figure 3 AES with dynamic S box

Detailed Hybrid structure using chaos and dynamic S-box generation is shown in the figure 2

- The main objective is to provide end-to-end security for data transmission using TLS in which input data is converted to blocks and then can be applied to a hybrid structure in which AES is improved by using chaos and dynamic S-box using cipher key, within the Fiestal network .
- The input data at the transmitter is converted into blocks and each block is divided into two sub blocks of exactly half the size and this is passed to a hybrid based AES which is constructed using Feistel equations and by incorporating the AES with dynamic S-box and chaos.

$L_n = R_{n-1} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$

$R_n = AES\left(L_n \oplus f(R_{n-1}, K_n)\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$

From Equation (2), each R_{n-1} and K_n is channelled into the round function, which basically revolves on a XOR function between these variables.

- The output of the round function is then XORed with L_n - before being channelled as input data for the AES algorithm. The key schedule process for the hybrid system uses concept of chaos. Two dimensional chaotic map [28] used here for key generation in AES. One generates the encryption key and other gives the number of shifts for the shift row round of AES. It will be enhanced by converting static S-box into dynamic which is forwarded to sub-bytes. This is done for 1, 5 and 10 rounds respectively.
- The result from the AES process represents R_n
- After completing it, Equations (1) and (2) are then iterated over a number of rounds using dynamic S-box chaotic key sequences.
- A complete Hybrid AES operation can be performed using 10 layers of Feistel calculations, including 10 sets of AES. This makes the system resistant to algebraic attacks and linear attacks.
- Lastly, all the encrypted blocks are put serially for transmission and similar action has been performed. The inverse process can be applied similarly at the receiver end for decryption.

4. EXPERIMENTAL RESULTS

The results carried out on the basis of encryption and decryption time. Computer Configurations used are Microsoft Windows 8.1, Intel i3 CPU 3210M @ 2.50 GHz, 4 GB RAM and Matlab 2013a. The results are tabulated table 1. For text file, “plaintext.txt” of 82

bytes, the number of bits is 656 For Image file, “smiley.jpg” of 2.35 KB, the number of bits is 19328.

Table 1: Based on Encryption Time on Text file

Algorithm	Bits in one block	Total number of bits	Encryption time	Decryption time
AES	128	656	0.0671268	0.00580755
AES with dynamic S box	128	656	0.151179	0.00257444
AES with chaos	128	656	0.021632	0.0323244

Table 2: Based on Encryption Time on Image file

Algorithm	Bits in one block	Total number of bits	Encryption time	Decryption time
AES	128	19328	1.25079	1.49089
AES with dynamic S box	128	19328	0.193199	205807
AES with chaos	128	19328	0.4356	0.3732

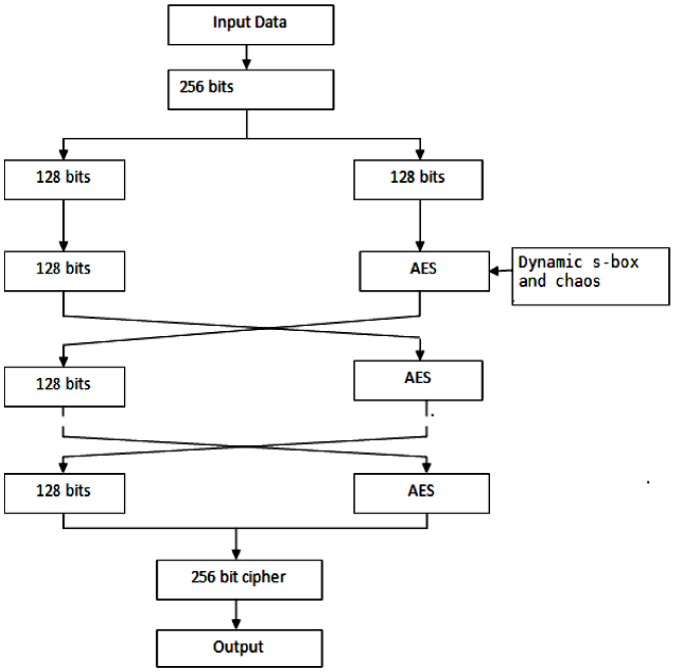

Figure 4: Fiestel AES with chaos and dynamic S-box

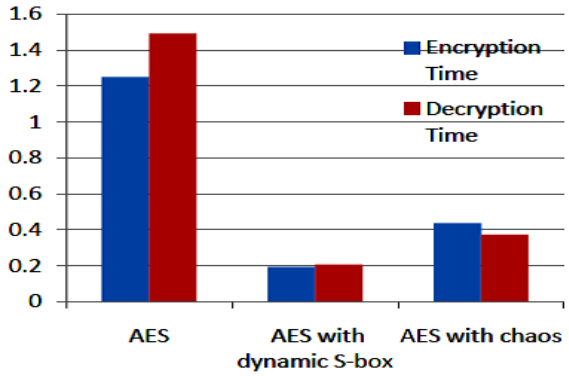

Figure 5: Graphical representation of results based on encryption time on Text file

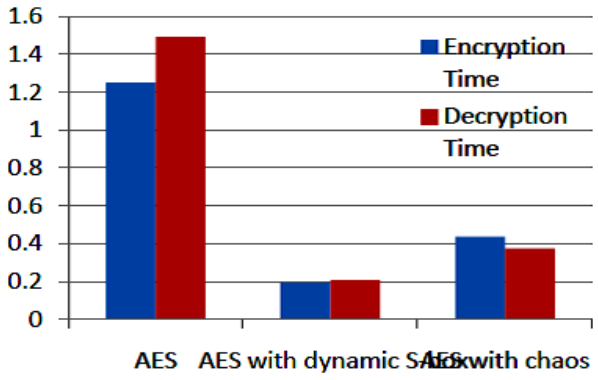

Figure 6: Graphical representation of results based on encryption time on Image file

5.Conclusion

4G technology offers high information rates that will produce new patterns for the market and prospects for set up and also for new media transmission organizations. The essential shortcoming in 4G security is that its utilization of cryptography does not give end-to-end security. So to give end-to-end security, SSL/TLS is utilized. TLS is a convention made to give validation, secrecy and information uprightness between two imparting applications. Consequently Transport Layer Security is utilized for security as a part of this venture. TLS utilizes AES as an encryption calculation. AES is one of the encryption strategies which is utilized most every now and again on account of its high effectiveness and effortlessness. Accordingly the enhanced model of AES gives a superior non linearity to the original AES and due to its round structure, there is better dissemination. Thus the likelihood of a arithmetic attack and linear attack on this model is reduced. It is upgraded by changing over static S-confine to dynamic AES itself. The S-box can be made dynamic utilizing cipher key. We would like increase the complexity of the system, by utilizing an AES Round(Fiestel) structure. The purpose behind increasing complexity is to make the system attack resistant and make the data secure from attackers. We additionally plan to assess the network for audio file, video file and utilize QPSK modulation/demodulation alongside AWGN channel to make 4G situation. This will be the future extent of the work.

7. REFERENCES

[1] Shannon C E, Communication Theory of Secrecy Systems, bell Systems Technical Journal,1949:28:656-715.

[2] M.B. Vishnu, S.K. Tiong. "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm," APCC 2008 OF IEICE, 2008.

[3] Xiang Li, Junli Chen, Dinghu Qin, Wanggen Wan. "Research and Realization based on hybrid encryption algorithm of improved AES and ECC," IEEE journal 2010.

[4] Dr. E. Ramaraj, S. Karthikeyan and M. Hemalatha. "A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA)," International Journal of The Computer, the Internet and Management Vol. 17.No.1, April 2009.

[5] GhadaZaibi, AbdennaceurKachouri, FabricePeyrard, Daniele Foumier-Prunaret, "On Dynamic chaotic S-BOX," IEEE 2009

[6] L Kocarev. "Chaos-based Cryptography:aBrief overview," IEEE Circuits and Systems Magazines,2001:1(3):6~22
[7] Gonzalo Alvarez1 and Shujun Li2, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006

[8] Blackledge, J., Ptitsyn, N.: Encryption using Deterministic Chaos. "ISAST Transactions onElectronics and Signal Processing," vol. 4,issue 1, pp. 6-17. 2010.

[9] Bruce Shneier, "Applied Crptography :protocol Algorithms," and source code in C.Johnwiley&Sons,Inc, 1996.

[10] LjupcoKocarev and ShiguoLian (Eds.): "Chaos-Based cryptography, Theory," Algorithms and Applications. Studies in Computational Intelligence ISSN 1860-949X, 2011 Springer-Verlag Berlin Heidelberg.