IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.
www.ijiset.com
ISSN 2348 – 7968

Secure Communication in Wireless Sensor Network using Symmetric and Asymmetric hybrid Encryption Scheme

Mrs.A.S. Bhave[1], Mr.S.R.Jajoo[2]

[1] Department of Electronics, Mumbai University, Datta Meghe College of Engineering, Airoli, Navi Mumbai, Maharashtra, India.

[2] Department of Electronics, Mumbai University, Datta Meghe College of Engineering, Airoli, Navi Mumbai, Maharashtra, India.

Abstract

One of the main goals of wireless sensor network (WSN) is to carry reliable information from one node to another node in a network. This paper is aimed in providing high security to wireless sensor networks using an improved AES-ECC hybrid encryption scheme.

The paper analyses the AES algorithm and S-box structure, S-box structure is proposed to improve AES encryption algorithm. Using AES algorithm, Plain text message sent by sender is changed into completely new cipher text, looking into which attacker cannot guess original message at receiver using AES decryption, same plain text is successfully recovered from AES encrypted cipher text.

Keywords: *Network Security, Algorithm Hybrid Encryption, AES, ECC.*

1. Introduction

Cryptography is a very basic technique for data security in WSN. Depending on key used this technique is classified in two categories symmetric encryption and asymmetric encryption. Both techniques have some benefits as well as some limitations. Symmetric key cryptography is fast in operation but as same key is need to be shared between sender and receiver security to this key is a challenging task. Whereas asymmetric key cryptography solves problem of secure exchange of key but it is comparatively slow than symmetric key cryptography.

To increase competency and to minimize drawbacks we propose a hybrid encryption scheme which combines two algorithms Advance Encryption Standard (AES) and Elliptical Curve Cryptography (ECC).

2. AES Algorithm

AES is a symmetrical encryption algorithm mostly suitable for encrypting bulk of data. It operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field [4].

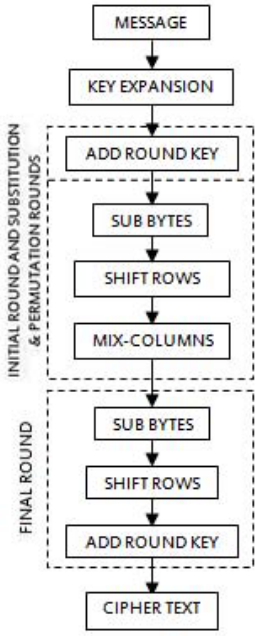

Fig 1: AES Algorithm

Fig shows basic steps to implement AES algorithm. This basically includes repetitive rounds of some permutations and combinations to change a simple text into complex data. We have performed such 10 rounds to convert plain text into cipher text.

3. IMPLEMENTATION

3.1 Step 1: Message

A 4*4 matrix is considered as the Plain text [A] for transmission -

ISSN 2348 – 7968

$$\begin{pmatrix} 0 & 17 & 34 & 51 \\ 68 & 85 & 102 & 119 \\ 136 & 153 & 170 & 187 \\ 204 & 221 & 238 & 255 \end{pmatrix}$$ 4*4 matrix.

Fig 2: Original message

Step 2 - Key Expansion

Actual Key Size used in this algorithm for encryption is 8 bytes. As plain text is a 4*4 matrix, key is expanded to – 44*4 matrix using reshape Transformation.

Mat lab code: W= (reshape (key, 4, 4));

Step 3 – Add Round Key

In this step 16 bytes of this expanded key called as round key is added(Bitwise XORed) to the plain text to get a new **text A'**.

Mat lab code: state_out = add_round_key (state_in, round_key);

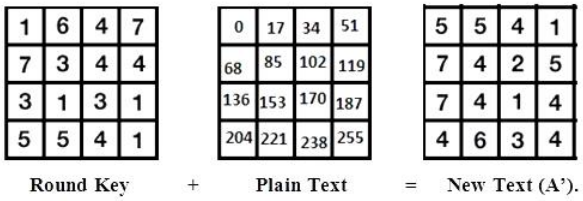

Fig 3: Add round key operation

Step 4 – Sub Bytes ()

Substitute bytes — Uses an S-BOX to perform a byte-by-byte substitution of the block. If first element in plain text is 05 it is replaced a by 0^{th} row 5^{th} column s- box element.

Matlab code: Text A'' = subbyte (Text A', s-Box).

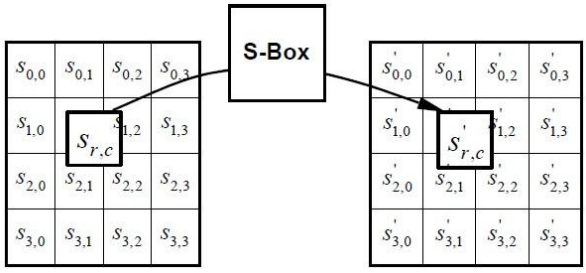

Fig 4: Sub Bytes () operation

Step 5 - Shift Rows ()

This step is a simple permutation where each byte in row is shifted left. Elements in 1^{st} row are shifted 1 position left, in 2^{nd} row are shifted 2 positions left and at the end again we got a new text **A'''**.

Matlab code: Text A''' = shift (Text A'')

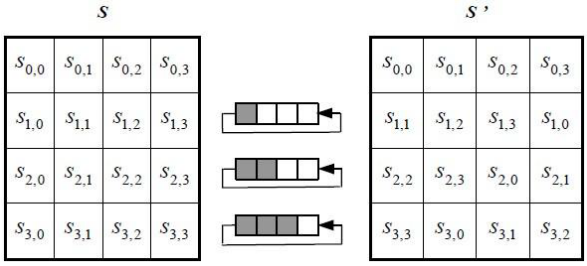

Fig 5: Shift Rows () operation.

Step 6 -Mix Columns ()

Transformation operates on the State column-by-column, treating each column as a four-term polynomial, the columns are considered as polynomials over GF (2^8).

Matlab code: state_out = mix columns (state_in, poly_mat).

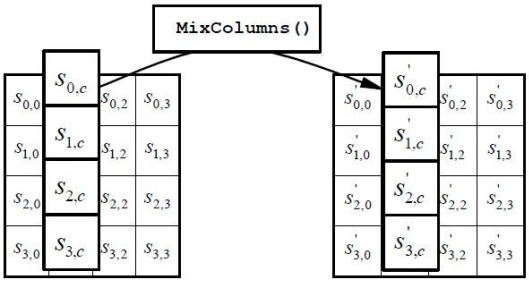

Fig 6: Mix Columns operation

3.2 RESULTS

Using all above steps plain text [0 17 34 51 68 85 102 119 136 153 170 187 204 221 238 255] is encrypted in Matlab 7.10.

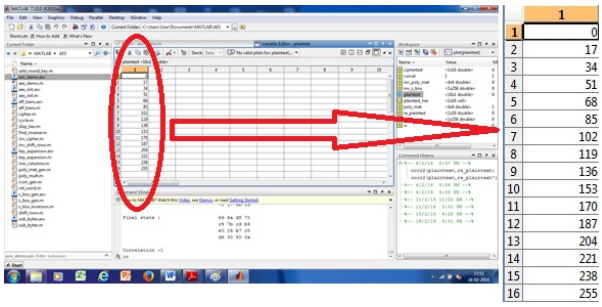

Fig 7: Input text to AES algorithm

After encryption plain text is converted in completely new cipher text [105 196 205 216 106 123 4 48 216 205 183 128 112 180 197 90]

ISSN 2348 – 7968

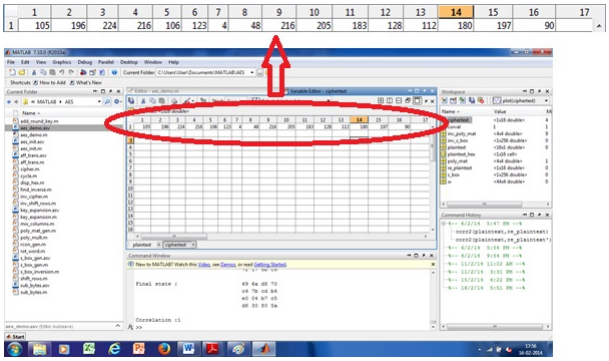

Fig 8: Output text of AES algorithm

At receiver, using decryption, using inverse s-box we again got the same plain text which was transmitted by transmitter and hence correlation obtained is 1.

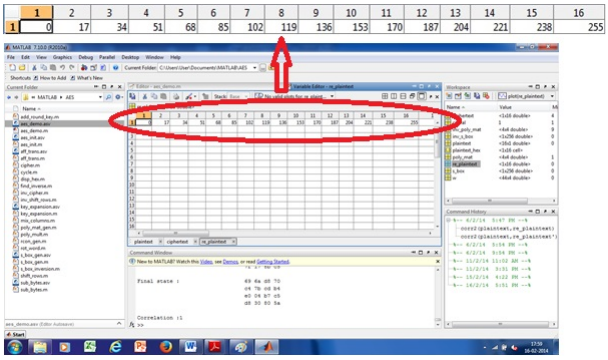

Fig 9: Original Text at receiver after decryption

4. Conclusions

Wireless sensor networks are frequently used for monitoring of crucial information therefore security of such networks is an important issue. Advanced Encryption standard has been rightly suggested as the most suitable symmetric cipher for wireless sensing network applications.

Advanced Encryption standard applies many complex mathematical calculations on plain text like reshaping of initial key, XOR operation with polynomial matrix. This algorithm uses 10 such rounds of operation so plain text gets converted into complete new cipher text. Use of s-box substitution makes easy reverse track but hard to find by attacker. Also time required for encryption is very less. For testing purpose 16 bytes of plain text data and key is considered in future implementation on larger data will be done.

4.1 Future Work

This paper only comments on the use of AES algorithm for encryption of plain text. Proposed work also includes implementation of ECC algorithm to get more complex cipher

Acknowledgments

I sincerely feel that the credit of this paper work could not be narrowed down to only one individual. This work is an integrated effort of all those concern with it, through whose able cooperation and effective guidance I could achieve its completion.

I express my gratitude to my guide **Prof. S. R. Jajoo** for being kind enough to spare his valuable time and guidance on the topic **"Secure Communication in Wireless Sensor Network using Symmetric and Asymmetric hybrid Encryption Scheme."**

I am also thankful to H.O.D. **Dr. D.J. Pete** for his support and encouragement. I sincerely thank to Principal **Dr. S. D. Sawarkar** for providing all facilities, every help for smooth progress of project work.

References

[1] "Cryptography and Network Security" by Atul Kahate.

[2] Veerpal Kaur, 2Aman Singh. "Review of Various Algorithms Used in Hybrid Cryptography" International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013.

[3] Anirudh Ramaswamy Ganesh,Naveen Manikandan P2, Sethu S P,Sundararajan, Pargunarajan, "An Improved AES-ECC Hybrid Encryption Scheme for Secure Communication in Cooperative Diversity based Wireless Sensor networks," IEEE-International Conference on Recent Trends in information Technology, ICRTIT 2011.

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

[5] Fan Ng, Juite Hwu, Mo Chen and Xiaohua (Edward) Li, "Asynchronous Space-Time Cooperative Communications in Sensor and Robotic Networks," IEEE 2005.

[6] Hirani, Sohail A. "*Energy consumption of encryption schemes in wireless devices*. Diss. University of Pittsburgh", 2003.

[7] Jailin.S, Kayalvizhi.R, Vaidehi. V, "Performance Analysis of Hybrid Cryptography for Secured Data Aggregation in wireless sensor Networks," IEEE 2011.

[8] Hua Jiang, Xianglei Xing, Sidan Du, "Distributed Optimal Cyclotomic Space-Time Coding for Full-Duplex Cooperative Relay Networks," IEEE 2013.

[9] Tianfu, Wang, and K. Ramesh Babu. "Design of a Hybrid Cryptographic Algorithm." International Journal of Computer Science & Communication Networks 2.2 (2012).

[10] Kakkar, Ajay, M. L. Singh, and P. K. Bansal. "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network." International Journal of Engineering and Technology 2.1 (2012): 87-92.

ISSN 2348 – 7968

[11] Ekşim, Ali, and Mehmet Ertuğrul Çelebi. "Performance Improvement of Binary Sensor-Based Statistical Space-Time Block Code Cooperative Diversity Using Limited Feedback." *IETE Technical Review* 27.1 (2010).

[12] K.Brindha, G.Ramya."Secured Data Transfer in Wireless Networks Using Hybrid Cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013.