International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Secure the Sensor Node Data Using AES-EECA and Shamir in Wireless Sensor Networks

Anushka Tyagi[1], Dr. Vishnu Sharma[2], S.P.S Chauhan[3]

[1]M TECH (SCSE), GU, Greater Noida, UP

[2]Professor in SCSE Department, GU, Greater Noida, UP

[3]Assistant Professor in SCSE Department, GU, Greater Noida, UP

Abstract: ***Nowadays a huge demand of resource-limited Wireless Sensor Networksis the need for consistent and effective security devices for them has improved various but its application is a non-trivial task. Restrictions in processing speed, battery power, bandwidth and storage constrain the applicability of present cryptography procedures for WSNs. In this paper, a hybrid process is proposed AES-EECA-Shamir analysed and their suitability for resource-limited wireless network security are associated built on performance principles such as average energy of every node and implementation time. Using simulation tests and logical models, we give a significant investigation and deliberations on practical feasibility of these cryptographic processes in sensor networks to help designers predict security performance under a set of limitations for wireless sensor network.***

Keywords: WSN, Sensor nodes, AES, EECA and Shamir, security etc

1. Introduction

Nowadays wide growth of WSN that incorporate data centric routing protocols life applications of wireless sensor network such as health care, environmental monitoring, structural monitoring, automobile services and data logging. Both civil and military applications are shifting near WSN as sensor nodes are easy to organize However, for this real life application, security devices are compulsory to defend WSNs from malicious attacks [1]. Battery life time of sensor nodes and energy of system are incomplete. It is a requirement to progress an energy effective security device that is hard to decrypt by third party and consumes low power. Cryptography and art of hiding the text intellect, is used to resolution critical security issues. Cryptography is a method of secret script where unique significant data is transmuted to a no-precise data which has no importance and non-understandable. Its application is encryption for alteration of original text to secret text recognized as cipher text and decryption to retrieve original text back from cipher text. This device is based on key organization and also it is built on the no. of keys employed for cryptography process, here the mostly two kinds of processes as presented in figure 1 [2].

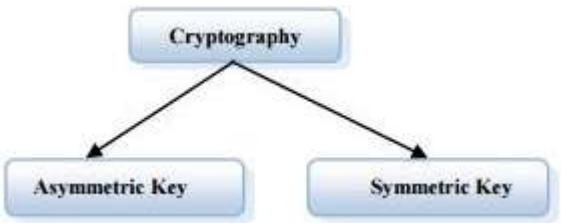

Figure 1: Classification of Cryptography

1.1 Public Key Cryptography

In cryptography PKC or asymmetric cryptology mechanisms are different keys for secure information. The PKC key is castoff for the encoded as public key. Transmitter will encode the information with the help of public key that is exposed for everybody, then it simply accepter has the secure or private decryption key to attain the innovative text.

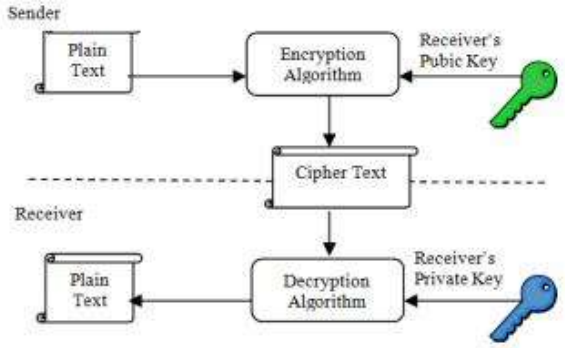

Figure 2: Public key cryptography

Some asymmetric key ciphers as per [3] are:
SSL handshake TinyPK
RSA

1.2 Symmetric key cryptosystem

For the security purpose this method uses the single key for both process which is encryption and decryption. It is work as mutual parties at both ends such as encryption and decryption. As signified in fig 2, the matching key have cast off through mutually transmitter and accepter.

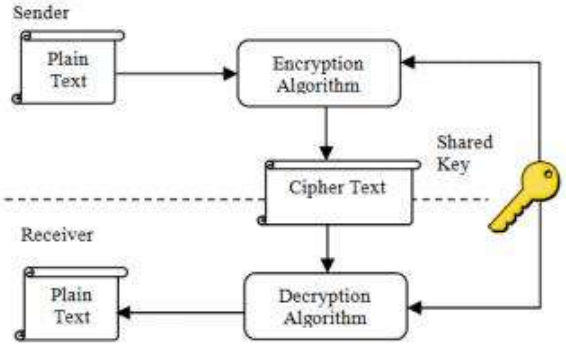

Figure 3: Symmetry key

Some symmetric cryptography systems as per [4] are: DES AES RC5

As specified through reference [5] symmetric key procedures are desired over the PKC. Public key procedures consume more energy and are less effectual than the symmetric key cryptography. The key problems for cryptographic procedure designer are: cost, security and performance [6]. In instruction to resolution severe security issues, we present a procedure on the basis of grouping of existing techniques like P-box, vigenere cipher; circular shift left

2. Architecture of Wireless Sensor Network

In wireless sensor network we can see the following mechanism:

1) Sensor particles– In this system Routers fixed in the procedure need to be accomplished of routing packages on the basis of other strategies. This mechanism controls the procedure and route equipment. The router is as ground device which haven't procedure sensor apparatus and does not border with the procedure.
2) Gateway or Access points – It gives the message transmission between Host request and area strategies.
3) Network administrator –When preserve the programmed message among procedures and outline of the grid for that Network Manager is important. Similarly achieves the steering boards and perceiving the ailment of the system.
4) Security manager – The task of Security Director is to manage the storing and organization of the Cryptology keys similar AES and DES. [5]

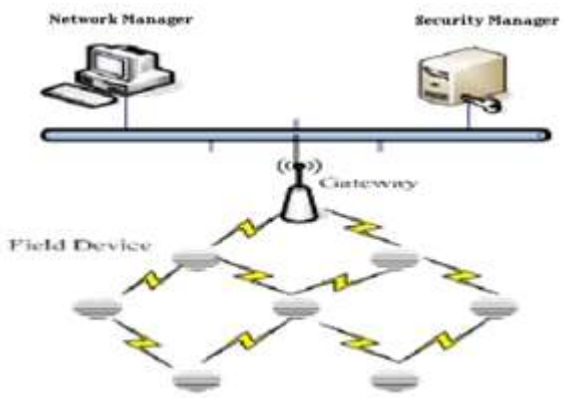

Figure 4: Wireless network sensor Construction

3. Proposed Methodology

3.1 Shamir for Key Generation

In initial stage the Information is encrypted with the secret key by using standard encryption algorithm. Second the key is splitted into multiple key executives. Each and every splitted key is encoded and stored. Currently as the consequence of encryption the information would be in the form of improved files(cipher text).In which Shamir's (k,n) Threshold System is used for the organization of keys that uses k segments out of n to reconstruct the key. Advanced Encryption Standard is a cryptographic Symmetric block cryptography procedure use similar key for cryptography procedure.

- Suppose one key is misplaced then other keys are used to improve the original key.
- It is challenging to hack the records storage in cloud by using numerous key managers.
- In which Shamir's (K, N) threshold system is used for the organization of keys.
- Single opinion of failure should not disturb the obtainability of information.

The shamir's threshold system is used for the group of keys which uses K shares out of n to rebuild the key during decryption. Currently the unique key is divided into numerous key directors. If one key is missing other keys are used to recover the secret key. Using various key managers the availability of nos. does not affected.

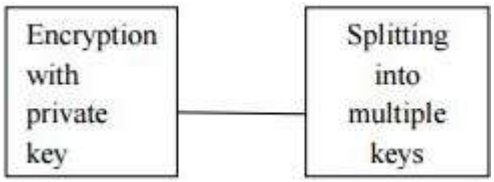

Figure 5: key splitting analysis

3.2 EECA

An EECA Procedure with 64-bit block distance and 128-bit key distance with modest procedures comparable exclusive-OR (XOR) and unstable is functional. It contributes hardware low-resource process that is appropriate to sense the policies. It is not simply includes of modest procedures but it is not necessary security like good encryption process. When it is decreases in the hardware properties also reduces the consumption of power in the WSN. We observe the efficiency of energy as symmetric key cryptology measures practical in wireless sensor networks and this reading deliberate both block cipher and stream ciphers. It originates the computational cost of energy for the ciphers under discussion through associating the no. of CPU cycles which is compulsory to accomplish encryption. When estimating a no. of symmetric key ciphers, we associate the energy enhancement of stream ciphers and block ciphers when it function to a noisy frequency in a wireless sensor network. In inference, we mention an insubstantial block cipher revealed to as byte-oriented substitution-permutation network (BSPN) for complete

efficiency of energy with a close of safety appropriate for WSNs.

3.3 Secure Transmission in Wireless Sensor Networks using AES cryptography

The simple idea of the projected cryptosystem technique depends on set theory. The encryption is definite as a relation among the language arranged and a set of sets "one set for each alphabetical element", although the decryption is a relation from a set of sets to the language alphabetic. As an instance the set of sets is the set of remainder classes for anassumed number N. Therefore, the encryption procedure is defensive a relation among the language alphabetic and the prime modular classes P for anexpected N integer no., where N>P, N signifies a secret dataamong the sender and the receiver, where each of them agree on using a secret channel. The sender uses the proposed encryption procedure to send a message to the receiver, concludedunsafe channel, and the receiver uses the proposed decryption procedure to read the received message. The proposed protocol pools the Advanced Encryption Standard (AES) beside with digital signature. AES is a block cryptogramthrough a block measurement of 128 bits. It involves of 10 sequences of dispensation for 128 bit keys, 12 iteration for 192 bit keys and 14 rounds for 256 bit keys. The encryption procedure and the decryption procedure are executed in the subsequent sub segment for the English alphabetical language. In this section, a secured power aware protocol is proposed using cryptography. This protocol is found to be more secured than other protocol. The protocol mutual with AES procedure and Shamir are originated to be more secured. Secured Power Aware Protocol for WSNs is based on the novel cryptosystem procedure.

Encryption Process

Encryption involves of 10 rounds of dispensation for 128 bits keys. Every round of

Dispensation contains unique particular byte created replacement step, a row-wise variation stage, a column-wise collaborating step, calculation of round key, modular periods for plain text and permutation for the consistent class. This uses a substitution-permutation system. The permutation and substitution method allows for a fast software process of the process. Intended for encryption, every round includes of the subsequent 4^{th}stages; substitute bytes, shift rows, mix columns and enhance over weight key. The former phase includes of XORing the production of the prior stages with four disputes after the key driver. A private key is used to encrypt and send the message beside with public key or round key.

Formerly some round-based dispensation for encoded, the contribution is XORed through the major four confrontations of the key package. The similar procedure take place for decryption, but cipher is XORed through latest four disputes of the key program.

Byte-by-byte substitution is accepted out in every round of encryption procedure. It decreases the association among the input bits and the production bits at the byte level. Shift rows are used to shift the rows of the state array.

Mix-column is castoff to combination up of the bytes in every column distinctly.

The modification rows stage beside with the mix column phase sources every bit of the encryption script to depend on each bit of the simple text after 10 circles of dispensation. A round key is additional to the productivity of the earlier step. The segmental classes for the input plain text are designed. The permutation process is useful to attain the cipher text.

Decryption Process

For decryption, every round contains the subsequent four stages; Inverse shift rows, Inverse temporary bytes, add round key and contrary mix supports. The previous stage involves of XORing the production of the prior stages with four words since the key program.

Formerly some round-based dispensation for encoded system, the contribution cipher text is XORed through the last four disputes of the key program.

Byte-by-byte Inverse substitution is approved out in every round of decryption procedure. It decreases the association among the contribution bits and the production bits at the byte close.

Inverse shift row alteration is used to shift the rows of the state array.

The Inverse round key is used for inverse add round key alteration.

Find the segmental classes for the input N

Apply an inverse permutation process to the input cipher text to achieve the plain text

4. Result

This work presents the hybrid cryptography of the AES-Shamir and EECA. In this investigation we reviewed the best collective approaches in the cryptography of a slab cipher system.

The resultant of Public-Key Processes is symmetric, that is to approximately use to encode the sensor data or given text by user is different from the key used to decrypt the message. The encryption key, identified as the

Public key which used to encode a communication, but the message can only be deciphered through the information that has the decryption key, recognized as the private key.

This type of encryption has a quantity of advantages over usual symmetric Ciphers.

It means that the recipient can create their public key approximately available- someone deficient to send them a communication usages the procedure and the receiver's

public key to do so. A viewer may have both the procedure and the public key, but will still not be capable to decode the text. Individual the receiver, with the private key can decrypt the message.

Confidential Data using AES-128, Shamir and EECA algorithm

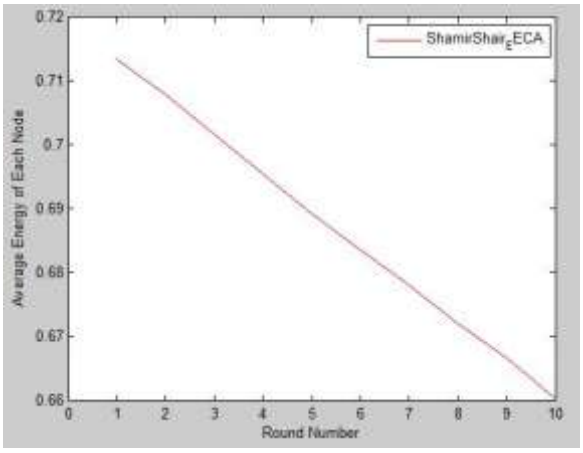

Figure 6: Average energy consumption of each node on round number

Figures [6] display the normal energy for the reproductionsparticipated in a 10 round in wireless sensor network. Each round displays the average energy feasting of analtered wireless device. The techniquethat consumes the leastquantity of influence is the noiseless negative technique with sleep/wakeup development.

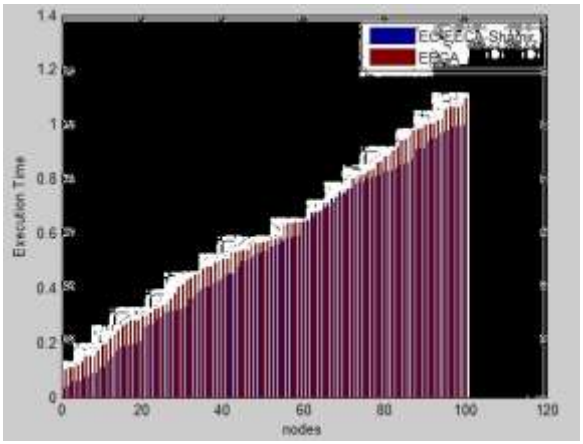

Figure 7: Execution Time

Above figure shows the execution time of EC-EECA-Shamir and EECA. We can see that the proposed method get low execution time as compare to EECA.

5. Conclusion

In most of the WSN system the time of battery life and the energy of the system are damaged. In this paper, it is exposed the enhanced EECA that contains the simple processes of S-box and move is appropriate to reduce the boundaries of radio sensor nodes. The outcome designates that the procedure accomplishes decline in hardware properties given that energy efficiency so increasing the life time of radio sensor nodes in the system.

There are particular disadvantages of AES Algorithm. In key based security organization, if decryption key is lost or corrupted during broadcast, it is difficult to improve the data. We can further eliminate the limitation of key-based security management.

References

[1] M. Rajalakshmi, 1 2C.Parthasarathy and 3R.V. Indrajith "Advanced Cryptographic Algorithm to Secure the Sensor Node Data in Wireless Sensor Networks" Middle-East Journal of Scientific Research 24 (6): 1926-1931, 2016

[2] Chowdhury, M. J. M., Pal, T., 2009 A New Symmetric Key Encryption Algorithm based on 2-d Geometry. In Proceedings of International Conference on Electronic Computer Technology (Macau, February 20-22, 2009), IEEE, 541-544.

[3] Lokesh, J., Munivef, E., 2009. Design of Robust and Secure Encryption Scheme for WSN using PKI (LWT-PKI) In Proceedings of the First international conference on Communication Systems and Network (Bangalore, January 5- 10, 2009), IEEE, 1-2

[4] Hager, C. T. R., Midkiff, S. F., Park, J. M., Martin, T. L. 2005. Performance and Energy Efficiency of Block Ciphers in Personal Digital Assistants In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications (Kauai Island, Hawaii, March 8-12, 2005), 127-136.

[5] Ahmad, S., Beg, M. R., Abbas, Q. 2010. Energy Efficient Sensor Network Security Using Stream Cipher Mode of Operation In Proceeding of International Conference on Computer and Communication Technology (ICCCT) (Allahabad, Uttar Pradesh, September, 17-19, 2010), 348- 354

[6] Karuppiah, A. B., Rajaram, S. 2012. Energy Efficient Encryption Algorithm for Wireless Sensor Network In Proceeding of International Journal of Engineering Research & Technology, ESRSA, 1(3), 1-7