High Performance and Efficient Secure Communication in Wireless Sensor Network with Non-linear S-box Using AES-CCMP

Velayutham Ramakrishnan and Siva Ganesh Elango

Department of Computer Science and Engineering, Einstein College of Engineering,Tamil Nadu, India

(Received: 06 May 2015; accepted: 05 July 2015)

A safe transfer of data among wireless sensor network (WSN) is an imperative challenge in current communication technology. In consequence, the communication requires a vital cryptographic algorithm to defend the data against attackers. This decisive pace has been implemented with Advanced Encryption Standards- Counter mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) with the Non-linear agreement of S-Box and Key scheduling. This is computationally realistic to solve various kinds of security issues with the ease of deployment. Non-linear arrangement has made the AES-CCMP algorithm further stronger to resist against all cryptanalysis attacks. Accordingly, the anticipated wireless sensor network comprises of base station that receives the encrypted data from other nodes. As a result, the encrypted data wraps with the non-linear AES-CCMP algorithm. The anticipated scheme exploits an Advanced Encryption Standard (AES) with CCMP which improvises the Confidentiality, Authentication and Integrity stabilizes the WSN with respect to both performance and security requirements. The proposed work implemented in Ns2. Experimental results show that the proposed scheme yields good solutions to increase the sensor network lifetime.

Key words: AES-CCMP, Non-linear, S-Box, NS2, Wireless Sensor Network.

WSN[1] is one of the essential technologies in recent computer networks. In fact, WSN have been successfully implemented in many campus networks and enterprise networks. The power supplies for sensors in the network are not usually rechargeable[2]. Cluster-based technique is considered an efficient approach to achieving energy efficiency. Low-energy adaptive clustering hierarchy (LEACH) protocol[3] is most popular clustering solutions to achieve energy efficiency. It is not suited for large network. Communication among today's WSN implies a great challenge among the users to maintain the integrity, confidentiality and authenticity of the transferred data[11]. In these situations users and devices need to be independently monitored based on location and authentication method. This network environment supports a wide variety of devices both wired and wireless sensor with many applications. In order to bring security amongst wireless sensor network, many of the cryptographic algorithms subsequently introduced for the practice of encryption and decryption of the needed data and also to resist from the attackers.

Security play vital role in WSN for sensitive application[14-16]. The cryptographic strength of the AES depends strongly on the choice of S-Box[5]. The result of the new attack methods shows that there may be some lacuna in the design of S-Box in the AES algorithm. The setback is the weakness of the existing linearity structure in the S-Box. After a detailed analysis on the AES algorithm a new performance scheme which comprises of Non-linear transformation in

* To whom all correspondence should be addressed.
E-mail: rsvel_kumar@yahoo.co.uk

the structure of S- box is presented in this paper. AES (128 bit key length) operates in a counter mode with CBC-MAC (CCM). Counter mode is used for data confidentiality and CBC-MAC is used for data integrity and authentication. As a result, the combination of AES-CCMP[7] improves authentication and increases the data transfer rate. The proposed solution has several advantages. The Non-linearity arrangement of AES S-Box makes the algorithm further stronger.

This work comprises of eight sections. Section 2 presents related works and its limitation. The proposed work furnishes the inclusion of AES algorithm with the CCMP protocol is discussed in section3. Section 4 describes the implementation and the achievement of Non-linear S-Box of the proposed system. Section V presents results and discussion. Finally, section 5 presents our conclusion and the scope of the work.

Advanced Encryption Standard (AES) provides strong encryption[4] that uses three key sizes: 128, 192 or 256-bit encryption key. The initial state is the plaintext and the final state is the cipher text for the encryption. The state consists of 4 rows of bytes. As the block length is 128 bits, each row of the state contains 4 bytes. The four bytes in each column form a 32 bit word. After an initial round key addition, a round function consisting of four transformations namely Sub Bytes, Shift Rows, Mix Columns and Add Round Key is applied to each data block. AES-128 applies the round function 10 times, AES-192 – 12 times and AES-256 – 14 times. A round is to perform the following four transformations:

Sub Byte

Transforming a byte value using a Non-linear Substitution table (S-Box);

Shift Row

Cyclically shifting the last three rows of an array by different offsets;

Mix Column

Using all the columns in an array and mixing their data to produce new columns;

Add Round Key

Adding the corresponding round key to an array;

Note that the round key is derived from the cipher key using key expansion.

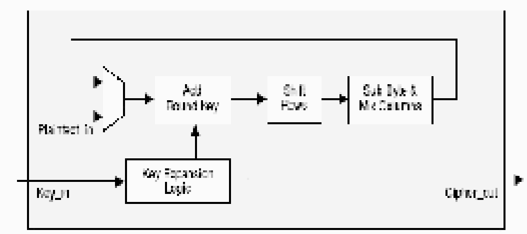

Fig. 1. Block Diagram of AES

NIST recommends that organizations with existing legacy IEEE 802.11 implementations develop and implement migration strategies to move to IEEE 802.11i based security because of its superior capabilities. IEEE 802.11i [10], an IEEE standard ratified in June 24, 2004, is designed to provide enhanced security in the Medium Access Control layer for 802.11 networks. The 802.11i specification defines two classes of security algorithms: Robust Security Network Association (RSNA) and Pre-RSNA. Pre-RSNA security consists of Wired Equivalent Privacy and 802.11 entity authentication. RSNA provides two data confidentiality protocols, called the Temporal Key Integrity Protocol, CCMP and the RSNA establishment procedure, including 802.1x authentication and key management protocols. Razvi Doomun *et al.*,[8] applied a systematic approach to determine computational complexity and efficiency of AES-CCMP designed for IEEE 802.11i.

AES security methodology

The only successfully published attacks against the full AES are side-channel attacks on some specific implementations. The National Security Agency reviews all the AES finalists, including Rijndael and states that all of them are secure enough for U.S. Government non-classified data and announced that AES may be used to protect classified information[12]. The design and strength of all key lengths of the AES algorithm are sufficient to protect classified information. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use by 2006, the best known attacks are on 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys. For enhancing Confidentiality and Integrity in IEEE 802.11i WSN, AES-CCMP is used. In a WSN, the security of the sensitive information will be maintained only through a cryptographic algorithm. As far as AES algorithm is concerned contravenes is with structure and the usage of S-

Box also does not focus with any protocol.

Nature of AES S-BOX

AES is used for the assessment of key generation. The key depends on 16x16 S-Box. It is perceivable to people from all known cryptographist, so we have to develop the S-Box by using some Non-linear transformation. Every transformation affects all bytes of the state. The transformation Sub Bytes is a Non-linear byte substitution that operates on each byte of the state using a table (S-Box). The numbers of the table is computed by a finite field inversion followed by an affine transformation. The resulting table is called an S-Box.

In AES algorithm the predefined S-Box is used for encryption and decryption[5]. The S-Box concept is applied in Sub Bytes transformation and Add Round Key transformation both in linear arrangement. So it is not secure. As of now, no successful attack has been reported against AES. But some of the inherent properties chosen for AES design itself pose a threat to its security. The cryptographic strength of the AES depends strongly on the choice of S-Box. Many cryptographists have discovered that there are some weaknesses in the design of the existing S-Box. The S-Box used in this algorithm is linear and so it is easy to predict the key. Carlet[9] introduced a method called Welch and the multiplicative inverse functions that used in the S-boxes of the AES to deduce bounds on the second order nonlinearity for classes of cryptographic Boolean functions. Mozaffari *et al.*,[10,17] used both S-box and inverse S-box and it was utilizing logic gates to malicious injected faults detection.

MATERIALS AND METHODS

CCMP

The computation occurs in two stages: First, the MIC is calculated and appended to the MPDU and then the entire MPDU is encrypted as shown in Fig. 2.

The implementation of CCMP represented as a block that use a sequence counter called the packet number (PN), which it increments for each packet processed. This prevents an attacker trying to reuse a packet that has previously been sent. The PN is 48 bits long and is large enough to ensure it never overflows. The first important point is that CCMP encrypts data at the MPDU level. There is one MPDU for each frame transmitted and the MPDU itself might be the result of fragmenting larger packets passed from a higher layer, called MSDUs. This is intentional to simplify implementation for access points that need to receive transmissions from a mixed group of TKIP and CCMP mobile devices. The format is shown in the Fig. 3.

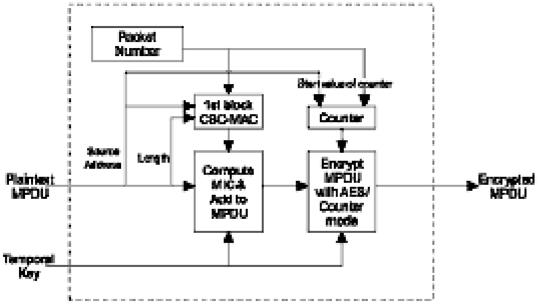

Fig. 2. CCMP Encryption block

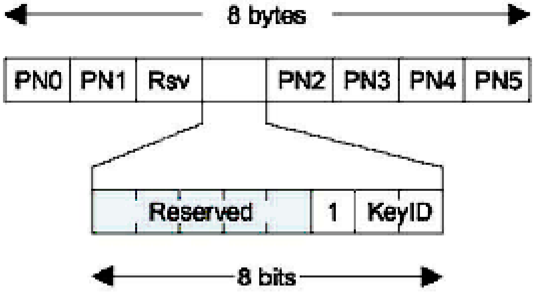

Fig. 3. CCMP Header

In CCMP the first block of the CBC-MAC computation is not taken directly from our MPDU but is formed in a special way using a nonce value. The nonce guarantees freshness by ensuring that each encryption uses data that has never been used before (under a given key). The packet number (PN) for the nonce is incremented for each MPDU and hence never repeats. However, one should remember that the key is shared between at least two communicating parties (more for the group key) and these parties may, each at some point, use a PN that has already been used by another party, violating the “use once per key” rule. To avoid this problem, the nonce is formed by combining the PN with the MAC address of the sender. The CCMP process gives protection against forgery, eavesdropping and copy/replay attacks.

Design and Implementation

The decryption phase has the same inputs as the encryption phase except that the input MPDU is encrypted. This is because the header information, including the CCMP header, is transmitted across the link in the clear text and can therefore be extracted by the receiver prior to decryption. Implementation of the CCMP block can be viewed as a single process with inputs and outputs, as shown in Fig. 4

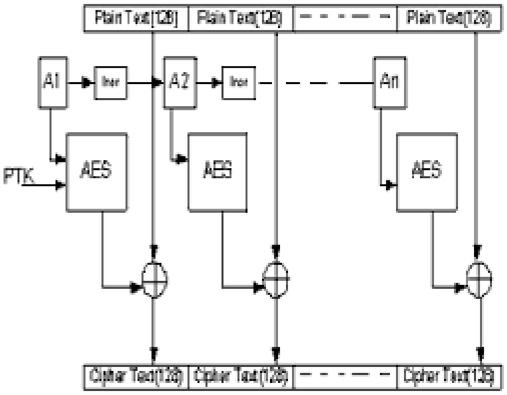

Fig. 4. Block diagram of AES CCM

Non-Linearity

In AES, the function of Non-Linearity is achieved by means of the Substitution Bytes step and Add Round Key Transformation. In the Sub Bytes step, each byte in the array is updated using an 8-bit substitution box[13]. S-Boxes substitute or transform input bit into output bit. It will have the property that each output bit will depend on every input bit. Here we propose to design a dynamic S-Box that is highly secure to all known attacks. In the Add Round Key step, 128 bit of state or message is XORed with 128 bit of round key. Since Non-Linearity is applied to the S-Box, the key is also protected. The key could not be known to the attackers due to the dynamic formulation of the S-Box. Thus it will provide an enhanced security.

Achievement of Non-linear AES S-Box

The entire construction is made tough by converting the existing linear structure of the S-Box into a Non-linear structure. The Non-linear structure can be achieved by substituting a random hexadecimal number to the actual S-Box value. When the real S-Box value is called it is mapped to a random hexadecimal number which is generated during the run time of the encryption process by the proposed structure. The same random number is inversed in the decryption process and mapped to the actual inverse S-Box. In AES, the functions of Non-Linearity are achieved by means of the Substitution Bytes and Add Round key steps. Here the design of a dynamic S-Box is highly secure. In the Non-linear implementation three S-Boxes is being used. The first S-Box is the default S-Box or linear S-Box. Each value in the default S-Box is converted to 2's complement and stored as 2's complement S-Box. After this, the default S-Box values and 2's complement S-Box undergo XOR operation and finally these values are stored as a virtual S-Box or Non-linear S-Box[10]. Since Non-Linearity is applied to the S-Box, the key is also protected. The key could not be known to the attackers due to the dynamic formulation of the S-Box. Thus it will provide an enhanced security.

During this encryption, the input value will be mapped to the virtually created S-Box and then this value will be mapped to the default S-Box to produce the encrypted result as shown in Fig. 6.

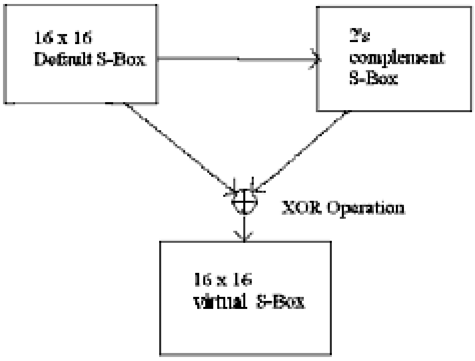

Fig. 5. Creation of dynamic S-Box

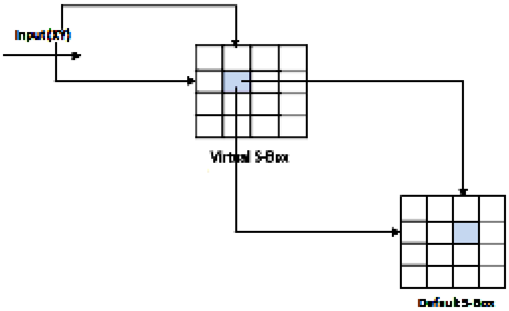

Fig. 6. Encryption using Virtual S-Box

During decryption, the input value will be mapped to the default S-Box and then this value will be mapped to the virtually created S-Box to produce the decrypted original result as shown in Fig. 7. The same creation of dynamic S-Box concept is used for the creation of 1's complement and hash value Non-linear S-Box also.

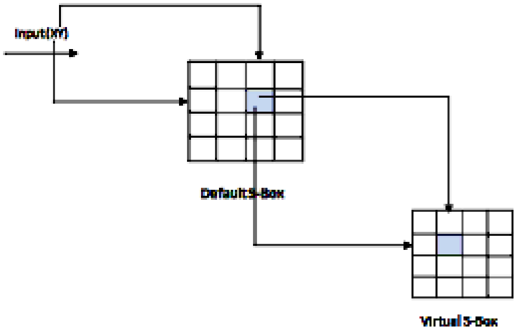

Fig. 7. Decryption using Virtual S-Box

RESULTS AND DISCUSSION

Simulation Analysis

In our Simulation Analysis, the sensor nodes are grouped based on the message id range and the number of nodes per cluster. The specific cluster group will be having unique characteristics associated with the cluster head, which is capable of receiving the multicast data from the corresponding sensor nodes. The locations of the static sensors are fixed in such a way that the cluster head is capable of receiving the encrypted data from each of its associated sensor node in a single-hop/multi-hop. Similarly all the cluster heads will be sending the encrypted data to the base station in a single-hop. The analysis of the flow of the data as follows.

a) A group of nodes has been formed as a cluster region.

b) Sensor node of a Cluster region selects a Random Data.

c) AES - CCMP was chosen for simulation that takes the private keys from the corresponding files and encrypts the data.

d) Encrypted data multicast to particular groups in the WSN.

f) Cluster head node received the data and decrypts the data with the assigned encryption mechanism.

f) If data received from malicious, it blocks the data in the cluster head itself.

g) The data from all the sensor nodes of its group will be collected in a similar manner and validated perfectly in the Cluster Head thereby blocking the malicious data being transferred to the base station.

h) Similar analogy is implemented at all the cluster heads with specification to its member nodes.

i) Separate Dynamic Key management is established for the different clusters. The private keys used for encrypting the data from the sensor nodes will be independent with respect to different clusters and unique within the cluster.

j) This mechanism of dynamic key management at the Cluster head is the efficient mechanism and the data traffic from the cluster head to the base station is optimized by the transmission of the valid data only from the nodes.

k) Separate encryption analysis is implemented at the Cluster head and the base station and the round keys for the encryption at the sensor nodes are generated from the Cluster head instead of base station.

l) This reduces the overhead of the base station and provides the facilitation of creating dynamic keys and the encryption standards at the cluster head itself.

Performance Evaluation

Based on the simulation environment, the data from the text database is transmitted to the base station from the sensor nodes through the cluster nodes. Individual encryption mechanisms using AES with CCMP is adopted. Also the malicious data included in the databank is successfully blocked in the cluster head. The performance analysis is carried out based on the following parameters: Packet delay, Data rate, Total number of packets received and packets lost. Table 1 shows the simulation parameter of the proposed system.

The figure 8 shows that the cluster formation and the data transmitted from the individual sensor nodes to the base station via the respective cluster heads.

Table 1. Simulation parameter

Parameter	Value
number of nodes (N)	50,100
Area	200 m × 200 m
Source location	175 m, 175 m
Sink location	20 m, 20 m
Pause time	300ms
constant bit rate	1 packet/s
packet frame size	30 bytes
Initial Energy	2 joules

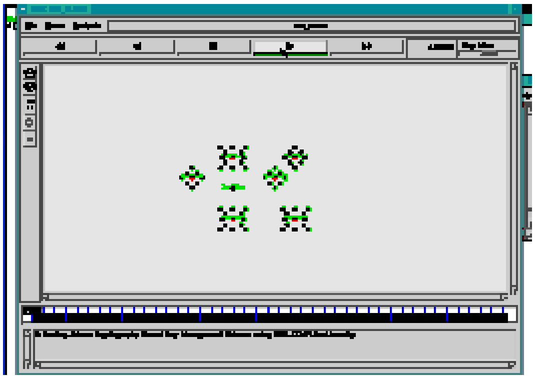

Fig. 8. Cluster Formation and Data Transmission

Fig. 9 shows comparative analysis of the number of packets transferred with respect to the Non- linear AES-CCMP algorithm and the number of packets transferred using linear AES-CCMP algorithm.

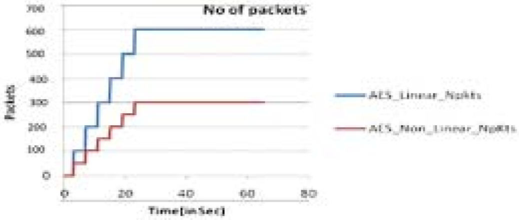

Fig. 9. Analysis of number of packets

Fig. 10 shows the performance analysis of successful transmission of packets between sender and receiver using parameter Packet transfer rate between the packets received with the linear AES-CCMP encryption and Non-linear AES-CCMP algorithm.

When comparing the performance analysis of number of packet transfer and the packet termination with the Non-liner AES-CCMP algorithm and without the AES-CCMP algorithm, much variation is not noted. The Fig.11 and Fig.12 shows that analysis of bit rate and packet delay.

It is understood that the performance of WSN is not degraded in any sort by the inclusion of the Non-linear AES-CCMP algorithm that provides secure data transfer between two nodes.

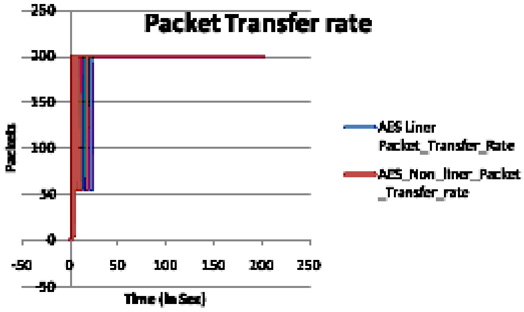

Fig. 10. Performance Analysis of Packet transfer rate

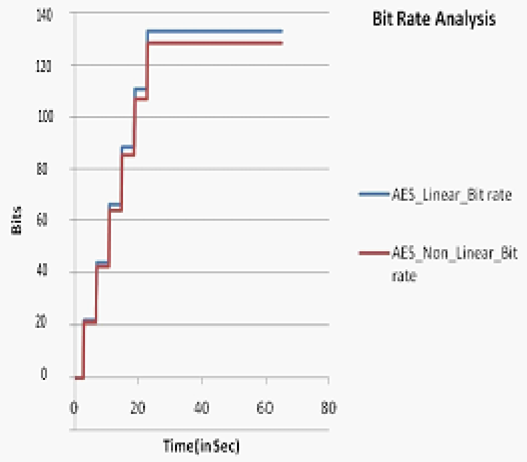

Fig. 11. Bit rate analysis

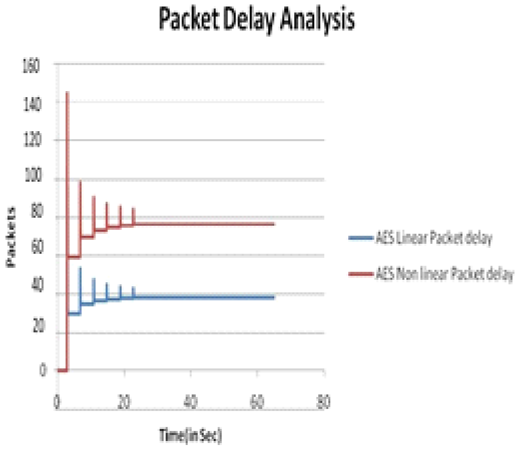

Fig. 12. Packet Delay analysis

CONCLUSION

In this paper, the environment has been simulated for the secured authenticated data transfer using the Non-linear AES with CCMP. The data transmission rate, performance and speed do not suffer in any form due to the inclusion of Non-linear S-Box and the result justifies that added authentication and integrity has been maintained. As the malicious data has been blocked in the cluster head itself by use of the AES-CCMP algorithm it does not spread across the heterogeneous sensor network. The various analysis show that the Non-linear S-Box scheme in AES with CCMP significantly reduces the communication overhead and increase successful data transmission ability with high security. The proposed methodology achieves both the security and data access control in dynamic nature using AES with CCMP encryption algorithm.

REFERENCES

1. Puccinelli, D., Haenggi, M., Wireless sensor networks: applications and challenges of ubiquitous sensing. *IEEE Circuits Syst Mag*., 2005; **5**(3);19–31.
2. Cui, S, Goldsmith, A.J., Bahai, A., Energy-constrained modulation optimization. *IEEE Trans Wireless Commun.*,2005;**4**(5);2349–60.
3. Heinzelman, W.R., Chandrakasan, A, Balakrishnan, H., Energy-efficient communication protocol for wireless microsensor networks. *In: Proceedings of the 33rd annual Hawaii International conference on system sciences. IEEE Computer Society*, 2000;10–20
4. Housley, R., National Institute of Standards and Technology (NIST), Advanced Encryption Standard, FIPS PUB 197; 2001;1-51.
5. Rachh, R.R. , Anami, B.S, Ananda Mohan, P.V. ,Efficient Implementations of S-Box and Inverse S-Box for AES algorithm” **,** *In:Proceeding of IEEE Region 10 Conference on TENCON*, Jan 23-26. , Singapore: IEEE.
6. Sivakumar, C., Velmurugan, A., High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11i), *Proceedings of International conference on ICSCN 2007*, MIT Campus, Anna University, Chennai, India. 2007; 398-403.
7. Chakib Alaoui, Taif., New Experimental Results for AES-CCMP Acceleration on Cyclone-II FPGA, *Int. J. Comp. Sci. Net. Secu*., 2010; **10**(4): 1-6
8. Razvi Doomun, M., Sunjiv Soyjaudah, K. M., Resource Saving AES-CCMP Design with Hybrid Counter Mode Block Chaining – MAC, *Int. J. Comp. Sci. Net. Secu*., 2008; **8**(10):1-13
9. Claude Carlet., Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and their Applications, *IEEE trans. Info. Theory.*, 2008; **54**(3): 1262 - 1272
10. Mozaffari-Kermani, M., Reyhani-Masoleh., Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard, *IEEE Trans. on Comp.*, 2010; **59**(5): 608 - 622
11. Daojing He., Jiajun Bu., Sencun Zhu., Sammy Chan., Chun Chen., Distributed Access Control with Privacy Support in Wireless Sensor Networks, IEEE trans. on wireless comm., 2011; **10**(10): 3472 - 3481.
12. Akashi Satoh., Sumio Morioka., Kohji Takano., Seiji Munetoh., A Compact Rijndael Hardware Architecture with S-Box Optimization, *Springer-Verlag Berlin Heidelber* , 2001;239–254.
13. *Sivaganesh, E., Velayutham, R., Manimegalai, D., A Secure Software Implementation of Non-linearAES S-Box with the Enhancement of Biometrics, Proceeding of* Inter. Conf. on Comp., Elect. and Electrical Tech.-ICCEET, 2012; 927-932.
14. Perrig, A., Stankovic, J., Wagner, D., Security in wireless sensor networks., *ACM Comm*.,2004; **47**(6): 53-57.
15. B. Schneier., Applied Cryptography: Protocols, Algorithms and Source Code in C, *John Wiley & Sons Inc*. 2nd Edition, 1996;
16. Menezes, A. J, Van Oorschot, P .C, Vanstone, S. A, Handbook of Applied Cryptography. CRC Press, 2001
17. Khambre ,P. D, Sambhare, S. S, Chavan, P. S., Secure Data in Wireless Sensor Network via AES (Advanced Encryption Standard), *Inter. J. Comp. Sci. Infor. Tech.*, 2012; **3**(2);3588-3592.