ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

# Transmission Security in WSN using AES Technique

Kavita Valmik Bodke[1], Dr. A.W.Kiwelekar[2]
M.Tech Student[1], Doctorate[2]
Department of Computer Engineering
Dr. Babasaheb Ambedkar Technological University, Lonere, India

**Abstract:**
Wireless sensor networks (WSN), which normally consist of hundreds or thousands of sensor nodes, each capable of sensing the information, processing information, and transmitting it over a sensor field through sensor node, or to detect and track certain objects in an area. Importance of sensor network is to provide information about sensing field for a period of time and security. We focus on securing wireless sensor network. In this paper, to maintain security we are using encryption algorithm like Advanced Encryption Standard (AES). AES provide suffcient level of security for protecting the confidentiality of data in wireless sensor network. The algorithm described by AES is a symmetric-key algorithm, means it used same key for encryption as well as decryption. We are using PRK technique for establishing pair wise keys in distributed sensor networks. Study shows that pair wise key establishment is a fundamental security services in sensor network. This enables sensor node to communicate securely with each other using cryptography technique.

**Keywords**: Wireless sensor networks (WSN), Advanced Encryption Standard (AES), Analog to Digital Converters (ADCs)

## I. INTRODUCTION

A wireless sensor network (WSN) consists of a thousands of tiny sensors, interconnected by a wireless communication network. Sensor data is shared between these sensor nodes and used to proper communication between them. Main objectives of sensor networks include reliability, accuracy, flexibility, cost effectiveness and ease of deployment. The sensor nodes are shown in Fig. 1.1. Each of these different sensor nodes has the capabilities to collect data and send data back to the sink. Data are send back to the sink as shown in Fig. 1.1 there is source and target node as mention the node 'A' is a targeted node and node 'E' is source node. Data can be route between the nodes A-B-C-D-E then send to the sink node. Then sink may communicate with the task manager node via Internet or satellite.

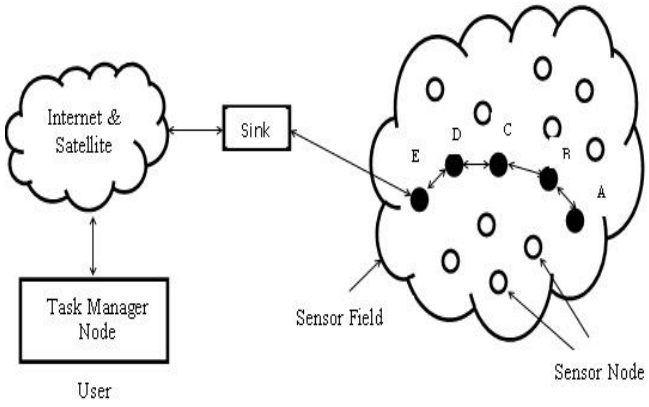


**Figure.1. Wireless Sensor Network Architecture**

In above diagram the sink node also use protocol stack which combines energy and routing information, combine data with networking protocols. All nodes in the sensor network act as information that can be collect from source, sensing and collecting data samples from their environment. Each node has one or more sensing unit. The main components of sensors consist of a sensing unit, a processing unit, a transceiver, and a power unit. There are also additional subunits, location finding system, mobilizer which shown in fig. 1.3.

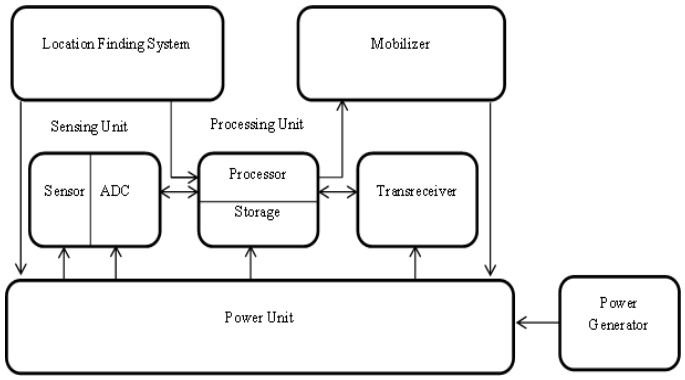


**Figure.2. Basic Components Of WSN**

(1) Sensing unit- Sensing units having two subunits: sensors and analog to digital converters (ADCs). ADCs convert analog signal to digital signal which comes from sensor and then give to the processing unit.

(2) Processing unit- Which having a small storage unit manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks.

(3) Transceiver unit- Connects the node to the network in given field.

(4) Power unit- Power units may be supported by a power scavenging unit such as solar cells.

(5) Location Finding System- Most of the sensor network routing techniques and sensing tasks require the knowledge of location. Thus, it is common that a sensor node has a location finding system.

(6) Mobilizer- A mobilizer may sometimes be needed to move sensor nodes when it is required to carry out the assigned tasks.

After all these basic requirement of wireless sensor network, there is lots of issue in wireless sensor network, in this report we are focusing on one of the main issue that is security in wireless sensor network. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes.

## II. RELATED WORK

Wireless sensor network is relatively new and very important research topic which is useful in education technology. Here we first discuss the few literature survey related to our project. The paper titled "Wireless Sensor Networks: A Profound Technology" by Namarta Kapoor, Nitin Bhatia, Sangeet Kumar, Simranjeet Kaur. In this paper they study about various application of wireless sensor network and it's routing protocol along with knowledge of simulators available for experimental work of wireless sensor network [1]. The paper titled "Wireless sensor networks: a survey " by I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci. In this paper they describe concept of sensor network, sensing task and sensor network applications. Several reviews were made on factors influencing the design of sensor network. They also describe the architecture of wireless sensor network algorithm and protocols. [2]. The paper titled "Wireless Sensor Networks Issues and Applications" by Rajkumar, Vani B A, KiranJadhav, Vidya S. In this paper they provide a survey of wireless sensor networks issues and application where the use of such sensor networks has been proposed. [3]. The paper title "Secure Communication in Wireless Sensor Network using Symmetric and Asymmetric hybrid Encryption Scheme" by Mrs. A.S. Bhave, Mr.S.R.Jajoo. In this paper their aimed to providing high security to wireless sensor networks using an improved AES-ECC hybrid encryption scheme [4]. The paper titled "A Review Study of Wireless Sensor Networks and Its Security" by Muhammad Umar Aftab, Omair Ashraf, Muhammad Irfan, Muhammad Majid, Amna Nisar, Muhammad Asif Habib. They find out an algorithm or mechanism that improves the performance and security issues of wireless sensor network and they also describe types of wireless sensor network [5]. The paper titled " Secure Wireless Sensor Networks: Problems and solutions" by Fei Hu, Jim Ziobro, Jason Tillett, Neeraj K. Sharma. They analyzed the security challenges in wireless sensor network and summarized key issues that should be solved for achieving the ad-hoc security and also they give the current solution for a specific wireless sensor network problem [6]. The paper titled " Don't fool me!: Detection, Characterisation and Diagnosis of Spoofed and Masked Events in Wireless Sensor Networks" by Vittoria P.llliano, Luis Munoz-Gonzalez and Emil C. Lupu. They provide simulation of different attacks and characterization of malicious nodes diagnosis technique and distinguish malicious data in wireless sensor networks [7]. The paper titled" Secure Data in Wireless Sensor Network via AES (Advanced Encryption Standard)" by P.D.Khambre, S.S.Sambhare, P.S.Chavan. They focus on security of wireless sensor network by AES encryption technique and also they analyses the performance of AES algorithm against attacks in wireless sensor network [8]. The paper titled " Establishing Pairwise Keys in Distribution sensor Networks" by Donggang Liu, Peng Ning. They present general framework for establishing pairwise keys between sensors. They also present a technique to reduce the computation at sensor required by their schemes [9]. The paper titled" AES Hardware-Software Co-Design in WSN" by Carlos Tadeo Ortega Otero, Jonathan Tse and RajitManohar. In this study they evaluate hardware, software, and hybrid implementation, including their one of design of Advanced Encryption Standard [1].

## III. PROPOSED WORK

On the basis of existing encryption technique, to maintain security in WSN we proposed encryption technique Advanced Encryption Standard (AES). The AES cipher is almost known to the block cipher Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. AES (Advanced Encryption Standard) with Rijndael (Symmetric Block Cipher) method used in 8-bit AVR Microcontroller for application in Military Sector and Field of Wireless Sensor Network AVR Microcontrollers are easy dynamic for programming as well as interfacing with other electronic modules and systems. AVR microcontroller is also used in Arduino (ATmega328) which is widely used in IoT (Internet of Things) however the paper can be implemented in same sector. In implementation of AES in Microcontroller we will create some custom instructions and Functions, which gives us easy recall of function in other function several times to save lines of coding as well as complexity. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. The number of internal rounds of the cipher is a function of the key length. Each intermediate cipher result is called a State. For ease of description, the block and cipher key are often represented as an array of columns where each array has 4 rows and each column represents a single byte (8 bits).

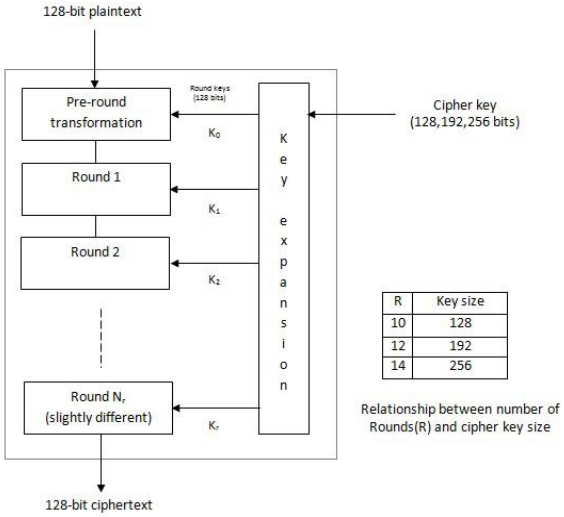


**Figure.3. Operation Of Aes**

The number of columns in an array representing the state or cipher key, then it can be calculated as the block or key length divided by 32 (32 bits = 4 bytes). An array representing a State will have Nb columns, where Nb values of 4, 6, and 8 correspond to a 128-, 192-, and 256-bit block, respectively. Similarly, an array representing a Cipher Key will have Nk columns, where Nk values of 4, 6, and 8 correspond to a 128-bit, 192-bit, and 256-bit key, respectively which shown in fig. 4.1 and encryption process shown in fig. 4.2.[4]

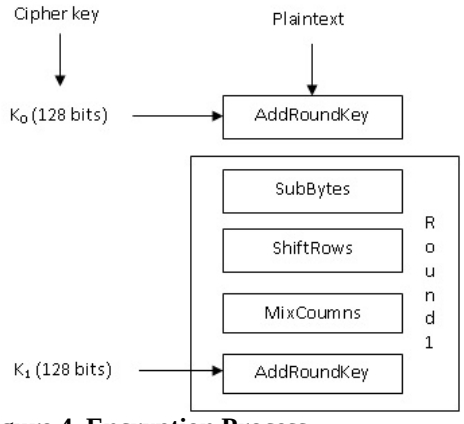


**Figure.4. Encryption Process**

## IV. METHODOLOGY AND IMPLEMENTATION

In WSN to maintain security we are using AES encryption technique which mention in above section the methodology we are using, for Encryption Round, Decryption Round, Each processing round involves four steps:-

**Step 1:- Message**

A 4*4 matrix is considered as the Plain text for transmission. For example plaintext is, Two One Nine Two (16 ASCII characters, 1byte each). Then convert into Hex i.e. 54776F204F6E65204E696E652054776F. Then generate 4*4 matrix is,

Plaintext

$$\begin{bmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{bmatrix}$$

**Step 2 - Key Expansion**

As plain text is a 4*4 matrix, key is 16 byte or 128 bits for round 10, 192 bits for round 12, and 256 bits for round 14. For example key is, Thats my Kung Fu (16 ASCII characters, 1byte each). Then converted into Hex i.e. 5468617473206D 79204B756E67204675. Then generate 4*4 matrix is,

Round 0 key

$$\begin{bmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{bmatrix}$$

**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 matrix. For example adding plain text and round 0 key we get new matrix,

Plaintext + Round 0 key = New Matrix

$$\begin{bmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{bmatrix} + \begin{bmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{bmatrix} = \begin{bmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{bmatrix}$$

**Step 4 – Sub Bytes ()**

Simply S-box convert the value which given byte in State S is given a new value in State S'. According to the S-box as an example, input State byte value of 01 will be replaced with a 7C in S-box value. For example the first byte of plaintext in above example is 00 which is replace by 63 means the $0^{th}$ row and $0^{th}$ column of S-box element. From above example leads to new state matrix which shown below,

$$\begin{bmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{bmatrix}$$

**Step 5 - Shift Rows ()**

The shift rows transformation cyclically shifts the bytes in the last three rows of the State array. In more general, rows 2, 3, and 4 are cyclically left-shifted by C1, C2, and C3 bytes. For example from above new matrix the value of $2^{nd}$ row of C0 get shifted by one position to the left then we get new matrix,

$$\begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix}$$

**Step 6 -Mix Columns ()**

The mixColumn transformation uses a mathematical function to transform the values of a given column within a State, acting on the four values at one time as if they represented a four-term polynomial. From above new matrix we get new matrix after apply mix column function,

$$\begin{bmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{bmatrix}$$

## V. CONCLUSION AND FUTURE SCOPE

Wireless sensor networks are large collection of tiny nodes that sense surrounding environment and communicate each other via wireless link. In this project we propose security of wireless sensor network. For the security we propose encryption algorithm like AES .AES provide sufficient level of security for protecting confidentiality of data in WSN. AES can be implementing on various platforms. In this project with AES we are using PRK technique for establishing pairwise keys in distributed sensor networks. In future work for securing WSN we are using encryption technique AES with PRK algorithm for pairwise key distribution which is counter part of our project.

## VI. REFERENCES

[1]. Wireless Sensor Networks: A Profound Technology. Namarta Kapoor, Nitin Bhatia, Sangeet Kumar, Simranjeet Kaur, Dept. of Computer Science, DAV College, Jalandhar, Punjab, India Lovely Professional University, Phagwara, Jalandhar, Punjab, India.

[2]. Wireless sensor networks: a survey , I.F. Akyildiz, W. Su*, Y. Sankara subramania m, E. Cayirci, Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology,

Atlanta, GA 30332, USA Received 12 December 2001; accepted 20 December 2001.

[3]. Wireless Sensor Networks Issues and Applications. Rajkumar, Vani B A, Kiran Jadhav, Vidya S. Sambhram Institute of Technology , Bangalore, Karnataka, India.

[4]. Secure Data in Wireless Sensor Network via AES (Advanced Encryption Standard). P.D. Khambre 1,S.S.Sambhare[2],P.S. Chavan[1] 1 BVUCOE, Pune 2 PCCOE, Pune.

[5]. Secure Communication in Wireless Sensor Network using Symmetric and Asymmetric hybrid Encryption Scheme. Mrs. A.S. Bhave[1], Mr.S.R.Jajoo[2]. Department of Electronics, Mumbai University, Datta Meghe College of Engineering, Airoli, Navi Mumbai, Maharashtra, India.

[6]. Establishing Pairwise Keys in Distribution sensor Networks, Donggang Liu, Peng Ning.

[7].AES Hardware-Software Co-Design in WSN, Carlos Tadeo Ortega Otero, Jonathan Tse and Rajit Manohar, 2015 21st IEEE International Symposium on Asynchronous Circuits and Systems.

[8]. A Survey on Various Cryptography Techniques, by Mitali, Vijay Kumar and Arvind Sharma.