Energy Optimization In Wireless Sensor Network Using Different Compression And Encrytion Techniques

Rakesh V

M.tech, Electronic and Communication
M.S.Ramiah Institute of Technology

Bengaluru, India

Rakeshvemu27@gmail.com

Sarala S M

Assistant Professor, Electronic and Communication

M.S.Ramiah Institute of Technology

Bengaluru, India

Saralasm@msrit.edu

Abstract- Wireless sensor networks(WSN) has been increased day by day to measure and monitor physical characteristics. It can implemented in the area where human cannot be reached. Each sensor node depends on power to do their activities. As the WSN has limited battery life time it's important to optimize power. There are many methods to optimize power in WSN. Here compression and encryption techniques are used for optimizing power in WSN. Here optimization means reducing the amount of energy consumption. If the input data is large then automatically the transmitters and receivers will take more amount of energy. So here by reducing the data size by compression and by sending an encrypted version of the compressed data, we are making the antennas to transmit and receive less amount of data than the actual data and also it will be more secured. At the receiving end by applying the decryption and reconstruction of the compressed data , we are able to recover the complete data. Then we will compare how much energy is optimized by different compression and encryption techniques.

Keywords – Sensor node, optimize, compression, encryption, battery, energy consumption

I. Introduction

Wireless sensor network (WSN) is most often set up in an ad-hoc mode by means of cheap small computational nodes distributed densely over a significant area. They consist of small power nodes with sensing, computational and wireless communicational capabilities that can be deployed deterministically or randomly over an area where the users wish to collect data. Typically, wireless sensor networks contain hundreds or thousands of identical sensor nodes. These sensor nodes have the ability to communicate with each other or directly to a base station. These sensor networks are highly distributed and the nodes are lightweight. A greater number of sensors will enable sensing over a large area. As the manufacturing of small of small, low cost sensors has been increasing technically and economically feasible, a large number of these networks can be networked to operate for variety of applications like military applications, disaster management, habitat monitoring, health monitoring, and home applications.

With the advent of ad hoc networks they can be distributed in remote site environments, so there is a focus on increasing the lifetime of sensor nodes though power transmission, power conservation and power management. Wireless sensor networks faces the problem of energy constraints in terms of limited battery life time. Each node depends on energy for its activities. Failure one node can interrupt the entire system. So it is important to optimize energy. Energy optimization is the goal to reduce amount of energy required to provide for products and services. There are various approaches to improve energy efficiency. Reducing energy use reduced energy costs and may result in a financial cost saving to customers if the energy savings offset any additional costs of implementing an energy efficient technology.

In order to expand the working time of individual devices, it is frequent practice that some nodes will be deactivated, including radio transceiver. They remain in inactive state for the most of time and activated only to transmit or receive data from other nodes. Radio transceiver can operate in one out of three modes, which differ in the consumption of power necessary for proper operation: Active state-consumes more energy when transmitting or receiving, Idle state- consumes less energy, it is turned on and ready to change to data transmission or receiving, Sleep state- nodes shut down the radio to save energy. Steps can be taken to save energy are to schedule the state of nodes (active, idle, sleep), changing transmission range between nodes, using efficient routing and data collecting methods and avoiding the handling of unwanted data as in the case of over heading.

General block diagram of wireless sensor network is as shown below:

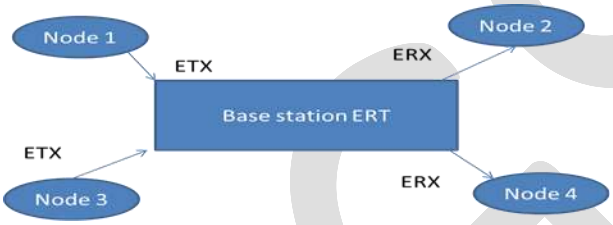

Figure 1: General block diagram of wireless sensor network

The above diagram consists of a wireless sensor networks consists of four nodes and one base station. These nodes are placed at different geographical locations. These nodes send data to base station and in turn also receive data from base station. Here base station is nothing but a router. When a wireless sensor network transmits a data to the base station or when a wireless sensor network receives a data from energy is utilized for accomplishing this task. Similarly energy is utilized by the base station to route the data. Suppose Node1 transmits the data to base station and let the energy utilized is ETX and Node2 receives the data from base station and the energy utilized is ERX. Similarly energy is also required by the base station to route the data and energy required for this purpose be ERT. Therefore total energy for overall process is the sum of all energies

T= ETX+ERT+ERX

Where T is total energy for overall task and ETX, ERT, ERX are the transmission energy, routing energy and receiving energy respectively.

The methods in which energy savings can be done are classified into two heads [1]:

Device level: Hardware component selection and their configuration to achieve low energy consumption in a wireless sensor node.

Network level: Choice of communication methods and protocols to minimize energy consumption.

In a sensor node there are four essential parts: processing unit, sensing unit, transceiver unit and power unit. Processing unit is a part of microcontroller unit which can read sensor data, perform some minimal computations and make a packet ready to transfer in wireless communication channel. In reality sensor unit is the medium for communicate between physical world and the conceptual world of processing unit. The senor unit is one of the vital part of wireless sensor mode, it sense and detect the physical state of environment and sends the data to processor. Processor manipulates data and decides where it has to promote or else transmit the data to base station. Sensor coverts energy forms one form to another form. In reality sensor act as the transducer where energy is converted into analog or digital. Sensor can be distinguished based on what kind of energy they detect or transfer to the system. A wireless sensor node can be built with different type of sensor, and different types of sensor use different amount of energy.

II. Methodology

In wireless sensor network the target is to optimize energy for transmission, routing and receiving of data. Here by using combination of various encryption and compression techniques energy can be optimized. If the input data is large nodes takes more energy to transmit, so by reducing data size by compression techniques the transmitter consumes less energy and by encrypting the data network would be more secured.

In the proposed methodology, during transmission data is first encrypted and compressed using combination of various encryption and compression algorithms and at the receiver end reverse process is applied. The flow chart of the proposed methodology is shown below:

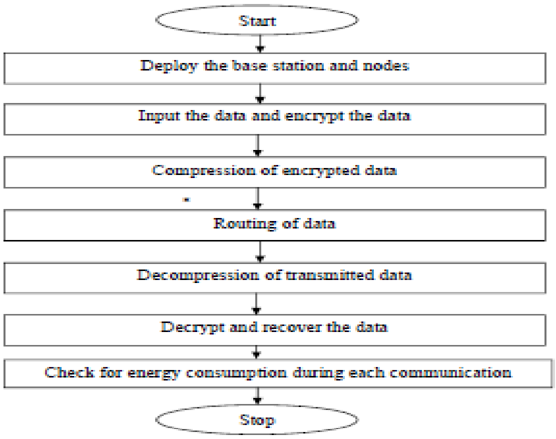
Start
Deploy the base station and nodes
Input the data and encrypt the data
Compression of encrypted data
Routing of data
Decompression of transmitted data
Decrypt and recover the data
Check for energy consumption during each communication
Stop

Figure 2: Flow chart of proposed methodology

III. Encryption Schemes Applied To Wireless Sensor Networks

In this approach the focus in on the energy efficiency of secure communication in wireless sensor networks. The encryption algorithms used are AES (Advanced encryption standard) and neural network based encryption/decryption. The input data used is image.

A. AES

AES is a symmetric block cipher where same key is used for both encryption and decryption. This standard specifies Rijnedael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192 and 256 bits. Here it consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical [12]. AES encryption algorithm is shown below:

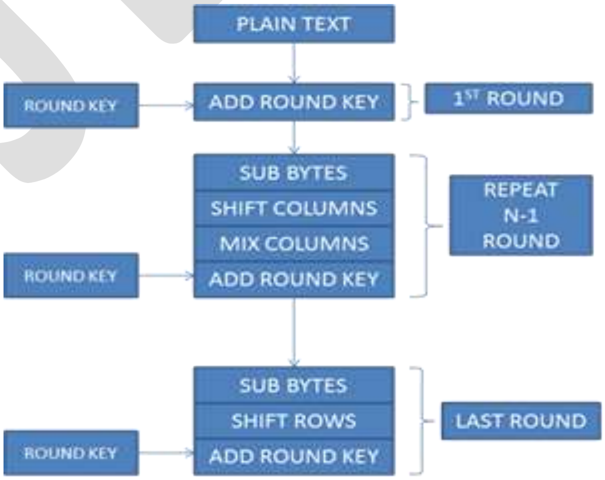

Figure 3: AES encryption algorithm

The input of AES algorithm is converted into 4*4 array, called state. Four transformations are performed for various operations on the state to calculate the output state. The transformations are add round key, sub bytes, shift rows and mix columns. Except for add round key each of these operations is invertible.

Sub bytes Transformation: This transformation is a non-linear byte substitution that operates independently on each byte of the state using a substitution table called S-box. This S-box is invertible. The S-box used in the sub bytes transformation is presented in hexadecimal form.

Shift Row Transformation: In this transformation, the bytes in the last three rows of the state are automatically shifted over a different number of states. The first row is not shifted. Second row is shifted left once, third row twice and last two three times it is shifted

Mix Columns Transformation: The mix columns transformation operates the state column by column, treating each column as a four term polynomial. The columns are considered as polynomials over GF (2^8) and multiplied modulo of x^4 +1 with a fixed polynomial a(x), given by a(x) = {3} x^3+ {1} x^2+ {1} x+ {2}. This can be written as multiplication matrix $s'(x)$ = a(x) * s(x).

Add round key Transformation: In add round key transformation, a round key is added to the state by a simple bitwise XOR operation.

Key Expansion: The AES algorithm takes the cipher key and performs key expansion to generate a key schedule. The key expansion generates a total of Nb (block length i.e. 4) * (Nr (total number of rounds i.e. 10) +1) words. The algorithm requires an initial set of Nb words and each of the Nr rounds require Nb words of key data. The resulting key schedule consists of an array of 4-byte words, denoted [w_i], where i is in the range of $0 \leq i \leq$ Nb (Nr + 1).

The expansion of the input key schedule proceeds according to pseudo code. It can be seen that for words in position that are multiple of Nk (length of expanded key), a transformation is applied to w[i- 1] prior to XOR , followed by a round constant which contains the values given by [x^{i-1},{00},{00},{00}], with x^{i-1} being powers of x (x is denoted as {02}) in the field GF(2^8). Then consists of a cyclic shift of bytes in a word, followed by substitution using S-box. Then every following word, w [i], is equal to the XOR of previous word, w [i-1], and the word Nk position earlier, w [i-Nk].

B. Neural Network Based Encryption and Decryption

As the encryption standards such as AES, DES, RSA has been increased so neural network is another approach of encryption. Neural network plays important role in information security. Most of the algorithms used are generic, because of which the key exchange has become has prerequisite prior to data exchange [11]. Hence the strength of such encryption lies on the key length. In this encryption process it uses random substitution, and impurity addition creating more confusion to misguide the cryptanalyst. At receiving end, it uses artificial neural network to obtain the original data.

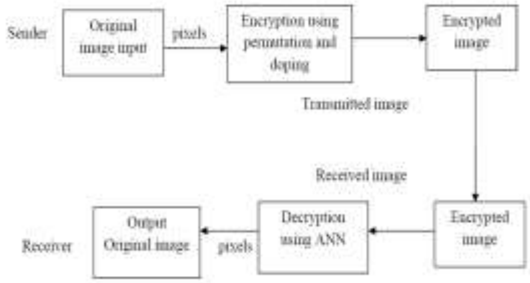

Figure 4: Block diagram of image transmission and reception

Artificial neural network: In general it is a highly interconnected, parallel distributed processing network with a large number of processing elements neurons. Each neuron is connected to other neurons by means of communication links each with associated weight. Typically, a neuron sends its activation as a signal to several other neurons. There are several architectures in which neurons can be connected. In this multilayer feedforward networks with backpropagation learning algorithm are used. It is made up of multiple layers. Architecture of this class consists of input and output layer also have one or more intermediate layers called hidden layers.

Here the neurons of one layer are connected to neurons of next layer and so on still the output layer. The hidden layer helps in performing useful intermediary computations before directing the input to the output. The training of a network by backpropagation involves three stages: the feed forward of input training pattern, the calculation and back propagation of associated error, and the adjustment of the weights. As the process converges, the final weights are stored in a file. After training, application of the network involves only the computations of the feedforward phase.

Encryption module: The image to be encrypted is read pixel by pixel and the transformation is done on these pixels using permutation, substitution, and impurity addition. Two levels of encryption are done to obtain high level encryption. The algorithm shown below does the necessary transformation.

Algorithm

First level encryption

Step 1: Get the pixel value of image file, [66] [01000010].

Step 2: Divide the pixel bytes into two parts (nibbles), [0100 0010].

Step3: Exchange the nibbles and concatenate to form byte, [00100100]

Step4: Calculate the impurity by XORing the original msb nibble and lsb nibble, [0110].

Step5: Shift the bits of impurity by 5 bits to the right [011000000] and EXOR with the step 3

[011100100] = [228].

Step6: Add impurity to the result obtained in step 5. The impurity chosen is 117

[117+228] = 345.

Step7: Continue step1 to step6 for all the pixels of image.

Addition of two columns:

Step8: Additional two columns are added and the value of 117 is added to first column and 627 to the second new column.

Second level encryption:

Step10: Add another level impurity to the resultant matrix obtained in step 8 such that impurity changes with respect to the position of the pixel

It is done in two levels because in the first level encryption all the pixels with same original value will have the same encrypted value and due to this intensity changes but the picture can be still visible. To overcome this second level encryption is done. During this impurity changes according to pixel position that means the pixel with same original value will have two different values after second level encryption.

Decryption module: At receiving end, decryption is achieved using an artificial neural network. The neural network is trained for standard mapping values and the weights are stored before applying input to it. The system is designed for three input layers- input, output and the hidden layer. The input and output layer has only one neuron, and the hidden layer has 695 neurons. Large numbers of neurons are essential for achieving high accuracy. The decryption process is achieved in three steps. During first stage, the impurity which was varying with respect to pixel is removed. In the second stage, the additional columns from the matrix which were added during encryption is deleted. During the third stage, the received image data and weights which are stored after training are used to simulate the network. The output of this stage is the recovered image.

IV. Compression Techniques Applied in Wireless Sensor Network

After encryption the following compression techniques are applied to the input. Compression means reducing the size if data so that it can save space while storing data and consume less energy while transmitting. There are two types of compression lossless compression and lossy compression. Lossless compression involve no loss of information. If data have been losslessly compressed, the original data can be recovered exactly from the compressed data. Lossy compression involves some loss of information. The data that have been compressed generally cannot be recovered or reconstructed exactly. Here lossless compression techniques and lossy compression is used. The lossless compression used is Huffman coding and Arithmetic coding.

I. Huffman Coding:

It is a lossless compression developed by David Huffman. It is an entropy encoding algorithm which uses variable length code table for encoding a source symbol. The variable length code has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol. It uses a specific method for choosing presentation for each symbol, resulting in prefix code. The Huffman coding can be constructed on two ideas: In an optimum code, the symbols that occur more frequently should have shorter codewords and the two symbols that occur least frequently will have same length.

II. Arithmetic coding:

It is a lossless compression based on the interval subdividing. In arithmetic coding source ensemble is represented by an interval between 0 and 1 on the real number line. Each symbol of the ensemble narrows this interval. As the interval becomes smaller, the number of bits needed to specify it grows. It assumes an explicit probabilistic model of the source. It uses the probabilities of the source messages to successively narrow the interval used to represent the interval less than low probability messages contribute fewer bits to the encoded ensemble.

III. Lossy Compression:

In a lossy compression the following steps are carried out. The first is that performs transform coding for the input data. The transform is done using discrete wavelet transform. It separates the high and low-frequency portions of a signal through the use of filters. Signal is passed through high & low pass filters and down sample by a factor of two. Multiple levels (scales) are made by repeating the filtering and decimation process on lowpass outputs. DWT is computed with a cascade of filtering followed by a factor 2 sub-sampling. The 2-D DWT is computed by successive low-pass and high-pass filtering of the image. By applying 2D DWT on an image, the image is decomposed into four subband LL, LH, HL, HH subband, corresponding to approximate, horizontal, vertical, and diagonal features respectively. The subband denoted by LL is approximately at half the original image. While the subband HL and LH contains the changes of images or edges along vertical and horizontal directions, respectively. The subband HH contains the detail in the high frequency of the image. LL subband is further decomposed into four subband. But as the level of decomposition is increased, there is a loss of resolution in the newly created subband. The first level of decomposition extracts finest resolution of details, the subband created in the second level of decomposition extract coarser details than the first one. Here Haar wavelet is used as it provides a simple and computationally efficient approach for analyzing the local aspects of a signal. Then next step is quantization, it converts a sequence of floating numbers to a sequence of integers. The simplest form is to round to the nearest integer. Another method is to multiply each number in by a constant k, and then round to the nearest integer. Next is entropy encoding here arithmetic encoding is used.

V. Routing and Energy Model

After compression the next step is routing of data it is done by LEACH (Low energy adaptive clustering hierarchy) protocol. It is a cluster cased routing protocol, which uses distributed cluster formation. LEACH randomly selects the cluster head based on the energy of the sensor node [5]. This is to form the sensor node based on the received signal strength and use cluster head as the routers to the base station. In LEACH, the cluster head gets the compressed data from the input sensor nodes. From cluster head it is passed to the base station. From base station it is transmitted to the other cluster head and then to the receiving node.

After routing of data the next important step is to calculate energy for transmission of data. Here we use first order radio model for wireless sensor networks. Here we have taken some assumptions for these networks. All sensors are within the wireless communication range when they communicate with each other or with the base station. Sensors should have homogeneous sensing, computing and communication capabilities. Base station is located in the center of the sensor networks and it has infinity energy. Thus, to transmit a k-bit message a distance d, the energy consumed is:

$$E_{tx}\,(k,d)= k*E_{elect}+k*E_{amp}*d^2$$

Where E_{tx} is energy consumed for transmission, $E_{elect\ is}$ transmission and receiving energy and E_{amp} is amplifier energy.

After calculation of energy we compare the energy consumed by different combination of encryption and compression techniques.

Some of the considerations for calculating energy are as shown below:

Parameter	Value
Initial energy of each node	5 J
Transmission and Receiving energy (E_{elect})	50n J/bit
Amplifier energy ($E_{amp)}$	0.0013pJ/bit/m^2
Type of distribution	Random
Energy level for node to be alive	0.009 J

Table 1: Energy model consideration for LEACH

IV. Results and Discussions

As mentioned earlier, before transmission of data to the networks it is encrypted using AES encryption and neural network based encryption/decryption and then using different compression techniques it is compressed. And then routing of data is done by LEACH protocol. Then energy is calculated for each combination and compared.

A. AES encryption results

The results of encryption and decryption are shown in below figure 4.1. The original size of image is 256*256*8. After encryption also it remains in same size so encryption here is just for security purpose.

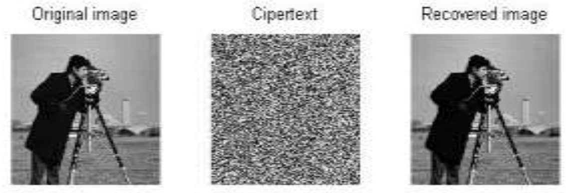

Figure 5: AES encryption and decryption

B. Neural network based encryption

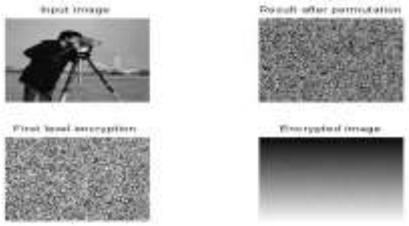

Figure 6: Output of Encryption

The encryption is done in two levels and decryption is done by using neural network

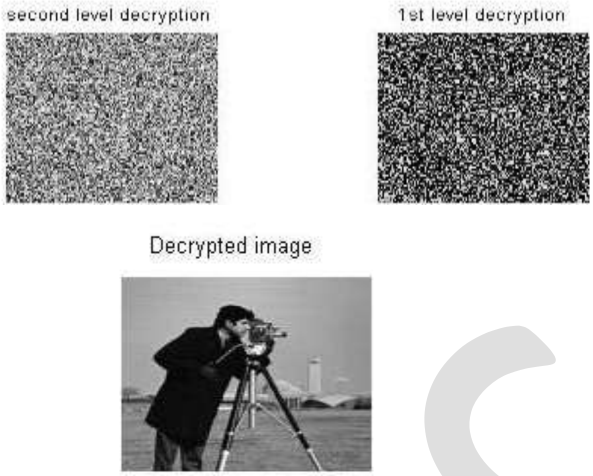

Figure 7: Output of Decryption

Energy consumed after encryption and compression results

Original Size of image	Transmission energy before compression	Energy consumed after Huffman compression	Energy consumed after arithmetic coding	Energy consumed after lossy compression
524288 bits	0.026739 J	0.023546 J	0.023430 J	0.00983 J

Table 2: Energy consumed by different compression techniques after encryption.

As we can see the above table the energy required for wireless sensor node to transmit the data for single time. After encryption the image size remains same. The energy consumption mainly depends on the size of data and distance between the nodes. As the data size is decreased the energy consumed will be less for wireless sensor network. For lossless compression the energy required is more but for lossy compressed data the energy required is less. The figure 8 gives the clear information about how many nodes are alive for how many rounds of communication.

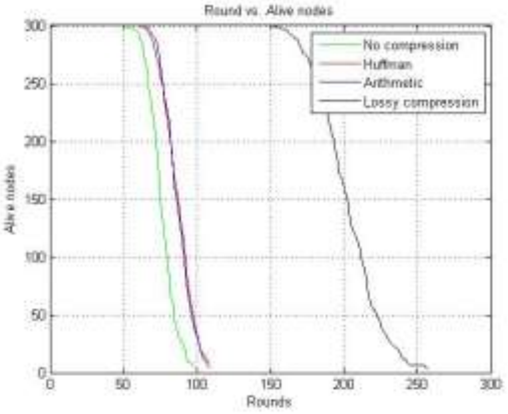

Figure 8: Number of rounds vs. number of alive nodes

V. Conclusion and Future work

In this project encryption is done so that the data will be more secured and to optimize energy various compression techniques and LEACH protocol has been applied. Here both lossless and lossy compression is done. We can see that more number of nodes is alive when the data is compressed. By these methods we can increase the life time of sensor nodes in wireless sensor network. There are many more issues to be resolved around energy management. By solving those we can reduce energy consumption of sensor nodes in wireless sensor networks. Particularly in the design of energy efficient protocol and its implementation has a significant scope.

REFERENCES:

[1]. Alba P.Sawlikar, Dr.Z.J.Khan & Dr.S.G.Akojwar “Power Optimization of Wireless Sensor Networks using Encryption and Compression Techniques” 2014 IEEE DOI 10.1109/ICESC.2014.43

[2]. C. M. Chao and Y. C. Chang “A power-efficient timing synchronization protocol for wireless sensor networks” Proc. Journal of Information Science and Engineering, pages 985-997.

[3]. IlkerDemirkol, CemErsoy, and FatihAlagöz, Bogazici University, “MAC Protocols For Wireless Networks: A Survey” IEEE Communications Magazine April 2006.

[4]. Kemal Akkaya and Mohamed Younis, “A Survey on Routing Protocols for Wireless Sensor Networks”, Ad hoc Networks, vol. 3, no. 3, May 2005, pp. 325-349.

[5]. Rajashree.V.Biradar , S. R. Sawant , R. R. Mudholkar , V.C .Patil “Inter-Intra Cluster Multihop-LEACH Routing InSelf-Organizing Wireless Sensor Networks”, International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 1, March 2011

[6]. R. Ramanathan and R. Rosales-Hain, “Topology Control of Multihop Wireless Networks Using Transmission Power Adjustment,” IEEE INFOCOM, 2000

[7]. J. M. Hellerstein and W. Wang, “Optimization of in-network data reduction,” in DMSN Proceeedings of the 1st international workshop on Data management for sensor networks. NewYork, USA:ACM,2004, pp.40–47.

[8]. Energy-Efficient Data Acquisition in Wireless Sensor Networks Using Compressed Sensing” IEEE Conference, Date: 29-31 March 2011.

[9]. C.Karthik Sendhil Kumar, R.Sukumar and M.Nageswari “Sensors Lifetime Enhancement Techniques in Wireless Sensor Networks - A Critical Review”International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 3, No.2, April 2013.

[10]. Oldewurtel, Frank and Mahonen, Petri, (2006) “Neural Wireless Sensor Networks”, International Conference on Systems and Networks Communications, ICSNC '06, pp.28

[11]. Saraswathi.D.Joshi,V.R.Udupi & D.R.Joshi “A Image Encryption Decryption Using Advanced Encryption Standard” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) ISSN 2278- 6856 volume 3, Issue 3, May – June 2014

[12]. Y. Wang, G. Attebury, and B. Ramamurthy “A Survey of Security Issues in Wireless Sensor Networks” IEEE Communications Surveys & Tutorials, vol.8, no.2, pp. 2-23, 2006

[13]. Swati G Mavinkattimath and N S Sirdeshpande “Design and Implementation of a Private and Public Key Crypto Processor” IJEETC Vol. 2, No. 4, October 2013.

[14]. Neda Enami, Reza Askari Moghadam, Kourosh Dadashtabar & Mojtaba Hoseini “Neural Network Based Energy Efficiency In Wireless Sensor Networks: A Survey” IJCSES Vol.1, No.1, August 2010.

[15]. J S Rauthan and S Mishra “An improved Cluster Based Multi-hop Routing in Self- Organizing Wireless Sensor Networks” International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 4, June – 2012