Enhancing Data Transmission and Protection in Wireless Sensor Node

Prajwali wamanrao Gawande[1], Prof. Vijay Bagdi[2]

[1]Department of Computer Science and Engineering Abha Gaikwad Pati College of Engineering Nagpur, Maharashtra, India
[2]Department of Computer Science and Engineering Abha Gaikwad Pati College of Engineering Nagpur, Maharashtra, India

---***---

Abstract - *In order to discover physical or environmental conditions, such as sound, temperature, pressure, etc. and to send their data through the network to the main location, a wireless sensor network (WSN) is used since it has many independent sensors. With the management requests and responses and the data issuing from the network's actual sensing application additional traffic is created. By sending and processing the data together the system's energy can be reduced, instead of performing the operations individually. The primary objectives of the routing protocol which is designed in wireless sensor network are energy consumption, balancing the network and extending the network's lifetime.*

In this paper, we have also proposed the technique for increasing the efficiency of a node as well as providing security to the data and we have also discussed the problems of transmitting data over wireless sensor network

Key Words: *Wireless Sensor network, Nodes, LEACH, Clustering, cluster-head, RC-6*

1. INTRODUCTION

A self-organized network composed by a large number of micro sensors that are randomly deployed in monitoring region through wireless communication is known as Wireless sensor network [1]. Energy-efficient mechanism is important because each sensor node in wireless sensor network has a constraint energy capacity. In wireless sensor network, the highest priority should be given to sending packets from the source node to the destination node rather than sensing an event. A typical node (Berkeley node) have a configuration of 8-bit CPU (4MHz),128KB flash,4KB RAM and Transmission range of 100 Feets [3].

In WSN the nodes are made up of electronic devices that which can sense, compute and transmit data from physical environments. Limited energy resources have been comprised by these sensor nodes. To extend the lifetime of network, energy resources for wireless sensor networks should be managed wisely. Transmitting data over the WSN securely is the another problem in WSN.

1.1 Efficiency of node:-

Energy wastage, in wireless communications shortens the network lifetime. Major reasons of energy wastage are as follows

- **Idle listening: -** Idle listening happens when the radio is listening to the channel to receive the possible data which is not sent.
- **Collisions**: - Collision occurs when two nodes transmit at the same time and interfere with each other.
- **Control:-**Control deals with packet overhead for protocols to exchange required information.
- **Overhearing: -** Overhearing occurs when a sensor node receives packets that are not destined to it. This is the dominant factor of energy wastage, when traffic load is heavy and node density is high.

This paper is organized as follows detailed description on Leach protocol is given in Section 2 gives, Section 3 gives the improvement in leach protocol in order to increase the efficiency of node, Section 4 gives the algorithm used to retain security, Section 5 gives the output obtained by using leach protocol and RC-6, Section 6 gives the comparison of data transfer over WSN using proposed method and existing method, Section 7 discusses the conclusion.

2. LEACH PROTOCOL

2.1 Protocol Description

In WSN, LEACH is the earliest proposed single-hop clustering routing protocol. It can save network energy greatly compared with the non-cluster routing algorithm. Many other clustering algorithm are proposed based on LEACH, such as TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol) [4] PEGASIS (Power Efficient Gathering in Sensor Information Systems) [5] HEED (Hybrid Energy-Efficient Distributed Clustering) [6] and so on. All clusters are self-organized in LEACH protocol; each cluster contains several non-cluster head nodes and a cluster-head. The cluster-head node consumes more energy than non-cluster head nodes. In order to balance network energy consumption and prolong the network life cycle, it selects cluster head randomly and each node has an equal chance to be the cluster-head [7]. The cluster structure update constantly in operation and one updating process is called a Round. The cycle of each round contains two stages: set-up phase and steady-state phase, set-up phase is the establishment phase of the cluster whereas steady-state phase is the stable data transfer phase. In Set-up phase, each node generates a random number from 0 to 1, and compares this number with the threshold value $T(n)$. If the number is less than $T(n)$, the no of node is selected as a cluster-head; the threshold $T(n)$ i set in the following manner: - s

$$T(n) = \begin{cases} \dfrac{p}{1 - p * (r \bmod \frac{1}{p})} & if\ n \in G \\ 0 & if\ n \notin G \end{cases}$$

Where *n* refers the identification of node in the current sensor network; *p* is the percentage of cluster-heads; *r* is the current round number; *G* is the set of nodes that have not been elected as cluster-head in the last *1/p* rounds.

Once the cluster-head is calculated, the cluster-head sends a broadcast message to the network and declares itself as the cluster-head. Each normal node decides which cluster to join in according to the signal strength of the received message and then sends a request message to the corresponding cluster-head.

The cluster-head receives all the messages which are sent by the nodes that are willing to join in the cluster. LEACH protocol has a relatively better function in energy consumption through dynamic clustering, keeping the data transmission in cluster which reduces the energy consumption through communicating directly between nodes and the base station, but there are still a lot of inadequacies.

The mechanism of cluster-head rotation is used in LEACH protocol. The cluster-head is elected randomly. After multiple rounds of data transmission, the residual energy of the nodes will have a great difference. The nodes or the cluster-head which are far from the base station will consume more energy in transmitting the data of the same length relatively. After that, if they are selected as cluster-heads, they will run out of energy and become invalid. As the number of invalid nodes increases, it'll have a great influence in the network performance and reduce the life of the network. On the basis of received signal intensity to join, Cluster member nodes selects the optimal cluster-head. Neither consider the distance from the node itself to the base station nor the distance between cluster-head and the base station. So normal node may choose the cluster-head that is far from base station as its optimal cluster-head, this not only is the heavy burden to the cluster-head but also increases the extra energy consumption, which is not beneficial to balance network energy consumption.

3. IMPROVEMENT OF THE LEACH PROTOCOL

This paper considers node energy and position information to improve the LEACH algorithm, energy balanced clustering algorithm named 2Head-LEACH algorithm to improve the energy of the node is proposed here.

Cluster-head Selection

Based on residual energy, there are many improved methods of the cluster-head selection the threshold equation in [2] is as follows

$$T(n) = \frac{p}{1 - p * (r \bmod \frac{1}{p})} * \frac{E_{cur}}{E_0} \ ,$$

Ecur is the current energy of node. *E*0 is the initial energy of the node. In this improvement the current energy is taken into consideration, and increases the probability of the high-energy nodes to become cluster-head, but there is also a significant problem. When the remaining energy of a node is very less than threshold value, the threshold *T* (*n*) becomes very small, the probability of the node random number being smaller than the threshold becomes small, the cluster-head nodes in the network will be too little, because of the untimely death, the selected cluster-head consumes too much energy and thus affects the network life. The above method doesn't consider the influence of the distance between nodes and the base station in electing cluster-head. In this paper, instead of threshold value we are selecting two cluster-head by comparing their energies. In normal leach protocol, there is only single cluster-head and it depends upon threshold value after sending a data node losses some energy so it again apply algorithm to find new cluster head. Hence transmission delay is being caused. In proposed technique there are two cluster-head if one goes down second take its position. By using 2Head- LEACH algorithm much energy can be saved and transmission delay can be reduced.

Example: -

When it transmits data to another node. If we have a WSN With the 100 nodes we divide that 100 node into the number of clusters say four. i.e.; each cluster contains 25 nodes. Now we compare the energy of nodes with another node in the same cluster. So we get max energy node. We consider it as cluster-head-1 and apply same process to find second cluster head-2. Perform the same operation for all the remaining clusters

IV. SECURITY

Low power design is the basic nature of WSN, which forces security mechanisms to fit under very limiting processing and bandwidth constraints, hence security to data, has been the challenging issue. The security requirements in WSN are the authentication of entity, message, data, especially in data critical applications. It is observed in [8] that due to Sensor Node Constraints and Networking Constraints in WSN's. Most of the protocols [9][10] are based on Symmetric key cryptography. We believe that RC6 is well-suited to meet all of the requirements of the Advanced Encryption Standard.

Details of RC6

Like RC5, RC6 is a fully parameterized family of encryption algorithms. A version of RC6 is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a nonnegative number of rounds r, and b denotes the length of the encryption key in bytes. Since the AES submission is targeted at w = 32 and r = 20, we shall use RC6 as shorthand to refer to such versions.

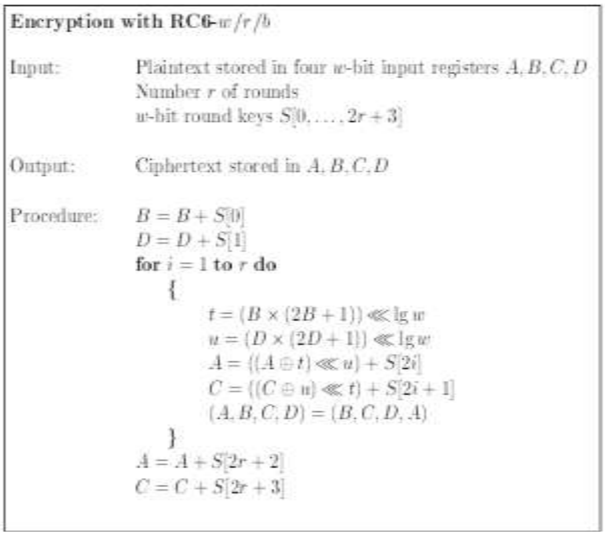
When any other value of w or r is intended in the text, the parameter values will be specified as RC6-w/r. Of particular relevance to the AES effort will be the versions of RC6 with 16-, 24-, and 32-byte keys. For all variants, RC6-w/r/b operates on units of four w-bit words using the following six basic operations. The base-two logarithm of w will be denoted by lgw.

a + b integer addition modulo 2^w
a - b integer subtraction modulo 2^w
$a \oplus b$ bitwise exclusive-or of w-bit words
$a \times b$ integer multiplication modulo 2^w.

a<<<b rotate the w-bit word a to the left by the amount given by the least significant lgw bits of b.

a>>>b rotate the w-bit word a to the right by the amount given by the least significant lgw bits of b.

The following figure shows the encryption and decryption algorithm of RC-6.



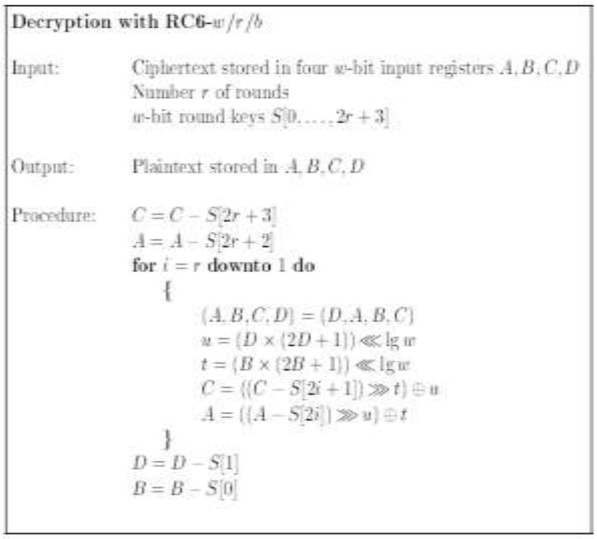
```
Encryption with RC6-w/r/b

Input:       Plaintext stored in four w-bit input registers A, B, C, D
             Number r of rounds
             w-bit round keys S[0, ..., 2r + 3]

Output:      Ciphertext stored in A, B, C, D

Procedure:   B = B + S[0]
             D = D + S[1]
             for i = 1 to r do
                 {
                     t = (B × (2B + 1)) <<< lg w
                     u = (D × (2D + 1)) <<< lg w
                     A = ((A ⊕ t) <<< u) + S[2i]
                     C = ((C ⊕ u) <<< t) + S[2i + 1]
                     (A, B, C, D) = (B, C, D, A)
                 }
             A = A + S[2r + 2]
             C = C + S[2r + 3]
```

Fig 1:- Encryption with RC-6



```
Decryption with RC6-w/r/b

Input:       Ciphertext stored in four w-bit input registers A, B, C, D
             Number r of rounds
             w-bit round keys S[0, ..., 2r + 3]

Output:      Plaintext stored in A, B, C, D

Procedure:   C = C − S[2r + 3]
             A = A − S[2r + 2]
             for i = r downto 1 do
                 {
                     (A, B, C, D) = (D, A, B, C)
                     u = (D × (2D + 1)) <<< lg w
                     t = (B × (2B + 1)) <<< lg w
                     C = ((C − S[2i + 1]) >>> t) ⊕ u
                     A = ((A − S[2i]) >>> u) ⊕ t
                 }
             D = D − S[1]
             B = B − S[0]
```

Fig 2:- Decryption with RC-6

It consists of six additions, two exclusive-ors, two squaring, two left-rotates by five bits, and two left-rotates by a variable quantity r. Note that we have counted B _ (2B + 1) = 2B2 + B as a squaring and two additions.
These basic operations can be implemented on an 8-bit processor in the following way (ignoring addressing instructions):

1. A 32-bit addition can be computed using four 8-bit additions with carry (ADDC).

2. A 32-bit exclusive-or can be computed using four 8-bit exclusive-ors (XRL).

3. A 32-bit squaring can be computed using six 8-bit by 8-bit multiplications (MUL) and eleven additions with carry (ADDC). Note that six multiplications are enough since we only need the lower 32 bits of the 64-bit product.

4. Rotating a 32-bit word left by five bit positions can be computed by rotating the word right by one bit position three times and then permuting the four bytes. Note that rotating the word right by one bit position can be done using four byte rotations with carry (RRC).

5. Rotating a 32-bit word left by r can be computed by rotating the word left or right by one bit position r0 times (r0 _ 4, with average two) and then permuting the four bytes appropriately. The five least-significant bits of r are used to determine r0 and the permutation which can be controlled using jumps (JB).

6. Most instructions take one cycle except that MUL takes four cycles and JB takes two cycles. Putting things together, we can estimate the total number of cycles needed for one round of RC6.

5. OUTPUT

If you want to send the data from node 1 to 14.

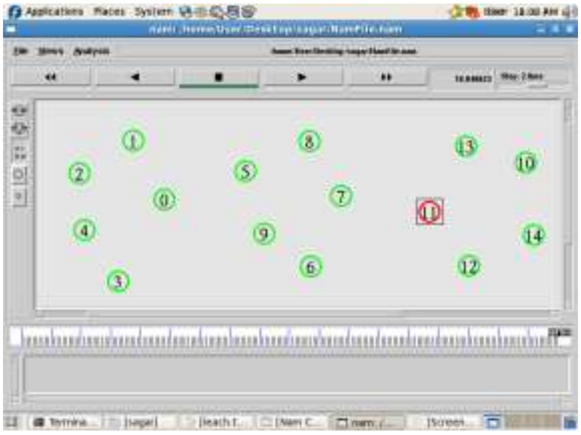


Fig 3:- By using Leach and RC-6

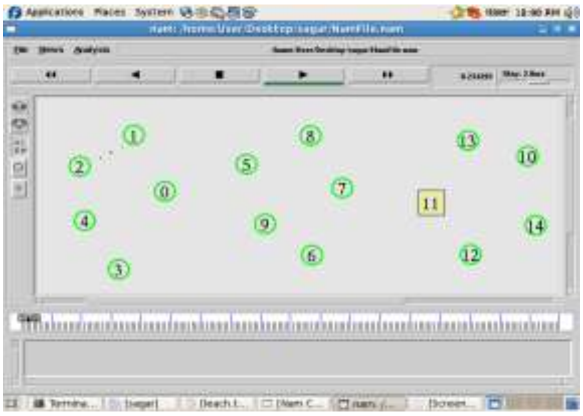


Fig 4:- node 2 is cluster head of 1st cluster

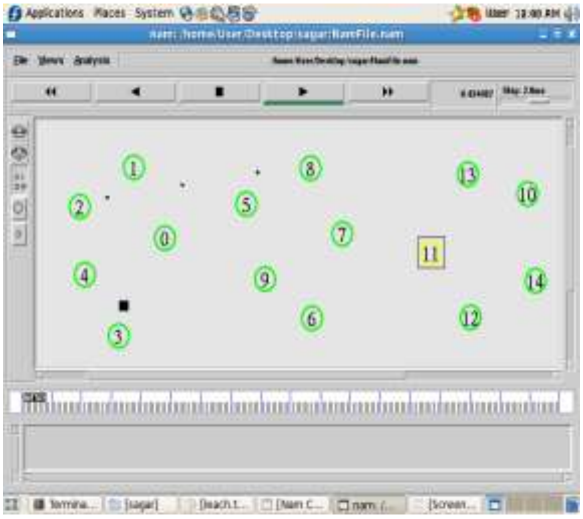


Fig 5:- node 8 is cluster head on 2nd

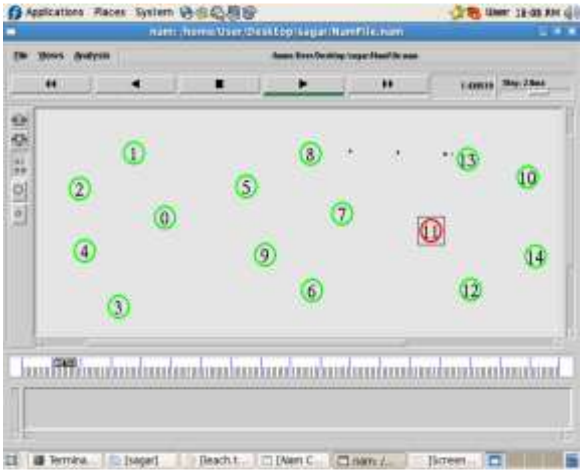


Fig 6:- node 13 is cluster head of 3rd head.

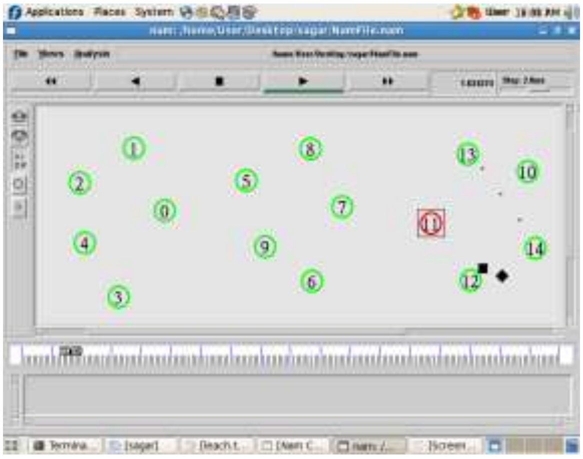


Fig 7:- data reach to node 14.

6. COMPARISON

This section deals with comparing energy efficient data transfer securely over WSN by leach protocol and by existing methods.

We compare this protocol on following parameters.

1. **On Transmission Delay**.

Transmission delay (or store-and-forward delay, also known as packetization delay) is the amount of time required to push all of the packet's bits into the wire. In other words, this is the delay caused by the data-rate of the link. Transmission delay is a function of the packet's length and has nothing to do with the distance between the two nodes. This delay is proportional to the packet's length in bits.

2. Energy Consumption.

Whenever a node transmits data to other node/base station it consumes some energy.

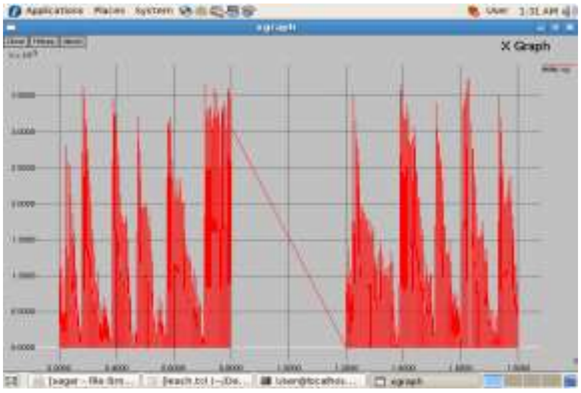


Fig. 8 The simulation of the data transmission using normal protocol

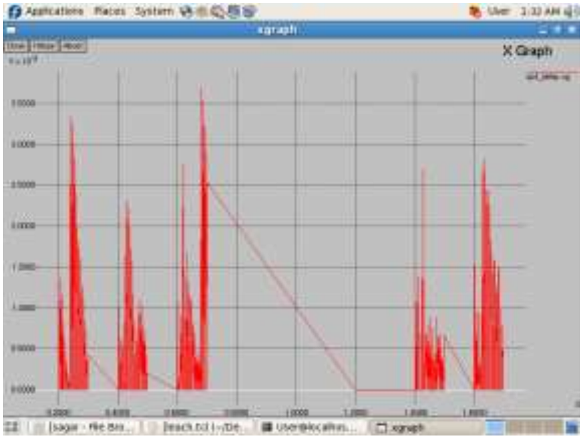


Fig. 9 The simulation of the data transmission using 2Head-LEACH protocol.

The above fig 8&9. Clearly shows that the data transmission by normal protocol is more than the data that is transmitted using leach protocol.

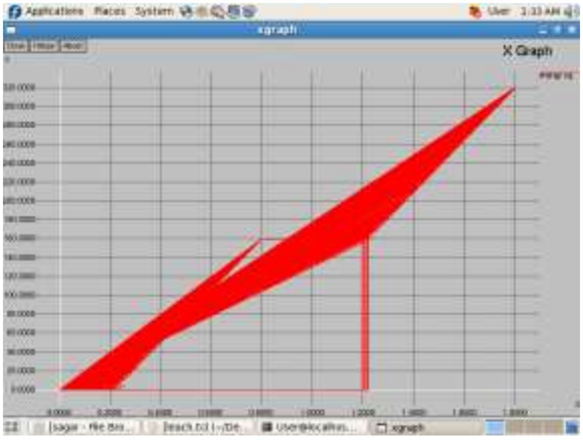


Fig. 10 Energy consumption using normal protocol

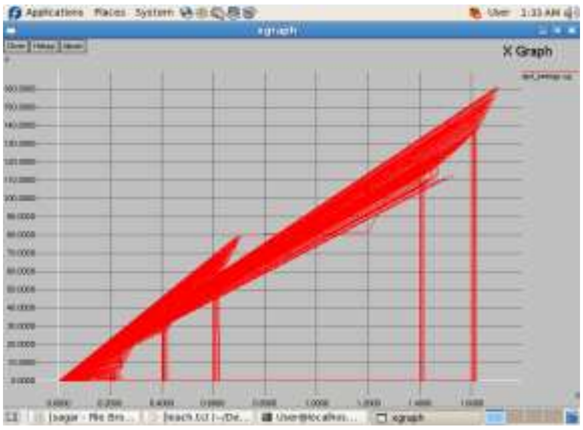


Fig. 11 Energy consumption using normal protocol 2Head-LEACH protocol

The above Fig 10&11 clearly shows that the energy consumed during transmission of data using normal protocol is more than that consumed by leach protocol

7. CONCLUSION

This paper proposes an energy balance algorithm and a technique to transmit data securely on the basis of traditional LEACH protocol and RC-6 algorithm. This algorithm comprehensively considers the residual energy and distance factors which improves cluster-head election and the strategy of non-cluster head node selecting the optimal cluster-head. As it is proved in the simulation result, the improved algorithm can effectively balance the network energy consumption, heighten system data transmission, and prolong the nodes and network life.

ACKNOWLEDGMENT

We would like to thank Vorugunti Chandra Sekhar, rudula Sarvabhatla, for their help concerning the enhancement of cryptographic techniques over wireless sensor network(WSN).

REFERENCES:

1) Feng Shang, Mehran Abolhasan, Tadeusz Wysocki. An Energy-Efficient adaptive Clustering Algorithm for Wireless Sensor Networks. International Journal of Information Acquisition, 2009, 6(2): 117-126.

2) Handy MJ, Hasse M, Timmermann D. Low energy adaptive clustering hierarchy with deterministic cluster-head selection [C] Proc of the 4th IEEE Conf. on Mobile and Wireless Communications Networks. Stockholm, 2002:368-372.

3) Jaydeep Sen, "A survey on Wireless Sensor netwrok Security", Technical Report 55-77, International Journal of Coomunication Netwroks and Information Security (IJCNIS) Vol 1, No2 August 2009.

4) Manjeshwar A, Grawal D.P. TEEN: A protocol for enhanced efficiency in wireless sensornetworks[C].Proceeding of the 15th Parallel and Distributed Processing Symp. San francisoi, 2001: 2009-2015.

5) Lindsey S, Raghavenda CS. PEGASIS: Power efficient gathering in sensor information systems[C]. Proceeding of the IEEE Aerospace Conf. NEW YORK, 2002: 1125-1130.

6) Younis O, Fahmy S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks [J]. IEEE Trans. On Mobile Computing.2004, 3(4):660-669.

7) LI-Qing GUO, YI XIE*, CHEN-HUI YANG and ZHENG-WEI JING: Improvement on LEACH by combining Adaptive Cluster Head Election and Two-hop transmission,[J]. Proceeding of the Ninth International Conference on Machine Learning and Cybernetics, Qingdao, July 2010, pp: 1678-1683.

8) Jochen Furthm¨uller, Stephan Kessler, and Oliver P. Waldhorst "Energy-efficient Management of Wireless Sensor Networks" The Seventh International Conference on Wireless On-demand Network Systems and Services IEEE/IFIP WONS 2010.

9) Farhana Ashraf, Riccardo Crepaldi and Robin H. Kravets University of Illinois at Urbana-Champaign "Synchronization vs. Signaling: Energy-Efficient Coordination in WSN" IEEE/2010

10) kai zeng, kannan govindan, and prasant mohapatra, university of california, davis"non-cryptographic authentication and identification in wireless networks" IEEE wireless communications -October 2010.

AUTHOR

The author#, Miss Prajwali Wamanrao Gawande was born on 20 January 1990.she has completed his B.E from Amaravati University and is currently pursuing M.E from Nagpur University. Her research interest is Wireless Sensor Network and Security.