SECURE DATA TRANSMISSION & IMPROVED ENERGY EFFICIENCY APPROACH IN WIRELESS SENSOR NETWORK

Ms.Varsha A. Khandekar[1], Mr.Sagar V. Hepat[2]
[1]*Lecturer in Info.Tech.Dept, Government Polytechnic Thane, (India)*
[2]*Senior Software Developer, Sushil Softech Solution Nagpur, (India)*

ABSTRACT

A wireless sensor network (WSN) have many independent sensors to discover physical or environmental conditions such as sound, temperature, pressure, etc. to send the data through the network to a main location. Additional Traffic is created with management requests and responses and the data issuing from the network's actual sensing application. The system's energy can reduce by sending and processing the data together, rather than individually. Energy consumption, balancing the network and extending the network's lifetime are the primary objectives of the routing protocol design in wireless sensor network. In this paper we have discussed the problems of transmitting data over wireless sensor network, proposed the technique for increasing the efficiency of a node along with providing security to the data.

Keywords: ***Cluster-Head, Clustering, Leach, Rc-6, Wireless Sensor Network***

I. INTRODUCTION

Wireless sensor network is a self-organized network composed by a large number of micro sensors that are randomly deployed in monitoring region through wireless communication [1]. Each sensor node in wireless sensor network has a constraint energy capacity, so energy-efficient mechanism is important. The highest priority in wireless sensor network, rather than sensing an event should be given to sending packets from the source node to the destination node. A typical node (Berkeley node) have a configuration of 8-bit CPU (4MHz),128KB flash,4KB RAM and Transmission range of 100 feets [3]. The nodes in WSN are made up of electronic devices that are able to sense, compute and transmit data from physical environments. These sensor nodes have limited energy resources. Energy resources for wireless sensor networks should be managed wisely so as to extend the lifetime of network. Another problem in WSN is transmitting data securely.

1.1 Efficiency of Node

In wireless communications, energy wastage shortens the networks lifetime. Following are the 4 reasons of energy wastage.

- Collisions:-when two nodes transmit at the same time and interfere with each other.
- Idle listening**:** - It happens when the radio is listening to the channel to receive a possible data that is not sent.
- Overhearing**:** - 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.
- Control**:**-packet overhead for protocols to exchange required information.

II. LEACH PROTOCOL

LEACH is the earliest proposed single-hop clustering routing protocol in WSN. 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. In LEACH protocol, all clusters are self-organized, each cluster contains a cluster-head and several non-cluster head nodes, and cluster-head node consumes more energy than non-cluster head nodes. With the purpose of balancing network energy consumption and prolonging the network life cycle, it selects cluster head randomly and each node has an equal chance to be 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 & steady-state phase is the stable data transfer phase. In Set-up phase, each node generates a random number between 0 to 1, and compares this number with the threshold value $T(n)$. If the number is less than $T(n)$, the node is selected as a cluster-head, the threshold $T(n)$ is set as follow:

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

Where n refers the node identification 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 determined, the cluster-head sends a broadcast message to the network, announced itself as the cluster-head. Each normal node decides which cluster to join in according to the signal strength of the received message, sends a request message to the corresponding cluster-head. The cluster-head receives all the messages sent by the nodes that would like to join in the cluster. LEACH protocol has a relatively good function in energy consumption through dynamic clustering, keeps the data transmission in cluster which reduces the energy consumption by communicating directly between nodes and the base station, but there are still a lot of inadequacies. The LEACH protocol uses the mechanism of cluster-head rotation, elects cluster-head randomly, after several rounds of data transmission. The residual energy of the nodes will have a great difference. Cluster-head or the nodes which are far from the base station will consume more energy in transmitting data of the same length relatively. If these nodes are selected as cluster-heads, will run out of energy and become invalid. Once the number of invalid nodes increases, it'll have a great influence in the network performance and shorten the life of the network. Cluster member nodes select the optimal cluster-head based on the received signal intensity to join it. & do not consider the distance from the node itself to the base station, either the distance between cluster-head or the base station. So normal node may chose the cluster-head that is far from base station as its optimal cluster-head, this not only gives the heavy burden to the cluster-head but also increases the extra energy consumption, which is not beneficial to balance network energy consumption.

III. IMPROVEMENT OF THE LEACH PROTOCOL

This paper considered node energy and position information to improve the LEACH algorithm. It proposed energy balanced clustering algorithm named 2Head-LEACH algorithm to improve the energy of the node.

3.1 Clusters-Head Selection

There are many improved methods of the cluster-head selection based on residual energy, the threshold equation in [2] is:

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

Ecur is the current energy of node. E_0 is the initial energy of node. This improvement takes the current energy 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 , $T(n)$ 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. The selected cluster-head consumes too much energy and thus affects the network life because of the untimely death. The above method doesn't consider the influence of the distance between nodes and the base station in electing cluster-head. In this paper we are selecting two cluster-head by comparing their energy instead of threshold value. 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. It causes transmission delay. In proposed technique there are two cluster-head if one goes down second take its position. By doing this 2Head- LEACH algorithm save much energy and reduces transmission delay. Example: - Whenever node transmit a data to the anther node it losses some energy. 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 logic to find the second cluster head-2. Continue doing this for all the remaining clusters.

IV. SECURITY

The basic nature of WSN is low power design, which forces security mechanisms to fit under very limiting processing and bandwidth constraints. So 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 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.

4.1 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.

The Fig.1 & Fig.2 shows the encryption and decryption algorithm of RC-6.

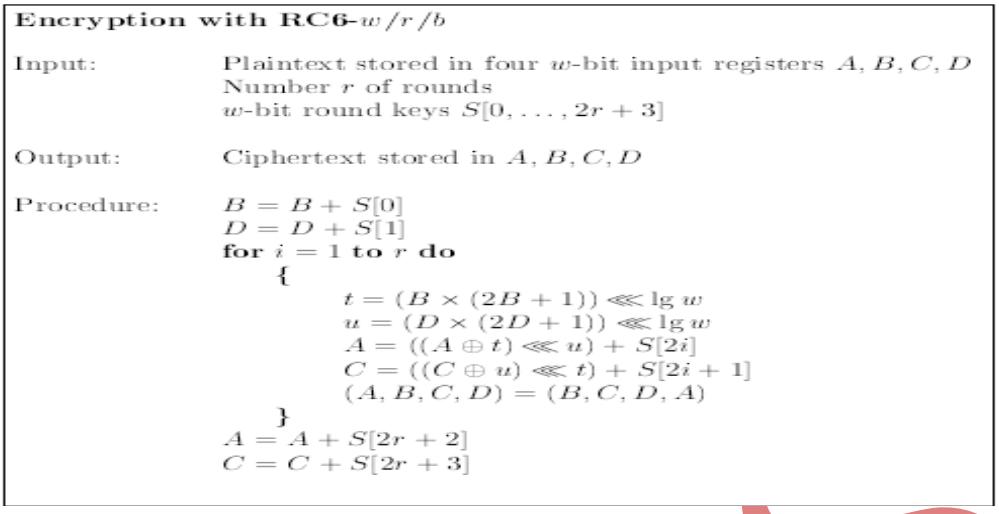

Figure 1: Encryption with RC-6

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.

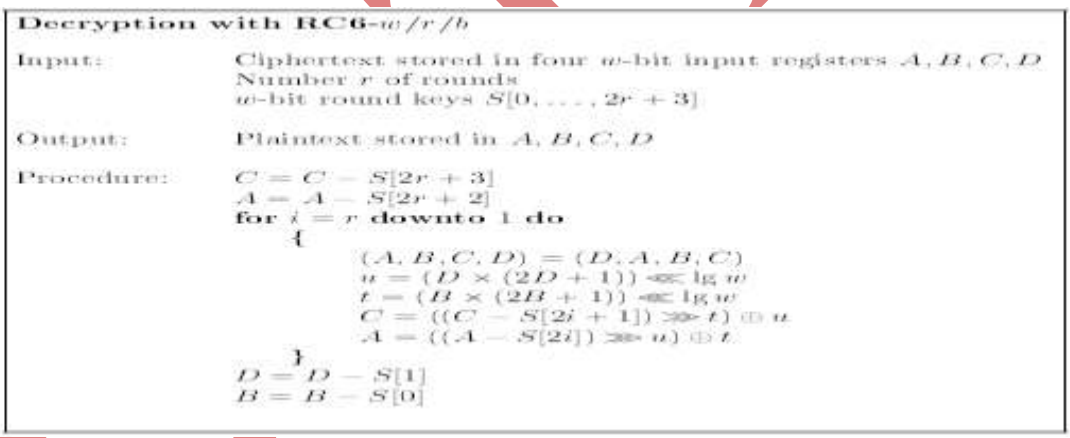

Figure 2: Decryption with RC-6

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.

V. OUTPUT

Following figures shows the transmission of data from node 1 to 14.

Figure 3: By using Leach and RC-6

Figure 4: Node 2 is cluster head of 1st cluster

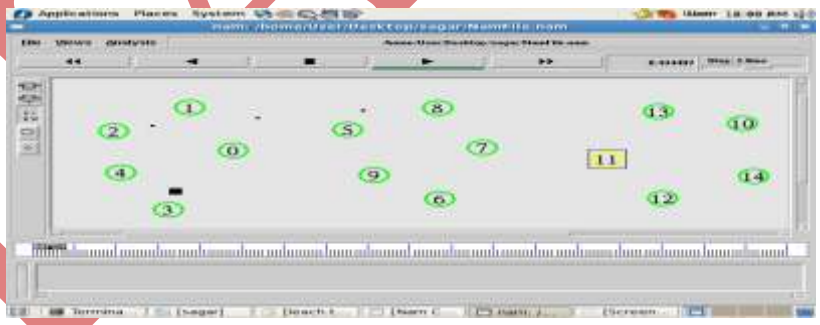

Figure 5: Node 8 is cluster head on 2nd cluster

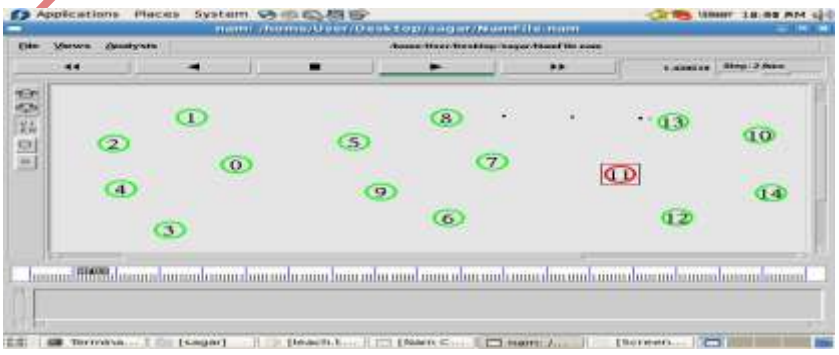

Figure 6: Node 13 is cluster head of 3rd head

Figure 7: Data Reach to Node 14

VI. COMPARISON

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

We compared this protocol on following parameters:

6.1 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.

6.2 Energy Consumption

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

Figure 8: The Simulation of the Data Transmission Using Normal Protocol

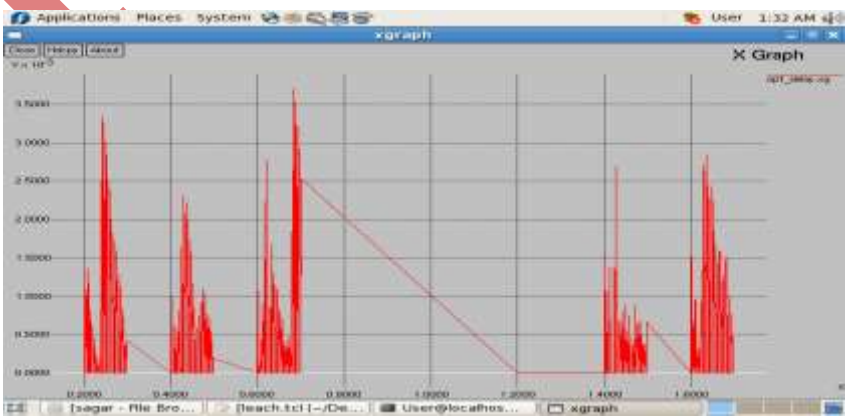

Figure 9: The Simulation of the Data Transmission Using 2Head-LEACH Protocol

The above Fig.8 & Fig.9 clearly shows that the data transmission by normal protocol is more than the data transmission by LEACH protocol. So transmission delay is more in normal protocol.

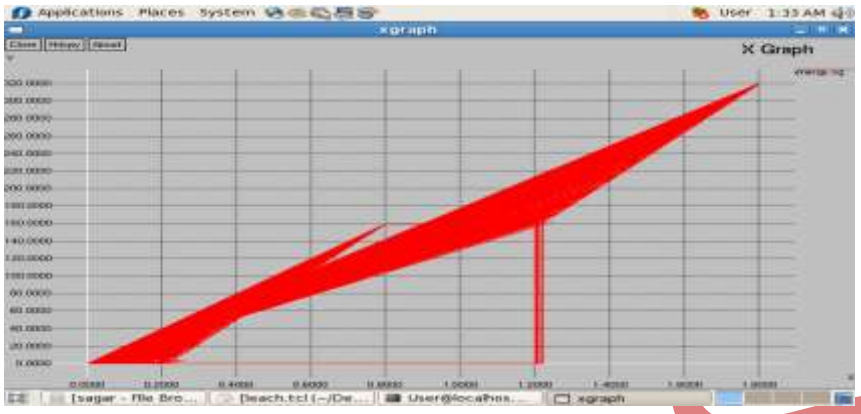

Figure10: Energy Consumption Using Normal Protocol

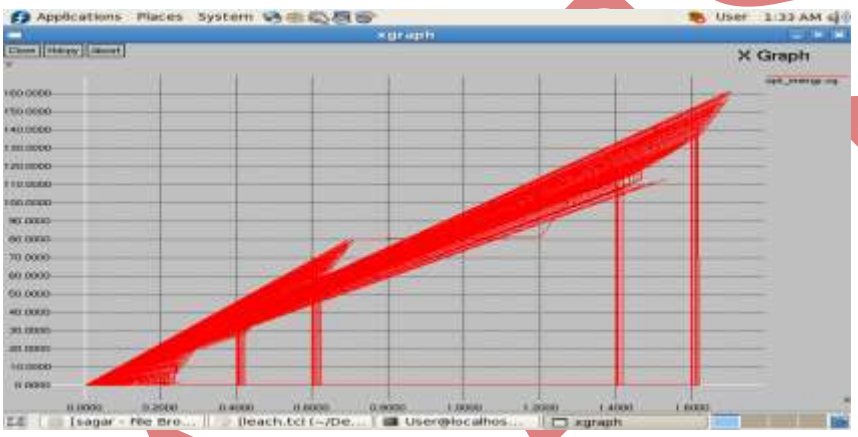

Figure11: Energy Consumption Using Normal Protocol 2Head-LEACH Protocol

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

VII. CONCLUSION

On the basis of traditional LEACH protocol and RC-6 algorithm, this paper proposed an energy balance algorithm and a technique to transmit data securely. This algorithm comprehensively considers the residual energy and distance factors, 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.

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 atUrbana-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.