International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), September 2015
www.ijarse.com

IJARSE
ISSN 2319 - 8354

ENERGY EFFICIENT AND SECURE CLUSTER BASED ROUTING PROTOCOL (LEACH) FOR WIRELESS SENSOR NETWORKS

Sowmya B S

Student, Dept. of CSE, Siddaganga Institute of Technology, Tumakuru, (India)

ABSTRACT

Due to the limitation of energy, the routing protocols of wireless sensor network (WSN) must minimize energy consumption and thus extend the network lifetime. Low energy adaptive clustering hierarchy (LEACH) is the first classical hierarchical routing protocol in WSN. A timer is introduced while electing the optimal sensor node as cluster head. During data transmission, we are using single hop and multi-hop hybrid routing to communicate with the base station, so that it can utilize energy more effectively and evenly. By analysing the disadvantage of LEACH algorithm, this paper proposes an improved LEACH algorithm. The improved LEACH protocol can reduce energy consumption and thus prolong the network lifetime. In order to provide security to the improved LEACH protocol, this paper uses security mechanism such as RSA cryptosystem and thus ensures the secure transmission.

Keywords: Cluster; Cryptosystem; Network Lifetime; Wireless Sensor Network;

I. INTRODUCTION

In the twenty-first century Wireless Sensor Networks (WSNs) are being widely considered as one of the most important technologies for many real time applications [1]. Wireless Sensor Networks consist of tiny sensor nodes and these sensor nodes are consist of sensors (temperature, light, humidity, radiation, and more), microprocessor, memory, transceiver, and power supply [2]. These sensor nodes are usually deployed in a physical area and communicated through internet and wireless links, which provide opportunities for a variety of civilian and military applications, for example, environmental monitoring, battle field surveillance, and industry process control [1].

Sensors are deployed in an ad-hoc manner in the area of interest to monitor events and gather data about the environment. They have the ability of sensing, data processing and communicating with each other in the network environment. Multi-hopping in the WSNs can cause a sensor node to communicate with a node with is far away from it. This allows the sensor nodes in the network to expand the monitored area and hence proves its scalability and flexibility property [3]. If the node is not able to communicate with other through direct link, i.e. they are out of coverage area of each other, than the data can be sent to the other node by using the nodes in between them. This property in WSNs is referred as multi-hoping.

A network can be divided into several clusters with the help of a property called clustering. Within each cluster, one of the sensor nodes is elected as a cluster head (CH) and other are called as with cluster members (CM). All sensor nodes work cooperatively to serve the requests within each cluster. Cluster head collects the data locally from the cluster members and with the help of fusion and aggregation it drops the redundant data and then transmits the aggregated data either directly or via multi-hop transmission to the sink. Since the cluster heads spend more energy than the non-cluster heads, so to distribute the workload of the cluster heads among the wireless sensor nodes their role is rotated among all nodes in order to equalize energy consumption [4]. This process is called the cluster head (CH) rotation. These networks (WSNs) are unique as compared to traditional wired and wireless networks because they having the seal-healing and self-organizing property which differentiate them from other networks.

The main problem in using these networks is limited battery life. This is due to fact that the size of a sensor node is expected to be small and this leads to constraints on size of its components i.e. battery size, processors, data storing memory, all are needed to be small. So any optimization in these networks should focus on optimizing energy consumption in the network [4].

An efficient and beneficial solution from overcoming this problem is to implement routing protocols that perform efficiently and utilizing the less amount of energy as far as possible for the communication among nodes within the network and along with between the networks. Sensor devices in WSNs monitor the same event and report on them to the base station. Therefore, one good approach is to consider that sensors located in the same region of the network will transmit similar values of the attributes. This fact notices inherent redundancy in the node transmissions that may be used by the routing protocol. Sensor networks need protocols, which are specific, data centric, capable of aggregating data and optimizing energy consumption. The sensor nodes are usually programmed to monitor or collect data from surrounding environment and pass the information to the base station for remote user access through various communication technologies [5].

1.1 Routing Challenges and Design Issues in WSNs

There are different parameters which provide a very challenging criterion in routing for WSN and they are as follows [6]

- Node deployment in the sensor network.
- Energy Consumption in the network should occur without losing of accuracy of the network.
- Data Reporting Method should be configured in the network.
- Nodes/Link Heterogeneity of the network.
- Scalability of the network.
- Network Dynamics.
- Transmission Media should be fault tolerance.
- Coverage area of different sensor nodes in the network.
- Data Aggregation process within the clusters in the network.
- QOS policies of the network.

1.2 Cluster Based Hierarchical Model

The basic objective on any routing protocol is to make the network useful and efficient. A cluster based routing protocol group's sensor nodes where each group of nodes has a CH [3, 7]. Sensed data is sent to the CH rather than send it to the BS; CH performs some aggregation function on data it receives then sends it to the BS where these data is needed.

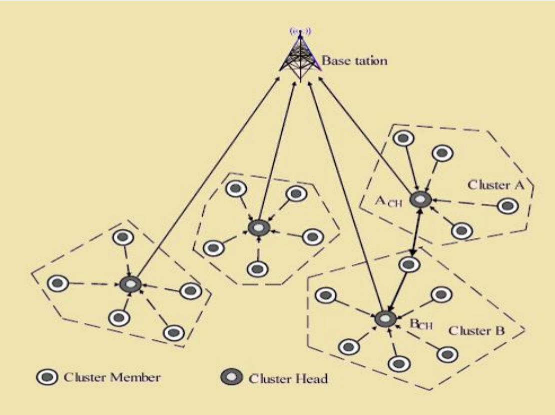


Fig.1 Clustering Model Hierarchical Routing

As shown in Fig. 1, a hierarchical cluster based approach divides the network into different clustered layers. Different sensor nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads or to the base stations.

Clustering mechanism provides inherent optimization capabilities of sensed information at the cluster heads. In the cluster-based hierarchical model, data is first aggregated in the cluster then sent to a higher-level cluster-head or to the base station. In cluster-based hierarchical model only the cluster-heads have to perform the data aggregation process, but in case of the multi-hop model every intermediate node performs data aggregation process. As a result of this process, the cluster-based model is more suitable for time-critical application.

However this cluster based approach having a disadvantage of, as the distance between clustering level increases, the energy spent in processing and communicating is directly proportional to the square of the distance between the cluster levels.

Advantages of clustering over different classes of algorithms are [6],

- Minimization of energy consumption of intra cluster and as well as inter cluster network.
- Scalability of the network.
- Network life time prolonging.
- Reduction of information packet delay.
- Handling heterogeneity of network.

II. EXISTING SYSTEM

Low Energy Adaptive Clustering Hierarchy (LEACH) is the first hierarchical cluster-based routing protocol for wireless sensor network. LEACH algorithm divides wireless sensor network into several clusters. The algorithm introduces a random clustering scheme for wireless sensor network. Using clustering scheme made data aggregation possible in this protocol, since dynamic re-establishment of the clusters balances the energy consumption over the nodes. The execution of the algorithm is a continuous cyclical process; this introduced the concept of "round", a cycle known as a round. A round is divided into clusters establish phase and stable data transmission phase. Stable data transmission phase must be longer than cluster establish phase in order to save energy [3]. LEACH algorithm running process is shown in Figure 2.

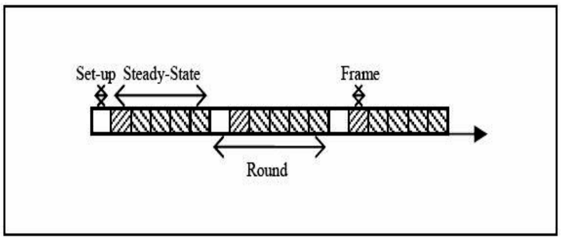


Fig.2 LEACH Protocol Phases

In cluster establish phase, each sensor node generates a random number between zero and one. The sensor node becomes a CH (cluster head) for the current topology update round if the number is less than the following threshold:

$$T\ (n) = \begin{cases} \dfrac{p}{1 - p\left[i \bmod \left(\frac{1}{p}\right)\right]} & n \in G \\ 0 & otherwise \end{cases}$$

Where '*p'* is the desired percentage of cluster heads (e.g.0.05), '*i'* is the number of current topology update interval, and 'G' is the set of nodes that have not been clusters heads in the last 1/ *p* rounds. In the first topology update interval, *i* = 0 and *T* (*n*) for all the sensor nodes is *p*. Therefore, in average 100 *p* percent of nodes become cluster heads in the first round. In the second round, *i* =1and *T* (*n*) = 0 for the nodes were cluster heads in the first interval and *T* (*n*) = *p* / (1- *p*) for the other nodes. As the average number of non-CH nodes in the first interval was 100(1- *p*) percent of nodes become cluster heads. For the rest of the intervals, the same percentage is kept accordingly.

Cluster head (CH) sends messages to neighbour sensors. The nodes receive messages and join a cluster by choosing the nearest cluster head (strongest signal). During the interval, cluster members (CM) will send request messages to cluster head to join a cluster. After receiving request messages, cluster head uses TDMA (Time Division Multiple Access) method to assigns a time slice for each cluster member to transmit data and send messages. To save energy, cluster members send data to cluster head only within its time slice and other time slices automatically get asleep waiting for the coming of its time slice in next frame, which can ensure the cluster heads sequentially receive all the data collected by the cluster members. The problem of data loss by cluster members sending data simultaneously is effectively solved.

In stable data transmission phase, cluster members send data to the cluster head only within its time slice and automatically enter sleep in other time slices to save energy. The cluster heads aggregate, compress, and route the data to the remote base station. Not only collecting data, but also integrating data and sending it to base station directly, cluster head consumes more energy obviously. After a period of time, network enter a new round to re-establishment a number of clusters, which selects new nodes as cluster heads, continuous cycle until all nodes energy become zero. That node energy is zero means that the node has died; while that the energy of all nodes is zero means that the network died.

2.1 Analyze of LEACH

LEACH algorithm assumes that all nodes are equal. Nodes can communicate with the base station directly and radio signals energy consumption in all directions is the same [8]. The theory of the algorithm is that all nodes have the equivalent initial energy, alternately elected cluster head. After several rounds of cycling, cluster heads consume a lot of energy, while nodes which haven't been elected as cluster head consume relatively few actually. Since the energy distribution of the entire network has been uneven, it will accelerate to be blind nodes and is extremely detrimental to the entire network if the original cluster head election mechanism continues to be used and nodes with less residual energy may be elected as cluster heads.

When cluster heads transmit data to the base station, energy consumption of transmitting the same size of data packet is proportional to the distance between cluster head and the base station. The cluster heads that are far away from the base station would consume a large amount of energy while taking single-hop method to send data to the base station [9]. After several rounds of circulation, cluster heads nearer to the base station remain with lot of energy, while cluster heads that are far away from the base station become almost blind spot detection. When more than half of nodes energy is zero, the network has lost its original meaning though remaining nodes are still working.

III. PROPOSED SYSTEM

To overcome the drawbacks of LEACH algorithm, an improved LEACH protocol is proposed. The improved algorithm makes use of the concept of "round". A round is divided into two sections; first is the setup phase where the clusters are established and the second is the steady phase where data transmission takes place. The steady phase must be longer than the setup phase, so that it will fully make use of energy.

The proposed improved LEACH algorithm is divided into four modules.

i. Network deployment

In this phase, nodes are deployed randomly. Here we are considering all the nodes as static and are deploying 50 nodes.

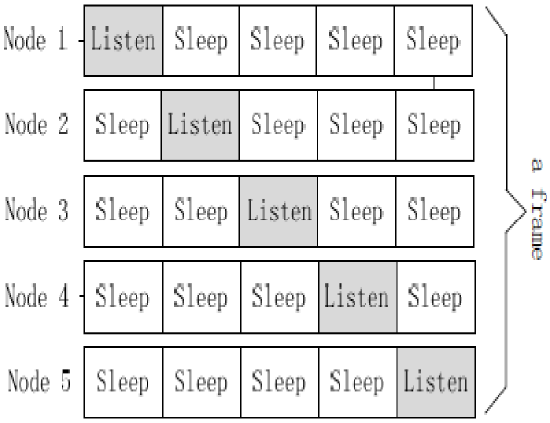
ii. Cluster head election

The sensor nodes that are close to the base station, sensor nodes with relatively high residual energy and sensor density are more likely to become the cluster heads. When a round is over, nodes can get their remaining energy and receive the number of neighbour nodes by communicate with the surrounding sensor nodes. Since after a certain period, sensor nodes energy will gradually lower and finally die, so the number of neighbour sensors would gradually reduce. Although setting up clusters will consumes energy every time, the energy consumption of transmitting unit data is proportional to the distance, energy consumption of communicating with neighbour sensors is relatively little.

The distance between nodes and the base station can be obtained through the first communication with the base station, as nodes are fixed in the network and they won't change. The node will generate a random number between zero and one when its regular time comes. Sensor nodes with more residual energy, intensity and relatively close to the base station are likely to produce a smaller random number. When random number is less than the threshold *T* (*n*), nodes will become a cluster head and send messages to around nodes; when random number is large than the threshold(*n*), the node will regenerate a random number. According to the random number whether less than the threshold *T* (*n*) identifying itself as a cluster head or original node.

Similar to LEACH protocol, it sends cluster head messages or requests to join a cluster according to node attributes. If the node receives messages from cluster heads before the end of regular time, it will abolition the timing and send request to join a cluster [10]. After cluster heads receive request message from original sensors, it will set a TDMA slot table and send it to all cluster members.

Figure 3 shows allotments of time slots in a cluster. Only one node is listening in a frame in a cluster.



Node 1	Listen	Sleep	Sleep	Sleep	Sleep
Node 2	Sleep	Listen	Sleep	Sleep	Sleep
Node 3	Sleep	Sleep	Listen	Sleep	Sleep
Node 4	Sleep	Sleep	Sleep	Listen	Sleep
Node 5	Sleep	Sleep	Sleep	Sleep	Listen

Fig. 3 Listen and Sleep Modes in Timeslots.

During stable data transmission phase, cluster members send collected data by timeslots table to cluster heads only within its time slice and automatically enter asleep in other time slices, waiting for the coming of its time slice in next frame. Cluster heads fuse data that collected and received from cluster member nodes, then send them to receiver. After one round, the entire network will start next round, re-enter building clusters phase [11, 12]. In the establish cluster phase, the process of sensors becoming cluster heads or original sensors is shown in Figure 4.

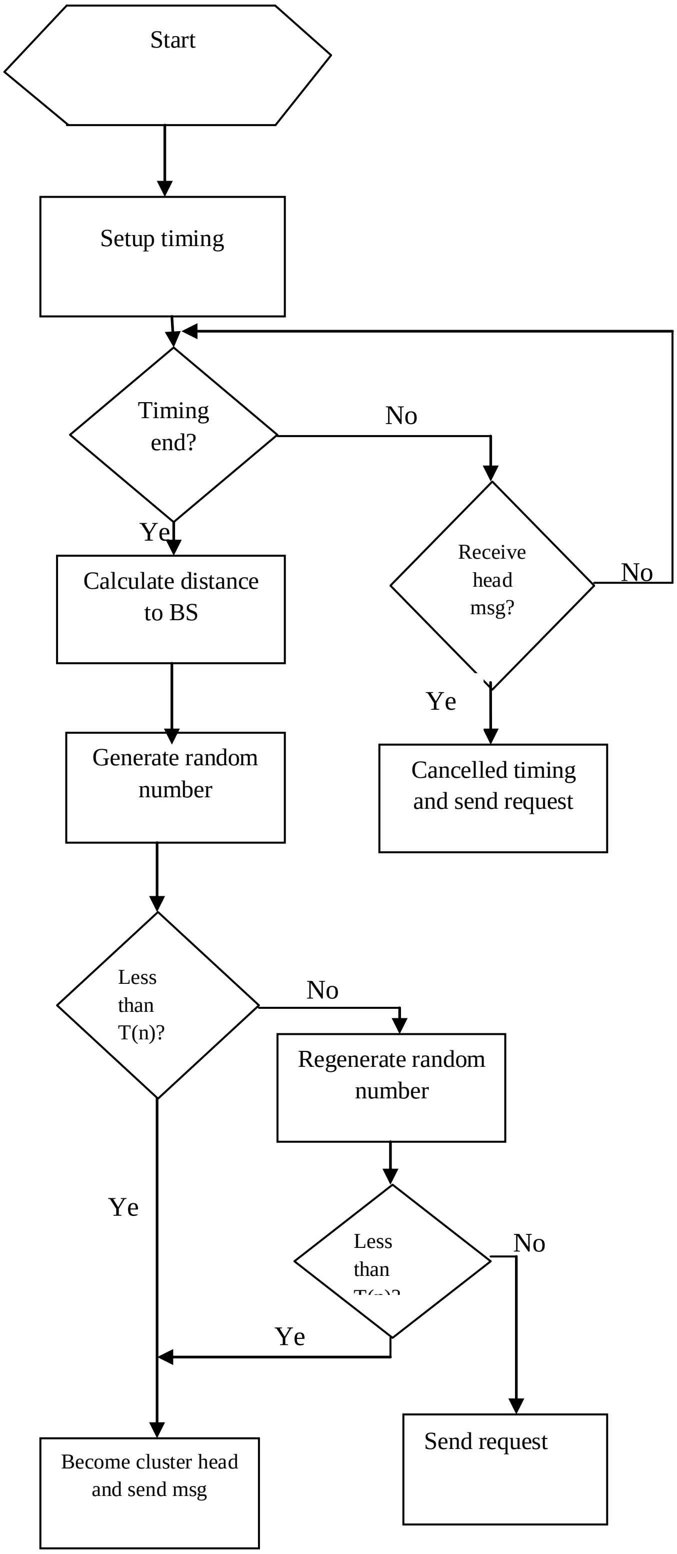


Fig. 4 Setup of Cluster of Improved-LEACH

iii. Data transmission

The improved protocol takes a mixture of single-hop routing and multi-hop routing to transmit data between the cluster head sensors and the base station. The base station can get the distance between sensors and the base station. When all sensors communicate with the base station at the first time. Average of all distances is the expected distance of sensors to base station. Base stations send the expected distance to all sensors by broadcast. When a sensor is elected as cluster head, it firstly compares its own distance to the base station with the expected distance between sensors and the base station [13, 14].

When the distance between the cluster head and the base station is less than or equal to the expected distance, cluster head will communicate with base station by single-hop mode directly.

It has the same principle with LEACH. When the distance between the cluster head and the base station is more than the expected distance, cluster head will communicate with base station by multi-hop method.

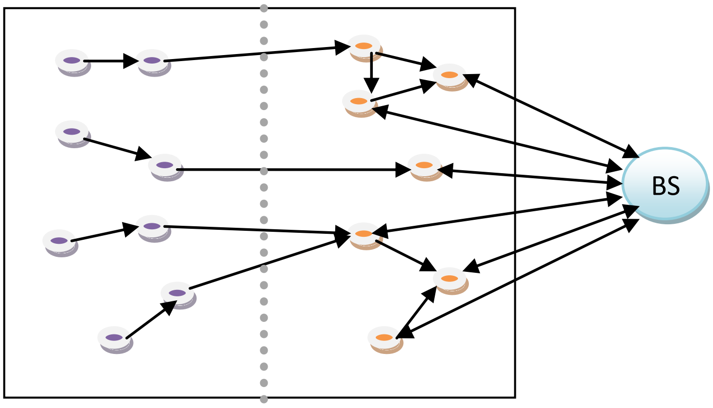


Fig. 5 Single-Hop and Multi-Hop Hybrid

iv. RSA security algorithm

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.

This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. Many protocols like SSH, OpenPGP, S/MIME, and SSL/TLS rely on RSA for encryption and digital signature functions. It is also used in software programs such as browsers, which need to establish a secure connection over an insecure network like the Internet or validate a digital signature

The RSA algorithm involves three steps: key generation, encryption and decryption.

A. Key generation

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.

- For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

2. Compute n = p*q.

- n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

3. Compute φ (n) = φ (p) *φ (q) = (p − 1)*(q − 1) =
n - (p + q -1)

- Where φ is Euler's totient function. This value is kept private.

4. Choose an integer e such that 1 < e < φ (n) and gcd (e, φ (n)) = 1; i.e., e and φ (n) are co prime.

- 'e' is released as the public key exponent.
- 'e' having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 2_{16} + 1 = 65,537. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.

5. Determine 'd' as d ≡ e_{-1} (mod φ (n)); i.e., d is the modular multiplicative inverse of e (modulo φ (n)).

- This is more clearly stated as: solve for d given d·e ≡ 1 (mod φ(n))
- This is often computed using the extended Euclidean algorithm. Using the pseudo code in the Modular integers section, inputs 'a' and 'n' correspond to 'e' and φ (n), respectively.
- 'd' is kept as the private key exponent.

The public key consists of the modulus 'n' and the public (or encryption) exponent 'e'. The private key consists of the modulus 'n' and the private (or decryption) exponent 'd', which must be kept secret. 'p', 'q', and φ(n) must also be kept secret because they can be used to calculate 'd'.

B. Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key d secret. Bob then wishes to send message M to Alice.

He first turns M into an integer m, such that 0 ≤ m < n and gcd (m, n) = 1 by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text 'c' corresponding to

$$c \equiv m^e \ (mod\ n)$$

This can be done efficiently, even for 500-bit numbers, using Modular exponentiation. Bob then transmits c to Alice.

Note that at least nine values of 'm' will yield a cipher text c equal to 'm'.

C. Decryption

Alice can recover m from 'c' by using her private key exponent 'd' via computing

$$m \equiv c^d \ (mod\ n)$$

Given 'm', she can recover the original message M by reversing the padding scheme.

IV. SIMULATION RESULTS AND ANALYSIS

The project is implemented in ns-2 simulator.

In our scenario, we are comparing the existing LEACH algorithm the proposed improved algorithm through some performance metrics.

a. Throughput: It is defined as the total number of delivered data packets divided by the total duration of simulation time.

The comparative throughput results of the existing LEACH algorithm and the proposed LEACH algorithm shows that the throughput of proposed LEACH algorithm is more compared to that of the existing LEACH.

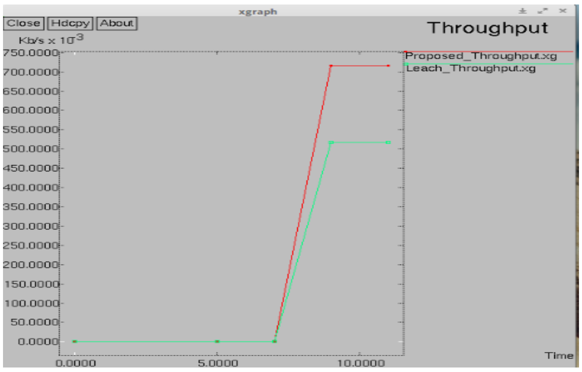


Fig. 6 Throughput

b. Packet Delivery Ratio (PDR): It is defined as the ratio between the numbers of packets received by the destination to number of packets sent by the source.

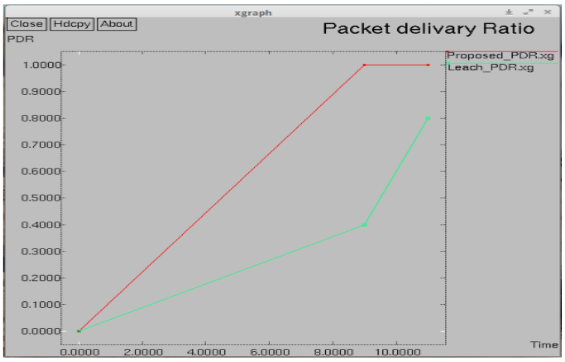


Fig. 7 Packet Delivery Ratio

The comparative PDR results of the existing LEACH algorithm and the proposed LEACH algorithm shows that the PDR of proposed LEACH algorithm is quiet good compared to that of the existing LEACH.

c. The comparative energy consumption results of the existing LEACH algorithm and the proposed LEACH algorithm shows that energy consumption in the proposed LEACH algorithm is less compared to that of the existing LEACH.

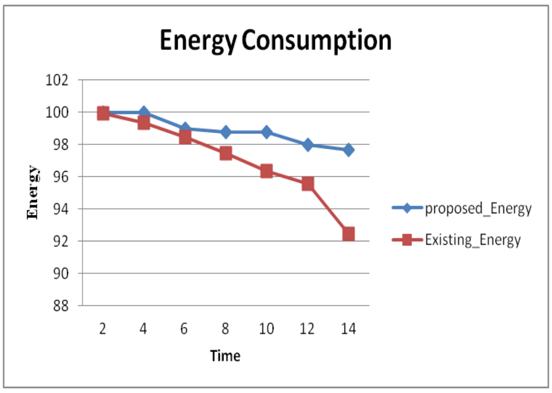


Fig. 8 Energy Consumption

V. CONCLUSION

The performance of wireless sensor network is mainly based on the routing protocol utilized by networks. In order to save node energy, the LEACH protocol has been improved. This paper presents a routing protocol based on the classical LEACH algorithm. Simulation results show that the network lifetime confirming that the improved-LEACH protocol can reduce energy consumption and prolong the network lifetime.

REFERENCES

[1] Shio Kumar Singh, M P singh D K singh, “A Survey of Energy- Efficient Hierarchical Cluster-Based Routing in Wireless Sensor Networks”, in Int. J. of Advanced Networking and Applications,Vol. 02, Issue 02, 2010, pp. 570-580.

[2] Rengugadevi G & Sumithra M G , “Hierarchical Routing Protocols for Wireless Sensor Network–A survey” in International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Vol. 2, Issue 1, 2012, pp. 71-75.

[3] Ali Norouzi1, Abdul Halim Zaim, “An Integrative Comparison of Energy Efficient Routing Protocols in Wireless Sensor Network”, in Scientific Research of Wireless Sensor Network, Vol. 4, 2012, pp. 65-67.

[4] Ravneet Kaur, Deepika Sharma and Navdeep Kaur, “Comparative Analysis of Leach and Its Descendant Protocols in Wireless Sensor Network”, in International Journal of P2P Network Trends and Technology, Vol. 3, Issue 1, 2013, pp. 51-55.

[5] Par minder Kaur, Mrs. Mamta Katiyar, “The Energy-Efficient Hierarchical Routing Protocols for WSN: A Review” in International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 11, November 2012, pp. 194-199.

[6] Amit Bhattacharjee, Balagopal Bhallamudi and Zahid Maqbool, “Energy-Efficient Hierarchical Cluster Based Routing Algorithm in WSN: A Survey”, in International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 5, May, 2013, pp. 302-311.

[7] S. Selvakennedy, S. Sinnappan, Yi Shang. A biologically-inspired clustering protocol for wireless sensor networks. Computer Communications 30, 2007, pp. 2786-2801

[8] Seapahn Megerian and Miodrag Potkonjak, "Wireless sensor networks," Book Chapter in Wiley Encyclopedia of Telecommunications, Editor: John G. Proakis, 2002.

[9] Hoda Taheri, Peyman Neamatollahi, Ossama Mohamed Younis, Shahrzad Naghibzadeh, Mohammad Hossein Yagh mae. An energy aware distributed clustering protocol in wireless sensor networks using fuzzy logic. Ad Hoc Networks 10, 2012, pp. 1469-1481.

[10] Ali Chamam, Samuel Pierre. A distributed energy-efficient clustering protocol for wireless sensor networks. Computers and Electrical Engineering 36, 2010, pp. 312-316.

[11] Ferng Huei Wen, Tendean Robby, Kurniawan Arief. Energy-efficient routing protocol for wireless sensor networks with static clustering and dynamic structure. Wireless Personal Communications, 2012, 65(2), pp. 347-367.

[12] Cho Seongsoo, Shrestha Bhanu, La KeukHwan, Hong BongHwa, Lee Jongsup. An energy-efficient cluster-based routing in wireless sensor networks. Communications in Computer and Information Science, 2011, 31 (4), pp. 15-22.

[13] M.C.M.Thein, T.Thein. An energy efficient cluster-head selection for wireless sensor networks. In: International Conference on Intelligent Systems, Modelling and Simulation, 2010, pp. 287-291.

[14] Heinzelman W R, Chandrakasan A, Balakrishnan H. An application specific protocol architecture for wireless Micro sensor Networks [J]. IEEE Transaction on Wireless Communications, 2002, 1(4), pp. 660-670.

[15] G. Ran, H. Zhang, S. Gong. Improving on LEACH protocol of Wireless Sensor Networks Using Fuzzy Logic, Journal of Information and Computational Science, 2010, pp. 767-775.