A Research Paper on Security Enhancement In Leach Protocol

[1]Deepika, [2]Manpreet,
[1]Student, [2]Assistant Professor,
[1]Computer Science, Global Research Institute of Management in Technology, Radaur, India

***Abstract*- Wireless sensor nodes are basically the group of nodes which communicate with each other and with the base station with the help of communication link. LEACH is a very important protocol which is used in sensors networks. Previously all the work in leach has been done to control the energy consumption by the nodes. Very less work has been done to enhance the security level of the leach. So the objective of this paper is to enhance the security level of LEACH with no compromise with energy level. In this proposed work DES encryption algorithm has been applied on the LEACH protocol. The results are obtained in the MATLAB.**

***Keywords*-Wireless sensor networks, Base station, Cluster Head, Low Energy Adaptive Clustering Hierarchy.**

I. INTRODUCTION

Wireless sensor networks (WSNs) are made up of a huge number of independent sensor nodes, which are placed at different locations to gather important information and mutually transmit that information to a base station. Now a day WSNs has become increasingly one of the sizzling research areas due to their wide use in real-time application like healthcare applications, environmental monitoring applications, and military applications. All sensor nodes have to transmit the sensed data to the Base Station (BS). The nodes in WSNs contact with each other wirelessly, although they have different limitations on resources like battery consumption, available memory, and processing capabilities.

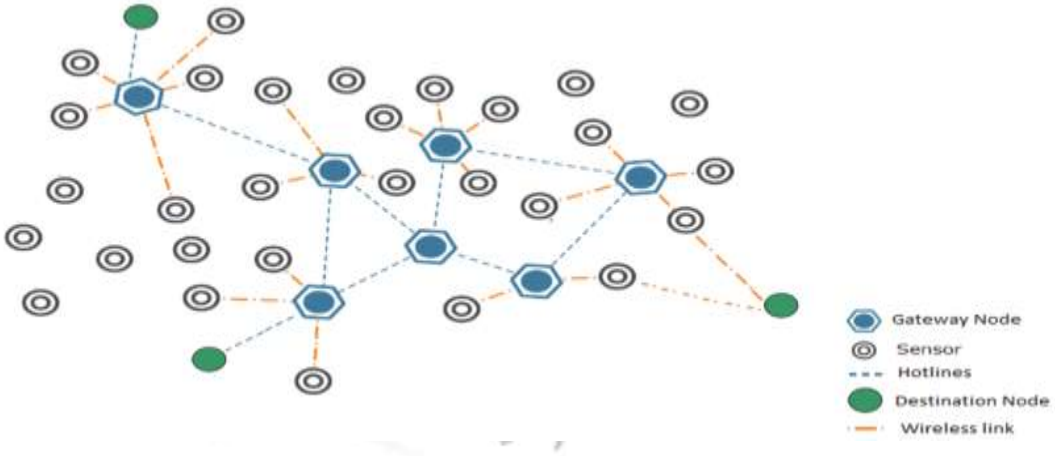


Fig 1 Wireless Sensor Network

Security in wireless sensor networks

The old network security method isn't good for sensing element networks attributable to its small computing power and limited space. A single key technique cannot complete all the demands for security as in Wireless sensor networks differing types of messages are changed having totally different demands for security. WSNs face security problems so there is a need of special key management schemes for WSNs because most of the routing protocols for WSNs liable to reasonably security threats (24).

Security Assumptions for WSN:

We make the following reasonable assumptions of the sensor network security schemes:

1. Each sensor has a different id with enough length to make difference between them.
2. BS has a node member table of node information. If a new node adds to network, its id adds to node member table.
3. BS has authentication system for any node in the network.
4. All CH in the network can reach the BS.
5. We assume that an adversary need at least time Capture to compromise a node.
6. Each exchanged message has a timestamp called "N" that guarantee the freshness of information (2).

II. LEACH PROTOCOL

LEACH was first proposed to reduce the total energy utilization in sensor networks. It is supposed that every sensor node can directly interact with a BS using a high sufficient transmitting power. By applying the clustered hierarchy, we can balance the

power utilization. Sensors send their data to particular sensors which they will be examine as cluster heads (CHs). CHs then combine all the data and send this to BS. This process helps in energy saving for nodes that are not elaborate in CHs since they can transmit with less transmission power, but at the same time we utilize the energy of CHs. To overcome this situation, LEACH proposed a dynamic CH rotation which achieve that there is a new CHs at each round. Each round, a new node will select as a CH. The network selects a new CHs using a distributed algorithm and then dynamically clustering the all nodes other than CH around the CHs. (2)

The operation of LEACH is divided into two phases:

1. Set-up phase
2. Steady state phase

In the set-up phase, the clusters are structured and cluster-heads are selected. In the steady

State phase, the actual information is send to the BS .The time period of the steady state phase is longer than the time period of the set-up phase in order to minimize overhead. During the set-up phase, a preset portion of nodes, *p*, elect themselves as cluster-heads as follows.

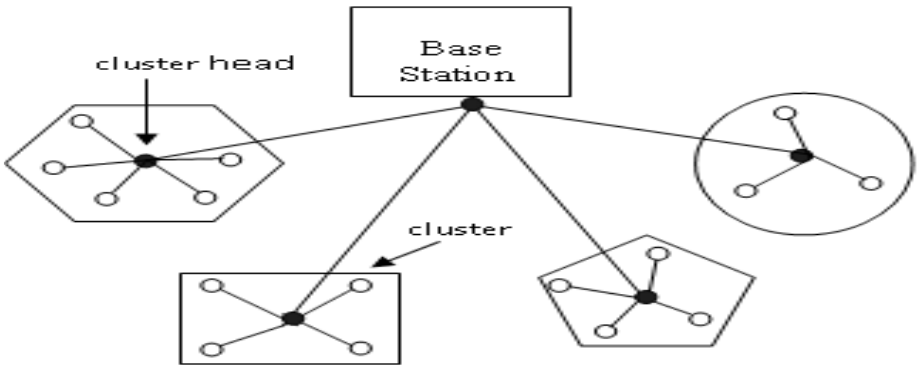


Fig.2: Clustering in LEACH

A sensor node chooses a arbitrary number, *r*, between 0 and 1. If this arbitrary number is less than a threshold value, $T(n)$, the node is selected as a cluster-head for the present round. The threshold value is computed based on an equation that organized the required percentage to become a cluster-head, in the current round, and the set of remaining nodes that have not been chosen as a cluster-head in the final $(1/P)$ rounds, denoted G.

It is given by Eqn :

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

Where G is the set of nodes that are take part in the cluster-head decision. All chosen cluster-heads broadcast an promotion message to the remaining nodes in the network that they are the new cluster-heads. All the non-cluster-head nodes, after getting this promotion message, make their own decision on the cluster to which they want to be a part. This decision is based on the signal strength of the promotion message. The non-cluster-head nodes notify the applicable cluster-heads that they will be a part of the cluster. After getting all the messages from the nodes that would like to be involved in the cluster and depend on the number of nodes in the cluster, the cluster-head build a TDMA schedule and allocate each node a time period when it can communicate. This schedule is broadcast to all the nodes in the cluster. During the steady-state phase, the sensor nodes can start sensing and broadcasting information to the cluster-heads. The cluster-head, after getting all the data, combine it before sending it to the BS .After a particular time, which is observed a priori, the network goes back into the set-up phase again and enters next round of choosing new cluster-heads. Each cluster send information using different CDMA codes to reduce obstruction from nodes related to other clusters. (6)

III. DATA ENCRYPTION STANDARD

This secret code is called cipher text. This cipher text is changed back to the original text. In this technique we encrypt the key by varying the key length. Information that can be easily understandable by the users without any special method is known as plaintext. The method which we use to enhance the security of plaintext and to hide its substance is called encryption. After Encrypting plaintext we get unreadable form of data which is known as cipher-text. The technique of getting original data back from reverting the cipher-text is called decryption. There are two techniques used for data encryption and decryption, which are: Asymmetric Cryptography: In this technique the keys used by sender and recipient to exchange the information are different keys so it is called asymmetrical or public key Cryptography. The key used for encryption is called the public key and the key used for decryption is called the private key.where as in Symmetric Cryptography same key is used by sender and recipient so it is called symmetrical or private key cryptography. It is always useful for long data streams. DES is a o symmetric block encryption algorithm. Hence we implement DES encryption in LEACH protocol to enhance the security level of leach. DES encryption use mathematical functions to change the original data into cipher text.

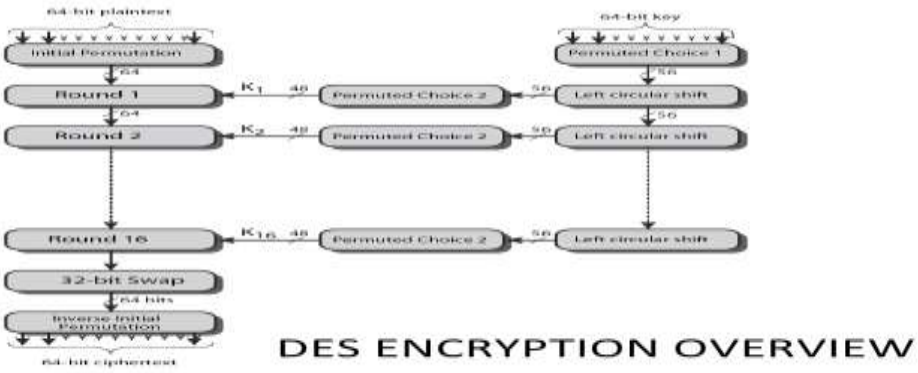


Fig 3. DES Overview

Since DES is based on the Feistel Cipher, all that is required to specify DES is –
Round function
Key schedule
Any additional processing − Initial and final permutation
Round Function: The main part of this cipher is the DES function; *f*. The DES function applies a 48-bit key to the rightmost 32 bits to generate a 32-bit output.
Key Generation: The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.
Initial and Final Permutation: The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES.

IV. RELATED WORK

Iman Almomani (2015) [7] et.al proposed two fold work. One is to experimentally analysis of the effect of existing DoS attacks on the performance of LEACH protocol, including Flooding attack, Black hole attack and Gray Hole attack will be presented. Secondly, a new type of DoS attack on LEACH called Scheduling attack will be developed. In this paper various types of attacks are performed on the leach protocol to measure the performance of leach protocol and their effects on the performance of the LEACH in terms of different terms including packet delivery ratio, network lifetime and energy consumption have been evaluated.

Roshani R. Patle (2015) [20] et.al proposed aggregated identity- based signature to transmit data securely and efficiently in clustered WSN.In this paper, the author uses two protocols which are SET-IBS and SET-IBOOS to transmit data securely and efficiently. SET-IBOOS uses Identity-Based Online/Offline Digital Signature scheme whereas SET-IBS security depends on the hardness of Diffy- Hellman problem in the pairing region.

Gurpreet Kaur (2015) [6] et al proposed secure and efficient data collection in wsn. In this paper, the author uses Data Encryption Standard scheme to enhance security in LEACH protocol. The objective of this paper is to add secret encryption scheme to the LEACH protocol. The author used the MATLAB to obtain the desired result.

Gurpreet Kaur (2015) [5] et.al proposed various key management schemes for leach in wireless sensor networks. In this paper, the author gives a brief description of wireless sensor networks and also about the leach protocol.

Yanhong Sun (2014) [25] et.al proposed a enhanced protocol for leach based wireless sensor networks. In this paper, the author proposed a SALEACH network security protocol. The benefit of using this protocol is that it consumes very less energy.

E. Sandeep Kumar (2014) [21] et.al proposed a random key distribution based artificial immune system for security in clustered wireless sensor networks.In this paper, author proposes a scheme, which uses random key distribution based Artificial Immune System (AIS) for detecting spoofing attacks. Result of this paper provide robust security an energy saving.

Meena Malik (2013) [12] et.al presents a detailed review and analysis of LEACH protocol. Comparison of various network parameters is done in the form of tables and graphs. The simulation work has been carried out by using own set of parameters and in the last of the paper conclusions is drawn**.**

Shah Kruti R (2012) [22] et.al introduces a new method to enhance the performance of the Data Encryption Standard (DES) algorithm. This is done by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0, 1). This replacement adds a new level of protection strength and more robustness against breaking methods.

Pengcheng Zhao (2012) [18] et.al According to the weakness of session key construction based on node's own location, the authour propose a hybrid key man-agement scheme which based on clustered wireless sensor networks. The use of hierarchical thinking, reducing the amount of key storage and computing, while supporting network topology, dynamic key management for which aims to prevent leakage. Through analyzing, it shows that the scheme have certain advantages in key connectivity, security, communication and energy consumption.

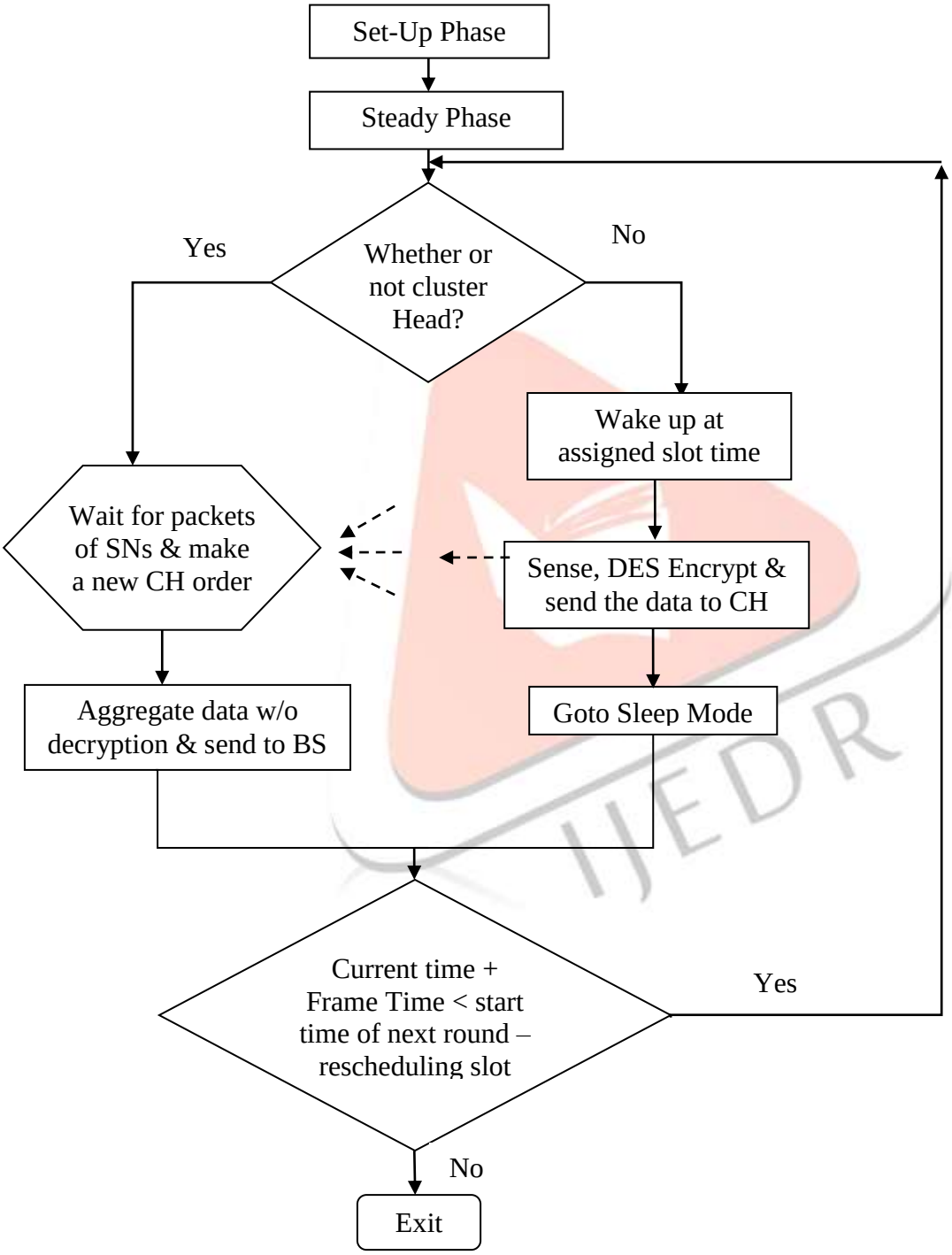
Ms. Parul Tyagi (2012) [17] et.al In this paper, author analyze recent routing protocols for wireless sensor network and classify in three types of approaches according to network architecture in WSN.The three main categories on the basis of network structure: Flat, Hierarchical and location based routing protocols. The author study tradeoff between energy and communication overhead savings in every routing protocols. This paper also highlighted the advantages and performance issues of each routing technique**.**

V. PROPOSED WORK

In the earlier days Security enhancement of information is very difficult task we have a lot of security techniques that are implemented but out of them few techniques are serving the needs of society. There is no algorithm which is perfect and overcome from all the problems. The main motivation of any encryption algorithm must be security from harmful attacks. As the data in both the private and public sectors are increased this requires Accessibility, verification, privacy, Integrity. So we are using DES algorithm to enhance the security of the leach protocol.

- Study of LEACH protocol
- Implementation of DES encryption with LEACH to enhance the security of data.
- Compare the results in MATLAB using LEACH protocols with and without DES Encryption.

Hence we implement DES encryption in LEACH protocol to enhance the security level of leach. DES encryption use mathematical functions to change the original data into cipher text. The proposed algorithm steps are depicted in flowchart below:

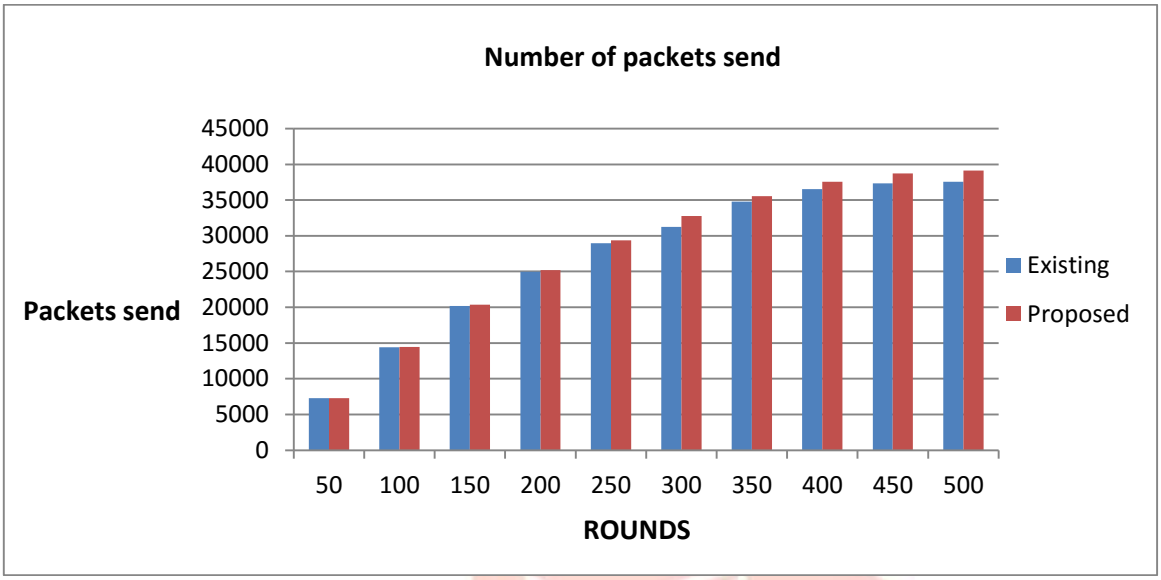


VI. SIMULATION RESULTS

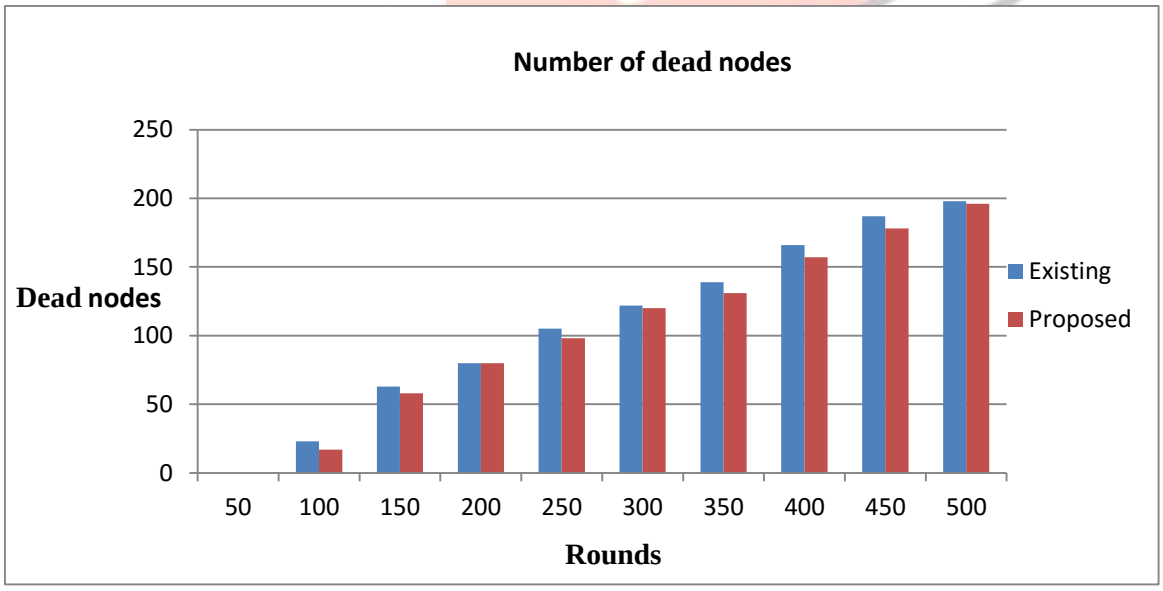
Performance of proposed work in which DES algorithm is applied on the leach is compared with the previous work. In this we a network which contain 200 nodes and the area of the network is 100m*100m and the location of the BS are (50, 175). Maximum no of rounds in network model is 1000. To perform this work mat lab is used. Table shows parameters of the network.

To compare the performance of the existing and proposed work we use three parameters which are: Dead nodes, no. of packets send, total energy used. Following table and graphs shows the comparison between existing and proposed work when nodes are 200.
We use three performance matrices to compare our results which are: packets send, no. of dead nodes, Energy. The following graph shows the no. of packets send. Performance of the existing and proposed work is measured up to 500 rounds. No. of packets send in proposed work are higher than existing work.

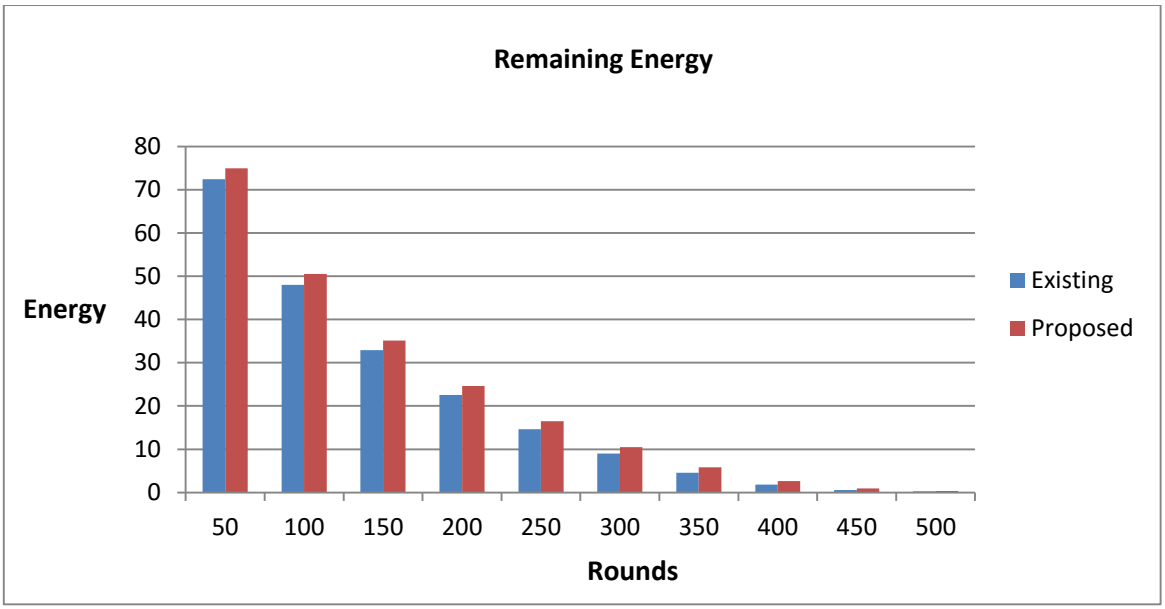
Total Number of packet Send:
This figure shows the total no. of packets send at different number of rounds.



Number of Dead nodes
This graph shows the no. dead nodes. Performance of the existing and proposed work is measured up to 500 rounds. No. of Dead nodes in proposed work are lower than existing work.



Total Remaining Energy:
This figure shows that when an encryption technique is applied total remaining energy of nodes increased.
So that they can perform function without consuming more energy.



VII. CONCLUSION

In this paper, we apply Data encryption standard on leach protocol to enhance the security of the leach protocol. We performed simulation in matlab. In our work we consider three matrices which are number of packets send, number of dead nodes, and energy. At different numbers of rounds different calculations have been taken to compare the working of existing leach with the proposed leach. When we take 200 nodes and probability is 0.5 then number of packets send in proposed work is 3.915e+004 whereas in existing leach it is 3.758e+004.Dead nodes are 198 in existing work whereas 196 in proposed work. Remaining Energy is 0.259 in existing work whereas 0.3218 in proposed work. This shows that after applying DES algorithm on Leach protocol the results are enhanced. we get the better result on applying DES algorithm on Leach and after varying the key length.

References

[1] Abdoulaye Diop, Yue Qi, Qin Wang et al, " Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks", I.J. Computer Network and Information Security, 2014, 8, 9-18.
[2] Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain et al, "An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks", International Journal of Computer and Communication Engineering, Vol. 1, No. 4, November 2012.
[3] Ajay jangra, Amisha Dhiman et al, **"** A Review on Low Energy Adaptive Clustering Hierarchy (LEACH) Routing Protocol in WSN", Volume 3, Issue 6, June 2013,IJARCSSE.
[4] Baiping Li**,** Xiaoqin Zhang et al, "Research and Improvement of LEACH Protocol for Wireless Sensor Network", 2012 International Conference on Information Engineering Lecture Notes in Information Technology, Vol.25.
[5] Gurpreet Kaur*, Navdeep Kumar et al, " Secure and Efficient Data Collection in WSN", Volume 5, Issue 5, May 2015, IJARCSSE.
[6] Iman Almomani, Bassam Al-Kasasbeh et al, "Performance Analysis of LEACH protocol under Denial of Service Attacks", ©2015 IEEE.
[7] Jaydeepsinh Barad, 2Bintu Kadhiwala et al, " Comparative study on dynamic key-management techniques for cluster-based sensor networks", © 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939.
[8] Jianli Wang, Laibo Zheng, Li Zhao, and Dan Tian et al, "LEACH-Based Security Routing Protocol for WSNs" ,© Springer-Verlag Berlin Heidelberg 2012.
[9] Lein Harn and Changlu Lin et al, "Authenticated Group Key Transfer Protocol Based on Secret Sharing", 2010 IEEE.
[10] Leonardo B. Oliveira, Hao C. Wong, M. Bern, Ricardo Dahab, A. A. F. Loureiro et al, "SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks", Supported by FAPESP under grant 2005/00557-9.
[11] Meena Malik1, Dr. Yudhvir Singh2 , Anshu Arora3 et al, " Analysis of LEACH Protocol in Wireless Sensor Networks", Volume 3, Issue 2, February 2013.
[12] Mohammed A. Abuhelaleh and Khaled M. Elleithy et al, "SECURITY IN WIRELESS SENSOR NETWORKS: KEY MANAGEMENT MODULE IN SOOAWSN", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010
[13] Namdeep Singh1, Er. Jasvir Singh2 et al, " A SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS", Volume 4, No. 7, July 2013**,** Journal of Global Research in Computer Science.
[14] Neha Mehndiratta, Manju, Harish Bedi et al, " Wireless Sensor Network LEACH Protocol: A Survey", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-3).
[15] Parul Bakaraniya#1, Sheetal Mehta et al, "**K-LEACH: An improved LEACH Protocol for Lifetime Improvement in WSN", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5- May 2013.**
[16] Ms. Parul Tyagi, Ms. Surbhi Jain et al, "Comparative Study of Routing Protocols in Wireless Sensor Network", Volume 2, Issue 9, September 2012.
[17] Pengcheng Zhao, Yong Xu, Min Nan et al," A Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks", Copyright © 2012 SciRes.

[18] Prashanti.G, Deepthi.S, Sandhya Rani.K, "A Novel Approach for Data Encryption Standard Algorithm" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.