Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Energy Efficiency Routing of Wireless Sensor Networks Utilizing Particle Swarm Optimization and LEACH Protocol

Akhila B Badni
Dept. of Computer Science and Engineering, SKSVMACET, Lakshmeshwar, India

Nivedita A Tippshetti
Dept. of Computer Science and Engineering, SKSVMACET, Lakshmeshwar, India

Mallikarjungouda B Patil
Dept. of Computer Science and Engineering, SKSVMACET, Lakshmeshwar, India

Shrikumar R Havaragi
Dept. of Computer Science and Engineering, SKSVMACET, Lakshmeshwar, India

Mr. Basavaraj K Muragod
Dept. of Computer Science
Assistant Prof. SKSVMACET, Lakshmeshwar, India

Abstract— WSN contains of a substantial quantity of little Associate in Nursing restricted power sensing element parts that are at random or physically sent over an unattended target region. WSNs have potential applications in atmosphere perceptive, bad luck cautioning frameworks, medicative services, security police work, and intelligence frameworks. the most disadvantage of the wireless sensing element network is that the restricted power sources of the sensing parts. Increasing the period of the Wireless sensing element systems, energy preservation measures are important for enhancing the execution of WSNs. This paper proposes LEACH-P that may be a novel approach to enhance existing LEACH protocol victimization PSO primarily based bunch. The projected algorithmic program is simulated loosely and also the results are compared with the present algorithmic program to see its control in terms of network period, stability amount and range of knowledge transmitted to the bottom station.

Index Terms—Wireless Sensor Networks (WSN), gateways, Cluster Head (CH), Particle Swarm Optimization.

I. INTRODUCTION

Wireless device Networks are having giant network within which the huge quantity of device nodes are the gift that are forming a network with their self-organizing property. The range of applications include health care, military, crucial infrastructure protection, and non-military personnel e.g., disaster management. In WSN the little device nodes are classified by restricted process power sources. during this manner, energy preservation of the sensors is that the most tightened concern for the long-standing time method of WSNs. various problems are contemplated for this reason that embrace low-power radio facility, power-aware medium access management (MAC) layer conventions so on. Therefore, energy economical cluster and routing procedures are the foremost encouraging regions that are contemplated wide in such manner. In an exceedingly two-level WSN, sensing components are partitioned off into many teams that are referred to as clusters. Each cluster features a pioneer known as cluster head (CH). All of the sensors sense neighborhood data and transmit it to their relating CH. At that time, the cluster heads mix the native data and so transmit it to the bottom station (BS) specifically or by suggest that of various CHs. A cluster-based mostly model of wireless device network. Cluster sensors have numerous benefits that are as follows: (1) It empowers data total at CH to get rid of the repetitive and unrelated information; consequently, it saves power of the sensing components. (2) Routing will be all the additional effectively achieved on the grounds that solely CHs got to maintain the close path started of various CHs and afterward need very little steering data; this successively enhances the ability of the system basically. (3) It preserves correspondence transfer speed because the device nodes communicate with their CHs solely and thus keep one's hands off from trade of excess data among them. Tragically, the gateways are likewise battery-worked and consequently, energy forced. Period of time of the gateways is exceptionally important for the long-standing time operation of the system. The transmission energy (E) connected with distance (d) on the premise of the following formula, i.e. E d λ ,where wherever is that the path loss exponent and a pair of and a pair of (Habib & Sajal, 2008) . During this method, the step-down of transmission separation will decrease the energy utilization. In any case, many applications are extraordinarily time-basic in nature. Afterward, they got to fulfill strict delay constraints so the SB will get the detected data inside a planned time sure. In any case, the delay is relative to the number of forwards on the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

dissemination path between supply and also the sink. With a selected finish goal to limit the delay, it's necessary to limit the number of forwards, which may be accomplished by boosting the separation between continuous forwards. In these lines, whereas outlining routine procedures we've got to fuse associate degree exchange off between transmission separation and amount of forwards as they stance 2 incompatible destinations. Moreover, load equalization is another crucial issue for the WSN cluster. Especially, this is often a drag that has to be self-addressed once the device nodes don't seem to be disseminated systematically. During this paper we tend to address the related to issues:

Energy expert routing with associate degree exchange off between transmission distance and range of data forwards.

Energy expert load-balanced grouping with energy preservation of the WSN.

Keeping in mind the top goal to amass a faster and expert arrangement of the cluster and routing issue with the on top of problems, a metaheuristic approach, for instance, particle swarm improvement (PSO) is extraordinarily enticing. The first goal of this paper is to boost existing LEACH with an efficient PSO-based cluster for WSNs with the thought of energy utilization of the device hubs for extending system lifetime.

II. PROBLEM STATEMENT

Our approach aims to balance the tradeoff between the energy consumption and security improvisation in Wireless sensor networks.

III. RELATED WORK

WSN finds its applications in various fields like military, forests and homeland. The WSN have many mission-critical tasks. Security is crucial in such net works. Providing security in WSN is difficult due to the resource limitations of WSN. There is always a conflict between resource consumption and security maximization. Overall cost of WSN should be as low as possible and also security must not be compromised. To achieve that we came up with an approach named non-redundant XOR technique. A Symmetric and an Asymmetric algorithm have been used for the comparison purposes. AES is the most popular Symmetric and RSA is the most popular Asymmetric algorithm.

The following section describes each algorithm briefly.

1. AES (Advances Encryption System) is an Iterative symmetric key encryption algorithm. Main operations performed in this technique include sequence of substitutions and permutations. It represents the text in terms of bytes rather than bits [6]. It is used for the encryption of either 12 or 14 or 32 bytes. It uses 10 rounds for 12 byte keys, 12 for 14 byte keys and 14 for 32 byte keys. The encryption and decryption processes are inverses to each other making the algorithm symmetric. It is the replacement of DES (Data Encryption Standard) against which potential attacks proved to be successful. The built-in future proofing feature makes exhaustive search incapable of cracking the key. The amount of security provided is dependent on the way how the symmetric key management is done.
2. RSA is one of the first public key encryption systems. Since it is an Asymmetric encryption key algorithm, it has two keys, private key and public key. Here the public key is shared with the BS and the private key is kept with the sensor node itself. This Algorithm represents the text in terms of bits [7].
   1) Encryption Function: It is the function used for converting the plain text into the cipher text and the cipher text can be decrypted only with the help of private key.
   2) Key Generation Function: Cracking the private key from a public key is as much difficult as factoring the product of two large prime numbers. An attacker cannot crack the private key unless the factoring is done. There exists no inverse to this function i.e. it is an one-way function. As, the key length increases, the security increases and becomes difficult for the attacker to crack the private key. The sensor node encrypts the data before transmitting to the next hop. Once encrypted and transmitted, the decryption takes place at the Base Station.
   3) Redundant XOR technique: This technique uses asymmetric key cryptography. The architecture, constraints and limitations involved in WSN are far different from the real life computer networks. Hence, not all security algorithms can be used in WSN as many of them do not meet the energy and storage limitations. Thus we chose XOR operation as the base of our security algorithm which is the least complex operation that can be performed in least time. Encryption of data takes place at WSN where as decryption is done at BS. Each node is assigned with a unique number from 1 to N (number of nodes). There will be two keys used in this technique. One key is a dynamic one which is generated once in each round, as the intruder cannot crack the key and even if cracked, he cannot use the same key again. The second key is a static/fixed one assigned to every node and it is constant in every round. First, the sensed data by the node is encrypted with the dynamic key by performing XOR operation between the data and dynamic key. The result obtained is again encrypted with the corresponding static key which was previously assigned. This final double encrypted data is transmitted to the BS (Base Station) with the help of intermediate hops where encryption is not performed.

      The algorithm can work in two cases:

      1) Number of encryptions is fixed: In this case, while deploying the nodes in the WSN environment, all the nodes are assigned numbers sequentially from 1 to N (Number of Nodes). Whenever a node senses the data in its vicinity, it encrypts the data same number of times as given to it during deployment. For example, if the node which is numbered one senses data, it encrypts the data only once and if the node number is 29,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

it encrypts the data 29 times before transmitting the data. These numbers which are assigned to the nodes remain constant until the life time of the entire network.

2) Number of encryptions are random: In this case, for every round, number of times of encryption is chosen randomly to be a value that is either less than half of the number of nodes or quarter of the number of nodes. i.e. the number chosen is either between [1 and N/2] or [1 and N/4]. Hence, the average number of times encryptions performed in this case are less than that of the first case. Also, finding number of encryptions is difficult as it keeps on varying for every round at each node. Hence, this case provides more security than that of the first case. Both the cases use only two keys and it is a low storage cryptographic technique.

IV. METHODOLOGY

In this technique we first encrypt the data with dynamic key once and then we encrypt the encrypted data with static key k times where k in first case is node number. In the second case, encrypted data is encrypted with static key k times where k is a random number generated between 1 and N/2 (N/4). In both the cases we are encrypting the encrypted data repeatedly with the same static key. Performing XOR operation on some data D repeatedly with same key even number of times will yield to D itself. Similarly performing XOR operation odd number of times would yield to D1 where D1 is equivalent to performing XOR operation only once. To overcome the drawback we came up with an algorithm named non redundant XOR technique. In the proposed algorithm, we first encrypt the message with the static key. Then encrypt the encrypted data with the dynamic key k times where k is the node number. The proposed approach varies with the existing XOR redundant technique in terms of frequency of key change i.e. each iteration of k iterations dynamic key is changed so that we can get different encrypted data in each iteration (Equation 1).

$$\text{DynamicKey} = (\text{DynamicKey} + k) \bmod (2^m - 1) \quad (1)$$

where, m is number of bits in key k is node number. Thus we are removing the redundancy from the above algorithm so that we can get different encrypted messages in each round. The complete algorithm is explained. Two variants of the non redundant XOR techniques are proposed to make the network more secure.

1) Dynamic Key Position Placement: Here position of dynamic key is P where P is generated randomly between two and length of the message and key is kept in that position. This position P is kept at the starting of the message. Base station checks start of the message retrieves P from the message, goes to the position P to extract the dynamic key and hence decrypt the encrypted data.
2) Encrypting Dynamic Key: Dynamic key is encrypted with a new key which is generated randomly. This encrypted dynamic key is sent with data along with the second dynamic key which is used to encrypt the dynamic key. The positions of encrypted dynamic key and second dynamic key can be static which is known to BS or the positions can be changed dynamically using dynamic key position placement method.

Leach protocol:

Leach protocol is the oldest protocol in wsn, it is to minimize the energy consumption it is done by electing the cluster heads among the sensor nodes and sends the data to its closest reachable cluster head. Cluster head responsibility is to transmit data to the base-station.

Step1: In this cluster heads are elected by a stochastic probability Algorithm.

Step2: Each cluster head advertises its availability to other surrounding sensor nodes.

Step3: Each sensor node associated with one of the cluster head using received signal strength and it is directly proportional to distance between the nodes in an optimistic environment.

Step4: In each round the cluster head initiates time division multiple axis for each of the sensor node and sends the corresponding data.

Step5: This protocol balances the energy consumption among the network node.

Drawbacks of leach:

A few of those assumptions area unit as per the following:

- All nodes will convey with adequate power to achieve the bottom station if necessary.
- Nodes faithfully have data to send.
- Nodes found a close to one another have connected data. It's not evident what number preset CHs area unit planning to be uniformly disseminated throughout the system. Therefore, there's a clear stage that the chosen CHs are going to be centered in one a part of the system. Later, some nodes won't have any cluster head nearer to them.
- CHs area unit chosen haphazardly in LEACH, thus nodes with less vitality may be picked up, and that may lead to those nodes die too fast.

Particle swarm optimization:

Particle Swarm optimization (PSO) is inspired by natural lifecycles, like bird flocking, fish schooling, and discretionary search techniques of organic process procedure (Kennedy & Eberhart, 1995) (Wei & Nor, 2014). It will be seen from the character that creatures, particularly winged animals, fishes, etc. invariably travel along in a very random seek for food in a very cluster while not colliding. it's as a result of each member tracks the cluster by modifying its position and speed utilizing the cluster-info. So it decreases individual's labor for trying of nourishment, shelter than on. PSO includes of a swarm of a predefined size (say NP) of particles. Every component provides a whole answer to the three-d optimisation issue. The dimension D of the wide range of particles is equal. A particle Pi, one $\leq$ i $\leq$ NP has location Lid, one $\leq$ d $\leq$ D, and speed Vid within the dth dimension of the hyperspace. The

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

equation for illustrating the ith particle Pi of the residents as follows: Pi = [(Li,1), (Li,2), (Li,3) , (Li,D)].

Every particle is calculable by a fitness operate to gauge the prevalence of the answer to the matter. to attain the world best position, the particle Pi monitors its individual best, i.e., personal best known as Pbesti and world best known as Gbest to update its individual position and speed. In each repetition, its position Xid and speed Vid and within the dth dimension is changed utilizing the incidental conditions.

$$V_{i,d}(t) = w * V_{i,d}(t-1) + k1R1 * (Lpbesti,d - L_{i,d}(t-1)) + k2R2 (Lgbestd - L_{i,d}(t-1))$$

$$L_{i.d}(t) = L_{i,d}(t-1) + V_{i,d}(t)$$

where w = mechanical phenomenon weight k1 and k2 = non-negative constants known as acceleration issue R1 and R2 = 2 completely different systematically disseminated discretionary numbers within the vary [0,1]. The changed procedure is iteratively recurrent till either a suitable Gbest is earned or a hard and fast range of iterations t Georgia homeboy is achieved.

Leach-PSO Algorithm

These are the steps involved in this below algorithm:

Step1: Select the number of nodes and select the probability. Step2: Define the network area.

Step3: Compute the probability, with the number of P rounds. Here P is the decide percentage of cluster head to be selected in each round.

Step4: The energy is calculated using Euclidean distance.

Step5: Apply the PSO (Particle swarm optimization) Algorithm.

Step6: Obtain the global best path from cluster head to the base station.

Step7: Nodes which are not in cluster head will send data to the closest cluster head.

Step 8: Cluster head aggregates data.

Step 9: Aggregated data is send to the base station by cluster head using global best path.

Step10: Desipiate the energy from cluster head and non-cluster head.

Step11: If the energy of a node is less than the minimum probability values than make it as dead.

Step12: Compute the number of dead nodes and plot the result.

Proposed (Leach-PSO) Algorithm

The simulations are performed using matlab tool for different architecture for a simple leach protocol and leach-PSO protocol having 50,100,150,200,250,300,350,400,450,500 sensor nodes. The Leach-PSO protocol has performed better than the leach. The number of dead nodes or round, total energy or round and the number of packets sent to the base station are used for the comparing the Algorithm.

PSO algorithm is used to reduce the energy consumption of life time of wsn network and it is done by multi-hopped shortest path from the sensor node to the base station .It is used to update the new path generated as a priority queue of each particle (node) updated in each iterations which gives the corresponding cost function.

V. EXPERIMENTAL RESULTS

Upon executing the program without any warnings we got the following outputs.

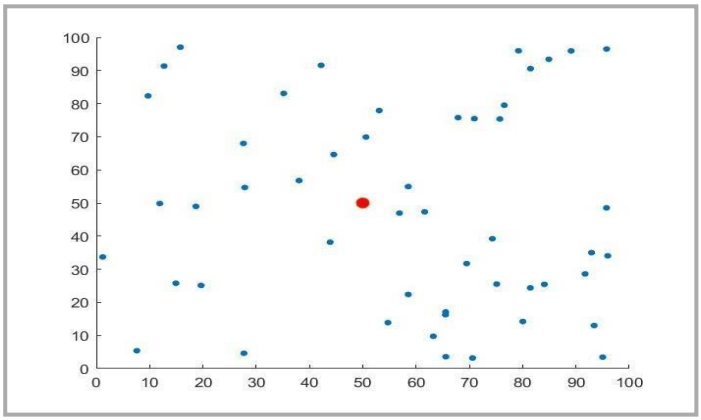

Fig.1.1 50 unit nodes deployment in 100*100 graph

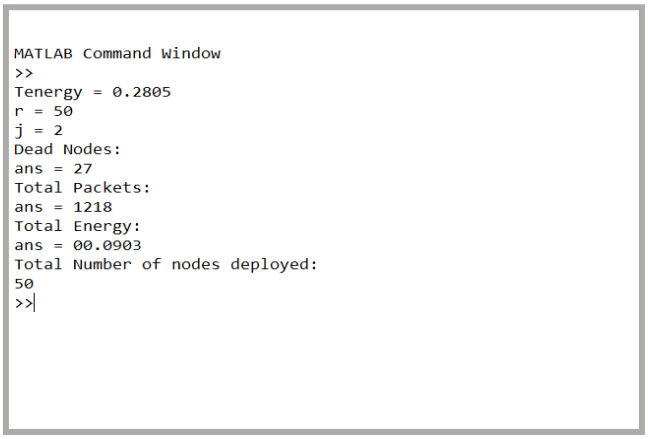

Fig.1.2 Results on MATLAB cmd Window

- Here 50 WSN nodes are deployed in 100*100 graph area in the above pictures (Left) and they are deployed using the Proposed Method.
- The 1st set of results are conducted with 50 nodes and 50 rounds of iterations, which finally gave the output results.

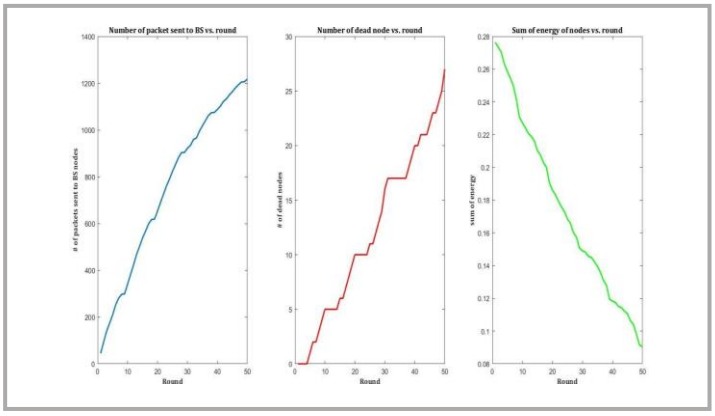

Fig.1.3 Graphical representation of Transmissions, Dead Nodes and Sum of energy vs round

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

- Upon viewing the results we can understand that compared to Previous Protocol this improvisation gives the better results, as we can see that even after 50 iterations there are still 23 nodes are alive and they are not completely depleted.

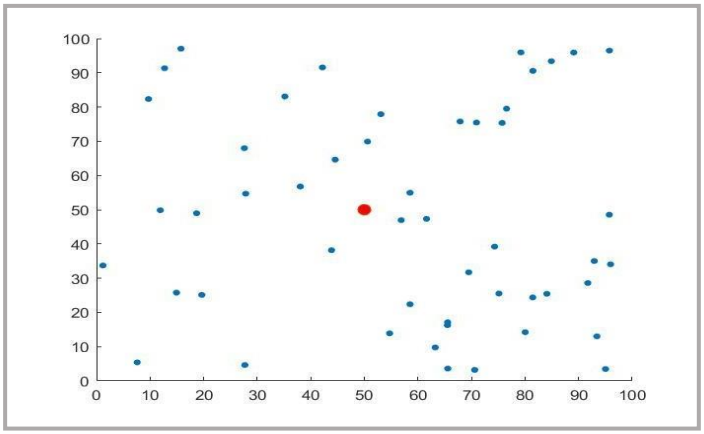

Fig.2.1 100 unit nodes deployment in 100*100 graph

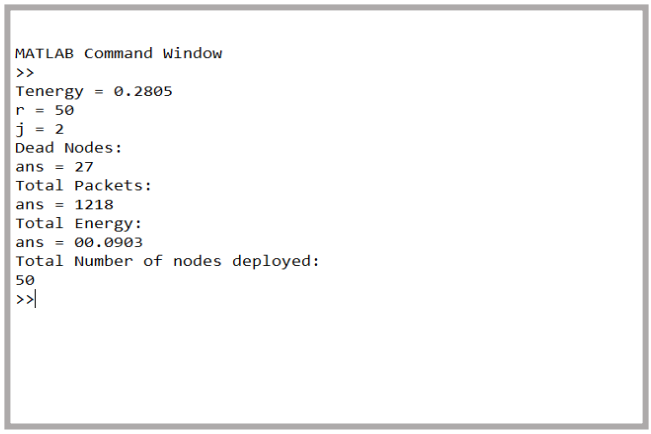

Fig.2.2 Results on MATLAB cmd Window

- Here 100 WSN nodes are deployed in 100*100 graph area in the above pictures and they are deployed using the Proposed Method.
- The 2nd sets of results are conducted with 100 nodes and 50 rounds of iterations. Which finally gave the output results

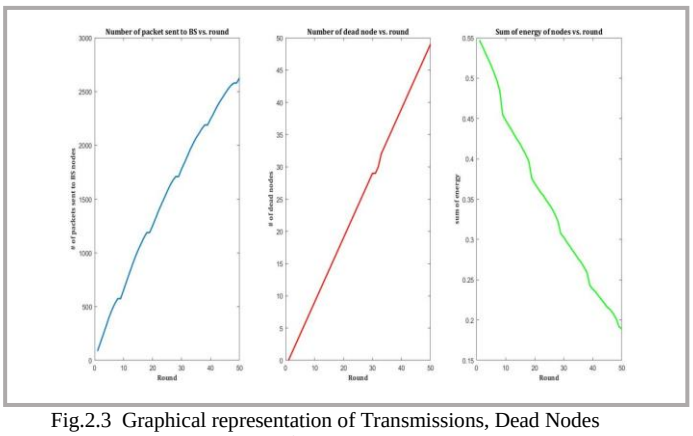

Fig.2.3 Graphical representation of Transmissions, Dead Nodes and Sum of energy vs round

- Upon viewing the results we can understand that compared to simple LEACH Protocol this improvisation gives the better results, as we can see that even after 50 iterations there are still 51 nodes are alive and they are not completely depleted.
- Every transmission energy is shown in the results as Tenergy, as in this case Tenergy=0.555 J.

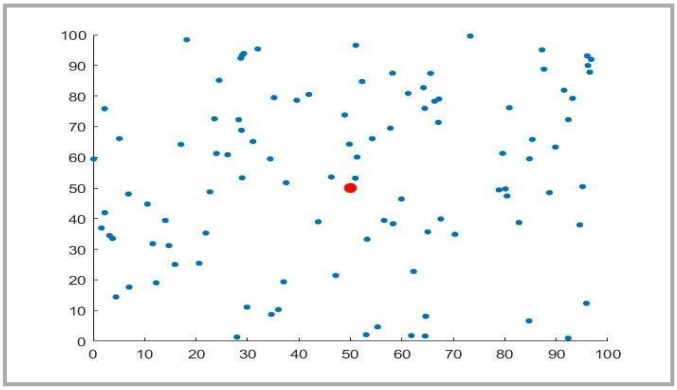

Fig.3.1 150 unit nodes deployment in 100*100 graph

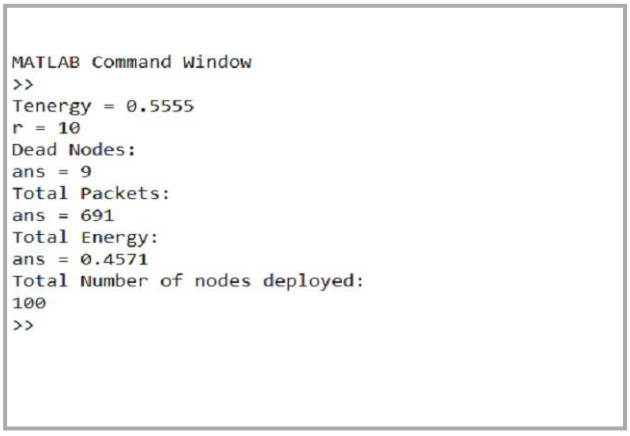

Fig.3.2 Results on MATLAB cmd Window

- Here 100 WSN nodes are deployed in 100*100 graph area in the above pictures (Left) and they are deployed using the Proposed Method.
- The 5th set of results are conducted with 100 nodes and 10 rounds of iterations. Which finally gave the output results

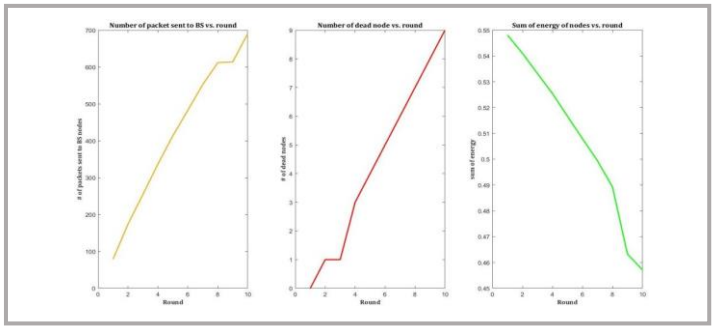

Fig.3.3 Graphical representation of Transmissions, Dead Nodes and Sum of energy vs round.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

- Upon viewing the results we can understand that compared to simple LEACH Protocol this improvisation gives the better results, as we can see that even after 10 iterations there are still 91 nodes are alive and they are not completely depleted.
- Transmission energy for this set is Tenergy = 0.5555 J.

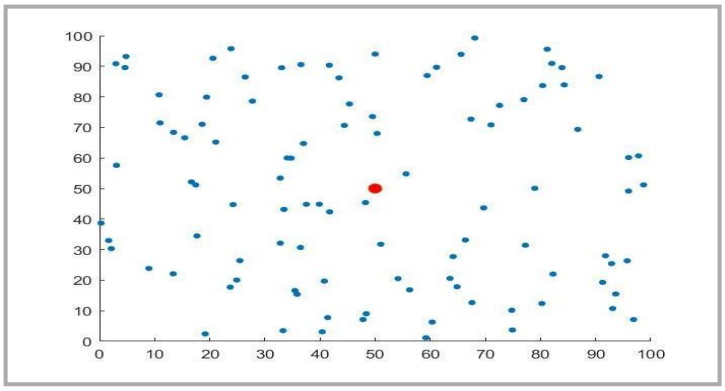

Fig.4.1 100 unit nodes deployment in 100*100 graph

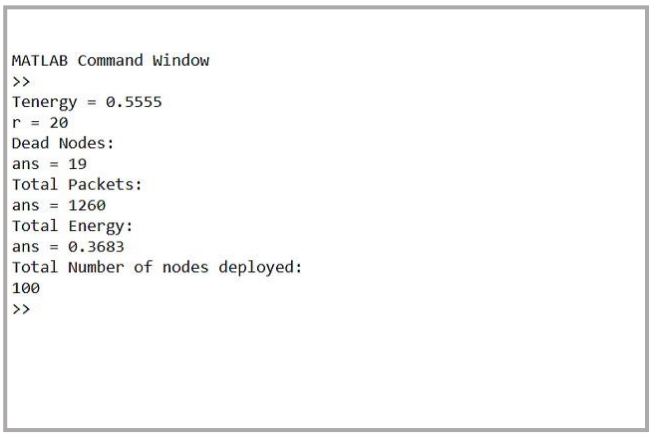

Fig.4.2 Results on MATLAB cmd Window

- Here 100 WSN nodes are deployed in 100*100 graph area in the above pictures (Left) and they are deployed using the Proposed Method
- The 6th set of results are conducted with 100 nodes and 20 rounds of iterations. Which finally gave the output results

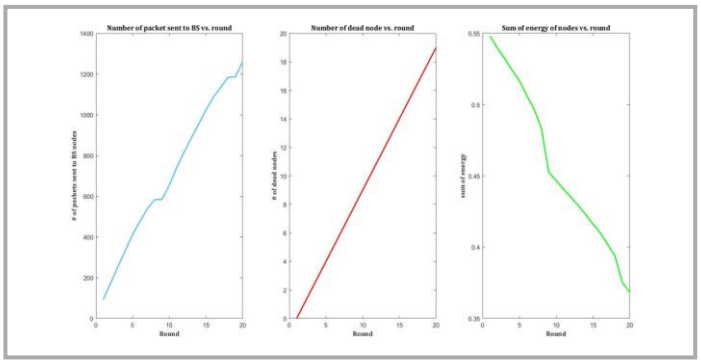

Fig.4.3 Graphical representation of Transmissions, Dead Nodes and Sum of energy vs round

- Upon viewing the results we can understand that compared to simple LEACH Protocol this improvisation gives the better results, as we can see that even after 20 iterations there are still 81 nodes are alive and they are not completely depleted.
- Transmission energy for this set is Tenergy = 0.5555 J.

CONCLUSION

Secure knowledge transmission in WSN has become one of the foremost active analysis areas for several years. The projected study developed a unique model of security paradigm particularly N-MSP which may perform economical, secure hash familiarized message authentication in associate degree energy-efficient manner. The projected technique most adheres to the options of HMAC primarily based SHA-1 to demonstrate each sensing element message before playacting knowledge aggregation on this. The obtained outcomes once simulating the projected HMAC during a} numerical computing simulation tool exhibit its effectiveness in achieving very less interval and energy consumption. It conjointly archives the optimum trade-off between energy and security. Moreover, the study ensures its extensibility in art movement sensing element applications. during this section, we tend to examine the improved protocol through NS2. A network of one hundred nodes is deployed in a section of one hundred m × one hundred m with SB at (50, 175). Several procedures are projected with totally different objectives for WSNs. a significant aim of most of those procedures is to unfold the service lifetime of the network by reducing the speed of energy ingesting by the nodes. This project projected associate degree formula that initial assumption that each one the nodes within the network ar low- steam-powered, and these nodes have the potential to pick out a CH. The network simulation was performed for various eventualities as shown in table (ex: two hundred nodes {in a|during a|in associate degree exceedingly|in a very} two hundred x two hundred money supply network) that showed an improved network performance victimization the urged improved (or Hybrid) LEACH formula during this project to schedule the active time of the network nodes. the choice of the CH within the projected LEACH protocol is completed in every spherical supported their energy state. this method of cluster head rotation in every spherical has not been thought-about by any study prior to now as most of the present studies recommend changes within the ranges of the CHs whereas the clusters stay unattended.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

REFERENCE

[1] Lewis F 2004 Wireless Sensors Networks, good Environments: Technologies, Protocols, and Applications Cook DJ, Das SK, John Wiley, NY 1-18.

[2] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Proceedings of the thirty-third Annual Hawaii International Conference on System Sciences, 2000, pp. 10. vol.2.

[3] M. Z. Hasan, H. Al-Rizzo; F. Al-Tudjman, "A Survey on Multipath Routing Protocols for QoS Assurances in period Wireless transmission sensing element Networks," in IEEE Communications Surveys & Tutorials, No.99, pp.1-1, 2017.

[4] B.E. Manjunath and P.V. Rao, "Trends of Recent Secure Communication System and its Effectiveness in Wireless sensing element Network" International Journal of Advanced applied science and Applications (IJACSA), Vol.7(9), pp131-139, 2016.

[5] A.K.Das, R.Chaki, and K.N.Dey, "Secure energy-efficient routing protocol for the wireless sensing element network," Foundations of Computing and call Sciences, Vol. 41, No. 1, pp.3-27, 2016.

[6] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," Network unit, Request for Comments, 2014 • Manjunath.B.E and Dr.P.V.Rao, "Balancing Trade-off between knowledge Security and Energy Model for Wireless sensing element Network" International Journal of Electrical and laptop Engineering (IJECE) Vol. 8, No. 2, April 2018, pp. 1048~1055.

[7] International Journal of Innovative analysis in laptop and Communication Engineering Vol.2, Special Issue one, March 2014 by K.SyedAliFathima, T.Sumitha.[1]

[8] International analysis Journal of Engineering and Technology Vol.4 Issued on seventh July 2017 by Miss.Divya Garg, Dr.Pradeep Kumar, and Miss.Kapal. [2]

[9] 2nd International Conference on electronics and telecommunication engineering 2018 by K.Jayashankar Reddy, K.Karthikeya Yadav, and BKSP Kumar.

[10] D. high dudgeon and R. Mersereau. three-dimensional Digital Signal process, chapter 6. Prentice-Hall, Inc., 1984 • D. Hall. Mathematical Techniques in Multisensor knowledge Fusion. Artech House, Boston, MA, 1992.