An Implementation of an Energy Efficient and Secured Algorithm to Increase Network Lifetime in Wireless Sensor Network

Apeksha Adulkar[1], Ayushi Evaney[1], Deeplaxmi Babde[1], Shwetal Warhade[1], Preeti Karmore[2]

[1]*UG Students, Department of Computer Science Engineering, Dr. Babasaheb Ambedkar College of Engineering and Research, Nagpur, Maharashtra, India.*
[2]*Assistant Professor, Department of Computer Science Engineering, Dr. Babasaheb Ambedkar College of Engineering and Research, Nagpur, Maharashtra, India.*

Abstract

Wireless sensor networks contain a far-reaching number of appropriated sensor contraptions, which are related and created through multi-hop guiding. To make use of the optimal lifetime in Wireless Sensor Networks (WSNs) the ways for information move are picked in a way that the aggregate vitality used along the way is limited. To help high versatility and better information aggregation, sensor nodes are consistently gathered into disjoint, non-covering subsets called clusters. Clusters make progressive WSNs which join proficient usage of restricted assets of sensor nodes and subsequently expands organize lifetime. The objective of this paper is to demonstrate a bleeding edge audit on clustering calculations announced in the writing of WSNs. This paper presents different vitality proficient clustering calculations in WSNs.

Keywords— *Clustering, Load balancing, Fault Tolerance, Latency, Data Aggregation, LEACH, PEGASIS, TEEN, HEED*

INTRODUCTION

Many advances in sensor technologies have been made in recent years, bringing new opportunities for many applications where they are deployed, such as military and medical surveillance. Wireless Sensor Network (WSN) consists of a large number of sensor nodes deployed in a hostile environment and self-organized for collecting and transmitting field data to a Base Station (BS). These networks are dispersed in an inaccessible area simulation.

Sensor nodes consume energy when data is received, processed and transmitted. Based on this criterion, and due to the limited power supply of the sensor nodes, the most important issue is energy efficiency, and to extend a WSN's lifetime, node energy needs to be used efficiently and in a good way. This is the common objective of the existing algorithms for clustering.

Nodes are grouped into small partitions called clusters in a WSN. In each cluster we define a Cluster Head (CH), also called a leader with the task of aggregating the data from the cluster's other nodes and then transmitting them to the sink. In order to reduce energy consumption, previous research suggested considering certain parameters of the WSN such as residual energy. In order to divide the entire network into several clusters, some of the algorithms involve cluster management, which consists of defining the appropriate number of clusters, dividing the surface into equal area regions that will be considered clusters or using spectral clustering K clusters using Euclidean distances of points to be clustered.Other protocols use a random number to select the cluster heads with the intention of balancing the energy consumption of the sensor nodes across the networks. Many existing WSN results use intra-cluster multi-hop communication to design a data relay tree for each cluster. These protocols aim to reduce the

number of transmitted packets and save energy, but they rarely consider other important criteria that are distances separating nodes, distance to BS, and control of density. All of these criteria help extend the WSN's lifetime, which is the biggest issue.

In this paper we introduce a new clustering protocol to extend the WSN's lifetime. A distributed competitive algorithm is this proposed approach called Energy Efficient Density Control Clustering Algorithm for Wireless Sensor Network. It chooses CH through three parameters: energy, density, and node distances from base station. Unlike CHs, all nodes enter a competition for energy and density based on the choice of CH. This choice is based on a random number in each round generated by the nodes. Each node must test its residual energy with the neighboring nodes ' residual energy in our algorithm. This range is the same for all nodes implemented in the area as opposed to the where the range decreases as their distance to the base station decreases.

In existence, system cluster head selection was done randomly and there is no security provided for the data transmission in wireless sensor network. So, we introduce an energy efficient and secured algorithm which chooses the best nodes in the network to become cluster heads based on certain parameters. As the data is outsourced through cluster members to aggregator then to base station, during this transmission if an attack happens on aggregator at that point existing framework gets fail. We recognize this issue by implementing a Homomorphic (Paillier) Encryption Algorithm for maintaining End to End Confidentiality and also provide a cache memory to cluster head for data loss recovery. A homomorphic encryption scheme enables arithmetic operations to be performed on ciphertexts. One example is a multiplicative homomorphic scheme, whereby the multiplication of two ciphertexts followed by a decryption operation yields the same result as, say, the multiplication of the two corresponding plaintext values. Homomorphic encryption schemes are particularly useful in scenarios where someone who does not have decryption keys needs to perform arithmetic operations on a set of ciphertexts.

METHODOLOGY

1. Network Generation -

Initially network is created where vertices/nodes are connected with the edges.

2. Clustering Process -

After the network creation, the clustering process is performed in which nodes are divided into number of clusters.

3. Cluster Head Selection -

After generating the group of clusters, from each group of clusters, the cluster head is selected on the basis of energy, distance from base station and neighbor nodes parameters.

4. Key generation and distribution -

Key generation and distribution to each node is done by the base station generates the key and distributes the keys. Perform the route generations from each node to the base station.

5. Data Encryption -

At each node data is generated and encrypted by using the Paillier Encryption Algorithm.

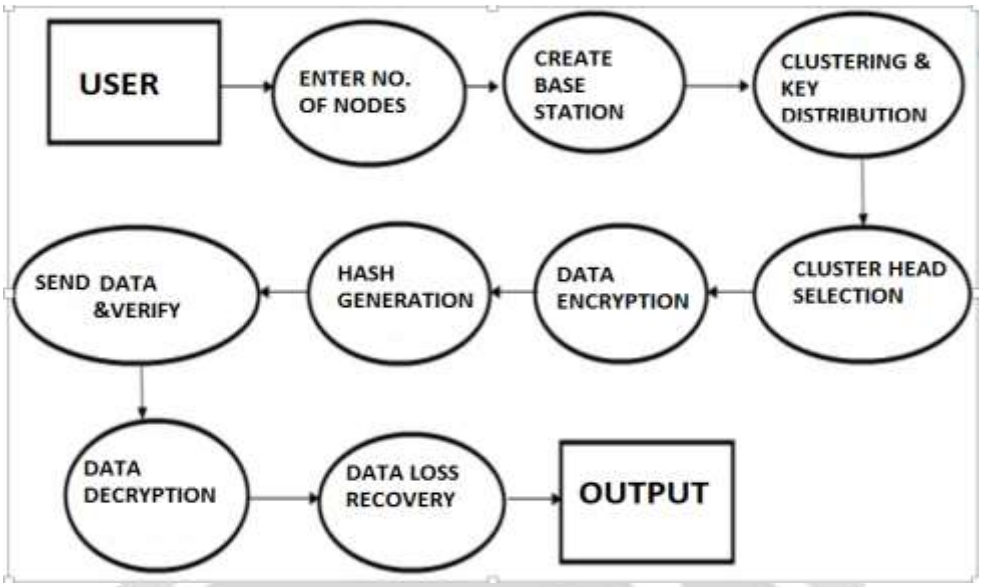


Fig. Data Flow

6. Hash value evaluation -

After the data is encrypted, hash value is evaluated and recorded the timestamp.

7. Data Collection -

After evaluating the hash value at each node, each node sends data to its cluster head. Cluster head collect all the data and verify the valid data.

8. Data aggregation -

Finally the process of data aggregation is done after verifying the valid data by the cluster head. And send data to the base station.

9. Data Decryption -

Base station receives the data from each cluster head and decrypts the data by the appropriate key.

10. Data Recovery -

If cluster Head memory is full then cluster head save the data in cache memory. While sending the data the CH first send the data from cache memory and then from cluster head memory. Base station checks for the lost data and run the cache based recovery system to recover the data.

IMPLEMENTATION

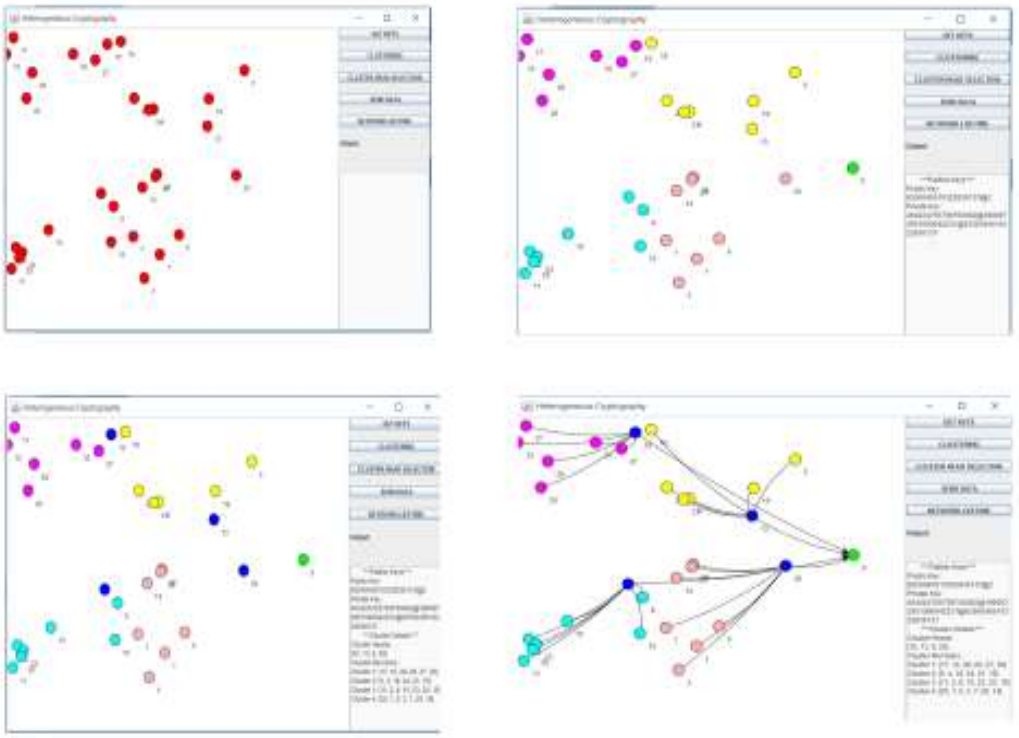
First network is created with sensor nodes, after that clustering algorithm is implemented and number of nodes are divided into number of clusters, cluster head is selected, key distribution is performed at each node through base station, route is generated from each node to the base station.

Encrypt the data by using the Paillier algorithm with the private key. Hash value is evaluated of the encoded data and timestamp is recorded. Cluster member send the data to the cluster head in all clusters.

Each sensor sets itself as a candidate, and this status will be changed or not depending on the comparison that will be made. If a node I find one of its neighbors with a higher energy than its own, the node will change its status as a member, otherwise the density will be compared and the sensor node I will be considered more Data is verified by its hash value, if it is verified then it is accepted otherwise rejected. If cluster head memory is full then cluster head use cache memory to save the data. After that aggregate all the data and send to the base station.

While sending data, cluster head first send the data from the cache then send the data from CH memory. Base station decrypts the data with the appropriate keys. Base station checks the lost data and run the cache based recovery system for data recovery eligible for CH if it has a higher density.

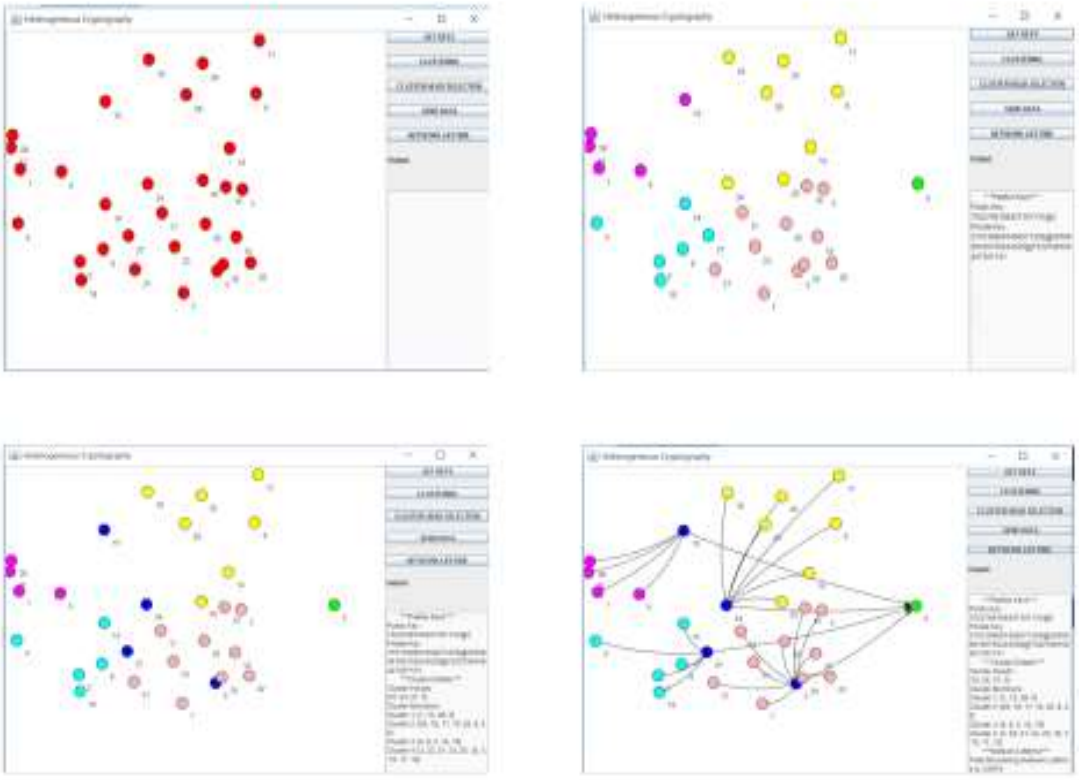
PROPOSED ALGORITHM RESULTS:



COMPARISON WITH LEACH ALGORITHM

- In LEACH, the nodes organize themselves into local clusters, with one node acting as the local ***base station*** or ***cluster-head***.
- These cluster-head nodes broadcast their status to the other sensors in the network.
- Each sensor node determines to which cluster it wants to belong by choosing the cluster-head that requires the **minimum communication energy**.
- The cluster-head nodes are **not fixed** and are **selected randomly.**
- The decision to become a cluster-head depends on the amount of energy left at the node.

EXISTING ALGORITHM RESULTS:

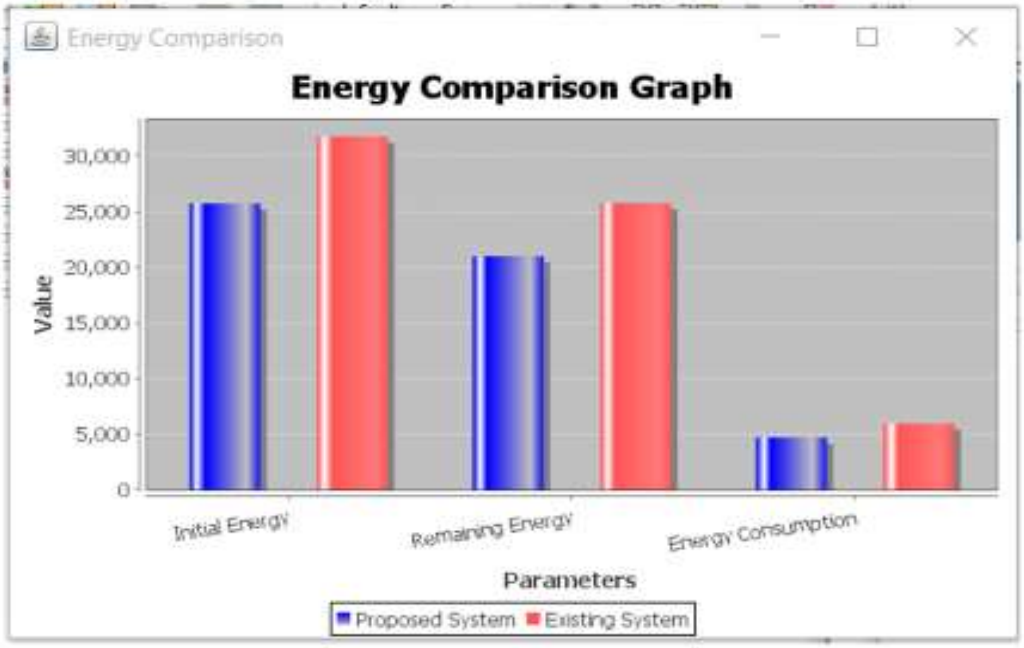


CONCLUSION

We examined the need of clustering in wireless sensor network. We compare leach algorithm from our proposed system but the major disadvantage of LEACH is, it considers homogeneous distribution of nodes in the network. K MEANS is widely used for clustering in data mining, but it is best suitable for smaller data sets. The larger data set of sensor network becomes the smaller data set of K MEANS. And for it the K MEANS works best. So we tried to combine the best of these two methods.

Our proposed scheme does not need the homogeneous distribution of the nodes over the Network. In initial phase we are performing clustering on the sensor nodes. In next phase we tried to optimize the clusters by checking three parameters. In first one we checked the energy of the CH; it is below some threshold new CH will be assigned to the sensor nodes. It helps to minimize the dropped nodes in the network. In second parameter, we check the density of the neighboring nodes, nodes having higher density will be selected as CH. And third parameter will calculate the distance of each node from base station .We have considered CHs in the sensor network such that minimum distance is maintained among them. It also provide security for encrypting and decrypting the data by using pallier encryption algorithm.

GRAPHS AND COMPARISION:



REFERENCES

1. W.B. Heinzelman, A.P. Chandrakasan and H. Balakrishnan, "Application specific protocol architecture for wireless microsensor networks", IEEE Transactions on Wireless Communications, vol.1, no.4, Oct 2002, pp.660- 670.
2. S. Lindsey and C.S. Raghavendra, "PEGASIS:Power efficient gathering in sensor information system", in Proc. of IEEE Aerospace conference, vol.3, March 2002, pp.1125-1130.
3. S. Banerjee and S. Khuller, "A clustering scheme for hierarchical control in multihop wireless networks", in Proc. of 20th Annual Joint Conference of the IEEE Computer & Communications Societies (INFOCOM'01), vol.2, April 2001, pp.1028-1037.
4. S. Banbyopadhyay and E.J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications IEEE Societies (INFOCOM 2003), vol.3, April 2003, pp.1713-1723. [5] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy efficient Communication Protocol for Wireless Micro-sensor Networks", Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000.
5. S. Lindsey and C.S. Raghavendra, "PEGASIS:Power efficient gathering in sensor information system", in Proc. of IEEE Aerospace conference, vol.3, March 2002, pp.1125-1130.
6. A. Manjeshwar and D.P. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks", Proceedings of the15th International Parallel & Distributed Processing Symposium, IEEE Computer Society, April 2000, pp. 2009-2015.
7. A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, FL, USA, April 2002, pp.195–202. [9] S. Banbyopadhyay and E.J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications IEEE Societies (INFOCOM 2003), vol.3, April 2003, pp.1713-1723.

8. O. Younis and S. Fahmy, "HEED: A Hybrid, Energy- Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks", IEEE Transactions on Mobile Computing, vol.3, no. 4, Oct 2004, pp.366-379.

9. S. Soro and W.B. Heinzelman, "Prolonging the lifetime of wireless sensor networks via unequal clustering," in Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, April 2005.

10. Y. Tao, Y. Zhang and Y. Ji, "Flow-balanced routing for multi-hop clustered wireless sensor networks," Ad Hoc Networks, vol.11, no.1, January 2013, pp. 541–554.

11. B. Zarei, M. Zeynali and V.M. Nezhad , "Novel Cluster Based Routing

12. Protocol in Wireless Sensor Networks", IJCSI International Journal of Computer Science, vol.7, no.4, 2010.

13. M. Ye, C. Li, G. Chen and J. Wu, "An energy efficient clustering scheme in wireless sensor networks," Ad Hoc and Sensor Wireless Networks, vol. 3, April 2006, pp.99– 119.

14. Y. Sangho, H. Junyoung, C. Yookun and J. Hong, "PEACH: Powerefficient and adaptive clustering hierarchy