P: ISSN NO.: 2394-0344 RNI No.UPBIL/2016/67980 VOL-3* ISSUE-7* (Part-1) October- 2018
E: ISSN NO.: 2455-0817 *Remarking An Analisation*

A Study on Security Measure in Networking and Its Significance

Abstract

A single-tier network can cause the gateway to overload with the increase in sensors density. Such overload might cause latency in communication and inadequate tracking of events. In addition, the single-tier architecture is not scalable for a larger set of sensors covering a wider area of interest because the sensors are typically not capable of long-haul communication.

Wireless Sensor Network (WSN) consists of a large number of low-cost sensors which communicate with each other via wireless channel. WSN has been proposed for a wide variety of applications such as target tracking, security, environment monitoring. A major application of WSN is to measure the environment parameters and transmit the sensor readings to remote server. Because neighboring sensors may detect the common phenomenon, there is high redundancy in their raw data and it is inefficient to transmit all raw data to remote server.

Keywords: Clustering, Network, Node, Data.

Gurpreet Singh
Research Scholar,
Deptt.of Computer Science,
Tantia University,
Sri Ganganagar,
Rajasthan

Kalpana Middha
Associate Professor,
Deptt.of Computer Science,
Tantia University,
Sri Ganganagar,
Rajasthan

Introduction

Clustering has been widely used in wireless sensor networks (WSNs) to increase scalability, improve energy efficiency and provide QoS guarantees. With clustering, sensor nodes are organized into clusters and a cluster head (CH) node is selected for each cluster according to certain rules, while other nodes act as members in the clusters. In cluster-based data gathering, data collected by cluster members are first sent to CHs, which in turn deliver the data to the data sink either by direct communication or through relays on intermediate CHs. While clustering is initially introduced to achieve energy efficiency, it can also help maintain low packet latency in delay-sensitive data gathering. This is because that packets from different members can be combined as aggregated packets at CHs to reduce the transmission overhead of packet headers and control packets (e.g., ACK packets), leading to shortened transmission delay. In addition, clustering simplifies the routing from the source node to the sink and shorter routing paths reduce network traffic as well.

Sensor nodes collect data from their environment and send it to the Base Station. Heterogeneous sensor network contains high energy sensor nodes as well as low energy nodes. The cluster head aggregates and transmits the data to the Base Station.

Hierarchical clustering is particularly useful for applications that require scalability to hundreds or thousands of nodes. Scalability in this context implies the need for load balancing and efficient resource utilization. All nodes in a network can be organized in hierarchical structures called clusters. Each cluster consists of a cluster head and several member nodes. The member nodes collect data and send it to their cluster heads.

The energy consumption of cluster heads is higher than that for member nodes. Clustering algorithms are required which can efficiently utilize the energy of nodes so that life of network can be increased. Here we are proposing Fuzzy Logic based clustering for homogenous sensor networks.

Review of Literature

Ajay Jangra et al. [1] present a novel security S-LEACH mechanism which is the extension of LEACH routing protocol used for detecting the Sybil attack. The mechanism is configured to initiate the Sybil attack whose detection is relayed on RSSI (an indicator of signal strength) when the number of cluster heads in WSN is above the threshold. The security mechanism is canvassed by the safety of the stage and energy consumption through a series of experiments.

Deng Zhejiang et al. [2] performed; due to the limitation of power and memory size for WSN, the routing protocol for wireless sensor networks must maintain small routing information and reduce the power consumption as much as possible. LEACH protocol and PEGASIS protocol are analyzed firstly in this paper. Use for reference of the ideas used in both of the two protocols of reducing power dissipation, a three-layered routing protocol for WSN based on LEACH(TL-LEACH) is given.

Fan Xiangning et al. [3] studies LEACH protocol, and puts forward energy-LEACH and multihop-LEACH protocols. Energy–LEACH Protocol improves the choice method of the cluster head, makes some nodes which have more residual energy as cluster heads in the next round. Multihop-LEACH Protocol improves communication mode form single hop to multihop between cluster head and sink. Simulation results show that Energy-LEACH and Multihop-LEACH Protocols have better performance than LEACH Protocols.

Fuzhe Zhao, You Xu, Ru Li, Wei Zhang et al. [4] propose a new method of choosing cluster-heads with decreases unnecessary consumption of energy spent on computing of each node during each round. In order to make the energy distribute more even in the network, the consideration of the dynamic change of sensor nodes energy will be introduced during the selection of CHs.

Fuzhe Zhao et al. [5] proposes a new method of choosing cluster-heads which decreases unnecessary consumption of energy spent on computing of each node throughout each round. Because the traditional selection formula neglecting to the change of nodes' energy will make the nodes acting as cluster-heads (CHs) too many times die early owing to consume more energy.

Haosong Gou et al. [6] this paper proposes an improved LEACH (LEACH-C) algorithm called partition-based LEACH (pLEACH), which firstly partitions the network into optimal number of sectors, and then selects the node with the highest energy as the head for each sector, using the centralized calculations. The idea behind LEACH is to form clusters of the sensor nodes depending on the received signal strength and use local cluster heads as routers to route data to the base station and the corresponding clusters.

Heewook Shin et al. [7] proposed a new energy efficient clustering scheme. He stated that in LEACH, however, extra energy and time are consumed to reform clusters at the setup phase of every round. This side effect is bad as the number of clusters increases. This paper present a novel energy-efficient clustering scheme to remove cluster recreating process required at every round after the first round, which is called COTS (Clustering with One Time Setup). The proposed COTS allow that the role of cluster head is rotated among members in a cluster without cluster reforming process. This way significantly saves the energy because the cluster reforming process is not needed, resulting in increased network lifespan.

Hu Jumping et al. [8] performed a wireless sensor network consists of hundreds or thousands of small energy-limited sensors that are densely deployed in a large geographical region. It has been demonstrated that Low-Energy Adaptive Clustering Hierarchy is an energy-efficient routing algorithm for Wireless Sensor Networks.

Jun YUE, Weiming ZHANG, Weidong XIAO, Daquan TANG, Jiuyang TANG et al. [9] presents a novel unequal cluster-based data aggregation protocol is proposed. It divides the network into some grids with unequal sizes, and implements cluster head rotation in each grid respectively. It is able to balance energy dissipation by setting proper sizes of grids to adjust the number of nodes that participate in cluster head rotation in different grids.

Y. Yang et al. [10] performed a work, Based on the analysis on the defect in LEACH including the fluctuation of the number of cluster heads and the ignorance of the node's residual energy, this paper presents a novel protocol called LEACH-B (LEACH-Balanced). At each round, after first selection of cluster head according to LEACH protocol, a second selection is introduced to modify the number of luster head in consideration of nodes residual energy. As a result the number of cluster head is constant and near optimal per round.

Muhamnmad Omer Farooq et al. [11] presents a multi-hop routing with low energy adaptive clustering hierarchy protocol.MR-LEACH follows the fundamental principle of multi-hop routing from cluster-heads to a Base station to conserve energy, unlike the leach protocol. In MR-leach they partition the network into different layers of clusters. Where Cluster heads in each layer collaborates with the adjacent layers to Transmit sensor's data to the base station. Ordinary nodes Join cluster heads based on the received signal strength indicator (RSSI).

In year 2010, Muhammad Omer Farooq et al [12] performed a work.In this paper, we present a Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy (MR-LEACH) protocol. In order to prolong the lifetime of Wireless Sensor Network, MR-LEACH partitions the network into different layers of clusters. Cluster heads in each layer collaborates with the adjacent layers to transmit sensors data to the base station. Ordinary sensor nodes join cluster heads based on the Received Signal Strength Indicator (RSSI).

Nandini. S. Patil, Prof. P. R. Patil et al. [13] presented a data aggregation framework on wireless sensor networks is presented. The framework works as a middleware for aggregating data measured by a number of nodes within a network. They compare the performance of TAG(Tiny Aggregation) in terms of energy efficiency in comparison with and without data aggregation in wireless sensor networks and to assess the suitability of the protocol in an environment where resources are limited.

Wei Bo Hu Han et al. [14] performed a work; Conventional LEACH includes distributed cluster formation, local processing to reduce global communication, and randomized rotation of the cluster-heads. The new protocol uses multi-hop

routing instead of 2-hop routing in LEACH, and related algorithm is proposed. Simulation results show that improved protocol is more energy-efficient that conventional LEACH.

Objective of the Study

Proposed function implements Fuzzy Logic based clustering which in enhanced form of weight based clustering in wireless sensor networks. Weight based clustering protocol has the disadvantage that it elects unnecessarily extra cluster head. Sometimes Nodes with high residual energy were not given a chance to become cluster head.

This disadvantage is overcome by Fuzzy Logic based clustering algorithm. All nodes with similar energy are given same chances to become cluster head.

Also a node with high residual energy even if it is lying in captivity of another cluster head will be elected as a cluster head. The proposed clustering technique is an enhancement our Weight based clustering. The overarching goal of our approach is to prolong network lifetime. For this reason, cluster head selection is primarily based on the residual energy of each node. Measuring this residual energy is not necessary, since the energy consumed per bit for sensing, processing, and communication is typically known, and hence residual energy can be estimated. Fuzzy logic is used for finding cluster head which always chooses optimal number of cluster heads. The use of fuzzy logic is appropriate, whenever it is not possible to employ a mathematical model for the system. Additionally, fuzzy can reduce the complexity of the model; computational effort and memory's receive context information from nodes as input and converts into fuzzy linguistic variable input.

First order radio energy is used for performing radio analysis. It takes the following form

Einit=0.5 in joules

Eelec=50*0.000000001

EMP=0.0013*0.000000000001

Eda=5*0.000000001

Where Einit is initial energy, Eelec is electrical energy, EMP is amplification energy, Eda is data aggregation energy.

The Pseudo code

The Pseudo code of Proposed Model is as Follows:

Step1: Start

Step 2: Create a Network

Step 3: Create Clusters from network using:

a. A CH is selected from the SNs by considering a multiple metrics i.e. residual energy and a distance from non-CH to CH using the concept of Fuzzy logic and Cluster is created.
b. Based on last step, Non-CHs select the best CH based on distance matrices to become its member.

Step 4: Stop

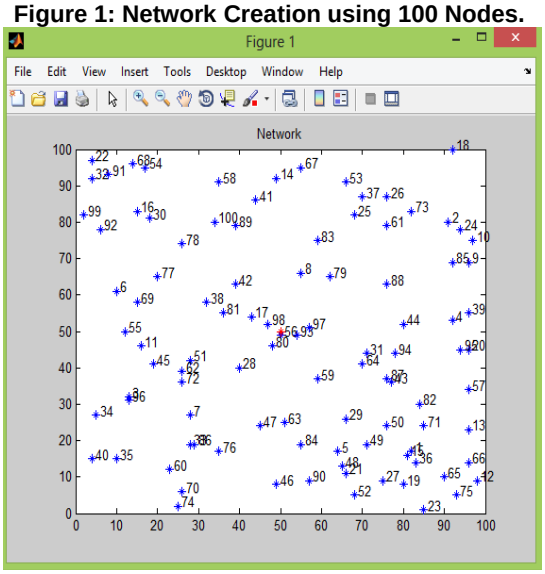
Research Methodology

This part presents the simulation and results of the presented model.

Simulation Scenario

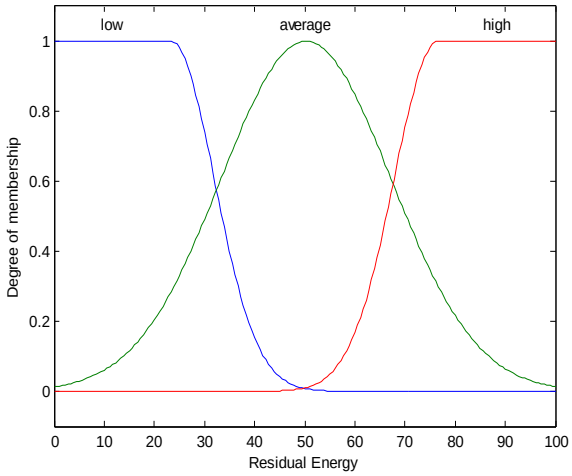
Initially there is a network in which nodes are distributed randomly as shown in figure 1.

Figure 1: Network Creation using 100 Nodes.



In figure 2 new scheme is implemented in which cluster head are elected based on the given logic of presented model. These cluster head are shown by star shape in blue color (*).Red stars are dead nodes.

Figure 2: Cluster Formation



Each Normal node will elect its cluster head based on Probability which can be calculated Fuzzy Logic System using the two input variables "distance between the node & cluster head" and "Residual Energy".

Figure 3 and figure 4 show both inputs and their corresponding graphical representation in fuzzy system.

Figure 3: Degree of Membership for Residual Energy As First Input For Fuzzy System

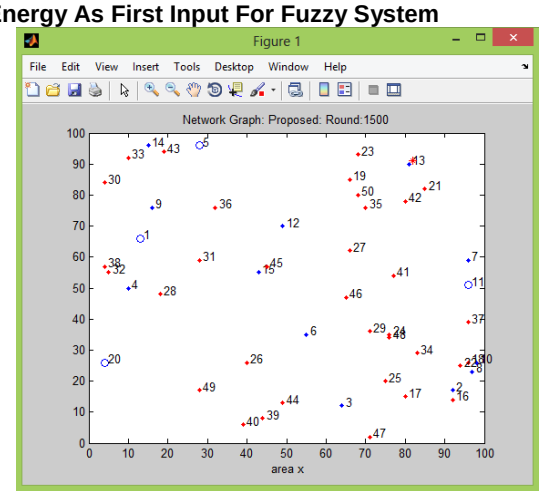
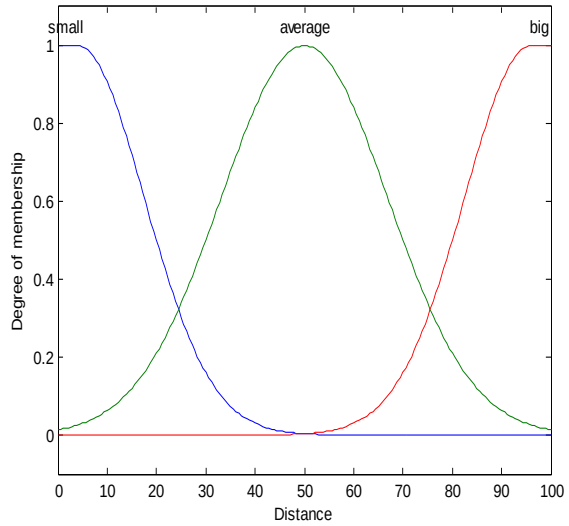
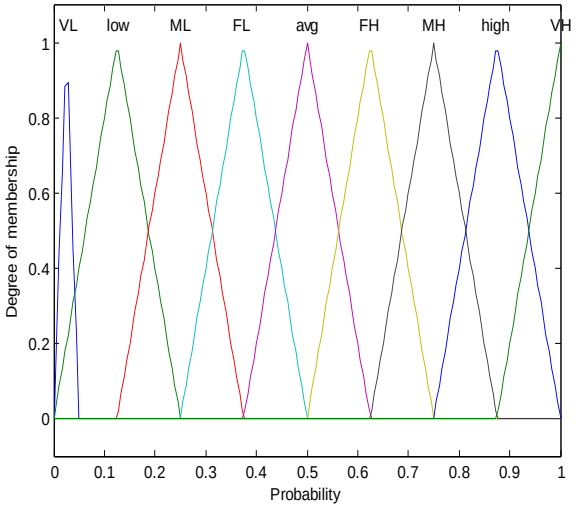


Figure 4: Degree of Membership for Distance As Second Input For Fuzzy System



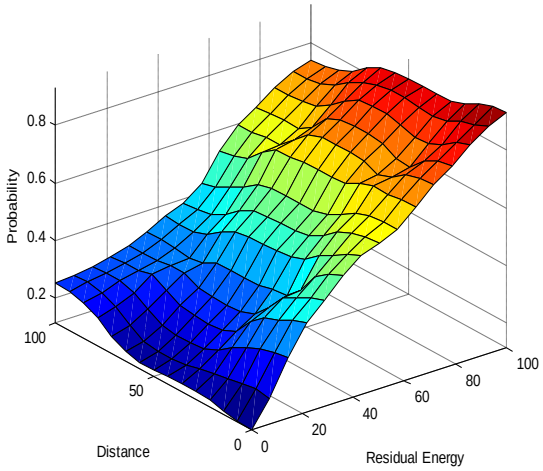
Correlation between Residual energy and Distance for Fuzzy system is shown in figure 5.

Figure 5: Correlation between Residual energy and Distance for Fuzzy system



Finally figure 6 shows the surface graph for probability calculation for cluster formation.

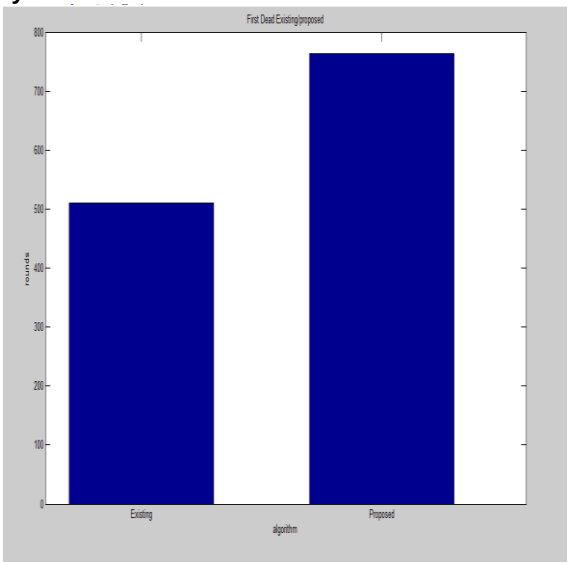
Figure 6: Surface Graph for Probability Calculation for Cluster Formation.



Using this Probability Calculation fuzzy logic, each normal node calculates the probability for each cluster head. The node which has the highest probability with respect to any cluster head will be the member of that cluster for cluster head in that round. In this way Cluster formation is done in the presented work.

Performance Evaluation

Figure 7: Comparison of Existing and Proposed System in Terms of First Dead.

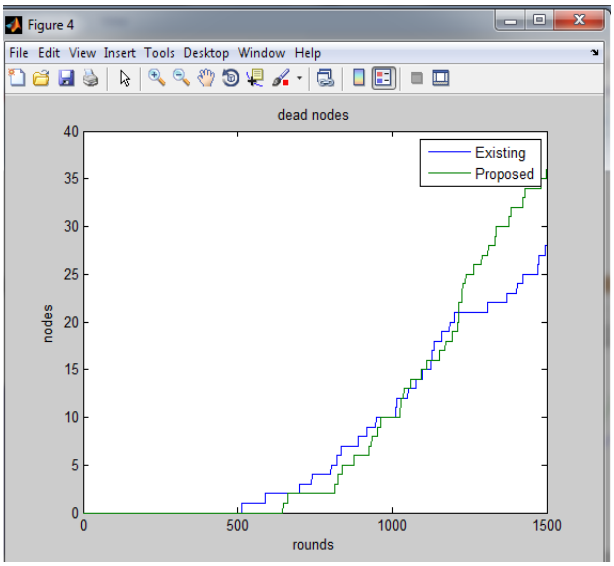


The figure 7 graph shows that first dead node in our proposed algorithm happens after 700 rounds in spite of existing weight based algorithm which is having its first dead very close to 500 round. Hence our algorithm is Energy efficient than existing algorithm.

Figure 8 gives the graph which compares the performance of existing and proposed system in terms of number of dead nodes with total number of clustering rounds. Green line represents the proposed system and blue line represents the existing system.

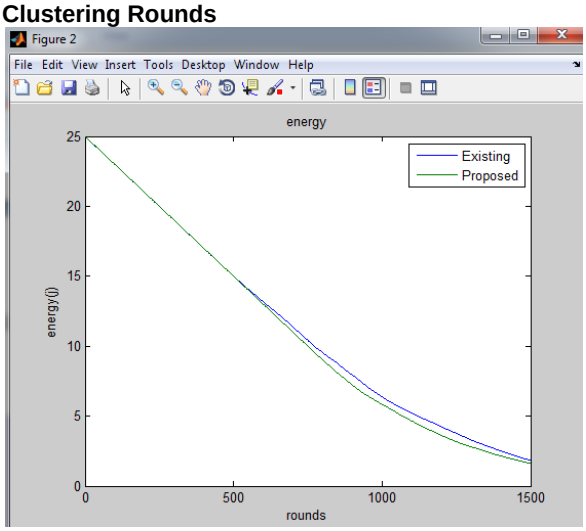
Graph shows that proposed system shows improved performance over existing system in 1000 rounds.

Figure 8: Performance Evaluation of Existing and Proposed System in Terms of No. of Dead Nodes& No. of Rounds



The graph 9 gives a comaprison of the performance of existing and proposed system in terms of number of dead residual energy with total number of clustering rounds. Green line represents the proposed system and blue line represents the existing system. Graph shows that proposed system have almost same residual energy up to initial 500 rounds as existing system is having.

Fig: 9 Comaprison of the Performance of Existing and Proposed System in Terms of Number of Dead Residual Energy with Total Number of Clustering Rounds



Hypothesis

Routing Threats

There are a multitude of potential threats facing the routing of ad hoc networks. These include confidentiality, integrity, and availability. When it comes to confidentiality within the realm of routing protocols, the primary threat is towards the, "privacy of the routing data itself." If the routing data were to be compromised, then a secondary threat could occur to other information such as, "the network topology, geographical location, etc."

The integrity of an ad hoc network essentially relies on the accuracy of each node's routing information. Potential attacks include those that would either alter existing routing data or introduce new, but incorrect, routing data. Finally, in the context of ad hoc routing, availability fundamentally equates to nodes being able to have on demand access to routing information at all times. Additionally, routing operations should not delay nodes from obtaining up to date information. Consequently, each node within the network should be able to function normally without unnecessary interference from either security or the routing protocol.

External Threats

With ad hoc networks, external threats are distinguished from internal threats by classifying external threats as potential attacks performed by unauthorized network nodes or other outside entities. In contrast, internal threats refer to potential attacks originating from internal authorized nodes. In terms of detection difficulty, external threats are typically easier to detect than internal threats. In ad hoc networks with an authentication protocol to block unauthorized nodes from joining the network, external threats typically focus on attacking the data link and physical layers of the network. Also, external attacks can be further classified into two broad categories, passive eavesdropping and active interference.

Passive eavesdropping generally refers to attacks that attempt to simply listen to the transmitted signals and network traffic without disrupting the network. The most basic of which simply involves the discovery of a wireless ad hoc networks by detecting the existence of the appropriate signals. By extension, passive eavesdropping can pose a threat to location privacy. More sophisticated attacks will attempt to capture messages, including routing updates. Routing updates can be used to infer the topology of the network and the identities of the more active, and possibly more critical, network nodes.

Internal Threats

Internal threats refer to potential attacks originating from authorized nodes on the network. These types of attacks are potentially very serious since, "internal nodes will have the necessary information to participate in distributed operations." Typically, the adverse behavior of internal nodes can be classified into four general categories: failed nodes, badly failed nodes, selfish nodes, and malicious nodes. The failed nodes category simply refers to nodes that cannot perform an operation. The badly failed nodes category refers to nodes that behave like failed nodes, but also send out incorrect routing information. The selfish node category refers to nodes that attempt to exploit the routing protocol to their own advantage by not cooperating when a personal cost is involved. Finally, the malicious node category refers to nodes that deliberately attempt to disrupt the network. Furthermore, a node may demonstrate behaviors from multiple categories and multiple nodes within the same category may have differing degrees of incorrect behavior.

Conclusion

We have presented an efficient technique for clustering of sensor node in the homogenous WSNs. In the existing LEACH protocol the clusters are formed using the distance calculation from the node to cluster head. But for a network to be good designed there should be a better cluster formation.

For a better cluster formation the concept of fuzzy logic is used in which non-CHs select the best CH by considering a multiple metrics, i.e. residual energy and a distance from non-CH to CH. Then, non-CHs compute a probability value to each CH candidate. The non-CH chooses the CH with a higher probability value and sends a join message to CH.

The use of fuzzy logic is suitable, whenever it is not possible to use a mathematical model for the system. Additionally, fuzzy can reduce the complexity of the model, computational effort and memory. Energy consumption is affected by message communication between nodes, so our technique is efficient than traditional LEACH protocol.

Also weight based clustering protocol has the disadvantage that it elects unnecessarily extra cluster head. Sometimes Nodes with high residual energy were not given a chance to became cluster head. This disadvantage is overcome by Fuzzy Logic based clustering algorithm. All nodes with similar energy are given same chances to become cluster head. Also a node with high residual energy even if it is lying in captivity of another cluster head will be elected as a cluster head.

Suggestions

This algorithm is implemented for homogenous wireless sensor networks. Algorithm can be further implemented for heterogeneous networks.

References

1. *Ajay Jangra, Swati, Priyanka, "Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS).*
2. *Deng Zhixiang, "Three-layered Routing Protocol for WSN based on LEACH Algorithm," IEEE, 2008.*
3. *Fan Xiangning, "Improvement on LEACH Protocol on Wireless Sensor Network," mt. Conference on Sensor Technologies and Applications, 7 July, 2007.*
4. *Fuzhe Zhao, You Xu, Ru Li, Wei Zhang, "Improved Leach Communication Protocol for WSN," Int. Conference on Control Engineering and Communication Technology,2012.*
5. *Fuzhe Zhao, You Xu, Ru Li, Wei Zhang, "Improved Leach Communication Protocol for WSN", 2012 International Conference on Control Engineering and Communication Technology IEEE.*
6. *Haosong Gou, "An Energy Balancing LEACH Algorithm for Wireless Sensor Networks," 7th Conference on Information Technology, 3 October, 2010.*
7. *Heewook Shin, SangmanMoh, and Ilyong Chung, "Energy-Efficient Clustering with One Time Setup for Wireless Sensor Networks" IEEE 2012.*
8. *Hu Junping, "A Time-based Cluster-Head Selection Algorithm for LEACH", IEEE, 1 August, 2008.*
9. *Jun YUE, Weiming ZHANG, Weidong XIAO, Daquan TANG, Jiuyang TANG, "A Novel Unequal Cluster-based Data Aggregation Protocol for Wireless Sensor Network," PRZEGLĄD ELEKTROTECHNICZNY, ISSN 0033-2097, R. 89 NR 1b/2013.*
10. *M. Ma and Y. Yang, "Data gathering in wireless sensor networks with mobile collectors," in Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS '08), April 2008.*
11. *Muhamnmad Omer Farooq, Abdul BasitDogar, Ghalib Asadullah Shah, "MR-LEACH: Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy"2010 Fourth International Conference on Sensor Technologies and Applications IEEE.*
12. *Muhammad Omer Farooq, "MR-LEACH: Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy," Fourth Int. Conference on Sensor Technologies and applications, 2 October, 2010.*
13. *Nandini. S. Patil, Prof. P. R. Patil, "Data Aggregation in Wireless Sensor Network," IEEE International Conference on Computational Intelligence and Computing Research,2010.*
14. *W.B.Heinzelman, A.P.Chanrakasan and H.Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," Transactions on Wireless Communications, Vol. 1, No. 4, pp. 660-670, October, 2002.*
15. *W.R. Heizelman, A.Chandrakasan and H.Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Proc. 33rd Hawaii Int. Conference on System Science, Vol. 2, 4-7 Jan, 2000.*
16. *Wu Xinhua, "Performance Comparison of LEACH and LEACH-C Protocols by NS2," 9th Int. Symposium on Distributed Computing and Applications to Business, Engineering and Science, 5 October, 2010.*
17. *Yuling Li, Luwei Ding, FengLiu, "The Improvement of LEACH Protocol in WSN", 2011International Conference on Computer Science and Network Technology IEEE*