Special Issue on Chemistry

Wireless Sensor Network to Improve Energy Efficient Using Clustering Algorithm

S. Peter Vijay and G. Veeramani

Issue Editor
Dr. A. Manikandan

Research Journal of Agricultural Sciences
An International Journal

P- ISSN: 0976-1675
E- ISSN: 2249-4538

Volume: 13
Issue: Special

Res. Jr. of Agril. Sci. (2022) 13(S): 071–074

CARAS

Res. Jr. of Agril. Sci. (2022)
13(Special): 071–074

ISSN: 0976-1675 (P)
ISSN: 2249-4538 (E)

www.rjas.org

Full Length Research Article

Wireless Sensor Network to Improve Energy Efficient Using Clustering Algorithm

S. Peter Vijay*[1] and G. Veeramani[2]

Received: 04 Dec 2021 | Revised accepted: 10 Feb 2022 | Published online: 25 Feb 2022

A B S T R A C T

Use of clustering in the field of Sensor Networks can be divided into two ways; one is leaf nodes and the other is to manage this leaf nodes i.e., the Cluster Head (CH). All the leaf nodes are controlled by the CH and the Base Station (BS) takes control of the CH. The duty of the leaf nodes is to sense the data and cannot directly communicate with the BS. On receiving the data, the sensed data is transmitted to the CHs. On receiving the data; CH will perform various data aggregation and fusion techniques and finally transmit it to the base station. Hence the architectural organization of CH should be designed in a way that CH is nearer to the base station. This leads to more energy consumption at CH level and hence, the target is to select the maximum energy node as CH, as failure of CH will lead to total collapse of the entire network. Clustering reduces energy consumption and the number of messages transmitted towards the base station. The main objective of clustering in Wireless Sensor nodes is to extend the network lifetime, as these nodes may carry some sensitive information to fulfil its application specific requirements.

***Key words*:** Sensor Networks, Wireless Sensor, Architectural organization

Reinforcement Clustering is a demonstrated procedure to guarantee vitality productive correspondence. A large portion of the examination chips away at group-based Sensor Network manages the issue of between bunch directing and not very many of them consider organize throughput and system delay as their proposal [1]. At present, enormous system traffic is produced by the sensors and gadgets of the Internet of Things (IoT), wise home and brilliant lattice systems. Throughput and postpone must be considered for effective administration and control of this kind of sensor-competent system. The proposed work considers the reinforcement grouping calculation to guarantee vitality level among secure hubs and dependable information transmission in the correspondence way. Intra-group directing is the procedure to discover the productive method to advance system traffic (or information) to the CH inside the bunch. Here some significant parameters are viewed as like connection throughput, delay, bundle misfortune proportion, impedance and remaining vitality to choose the connections and relating sensor hubs to build up the way of intra-group correspondence [2]. The proposed model ensures clustering among nodes by making the node to act as CH only when the nodes fall in secure region during the time of deployment. The clustering algorithm is developed to gather local available information and to reduce energy consumption. Here, the cluster formation has a set of rules to be followed. Cluster of sensor nodes are formed based on the local density and the available energy level in plurality of sensors [3-4].

During the initialization process, nodes broadcast their willingness to act as a CH (CH) and a node with maximum energy and maximum nodes in the sensing range will be selected as the CH [6]. In certain scenarios, if another node with higher energy level and maximum nodes in the sensing range is detected, it will be assigned as a Backup CH (CH_{backup}). When the energy level in the CH falls below the designated threshold level, this CH_{backup} will act as a new CH. This will reduce the additional computation resource in selecting new CH;all the other nodes will be added as the leaf node to the cluster.

Cluster formation model

Consider the scenario of M sensors deployed evenly over an N x N field. During the set-up phase, all nodes are assigned with same initial energy level by following the steps The node deployment is of ZigBee enable beacon devices and hence in order to find the neighbours, all nodes will transmit beacon signals to feel their presence in the network. As shown in figure 3, the BS has to filter all the Secured Region nodes and fixes a unique group ID which is broadcasted to all secure region nodes in the network. All maximum number of Secured Region nodes are set as i_{max}. Two cases are tested to find whether the node falls in secure region or Vulnerable Region.

Test case 1: For the first node i that wants to actively participate in communication checks for the condition of i <=

* **S. Peter Vijay**
✉ petervijay.solomon@gmail.com

[1-2] Department of Chemistry, Bharath Institute of Higher Education and Research (BIHER), Chennai - 600 073, Tamil Nadu, India

i_{max} where i_{max} is the total number of Secured Region filtered from the total number of nodes deployed in the network.

Test case 2: The above test case 1 succeeds only when the given i value is less than i_{max}. If this true, then the second condition is to check whether the energy level of node i is less than or equal to the energy threshold $E_{g\text{-}th}$. The threshold value is calculated by considering the energy level of maximum number of nodes in a cluster divided by maximum number of eligible CHs in the network. Therefore, from equation (1), it is clear that the energy of a particular node e_g is compared with the threshold value $E_{g\text{-}th.}$ ($e_g \leq E_{g\text{-}th}$). If the condition is satisfied then that particular node is elected as CH.

In this scenario, if test case 1 fails, the execution is stopped and the whole process is restarted. For the test case 2, if the condition fails to choose a CH, then the current cluster will be selected as the leaf node for the corresponding CH.

Algorithm parameters

The CH (CH) and Back-up CH(CH_{backup}) formation model is depicted in algorithm 3.1. Initially all nodes in the network have the right to act as a CH. The nodes that are interested to act as CH will broadcast its willingness by sending its energy level and the unique group ID to its single hop cluster members. The node with maximum energy will meet the requirement and will be checked for the condition as given in the algorithm 1. The node that wins will check its group id with $S_{n(id)}$. If it is true then the particular node will be eligible for acting as CH. By having the eligibility ticket of acting as CH it will have to meet two test conditions in order to avoid the bogus node from becoming CH. As a first step the energy level of the eligible CH will check with the maximum threshold value and if it is found to be less or equal, then from there it will a count the number of beacon signals it can receive from its Sensing Range (S_R). Let the maximum number of beacon signal sensed by a Network Cluster (NC) be Network Cluster threshold (NC_{TH}). If Network Cluster Sensing Range (NC_{SR}) is equal to or greater than the NC_{TH} and if it is the first CH to meet the condition then the current node will act as CH. If this is not the case and already a CH been chosen, then it is the time for CH_{backup} to meet the condition and be elected as Bach-up CH for the respective cluster. Finally, if a node does not meet any of this condition then the node will be set as leaf node for the corresponding CH. Now, after this selection procedure, the CH and CH_{backup} finally broadcast the information to BS and to all other nodes in the cluster.

The cluster formation model with efficient Back-up CH is designed by considering the various Sensor Network constraints. Complexity in the selection procedure of heads will lead to more depletion of energy at node level. The regular bunching calculations intended for Wireless Sensor Network is appropriate for CH development just and won't worry about the information that is transmitted. Every hub can be a CH, on the off chance that it has the vitality to be accessible for the entire round. By choosing the reinforcement hub, the successive grouping component is diminished and in this way vitality is spared [8,9]. This prompts the most brief course arrangement for the non-uniform dissemination of group part hubs inside a bunch. All the main level CHs will be the part for the second level CHs shaping a various leveled structure, having Base Station as the root.

The hindrance of the LEACH calculation is the lopsided conveyance of the hubs in a bunch. Each CH executes the one-advance most brief way chart calculation and finds the most brief course from the CH to every one of its individuals. In the event that one turns around the course of each most limited way, at that point every individual from sensor hub sends the information to the CH through a similar way bringing about poor transmission capacity. The other existing model of utilizing hand-off hubs as back up hubs accept that all the part hubs which are inside the detecting territory of the CH hubs i.e the hubs which get the communicate message in 1 bounce by single flooding, are qualified for reinforcement hubs [10]. Each group part hubs in the wake of getting the 1 jump message, sends the answer to be enlisted as the reinforcement CH. The hubs are recorded in a line and in the following round the CH sends the duty to the primary hub in line list dependent on the intensity of the hub [11]. Due to this nature, a situation may arise wherein a middle node waiting in the queue with highest power will not at all get a chance of acting as CH_{backup}. Both drawbacks are overcome by the proposed model by using efficient and secure Back-up Clustering formation.

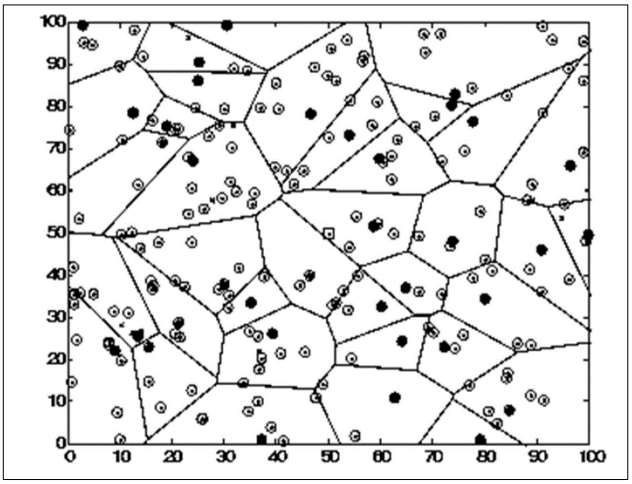

Fig 1 Simulation environments, considering 100 nodes in 100 x 100 meters

Table 1 Parameter specifications

Symbols	Description
$S_{n(i)}$	Secure Region Node of i
$S_{n(id)}$	Secure Region Nodes Unique group id
CH	CH
NC_{SR}	Network Cluster Sensing Range
NC_{TH}	Network Cluster Threshold
Count (S_R)	Count of no of beacons received

Performance evaluation

Simulation settings

The performance of the proposed Back-up CH with intra-cluster routing approach was examined by simulation using a computational tool. The energy dissipation, lifelong awareness, throughput, average packet delay, and connectivity rate are examined to validate the proposed algorithm. The results of the proposed work are compared with the results of the benchmark routing protocol LEACH [12]. However, performance of "An Energy Aware clustering and relay node selection Algorithm in Wireless Sensor Networks" is also compared with the results obtained with the proposed method of justifying improved performance. The LEACH is only 1-stage routing and the relay node election Algorithm is 2-stage routing with backup path [13]. The simulation performance scenario is shown in figure 4, where the square boxes represent the Command Node (CN) position, the black circles shown as Sensor Nodes (SNs) fall under secure region, and the black shaded circles

are represented as Vulnerable Region nodes. There are a total of 100 nodes used in 100x100 square meter field. The simulation parameters and their assumed values are shown in (Table 1).

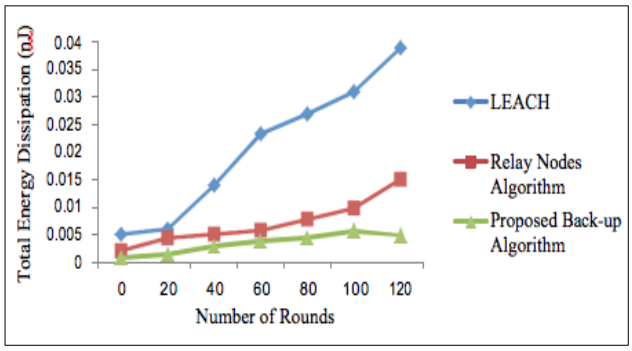

Fig 2 Comparison of energy dissipation of nodes (nJ)

Simulation results

The proposed back-up clustering algorithm is compared with other two algorithms and the comparison of total energy dissipation is shown in figure 2 and the values are recorded in table 2. The total energy dissipation in so called benchmark routing protocol LEACH is higher because of its random selection of CH (CH) and uneven distribution of nodes. In the other existing model of setting relay nodes is done based on receiving the acknowledgement of single hop nodes. All nodes in one hop will contend for relay node selection based on assumption that all nodes are in the same sensing range. In both the cases, only few nodes get a chance of acting as CH or relay nodes resulting in more energy dissipation on those nodes. The proposed model shows lower dissipation by selecting CH and CH_{backup} where all nodes get the chance of acting as CH and CH_{backup} resulting in equal energy distribution among nodes. Apart from this, the proposed model selects the nodes in secure region to act as CH or CH_{backup} to add security to nodes from unauthorized access. Lifetime of CH is another important metric to measure the performance of the Wireless Sensor Network [14]. The node which has longer life can involve in communication over a longer period of time. As the changeover of CH's in both the existing model is restricted to only few node, this will lead to over dissipation of energy to few set of nodes especially the nodes acting as CH,this will lead to degradation of overall performance of the system. The comparison in figure 3 and 4 clearly depicts about the bench mark existing protocol, existing and the proposed model [5].

Table 2 Simulation parameters

Simulation parameters	Symbols	Values
Topology	---	Hierarchical
Number of nodes	N	100
Area size	S	100 x 100
MAC	---	IEEE 802.15.4
Packet size	P	512 bits
Initial energy	I_e	0.5 J
Transmission energy / bit	T_{Eg}	50 nJ/bit
Receiving energy	R_{Eg}	50 nJ/bit
Traffic source	T_s	Constant bit rate (CBR)
Radio communication range	R_{Cg}	20 m
Sensing energy	S_{Eg}	50 nJ/bit
Channel bandwidth	C_b	5 Mbps
Beacon interval	B_i	5 secs
Simulation time	S_t	100 secs
Data rate	d_r	250 kbps
Operating frequency	O_f	2.4 GHz
Vulnerable region nodes	V_n	1 to 10

Table 3 Total energy dissipation (nJ)

Number of rounds	Leach	Existing algorithm (Relay node)	Proposed back-up algorithm
0	0.005	0.002	0.001
20	0.00595	0.00435	0.0015
40	0.014	0.005	0.003
60	0.0234	0.00575	0.004
80	0.027	0.0078	0.00454
100	0.031	0.0098	0.0058
120	0.039	0.015	0.005

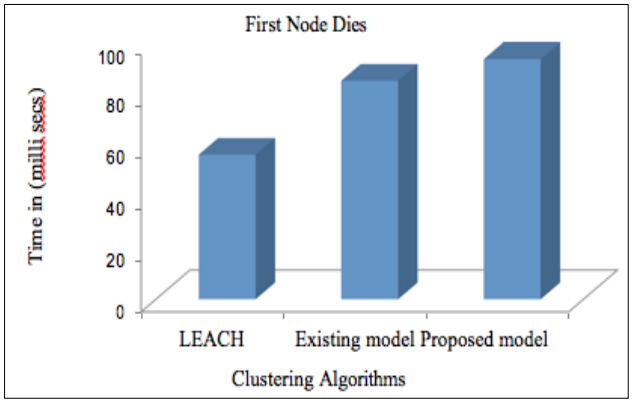

Fig 3 Lifetime of first node

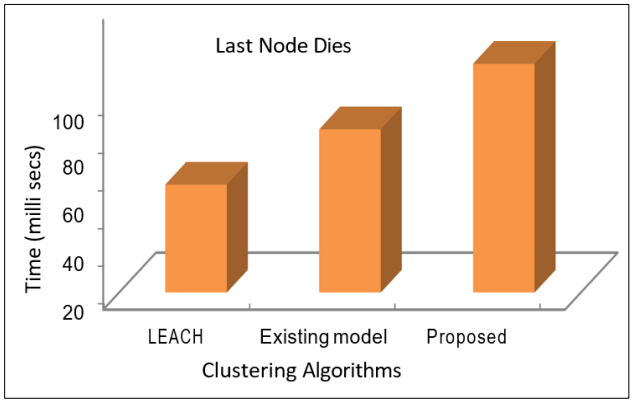

Fig 4 Lifetime of last node

CONCLUSION

The efficient selection of Back-up CH is proposed in this research. The simulation results show the energy efficiency and the longer lifetime of Sensor Networks. Although the proposed routing protocol has a lower average connectivity rate, the back-up node selection based on maximum energy level and average energy calculation based on various testing condition of the sensor node help to provide packets with a higher throughput and a lower rate of average packet transfer delay. The proposed

model uses a new technique of making secure region nodes as CH and CH_{backup} in order to have a best and equal distribution of energy usage among nodes, as the nodes are intended in carrying high sensitive data. The main aim is, not to elect the nodes as CH or CH_{backup} from Vulnerable Region (V_n), as those nodes can be compromised by an adversary at any time. If not, then a compromised V_n will take control over the network, thereby creating chaos in the performance of the node and also increases the probability of high energy depletion in the network. Even though the CH and CH_{backup} are formed with at most care, the drawback of the proposed work is not ensuring security overthe network. This means the exchange of messages happening between secure region and Vulnerable Region is prone to attack at the node level by physical access where an adversary takes control over the network resulting in random change of CH and CH_{backup}. In order to overcome the drawback, an Asymmetric Keying mechanism (AK_P) is proposed in the future work to improve the security parameters and to achieve reliable communication even for the nodes that fall over Vulnerable Region. In conclusion, the proposed model shows betterment in lifetime of node, which in turn extends the life time of the network.

LITERATURE CITED

1. Akyildiz IF, Su, W,Sankara Subramaniam, Cayircie 2002, 'Wireless Sensor Networks : A Survey ', Computer Networks, vol.38, no.4, pp. 393-422.
2. Al Karaki,JN &Kamal,AE 2004, 'Routing Techniques in Wireless Sensor Networks : A Survey', IEEE Wireless Communications, vol. 11, no.6, pp.6-28.
3. Anita,X, Bhagyaveni,MA &Manickam,JML 2015, 'Collaborative lightweight trust management scheme for wireless sensor networks', Wireless Personal Communications, vol. 80, no. 1, pp. 117-140.
4. Baoxian Zhang &Mouftah, HT 2005, 'QoS Routing for Wireless Adhoc Networks : Problems, Algorithms and Protocols', IEEE Communications Magazine, vol.43,no.10,pp.110-117.
5. Benjie Chen, Kyle Jamieson, HariBalakrishnan& Robert Morris 2002, 'SPAN: An Energy-efficient Coordination Algorithm for Topology Maintenance in Ad Hoc WirelessNetworks', Wireless Networks, vol. 8, no. 5, pp. 481–94.
6. Boukerche,A 2001, 'A Performance Comparision of Routing Protocols for ad hoc Networks', Proceedings of 15th International Parallel and Distributed Processing Symposium, pp.1940-1946.
7. Braginsky,D &Estrin,D 2002, 'Rumor Routing Algorithm for Sensor Networks', Proceedings of 1st ACM International Workshop on Wireless Sensor Network and Applications, pp. 22-31.
8. Camenisch,J, Groth,J 2004, 'Group signatures: Better efficiency and new theoretical aspects', In Proceedings of International Conference on Security in Communication Network , pp. 120-133.
9. Chan,H,Perrig,A& Song,D 2003, 'Random key pre distribution schemes for sensor networks', In Proceedings of the IEEE Symposium on Security and Privacy, pp. 197 - 213.
10. Chang JH and LeandrosTassiulas2004, 'Maximum Lifetime Routing in WIreless Sensor Networks', IEEE/ACM Transactions on Networking, vol.12, no.4, pp.609-619.
11. Cheikhrouhou, O,Koubaa,A,Boujelben, M and Abid M. 2010. A lightweight user authentication scheme for wireless sensor networks. *In Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications*. pp 1-7.
12. Dang, T, Bulusu, N, Feng, W & Park, S 2009, 'DHV:Acode consistency maintenance protocol for multi-hop wireless sensor networks,' In Proceedings of 6th European Conference on Wireless Sensor Networks, pp.327–342.
13. Daojing He, Sammy Chan& Mohsen Guizani, 2015, 'Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks', IEEE Transactions on Wireless Communications, vol. 14, no. 1, pp. 387-397.
14. Daojing, He, Jiajun, BU, Sammy Chan & Chun Chun2011, 'Distributed Access Control with Privacy in Wireless Sensor Networks', IEEE Transactions on Wireless Communications, vol.10, no.10, pp.3472-3481.
15. Daojing, He, Sammy Chan & Mohsen Guizani2015, 'Secure and distributed data discovery and dissemination in wireless sensor networks', IEEE Transactions on Wireless Communications, vol. 26, no. 4, pp. 1129-1139.