International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com‖ Volume 2 Issue 4‖ April 2016 ‖ PP 60-66

Cluster Head Selection in Wireless Sensor Networks

Blessy Varghese[1] Soumya P[2]
[1](*Computer Science Department, Thejus Engineering College/ Calicut University, India)*
[2] *(Assistant Professor, Computer Science Department, Thejus Engineering College/ Calicut University, India)*

ABSTRACT: Wireless sensor networks are wireless networks with sensors. Wireless networks are networks without wires. Energy consumption is remains a major challenge in wireless sensor networks. Energy saving can be achieve using good clustering. Clustering is defined as the dividing of sensor network in to small manageable units. Clustering approach is to improve the scalability of network (prolong) and lifetime of network. For better clustering, cluster head selection should be better. Introduce an algorithm for cluster head selection using different parameters like high energy, high throughput, minimum distance from base station and also consider the potential of each nodes. There is a chance for malicious node to become cluster head. So remove malicious nodes using Node Replication Attack Detection Protocol and Replay Attack Protocol. In clustering one node will act as a cluster head and remaining nodes will act as member nodes. Clustering is done using Association. Association means spatio-temporal stability. The cluster stable over a long period is the goal of this protocol.

KEYWORDS -Clustering, Cluster Head Selection, Cluster Member, Energy Consumption , Wireless sensor networks

1. INTRODUCTION

One of the vital activities in wireless sensor networks, to reduce energy consumption networks is clustering. In clustering, one node is selected to be a cluster head. Cluster head handles majority of the processing for the nodes and computation in cluster. Clustering is very important process in network, because data transfer between clusters Wireless Sensor Networks cans be used in agricultural fields, military fields, smart homes, tracking systems, environmental fields etc. The most important concern of protocols in wireless sensor networks are to control the energy consumption and maintaining the security in network. Due to extensive use of wireless sensor networks it is necessary to improve its security.

WSN nodes are prone to physical attacks, hence some security advanced methods should also be included in cluster based routing protocols for the both requirements to go hand in hand. The key requirements of security includes authentication, secrecy, integrity, resilience against node capture, resistance against node replication, etc. and that for energy efficiency includes network connectivity, maximum supported network size, minimum memory storage, low computational and communication overhead.

A clustered design organises the sensing element nodes into clusters. A dedicated node called as cluster head governs each cluster. The nodes in the cluster communicate directly to its cluster head and then to the base station. The sensed data gathered by all the members in each cluster is fused by the cluster head and then the aggregated message will be sent to the base station. The advantages of WSN clustering include more scalability, aggregation of data, less load, collision avoidance, less energy consumption, etc.

2. RELATED WORKS

Heinzelman *et al. [1]* introduced a Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH selects the CHs randomly. This is the main goal of the LEACH. Selection of CHs randomly, so high energy is dissipated in the communication to the BS. LEACH has two phases, first phase is Set-up phase and second phase is Steady-state phase. In set-up phase, all nodes decides to become CH or not for that round. The decision of CHs is decided by percentage of Cluster Heads in the network and how much the node become a CH. If value of the node is less than the threshold then that node become a Cluster Head (CH).

Younis *et al. [1]* proposed a Hybrid Energy-Efficient Distributed clustering (HEED). HEED is a multi-hop clustering algorithm. HEED is an energy-efficient clustering routing with unambiguous concern of energy.

HEED does not selects CH randomly. HEED is very different from LEACH. The way of formation of cluster is achieved on the combination of two factors. First factor is communication cost of intra-cluster and second factor is residual energy. In HEED, Cluster Head have comparatively high average residual energy related to MNs.

3. PROPOSED SYSTEM

Register all nodes to be clustered. Then clustering is done based on association between nodes. Then select nodes with high energy, high throughput and minimum distance from BS using Secure and Fault Tolerant Clustering Algorithm. Find the potential for all other nodes. If calculated potential greater than Threshold, then sort nodes & select largest potential node. Then again checking whether malicious nodes are present. If detect malicious node, remove the node. There is a chance for Highest potential node to become malicious. Send broadcast message as CH to other nodes. Then send data through Cluster Head. Fig 1. Shows General Data flow Diagram.

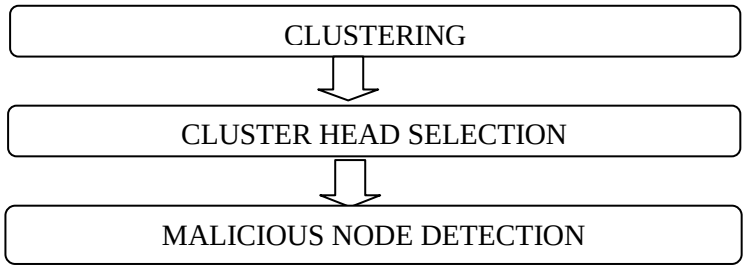

Fig 1. General Data flow Diagram

3.1CLUSTERING

Register all nodes to be clustered & given representation like node1,node2,…nodeN. After registering all nodes, nodes must be clustered. In a cluster one node will act as CH .Other cluster nodes act as cluster members (CM).

Clustering is defined as the dividing of sensor networks into small manageable units. Clustering approach is to improve the scalability of network (prolong). One node will act as a cluster head (CH) in cluster & remaining nodes will act as member nodes (CM). Clustering helps to reducing number of exchanged communications in network. Each communication in cluster, is handled by cluster head (CH).

3.1.1 CLUSTERING BASED ON ASSOCIATIVITY

The associativity based clustering[7] is present on cluster formation scheme. In cluster formation scheme forms clusters based on the spatio-temporal stability. Spatio-temporal stability of the mobile stations forming the ad hoc network. Goal of this protocol is to form clusters in such a way that the cluster is stable over a long period of time.

The node selected as the CH is such a way that it has maximum associativity as well as satisfies a minimum connectivity requirement.

The CH periodically sends cluster head beacon (CHB) which has the format as shown below and serves to advertise the existence of the cluster.

3.2 CLUSTER HEAD SELECTION

A cluster head (CH) is selected for each cluster based on the energy level of the node or distance based also. The main objective is to make only the cluster head communicate with the base station so that the remaining node can be put to a sleep state. Selection of cluster head has a vital role in clustering.

Selection of cluster head is good manner, then communication between clusters is easily taken. There is chance of errors in cluster head selection. There is a chance for cluster head to be malicious. So checking whether nodes are malicious, is very important. Here Fig. 2. shows a cluster head model in wireless sensor networks.

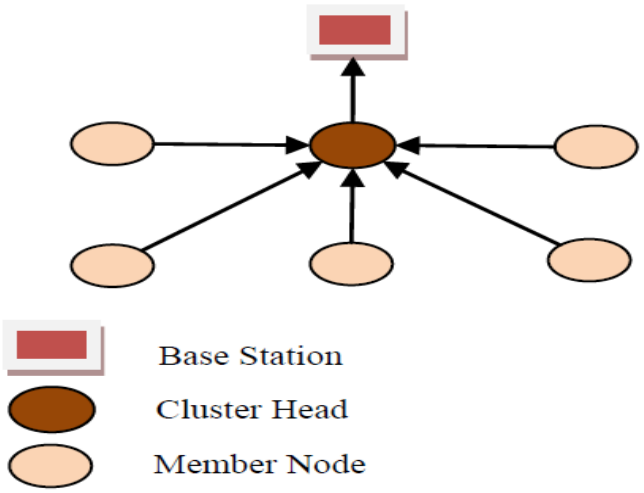

Fig. 2. Cluster Head Model

3.2.1 SELECT HIGH ENERGY, THROUGHPUT & MIN DISTANCE NODES

Secure and fault tolerant clustering algorithm[5] used for cluster head selection in wireless sensor network. Secure And Fault Tolerant Clustering Algorithm selects the nodes having the threshold value above the average. From the selected nodes, the node with maximum energy, at a minimum distance and having maximum throughput is selected as the cluster head .The method is dynamic in nature because selection process is refreshed periodically.

To select cluster head (CH), high energy, high throughput and min distance are major factors. Selection of the Cluster Head is a tedious job in wireless networks. The eligible node for the CH should have

1. Minimum distance from the sink node.
2. Highest energy.
3. Highest throughput.

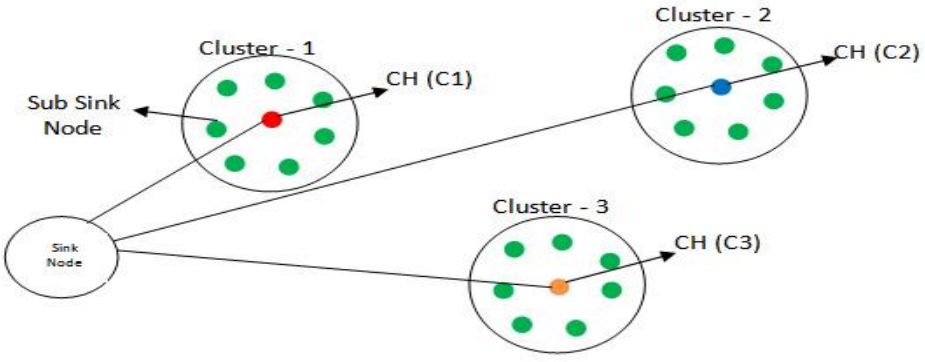

Fig. 3. Cluster Formation

Network of sensor nodes is divided into different clusters. Every cluster chooses its Cluster Head(CH) & others act as cluster members. CH of each clusters communicates with the sink node. There are 3 clusters are shown in figure. Cluster-1 (C1), Cluster-2 (C2), Cluster-3 (C3) are three clusters. A node is eligible to become a cluster head (CH) if it has the highest available energy, highest thoughput, minimum distance from the Base Station or sink node and high throughput value as depicted in fig. 3.

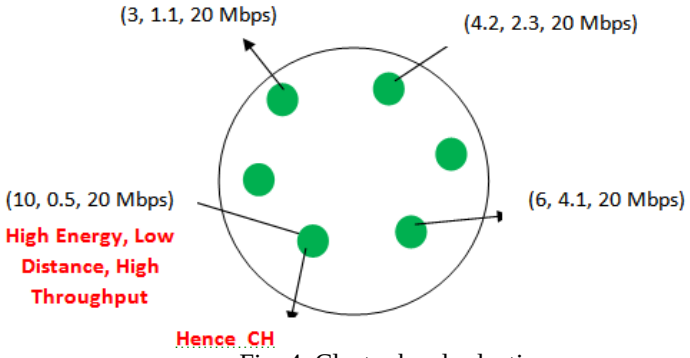

Fig. 4. Cluster head selection

Here shows cluster head selection from cluster members(CM). In each cluster (energy, distance, throughput) is calculated & evaluated. In figure all nodes have same throughput. If throughput same for all nodes ,then consider other parameters. In the fig. 4. Highest energy & minimum distance from BS is shown. Then node (10, 0.5, 20Mbps) is selected. Because the node have high energy, low distance from base station (BS), high throughput compared to other nodes.

Fuzzy System design for cluster head selection.
Fuzzification of inputs and outputs:

INPUT VARIABLES:
(RESIDUAL ENERGY) Residual Energy: For node to become a CH it should have more RESIDUAL ENERGY compared to other nodes.
(REACHABILITY)Node's reachability: It is measure of how much the node is reachable to its neighbour nodes within its transmission range. Reachability *r(i)* of a node *i* is defined as,

$$r(i) = \frac{1}{N \cdot \left(\sum_{j=1}^{j=N-1} dij \right)} \tag{1}$$

Where N is number of nodes (found during the neighbor finding), dij is distance between node i and j. For a node to become a CH it should have more number of neighbouring nodes and hence a lower value of REACHABILITY.

Link Quality Indicator/distance of node from BS (LQI/DISTANCE): Link Quality Indicator (LQI) characterizes quality reception of a packet at a node. It is defined in 802.15.4 standard and it can be easily estimated by chips. LQI is divided by distance of node from Base Station. With fixed message length, deterioration in quality of reception of a packet is marked with decreased LQI. Further, a lesser distance of node from BS ensures energy savings in communication to BS. Thus for a node to become a cluster head it should have a high LQI and should be at a lesser distance from the BS.

OUTPUT VARIABLE:
Potential (POTENTIAL): It is a node's ability to become a cluster head. A large value of POTENTIAL indicates more ability of a node to become a cluster head.

Variables used to represent RESIDUAL_ENERGY, REACHABILITY and LQI/DISTANCE are divided into three levels: medium, low and high. The linguistic variable POTENTIAL is divided into seven levels: very small, rather large, large, small, rather small, medium, and very large.

Defining membership functions: Triangle and trapezoidal membership functions are used, since their degree can be easily determined. Triangle membership functions are represents the fuzzy input sets medium and trapezoid membership functions to represent low and high fuzzy sets. Similarly, triangle membership functions are represent output sets small, rather small, medium, rather large, large and trapezoid membership functions to represent very small and very large fuzzy sets.

Application of fuzzy rule evaluation and fuzzy operators: With 3 levels and 3 input variables for each, there are possible combinations for Rule base. Table. 1. shows the rule base defined using "if then" rules with "and" operators among input variables.

Output Aggregation: For values of 3 inputs there will be multiple rules are considered. According to degree of membership for all rules fired, the outputs are unified. The maximum region covered for the output value is taken.

The aggregate of a fuzzy set encompasses a range of output values, and so must be defuzzified in order to resolve a single output values from set. Centroid method is used for defuzzification.

Table. 1. Fuzzy rule base for cluster head selection

L=Low, M=Medium, H=High, S=Small, RS=Rather Small, VS=Very Small, L=Large, RL= Rather Large, VL=Very Large				
Node no	Antecedents			Consequents
	RESIDUAL_ENERGY	RECHABILITY	LQI/DISTANCE	POTENTIAL
1	L	L	L	S
2	L	L	M	RS
3	L	L	H	M
4	L	M	L	S
5	L	M	M	RS
6	L	M	H	M
7	L	H	L	VS
8	L	H	M	S
9	L	H	H	RS
10	M	L	L	RL
11	M	L	M	RL
12	M	L	H	L
13	M	M	L	L
14	M	M	M	RL
15	M	M	H	L
16	M	H	L	RS
17	M	H	M	M
18	M	H	H	RL
19	H	L	L	RL
20	H	L	M	L
21	H	L	H	VL
22	H	M	L	L
23	H	M	M	RL
24	H	M	H	L
25	H	H	L	M
26	H	H	M	RL
27	H	H	H	L

Each node calculates value of POTENTIAL using fuzzy if-then rule discussed above. If potential >T % (Threshold value varies from 1 to 100) then node becomes a COMPETITOR node for being a cluster head. Value of T must be selected such that it guarantees enough COMPETITOR nodes for quality cluster head selection and also results in less control message overhead. Each node then uses a non-persistent CSMA MAC protocol to advertise a COMPETITOR_MESG (containing its POTENTIAL, ID, location) to reach nodes within its transmission range. The node with highest value of POTENTIAL becomes cluster head (CH).

3.2.3.1 DATA GATHERING AT CLUSTER HEAD

Once TDMA schedule is known to all cluster nodes data gathering operation starts. It is broken into frames. The CMs send their data packets to cluster head (with transmit power enough to reach its CH) once per frame during their allocated transmission slot to reduce collisions. Its radio is turned off for rest of the time to save energy. On receiving data packets, cluster head performs data aggregation and aggregated data packets are relayed to BS through several cluster heads during data transfer to BS.

3.2.3.2 DATA TRANSFER TO THE BS

Data transmission to BS is carried out using dijkstra's shortest path routing algorithm through cluster heads in a multihop manner.

3.2.3.3 MALICIOUS NODE DETECTION & REMOVAL

All detected malicious nodes are must removed in clustering, because there is a chance for malicious node to become cluster head. So checking the node whether it is a malicious node is very important task in cluster head

selection. When we remove malicious nodes, chance of cluster head to become malicious is comparatively low. Malicious node detected using Node Replication Attack Detection Protocol & Replay attack detection protocol. One of the common attacks is node replication attack or clone attack, where an adversary node captures some nodes and makes copies or duplicates of original node including all information such as cryptographic and then inserts these copies in network. These copies use the same ID as the original node in the network. It takes full control over the network. Consequence of this attack is modify the data, injecting false data, dropping packets, initiating a warm-whole attack, thus all these results in leaking of authorized data to an adversary. Several attacks includes Sybil attack, Denial of Service, black hole attack, attacks on information, warm hole attack and clone attack [3]. One of the common attacks is node replication attack or clone attack, Node Replication Attack Detection Protocol for the detection of replicas in the network. Node Replication Attack Detection Protocol [3] the witness is selected dynamically using randomized hash function.

Replay Attack Detection Protocol[2] control traffic is signed for every hop. This means only one signature is needed, although several messages are stacked in one packet. To prevent replay attacks, timestamps are used. To exchange these timestamps in the initial connection of two nodes, a two-way timestamp exchange mechanism is utilized. The solution does not rely on synchronized time. The Replay Attack Detection Protocol sequence numbers are also weak because of their length.

4. CONCLUSION

Wireless Sensor Networks must be energy efficient to prolong network lifetime. To achieve enhancement in network lifetime, efficient communication and reliable in WSNs, deploying a good clustering technique is essential.

Clustering is done using Associativity. The associativity based cluster formation scheme forms clusters based on the spatio-temporal stability. Secure& Fault Tolerant Clustering algorithm works on sensor networks, the complete process of selection is refreshed after every second to finalize the cluster head. In this, first of all the nodes having threshold value, above the average threshold value for of the network are termed as eligible for the cluster head. From these eligible nodes, the node having maximum energy available and node at a minimum distance from sink and having maximum throughput is selected as cluster head node. Using fuzzy rules potential value calculated for each node. After sorting nodes by potential value, again checking whether nodes have malicious behaviour. So there is no chance for a malicious node to become cluster head. Having all these features better cluster head selection is possible. Better cluster head selection increase security in data transfer through WSN. Secured clustering increases the lifetime of wireless sensor network.

Detect malicious nodes and never allows them to be the cluster head. Node Replication Attack Detection Protocol is used to detect malicious node. Clones are generated some malicious nodes. Node Replication Attack Detection Protocol detect clones & Replay attacks detected using replay attack detection protocol. Replay attack detection protocol is based on timestamps.

REFERENCES

Journal Papers:

[1] Suhas K. Pawar, Abhishek R. Tawde, ArchanaPokharkar, PriyaPanjwani, Prof.SuhasPatil "*A Survey of Cluster formation Protocols in Wireless Sensor Networks*";2014 p. 40-49

[2] Andreas Hafslund, Andreas, Roar Rotvik, Jon Andersson and Kure *"Secure Extension to the OLSR protocol*", OLSR Interop and Workshop, 2004.

[3] P.Abinaya, C.Geetha "*Dynamic Detection of Node Replication Attacks using X-RED in Wireless Sensor Networks*" IEEE 2014 International Conference on Information Communication and Embedded Systems (ICICES) - Chennai, June 2014

[4] Akshay Kumar, Payal Pahwa, Deepali Virmani, Sahil, Vikas Rathi, Sunil Swami *"Dynamic Cluster Head Selection Using Fuzzy Logic on Cloud in Wireless Sensor Networks"* , International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India

[5] Deepali Virmania, Savneet Kaurb, Satbir Jainc: *"Secure and Fault Tolerant Dynamic Cluster Head Selection Method for Wireless Sensor Networks"* International Conference on Information and Communication Technologies (ICICT 2014)

[6] Sachin Gajjar , Mohanchur Sarkar "*Cluster Head Selection Protocol using Fuzzy Logic for Wireless Sensor Networks"* International Journal of Computer Applications (0975 – 8887) Volume 97– No.7, July 2014

[7] Arvind Ramalingam, Sundarpremkumar Subramani, and Karthik Perumalsamy *"Associativity based cluster formation and cluster management in ad hoc networks*".