

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 4, Issue. 10, October 2015, pg.61 – 68

REVIEW ARTICLE

Review Paper on Enhancement of Least Fault Clustering Protocol to Reduce Energy Consumption in Wireless Sensor Nodes

Bhupinder Kaur¹, Mankirat Kaur²

PG student ECE Department, CGC College of Engineering, Landran, Punjab¹

PG student ECE Department, CGC College of Engineering, Landran, Punjab²

ABSTRACT

Recently the implementations of wireless sensor networks have developed immensely. There is one device which is used in wireless sensor networks (WSNs) to increase the lifetime of the network and give very effective functioning process that is clustering. It is the process in which the whole section or part is divided into small parts which understand the domain of sensor network in the directions of clusters. A carrier or head is chosen by each cluster which is called as cluster head. In the cluster the cluster head is chosen by the sensor nodes. If the clustering is very effective then we can save lots of energy in the network. The credibility of WSNs is influence by faults which is occurred by many reasons like if the hardware is in the defective manner, software defect and disruption. The WSNs are not ready to handle this type of situations in overall lifetime. In this paper we introduce a survey on the access of fault tolerance and its location in clustering protocol or we studied the methods of detecting and recovering faults. And the main thing is by using low energy protocols we have to send the information in an effective way from upper level to base station means one end to another end.

Keywords: cluster count, lifetime, wireless sensor networks, cluster density

1. INTRODUCTION

Wireless Sensor Network is an appearing technology for supervising the physical world. Wireless Sensor Networks are defined as the accumulation of stationary nodes or mobile which are capable to communicate with each other for conveying information or data more effectively and independently [1]. The wireless sensor networks are made up of wide number of small sensor nodes which have narrow energy. The significant necessity for the applications of wireless sensor networks are extend the network for a long time, to adjust the network with specific conditions, the moveability of the node and the symmetry of the node. In wireless sensor networks (WSN) have restricted energy source, so the main intend is to improve the network for lifelong by symmetry or balancing its energy. To improve the network for lifetime dynamic clustering is to be used. Sensor networks are made up of few sensors which is performed by battery and the main aim of this, to collect the data and then further send it to the base station. The sensor networks is composed of comprehensive, working communication skills which makes it capable to supervision and reaction the particular occurrence and circumstances in particular surrounding. WSN are made up of hundred to thousand of nodes. These nodes gather information and then send the information to the administrator. Each node is linked with one or distinct sensors. Sensor nodes are restricted resource of Power, Processor, Recollection and the range of frequencies within the band [2]. In WSN the main restriction is there is restricted battery power which performs a huge impact on lifelong characteristics of the network. To fulfill energy consumption and productivity requirement many routing methods were designed for WSN. Competence, adjustment and lifetime of WSN is increased by hierarchical routing. In this routing is done according to the rank. In this the sensors are arranged themselves into clusters and every cluster have a cluster head of its own. The main work of cluster heads is to supply information between sensor nodes and the base station [1].

The Figure (1)[3] shows how every cluster have a cluster head which gather information from its cluster group, accumulate it and then sends it to the base station. In this the nodes 1.1.1, 1.1.2, 1.1.3,1.1.4,1.1.5 and 1.1 design a bunch or cluster with node 1.1 and it becomes as the cluster head. Similarly other cluster heads are also made by this procedure. In this the cluster heads changed their position and make a cluster with node 1. So the node 1 becomes a second straight cluster head. And by this way means this process is done again and again and then the hierarchy of the clusters is made and in this the higher level clusters nodes straightly communicate to the base station [3].

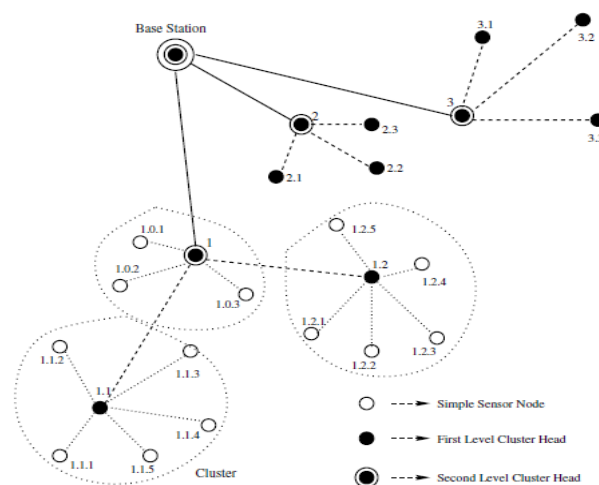


Figure 1. Hierarchical Clustering

2. CLASSIFICATIONS OF CLUSTERING PROTOCOLS

In this we talk about the arrangement of the characteristics which is being used to differentiate the clustering protocols for WSN.

2.1 CLUSTERING METHOD

The two fundamental access for the harmony of whole clustering procedure are centered and allocated. In the allocation of the clustering in which every sensor node may activate its own algorithm and decides for becoming the cluster head. In the center of the clusters the power group of the nodes making cluster heads and clusters. So that the Hybrid scheme is to be implemented there.

2.2 CLUSTER PROPERTIES

There are many properties of the clusters which are used to form the clusters.

2.2.1 Cluster Count: In this we enumerate the number of clusters in one orientation.

2.2.2 Cluster Size: In this we studied about the cluster size is the greatest route length between the groups of nodes from cluster head.

2.2.3 Cluster Density: It is defined as the ratio of the number of cluster group in the cluster and cluster area.

2.2.4 Message Count: In this the number of intimation is needed for cluster head choice [4].

3. RELATED WORK

Ruben Rios and Javier Lopez in 2011 [5] work on the location awareness in the wireless network. Wireless network are work with the sensor node that are not so much costly but no of thing are effected the sensor such as temperature, location, humanity etc. The security of the network play the important role for data security when the information are gather about the traffic load, location of the network it's can't be access by any one[6]. Packet are track by the attacker so for the security purpose the packet are send from sender to receiver by different path. Ozturk defined there are no of protocol are used for the routing purpose but with low security.

3.1 Contexts-Aware Location Privacy

Context-Aware Location Privacy work with the sensor node to take advantage and find the location of node and then send the packet to the receiver node. This technology is used mainly for capture the location of the moving object. Phantom Routing [7], two-way greedy random walk routing [8], Random Parallel routing, cross-layer approach these are the different kind of the approaching that are used for the location protection purpose but there are some problems facing as shown in Figure (2) [5].

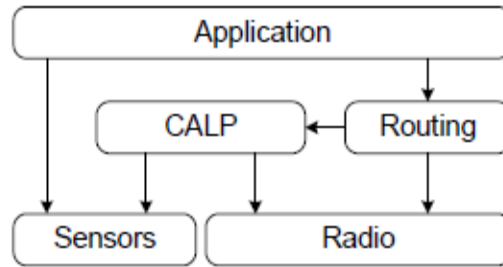


Figure 2. Components Interdependence

Shortest path CALP routing find out the shortest path from sender to receiver to send the packet. The nodes are activated and up to date time to time by receiving the information from the neighbors' node because it is a dynamic network as shown in table (1)[5].

Neighs	Angle	Distance
A	$\pi/4$	2
B	$\pi/5$	4
C	$5\pi/9$	5
D	$8\pi/9$	3
E	$11\pi/18$	4

Table1. Distance table

The long path not only time wastage but also required the high energy consuming and low protection from the attacker. Network is large work as the advantage for the user for in selection.

3.2 Cluster Based Fault

G. Vennira Selvi 1, R. Manoharan [9] defined the concept of the fault in crusting, fault reason, fault detection, fault recovery method and compare the different methods. As the time passed the no of user are increase day by day so fault accuracy are increase so the fault detection method not only reduced the fault in the network but also increase the life of network and save the energy in the network as shown in this figure.

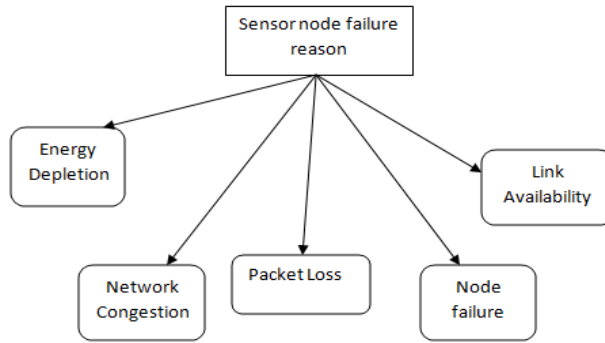


Figure 3. Sensor node failure reason

The node failure can be predicted by two methods that are given below.

1. **Monitoring Node Status:** - Before assign the node to user firstly check the statue of the node like node is free or not free. Chart is maintain for each and every node for holding all information like which frequency slot are allotted, how much energy are consume by the node etc.
2. **Monitoring Link Availability:** - Before sending the data on the link we must know that link is free or not if some other user sending its own data on the link than wait for the link.

3.3 Failure Classification [10]

Crash: - Crash is done by the services when some services are not responding to the request of the user. No of request sending before it declared to the failure.

Timing: - We all know that time is money when users send the request to a services and it response after time out that failure called the time failure. It used at some place where data and time are very closely related to each other.

Value:-It is occur due to the inaccuracy of the value in the response of some request. There are many reasons behind of this failure.

Arbitrary: - It includes all type of failure that not classified in above category. Byzantine identifies the different kind of failure that called arbitrary[11].

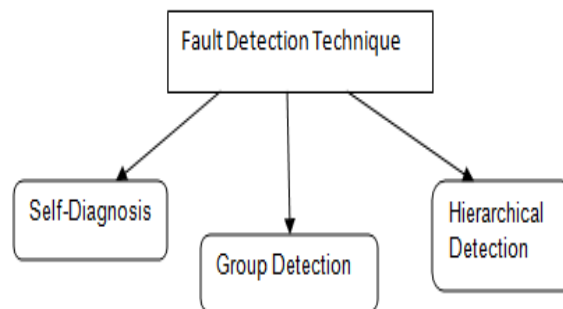


Figure 4. Fault Detection Technique

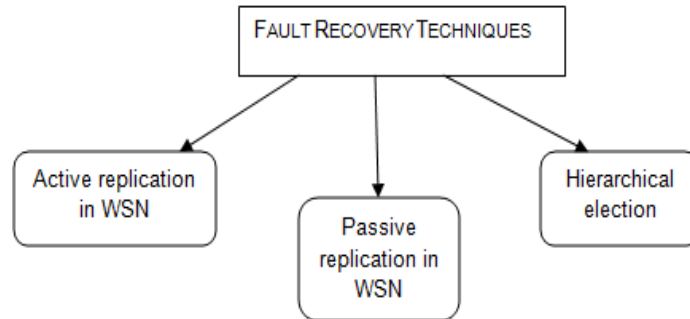


Figure 5. Fault Recovery Techniques

3.4 CLUSTERING ALGORITHMS AND PROTOCOLS FOR WSN

Probabilistic (random or weighted) clustering algorithms work in starting of the network a random no[12] assign to each and every node that are used for the path selection in random way and communication in the network. It helps us to find the shortest path in the network.

Energy-Efficient Communication Protocol for Wireless Micro sensor Network (LEACH) [13] that protocol assign an unique no to each node and each node can selected its own cluster head after each cycle random no are changed. So it saves the energy in the network.

A Stale Election Protocol for Clustered Heterogeneous Wireless Sensor Networks (SEP) in this protocol when first cluster node are dead then second are selected on the bases of the energy saved by node. It protocol don't required the information of the hole cycle like LEACH.

Hybrid Energy-Efficient Distributed Clustering (HEED) there is limited energy for the every node and control of the network is limited not fixed at the center point of the network.

No of the method are used in the clustering to make network fully balanced are user can be communication without any problem. Energy control is also a part of the protocol because the protocol maintains the network.

3.5 Energy-efficient fault-tolerant (EFP) protocol

Data is play an important role in today world we can think our life without the meaning full data that called the information. Information is just like blood in today fast world. Zohre Arabi and Roghayeh Parikhani [14] work on the sending the data from one end to other end ant it receive the data without any losses by using the low power with the help of the new protocol that are energy-efficient fault-tolerant (EFP) protocol that take the advantage of the another method.

Wireless sensor is the very small but very power full device that is used for the communication. The power is distributed at very low level. Sensors are work on the different level such as temperature, frequency, time etc. So they can be used at different place like monitoring, detection in the different place like battle field, mole, MNC and other place for security or facility purpose which is as shown in figure(6)[14].

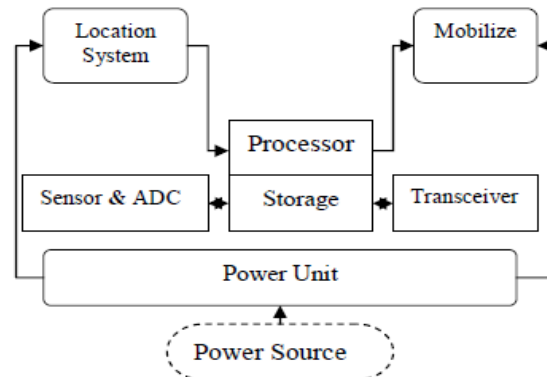


Figure 6. Sensor Node

In the energy-efficiency fault tolerant protocol when the user are sending the data all user are equal energy that send the data to the base station. Node those are more close to the base station and with the high power that are selected for the cluster head for data sending. Main objective of the EEF is to consuming of the energy in the each round of data sending that save the cost of communication.

3.6 Proposed Fault Tolerant Optimal Path Clustering Protocol (FTOCP)

FTOC protocol work with on dynamic cluster in which when sender send the data to the cluster head. The cluster head see the free path if path are not free than it go in the sleep mode or wait state that reduced the traffic list of the in the network. It balances the energy level of the node in the network and reduced the energy consuming in the network. And time to give getting the update of the network like free link, busy link, cluster node, cluster head etc as shown in Figure (7)[2].

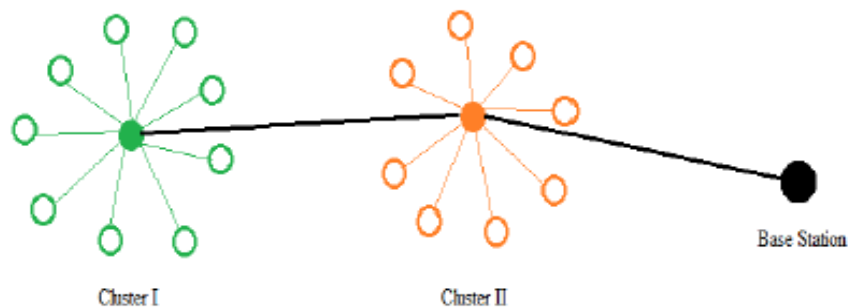


Figure 7. Cluster Communication

4. CONCLUSION

In this paper we discuss the location of the sensor node in the network and the attackers try to find out the location of the mode. So we required to send the packets from different paths. fault toleration means firstly try to avoid the fault so by doing this we save our time and energy but if the faults are in the nodes of the network at different levels then we try to detect it and recovery of the fault in the network as soon as possible that save the energy of the network and node. Energy is consumed by the node to transmit the signal. There are various methods available for the clustering.

REFERENCES

- [1]. Razieh Sheikhpour, Sam Jabbehdari, Ahmad Khadem-Zadeh “Comparison of Energy Efficient Clustering Protocols in Heterogeneous Wireless Sensor Networks” International Journal of Advanced Science and Technology Vol. 36, November, 2011.
- [2]. Deepali Virmani HOD (IT), BPIT, GGSIPU “ Fault Tolerant Clustering Protocol for Data Delivery in Wireless Sensor Networks” International Journal of Future Generation Communication and Networking Vol.7, No.2 (2014), pp.21-34 <http://dx.doi.org/10.14257/ijfgcn.2014.7.2.03>.
- [3]. Arati Manjeshwar and Dharma P. Agrawal Center for Distributed and Mobile Computing, ECECS Department, University of Cincinnati, Cincinnati, OH 45221-0030 “TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks” 0-7695-0990-8/01/\$10.00 (C) 2001 IEEE.
- [4]. Sanjeev Kumar Gupta, Neeraj Jain, Poonam Sinha “Clustering Protocols in Wireless Sensor Networks: A Survey” International Journal of Applied Information Systems (IJ AIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 5– No.2, January 2013 – www.ijais.org.
- [5]. Ruben Rios and Javier Lopez “Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks”, The Computer Journal, vol. 54, issue 10, pp. 1603-1615, Sept. 2011.
- [6]. Pai, S., Bermudez, S., Wicker, S., Meingast, M., Roosta, T., Sastry, S., and Mulligan, D. (2008) Transactional Confidentiality in Sensor Networks. IEEE Security & Privacy, 6, 28-35.
- [7]. Ozturk, C., Zhang, Y., and Trappe, W. (2004) Source-Location Privacy in Energy-Constrained Sensor Network Routing. SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, New York, NY, USA, pp. 88-93. ACM.
- [8]. Xi, Y., Schwiebert, L., and Shi, W. (2006) Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks. Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, April 8 pp.
- [9]. G. Vennira Selvi 1, R. Manoharan “Cluster Based Fault Identification and Detection Algorithm for WSN- a Survey” International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 10 – Oct 2013.
- [10]. Luciana Moreira S’a de Souza, Harald Vogt, Michael Beigl “A Survey on Fault Tolerance in Wireless Sensor Networks” <http://www.cobis-online.de/>.
- [11]. C.-Y. Koo. Broadcast in Radio Networks Tolerating Byzantine Adversarial Behavior. In Proceedings of the twenty-third annual ACM symposium on Principles of distributed computing, pages 275–282, 2004.
- [12]. Yan Zhang, Laurence T. Yang & Jiming Chen, 2010, RFID and Sensor Networks, Auerbach publication, International Standard Book Number: 978-1-4200-7777-3
- [13]. W. Rabiner Heinzelman and H. Balakrishnan, 2000. Energy-Efficient communication Protocol for Wireless microsensor networks, IEEE, Proceeding of the 3rd Hawaii International Conference on System Science.
- [14]. Zohre Arabi1 and Roghayeh Parikhani2 “EFP: NEW ENERGY-EFFICIENT FAULT TOLERANT PROTOCOL FOR WIRELESS SENSOR NETWORK” International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.6, November 2012