ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Enhanced Routing Scheme Using Dynamic Clustering For Energy Reduction in WSN

Amandeep Kaur
M.Tech Research Scholar,
Computer Science Section,
Yadavindra College of Engineering,
Talwandi Sabo, Bathinda, Punjab.
amandeepk235@gmail.com

Raj Bhupinder Kaur
Assistant Professor,
Computer Engineering Dept.,
Yadavindra College of Engineering
Talwandi Sabo, Bathinda, Punjab.
er.rajbhupinder@gmail.com

Abstract- *Wireless sensor networks (WSNs) have gained enormous attention for their wide range of applications such as environmental monitoring, military surveillance, health care, disaster management. Energy is the main constraint of wireless sensor network due to irreplaceable and limited power source of the sensor nodes. Clustering is the most popular topology control method to reduce energy consumption and improves scalability of WSN. Here we proposed a distributed fault tolerant clustering algorithm called DFCA which uses a cost function of the cluster heads for the formation of cluster. We also present a distributed run time recovery of the sensor nodes from the faulty cluster due to sudden failure of the cluster head. The experimental results show the strength of the proposed algorithm. We can remove this fault by using back up cluster or we can set the root information as a prefix.*

Keywords: WSN, Routing protocols, Energy Consumption, DFCA, Sensor Nodes.

1. INTRODUCTION

1.1 WIRELESS SENSOR NETWORK

WSN networks compose possibly large number of wireless sensor nodes that are resource constrained in terms of energy, memory, computing capabilities and communication strange. A sensor node will be also referred to as just node or sensor in the sequel. There are various type of applications of WSN that are already present in health care, navigation, rescue, intelligent transportation, social networking, gaming application fields, and critical infrastructure protection. This network is often unattended and deployed in harsh environments. WSNs are hence subject to several threats because of their nature. Basically in this paper the focus on the security and efficient use of the WSN. In particular, to cope with a fundamental, specific, and dreadful security attack WSNs are subject to; like the clone attack.

1.2 WSNs can be divided in two classes:

- Structured
- Unstructured.

1.2.1 Structured WSN: all or some of the sensor nodes are deployed in a pre-planned manner at fixed locations. The advantage of a structured WSN is that further devices can be deployed with lower network maintenance and management costs.

1.2.2Unstructured WSN: contains a dense collection of sensor nodes, which are randomly placed into the field .An ad-hoc deployment is preferred over a pre-planned deployment when the network is composed of hundreds to thousands of nodes in order to cover a larger area or when the environment is not directly accessible by humans attempting to construct WSN, e.g. Polar Regions, deep sea, or disaster areas such as a nuclear accident area or a war zone.

1.3 Energy Dissipation Model in WSN

1.3.1 Compressive Sensing

Wireless Sensor Networks (WSNs) are comprised of spatially distributed sensor nodes, where each node contains units for sensing, processing, and communicating data. In general, sensor nodes are assumed to have limited processing power and highly constrained energy resources. A typical WSN topology includes a base station - a powerful entity more capable than the ordinary sensor nodes with a significantly higher energy budget. Ordinary sensor nodes transfer processed or raw sensed data to the base station, which performs the final information aggregation and extraction tasks.

1.3.2 Mixed Integrated Programming

Mixed Integer Programming (MIP) based analysis of communication networks is extremely useful for uncovering the fundamental performance limits. Choosing an MIP based analysis method has a number of advantages. One of them is the abstraction from a specific protocol which enables us to investigate energy cost in ideal conditions with optimal routing decisions. Secondly, due to global knowledge in the optimization problem solver, the results can be obtained in an efficient and consistent manner.

1.3.3 Issues in WSN

The requirement of security not only affects the operation of the network, but also is highly important in maintaining the

availability of the whole network .It is necessary to know and understand these security requirements first before implementing security scheme for WSN.WSN should take the following major security requirements which are basic requirements for any network into consideration of secure mechanism:

1.3.4Data Integrity: Data integrity in sensor networks is needed to ensure the reliability of the data. It ensures that data packets received by destination is exactly the same with transferred by the sender and any one in the middle cannot alter that packet. The techniques like message digest and MAC are applied to maintain integrity of the data. By providing data integrity they are able to solve the Data integrity attacks. Data integrity is achieved by means of authentication the data content.

2.8.3Data Confidentiality: Confidentiality is to protect data during communication in a network to be understood other than intended recipient. Cryptography techniques are used to provide confidentiality. Data confidentiality is the most important issue in all network security. Every network with any security focus will typically address this problem first Data confidentiality of the network means that data transfer between sender and receiver will be totally secure and no third person can access it(neither read nor write) .Confidentiality can be achieved by using cryptography: symmetric or asymmetric key can be used to protect the data.

1.3.5 Data Availability: Availability ensures that the services are always available in the network even under the attack such as Denial of Service attack (Dos). The researchers proposed different mechanisms to achieve this goal. Availability is of primary importance for maintaining an operational network. Data Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. Availability ensures that sensor nodes are active in the network to fulfill the functionality of the network.

2. REVIEW OF LITERATURE

Yuling et al [1] suggested that wireless sensor network is composed by wirelesses sensor nodes, which have capabilities of perception, computing and communication. Network coverage is the main support technology in wireless sensor network application; it can achieve the physical information perception of the target region and the target object through the spatial distribution of sensor nodes in the network. Network coverage fundamentally reflects the network's perception ability for physical world. In addition, it largely affects the cost of the network and the performance of specific application.

Shim et al [2] suggested that many studies have explored data aggregation indifferent network architectures. There are two critical methods in data aggregation: Directed Diffusion in flat networks, and Tree-Based Data Aggregation in hierarchical networks. However, each data aggregation method has problems in multiple-sink environments. In Directed Diffusion, even if one sink has already reinforced a high-quality path to the sink, other nodes continue to receive exploratory events. In Tree based Data Aggregation with multiple sinks, high energy transmission costs are needed to make a tree for each sink node. Both waste much energy-transmission costs. In this paper, the propose Data Aggregation with multiple sinks in an Information-Centric Wireless Sensor Network, which can complement the drawbacks of each data aggregation method.

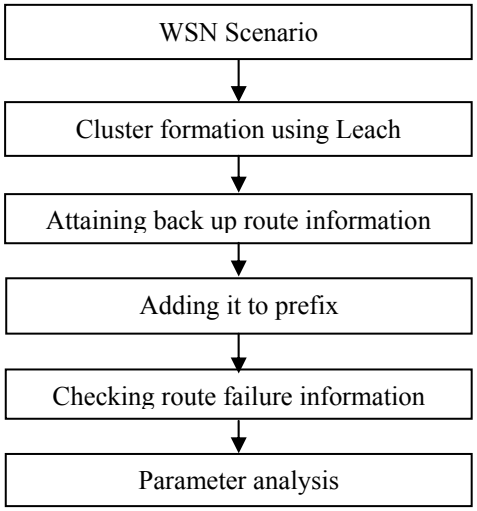
Yuan et al [3] suggested that one data aggregation method in a wireless sensor network (WSN) is sending local representative data to the sink node based on the spatial-correlation of sampled data. The proposed correlation degree is a spatial correlation measurement that measures the correlation between a sensor node's data and its neighboring sensor nodes' data. Based on this correlation degree, a data density correlation degree (DDCD) clustering method is presented in detail so that the representative data have a low distortion on their correlated data in a WSN. In addition, simulation experiments with two real data sets are presented to evaluate the performance of the DDCD clustering method. The experimental results show that the resulting representative data achieved using the proposed method have a lower data distortion than those achieved using the Pearson correlation coefficient based clustering method or the α-local spatial clustering method. Moreover, the shape of clusters obtained by DDCD clustering method can be adapted to the environment.

Manisha et al [4] suggested that a wireless sensor network is a group of devices that uses radio to monitoring and sensing physical or environmental conditions at different location. Commonly monitored parameters are pressure, temperature, humidity, wind direction and speed, sound intensity, power-line voltage, and chemical concentrations. However, Energy efficiency is an essential design issue is a challenging task. In this simulation the focused on energy parameter which is work on an energy efficient and reliable location wise data in wireless sensor network called as EERLA and compare with two DRINA and LBERP from this result more energy will save and also it improve network lifetime.

Omar et al [12] suggested that in the area of wireless sensor networks (WSNs), research on secure data aggregation has grown dramatically in the past few years, since the sensors are deployed in unattended and hostile environments. For this purpose, end-to-end solutions known as concealed data aggregation have been proposed to provide privacy between the sensors and the sink. The recent experiments showed that the Elliptic Curve El Gamal (ECEG) is the most suitable cryptosystem for WSNs in order to provide the end-to-end confidentiality with a high level of security based on elliptic curve cryptography (ECC). However, the execution time remains the major drawback due to the complexity of ECC operations and the nature of sensor nodes which are equipped with limited computer resources. Therefore, an efficient implementation of such operations is then crucial. In this paper, the present a fast and secure

implementation of ECEG in MicaZ mote, based on an enhanced version of Tiny ECC library, a fast scalar multiplication is employed, which is also secure against side channel attacks (in particular simple power analysis). Moreover, a fast point decompression algorithm needed for homo morphic operation is used to efficiently computing square roots in prime fields, satisfying p = 3 mod 4. Our results show that a secure encryption of ECEG takes only 1.29s, which is considerably better than previous software implementations on 8-bits platforms.

3. METHDOLOGY



Phase 1: Wireless scenario is generated by initializing all the scenario parameters which includes Queue type IEEE standard, Number of nodes, Protocol to be used, Antenna Type etc.

Phase 2: In Second Phase Leach protocol is installed and cluster formation is done on the basis of LEACH. Node with the highest energy is elected as a cluster Head.

Nodes in a cluster Communicate in Hierarchy like cluster head communicate with sub-cluster head & sub cluster head communicate with cluster member in the end all cluster heads communicate with base station.

Phase 3: As cluster communicates in hierarchy, Node is working like back nodes. Because if sub cluster head fails than data is recover through cluster member & if cluster heads fails than sub cluster is act like a recovery node.

Phase 4: In this phase failure information is finding out by calculating the energy of the nodes. The node with the highest residual energy will be cluster head for the next round.

Phase 5: In the end parameter analysis is done on the basis of Quality of service parameters (QOS) like Lifetime, PDR (Packet Delivery Ratio), delay, Throughput etc.

4. RESULTS

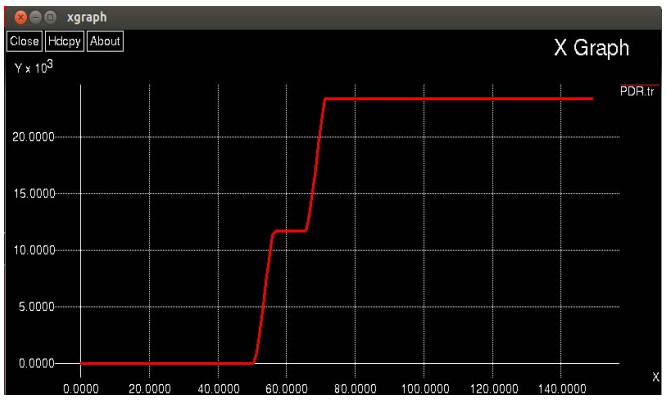


Fig 4.1 Packet Delivery Ratio

In this X-axis represent the Time and Y-axis represent the Bytes send over the network. This figure is use to represent the Packet Delivery Ratio. Packet Delivery Ratio is defined as the number of packet deliver with respect to time.

Fig 4.2 Life time

This figure is use to represent the Lifetime of a node. Lifetime is defined as the total time in which node can survive without any disturbance.

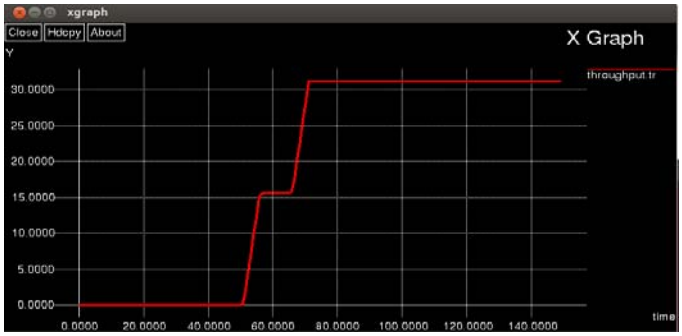


Fig 4.3 Throughput

This figure is use to represent the Throughput. Throughput is defined as the number of packet delivered successfully over the network.

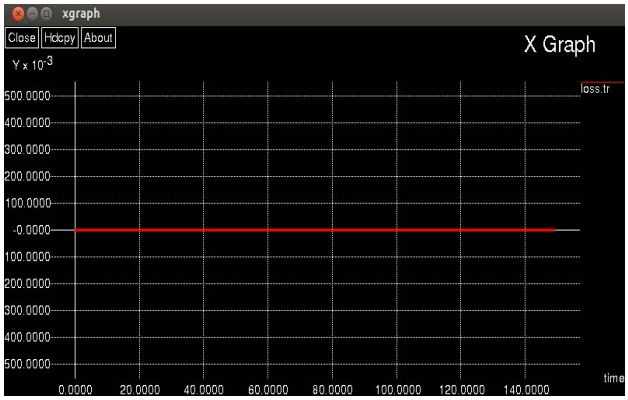


Fig 4.4 Packet Loss

This figure is use to represent the Loss of packets. Loss is defined as the number of packet loss when we transfer packets over the network

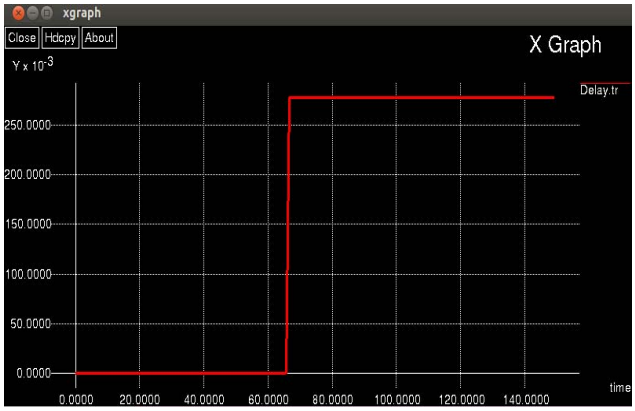


Fig 4.5 Packet Delay

This figure is use to represent the Packet Delay. Packet Delay is defined as the Delay between packets during transmission.

Table 4.1 Comparison Table based on performance evaluation parameters

Parameter	Purposed	Previous
Throughput	80 %	72 %
Packet Delivery Ratio	79 %	63 %
Packet loss	0	100
Average Delay	0.25 ms	0.5 ms
Energy Consumed	20 J	30 J

5. CONCLUSION & FUTURE SCOPE

A wireless sensor network is a gathering of specific transducers with a corresponding foundation for observing and recording conditions at diverse areas. Generally checked parameters are temperature, humidity, weight, wind direction and velocity, enlightenment force, vibration power, sound force, force line voltage, substance focuses, pollutant and basic body capacities. WSN is used for sensing the information from environment. These sensors have sensor range and sense the information from particular area. Various protocols were purposed for proper utilization of energy in wireless network. Leach was a basic protocol that was used as energy model in WSN. In this paper various approaches were described that were used for WSN. Leach is used in wireless sensor network and multi-hop leach protocol is used for energy consumed in a single hop for defining energy consumed in a single hop .By receiving various protocols the conclusion occur that leach is best protocol for WSN**.**

6. REFRENCES

[1] Yuling Lei, Yan Zhang ; Yanjuan Zhao "The Research of Coverage Problems in Wireless Sensor Network", pp. 31 – 34, IEEE, 2009.

[2] Yonghui Shim, Younghan Kim "Data Aggregation with Multiple Sinks in Information-Centric Wireless Sensor Network", IEEE Conf. on Data Aggregation, 2014, pp. 13-17.

[3] Fei Yuan "Data Density Correlation Degree Clustering Method for Data Aggregation in WSN" IEEE conference on IEEE Sensors Journal, 2014, pp. 1089 – 1098.

[4] Manisha V. Bhosle "An Energy Efficient and Reliable Location Wise Data Aggregation in WSN" IEEE conference on Computing Communication Control and Automation (ICCUBEA),2015,pp. 322 – 326.

[5] Omar Rafik Merad Boudia "Fast and secure implementation of ECC-based concealed data aggregation in WSN" IEEE conference on Global Information Infrastructure Symposium, 2013,pp. 1 – 7.

[6] Goran Horvat "Power consumption analysis and optimization of ARM based WSN data aggregation node" IEEE conference on Telecommunications and Signal Processing (TSP),2015,pp. 1 – 5.

[7] Roshan Zameer Ahmed "Data aggregation for pest identification in coffee plantations using WSN: A hybrid model" IEEE conference on Computing and Network Communications (CoCoNet),2015,pp. 139 – 146.

[8] Miloud Bagaa "Data Aggregation Tree Construction Strategies for Increasing Network Lifetime in EH-WSN" IEEE conference on Global Communications Conference (GLOBECOM),2015,pp. 1 – 6.

[9] Vv Enam, R.N "Energy efficient differential data aggregation in a dynamic cluster based WSN", IEEE Conf. on Collaboration Technologies and Systems (CTS), 2013, pp.580 – 583.

[10] Md Mizanur Raman, Hossain, M.A. ; Mahmud, M. ; Chaudry, M.I. "A Lightweight Secure Data Aggregation Technique for Wireless Sensor Network", IEEE Conf. on Multimedia (ISM), 2014, pp.387 – 392

[11] Mittal, R., Bhatia, M.P.S "Wireless sensor networks for monitoring the environmental activities",pp. 1 – 5, IEEE, 2010.
[12] Md Azharuddin, Kuila, P. ; Jana, P.K "A Distributed Fault-tolerant Clustering Algorithm for Wireless Sensor Networks", IEEE, 2013.
[13] Ozdemir, S., Cam, H. "Integration of False Data Detection with Data Aggregation and Confidential Transmission in Wireless Sensor Networks", IEEE Conf. on Networking, IEEE/ACM Transactions, 2010, pp 736 – 749.
[14] Xuhui Chen, Peiqiang Yu "Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes", pp. 2863 – 2867, IEEE, 2010.
[15] Yong-Sik Choi, Young-Jun Jeon ; Sang-Hyun Park "A study on sensor nodes attestation protocol in a Wireless Sensor Network", pp. 1738-9445, IEEE, 2010.