Fault Tolerant Clustering Mechanism for Wireless Sensor Network

[1]D. P. Mishra , [2]Ramesh Kumar
Research Scholar CSVTU, Professor BIT Durg
[1]mishradprasad@gmail.com, [2]rkbitd@rediffmail.com

Abstract: Wireless Sensor Network (WSN) is emerged as revolution in all the aspect from past few years, WSN gained attention of lots of researchers for using them in different applications. WSN is having unique specification of their own that distinguishes them from other network. Fault tolerance is one of the most significant and challenging area for WSN, since sensor nodes are prone to various types of attacks and failures due to hardware, battery power, malicious attacks, etc. Faulty sensors are likely to report arbitrary readings that do not reflect the true state of observed physical process. These faulty sensors nodes should be recognized and timely excluded from the data collection process inorder to ensure the overall data quality, so while designing and developing WSN based solutions, it is highly recommended to accomplish five key features in WSN solutions: scalability, security, reliability, self-healing and robustness. This paper will discuss different mechanisms used for fault detection and fault recovery in WSN and propose cluster based recovery technique.

Keywords: Wireless Sensor Networks, Fault Recovery algorithm, Data Fault Detection, Functional Fault, Cluster Head

1. INTRODUCTION

Wireless Sensor Networks have emerged as an important new area in wireless technology. A wireless network consisting of tiny devices, which monitor physical or environmental conditions such as temperature, pressure, motion or pollutants etc. at different areas. Such networks may be used for variety of applications like environmental, commercial, civil, military applications such as surveillance, vehicle tracking, climate and habitat monitoring, intelligence, medical, and acoustic data gathering. The key limitations of wireless sensor networks are the storage, power and processing [23]. These limitations and the specific architecture of sensor nodes call for energy efficient and secure communication protocols. The key challenge in sensor network is to maximize the lifetime of sensor nodes and the accuracy of data is very important to the whole system's performance, detecting faulty node is main challenge in network management. The accuracy of individual node's readings is crucial; the readings of sensor nodes must be accurate to avoid false alarms and missed detection. There are certain applications, whichare designed to be fault tolerant to some extent, by removing faulty nodes from a system with some redundancy or by replacing them with good ones, will significantly improve the whole system's performance and prolong the lifetime of the network. To overcome the burden of after deployment maintenance (e.g., remove and replace), it is essential to investigate methods for detecting faulty nodes.

2.SENSOR NETWORK FAULTS

Wireless sensor networks consist of a large number of tiny sensor nodes deployed in harsh environment for unattended operation to sense and forward some data to base station through single-hop or multi-hop transmission since sensor nodes have self-organized capabilities [1]. Since most of the sensor network operates in unattended environment, there is the possibility of fault due to hardware failure, energy utilization, security attacks and signal strength / signal obstacle [2]. **Fault** is an unintended defect that ultimately channelizes to the cause of an error. **Error** is an indication of false (incorrect) state of the system. Imperfection quality of the system state caused by error, ultimately leads to the failure. A **failure** is the condition where the system becomes ineffective to perform the intended regulated functionalities, due to error.

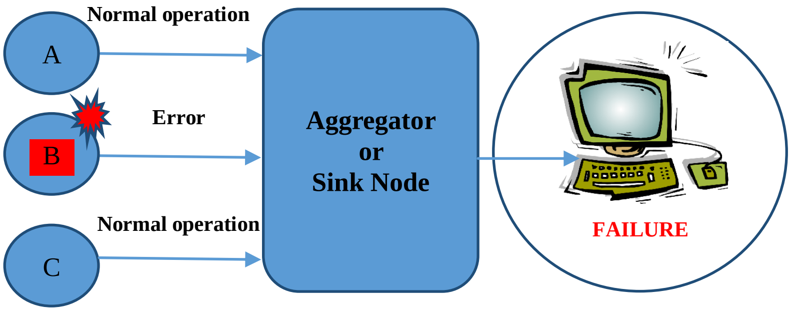

Fig.1: Relation between fault error and failure

Fig. 1 depicts the basic difference between fault, error, and failure. The principle operation of sensor node A, B and C are reporting periodical sensed data to the gateway node, which aggregates different generic sensor data's for future analysis. Each sensor service is normal until node B suffers a fault. Thus, the immediate occurrence of fault (any) causes an error in performing normal service by node B. Due to the occurrence of fault on node B, it provide an errored service to the gateway node. These errored services contain inappropriate information for the analysis of entire application/system. The faulty service provided by node B results as cause ofsystem failure.Fig. 2 shows sensor form, in which node no.13 is not responding, that isolates other part of networkthat results in collapse of application.

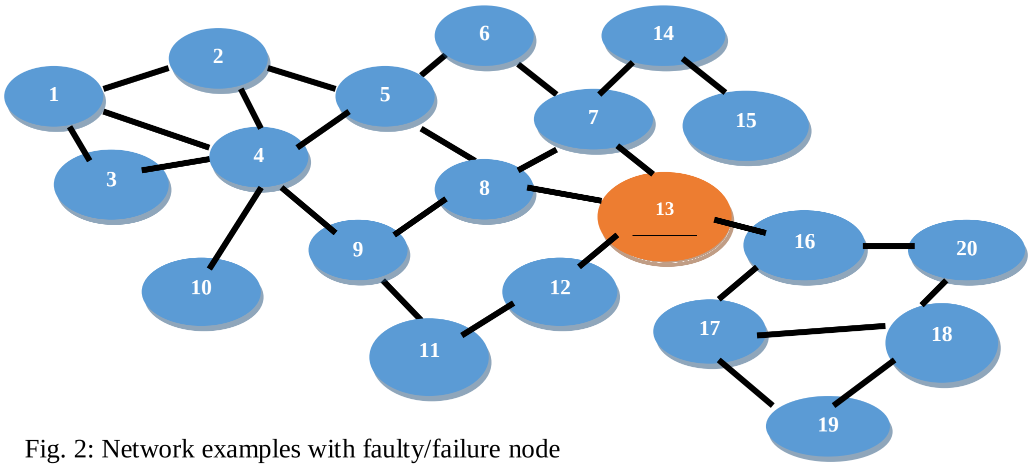

Fig. 2: Network examples with faulty/failure node

2.1 Types of Faults

Almost all the WSN researchers are asking a common typical question - "What will be the most vigorous causes and deep impact of fault on WSN?" There are different possible answers for this question. From [5], it's conceptually expressed or assumed that under any circumstance, entire functionality of WSN should not be disturbed as a whole in order maintain and ensure high reliability. First step to build a WSN fault tolerant system will closely relate various faults; inspect the variety and nature of faults. WSN faults are categorized into three major categories and they are Sensor reading faults, Software faults and Hardware faults. Each of these categories are elaborately depicted in Fig. 3.

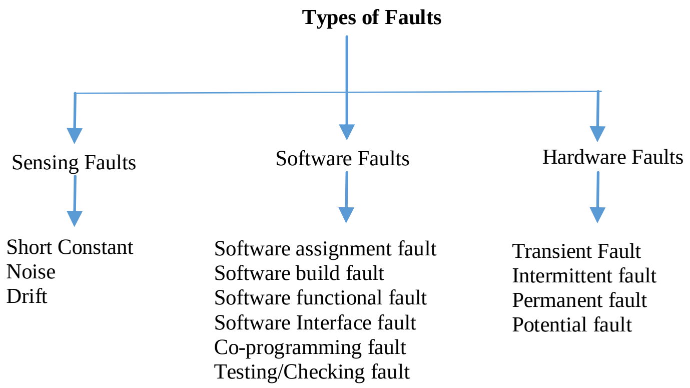

Fig. 3: Network examples with fault node

2.2 Generic lifecycle of Fault Tolerance:

Increasing fault tolerance potentiality of WSN depends on continuous well-organized multi-operational procedures of three phases (prevention, diagnosis and recovery), that are involved in FT management. On following analysis with three phases, a generic lifecycle has been furnished, which is depicted in Fig.4.

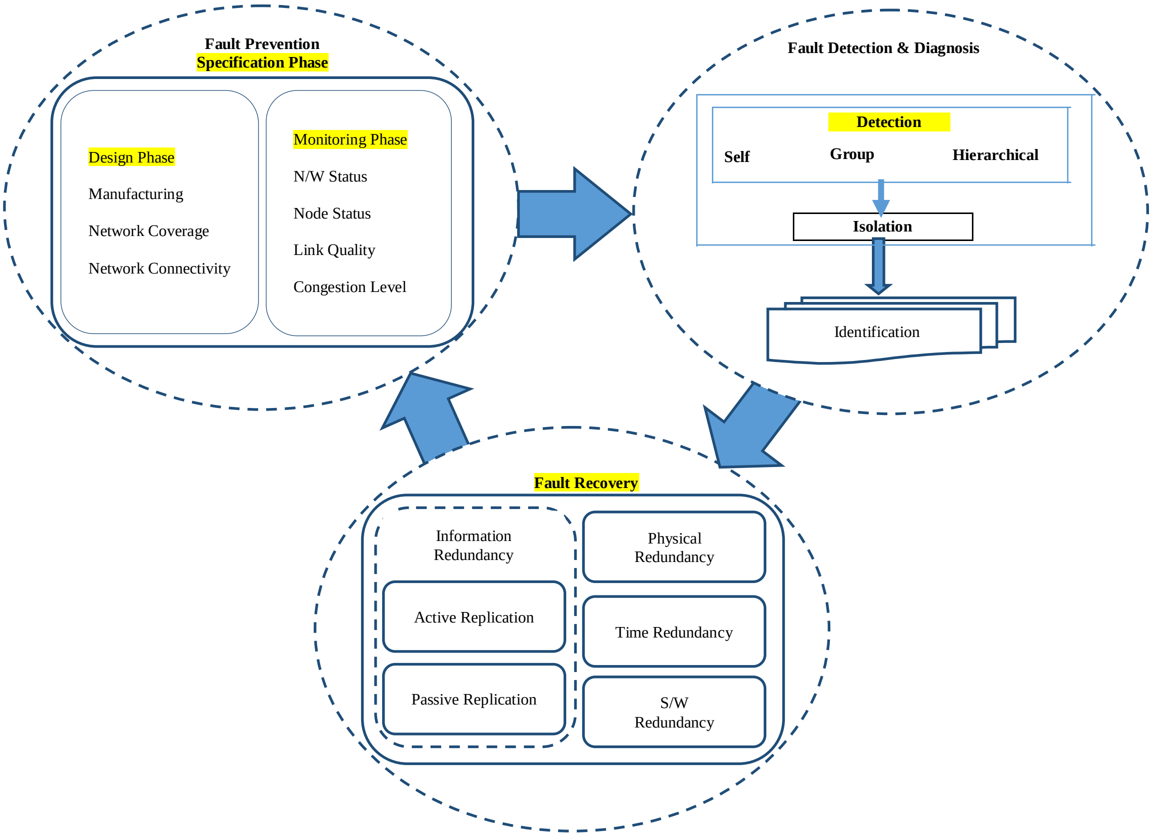

Fig.4: A generic life cycle of Fault Tolerance

2.2.1 Fault Prevention

Fault prevention is an act of pre-assessment and finding of an abnormal fault causing activities that usually takes place in WSN applications. So, responsibility or role of prevention can be incorporated along with the major concerned phases of WSN application design, they are i) Specification phase ii) design and development phase and iii) monitoring phase. During specification phase, it avoids incomplete specifications and equivocal specifications. By adopting suitable standard of quality for hardware components and certain definition of flow along with controlled structures at network coverage and connectivity level, ensures the involvement of prevention act in design and development phase. Generation of fault may happen by incorrect usage/handling of resources/events or functional degradation due to several factors. It is very important to have viable monitoring phase that would always be concerned to watch-out on node status, link quality and congestion level.

2.2.2 Fault Diagnosis

Since WSN experiences perpetual changes, stringent fault prevention enrolment may not ensure 100% prevention of fault invasion. A primary fault diagnosis system is always needed to detect and isolate the generated faults. Such a procedures can be handled in any of the following three ways i) self, ii) group and iii) hierarchical diagnosis at centralized-oriented or distributed-oriented networks. After the fault detection and isolation procedures, each isolated faults are to be identified, to study the characteristics and behavioral nature of that fault.

2.2.3 Fault Recovery

Fault recovery phase is the primary in-charge to evacuate the effects of faults through all the phases. It would be achieved by using appropriate redundancy techniques. The common redundancies applied at several levels are information, physical, time and software redundancies. Information redundancy provides FT by active/passive replication of required information

In case of active replication, all request are processed by multiple instance (all replicas) while in the case of passive, single instance process the request, only when it fails to do so, other instance takes the charge of processing the request. Physical redundancy ensures FT by providing additional equips, hence also be called as hardware redundancy. Similarly, software redundancy seeks to provide required redundant software code. Time redundancy attains FT capability by performing certain needed operations at several times.

2.3 Fault Detection Approaches:

Fault detection is the first phase of fault management; it deals with unknown failure that needs to be properly identified by the network system. To deal with faults in WSN, there are phases and they are Fault detection and Fault recovery. First phase is fault detection. There are two approaches for fault detection and they are centralized and distributed approach [7]

2.3.1 Centralized Approach

Centralized approach is a common solution to identify and localize the cause of failures or suspicious nodes in WSNs. Usually; a geographically or logically centralized sensor node (in terms of base station [14, 16, and 17], central controller or manager [4], sink) will take care of monitoring and tracing faulty nodes in the network. Almost all these approaches consider the central node has unlimited resources (e.g. energy) and is able to execute a wide range of fault management maintenance. They also believe the network lifetime can be extended if complex management work and message transmission can be shifted onto the central node.

Since base station, central controller or manager, sink node is used for monitoring and tracing the failed node in the network. [8][11] The Central node adopts an active detection model to take back the states of network performance and individual sensor nodes by periodically injecting queries to the network. Central node analyzes the information to identify and localize the failed or suspicious nodes. In [16], the base station uses marked packets (containing geographical information of source and destination locations etc.) to probe sensors. It relies on nodes response to identify and isolate the suspicious nodes on the routing paths when an excessive packet drops or compromised data has been detected. In addition, the central manager provides a centralized approach of prevention from potential failure by comparing the current or historical states of sensor nodes against the overall network information models (i.e. topology map, and energy map). Only issue of this approach is that central node becomes data traffic concentration that leads to high message traffic and quick energy utilization specific areas of network and specially nodes closer to base station. As a summary, the centralized approach is very accurate and efficient to identify the WSN faults.

2.3.2 Distributed Approach

In this case Central node should not be informed unless there is really a fault occurred in the network i.e. all the nodes are allowed to make various decisions before communicating with the central node. [9]. The distributed approach believes that more decision a sensor can make, the less information needs to be delivered to the central node. In other word, the control center should not be informed unless there is really a fault occurred in the network. It addresses the use of decision fusion center (i.e. several fusion nodes across the network) to make the final decisions on suspicious nodes in the network [16, 18, 19, 20]. Some of the examples are

- Self-Detection of Node- Faults occurred by depletion of energy detected by sensor node itself. [6]
- Neighbor Coordination- Nodes communicates with neighbor nodes to identify the failed nodes.[9]
- Clustering approach - Cluster head identifies faulty node by sending the heartbeat messages. In case of fault detection the information is passed to the all clusters

Pros and cons of different techniques discussed is summarized in table 1 along with their working principles

Table1- Comparison of different fault detection techniques

Technique	***Working Principle***	***Pros***	***Cons***
On-line Fault Detection	Approach applied on arbitrary type of fault model, with probability based identification of faulty nodes	Accuracy in presence of Gaussian noise even for relatively sparse networks.	Efforts restricted only to faults in sensors rather than taking other communication and computation units of a node into consideration
Centralized Fault Detection	Centralized sensor node takes responsibility of identifying and locating the failed or misbehaved node.	Accurate and Fast for identifying faulty node.	Central node becomes single point of data traffic concentration and also causes high volume of message and quick energy depletion
Sympathy [14]	Message flooding approach to pool event data and current states from sensor nodes to a Sympathy node which further transmits to sink node	Fetches data to a sympathy node rather than each node sending directly to sink node	Message broadcasting creates redundancy of data at sympathy node

WATCHDOG [15]	A node can listen on its neighbor if data packets have not been transmitted properly by its neighbors it is currently routing to.	Encourages concept of local decision-making. More decision a node makes the less will be required to deliver to sink node	Slow and error prone as it is always difficult to keep an eye on all its neighbors
FT-DSC Protocol	Clustered based approach in which CH receives info from members only when event of interest occurs	Energy saving by not delivering messages to CHs in every time slot of a frame	Selection of cluster head is always done on basis of level of energy remaining
FREM [16]	Only requires the touch set on the destination node for quick restart, the remainder of image is transferred after process is restarted on destination.	Allows fast restart of a failed process without requiring the availability of entire checkpoint image.	Issues with this are how to accurately identify the touch set, how to set the tracking window, how to load partial image on destination node.

3. BACKGROUND THEORY OF CLUSTERING

Low-energy adaptive clustering hierarchy (LEACH) [10, 12] is, a clustering based protocol that includes the features like –

- Randomized adaptive self-configuring cluster formation.
- Localized control for data transfers.
- It reduces the energy required for media access and data processing task like aggregation.

LEACH randomly selects a few sensor nodes as cluster heads (CHs) and rotates this role to evenly distribute the energy load among the sensors in the network. All the iteration specific to selection of CHs is called a round. The operation of LEACH is split into two phases: Set up & Steady

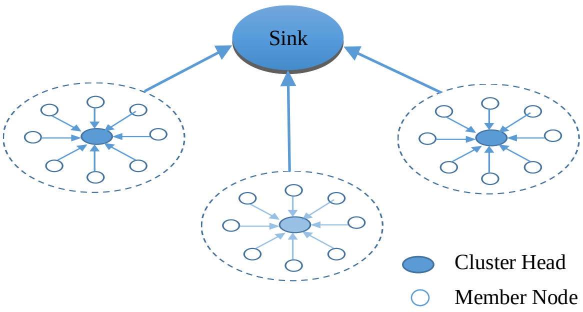

Fig.5: Leach Architecture

During the setup phase, a predetermined fraction of nodes, p, elect themselves as CHs as follows. Sensor node selects a random number, r, between 0 and 1. If the selected random number is less than a threshold value, T(n), then the concern node becomes a cluster-head for the current round. Threshold value T (n) is calculated with formula given below.

$$T(n) = \frac{P}{1 - p\left(r \bmod \left(\frac{1}{p}\right)\right)} \quad if\ n\ \in G$$

Where

P: is the desired percentage of nodes, which are CHs,
r: is the current round, and
G: is the set of nodes that has not been CHs inthe past 1/P rounds.

During steady state phase, data transmission takes place based on TDMA schedule and the CHs perform data aggregation through local computation. The BS receives only aggregated data from cluster-heads, leading to energy conservation. After a certain time, the network goes back into the setup phase again and enters another round of selecting new CH. Each cluster communicates using different CDMA codes to reduce interference from nodes belonging to other clusters.

3.1 Proposed Mechanism

There are four phases in this scheme – Advertising, Data Transmission, Fault Detection and Fault Recovery, which is depicted in Figurre-6

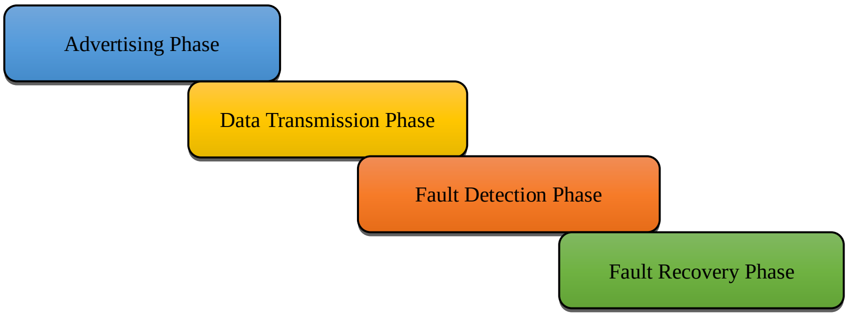

Fig.6: Four Phases of proposed Mechanism

As shown in Fig.-6, in First phase i.e. advertising phase, the clusters are prepared and selection of cluster heads (CHs) is done. After selection, the CHs advertise their selection to all neighboring or remaining nodes. All concerned nodes select their nearest CH based on the received signal strength during advertisement. Later on concern, CHs assign a TDMA schedule to their cluster members.

The second phase, data transmission phase, all subordinate nodes can start sensing and transmitting data to the cluster-head. After receiving data, the cluster-head aggregate it before sending it to the Base-Station (BS).

The third phase is the fault detection phase. In hostile environments, unexpected failure of CH may partition the network or degrade application performance. If no response comes from CH to BS or subordinate nodes within a time interval, BS marks or put flag for concern CH as a faulty node and forwards this information to the rest of the network and initiate fault recovery process.

In the final phase, cluster head immediately starts fault recovery processafter detection. When a faulty CH node is identified, all the cluster members associated with it are gradually informed about the CH failure. For the CH recovery operation, the sink node chooses a new CH from the cluster members, based on cluster member's sensor nodes residual energy. According to this scheme, simply replace the faulty cluster-head by the next highest energy node in the cluster.

3.2Fault Detection Algorithm

```
Step1. Initialize CH1 & CH2 & subordinates
Step2.  IF no response comes within a TDMA slot Then
Step3. Set CH1 as Faulty Step Else
Step4. For CH2
Step5. IF no ping message comes periodically Then
Step6. Set CH2 as Faulty
```

3.3 Fault Recovery Algorithm

```
Step1.   Start
Step2.   Initialize CHs & subordinates
Step3.   Compare residual energy of current CH (CHR) and each subordinate in the cluster.
         IF CHR less than each subordinate,      Then
         Replace CHR with next highest energy node.  Else
         Set CHR  as CH for next setup round.
Step4.   Stop.
```

3.4 Performance evaluation

The energy model used is a simple model shown in [19] transmitter, receiver dissipates energy to run the power amplifier to run the radio electronics. In the simple radio model [19], the radio dissipates Eelec = 50 nJ/bit to run the transmitter or receiver circuitry and Eamp = 100 (pJ/bit)/m2 for the transmit amplifier in-order to get acceptable signal-to-noise ratio. We have used MATLAB Software as the simulation platform[13] and utlised simulation parameters specified in Table2

Table 2 – Simulation Parameters

Simulation Parameter	Value
Terrain Dimension	1 KM^2
Total number of nodes in terrain, N	100 – 1500
Transmission range	100 – 450m
Cluster size limit, s	10 – 50
Supported degree, D	3 – 10

3.5 Characteristics of the Clusters

Fig. 7 depicts the percentage of cluster heads observed with varying cluster range. The cluster range was varied from 200 to 400. The size limit, S in our algorithm was set to 50 with admissible degree, D set to 3. The percentage of cluster heads was observed and noted for about 10 runs of the clustering algorithm. The percentage of cluster heads does not increase or decrease over various rounds of the algorithm. This is because for a total number of N nodes in terrain, the limit S is set to 50 leading to N/50 cluster heads or clusters. Due to this limitation the results do not having variation in terms of decrease or an increase in the cluster heads. Even though the percentage of cluster heads is not changing, the responsibility of cluster head is delegated or exchanged with the nodes in the network

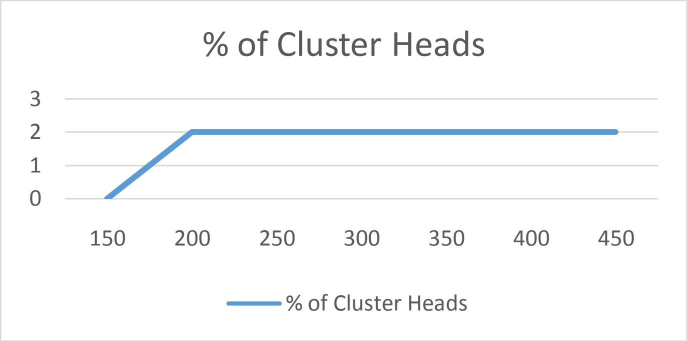

Fig. 7: Percentage of cluster heads observed with varying cluster range

3.6 Energy characteristics in Clusters Fig.-8 depict the energy drain during the cluster formation. Energy drain is the loss of energy in all the node after cluster formation and operation. Energy loss is based on the relation in the first order radio model. Total energy loss would be the energy loss due to transmission added to the loss due to receiving. Energy utilization depends on parameters used in first order radio model, distance and the number of bits, k. Energy consumption is also dependent on the no. of concerned nodes i.e. transmitting to and receiving from. In clustering algorithm the distance is sensing range, which is about 50 % of the transmission range. Also the number of nodes each node would handle is D. These two factors make energy loss regular and uniform

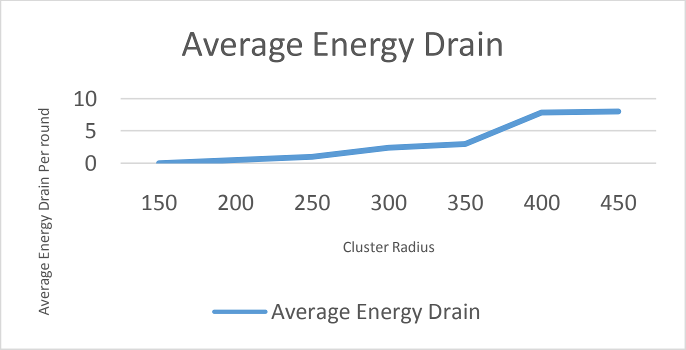

Fig.8: Ratio of average balance energy drain per round with varying cluster radius

4.EVALUTION OFPROPOSED ALGORITHM

We compared our work with that of algorithm [21], which is based on recovery due to energy exhaustion. Where the nodes in the cluster are categorised in four categories: boundary node, pre-boundary node, internal node and the cluster head. Boundary nodes does not require any recovery but pre-boundary node, internal node and CH will take appropriate actions to connect the cluster. Usually, if node energy becomes below a threshold value, it will send a fail_report_msg to its parent and children. This will initiate the failure recovery procedure in order to maintain the connectivity of failing node parent and children to the cluster. A join_request_mesg is sent by the healthy child of the failing node to its neighbors. All the neighbors with in the transmission range respond with a join_reply_mesg/join_reject_mesg messages. The healthy child of the failing node selects a suitable parent by verifying that selected neighbor is not one among the children of the failing node.

In proposed mechanism, normal nodes does not require any recovery but they switch them-self tolower computational mode by informing their cell managers. In existing algorithm[21], CH failure results in children to exchange energy messages.Important aspect over here is failed children are not considered for the new cluster-head election. The healthy node/child with the maximum residual energy is selected as the new cluster head and and responsible for sending a final_CH_mesg to its members. After the new cluster head is selected, the other children of the failing cluster head are attached to the new cluster head and new CH becomes the parent for these children. CH failure recovery procedure requires more messages to be exchanged to select the new cluster head that require more energy to exchange series of messages. Also,in case of failing CH require appropriate steps to get connected to the cluster, which is time consuming as well abrupt network operations. In our proposed algorithm, back up secondary cluster heed is employed which will replace the cluster heed in case of failure.

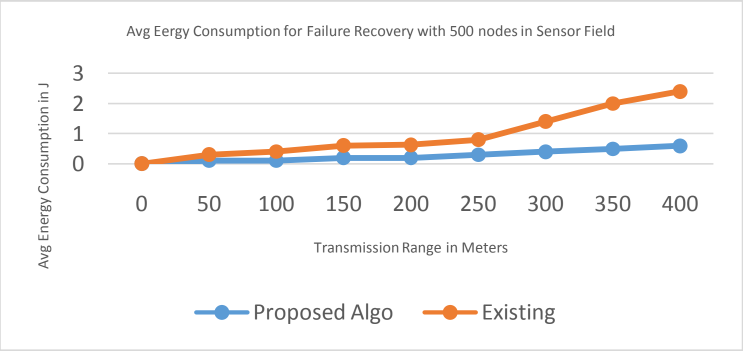

Fig.-9: Average time for cluster head recovery

No further messages are required to send to other cluster members to inform them about the new cluster heed Fig.. 9 and 10 compare the average energy loss during failure recovery of different algorithms. It can be observed from Fig..9 that when the transmission range increases, after analyzing the greedy algorithm with Gupta algorithm [22] and the proposed algorithm it observed that greedy algorithm expends the maximum energy. However, from Fig. 10, we may say that the Gupta algorithm spends the more energy as compared to other algorithms when the number of nodes in sensor field increases.

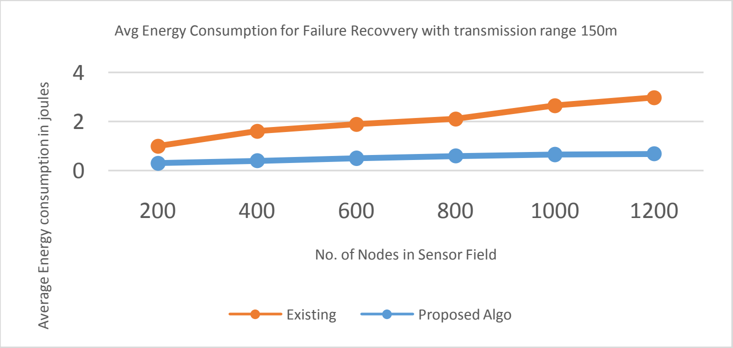

Fig.10: Average time for cluster head recovery

5.CONCLUSION AND FUTURE WORK

In this paper, we have explained about the issues specific to network disruption due to cluster head failures in wireless sensor networks and we have tried to find a solution for that. We have proposed a fault management mechanism for wireless sensor network to diagnose faults and perform appropriate measures to recover sensor network from failures. We have compared our algorithm with the algorithm [21], is recent approach of fault detection and recovery in wireless sensor networks and proven to be more efficient than few existing algorithms. It is more energy efficient when compared with Gupta and Greedy Therefore; we conclude that our proposed algorithm is also more efficient than Gupta and Greedy [22] in term of fault recovery. The faster response time of proposed algorithm provides uninterrupted operation and healthy lifetime for the prolonged operation of the WSN. In future, we would incorporate the mobility and autonomic fault management aspect in the context WSN fault tolerant system.

REFERENCES

[1]. I.F.Akyildiz, W.Su.,Y.Sankarasubramaniam, E. Cayirci, ―A survey on sensor networks‖ , IEEE communications Magazine 40 (8), Published in 2002, pp. 104-112.

[2]. Liu. H.,Nayak. A., Stojmenovic. I., ―Fault Tolerant Algorithms/Protocols in Wireless Sensor Networks.‖ Guide to Wireless Sensor Networks. Springer London.,2009, pp.261-291,.

[3]. A. Abbasi, M. Younis, and K. Akkaya, ―Movement-assisted connectivity restoration in wireless sensor and actor networks, IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 9, Sep. 2009, pp. 1366–1379,.

[4]. Mishra D. P. and Kumar Ramesh ,"A Vision of Hybrid Security Framework for Wireless Sensor Network", Indian Journal of Applied Research, Volume:5 , Issue:1, Jan 2015, ISSN-2249-555X pp. 167-171

[5]. Mishra D. P. and Kumar Ramesh, "IDS Foundation for Wireless Sensor Network", GJRA - GLOBAL JOURNAL FOR RESEARCH ANALYSIS, Volume-5, Issue-11, November - 2016 , ISSN No 2277 - 8160

[6]. Liu. H.,Nayak. A., Stojmenovic. I., ―Fault Tolerant Algorithms/Protocols in Wireless Sensor Networks.‖ Guide to Wireless Sensor Networks. Springer London. 2009, pp.261-291,.

[7]. M. Yu., H. Mokhtar., ―A Survey on Fault Management in Wireless Sensor Networks‖ , ISBN, 2007.

[8]. A.Perrig, R.Szewczyk, V.Wen, D.Culler, J.D.Tygar. ―SPINS: Security protocols for sensor networks.‖ in ACM MobiCom'01. Rome, Italy:ACM Press,2001

[9]. K. Farinaz., P. Miodrag., S. Alberto., ―Fault Tolerance Techniques for Wireless Ad Hoc Sensor Networks.‖ 2000.

[10]. Ann T. Tai, Kam S. Tso, William H. Sanders. ―Cluster-Based Failure Detection Service for Large-Scale Ad Hoc Wireless Network Applications in Dependable Systems and Networks‖ DSN ' 04. 2004.

[11]. S. Jessica, B. Dirk,D. Glenn, ―Efficient Tracing of Failed Nodes in Sensor Networks.‖ in First ACM International Workshop on Wireless Sensor Networks and Applications.. Altanta, GA, USA: ACM. 2002

[12]. Mishra, D. P., Kumar, R. (2016). Analysis of Wireless Sensor Networks Security Solutions and Countermeasures. Journal of Scientific and Technical Research, 8, 10.

[13]. Mishra, D. P.,Kumar, R (2015) "Qualitative Analysis of Wireless Sensor Network Simulator" International Journal of Computer Applications (0975 – 8887) National Conference on Knowledge, Innovation in Technology and Engineering (NCKITE 2015)

[14]. N. Ramanathan, K. Chang, R. Kapur, L. Girod, E. Kohler, and D. Estrin, "Sympathy for the sensor network debugger", in SenSys '05: Proceedings of the 3rd international conference on Embedded networked sensor systems, pp. 255-267, 2005.

[15]. A. Mahmood, E. J. McCLUSKEY, "Concurrent Error Detection Using Watchdog Processors", IEEE TRANSACTIONS ON COMPUTERS, pp. 160-174, 1988

[16]. Rana Ejaz Ahmed, and Abdul Khaliq, "A Low-Overhead Checkpointing Protocol for Mobile Networks", Electrical and Computer Engineering, IEEE CCECE 2003, pp. 1779-1782, 2003.

[17]. Yawei Li, ZhillingLan, "A Fast Restart Mechanism for Checkpoint/Recovery Protocols in Networked Environments", Dependable Systems and Networks with FTCS and DCC, 2008, pp. 217226, 2008.

[18]. Y. Sankarasubramaniam, O. B. Akan, and I. F. Akyildiz, "Esrt: event-to-sink reliable transport in wireless sensor networks", in MobiHoc '03: Proceedings of the 4th ACM International symposium on Mobile ad hoc networking & computing, pp. 177188, ACM, 2003.

[19]. Q. Han, I. Lazaridis, S. Mehrotra, and N. Venkatasubramanian, "Sensor data collection with expected reliability guarantees", Pervasive Computing and Communications Workshops, pp. 374378, March 2005.

[20]. Ramakrishna Gummadi, Todd Millstein, and Ramesh Govindan, "Declarative Failure Recovery for Sensor Networks," AOSD '07, March 12-16 2007.

[21]. G. Venkataraman, S. Emmanuel and S.Thambipillai, "Energy-efficient cluster-based scheme for failure management in sensor networks" IET Commun, Volume 2, Issue 4, April 2008 Page(s):528 – 537

[22]. G. Gupta and M. Younis, "Load-Balanced Clustering in Wireless Sensor Networks", in the Proceedings of International Conference on Communication (ICC 2003), Anchorage, AK, May 2003.

[23]. Mishra D. P. and Kumar Ramesh, "Hybrid Framework for Intrusion Detection in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science, Volume 8, No. 3, March – April 2017, ISSN No. 0976-5697