ISSN:2231-0711

Saurabh Mondal et al | IJCSET |March 2013 | Vol 3, Issue 3, 109-115

Energy Efficient Fault Tolerant Scheme for Wireless Sensor Networks (EEFSWSN)

Saurabh Mondal[1], Debajyoty Banik[2]

[1]Department of solutions (data warehousing),
Noumura Research Institute Financial Technologies India Pvt. Ltd,
Salt lake electronics complex, Kolkata 700091,
West Bengal , India
[2]Department of computer science and engineering,
National Institute of Technology, Durgapur,
West Bengal 713209, India

***Abstract*— Sensor Network has been identified as the most important technology for the next century. Despite of its potential application, wireless sensor network encounters resource restrictions such as low computational power, reduced bandwidth and specially limited power resource. In wireless sensor networks, fault-tolerant and energy efficiency are two important topics. Some link failures may happen during data transmission. In this Paper, we address fault tolerance in wireless sensor networks in power efficiency perspective. In order to make the presentation self-contained, we start by providing a short summary of sensor networks and classical fault tolerance techniques. Then we have discussed about the faults in different layers, have studied failures, errors. Therefore, failures have been classified. Some fault detection and recovery techniques are discussed. Thus we have proposed some methods to make our WSN fault tolerant. Among the different techniques we have chosen a graph based technique to deal with the fault tolerance in WSN. Our simulation result depicts that our proposed scheme is better than the existing algorithms.**

***Keywords*— Fault tolerance, fitness function, multiple fit neighbors.**

I. INTRODUCTION

Wireless sensor network (WSN) can be treated as a special family of wireless ad hoc networks. It is a self-organized network that consists of a large number of low-cost and low-powered sensor devices, called sensor nodes. Senor nodes can be deployed on the ground, in air, in vehicles, on bodies, underwater and inside buildings [15]. Each sensor nodes equipped with a sensing unit which used to capture events of interest and a wireless transceiver which is used to transform the captured events back to base stations, called sink node.

Reliability of a WSN is affected by faults. Faults occur mainly due to: malfunctioning hardware, software glitches, dislocation or environment hazards e.g. fire, flood etc. To discuss fault tolerance it is necessary to discuss the importance of a WSN to be fault tolerant. In a scenario where a WSN is deployed to monitor volcanic activity in a certain area, and if any fault occur. The WSN gives some erroneous result that everything is normal while there is very much possibility of a volcanic explosion. This may leads to a catastrophe. Also in case of military monitoring applications it is so important to give information of any intrusion instantly.

So far as we discussed fault tolerance is one of the most important criteria that every WSN should satisfy. A system of wireless sensor nodes, each equipped with a certain amount of sensing, actuating, computation, communication, and storage resources. Sensor nodes work cooperatively to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants [2]. Nodes in WSNs are prone to be faulty due to energy depletion, hardware failure, communication link errors, malicious attack and other types of attack. So fault tolerance is one of the critical issues in WSNs. Also multi-hop communication is one unavoidable characteristics of WSN as sink is not directly connected with each node due to its ad hoc characteristics. So fault in a single node can lead to fault in the entire network.

There are different approaches that can be served the purpose of making WSN fault tolerant. An approach can be taken in which redundant nodes are inactive initially but activated when some of its active neighboring node goes inactive [6]. Thus the problems due to fault can be solved. Although this method is not cost efficient. Self-healing [5] is one of the approaches but it is time and energy consuming. In a K-Connected network [4] the problem is also energy consumption as a single data is sent in multiple paths.

A wireless ad hoc network consists of several sensor nodes $\pounds=\{t_1; t_2; \ldots; t_n\}$ located in the plane and communicating by radio. The underlying physical topology of the WSN is dependent on the distribution of the wireless nodes (location) as well as the transmission range of each node. The transmission range of node t is determined by the status of that node, denoted by p(t). Status is the power of each node in fault tolerance perspective; that is the remaining power of each node. This is customary to assume that the minimal status required to transmit to distance d is d^{α}, where the distance-status gradient α is usually taken to be in very small interval [13]. Thus, node t receives transmissions from s if $p(s) \geq d(s, t)^{\alpha}$. Where d(s, t) is the Euclidean distance between s and t. A power assignment for sensor nodes £ is a vector of transmission powers $A = \{p(t) \mid t \in \pounds\}$. The transmission possibilities resulting from a power assignment induce a directed communication graph $H_A=(\pounds,\epsilon_A)$, where $\epsilon_A=\{(s, t) \mid p(s) \geq d(s, t)\}^{\alpha}$. is the set of directed edges resulting from the power assignment. In section IV we propose an algorithm so that the graph H_A

is remain connected after at least k number of fault in each node, where k is the number of neighbor of that node. The cost of the power assignment is defined as the sum of all transmission powers, $C_A=\sum t \in £ p(t)$.

There are two possible fault tolerant models: symmetric and asymmetric. In symmetric settings node s can reach node t if and only if node t can reach node s. That is, for any s, t Є T, $p(t) \geq d(s, t)^{\alpha} \leftrightarrow p(s) \geq d(s, t)^{\alpha}$ .The symmetric models mainly exist between sink and other nodes. We can also refer to it as the undirected model. The asymmetric variant allows directed links between two nodes.

The most fundamental problem in wireless ad hoc networks is to find a power assignment which induces a communication graph that satisfies some topological property, while minimizing the total cost. Here most important topological property is fault tolerance. The strong connectivity (all-to-all) property is extremely useful in certain applications of wireless networks. But it may not possible in every case because of cost of implementation. Broadcast (one to all) and multicast (one to many) properties represent a major part of the activities in real life multi-hop radio networks. The transmission is initiated by some source s and the message needs to be transmitted to all or some nodes, respectively. The converge cast (all-to-one) property has received less attention but might prove to be useful in networks where it is important to have transmissions from all nodes directed to one special node (e.g. temperature reading from multiple sensors).

In this paper we have developed an algorithm based on graph of automata [3] to make sensor network fault tolerant. A graph of automata (GA) is a connected bounded degree graph G = (V, E) is a 5-tuple (S, G, d, N, ∂) where S is a finite set with at least two elements called set of states , G is a graph where degree is bounded by d, N:N→({1……d})→V) gives for each vertex its neighbors vector , i.e. an order on its neighbors and ∂ : (S ⊔ {Є}d+1) →S is the transaction function where Є is a special element used when vertex has less than d neighbors .

The proposed approach is a localized one. We first determine neighbor of each node and sort them according to their fitness value and sensor nodes usually communicate with their fittest neighbor. Due to fault some node's fittest neighbor goes down then that node chooses the next fittest neighbor as fittest and continues to communicate.

This paper is arranged as follows. In section II we first relates fault, error and failure, then classify them and by discussing some fault detection and recovery techniques we have tried to find a better way to deal with fault. The Section III describes mathematical model of our problem. Our proposed scheme is presented in Section IV. Section V reports the performance of our proposed scheme. Finally, section VI concludes the paper.

II. RELATED STUDY

In most cases WSN are used remote/hostile environment. Therefore it should be dependable. WSN must offer characterizes such as reliability, availability, maintainability. The availability of the services provided by a WSN to a large extent depends on fault tolerance, since usually it cannot be assumed that all sources of error can be eliminated, even through careful engineering. Service availability implies the probability with which a request will lead to a valid and useful response. Availability is defined as: Measure of Availability [2], P(A) =MTTF / (MTTF+MTTR), where MTTF denotes Mean Time to failure and MTTR denotes Mean Time to Repair [2]. The equation shows that a WSN that constantly fails but repair or recover quickly shows high availability. To understand fault tolerance, it's important to understand what is fault and what the difference between faults, error, failures [2].

Fault: -A fault is any kind of defect that leads to an error.

Error:-An error corresponds to an incorrect undefined) system state. Such state may leads to failure.

Failure:-A failure is the (observable) manifestation of an error, which occurs when the system deviates from its specification & deliver its intended functionality.

Source of Faults in Real WSN Applications

Node Faults:- Nodes have several hardware and software components that can produce malfunctions. E.g. Hardware of sensor is exposed to the extreme environment, cluster head problem.

Network Faults:-Routing is one of the fundamental building blocks in WSN. Collecting sensor data, distributing software & configuration update & coordinating among them. There may be application specific routing protocol.

Sink Faults:-On the higher level of network a device (sink) that collects all the data generated in the network & propagates it to the back end. To overcome battery problem solar cell is used. Sometimes the help of satellite are also being taken.

Failure Classification

Crash or Omission:-When service sporadically not responding to the requests & at a point of time stops responding.

Timing:-When there is timeout or providing data too early.

Value:-Providing incorrect value for some time. This is due to malfunctioning software, hardware, corrupt messages or even malicious node generating incorrect data.

Arbitrary:-All types of failure those are not included in the above category.

Fault Detection techniques

Self-diagnosis:-Node checks itself. e.g. ----Based on the measurement of accelerometer to determine if the node suffers from an impact that could lead to hardware malfunction. Similar approach is taken where it can determine when it is moved. It can check the battery level.

Group Detection:-Detection of services failing due to incorrectly generated values only possible if a reference value is available (aggregation/fusion).

Hierarchical Detection:-A tree structure where a child-parent based monitoring exists.

Fault recovery techniques

Active Replication in WSN:-Active replication is wireless sensor networks are naturally applied in scenarios where all or many nodes provide the same functionality.

Multi path routing:-A network should be K-Connected. This allows k − 1 nodes to fail while the network would still be connected**.** Multi-path routing can be used to actively replicate routing path.

Sensor value aggregation:-Provides high-level information derived from a number of low level sensor's input. Inherent redundancy of sensors can provide fault-tolerant data aggregation. This is achieved through a trade-off between the precision of resulting sensor reading interval & no of faulty node.

Ignore values from faulty nodes:-A simple method is just ignoring values from faulty node

Along with fault tolerance also we must consider the matter of intrusion tolerance [6]. Fault is something that does not happen intentionally. Where intruder attacks the system as they wish. So we must design our system such a way that it is also tolerant to fault and intrusion both.

Cost and energy are the two main constrain of designing WSN. We can achieve our 1st constrain by structuring the WSN in a tree like hierarchal model [7] [8]. Here we classify the node of sensor network into three categories---- First type of node is called base station. It controls all the other nodes and all other nodes transmit their information to it. Second type of nodes is some specialized nodes which not only collect data but also gather data other ordinary nodes and then transmit it to base station. Third type of node is ordinary node which only collects data and transmits it to nearest active specialized node or base station. Thus we can minimize cost by making number of ordinary larger than other type of nodes as they cost are lowest. Although this model can tolerate fault but they are very vulnerable to intrusion, as intruder always want to attack base station or specialized nodes rather than ordinary node.

Energy is our second constrain. A WSN is consisting of sensor powered by small batteries and they are deployed in remote hostile environment as discussed in section II. Most of the cases sensor nodes are not recharge able; so energy becomes most important constrain in most of the WSN. Introducing the concept of cellular automata [15] the average energy consumption of a sensor network can be minimized.

III. PROBLEM FORMILATION

We are given a set of Sensor node £ and a natural number k ≥ 1 (the fault resistance parameter). Our goal is to find a scheme so that the set of sensor nodes £ is k-fault resistant in the induced communication graph HA and the power assignment cost CA is minimized. Namely, the optimization problem is defined as:

EEFSWSN (£, k)
Input: A set £ of Sensor node and a fault resistance parameter k > 1.
Output: A power assignment A(£) so that £ is k-fault resistant in $P(H_A)$.
Target Function: Minimize C_A

We address the following topological properties defined for a directed graph G = (V, E).

The problem is like that given a set of nodes we are to find a connection scheme for which fault will be minimum. We introduce concept of graph of automata [3] to achieve our objective of fault tolerance.

Definition: A graph of automata (GA) is a connected bounded degree graph G = (V, E) is a 5-tuple (S, G, d, N, ∂) where S is a finite set with at least two elements called set of states , G is a graph where degree is bounded by d, N:N→({1……d)}→V) gives for each vertex its neighbors vector , i.e. an order on its neighbors and ∂ : (S ⊔ {Є}d+1) →S is the transaction function where Є is a special element used when vertex has less than d neighbors . Our approach is a localized approach. . Each node is unidentified with unique index number. In this scheme each node only knows its neighbors. Each node calculates fitness value of all its neighbors and sorts its neighbors according to their fitness value order. Then each node communicates with their fittest neighbor. This algorithm is discussed later part elaborately.

IV. PROPOSED ALGORITHM

A. Overview of the algorithm

Section II depicts that availability is one of the greatest measures for fault tolerance. Therefore a WSN where fault may occur frequently but repairs itself is highly fault tolerant and so degree of fault tolerance will be increased. In the next algorithms we have taken such strategies that a WSN will recover from any kind of fault as soon as it realized it. Our algorithm is as follows-

Suppose there is a set of sensor nodes like in figure 1 below

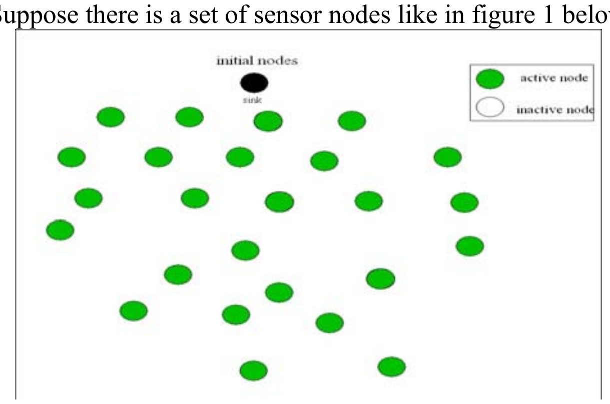

Fig 1. Shows a set of sensor nodes deployed in an area

In our main algorithm is given below---

EEFSWSN Algorithm1

Call function initialization of nodes

For j=0 ; j<n; j++ /* n is the total number of sensor nodes*/
Begin
IF(j != i)
For i = 0; i < n ; i++
Begin
j sends a message M_{ji} to node i at time t_{ji};
Node i receives M_{ji} and append its index i and energy level
E_i with m_{ji} and sends it back to node j;
j recives that updated M_{ji} at time t'_{ji} ;
j calcultes $t_i = | t_{ji} - t'_{ji} |$ and stores i , t_i , E_i in list L_j ;
End
End IF
End

After applying our algorithm the graph will be linked like figure 2

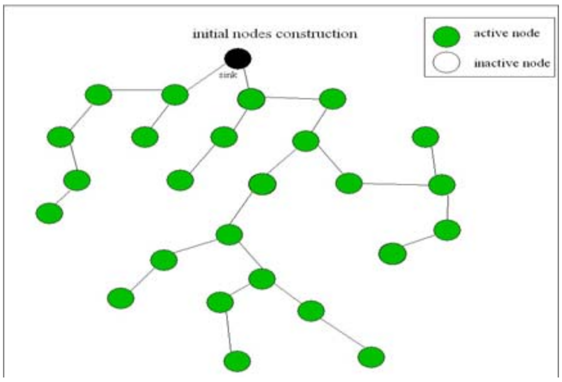

Fig 2. After applying our algorithm nodes will be linked like this figure

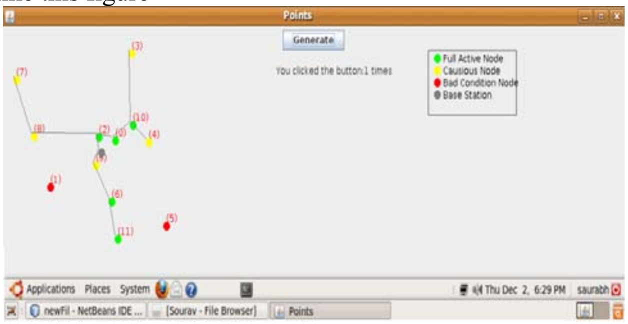

Fig 3. Shows screen shot of proposed algorithm where have connected randomly generated sensor nodes to form a WSN

B. Determination of neighbors

The function *init_nodes* takes values and initialized them to each node. Each node has the following parameters—distance to source, status, neighbors index number, total number of neighbors. Distance to source is determined in terms of hop count from sink. Status is the degree of workability of each node. The parameters of status can be residual energy, available bandwidth etc. Total number of neighbors and there indexes are determined by message passing of each node within the transmission range (nodes in one hop distance). Here we use indexes of each node as a unique identity of that node.

C. Fittest neighbor selection

This is the main stage of the whole process. The function *list of fittest nodes* accomplishes this task. The process is as follows—in this stage each node i looks into its list L_i and depending on the information of L_i node i sort other nodes in L_i. To achieve this task our algorithm is as follows—

Call function list of fittest nodes

While r<N begin
 If *the energy level Er is<threshold*
 then
  Mark it as inactive.
 Else If *any two nodes, t , j* $(|(t_r-t_i)| != |(t_j-t_i)|)$
  Sort nodes according to $|(t_r-t_i)|$ value in ascending order.
 Else
  Sort nodes according to their energy level in descending order.

  End if.
 End if.
Modify list L_i accordingly.
End while.

This function is called fitness function. Each node i , connect to the node in 0th position in its list L_i . Thus the graph is created initially.

D. post graph construction process

After construction of the initial graph each node only communicates with its fittest neighbor. If for some node r, any fault has occurred in its fittest node then after realizing it node r will select its next fittest neighbor as fittest one and continues communication. Figure 3 shows such a situation-

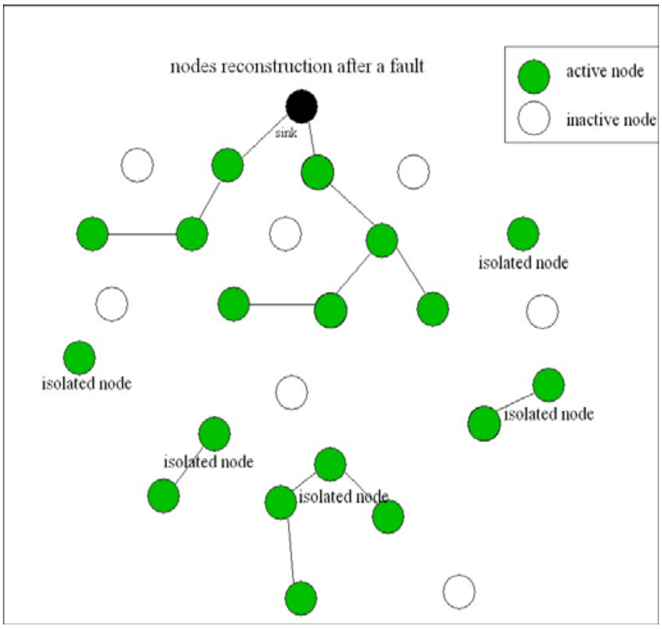

Fig 4. These shows a situation where some nodes become faulty

In figure 4 we can see that as fault has occurred in some nodes fittest neighbor so that node chooses its next fittest neighbor as fittest one. For some other nodes as it has not have any neighbors left to communicate with sink so they become isolated. Figure 5 shows such a scenario -----

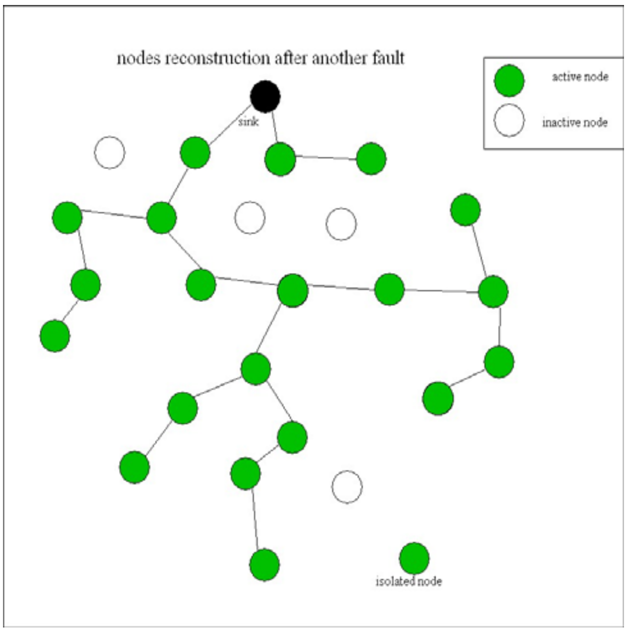

Fig 5.Shows reconstructed graph

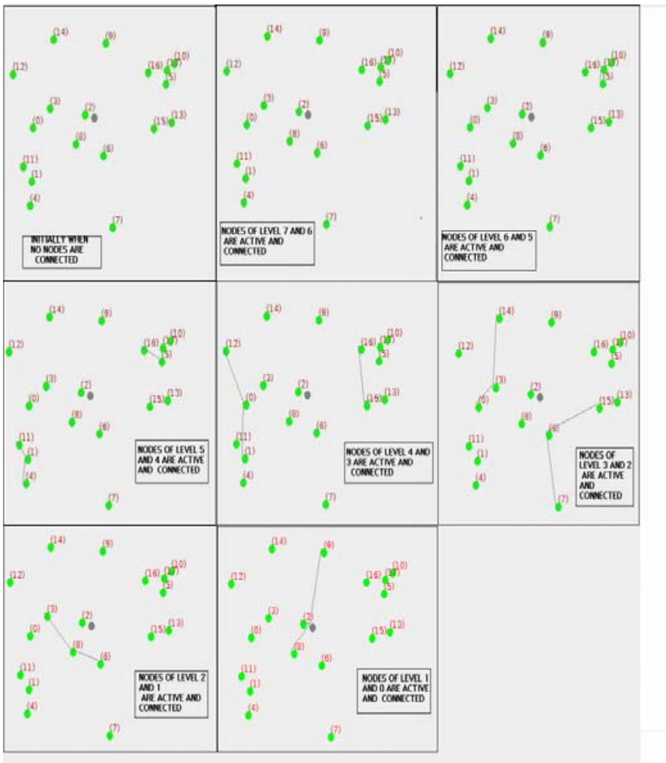

Fig 6. Shows a screen shot of our program where we use cellular automata to choose which nodes will be active and d be connected

After transmission of each message node's status will be updated as follows-
Present status = previous status - status wasted due to transmission. To reduce total energy consumption we use cellular automata.Using rules 27, 77, 108 we have created a system of cellular automata so that at a time only some of the nodes will be active. But we also preserve the data propagation uniformly

V. PERFORMANCE RESULTS

The evaluation of new approaches and algorithms in the field of WSN is a challenging task. Fault-tolerant sensor assignment is a NP-complete problem. Therefore, in general, one does not find the optimal solution for a given instance. Another reason is that there are no established benchmarks and previously published results for the addressed problem.
We have generated nodes randomly and deployed them also in random fashion. The individual nodes information is taken randomly. Each node is assumed to be within radio distance of its neighbors. The performance of our scheme is compared with the EEFTMR [10] and AOMDV [11] scheme.
The performance results are presented in the next section.

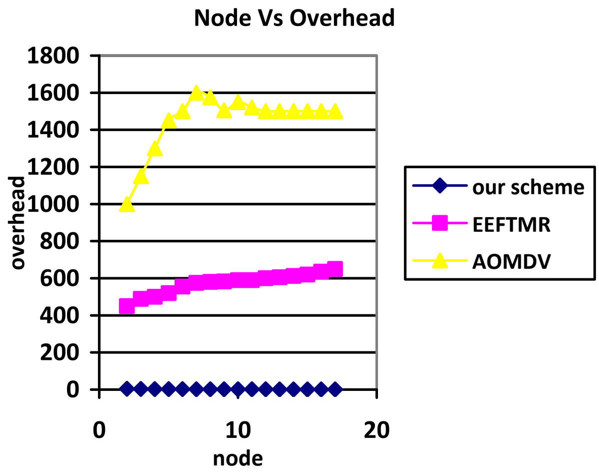

Fig 7. This shows comparison between our scheme EEFTMR, AOMDV of no of Node Vs increasing Overhead

Figure 7 shows the results of overhead (The overhead is defined as the total number of routing control packets normalized by the number of received data packets) for the nodes 0 to 100 .Clearly our scheme is achieves better results (as the number of nodes increases overhead decreases) than EEFTMR (Energy Efficient Fault Tolerant Multi path Routing) proposed in [10], and AOMDV.

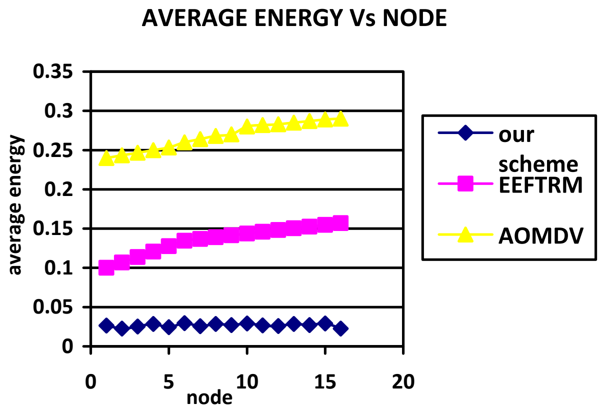

Fig 8. This shows comparison between our scheme, EEFTMR, AOMDV of average energy consumption Vs increasing no of node

Figure 8 shows the results of average energy consumption (It is the average energy consumption of all nodes in sending, receiving and forward operations) for the nodes 0 to 100 .Clearly our scheme is achieves better results (as the energy consumption is almost constant) than EEFTMR (Energy Efficient Fault Tolerant Multi path Routing) proposed in [10], and AOMDV.

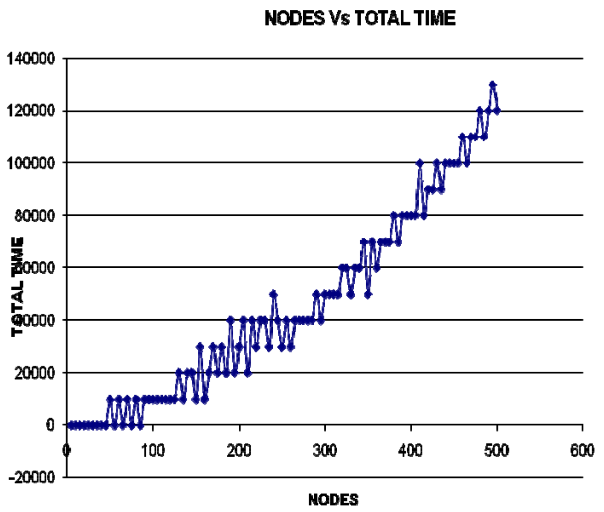

Fig 9. .Shows the results of total time consumption to construct the graph for different number of nodes

Figure 9 shows the results of total time consumption (It is total time taken to construct the graph) to construct our graph of automata. We have executed our program for 700 hundred nodes in increasing order with an interval of 7 and have taken corresponding time and plot the above graph. The above shows as the number nodes in our sensor network increases the required time to construct the graph increases but in linear flat fashion.

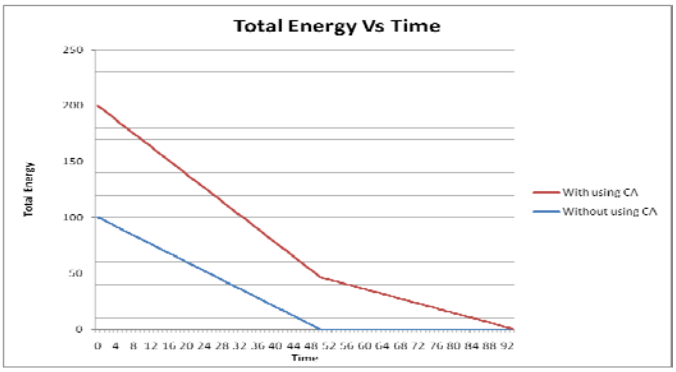

Figure 10. This shows remaining life of a sensor network compared between schemes with and without using Cellular automata

Figure 10 shows Energy vs. Time graph. Here energy is the average energy (summation of energies divided by total number of nodes) of sensor network. Clearly this graph shows that average energy consumption is reduced using cellular automata (CA); as using CA we have controlled data flow using it.

VI. CONCLUSIONS

In this paper we provided a thorough investigation of faults that occurred in real WSN. This concise investigation provides a valuable knowledge to understand why the techniques proposed previously are not so efficient in all the perspectives. This motivates us to find such a solution to fault tolerance that will satisfy most of the conditions for an efficient fault tolerance. These conditions not are not only in terms of fault tolerance but also energy efficiency and low overhead. Hence we have developed an algorithm with the help of graph of automata [3].

The key idea is to create a list of neighbor in fitness order and communicates with only fittest neighbor. Whenever a node's fittest neighbor goes down due to some fault then choose next fittest neighbor as fittest one and continue communication. And also by introducing the concept of Cellular Automata we have controlled the data flow ; thus we have reduced the energy consumption of WSN. This also increases the life time of WSN. The main advantage of this algorithm of our algorithm is that it is a localized. Means any node only knows its neighbor, it need not to know location of other nodes. Here comes energy efficiency as to construct the graph , message transmission per node or average energy consumption is constant. Because each node may have certain number of neighbors and this is independent of total number of nodes.

Also as after construction of the graph the WSN can tolerate faults up to a certain number of times hence it decrease the number of times to reconstruct the graph and reduces energy consumption.

It is clear that our proposed scheme has advantage over those schemes discussed earlier and much more power efficient. In case of WSNs sensor nodes are basic building blocks. A Sensor node does work like data sensing and sending the data to some other node. Along with that in case of fault due to the every time a WSN need to be reconstructed. Due to its adhoc characteristics, most power consuming task for these wireless sensor nodes is data transmission. Not only for sending sensed data but also to reconstruct WSN sensor nodes need to send data in wireless medium.

We have designed our algorithm such a way once WSN is constructed we don't need to do some data exchange between sensor nodes to reconstruct it. This reduces energy wastage greatly. Not only that but also by introducing the concept of cellular automata we have given WSN capability to keep its nodes in standby mode when not needed and selects when to sense data and when to transmit it. Thus by introducing the concept of cellular we have reduced the energy consumption greatly.

REFERENCES

[1] R. R. Brooks and S. S. Iyengar, “Multi-Sensor Fusion:Fundamentals and Applications With Software,” Prentice-Hall, 1997 [Bro97] .

[2] Luciana Moreira S´a de Souza[SAP Research Karlsruhe, Germany], Harald Vogt [SAP Research Karlsruhe, Germany], Michael Beigl [Technische Universit¨at Braunschweig Braunschweig, Germany],”A Survey on Fault Tolerance in Wireless Sensor Networks”.

[3] Bruno Martin 30 august 1999,”Geometrical Hierarchy on Graphs via cellular automata”.

[4] Hai Liu1, Amiya Nayak1, Ivan Stojmenović2,1School of Information Technology & Engineering, University of Ottawa, K1N 6N5, Canada, 2EECE, The University of Birmingham, Birmingham, B15 2TT, United Kingdom],” Fault Tolerant Algorithms/Protocols in Wireless Sensor Networks”.

[5] Farinaz Koushanfar EECS Dept. UC Berkeley Berkeley, CA, USA farinaz@eecs.berkeley.edu Miodrag Potkonjak CS Dept. UCLA Los Angeles, CA, USA miodrag@cs.ucla.edu Alberto Sangiovanni Vincentelli EECS Dept. UC Berkeley Berkeley, CA, USA “Fault Tolerance Techniques for Wireless Ad Hoc Sensor Networks”.

[6] Liang-min Wang, Jian-feng Ma, Chao Wang, Alex Chichung Kot, Senior Member, IEEE –[Xidian University.Key Laboratory of CNIS of Education Ministry Xi’an Shaanxi, 710071, P.C. China. Nanyang Technological University School of Electrical and Electronic

Engineering, 639798, Singapore eackot @ ntu. edu.sg], “Fault and Intrusion Tolerance of Wireless Sensor Networks”.
[7] İlker Bekmezci, Fatih Alagöz [Satellite Networks Research Laboratory (SATLAB), Boğaziçi University 34342 Bebek, Istanbul, TURKEY].” Energy Efficient, Delay Sensitive, Fault Tolerant Wireless Sensor Network For Military Monitoring”.
[8] Skender Ben Attia1, André Cunha1, Anis Koubâa1,2, Mário Alves1 1 IPP-HURRAY! [Research Group, Polytechnic Institute of Porto, Rua António Bernardino de Almeida, 431, 4200-072 Porto, Portugal 2 Al-Imam Muhammad Ibn Saud University, Computer Science Dept., 11681 Riyadh, Saudi Arabia]“Fault-Tolerance Mechanisms for Zigbee Wireless Sensor Networks”.
[9] Farinaz Koushanfar1, Miodrag Potkonjak2, Alberto Sangiovanni-Vincentelli [Department of Electrical Engineering and Computer Science University of California, Berkeley Berkeley, CA, US 94720 2Department of Computer Science University of California, Los Angeles Los Angeles, CA, US 90095], ” fault tolerance in wireless sensor networks”.
[10] C. Kavitha Dr. K.V.Viswanatha Assistant Professor, Dept of CSE Professor & P.G Co-ordinator R.V.College Of Engineering Department Of Computer Science Banglore, India R.V.College Of Engineering ckavithaphd@gmail.com Bangalore, India “An Energy Efficient Fault Tolerant Multipath(EEFTM) Routing Protocol for Wireless Sensor Networks”.
[11] Mahesh K. Marina and Samir R. Das "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks" Network Protocols, 2001. Ninth International Conference on Publication Date:11-14 Nov, 2001.
[12] A. Birolini. Quality and Reliability of Technical Systems:theory, practice, management. Springer, 1997.
[13] K. Pahlavan, A.H. Levesque, Wireless Information Networks, Wiley-Inter science, 1995.
[14] S.O. Krumke, R. Liu, E.L. Lloyd, M.V. Marathe, R. Ramanathan,S.S. Ravi, Topology control problems under symmetric and asymmetric power thresholds, in: AdHoc-NOW’03, 2003, pp. 187- 198.
[15] Indrajit Banerjee, Sukanta Das, Hafijur Rahaman and Biplab K Sikdar 2006 IEEE International Conference on Systems, Man, and Cybernetics October 8-11, 2006, Taipei, Taiwan “An Energy Efficient Monitoring of Ad-Hoc Sensor Network with Cellular Automata”.