National Conference on Recent Innovations in Computer Science & Communication Engineering, *July 2016* *ISBN: 978-93-86005-02-1*

A Preventive Measure to Provide a Fault Tolerance in Wireless Sensor Network

Jaydip Mukhopadhy* **and Sayanka Saha**

RCC Institute of Information Technology, Kolkata - 700015, West Bengal, India; jaydipcu@gmail.com, sayanka.saha@gmail.com

Abstract

Wireless Sensor Networks (WSNs) have wide-ranging change of applications and deliver enormous future potentials. Nodes in WSNs are prone to failing due to energy reduction, hardware failure, communication link errors, malicious attack, and etc. Here Fault Tolerance is very serious issue. Here it is proposed to form a sensor network considering fault detection and few preventive measures to provide a fault tolerant sensor network.

Keyword: Fault Detection, Fault Tolerance, Fault Tolerant Network, Wireless Sensor Network (WSN)

1. Introduction to Sensor Network and WSN

A sensor network is a collection of specific transducers with a communications structure proposed to monitor and record conditions at various locations. Normally parameters are checked by the temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions[1]. The various modern networks are bi-directional, also enabling control of sensor activity.

A WSN is a self-organized network that consists of a huge number of low-cost and low-powered sensor devices are called sensor nodes, that can be deployed on the land, in the air, in vehicles, on bodies, under water, and inside buildings. Every sensor node is prepared with a sensing unit, that is used for capturing events of interest, and a wireless transceiver, that is used for transforming the captured events back to the base station are called sink node. Sensor nodes work together with each other for performing tasks of data sensing, data communication, and data processing[1].

The WSN is completed of nodes from a more than a few hundred, where each node is connected to one or more sensors.

*Author for correspondence

The basic mechanism of a node is:

- Sensor and actuator is an interface to the physical world designed which is mainly sensed the environmental parameters such as pressure and temperature etc[2].
- Controller is to control various types' modes of operation to process of data.
- Memory is storage for programming data.
- Communication is a mainly device such as antenna to send and receive data over a wireless channel.
- Power Supply is a supply of energy for smooth operation of a node just like battery.

The topology of the WSNs can be different from a star network to a modified wireless mesh network. The broadcast technique between the nodes of the network could be routing or flooding. The power of the wireless sensor networks depend on the capability for deploying huge numbers of tiny nodes which assemble and configure themselves. In adding to severely decreasing the installation costs, wireless sensor networks have a capability to dynamically adapt for changing environments. Adaptation mechanisms can lead to change in network topologies or can cause the network to shift between different modes of operation[3].

A sensor network consists of multiple detection stations are called sensor nodes and each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source[3]. The transducer generates electrical signals depends on the sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver that can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from the electric utility or from a battery[3].

2. Problem Analysis

2.1 Problems Related to Sensor Networks

Nodes in WSNs tend to fail due to energy depletion, communication link errors, hardware failure, malicious attack, and so on. Two components of a sensor node-wireless transceiver and sensing unit, usually directly interact with the environment, which is subject to variety of physical, biological and chemical factors. It results in low reliability of performance of sensor nodes[4]. The communication between sensor nodes is affected by many factors, such as antenna angle, obstacles, signal strength, weather conditions, and interference, even if condition of the hardware is good.

2.2 Analysis of the Problem

A fault may be thought of as a kind of defect that leads to an error. An error corresponds to an erroneous system state[5]. Like state may lead to a failure. Wireless sensor networks are commonly organize in harsh environment and are subject to faults in quite a few layers of the system. A fault in each layer of the system has the possibility for propagating on top of levels[5].

Thus to prevent propagation of fault in a sensor network, the faults must be detected after every definite time span. But since sensor nodes are very much prone to faults, so it is always not possible to keep the track of data transfer. Thus a fault tolerant sensor network is to be created for better result.

2.3 Necessity of a Fault Tolerant Sensor Network

Recently, the usage of WSN has increased a lot. In this critical industrial environment WSNs must offer characteristics like reliability, maintainability and availability. There is as a minimum three major reasons why research in fault tolerant sensor networks should receive attention.

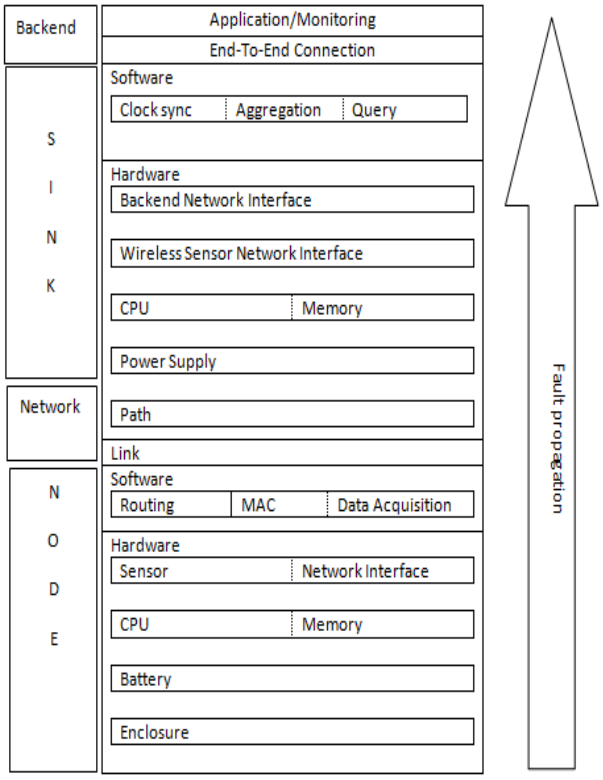


Figure 1. Sensor Network Framework.

- At least two components of a sensor node, actuators and sensors will cooperate with the environment directly and will be subject to a variety of physical, chemical, and biological factors[6]. Thousands of these nodes will form a distributed embedded network system that will handle a variety of sensing, communicating, actuating, signal processing, computing, and communication tasks[7]. Nodes operate under strict energy constraints that will make energy budget committed for testing and fault tolerance limited.
- The second reason is that sensor networks will often operate autonomously without a human in the loop. Furthermore, privacy and security concerns can also be restored in this system. Also, applications will require as sensor nodes are often deployed in uncontrolled and even hostile environments.
- The final reason is that wireless sensor networks themselves are new scientific and engineering fields and it is not still quite clear as to what is the best way to address a particular problem.

Thus our objective is to develop fault tolerant sensor network.

2.4 Solution Strategy

After analyzing the project we tried to create a fault tolerant sensor network where the network topology is such that it can tolerate or overcome any fault up to certain extent. We used NS2 a discrete-event network simulator, primarily used in research to simulate a fault tolerant hierarchical sensor network in this project. Two ways of overcoming faults at two levels of a hierarchical sensor network has been implemented.

3. Formulation/Algorithm

The step by step approach to create a fault tolerant sensor network is as follows:

3.1 Cluster Formation in a Sensor Network

Specialized data gathering and energy-aware routing protocols provide high scalability in order to sensor network lifetime.

Combining sensor nodes into clusters has broadly been adopted by the research community to satisfy the above scalability objective and usually achieve extended network lifetime and high energy efficiency

in large-scale WSN environments. The corresponding data and hierarchical routing protocols indicate cluster-based organization of the sensor nodes in order that data fusion and aggregation are possible, thereby leading to significant energy savings[8,9].

3.1.1 Algorithm to Form Clusters

- The Base Station (BS) transmits a level-1 signal with lowest power level.
- All nodes that attend to this message set their level as 1.
- Later, the base station increases its signal power to reach the next level and transmit a level-2 signal. Every node that receive the massage but do not place the previous level put their level as 2.

This process continuous until the base station transmits related massages to all levels. The total number of messages of levels is equal to the number of different transmit signal at that the Base Station can sends.

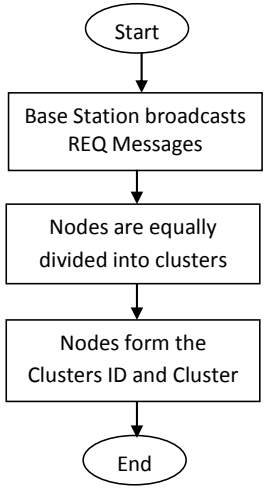


Figure 2. Cluster Selection Flowchart.

3.1.2 Cluster Head Selection

Cluster head can be selected by various means to overcome specific needs in a sensor network. The various ways of selecting cluster head are as follows:

- Energy based CH selection.
- SNR (Signal to Noise Ratio) based CH selection.
- Data forwarding through Inter cluster routing.
- Identifying the intruder, etc.

According to the sensor network requirements any one of the above can be utilized.

- In the hierarchical network construction each cluster has a leader that is also called the Cluster Head (CH).
- Sometime general Sensor Nodes (SN) as members.
- The cluster structure procedure eventually leads to a two-level hierarchy where the CH nodes form the higher level and the cluster-member nodes form the lower level.
- The sensor nodes sometimes transmit their data to the related Cluster Head nodes.
- The Cluster Head nodes combined the data (in this reason decreasing the total number of relayed packets) and broadcast them to the Base Station (BS) connect directly or through the intermediate communication with other CH nodes.
- The Base Station is the data processing point for the data received from the sensor nodes, and where the data is accessed by the end user. It is generally considered fixed and at a far distance from the sensor nodes[12].
- The CH nodes really act as gateways between the sensor nodes and the Base Station.

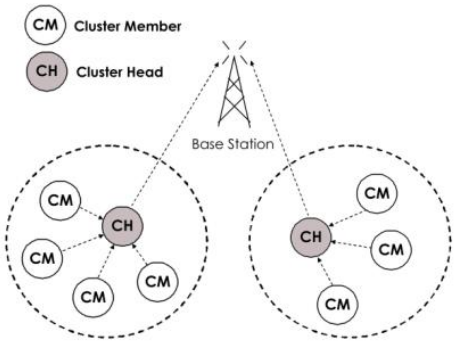


Figure 3. Cluster Network.

3.2 Detection of Faulty Sensor Nodes

Fault detection is the first phase of fault management, where an unexpected failure is properly identified by the network system. The discrete clustering approach to detect the faulty sensor node is as follows

3.2.1 Algorithm: Detection of the faulty node

Steps

1. Initialize all Sensor nodes in the Network.
2. Select 3 sensor nodes for round trip path (m=3).
3. Determine the number of round paths in WSN.
4. Set the counter for round trip paths.
5. Select the round trip path (e.g. Si-Sj-Sk-Si).
6. Now calculate the instantaneous round trip delay(RTD) time of this path by using the equation t_RTD=t(i,j)+t(i,k)+t(k,i).
7. Estimate confidence factor of respective roundtrip path by using following condition D_RTD= 1 (if t_RTD < t_RTD-T_r) otherwise 0, where t_RTD-T_r is the threshold value of round trip delay adjusted for the maximum value of time and D_RTD is a confidence factor for the selected round trip path in WSN.
8. Go to step 4, decrement the counter for RTD path and repeat till step 7 to determine the confidence factor of all paths in the WSN.
9. Complete the look-up table entries for all RTD paths.
10. Stop.

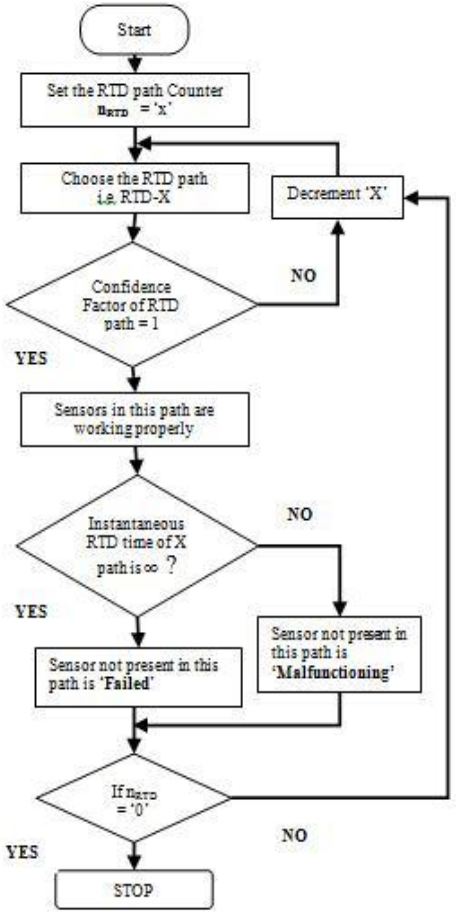


Figure 4. Flowchart: Detection of the faulty node.

3.3 Fault Tolerance in a Sensor Network

If a cluster head is faulted. Then in order to extend network lifetime, no need to only communicate with their nearby neighbors and they start for communicating with the base-station. The goal is to keep the sensor web operating as long as possible. With the direct approach, all nodes transmit directly to the BS which is usually located very far away. Therefore, each node will consume a major amount of power to broadcast to the BS in each round. Since the nodes have a limited quantity of energy, nodes will die quickly, causing the reduction of the system lifetime. In this reason decrease the energy consumption for each node to receive and transmit to close neighbors and to take turns being the leader for transmission to the Base Station[10]. This approach will distribute the energy load evenly among the sensor nodes in the network.

The required algorithm for our desired result is:

- We initially place the nodes randomly in the play field, and therefore, the i th node is at a random location.
- All nodes have global knowledge of the network and employ the greedy algorithm.
- To make the chain then we start with the outermost node from the Base Station.
- We begin with this node in order to construct sure that nodes farther from the Base Station have close neighbors, as in the greedy algorithm and the neighbor distances will increase slowly since nodes already on the chain cannot be revisited.
- When a node dies, the chain is reconstructed in the same manner to bypass the dead node.
- This network can tolerate fault of maximum 4 nodes.

4. Results and Discussion

In the adjacent Figure node 0 connecting to node 3, node 3 connecting to node 1, and node1 connecting to node 2 in that order. When a node dies, the chain is reconstructed in the same manner to bypass the dead node[11].

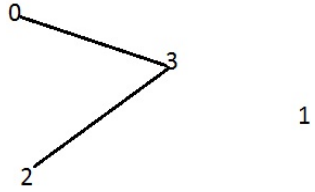


Figure 5. Level 1 Simulation Result.

Therefore the result

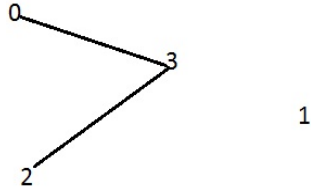


Figure 6. Level two Simulation Result.

Therefore the network looks like:

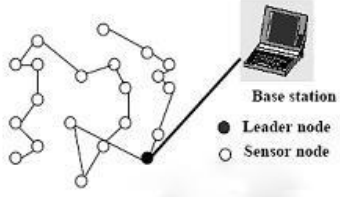


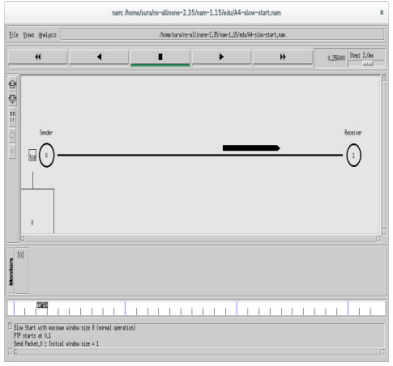
Figure 7. Network System.

4.1.1 Fault Tolerance in Sensor Nodes

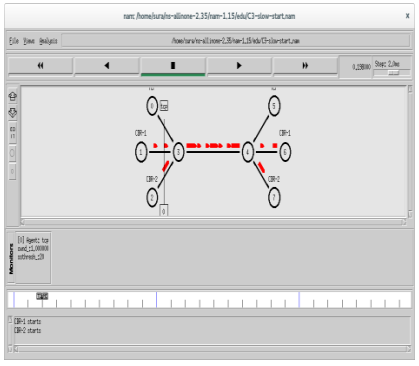
- After detection of fault in a node in the cluster member, the other nodes at its vicinity (in a definite transmission range) will substitute the faulted nodes.

- The data sensed by the nodes at the vicinity of the faulted node when collected at the base station are averaged and determined as the data sensed by the faulted node.
- That is let number of nodes be n in a particular transmission range if 1 node is faulted then no. of nodes working in its transmission range is n-1 therefore data determined to the faulted node = data collected by (1st+2nd+3rd+...+n-1) nodes/no. of nodes working i.e., (n-1).

(a) Creation of a basic simple sensor network using two nodes



(b) Inter node data transmission.



Inter cluster Transmission

(c) Detection of faulty node in the Sensor network:

In the adjacent Figure node 0 connecting to node 3, node 3 connecting to node 1, and node1 connecting to node 2 in that order. When a node dies, the chain is reconstructed in the same manner to bypass the dead node.

Sensor Nodes

5. Limitations

5.1 Limitation of a Wireless Sensor Network

- One of the biggest disadvantages of large scale wireless sensor networks lies on the complexity of logistics involving selective replacement of sensors that have ran out of energy.
- Lower speed compared to wired network.
- Less secure because hacker's laptop can act as Access Point. If you connected to their laptop, they can access all your information (username, password etc).
- More complex to configure than wired network.
- Affected by surrounding. Eg., walls (blocking), microwave oven (interference), far distance (attenuation).
- Gets distracted by various elements like Blue-tooth.
- It does not reduce costs for installation of sensors.

6. Conclusion

Due to the potential deployment in uncontrolled and harsh environments and due to the complex architecture, wireless sensor networks are prone to a variety of malfunctioning. Our goal was to identify the most important types of faults, techniques for their detection and diagnosis, and to apply a technique for ensuring efficiency of fault resiliency mechanisms. Although extensive works have been done on fault tolerance in each layer of the WSN system, cross-layer solutions are expected in future. Use of the resource could be more efficient if resource can be properly integrated and scheduled in different layers. Therefore, cross-layer solutions are expected to have better performance than current solutions.

Future research in this field will enrich it with newer techniques and better performance. This method is energy efficient for the sensor network. By removing the faults in the network the performance of network changed in terms of lifetime, throughput and average energy dissipation.

7. References

1. Tseng YC, Kuo SP, Lee HW, Huang CF. Location tracking in a wireless sensor network by mobile agents and its data fusion strategies. Lecture Notes in Computer Science, Springer Link. 2003; 2634:2–3.
2. Chen P. Application of chemometric algorithms to ion mobility spectrometry and matrix assisted laser desorption/ionization time-of-flight mass spectrometry; 2008 Jun.
3. Taniar D. Mobile computing: Concepts, methodologies, tools, and applications. Information Science Reference - Imprint of: IGI. Publishing Hershey; 2008.
4. Siddiqua A, Swaroop S, Krishan P, Mandal S. Distance based fault detection in wireless sensor network. IJCSE. 2013 May; 5(5). ISSN: 0975-3397.
5. Mythili T, Narmadha RT, Nivetha RT. A survey on wireless sensor network protocols. International Journal of Computer Science and Mobile Computing. 2014 Jan; 3(1):423–7.
6. Verma A. Time constrained fault tolerance and management framework for k-connected distributed wireless sensor networks based on composite event detection. Department of Computer Science and Engineering, National Institute of Technology Rourkela; 2011 May.
7. Titouna F, Titouna C, Benferhat S. Probabilistic checkpointing protocol to sensor network fault tolerant. IJCSI. 2012 Sep; 9(5).
8. Mandal K, Sen A, Chakraborty A, Roy S, Batabyal S, Bandyopadhyay S. Road traffic congestion monitoring and measurement using active RFID and GSM technology. 14th International IEEE Annual Conference on Intelligent Transportation Systems; Washington, DC. 2011 Oct 5-7. p. 1375–9.
9. Roy S, Bandyopadhyay S, Das M, Batabyal S, Pal S. Real time traffic congestion detection and management using active RFID and GSM technology. The 10th International Conference on Intelligent Transport Systems Telecommunications, ITST 2010; Kyoto, Japan. 2010.
10. Suresh D, Selvakumar K. Improving network lifetime and reducing energy consumption in wireless sensor networks. International Journal of Computer Science and Information Technologies. 2014; 5(2):1035–8.
11. Kaur N, Kumar D. Analysis of clustering algorithms in wireless sensor network. IOSRJEN. 2014 May; 4(5).
12. Kaur A, Garg EU. Enhanced cluster based distributer fault tolerance algorithm for mobile node in WSN. International Journal Of Engineering And Computer Science. 2014 Oct; 3(10):8487–92.