A Survey on Classification of Fault Tolerance Techniques Available in Wireless Sensor Network

A. Samson Arun Raj
Post Graduate Student
Karunya University, Karunya Nagar,
Coimbatore - 641114

Mrs. K. Ramalakshmi M.E
Assistant Professor (SG)
Karunya University, Karunya Nagar,
Coimbatore – 641114

Mrs. C. Priyadharsini M.E
Assistant Professor (SG)
Karunya University, Karunya Nagar,
Coimbatore – 641114

Abstract

Wireless sensor network are prone to different types of failures like connectivity, link, node and malfunctioning of nodes, due to various environmental, hazards. In such situation, the efficiency of the sensed information will be less and the purpose of deploying wireless sensor network is not effective. Wireless sensor network will be efficient if it is capable of identifying the faults and rectify it, instead of discarding it. This paper concentrates on the survey based on the various faults occurring in wireless sensor network. Once the fault has been rectified, then the fault tolerant capability under the faulty condition of the wireless sensor network can be enhanced.

Keyword: Fault Tolerance, Fault Detection, Security, Aggregation.

1. Introduction

There are various improvements that have been made in the sensor nodes in both size and capable of processing the sensed data for effective communication between sensor nodes and the base station. The sensor nodes can be placed in various applications like college campus, office building, hospitals and temperature reading from a particular region. Each sensor node will be having a battery lifetime of one year which is based on the application used. The sensed data from the sensor nodes will not be reported to the base station correctly due to collision between the sensor nodes, finding an alternative path to reach the destination and some sensor node will be using full usage of battery power to transmit large amount data and hence some data will be lost during transmission. The sensor nodes can be placed in the field by either randomly or by using Grid based approach.

A sensor node has four basic components as shown in Figure 1; they are as follows (a) *Sensing Unit* a sensor node will be carrying all the sensed data and it is converted into digital format using Analog Digital Converter (ADC), (b) *Transceiver Unit* the digital signals will be transmitted or received between the sensor nodes through wireless communication, (c) *Processor Unit* all the sensed data will be processed though a inbuilt processor like microcontroller and each sensor node will be having a fixed size of memory for temporary storage like timestamp and co-ordinates of the object, (d) *Power Unit* each sensor node will be having limited battery power. Hence the more sensing of data takes place, the more battery power it will be consumed. Once the sensor nodes are being deployed in the environment it is hard to replace or recharge the battery of that particular sensor node.

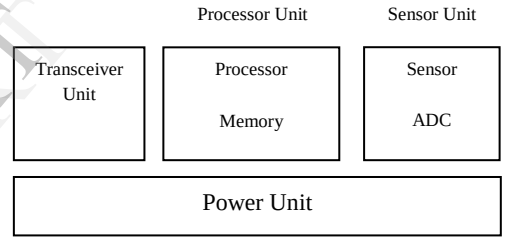

Figure 1 Components of a Sensor node

2. Classification of Fault Tolerance

The hierarchy of the fault tolerance is classified based on the different kinds of fault, which occur in Wireless Sensor Network. Figure 2 shows the faults such as: (a) Connectivity fault, (b) Link fault, (c) Node fault and (d) Malfunction nodes.

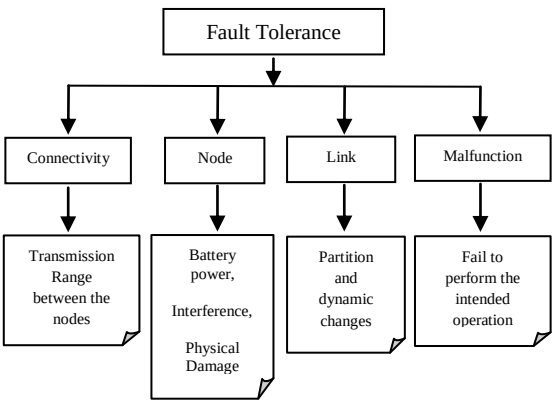

Figure 2 Hierarchy of Fault Tolerance

The connectivity fault which occurs between two sensor nodes, it is due to shortage of transmission range. In order to overcome this fault we will use additional sensor nodes i.e. which is called as *relay nodes*, these relay nodes are being placed between two sensor nodes and provides connectivity between them. These relay nodes can be placed either random deployment or by using Grid based approach.

The node fault is one of the major source faults that being occurred in the wireless sensor network, this fault is fully based on the battery power. Physical damage is one of the node faults and it depends on the application used, because some application the sensor node will be affected due to the environment aspects.

The link fault is another major source faults that being occurred in the wireless sensor network, this fault is fully based of the link between the sensor nodes. Once the link between the two sensor nodes are failed, the remaining sensor nodes must update the routing table and move further to the network for finds a replacement for that link.

The malfunction nodes in the wireless sensor network, it does not perform the intended operation according to user choice, but rather than it performs other operations like sending incorrect sensed information to the base station. Hence, we must find the faulty sensor node and separate it from being a communication node.

2.1 Link based fault tolerance for Wireless Sensor Network

Consider a tree structure topology, where the root will be base station and the leaves will be sensor nodes. A relay node will be placed between the base station and sensor nodes, it will be acting as a sub-root in the topology [1]. The sensor nodes will be sensing the information and transmits the sensed information to the relay node, once the relay node has the sensed information it will be forwarding the information to the base station. The relay node will be high power capability and each relay node can handle up to nine sensor nodes. A unique address will be given to each sensor node when new sensor node joins the network. The level of the topology will be 4, if the level is 5 then no further sensor nodes will be added to the network. The entire relay node will be maintaining a routing table; it contains the location and address of the sensor nodes. If the link is failed between the base station and relay node, then the failed link should update and re-establish a new link between them. Some sensor nodes can be connected directly to the base station, but their network lifetime will be reduced due to more energy consumption. For the applications like military field, office building and industrial plants, there are chances that an intruder can easily access the sensed information through the links. For a secure and efficient network, we will be using a technique called HSPREAD [4]. This technique will be finding all the possible ways to reach sensor nodes from the base station. Any sensed information flow from the base station to the sensor nodes, this HSPREAD will be tagging the route with sink ID and other neighbour sensor node ID. By using this HSPREAD technique, only a limited number of possible paths can be identified. Hence, they make sure that the topology level of sensor nodes doesn't goes beyond level 4. For a random topology, the sensor nodes are deployed randomly [2]. The sensor node will be using full energy in order to transmit even a single bit of information from a far distance to the base station. Hence, the link between the sensor nodes will be disconnected due to more energy it consumes. In order to save the energy of the sensor nodes, we will be using a cluster; the cluster will be collecting all the sensed information from all the sensor nodes and directly transmits the sensed information to the base station. A cluster can be also called as LEACH. The LEACH will be having high power capability and has wide sensing range, so that more number of sensor nodes can join and transmit the information. LEACH-Coverage is an extension of LEACH. The sensing coverage will be improved and more sensor nodes can join the cluster, when comparing with LEACH. Sensor network will be having a two-tier hierarchy [4], the upper layer will be for the relay node which is responsible for forwarding the sensed information to the base station, and it can use a multi-hop path to reach the base station. The lower layer will be for the sensors, it will be sending all the sensed information to the relay node. Hence, the sensor nodes no need to perform routing and forwarding the sensed information to the other nodes. The motivation of this two-tier hierarchy is that, the sensor network should contain only minimum number of relay nodes and the location of these relay nodes should be specified. If relay node fails, it disrupts the information flow of other relay nodes. Hence, redundancy should be provided to other relay nodes. The information flow from Relay node to the base station can be either (a) Single Hop or (b) Multi Hop. For a Single hop routing, the sensed information from the sensor nodes to the relay nodes will be directly forwarded to the base station. For a Multi hop routing, the sensed information from the sensor to the relay nodes will be forwarded to other relay nodes or receives sensed information from some other sensor nodes and finally, a large number of sensed information is sent to the base station. The relay nodes can be placed either (a) Grid based approach or (b) Intersection based approach. The Grid based approach will be easy and simple for placing the relay nodes in the environment. The relay nodes can be placed either in the center or in the corners of the grid. For the intersection based approach, we will be placing the relay nodes at the intersection point between the two relay nodes. The backup relay node can be placed in the next near intersection point. Initially, the sensor nodes will be transmitting sensed information to the base station

and waits for the action for that sensed information. The base station first gathers all the sensed information from all the sensor nodes and performs the corresponding action and sends the reply to the sensor nodes. Hence, the sensor node will be waiting for the reply as well as the energy level will be drained. There can be single point failure, if the base station fails then the entire sensor nodes must wait for the replacement of base station. In order to overcome this single point failure, we will be using a peer topology [5]. We will be using technique called Consensus problem which is an extension of Byzantine agreement problem, in which all the sensor will be formed as peer-to-peer structure with at most five sensor nodes as group and makes an agreement without the help of the base station. This group will be having its own value to make agreement and these agreement values will be broadcasted to its neighbouring groups. If a single sensor node is not agreeing the value, the other sensor nodes will check the majority and takes the corresponding action for the final agreement value.

2.2 Monitor node in Wireless Sensor Network

A monitor node will be added separately in the sensor network, where it will be detecting the faults and report them to base station what type of fault which is occurred in the network and the monitor node maintains the health of the network. Hence, we will be using an out-of-band monitoring [6]. The monitor node transmits all the monitor traffic and dedicated monitors in a separate channel. A monitoring node can either be placed directly on a sensor node or inside the sensor network near to the sensor nodes.

2.3 Node based Fault Tolerance in Wireless Sensor Network

Consider a tree structure topology [1]. The base station will be gathering all the sensed information from the sensor nodes and it performs the corresponding action to the sensed information and the reply is being send back to the sensor nodes. The base station will be calculating the aggregate values from different sensor nodes [7]. The aggregation will be having the following operations like sum, count and average. In order to reduce the aggregate computation failure, we will be using multi-tree aggregation for reducing the variance. If any failure that occurs on the sensor node, there are two techniques available (a) Rebuilding and (b) Local fixing. For Rebuilding technique, if there is a failure on the sensor node we can able to rebuild the topology. For Local fixing, if there is a failure on performing the aggregate operation we can able to find the sensor node by identifying the address of the sensor node [1]. Once the sensor node is found, we can easily fix the sensor node. There are two models for a multi-tree aggregation (a) Levelized Multi-trees, where all the sensor nodes and the parent nodes will lie on a same level. (b) Arbitrary Multi-trees, there are no restrictions in position of sensor nodes. If the sensor node is not performing the operation correctly due to battery power, we use a technique called Amendment process [8]. This process will be performed automatically in the middle of the operation. There are two algorithms available (a) Localized aggregation tree repairing algorithm and (b) Distributed rescheduling algorithm. For the Localized repairing algorithm, it is similar to local fixing [7]. For Rescheduling algorithm, once the amendment process is over we can able to provide an alternative path to reach the base station. If the root node has failed, every child node should find a new parent and update its address [1]. If the child node has failed, the parent node will just remove its address and removes the sensor node from the sensor network. Once the amendment process is over, the entire topology level of the sensor nodes will be at different level and goes beyond the predefined topology level.

2.4 Connectivity based Fault Tolerance in Wireless Sensor Network

To achieve a proper level of connectivity among the sensor nodes, we will be placing a relay node between the sensor nodes by providing 2-(edge, vertex) connectivity [9]. The problem will be addressing connectivity and limited communication between the sensor nodes. For placing a relay node in the network, we must calculate the distance between two sensor nodes by using Euclidean distance. A link E=(x, y) belongs to E between two sensor nodes, if nodes x and y are within unit distance. Hence, the connectivity will be simple but if the distance is more then we will be placing a relay node. There are two techniques performed in order to achieve a proper connectivity, they are (a) Depth First Traversal and (b) Cycle Creation. For Depth First Traversal, we will be labelling the sensor nodes according to their address [1] and we must connect these sensor nodes in order to form a cycle. Once these sensor nodes are connected, a cyclic structure will be formed in the network and we will remove the relay nodes from the network. Hence, we can able to see that, there is connection from the first sensor node to the last sensor node and we can able to get a proper communication from all these sensor nodes. There are six different ways to place a relay node in the sensor network. Hence, there is difficulty in placing the relay nodes in the polygonal regions of the network. We call these regions as forbidden regions.

2.5 Malfunction nodes based Fault Tolerance in Wireless Sensor Network

There is certain amount of sensor nodes in the network which is called faulty nodes, the faulty node doesn't perform according to the user choice or it can be called as faulty due to low battery power. These faulty

nodes can be identified by using a technique called Fault Detection for Wireless Sensor Network (FDWSN) [11]. In FDWSN, a comparison will be taken between two sensor nodes and broadcasts the decision made to all the neighbouring nodes. Hence, this comparison between the sensor nodes is time consuming. In order to eliminate delay, we will be using a sliding window which contains the previous comparison results. Once the faulty node has been identified, we must ensure that the link between the sensor node and faulty node are separated from the other remaining sensor nodes. For a secure link between the sensor nodes, we will be using a standard technique called communication graph. The communication graph can be represented as G (V, E) where V are the sensor nodes and E is the link between the sensor nodes. Consider there are two sensor nodes vi and vj with a link E and the distance between them will be d (vi, vj). The sensor node vi is compared to the vj with the help of sliding window; if the outcome between these sensor nodes are fault-free, a label cij=0 will be placed on the edge E. If the outcome between these sensor nodes are faulty, a label cij=1 will be placed on the edge E. There are two performance parameters in FDWSN; they are (a) Detection Accuracy and (b) False Alarm Rate. For Detection Accuracy (DA), it will be identifying which are the faulty nodes are currently active from the previous results. For False Alarm Rate (FAR), it will be identifying which are the fault-free sensor nodes in the sensor network which are considered as faulty nodes. A cluster can handle several number of sensor nodes within its coverage and the cluster contains a self diagnosis to monitor each sensor node and identify the faulty nodes [11]. The result is periodically launched to base station through clusters. There are techniques available to identify the faulty node; they are (a) Proactive approach and (b) Passive approach. For Proactive, a debugging agent is attached within the sensor node. For Passive, a separate monitor will be placed within the network [6] and it will be sending the traffic analysis periodically to the base station through a separate channel.

3. Conclusion

The hierarchy gives the overview of various faults that are occurring in wireless sensor network and the most common faults that are link and node fault. For link fault, we will be placing a relay node with high power capability of transferring the sensed information to the destination. If the link fails between the relay node and sensor nodes, the sensor node should update its address while joining with a new relay node. Hence, the relay node will be consuming more energy and some relay nodes does not perform any operation. For node fault, there is a standard approach to identify the faulty sensor node is by using communication graph. The values between the two sensor nodes are being compared with the help of a sliding window, which contains previous results. Hence, the faulty node identification is needed to be improved because once the pendant is formed in the network, no further action will be taken for these faulty nodes rather than it gives only the result that there is faulty sensor node in the network. For the future enhancement we should further increase energy of the sensor node as well as the information flow to the base station with minimum relay nodes.

4. References

[1] Anurag D, Somprakash Bandyopadhyay, “Achieving fault tolerance and network depth in hierarchical wireless sensor networks”, San Francisco, 2008.

[2] Amini Navid, et al, “Cluster size optimization in sensor networks with decentralized cluster-basd protocols”, Computer Communications, 2012.

[3] Bari Ataul, et al, “Design of fault tolerant wireless sensor networks satisfying survivability and lifetime requirements”, Computer Communications, 2012.

[4] Challal Y, et al, “Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks”, Journal of Network and Computer Applications, 2011.

[5] Chen Xian, et al, “Fault-tolerant monitor placement for out-of-band wireless sensor network monitoring”, Ad Hoc Networks, 2012.

[6] Chitnis Laukik, et al, “Analyzing the techniques that improve fault tolerance of aggregation trees in sensor networks”, Journal of Parallel and Distributed Computing, 2009.

[7] Feng Yunxia, et al. “Fault tolerant data aggregation scheduling with local information in wireless sensor networks”, Journal of Science and Technology, 2011.

[8] Hsieh Hui-Ching, et al, “A fault-tolerant scheme for an autonomous local wireless sensor network”, Computer Standards and Interfaces, 2010.

[9] Kashyap Abhishek, et al, “Relay placement for fault tolerance in wireless networks in higher dimensions”, Computational Geometry, 2011.

[10] Lee Myeong-Hyeon, et al, “Fault detection of wireless sensor networks”, Computer Communications, 2008.

[11] Zhaoa Xibin, et al, “A novel fault diagnosis mechanism for wireless sensor networks”, Mathematical and Computer Modelling, 2011.