International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 9, Issue 2 (November 2013), PP. 53-56

Detecting Sensor Node Failure and Node Scheduling Scheme for Wsn

J. Dhananandhini[1], C.M. Niranjana[2], K. Rajeswari[3], R.Karthick[4]
[1,2,3,4]*II-ME,Department of Computer Science and Engineering, Muthayammal Engineering College, Rasipuram – 637 048, Tamilnadu, India.*

Abstract:- The Wireless Sensor Network is build of "nodes"- from a few to several hundreds or even thousands, where each node is connected to one sensor. A node in a wireless sensor network that is capable of performing some process and gather sensor information and communicating with other connected nodes in the network. The nodes to perform transmissions not successfully, because there are some of the problems may arise in that they are 1) if node failure will occur in any stage, 2) security issues arises due to transmission involves number of nodes, 3) increasing transmission time due to more number of nodes will be active at a time to complete a particular task. To solve this problem we propose new algorithms are 1) node sensing and node failure for activity detection, 2) discovering routes and give security using neighbourhood keys, 3) which node involves to perform the action that current node only to be active at a time other to be sleeping mode using node scheduling scheme.

Index Terms:- Wireless sensor networks, neighbourhood node, node failure, sensor node scheduling , fault-tolerance, Security.

1. INTRODUCTION

Wireless Sensor Networks

Wireless sensor networks are composed of a large number of small sensor devices which are commonly known as nodes. These devices range in size from about the size of a matchbox to the size of a pen tip. The nodes have a low clock rate processor on board and also small amount of memory. They also have some form of sensor attached to them in order to monitor some physical property. Collectively these nodes are able to configure into autonomous ad-hoc networks using a variety of communication devices. In addition to being able to form networks autonomously protocols exist to allow sensor networks to reconfigure dynamically around moving nodes. These networks of nodes are able to collect, process and store data from sensors. They are capable of transferring data with each other and of transmitting data through the network back to a base station. The concept of WSNs is based on a simple equation: Sensing + CPU + Radio = Thousands of potential applications. Each element of the network is commonly called a "mote" or smart sensor. Sensor node requires Low Power, Support Multi-hop Wireless Communication, to configure itself, Physically small in Size, and Can Reprogram over Network.

In computer algorithm neighbourhood node represented using graph through adjacency matrix representations. Neighbourhood used in clustering coefficient of graph, that is a measure of the average density of the neighbourhoods. Many important classes of graphs may be defined by properties of their neighbourhoods, or by symmetries that relate neighbourhoods to each other. A current node can be updated using their neighbour node in the scheme of node updation. A new approach to help maintain sufficient activity detection accuracy in the presence of sensor failures. If sensor failures that affect the high-level application- level behavior of the system need to be repaired. Common failures in the system includes: Node Failure, Area Failure and Lost Message. In communication system important aspect of analysis and design is fault detection and testing.

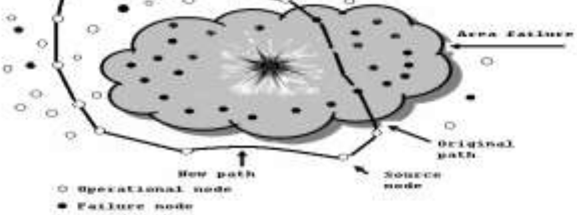

Fig 1 : Node Failure in WSN

The nodes in wireless sensor networks have a limited lifetime span due to the fact they are powered by batteries. Nodes may fail due to hardware failure. There may be environmental condition changes, such as electromagnetic noise and physical destructions, which may cause a node to fail, or temporarily changes to participate in the current network topology. With these node failures, topology management schemes must consider the fact that some nodes may randomly fail in the network. In this case sensor need for other active nodes to compensate for these failed nodes.

In WSNs not every sensor node needs to be active at the same time for sensing and communication. To reduce unnecessary power consumption, only a minimum number of sensor nodes operate in active mode and the others are kept in sleep mode. In such a case, however, the network service can be easily unreliable if any active node is unable to perform its sensing or communication function because of an unexpected failure. Thus, it is important to maintain the original sensing level even when some sensor nodes fail.

Ad-hoc networks are cooperative in nature and rely on implicitly trust the neighbour route packets among participants of all nodes. Different security attributes are used to improve the quality of an security of an ad-hoc network. In this secure routing method information in the secure routing to be protected in this SAR protocol to be used for secure route discovery, update the states of every node.

II. METHODS AND ALGORITHMS

1) To sense the node and Dynamic Discovering Routes are used to detect if any failure occurs in the communication process- Testing based Procedure cross validation Algorithm to be used.

2) Security using neighbourhood keys- Security Aware Routing Protocol to be used.

3) Node Scheduling Scheme using – Adaptive Node scheduling method.

a) Node sensing and node failure for activity detection

The basic idea is node or area failures is quite simple: every node maintain states of its parent node. When it finds that parent node has failed, it asks its neighbour nodes for their connection information using neighbourhood key. It then chooses a new parent node from its neighbour nodes based on this connection information between the nodes. A dynamic discovering routing method that can be integrated in any routing protocol for WSN to make it fault tolerant. It dynamically repairs a routing path between a sensor node and a base station. Using Random number generator a failed node to be identified. The random number will identify which node in the sensor network will fail during each cycle in the test. In order to maintain a connected network another node must compensate for the failed node. To perform this test the neighbour node will increase the energy level.

Three methods to be used to maintain routing paths in the occurrence of node failure, first one is routing paths to be reconstructed then the center of attention on how each sensor node maintains its routing path to base stations. Make the set up early initial routing method from each sensor node to a base station. For e.g. the TinyOS beacon protocol. In that each node already has a path to the base station, and knows its parent node, neighbor nodes and the number of hops it is from the base station. This information can be initialized by using the TinyOS beacon protocol for setting up routing paths. Second methods is multiple paths are used here the data to be passed based on this method. Data can be transmitted to base station because of each path from a sensor node to a base station is broken by failed node. This method will increase the energy consumption and packet collisions, because data is sent through multiple paths, irrespective of whether there is a node failure or not. Last method is to select the path basis on probabilistic manner. In this within certain probability a node chooses another node to forward a packet.

The practical method in fault finding is to distinguish a random noise to run a maximum likelihood approach on the multi sensor fusion measurements. A random noise would exist, if running these procedures improves the accuracy of the final results of multi-sensor fusion. There have been several efforts to minimize random errors, very little has been done for fault detection. In multi-sensor fusion, the measurements from different sensors are combined in a model for consistent mapping of the sensed phenomena. The main goal of on-line testing to detect the faults in the sensors. Test vector generation is one of the on-line testing method in this method already available sources of excitations and alternative is to use one or more actuators in addition to that. The actuators maximize the chances for detection of faults in the maximum number of sensors.

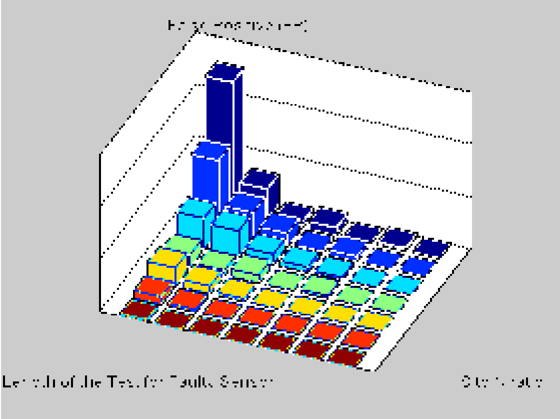

Fig 2: Number of false positive reporting during fault detection for sensor network of 200 light sensors and 60 faulty sensors.

Testing based Procedure cross validation Algorithm

Step 1: Using Non-linear function minimization perform the sensor fusion function

Step 2: Set the while condition for stopping criteria if it doesn't stop the function to continue the process

Step 3: To perform the sensor fusion process using non-linear function minimization in that set the initial value to i and each step of process increase the value of i using for loop.

Step 4: Alert trigger event will be given for sensor fusion and to identify most discrepant sensor.

Step 5: To update the already fixed stopping criteria

Step 6: Faulty sensors to be eliminated in that interval confidence between that to be Established

Step 7: With High intervals of confidence the eliminated sensors to be reinstalled.

b) Security using neighbourhood keys

To give the security between the nodes we must protect the information for communication purpose. Ad-hoc routing protocols are cooperative in nature and to route packets among participants nodes for rely on implicit trust your neighbourhood node relationship. In ad-hoc routing recovery scheme based on the metrics geographic location and signal stability can improve the quality of the relevance of the routes. Attributes of secure route to be identified and the level of security to be defined. The solutions based on digital signatures, receiver nodes authenticate received broadcast messages by verifying the senders' signature attached to the message.

c) Node Scheduling Scheme

The node scheduling scheme is mainly focus on achieving coverage with maximum network lifetime and minimum sensing level. Many algorithms are dealt with the problem of sensing level but this fault-tolerant sensor node scheduling scheme little modification on that scheme will produce more efficiency, Which will handle the sensor node failure. The proposed FNS(Fault tolerant node scheduling) algorithm designates a set of backup nodes for each active node in advance. If an active sensor node fails, the set of backup nodes pre-designated for the active node will activate themselves to replace it, enabling to restore the lowered sensing level for the coverage of the failed node. Backup node selection strategy can be applied to the existing node scheduling algorithms such as Coverage Preserving Node Scheduling (CPNS)The backup nodes for an active node are a set of nodes by which the sensing area of the active node is completely covered.

To save the power consumption, only a minimum number of sensor nodes operate in active mode and the others are kept in sleep mode. In that case the wireless network service can be easily unreliable if any active node is unable to perform its sensing or communication function because of if any unexpected failure occurs for the transmission process. Thus, it is important to maintain the original sensing level even when some sensor nodes fail. In the proposed FNS algorithm, a set of backup nodes are prepared for each active node to be used to replace the active node in case of its failure. All nodes are scheduled to be in active mode broadcasts a BREQ message which contains its ID and node lifetime period. To sense each node in sleep mode periodically wakes up and checks the lifetime of the packets from its neighbouring active nodes. If any failure occurs in the active node it doesn't send the information to the particular lifetime, it decides that some fault occurs in the active node and switches itself to active mode. So the CPNS algorithm is performed locally in these waken-up nodes.

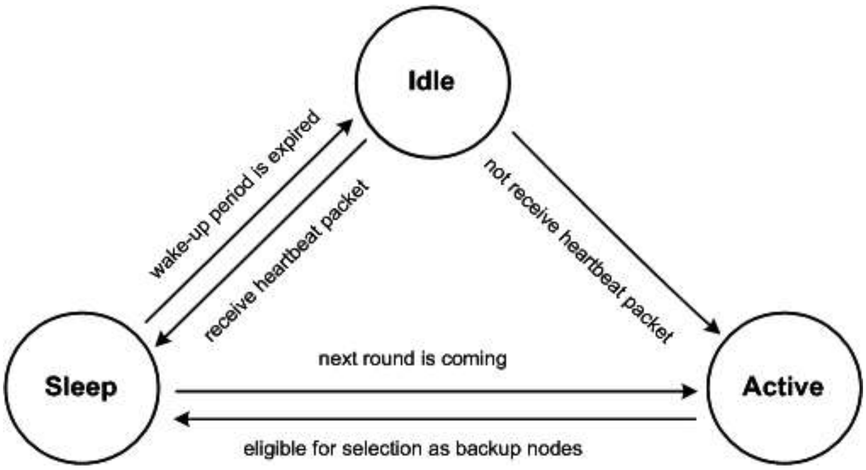
Idle
Sleep
Active
wake-up period is expired
receive heartbeat packet
not receive heartbeat packet
next round is coming
eligible for selection as backup nodes

Fig: State transition diagram of a backup node in FANS.

Backup node selection algorithm

Step1: all node to scheduled that to be active mode, set the timer for lifetime
Step2: check the lifetime if it is expired broadcast the BREQ message to all other neighbour nodes.
Step3: End the active mode selection process.
Step4: all node to scheduled that to be sleep mode, set the timer for lifetime
Step5: if BREQ message is received calculate the angle between the nodes, between that angle pass the BREP message to the receiver.
Step6: the message is received before the timer is expired check the BREP message with the angle if it is not discard the message otherwise broadcast the message, set self backup node selection strategy.
Step7: self backup node is selected the process to be successfully done.

IV. CONCLUSION

In Wireless Sensor networks are transfer the information in unreliable wireless environment this may arise different types of node failure and security issues in the unreliable wireless environment. To solve the issues some of the mechanism to be introduced and solved manually. To implement the problem using the following methods 1) To sense the node and Dynamic Discovering Routes are used to detect if any failure occurs in the communication process- Testing based Procedure cross validation Algorithm implemented. 2) Security using neighbourhood keys- Security Aware Routing Protocol and 3) Node Scheduling Scheme using – Adaptive Node scheduling Algorithm to be implemented. This algorithm will increase the performance of node detection and decrease the security issues of the user related information.

REFERENCES

[1]. Mokhtar Beldjehem " Toward a Multi-Hop, Multi-Path Fault-Tolerant and Load Balancing Hierarchical Routing Protocol for Wireless Sensor Network" Wireless Sensor Network, 2013, 5, 215-222

[2]. Amin Hassanzadeh, Radu Stoleru, Jianer Chen Department of Computer Science and Engineering, Texas A&M University "Efficient Flooding in Wireless Sensor Networks

[3]. Secured with Neighborhood Keys" 2011 IEEE 7th International Conference on Wireless and Mobile Computin978-1-4577-2014-7/11

[4]. Arabinda Nanda, Amiya Kumar Rath, Saroj Kumar Rout "Node Sensing & Dynamic Discovering Routes for Wireless Sensor Networks" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010

[5]. JUNGEUN CHOI, JOOSUN HAHN AND RHAN HA, "A Fault-tolerant Adaptive Node Scheduling Scheme for Wireless Sensor Networks, JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 25, 273-287 (2009)

[6]. Farinaz Koushanfar EECS Dept., UC Berkeley, Miodrag Potkonjak CS Dept., UC Los Angeles, Alberto Sangiovanni-Vincentelli EECS Dept., UC Berkeley" On-line Fault Detection of Sensor Measurements" 0-7803-8133-5/03/$17.00 ©2003 IEEE

[7]. L. Bao and J. J. Garcia-Luna-Aceves, "Topology management in adhoc networks", MobiHoc'03, Annapolis, Maryland, ACM, June 1-3,2003.

[8]. Yenumula B Reddy Grambling State University Grambling, LA 71245

[9]. " Security issues on WSN " SENSORCOMM 2011, 26/09/2011.