International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 2, Volume 2 (February 2015) www.ijirae.com

FAULT TOLERANCE IN WIRELESS SENSOR NETWORKS

C.Ahila Jerlin[#1]
Anand Institute of Higher Technology,
Department of ME Embedded System Technologies ,
Kazhipattur, Chennai-603103

N.Rajkamal[#2]
Anand Institute of Higher Technology,
Department of ME Embedded System Technologies,
Kazhipattur, Chennai-603103

ABSTRACT: ***Wireless sensor networks have the potential to enable a substantial class of applications like battlefield surveillance, environmental monitoring, intruder detection systems, intelligent infrastructure monitoring and scientific data collection. The sensor nodes in wireless sensor networks may be deployed in unattended and possibly hostile environments. The environment affects the monitoring infrastructure that includes the sensor nodes and the network. In addition, node failures and environmental hazards cause frequent failures in communication. Thus, the faults in WSNs are likely to occur frequently and unexpectedly as compared to that of traditional wireless networks. The fault is an incorrect state of hardware or a program as a consequence of a failure of a component. Thus, in order to guarantee the network quality of service, it is essential for the sensor network to be able to detect and heal failures. Motivated by the need to determine the ability of a sensor system to tolerate the failure of sensors, we propose a self-healing capability in the system. The proposed measure is to characterize the likelihood that a system is still working in the presence of sensor failures.***

Key Words: Nodes, Network Simulator, Routing, Sensor nodes, Self-healing.

I.INTRODUCTION

A Wireless sensor network is a set of small devices, called sensor nodes, which are able to sense, process, and communicate data. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process Monitoring and control, machine health monitoring, and so on. They usually consist of a processing unit with limited computational power and limited memory, sensors or, a communication device (usually radio transceivers or alternatively optical), and a power source usually in the form of a battery. The base stations are one or more components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables.

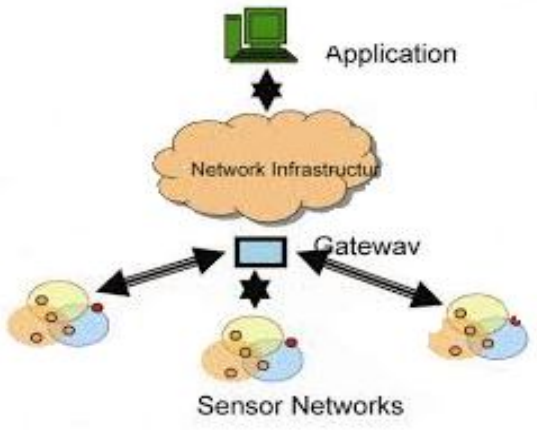

Fig 1 Wireless Sensor Network

One important issue among the various design challenges in developing sensor nodes is to ensure network-wide wireless communication among a multitude of nodes, each with limited Trans processing capabilities while using a shared communication medium. A lot of effort has been invested in developing topology control and routing strategies to reduce the communication overhead and guarantee message delivery**.**

II. HARDWARE FOR WSN

A sensor node is made up of four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. They may also have application dependent additional Components such as a location finding system, a power generator and a mobilizer. Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs).the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit.

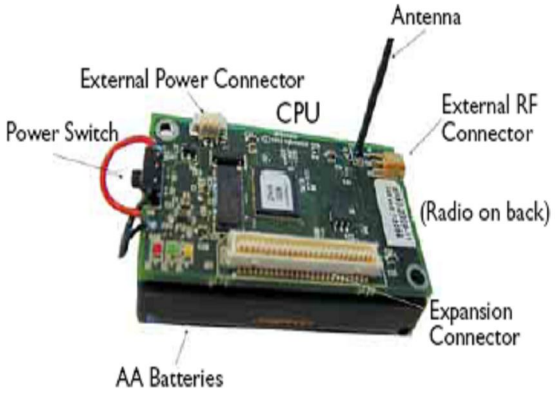

Fig 2 Wireless sensor node

The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit.

III. NODE FAILURE

A physical network node is an active electronic device that is attached to a network, and is capable of sending, receiving, or forwarding information over a communications channel. A passive distribution point such as a distribution frame or patch panel is consequently not a node.WSN is a self-organized network that consists of a large number of low-cost and low powered sensor devices, called sensor nodes, which can be deployed on the ground, in the air, in vehicles, on bodies, under water, and inside buildings. Each sensor node is equipped with a sensing unit, which is used to capture events of interest, and a wireless transceiver, which is used to transform the captured events back to the base station, called sink node. Sensor nodes collaborate with each other to perform tasks of data sensing, data communication, and data processing.

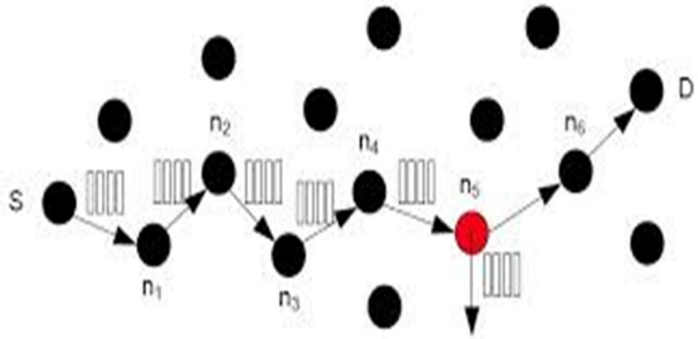

Fig 3 Fault Node

Nodes in WSNs are prone to failure due to energy depletion, hardware failure, communication link errors, malicious attack, and so on. Unlike the cellular networks and ad hoc networks where energy has no limits in base stations or batteries can be replaced as needed, nodes in sensor networks have very limited energy and their batteries cannot usually be recharged or replaced due to hostile or hazardous environments. So, one important characteristic of sensor networks is the stringent power budget of wireless sensor nodes.

IV.FAULT TOLERANCE

Fault tolerance means to maintain sensor network functionalities without any interruption due to failure of sensor node because in sensor network every node have limited power of energy so the failure of single node doesn't affect the

overall task of the sensor network. Adaptable protocols can establish new links in case of node failure or link congestion. Network can able to adapt by changing its connectivity in case of any fault. In that case, well- efficient routing algorithm is applied to change the overall configuration of network. Sensor networks share common failure issues (such as link failures and congestion) with traditional distributed wired and wireless networks, as well as introduce new fault sources (such as node failures). The rapid growth of the Internet in the last 10 years was the first major facilitator of the renewed interest in fault tolerance and related techniques such as self-repair. Sensor nodes are prone to failure because of unattended environment. A sensor node may fail due to hardware or software problem or energy exhaustion. If a few of sensor nodes fail, working protocol should handle this type of fault tolerance. However, the accuracy of readings from sensitive electronic sensors often deteriorates over time due to natural effects such as overheating, sensor surface chemical fouling or low battery power.

V.AUTOMATIC PATH RECOVERY

The process which implemented in sector is automatic fault Recovery when a mica motes connected in a certain topology the signal which may transmitted to a particular level of the frequency the frequency of the mote is 2.4ghz and finally. The transmission may occur it from one mote to another Mote finally it transmit the data to the base station the data transmission may vary for every path of the transmission and The path of transmission may occur due to distance between one mote and the another mote let us consist of large number Motes are transmitted the data to the base station if one mote is under malfunctioning in the transmission path. Finally the path of transmission of destination to source is assign through shortest distance between one node to another node.

VI.ENERGY EFFICIENT ROUTING IN WSN

Routing is the process of selecting best paths in a network. In the past, the term routing was also used to mean forwarding network traffic among networks. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time.

Routing in WSNs is very challenging due to the inherent characteristics that distinguish these networks from other wireless networks like mobile ad hoc networks or cellular networks. First, due to the relatively large number of sensor nodes, it is not possible to build a global addressing scheme for the deployment of a large number of sensor nodes as the overhead of ID maintenance is high.

VII. PROPOSED SYSTEM

In this paper we propose an energy efficient node fault diagnosis and recovery for wireless sensor networks referred as fault tolerant multipath routing scheme for energy efficient wireless sensor network (FTMRS).

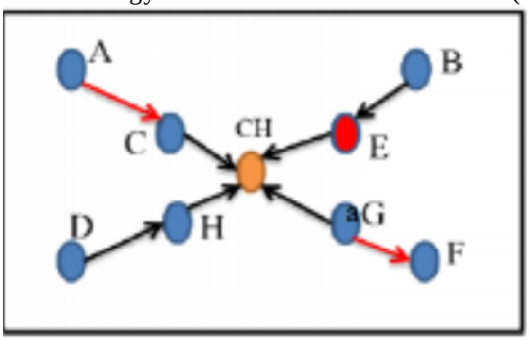

Fig 5 Data Transmission in Nodes

The FTMRS is based on multipath data routing scheme. One shortest path is use for main data routing in FTMRS technique and other two backup paths are used as alternative path for faulty network and to handle the overloaded traffic on main channel .Shortest path data routing. The performance analysis of FTMRS shows better results compared to other popular fault tolerant techniques in wireless sensor networks. The FTMRS technique recovers node fault and transmission fault and transmits data in energy efficient manner. In FTMRS technique, fault tolerant percentage is very high compare to other fault tolerant techniques. Data routing time in FTMRS is very fast and energy aware even at high percentage of nodes fault.

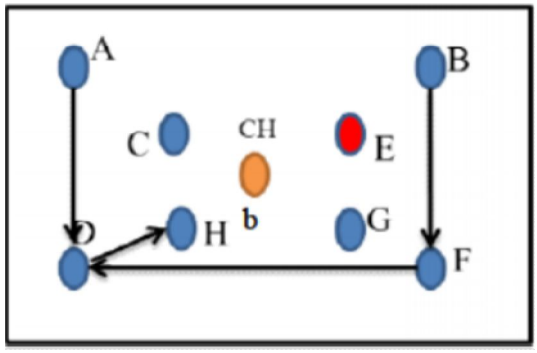

Fig 6 Recovery Path

The FTMRS also proposes a faulty node recovery scheme that effectively reuses or replace the faulty node. The simulation results establish that the proposed routing give better monitoring of the nodes that effectively leads to an energy efficient maximally fault tolerant in sensor network.

VII.NETWORK SIMULATOR

Many network details in WSNs are not finalized and standardized. Building a WSNs test bed is very costly. Running real experiments on a test bed is costly and difficulty. Besides, repeatability is largely compromised since many factors affect the experimental results at the same time. It is hard to isolate a single aspect. Moreover, running real experiments are always time consuming. Therefore, WSNs simulation is important for WSNs development. Protocols, schemes, even new ideas can be evaluated in a very large scale .Network Simulator Version 2, also known as NS-2 is an event driven packet level network simulator developed as part of the VINT project (Virtual Internet Test bed). It is an open source software package available for both Windows and Linux platforms.NS is an Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network set-up (plumbing) module libraries.

VIII.SIMULATION

The general process of creating a simulation can be divided into several steps: Topology definition: to ease the creation of basic facilities and define their interrelationships, ns-3 has a system of containers and helpers that facilitates this process. Node and link configuration: models set their default most of the time this is done using the attribute system. Execution: simulation facilities generate events, data requested by the user is logged. Performance analysis: after the simulation is finished and data is available as a time-stamped event trace.

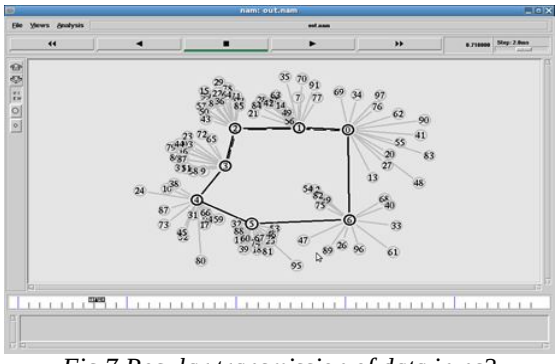

Fig 7 Regular transmission of data in ns2

NAM provides a visual interpretation of the network topology created. The application was developed as part of the VINT project. The output of the project shows that communication between the nodes is achieved in the presence of fault by path recovery.

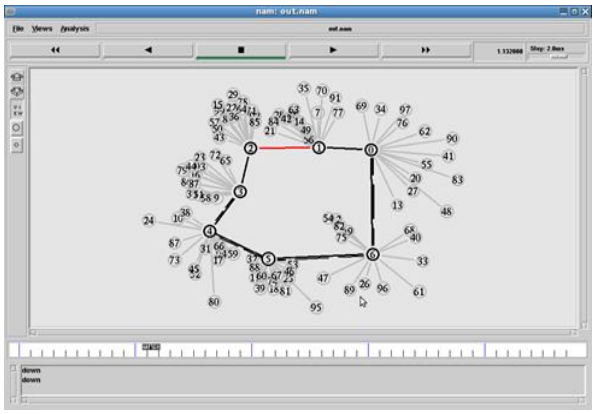

Fig 8 Occurrence of fault during transmission

When the middle mote is under malfunctioning it may selects two set of path for transmission to reach the base station. It selects the path as per the shortest between the one node to another node of transmission.

IX.CONCLUSION

Thus implementation of Self-Healing in Wireless Sensor Network is been done by using Network Simulator which is used to work in all environments and it overcomes the issues of path failure. Node performance has been analysed and evaluated using ns simulator. Simulation results show that higher delivery rate and longer network lifetime. Thus more research work needs to be done in future to find the respective application scenarios like environmental factors, such as operation scenarios, specific data types etc.

REFERENCES

[1] Arunanshu Mahapatro and Pabitra Mohan Khilar. [2013] ” Fault Diagnosis in Wireless Sensor Networks: A Survey” IEEE Communications Surveys & Tutorials ,Vol.15, No 4.
[2] Osianoh Glenn Aliu, Muhammad Ali Imran . [2013] ” A Survey of Self Organisation in Future Cellular Networks” IEEE Communication Surveys& Tutorials, Vol. 15, No. 1.
[3] Paul Meeneghan and Declan Delaney. [2005]”An Introduction to NS, Nam and OTcl Scripting” IEEE sensor journal.
[4] Themistoklis Bourdenas, Morris Sloman. [2009]” Towards Self-healing in Wireless Sensor Networks” IEEE sensors journal.
[5] Xin Miao, Kebin Liu, Yuan He, Dimitris Papadias, Qiang Ma, and Yunhao Liu. [2013] ” Agnostic Diagnosis: Discovering Silent Failures inWireless Sensor Networks” IEEE Transactions on wireless Communications, Vol. 12, No. 12.
[6] Arunanshu Mahapatro and Pabitra Mohan Khilar. [2013] ” Fault Diagnosis in Wireless Sensor Networks: A Survey” IEEE Communications Surveys & Tutorials ,Vol.15, No 4.1.

