FAULT TOLERANCE IN WIRELESS SENSOR NETWORK- A SURVEY

Smt. VIJAYALAXMI S.SADLAPUR

Senior Lecturer

Department of Electronics & Electronics Engg.,

Government Polytechnic Vijayapur, Karnataka. India.

ABSTRACT

A WSN is a collection of sensor nodes organized into a co-operative network. Each sensor node is consisting of microcontroller, memory unit, battery unit and communication interface. WSN were invented to study, control and monitor events and phenomenon. WSNs are having variety of applications in industrial, medical and military areas. Sensor node senses the data, processes it and shares it via communication unit to a base station or a sink node. As these nodes are mostly deployed in harsh environments or unattended areas with limited energy sources, they are more prone to failures. These failures may be due to battery depletions, hardware failures or communication link failures. These may lead to lower desired level of functionality. In this paper, areas of fault occurrences in nodes, importance of fault tolerance and some fault tolerance mechanisms for WSNs are covered in detail.

General Terms

Necessity of fault tolerance. Fault tolerance mechanisms.

Keywords

Fault detection, Fault tolerance mechanisms

INTRODUCTION

A WSN is a collection of hundreds of sensor nodes equipped with capabilities of sensing, computing and communicating. And most of them are battery operated.

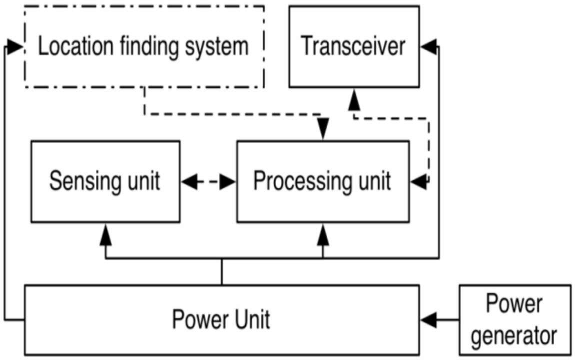

Fig 1: Structural view of sensor node

Figure :1 shows the structural components of a sensor node consisting of mainly sensing unit, computational unit and transmission unit.

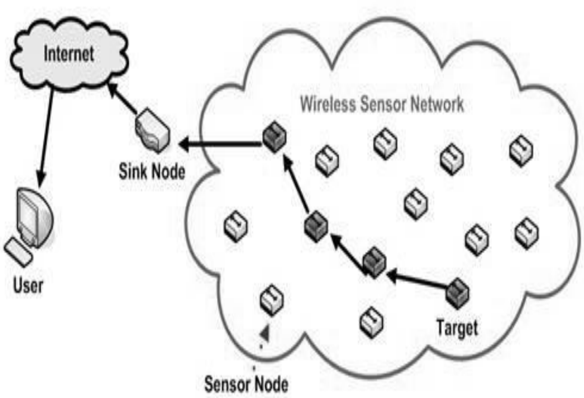

Fig.2. Communication architecture of a WSN

Figure: 2 represents how sensor node communicates to the user. The sensors are deployed randomly at the interested area of study. The sensed data at each sensor node is forwarded to the sink node (also known as base station) by following some MAC and Routing protocols. The user can then accesses this data.

Sensor in the node will have to continuously monitor its surroundings, to collect the appropriate data. And for this monitoring, the power unit will lose its energy level. Once the energy level goes down, the sensor node fails. As the nodes are in the unattended areas, it may not be able to replace the power units. Hence recovery of the sensor node will not be possible.

In brief, reasons for failure of the sensor nodes can be due to: (i) deployment of nodes in unattended and harsh environment. (ii) limited battery power (iii) failure in communication links.

Therefore, it is necessary to detect network failures in advance and to keep the network in reoperation state. This process of finding faults is termed as Fault detection. Fault is generally a defect that may lead to an error. An error represents an incorrect system state which leads to failure. Failure occurs when the system deviates from its specifications and cannot perform its intended functionality.

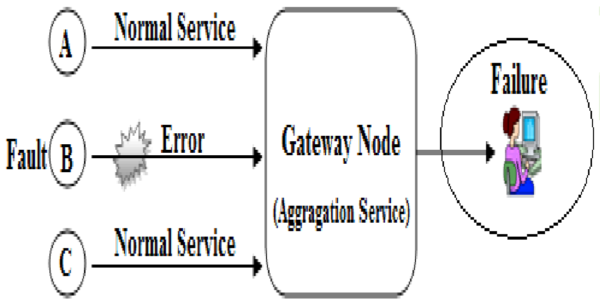

Fig 3: Relationships between Fault, Error and Failure

Figure 3 depicts the basic difference between fault, error, and failure. The principle operation of sensor node A, B and C are reporting periodical sensed data to the gateway node (sink node or base station node) which aggregates different generic sensor data for future analysis. Each sensor service is normal until node B suffers a fault. Thus, the immediate occurrence of fault (any) causes an error in performing normal service by node B. Due to the occurrence of fault on node B, it provides an error service to the gateway node. These error services contain inappropriate information to the analysis of entire application/system. The faulty service provided by node B ultimately causes system failure.

The objective of fault detection is to find that the services being provided are functioning properly. These faults may occur at different level as discussed in section 3. If these faults are not treated properly, then the entire system is considered faulty.

The remainder of this paper is organized as follows: section 2 deals with Why is fault tolerance in WSN necessary. Section 3 deals with fault tolerance at different levels of the sensor network. Section 4 deals with fault detection. Section 5 deals with some of the fault tolerance mechanisms.

NECESSITY OF FAULT TOLERANCE IN WSN

Wireless sensor networks impose a number of technical challenges to fault-tolerance. Three major reasons why fault tolerant sensor networks should receive a significant attention is as follows [Ref 2]:

1. Technology and implementation aspects: At least two components of a sensor node, sensors and actuators, will directly interact with the environment and will be subject to a variety of physical, chemical, and biological forces. Therefore, they will have significantly lower intrinsic reliability than integrated circuits in fully enclosed packaging. In addition, wireless sensor nodes themselves are exceptionally complex systems where a variety of components interact in a complex way. Furthermore, hundreds or maybe thousands of these nodes will form a

distributed embedded network system that will handle a variety of sensing, actuating, communicating, signal processing, computation, and communication tasks. Wireless sensor networks will be often deployed as consumer electronic devices that will put significant constraints on the cost and therefore, quality of used components. More importantly, nodes operate under strict energy constraints that will make energy very limited to testing and fault tolerance.

2. Applications will be equally as complex as the involved technology and architectures: More importantly, sensor networks will often operate in an autonomous mode. Furthermore, security and privacy concerns will often prevent extensive testing procedures. Note that not just testing and fault tolerance will be adversely impacted, but also related tasks such as debugging, where reproduction of specific conditions under which fault has occurred will be difficult. Also, in most of the applications sensor nodes are deployed in uncontrolled and sometimes even hostile environments.

3. Wireless sensors networks are well known and are more easily installed and used, but still a lot of research work has to be carried out to address the problems of fault tolerance and detection. In this situation, it is also difficult to accurately predict the best way to treat fault tolerance within a particular wireless sensor network approach. In addition, technology and protocols and applications for wireless sensor networks are changing at a rapid pace. For example, if we consider power consumption, each particular scheme will depend significantly on the relative power consumption of different approaches. Specifically, if communication energy is significantly higher than the computation energy, then it is important to develop localized algorithms that will require only a limited amount of communication. As another example , if a sensor node present in the routing path fails, the sender node will have to set a new path with available information. Therefore, with respect to fault tolerance, it is important to consider schemes that conduct error detection using only local information. Or, if one wants to ensure fault tolerance during the sensor fusion, the goal is to design fault tolerant techniques that do not significantly increase the communication overhead. On the other hand if the computation energy is significantly higher than the communication requirements, it is a good idea to support communication resources at one node with the computation resources at other nodes. It is preferable to develop fault tolerant sensor fusion approaches that require little additional computation regardless of any additional communication requirements.

FAULT TOLERANCE AT DIFFERENT LEVELS OF THE SESOR NETWORK

The study in [Ref 2] gives five different levels of fault tolerance required in sensor network.

Physical layer

The Physical layer is responsible for establishing communication in a given medium between two nodes. Functions at physical layer are modulation-demodulation and encoding-decoding by using different techniques. These techniques are selected based on the requirement of maximizing the energy efficiency and minimizing the cost and size of the sensor node. A software radio is a wireless communication device in which parts or all of the physical layer functions are realized in software.

The hardware and software radios will be deployed with the capability to solve interoperability problems and to enhance performances in noisy media, and they must be suited for realization of variety of fault tolerance techniques at the physical layer. For example if some components of the software radio are not functional, one can switch to modulation and encoding schemes that can be realized with still operational hardware resources.

Hardware

At hardware level, different components are considered:

(i) Computational subsystem: The components like microprocessors, DSP processors and controllers are very reliable with a very low rate of malfunctioning and are also incorporated with sophisticated fault tolerance techniques.

(ii) Storage components: Here volatile memories like SRAM and DRAM are used for short term storage. Non-volatile memories such as flash are used for storage of system programs. Memories are designed using the standard semiconductor processes. Hence the storage systems are generally fault resilient and it rarely undergoes faulty problems.

(iii) Energy supply: Fuel cells and energy scavenging subsystems are used. For energy distribution, the standard solution to enhance fault tolerance is to deploy multiple distribution networks.

(iv) Wireless radio: fault tolerance can be enhanced here, by using aggressive error correction schemes and retransmission. Or using two or more radios. The primary goal of these solutions is to save energy and to enhance fault tolerance.

System software

System software consists of operating system and utility programs. There are many ways to address fault tolerance at the system level with respect to the computational subsystem. The main subsystem where the fault tolerance is to be realized is at the system software level is the communication unit. For example, rerouting messages using different paths in multihop network. As another example, the message may have to be broadcasted on multiple channels, in order to go for fault tolerance, so that, if one node in a path fails, another path can be selected as an alternative. But there is always trade-off between complexity and effectiveness of communication protocols.

Middleware

Middleware level deals with data aggregation, data filtering and sensor fusion. It deals with whether there is interoperability of data handling between the nodes. Interoperability is one of the important aspects in wireless sensor networks to achieve high throughput. It also deals with, how many sensors of each type should be placed on a particular network and on which position.

Application

Addressing fault tolerance at the application level may be very efficient, but requires customized way to properly address the issue. Application level fault tolerance can be used to address faults in essentially any type of resources.

FAULT DETECTION

Fault detection is the first phase of fault management, where an unexpected failure should be properly identified by network system. Existing failure detection approaches in WSNs can be classified into two types [Ref 3]: Centralized approach and Distributed approach.

Centralized approach

Here a logically centralized sensor node [Base station or Sink node] identifies and localizes the cause of failure or suspicious nodes in WSNs. The central node normally adopts an active detection model to retrieve states of the network performance and individual sensor nodes by periodically injecting requests or queries into the network. It analyses this information to identify and localize the failed or suspicious nodes. Also the centralized sensor node will have to maintain its back up node, so as to replace itself, if it finds itself to be in the suspicious mode. That is, it also has to monitor itself. Centralized approach is efficient and accurate to identify the network faults in certain ways.

Distributed approach

Distributed approach encourages the concept of local decision-making , which evenly distributes fault management into the network. Each node have to make certain levels of decision before communicating with central node. Central node will not be informed unless there is really a fault occurred in the network. Also several fusion nodes across the network work together to make the final decisions on suspicious nodes in the network.

FAULT TOLERANCE MECHANISMS

As in the study of my previous paper [Ref 4] integration of protocol layers has been implemented. One of the important applications of WSN is event detection and reporting. These applications exhibit prolonged periods of inactivity till the time an event of interest is detected. For such applications, integration of protocol layers to reduce the protocol overhead, and to make the protocol stack lightweight can be applied. In this paper, a buffer based MAC cum routing in wireless sensor networks is developed. Here, amongst all the nodes which have detected the events, a node with maximum occupied buffer is given chance to access the medium, and routing is carried through greedy algorithm. But if the fault occurs at any node due to reduced energy, then the buffered information will be lost. In order to gain fault tolerance for this protocol, self diagnosis at each node level can be applied, such that, each node has to keep a watch on its energy levels. If the energy level at a node goes below the threshold energy level, it has to declare itself in inactive mode and pass the buffer content to next appropriate note in its neighborhood.

The fault tolerance mechanism discussed in [Ref 5] puts forward a FTRSDDB (Fault-Tolerant Routing based on Structural Directional De Brujin) Algorithm for wireless Sensor networks to enhance the performance of fault tolerant routing in WSN. The algorithm deploys some super nodes with abundant energy and powerful performance in WSN. These nodes are responsible for the collection of topology information from the WSN to build redundant routing table, and provide data forwarding and routing update service for popular nodes. The FTRSDDB algorithm optimizes network topology structure using de Brujin graph and can quickly find neighbor nodes failure and invalid routing path, and then calculate new routing information with low cost, which improves the performance of fault-tolerant routing of WSN.

In [Ref 6] LIFT –Layer Independent Fault Tolerance mechanism for WSN aims at reducing message loss avoidance along prone-to-failure paths that monitor reports, which would follow from sensors to sink stations. It proposes an original layer independent scheme. This mechanism creates fake data sources that act as storage nodes during the failure of links leading to the sink station. Few control messages will be required during gradual recovery phase, and hence maintains a negligible overhead in terms of message complexity and also results in improved data delivery ratio.

In [Ref 7] Energy efficiency of a system is measured based on the energy dissipated by the system in its lifetime plus the data loss rate. This fault tolerance mechanism deals with Informer Homed Routing [IHR] protocol which is more energy efficient than Low Energy Adaptive Clustering Hierarchy (LEACH). In IHR mechanism, Node Cluster Heads [NCH] send data to Primary Cluster Heads [PCH] but not to Backup Cluster Heads [BCH] in regular run time. In every round of data transmission, BCHs check the aliveness of PCHs using beacon messages. After three rounds, if BCHs cannot receive any acknowledgment from PCHs they declare that PCHs have failed. BCHs also inform NCHs to transmit data to BCHs instead of PCHs from now. IHR decreases the cost of energy and also improves network throughput and lifetime with better data loss rate. The communication overhead is lesser than the energy consumed in data communication, as the size of beacon packet is smaller than data packet size.

Fault Tolerance Mechanism for efficient Cluster Based Power Saving scheme [Ref 8] deals with algorithm which assumes that the base station receives the information of location and residual energy for each sensor node and the average residual energy can be calculated. When the residual energy of sensor node is higher than the average residual energy, the sensor node becomes a candidate of cluster head. In case of failure of primary cluster head, back up cluster head will take the place of primary cluster head automatically.

A Self healing system [Ref 9] is one of the fault tolerant computing systems. Self healing is defined as the property which enables a system to understand that it is not working properly and makes necessary adjustments to restore itself to normalcy. For example: if a node in the network fails a back up sleeping node can be awaked to cover the required cell or mobile nodes can be moved to fill the coverage hole. And if the base station fails, a secondary cell can be assigned as the base station. Self Healing systems try to heal themselves from observed faults. They are more concerned about post fault or post attack states.

CONCLUSION

Due to the deployment of sensor nodes in harsh and uncontrolled environments, and also due to the complex architectures, WSNs will be prone to different kinds of failures and malfunctioning. Intention in this paper was to identify the different fault occurring levels in WSN, and to study some fault detection and tolerance mechanisms in WSN. This work provides a concise survey and classification in this area. Through the ideas proposed it is possible to compare the different solutions identifying the strong and weak points of each of them. This allows for a correct selection of the techniques that are more suitable to specific applications.

FUTURE SCOPE

A major problem in WSN, is where the data collected by the sensor may not reach the sink or base station correctly. One of the reasons may be due to jamming of information. As in my paper [Ref 4] Buffer based MAC cum Routing protocol was considered in order to avoid jamming of data, but if the intermediate nodes in the path of route fails, a fault tolerant protocol will have to be applied. Hence, as an extended work, a Multichannel and Multicarrier system in which an idea of transmitting the same information over multiple channels, signal diversity will be provided, with which the base station can exploit to recover information can be implemented. Also another form of multichannel communications is multiple carrier transmission, where the frequency band of the channel is subdivided into a number of sub channels and information is transmitted on each of the sub channels. This idea will have to be implemented at the hardware level (wireless radio), system software level of fault tolerance of the sensor network.

Most of the present research works have not worked on Multichannel and Multicarrier idea related to fault tolerance in wireless sensor networks, and hence, this new idea can be thought of.

REFERENCES

[1]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002

[2]. Farinaz Koushanfar1, Miodrag Potkonjak, Alberto Sangiovanni-Vincentelli , "Fault tolerance in wireless sensor Networks".

[3]. Er. Saurabh, Dr. Rinkle Rani Aggarwal, "A Review of Fault Detection Techniques for Wireless Sensor Networks" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013

[4]. S. S. Manvi , V. Sadlapur, "Buffer based Media Access cum Routing Protocol in WSNs," IEEE Region 10, TENCON 2008.

[5]. Chaganti B. N. Lakshmi, Dr. S. K. Mohan Rao A "Review on Fault Detection and Tolerance in Wireless Sensor Networks" International Journal of Electronics Communication and Computer Engineering. Volume 6, Issue (5) Sept., NCRTCST-2015, ISSN 2249–071X

[6]. Chuiwei Lu, Defa Hu " A Fault-Tolerant Routing Algorithm for Wireless Sensor Networks Based on the Structured Directional de Bruijn Graph" cybernetics and information technologies Volume 16.

[7]. Antoine Gallais, Thomas Noël, "LIFT: Layer Independent Fault Tolerance Mechanism for Wireless Sensor Networks" https://www.researchgate.net/publication/221638558

[8]. Charney Jeevanandam, K. Ramalakshmi, Deva Priya I. " A Survey on Energy Efficient Fault Tolerance Mechanisms in Wireless Sensor Networks". International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 1, January 2014)

[9]. Navmeet Kaur1, Kamaljit Kaur2 Fault Tolerance Mechanism using Clustering for Power Saving in Wireless Sensor Networks *International Journal of* Engineering Trends and Technology (IJETT) – Volume 4 Issue 8- August 2013