International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Fault Tolerance in Wireless Sensor Network

Manasvi Mannan†* and Shashi B. Rana†

†Department of Electronics and Communication Engineering, Guru Nanak Dev University Regional Centre Gurdaspur, Punjab, India

Accepted 24 May 2015, Available online 26 May 2015, **Vol.5, No.3 (June 2015)**

Abstract

As the wireless sensor network emerges as a revolution in all aspects of our life like health monitoring, wildlife monitoring, search and rescue, so it is desirable to have a reliable routing protocol for dealing with the routing issues of mobile sensor nodes. There exist a problem of battery which is also the main constraint for sensor nodes so routing protocol should be energy efficient. Also, fault tolerance is one of the most significant of many challenges in these networks. So in this study, the fault tolerant at different levels has been discussed and the solution to this problem achieve fault tolerance of cluster heads while routing and mobility management of mobile sensor nodes to reduce packet loss during data transmission in MWSN.

Keywords: *Wireless sensor network (WSN); fault tolerance; cluster head; fault tolerant systems; fault Diagnosis*

1. Introduction

One of the most important technologies for the twenty-first century is wireless sensor networks (WSN).It has received tremendous attention from both academic and industry all over the world in the past decades. A WSN typically consists of a large number of low-cost, low-power, small size and multifunctional wireless sensor nodes, with sensing, gathering and computation capabilities. These sensor nodes can be communicated over a short distance via a wireless medium and collaborate to complete a common task, for example, environment monitoring, health monitoring, military surveillance, and industrial process control. The deployment of sensor nodes is performed in an ad hoc fashion without careful planning and engineering in various WSN applications. If theses sensor nodes are once deployed, then they must be able to autonomously organize themselves into a wireless communication network. The nodes of WSN are battery-powered and operate without attendance for a relatively long period of time. In many cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes. WSNs are characterized with denser levels of sensor node deployment, server power higher unreliability of sensor nodes, computation, and memory constraints. Thus, these unique characteristics and constraints provides many new challenges for the development and application of WSNs. Due to the various energy constraints of large number of densely deployed sensor nodes, they need a suite of network protocols to implement various network control and management functions such as synchronization, network security and node localization. The traditional routing protocols have several shortcomings when applied to WSNs, which are mainly due to the energy-constrained nature of such networks. For example, flooding is a technique in which a given node broadcasts data and control packets that it has received to the rest of the nodes in the network. This process repeats until the destination node is reached.

Note that this technique does not consider the energy constraint imposed by WSNs. The result show that when used for data routing in WSNs, the problems such as implosion and overlap can occur. It is given that flooding is a blind method & there is a circulation of duplicated packets in the network, and hence these duplicated packets will be received by sensors, causing an implosion problem. Also, when same region is sensed by the two sensors and their sensed data is broadcasted at the same time, then the neighbors will receive the duplicated packets. The shortcomings of flooding can be countered by another technique called gossiping can be applied. In the technique gossiping, when a packet is received, a sensor would select one of it neighbors randomly and send the packet to neighbor. This process continues until all sensors receive this packet. A given sensor node would receive only one copy of a packet being sent, by using this technique. During the tackling of the implosion problem, there is a significant delay for a packet to reach all sensors in a network. Moreover, these inconveniences gets focused when the number of nodes in the network gets increased, figure 1 show the typical wireless sensor network.

*Corresponding author: **Manasvi Mannan**

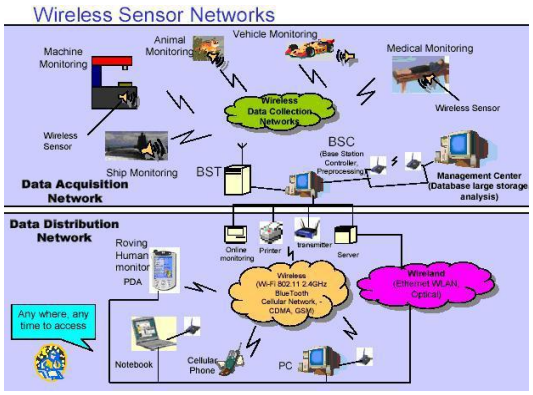

Fig. 1 Wireless sensor network.

2. Communication in Wireless Sensor Network

In this technology, further developments have led to integration of sensors, radio communications and digital electronics into a single integrated circuit (IC) package. Wireless sensor network have a base station that communicates via radio connection to other neighboring sensor nodes. The required data then collected at sensor node is being processed, compressed and sent to sink node either directly or through other sensor nodes. The sensor nodes are deployed in a sensor field as shown in Fig. 1. These scattered sensor nodes has the capability to gather data and route data back to the sink. Data can be routed back to the sink via a multihop infrastructure less architecture through the sink. The sink may communicate with the task manager user via Internet or satellite as shown in Fig. 2.

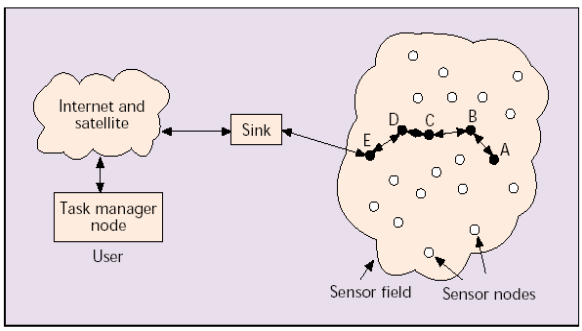

Fig. 2 Wireless sensor nodes scattered in a sensor field

3. Fault Tolerance

Fault tolerance technique prevents lower level errors from propagating into system failures. By the use of various types of structural and informational redundancy, such techniques either form a fault or detect a fault and then effects a recovery process which, if successful, prevents a system failure. If not, then there is a permanent internal fault, and the recovery process then usually includes some form of structural reconfiguration that prevents the fault from causing further errors. The mixture of fault tolerance techniques that complement the techniques used for fault prevention will be incorporated by fault tolerance system designs. Fault tolerance techniques are LEACH, HEED, DFCA and etc. Due to lack of power, physical damage, or environmental interference, some sensor nodes may fail or can be blocked in WSNs. The overall task of the sensor network should not be affected by the failure of sensor nodes. Fault tolerance is the ability of a system to continue providing its specified service despite of its component failures. It is carried out through fault detection and fault recovery process. Since the sensor nodes are prone to failure, WSNs must offer features such as: availability, reliability and fault-tolerance ability, security etc.

3.1 Source of Faults in Real WSN Applications

Wireless sensor networks are commonly spread wide in harsh environment and are subject to faults in several layers of the system. Fig. 3 presents a layered classification of components in a WSN that can suffer faults. A fault that causes in each layer of the system has the possibility to propagate to above levels. For instance, the entire node will be failed if any power failure of a node occurs. If this node relies on a routing path, then the messages of other nodes that are relying on the same routing path will not be delivered making an entire region of the network silent till the routing path is restored.

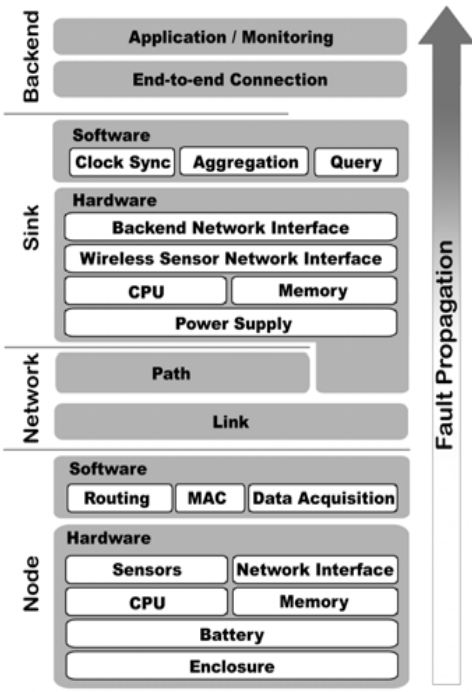

Fig.3 Fault classification and propagation

In this paper, we will concentrate on faults that can occur in the sensor nodes up to the sink.

1) Node Faults: Nodes have various hardware and software components which can produce malfunctions. The sensor nodes were exposed to direct contact with

water causing short circuits due to stress from the environment and inadequate enclosures. The observer reported that the large-scale deployment in a potatoes field indicated that the antennas from the nodes were quite brittle and would become loose while inserting the node into the packaging.

2) Link Faults: Communication links between nodes are highly volatile in WSNs. There are constant changes in the routing paths due to instability of the links between nodes. Link between nodes will become faulty, when radio interference occurs. For Example, in agricultural fields the deployment of the nodes must be carefully planned to take into consideration that when plants start growing the link range between nodes is considerably reduced.

3) Sink Faults: On a higher level of the network, a device (sink) that collects all the data generated in the network and propagates it to the back-end system causes faults of its components. The sink can be deployed in areas where no permanent power supply is present, in such applications batteries together with solar cells are commonly applied to provide the amount of energy necessary. However, this traditional technique has proven to be inefficient. Although this worked perfectly for other experiments, in the glacial environment the sink suffered a power failure due to snow covering the solar cells for several days.

3.2 Fault Tolerance at Different Levels

Five levels of fault tolerance are physical layer, hardware layer, system software layer, middleware layer, and application layer. On the basis of study, we classify fault tolerance in WSNs into four levels from the system point of view. More specifically, fault tolerance in a WSN system may exist at hardware layer, software layer, network communication layer, and application layer.

Hardware Layer

Faults at hardware layer can be caused by malfunction of any hardware component of a sensor node, such as memory, battery, microprocessor, sensing unit, and network interface (wireless radio).

Software Layer

Software of a sensor node consists of two components: system software, such as operating system, and middleware, such as communication, routing, and aggregation. Software bugs are a common source of errors in WSNs.

Network Communication Layer

Faults at network communication layer are the faults on wireless communication links. Link faults can be caused by surrounding environments or by radio interference of sensor nodes.

Application Layer

Fault tolerance can be addressed also at the Application layer. For example, finding multiple node-disjoint paths provides fault tolerance in routing. The system can switch from an unavailable path with broken links to an available candidate path.

3.3 The Need for Fault Tolerant Protocols and Design Issues

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). Fault tolerant techniques for distributed systems include tools that have become industry standard such as SNMP and TCP/IP, as well as more specialized and/or more efficient methods that have been extensively researched. The faults in sensor networks cannot be approached in the same way as in traditional wired or wireless networks due to the following reasons:

a) traditional network protocols are generally not concerned with energy consumption, since wired networks are constantly powered and wireless ad hoc devices can get recharged regularly;

b) traditional network protocols aim to achieve point-to-point reliability, whereas wireless sensor networks are concerned with reliable event detection; in sensor networks, node failures occur much more frequently than in wired, where servers, routers and client machines are assumed to operate normally most of the time; this implies that closer monitoring of node health without incurring significant overhead is needed;

d) traditional wireless network protocols rely on functional MAC layer protocols that avoid packet collisions, hidden terminal problem and channel errors by using physical carrier sense (RTS/CTS) and virtual carrier sense (monitoring the channel). Many of the recent fault detection algorithms have either vaguely defined fault models or an overly general fault definition. Looking beyond fault detection and correction techniques, there has been relevant work that frames our thrust to provide fault taxonomy.

4. Taxonomy of Fault Tolerant Techniques

Recent research has developed several techniques that deal with different types of faults at different layers of the network stack. To assist in understanding the assumptions, focus, and intuitions behind the design and development of these techniques, the taxonomy of different fault tolerant techniques used in traditional distributed systems was given as:

a) Fault prevention: this is to avoid or prevent faults;

b) Fault detection: this is to use different metrics to collect symptoms of possible faults;

c) Fault isolation: this is to correlate different types of fault indications (alarms) received from the network, and propose various fault hypotheses;

d) Fault identification: this is to test each of the proposed hypotheses in order to precisely localize and identify faults;

e) Fault recovery: this is to treat faults, i.e. reverse their adverse effects.

Fault identification and isolation, sometimes are collectively referred to as fault diagnosis. Note that there do exist some techniques that address a combination of all these aspects. In fact, these techniques operate at different layers of the network protocol stack. Most fault avoidance techniques operate in the network layer, adding redundancy in routing paths; a majority of fault detection and recovery techniques operate at the transport layer; and a few fault recovery techniques perform at the application layer, concealing faults during online data processing.

Conclusion

Wireless sensor networks are easily prone to a variety of malfunctioning. So, our goal in this paper was to identify the most important types of faults, techniques for their detection and diagnosis, and to summarize the first techniques for ensuring efficiency of fault resiliency mechanisms. In addition to a comprehensive overview of fault tolerance techniques in general, and in particular in sensor networks, we discussed techniques that ensure fault resiliency during sensor fusion as well as the approach for heterogeneous built-in-self-repair fault tolerance. We concluded by outlining the potential future research directions along several dimensions.

References

Ian F. Akyildiz, Ismail H. Kasimoglu,(2004) Wireless sensor and actor networks research challenges, Elsevier Ad Hoc Networks2, pp. 351–367

Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, (2008) Wireless sensor network survey, Elsevier Computer Networks 52, pp. 2292–2330

L. Paradis and Q. Han, (2007) A survey of fault management in wireless sensor networks, Journal of Network System Management, pp. 171-190

A. Mahmood, E. J. Mccluskey, (1988) Concurrent Error Detection Using Watchdog Processors, IEEE Transactions on computers, pp.160-174

F. Koushanfar, M. Potkonjak, and A. Angiovanni-Vincentell, (2002) Fault tolerance techniques for wireless ad hoc sensor networks, Sensors 2002, Proceedings of IEEE, pp. 1491-1496

Rana Ejaz Ahmed, and Abdul Khaliq,(2004) On the Role of Base Station in Fault- Tolerant Mobile Networks, Electrical and Computer Engineering, Canadian Conference 2004, pp. 473-476

Ivan Stojmenovic and Stephan Olariu, (2005) Data-centric protocols for wireless sensor networks. In Handbook of Sensor Networks, Chapter 13, pages 417–456

A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler,(2002) Spins: security protocols for sensor networks, Wireless Networks, pp. 521-534

Y. Sankarasubramaniam, O. B. Akan, and I. F. Akyildiz, (2003) Esrt: event-to-sink reliable transport in wireless sensor networks, in MobiHoc '03: Proceedings of the 4th ACM International symposium on Mobile ad hoc networking & computing, pp. 177-188,

Karim, L., Nasser, N., Salti, (2010) T.E.: ‗Relma: a range free localization approach using mobile anchor node for wireless sensor networks'. IEEE Globecom 2010, Miami, Fl, 6–10

Tang, F., Guo, M., Li, M., Wang, Z., Cheng, (2008) Z.: ‗Scalable and secure routing for large-scale sensor networks,'. IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing, EUC '08, 2008, vol. 2, pp. 300–305

Cho, J., Choe, J, (2008) A cluster-based routing protocol for supporting mobile sinks in sensor network. Int. Conf. on Information Networking, ICOIN 2008, pp. 1–5

Karim, L., Nasser, N (2011) Energy efficient and fault tolerant clustering protocol for mobile sensor network. IEEE Int. Communications Conf. (ICC'11), Kyoto, Japan, 5–9

S. Misra et al. (eds.), (2009) Guide to Wireless Sensor Networks, Computer Communications and Networks, DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited

Jun Zheng and Abbas Jamalipour,(2009) Wireless Sensor Networks: A Networking Perspective, a book published by A John & Sons, Inc, and IEEE

Monica R Mundada , Pallavi B. Kamble Dept of Computer Science ,T Bhuvaneswari,(2013) Cluster Head Location based Base Station Mobility in Wireless Sensor Networ ,International Journal of Computer Applications (0975 – 8887) Volume 67– No.17

Sunkara Vinodh Kumar and Ajit Pal,(2013) Assisted-Leach (A-Leach) Energy Efficient Routing Protocol for Wireless Sensor Networks International Journal of Computer and Communication Engineering, Vol. 2, No. 4