www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13216-13220

WSN Based Cluster Head Fault Tolerance Mechanism

J.Rajprabaharan

Assistant Professor, Department of E & I, RVS College of Engineering and Technology, Tamilnadu, India,
prabu1303@gmail.com

Abstract

Sensors in a wireless sensor network (WSN) are prone to failure, due to the energy depletion, hardware failures, etc. Fault tolerance is one of the critical issues in WSNs. The existing fault tolerance mechanisms either consume significant extra energy to detect and recover from the failures or need to use additional hardware and software resource. In this paper, we propose a novel energy-aware fault tolerance mechanism for WSN, called Informer Homed Routing (IHR). In our IHR, non cluster head (NCH) nodes select a limited number of targets in the data transmission. Therefore it consumes less energy. In this paper, we propose an agreement-based fault detection and recovery protocol for cluster head (CH) in wireless sensor networks (WSNs). The aim of protocol is to accurately detect CH failure to avoid unnecessary energy consumption caused by a mistaken detection process. Our experimental results show that our proposed protocol can significantly reduce energy consumption, compared to two existing protocols: Low-Energy Adaptive Clustering Hierarchy (LEACH) and Dual Homed Routing (DHR).

Index Terms – Wire less Sensor Network,Fault Detection,Cluster Head.

1.INTRODUCTION

A wireless sensor network (WSN) consists of a large number of sensor nodes that collect meaningful environmental information and send them to a central repository. The evolution of communication technologies has motivated applications of WSNs and the development of wireless communications. Embedded system technologies make it possible to develop low-cost, low-power, and small-sized wireless sensor nodes. WSNs have infiltrated every aspect of our daily life, such as home automation monitoring, medical monitoring, vehicle anti-theft monitoring, weather monitoring, building structures monitoring, and industrial plant monitoring . Since WSNs become more and more popular, the quality of ser-vice provided by a WSN in the aspects of information integrity, data correctness and transmission in a timely manner have drawn more and more attention to researchers and system designers. However, nodes in WSNs are prone to failure due to the energy depletion, hardware failure, communication link errors, malicious attacks, etc. Therefore, fault tolerance is one of the most critical is-sues in WSNs. Fault tolerance is the ability of a system to deliver a desired level of functionality in the presence of faults. Many fault tolerant mechanisms have been proposed and studied. How-ever, these mechanisms either consume lots of extra energy to detect and recover failures or even need additional hardware and software resources.

In this paper, we design a fault tolerance mechanism for WSNs called Informer Homed Routing (IHR). This algorithm advances the existing fault tolerance mechanism, such as the Dual Homed Routing (DHR) mechanism in the aspect that it reduces energy consumption, prolongs the lifetime of a WSN, and transmits more information in the situation when node faults happen. In our algorithm, instead of sending data information to the primary cluster head and making backup of cluster head simultaneously, the collector node only sends data when it founds the primary cluster head fails. This feature of IHR leads to less energy consumption compared to the DHR. In addition, it can still transmit information when cluster head faults happen.

2. RELATED WORKS

In this section, we present the related work of fault tolerance mechanism in WSN and discuss advantages and disadvantages of different WSN fault tolerance protocols. We also introduce the existing simulation tool. For the ease of reading, we list the abbre- viations in Table 1.

There have been studies on fault tolerance in wireless sensor networks [17,18]. Most of current fault tolerance protocols intro- duce redundancy. For example, one of the techniques to tolerate wireless link failure is retransmission, which introduces extra traf- fic in the network and causes extra energy consumption. Receivers need to confirm the receipt of messages, which require extra en- ergy compared to the scheme without retransmission is not re- quired. when the number of retransmissions is large, the delay is significant and causes out-of-date information and meaningfulness lose.

A typical example is the fault tolerance mechanism used in Zig- bee standard [19]. The IEEE 802.15.4/ Zigbee standard is a

low-cost, low-power, wireless sensor networking stack that has been consid- ered as a promising technology for WSNs. First, the low cost allows the technology to be widely deployed in wireless control and mon- itoring applications. Second, the low power-usage promises longer life with smaller batteries. However, the Zigbee protocol currently lacks of efficient fault tolerance mechanisms to support reliability for real-time applications.

IEEE 802.15.4/ Zigbee supports a native fault-tolerance mecha- nism called as the orphaned device realignment.This recovery/repair procedure is activated when there are repeated communication failures in the request for data transmission.

Name	Meaning
LEACH	Low- Energy Adaptive Clustering Hierarchy
DHR	Dual Homed Routing
IHR	Informer Homed Routing
CH	Cluster Head
PCH	Primary Cluster Head
BCH	Backup Cluster Head
BS	Base station
AFDEP	Agreement Based CH Failure Detection and Election Protocol

3. MODEL AND BACKGROUND

3.1 NETWORK TOPOLOGY MODEL

The network topology model used in our simulation tool can be depicted in Fig. 1. The network has only one sink node. Without lost of generality, we refer it as BS in the rest of the paper. This sen- sor network has N sensor nodes uniformly deployed over a square area. Cluster heads (CHs) are selected with a defined probability, which equals the ratio of the expected number of CHs to N. CHs not only forward data, but also sense the environmental informa- tion and aggregate their own data with the information collected from their children. Other sensor nodes can be associated with CHs. These sensor nodes are called as Non Cluster Heads (NCH). NCHs can communicate with BS through single or multi-hops rout- ing. Bi-directional symmetrical links are assumed. The maximum number of hops in this network topology model is two.

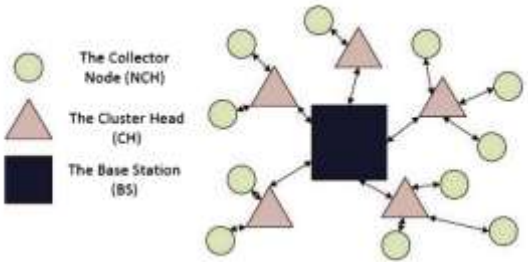

Figure1:Network Topology Model

3.2 Energy Model

The energy dissipation $E_T(k , d)$ of transmitting k-bit data between two nodes separated by a distance of d meters is given as follows:

ET (k,d) = {k(Eelec + εFS * d^2) (d< d0)}

ET (k,d) = {k(Eelec + εMP * d^4) (d >d0)}

Where $d_0 = \sqrt{\varepsilon_{FS}/\varepsilon_{MP}}$, E_{elec} denotes electronic energy, ε_{FS} and ε_{MP} denote transmit amplifier parameters corresponding to the free-space and the two-ray models. The energy dissipation of the receiver is

ER(k) = k * Eelec

Also, the energy dissipation of fusing k-bits data is

EF(k) = k * Edf

Where Edf is the energy dissipation of fusing one bit data.The parameters used in this paper are given below : Edf = 5nJ/bit,εFS = 10 pJ/bit/m^2, Eelec = 50 nJ/ bit, εMP = 0.004 pJ/bit/m^4 and dtoBS > d0.

3.3 Fault Model

In order to evaluate whether a mechanism used for a WSN is fault tolerant or not, we need to observe how the network reacts when faults happen. The existing tools do not support any fault injection to a network. The only reason a fault happens in the existing tools is battery depletion. However, there are several other reasons that cause a WSN fails. There are different ways to classify these faults into different categories based on different criteria. According to the layer in the network architecture where the fault happens, the faults could be divided into hardware layer faults,software layer faults, network communication layer faults, andapplication layer faults. According to the time the faults last, the faults could be divided into ephemeral faults, intermittent faults, and permanent faults.

In our paper, we tackle hardware faults happen at cluster head. The hardware faults may be caused by battery depletion, hardware deterioration, transmitter failure, malicious human behavior, etc. The impact of this kind of fault is severe, because when a cluster head fails, its children are cut off from the cluster tree, resulting in the loss of communication with the outside. This will significantly reduce the availability of the sensor network.

To evaluate the robustness and behavior of WSN when faults happen, we add a fault model in our simulation tool to inject CH faults into WSN network. The fault generating scheme is as the following:

For every cluster head, if the time arrival of thekth fault is Tk, then the inter-arrival times are defined as follows:

X1 = T1,Xk = Tk – Tk-1 ; for k = 2,3,… (3.3)

We supposeXi is independent, identical distributed random variable, and belongs to the classical exponential distribution with rate parameterλ:

fTi(t) = λ * e ^ (λ * t), t > 0

The inter – arrival time stream, X1, X2, X3,….., actually forms a Poisson process. E(Xi) equals 1/ λ, which is the expected value of Xi. Apparently, the larger the λ, the less frequent the faults happen. To generate the Poisson process, we set the time interval between two consecutive faults at -1/ λ lnx, where x is uniformly distributed over 0 and 1.

4.FAULT TOLERANT MECHANISMS

4.1 Dual CH Mechanism

To design a good fault tolerant mechanism for a WSN, we need to keep low data loss rate, maintain minimum energy cost, while guarantee high throughput and short latency to achieve the goal of prolonging network's lifetime. Based on the above findings, we designed our own Dual CH Mechanism, which is derived from DHR, the sensors will dissipate energy. The DHR

sends data to PCH and BCH at the same time, half of the energy cost is wasted. In our Dual

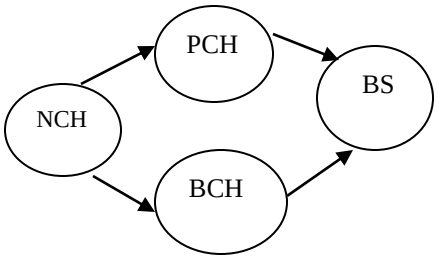

Figure 2: Dual CH Mechanism

CH mechanism, instead of sendingdata to PCH and BCH at the same time, the collector nodes only send data to PCH in the regular runtime. In each data transmission round, the BCH will check the aliveness of PCH based on the beacon message it receives from PCH. After three rounds, if it cannot receive any respond message from PCH, it will declare that the PCH has failed and inform NCHs to transmit data to BCH. In this design, we can achieve at least the same dependability as DHR. While the energy cost decreased, it can improve the network throughput and prolong network lifetime and result in better data loss rate. Because the beacon packet size is much smaller than the data packet size, the communication overhead is much less than the data communication energy consumption in DHR.

4.2 IHR Mechanism:

Characteristics of a good fault tolerant mechanism are reduced data loss rate and energy cost. It must also assure short latency and high throughput to achieve an increased lifetime of WSN. LEACH increases the network's lifetime by initializing different nodes as CHs, but it lacks the functionality to take care of the aliveness of CH. DHR transmits data to both PCH and BCH simultaneously, resulting in twice the expenditure of energy. In IHR mechanism, NCHs send data to PCHs but not to BCH in regular runtime. In every round of data transmission, 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 on. 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. BCHs check the aliveness of PCHs using beacon messages. 4.3 AFDEP Protocol:

Clusters are formed only once during the setup phase before the network starts to run. Initially, some sensor nodes are randomly selected as a CH, because energy of each sensor node is equal in amount. CHs send advertisement messages that contain energy and location information of CHs to neighboring sensor nodes. Each sensor node that listen to this advertisement message responds with a return message comprising its residual energy and location. However, a sensor node may be in the range of multiple

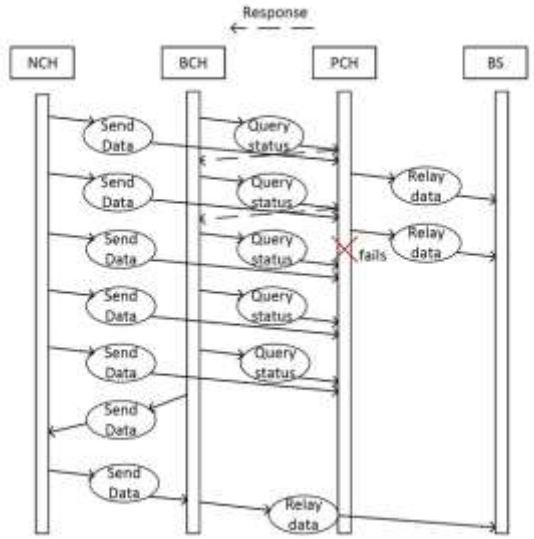

Figure 3:IHR Mechanism

CHs, but finally it must be associated with a single CH. If any sensor node falls within the overlapping region of more than one CHs, it decides its association to a CH by calculating the value of e/d (energy/distance). CH, has maximum e/d value is selected as final CH for that sensor node. If more than one CHs yields same maximum e/d value, then any of them is randomly selected. If a sensor node does not fall within the range of any CH, it declares itself as a CH and gets activated in high power transmission mode.When clusters are established, the CHs collect the data from cluster members, perform local data aggregation and communicate with the BS.

Failure Detection: The detection process runs parallel with normal network operation by periodically performing a distributed detection process at each cluster member. For failure detection mechanism each cluster member maintains a status vector. In status vector each bit corresponds to a cluster member. Initially all bits of are set to zero of status vector on each sensor node. A bit in the vector is set once its corresponding cluster member detects that CH has failed. CH of each cluster periodically sends a hello message (i.e. notification that CH is alive) to cluster members. Cluster member, who does not listen hello message, sets its corresponding bit as one in status vector and locally decides that CH has failed and broadcasts data plus status vector. Other cluster members also listen this message. They extract status vector from message and merge it with own status vector and this process continuous up to the end of the TDMA schedule. At the end of the TDMA frame, cluster members reach on an agreement about failure of CH. If all bits of status vector are set then it is decided that CH has failed.

Failure Recovery. By using agreement protocol when cluster members confirm about CH failure then cluster member who has last slot in TDMA schedule informs to back up node about failure. Back up node elects itself as a CH and sends an advertisement message in high power transmission mode. It keeps on working as CH till its residual energy level reaches a critical limit or it fails. New back up node is required for new CH, so CH start election process for new back up node with sending in low power transmission mode. Back up node election process is similar to election process of CH.

4.4 Simulation Results:

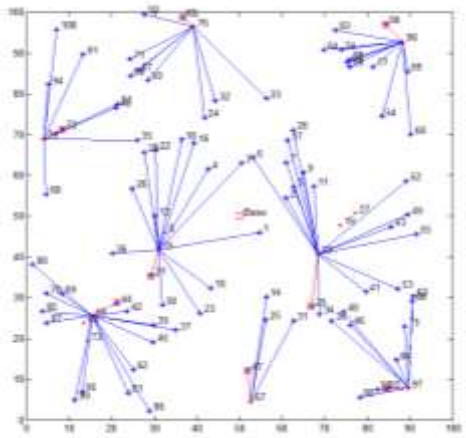

Figure4:BCH Selection When PCH is Dead

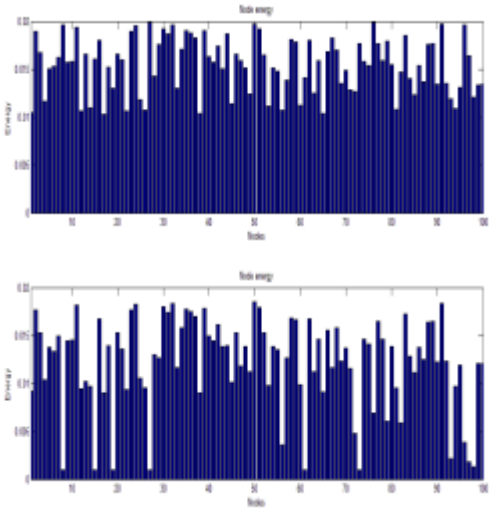

Figure5:Total Amount of Node Energy Vs Node Energy

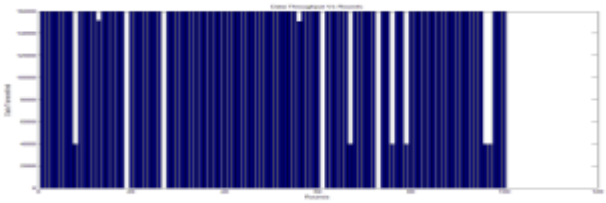

Figure 6:Total Amount Of Data Transmitted

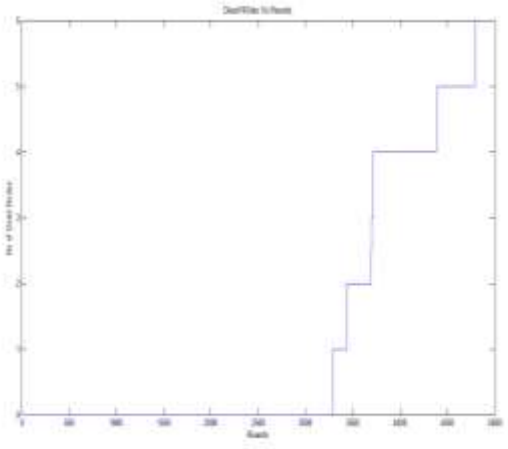

Figure 7:No of Dead Nodes

5.CONCLUSION

Three fault tolerance mechanisms: LEACH, DHR and IHR when tested with a fault injection function, in order to evaluate the robustness of IHR; it has proven to save energy consumption significantly and also has lowered the data loss rate. IHR performs better in the facet of energy dissipation compared to DHR. It also is better in terms of dependability compared to LEACH. The disadvantage of IHR protocol is that it introduces communication overhead. However, avoiding the redundant transmission saves enough energy to compensate the energy consumed in communication overhead. AFDEP periodically checks for CH failure. This detection process runs parallel with network operation. It provides high accuracy, because it allows each cluster member to detect its faulty CH independently. It employs a distributed agreement protocol to reach an agreement on the failure of CH among multiple cluster members. In order to recover from faulty CH, back up node is elected as new CH and new back up node is elected locally. Election of CH and back up node is based on residual energy of sensor nodes. Simulation results show, AFDEP achieves high detection accuracy in harsh environment.

References:

[1] K. Sha, J. Gehlot, and R. Greve, "Multipath routing techniques in wireless sensor networks: A survey," Wireless Personal Commun., vol. 70,no. 2, pp. 807–829, 2013.

[2] M. Asim, H. Mokhtar, and M. Merabti, "A fault management architecture for wireless sensor network," in Proc. IWCMC, Aug. 2008, pp. 1–7.

[3] M. Younis and K. Akkaya, "Strategies and techniques for node placement in wireless sensor networks: A survey," Ad Hoc Netw., vol. 6, no. 4, pp. 621–655, 2008.

[4] P. Jiang, "A new method for node fault detection in wireless sensor networks," Sensors, vol. 9, no. 2, pp. 1282–1294, 2009.

[5] I. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive fault tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks," IEEE Trans.

Dependable Secure Comput.,vol. 8, no. 2, pp. 1–35, Mar./Apr. 2011.

[6] A. A. Boudhir, B. Mohamed, and B. A. Mohamed, "New technique of wireless sensor networks localization based on energy consumption," Int. J. Comput. Appl., vol. 9, no. 12, pp. 25–28, Nov. 2010.

[7] W. Y. Poe and J. B. Schmitt, "Node deployment in large wireless sensor networks: Coverage, energy consumption, and worst-case delay," in Proc. ACM, AINTEC, Nov. 2009, pp. 1–8.

[8] M. Lee and Y. Choi, "Fault detection of wireless sensor networks," Comput. Commun., vol. 31, pp. 3469–3475, Jun. 2008.

[9] A. Akbari, A. Dana, A. Khademzadeh, and N. Beikmahdavi, "Fault detection and recovery in wireless sensor network using clustering,"
IJWMN vol. 3, no. 1, pp. 130–138, Feb. 2011.

[10] C.-C. Song, C.-F. Feng, C.-H. Wang, and D.-C. Liaw, "Simulation and experimental analysis of a ZigBee sensor network with fault detection and reconfiguration mechanism," in Proc. 8th ASCC, May
2011, pp. 659–664.

J.RAJPRABAHARAN received the ME degree from the Electrical Department, Anna University, Chennai, India. He is a Assistant professor at the Faculty of Electronics and Instrumentation Engineering, RVS College of Engineering Dindigul Tamilnadu India. His innovative interests are concentrated in Embedded system, Process control, Digital Electronics, Industrial networks.

[11] A. Mojoodi, M. Mehrani, F. Forootan, and R. Farshidi, "Redundancy effect on fault tolerance in wireless sensor networks," Global J. Comput. Sci. Technol., vol. 11, no. 6, pp. 35-40, Apr. 2011.

[12] S. S. Ahuja, R. Srinivasan, and M. Krunz, "Single-link failure detection in all-optical networks using monitoring cycles and paths,"IEEE/ACM Trans. Netw., vol. 17, no. 4, pp. 1080–1093, Aug. 2009.

[13] R. N. Duche and N. P. Sarwade, "Sensor node failure or malfunctioning detection in wireless sensor network," ACEEE Int. J. Commun., vol. 3,no. 1, pp. 57–61, Mar. 2012.

[14] T. W. Pirinen, J. Yli-Hietanen, P. Pertil, and A. Visa, "Detection and compensation of sensor malfunction in time delay based direction of arrival estimation," IEEE Circuits Syst., vol. 4, no. 1, pp. 872–875, May 2004