Fault Management Using Cluster-Based Protocol in Wireless Sensor Networks

M. Hla Yin and Z. Win

***Abstract*—Fault tolerance has been identified as key challenges in the design and operations of Wireless Sensor Network (WSNs). Failures are inevitable in wireless sensor networks due to inhospitable environment and unattended deployment. Therefore, it is necessary to detect the networks for recovery from the failure to sustain it. WSNs are self-organized using clustering algorithms to conserve energy. LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is one of the significant protocols for routing in WSN. In LEACH, sensor nodes are organized in several small clusters where there are cluster heads in each cluster. These CHs gather data from their local clusters aggregate them & send them to the base station. The proposed scheme is supposed to be an efficient fault detection and recovery mechanism to make the network fault-tolerant and achieve reliability and quality of service. Performance analysis and evaluation will be made using several scenarios of wireless sensor networks.**

***Index Terms*—Fault detection, fault recovery, fault tolerance, LEACH protocol.**

I. Introduction

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed sensors which cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control [1].

The important operations in a Wireless Sensor Network are data dissemination and data gathering. Data dissemination is the process of routing data or queries throughout the network and data gathering is the collection of observed data from individual sensor node to sink. Due to the nature of these networks a sensor node may fail and hence the route between the source to sink may also fail. Hence providing for fault tolerance is an important requirement of this network.

Routing in Wireless Sensor Networks is the process of moving the sensed data from source to sink (destination). A routing protocol should ensure that the WSN can reconfigure be energy efficient and resilient to failures. So far routing in sensor networks has focused upon methods for constructing the best route, or routes, from data source to sink (destination) before sending the data.

Moreover, due to the deployment of WSNs in hostile and un-attended environments faults and failures are normal facts, therefore, fault tolerance and reliable data dissemination is also of great importance. Thus, energy-efficient and fault tolerance have been identified as one of the key challenges in the design and operations of WSNs. To address the above mentioned challenges, we proposed a Fault-Tolerant Management Architecture for WSNs that offers efficient fault detection and recovery mechanisms to make the network fault-tolerant.

Manuscript received January 16, 2013; revised April 21, 2013.

Hla Yin Min is with the Faculty of Information and Communication Technology, University of Technology (Yatanarpon Cyber City), Pyin Oo Lwin, Myanmar (e-mail: hlayinminutycc@gmail.com)

Win Zaw is with the Department of Information Technology, Technological University, Thanlynn, Myanmar (e-mail: winzaw@gmail.com)

II. Related Work

Fault tolerance problem is a very big problem in WSN. Several works has been done on fault tolerance over many clustering algorithms. One fault tolerance approach has been discussed in [2]. Here also the research work is done on LEACH. Here fault recovery is suggested in two ways: inter-cluster recovery & intra cluster recovery.

Another research work on fault tolerance is a Dynamical Jumping Real-time Fault-tolerant Routing Protocol (DMRF) has been proposed [3]. Once node failure, network congestion or void region occurs then the transmission mode will switch to jumping transmission mode leading to reduced transmission delay and guarantees the data packet to be sent to its desired destination within the specified time limit. Each node can dynamically adjust the jumping probabilities to increase the ratio of successful data transmission by using feedback mechanism. This mechanism results in reduced effect of failure nodes, congestion and void region and reduced transmission delay, reduced number of control packets and higher ratio of successful transmission.

One more fault tolerant work is discussed in [4]. Basically, WSNs faces resource limitations, high failure rates and fault caused by wireless channels & wireless sensor nodes. It increases the reliability & robustness of the network by creating a backup path for every node on a main path of data delivery. When a node gets failure it immediately applies its backup path as the main path for data delivery of next incoming packets. This protocol reduces the number of dropped data packets and increases robustness of the entire network by maintaining the continuity of data packet transmission even in presence of faults.

DOI: 10.7763/IJFCC.2014.V3.263

III. Source of Fault in WSNs

Fault is any kind of defect that leads the system to failure, and failure is a situation when the system deviates from its specification and can't deliver its intended functionality [5] categorized faults into three types:

- Permanent faults – These faults are continuous and stable in nature e.g. Hardware faults within a component of a sensor node.
- Intermittent faults – An intermittent fault has an occasional manifestation due to the unstable characteristics of the hardware, or as a consequence of software being in a particular subset of space.
- Transient faults – Transient faults are the result of some temporary environmental impact on otherwise correct hardware, e.g. the impact of cosmic radiation on the sensing enclosure of a sensor node. Faults in WSNs can occur for various reasons. Some of prominent sources of faults mentioned in [6], [7] are:

Node Level Faults: Nodes are fragile; they may fail due to the depletion of batteries, node's hardware/software malfunction and the external impact of harsh environmental conditions (direct contact with water causing short circuit, node crash by tree falling etc).

Network Level Faults: Instability of the link between nodes causing network partitions and dynamic changes in network topology leads to network level faults.

Sink Level Faults: Failure of the sink leads to a massive failure of the network. At the sink level, software, that store and process data are subject to bugs and can lead to loss of data within the period when fault occurs.

Faults caused by adversaries: Since WSNs are often deployed for critical application, attacks by adversaries may cause node faults and consequently, lead the network to failure.

The lack of infrastructure and broadcast nature of wireless medium enable adversaries to intrude into the network, and disrupt the whole functionality (e.g. routing, aggregation etc) of an individual sensor node [8].

IV. Fault Management in WSNs

Fault management is a very important component of network management concerned with detecting, diagnosing, and recovering faults in the network. Proper implementation of fault management can keep the network running at an optimum level and minimize the risk of failure, consequently, make the network more fault tolerant [9]. Important functions of fault management include:

- constant monitoring of system status and usage level
- general diagnostics
- tracing the location of potential and actual failure
- Auto-recovery and self-healing in the event of failure

Fault management in WSNs can be classified according to its network management system architecture [8]: centralized, distributed or hierarchical.

Centralized Architecture: Base station or the central manager has rich and unlimited resources. Therefore, it performs complex management tasks and controls the whole network.

Distributed Architecture: Instead of having a single central controller, distributed architecture employs multiple manager stations throughout the whole network. Each manager controls a sub-region of the network and may communicate directly with other manager stations in a co-operative manner in order to perform management functions.

Hierarchical Architecture: It is a hybrid between centralized and distributed architectures. Sub-controller or managers are distributed throughout the network in a tree shape hierarchical manner, having lower and higher level of hierarchy. These managers are referred as the Intermediate managers, manage a sub-section of a network and perform the management functions, but they don't communicate directly with each other.

A. Problems and Issues

In this section, we highlighted different issues and problems existed in already proposed fault management approaches for WSNs [10]. It is clear from the literature survey that different approaches for fault management in WSNs suffer from the following problems:

- Most existing fault management solutions mainly focus on failure detection, and there is still no comprehensive solution available for fault management in WSNs from the management architecture perspective.
- Different mechanisms proposed for fault recovery [11] are not directly relevant to fault recovery in respect of the network system level management i.e. network connectivity and network coverage area etc.
- Failure recovery approaches are mainly application specific, and mainly focus on small region or individual sensor nodes thereby are not fully scalable.
- Some management frameworks require the external human manager to monitor the network management functionalities.
- Another important factor that needs to be considered is vulnerability to message loss.

We therefore content that there is still a need of a new fault management scheme to address all the problems in existing fault management approaches for wireless sensor networks. We must take into account a wide variety of sensor applications with diverse needs, different sources of faults, and with various network configurations. In addition, it is also important to consider other factors i.e. mobility, scalability and timeliness.

V. Background Theory

Because Low-energy adaptive clustering hierarchy (LEACH) [12] is a clustering based protocol that includes the following features:

- Randomized adaptive self configuring cluster formation.
- Localized control for data transfers.
- Low energy media access and

- Application specific data processing such as data aggregation.

LEACH randomly selects a few sensor nodes as cluster heads (CHs) and rotates this role to evenly distribute the energy load among the sensors in the network. Each iteration of selection of CHs is called a round.

The operation of LEACH is split into two phases: Set up & Steady.

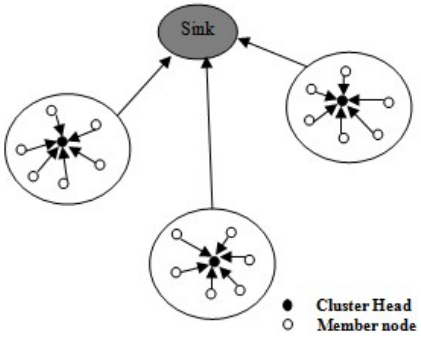

Fig. 1. Leach architecture

During the setup phase, a predetermined fraction of nodes, p, elect themselves as CHs as follows. A sensor node chooses a random number, r, between 0 and 1. If this random number is less than a threshold value, T (n), the node becomes a cluster-head for the current round.

The threshold T (n) is calculated as:

$$T(n) = \frac{P}{1-p(r \bmod (1/p))} \quad if\ n \in G \qquad (1)$$

where P is the desired percentage of nodes which are CHs, r is the current round, and G is the set of nodes that has not been CHs in the past 1/P rounds.

During the steady state phase, data transmission takes place based on TDMA schedule and the CHs perform data aggregation/ fusion through local computation. The BS receives only aggregated data from cluster-heads, leading to energy conservation. After a certain time, the network goes back into the setup phase again and enters another round of selecting new CH. Each cluster communicates using different CDMA codes to reduce interference from nodes belonging to other clusters.

VI. Proposed System

There are four phases in this scheme. They are:

- Advertising Phase
- Data Transmission Phase
- Fault Detection Phase
- Fault Recovery Phase

In the advertising phase, the clusters are organized and CHs are selected. After selection the CHs advertise their selection to all other nodes. All nodes choose their nearest CH after receiving advertisements based on the received signal strength. The CHs then assign a TDMA schedule for their cluster members.

The second phase, data transmission phase, all subordinate nodes can begin sensing and transmitting data to the cluster-head. After receiving all the data, the cluster-head nodes aggregate it before sending it to the Base-Station (BS).

The third phase is the fault detection phase. In hostile environments, unexpected failure of CH may partition the network or degrade application performance; therefore, CH node fault detection is very important. If no response comes from CH to BS or subordinate nodes within a time interval, it flags this CH as a faulty node and disseminates this information to the rest of the network and CH fault recovery process is initiated.

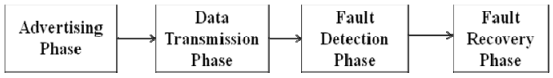

Fig. 2. Block diagram for proposed system

In the final phase, cluster head node fault recovery process starts immediately after a CH fault is detected. When a faulty CH node is identified, all the cluster members associated with it are gradually informed about the CH failure. For the CH recovery operation, the sink node chooses a new CH from the cluster members. This choice is based on each cluster member's sensor nodes residual energy. Therefore a new selected CH node has the highest energy reserves in the cluster. According to this scheme, replace the faulty cluster-head by the next highest energy node in the cluster.

VII. Proposed Algorithm

A. Fault Detection Algorithm

Step 1 Initialize CH1 & CH2 & subordinates
Step 2 IF no response comes within a TDMA slot
THEN
Step 3 Set CH1 as Faulty
Step 4 ELSE
Step 5 For CH2
Step 6 IF no ping message comes periodically
THEN
Step 7 Set CH2 as Faulty

B. Fault Recovery Algorithm

Step 1 Start
Step 2 Initialize CHs & subordinates
Step 3 Compare residual energy of current CH (CH_R) and each subordinate in the cluster.
IF CH_R less than each subordinate, **THEN**
Replace CH_R with next highest energy node.
ELSE
Set CH_R as CH for next setup round.
Step 4 Stop.

VIII. Expected Results

The proposed system enables the network to maintain maximum network connectivity and quality of service under failure conditions. Fault detection and recovery system

provides in case of link or node failure. Both features save energy and prolong the network lifetime. The performance of proposed system can be analyzed using simulation tool. Compare the performance of proposed system with well-known cluster-based routing protocols.

IX. Conclusions And Future Work

Wireless sensor network are composed of many wireless sensing devices called sensor nodes. These nodes are small in size, limited in resources and randomly deployed in harsh environment. Therefore, it is not uncommon for sensor networks to have malfunction behavior, node, and link or network failure. In this paper, we have explained about the problem of network disconnectivity due to cluster head failures in wireless sensor networks and we have tried to find a solution for that.

We have proposed a fault management mechanism for wireless sensor network to diagnose faults and perform appropriate measures to recover sensor network from failures. It maintains the connectivity of the network and the reliability of data transfer even when a node in the network runs out of energy. In future, we plan to extend our proposed design by incorporating the mobility and autonomic fault management aspect in the context of network management system.

Acknowledgment

My Sincere thanks to my supervisor Dr. Win Zaw, Associate Professor, Head of Department of Information Technology, Technological University (Thanlynn), Myanmar for providing me an opportunity to do my research work. I express my thanks to my Institution namely University of Technology (Yatanarpon Cyber City) for providing me with a good environment and facilities like internet books, computers and all that as my source to complete this research. My heart-felt thanks to my family, friends and colleagues who have helped me for the completion of this work.

References

[1] K. Kulothungan, J. A. A. Jothi, and A. Kannan, "An Adaptive Fault Tolerant Routing Protocol with Error Reporting Scheme for Wireless Sensor Networks," *European Journal of Scientific Research*, vol. 16, no. 1, 2011, pp, 19-32.

[2] A. Mojoodi, M. Mehrani, F. Forootan, and R. Farshidi, "Redundancy Effect on Fault Tolerance in Wireless Sensor Networks," By Islamic Azad University.

[3] W. Guowei, L. Chi, X. Feng, Y. Lin, Z. He, and L. Bing, "Dynamical Jumping Real-Time Fault-Tolerant Routing Protocol for Wireless Sensor Networks," University of Technology, China.

[4] A. S. Ben, C. André, K. A. Koubâa1, and M. Alves, " Fault-Tolerance Mechanisms for Zigbee Wireless Sensor Networks," Imam Muhammad Ibn Saud University, Computer Science Dept., 11681 Riyadh, Saudi Arabia.

[5] F. Koushanfar, M. Potkonjak, and A. S. Vincentell, "Fault tolerance techniques for wireless ad hoc sensor networks," in *Proc. of IEEE Sensors*, vol. 2, 2002, pp. 1491-1496.

[6] L. Paradis and Q. Han, "A Survey of Fault Management in Wireless Sensor Networks," *Journal of Network and System Management, Springer Science + Business Media*, LLC, June 2007, vol. 15, pp. 171-190.

[7] M. Ding, D. Chen, K. Xing, and X. Cheng, "Localized fault-tolerant event boundary detection in sensor networks," in *Proc. of 24th Annual Joint Conference of the IEEE Computer and Communications Societies*. vol. 2, 2005, pp. 902-913.

[8] R. Linnyer Beatrys, G. S. Isabela, B. E. O. Leonardo, W. H. Chi, S. N. Marcos, and A. F. L. Antonio, "Fault management in event-driven wireless sensor networks," in *Proc. of the 7th ACM* international *symposium on Modeling, analysis and simulation of wireless and mobile systems Venice, Italy*: ACM, 2004, pp. 149-156.

[9] J. Suhonen, M. Kohvakka, M. Hannikainen, and T. D. Hamalainen, "Embedded Software Architecture for Diagnosing Network and Node Failures in Wireless Sensor Networks," in *Embedded Computer* Systems*: Architectures, Modeling, and Simulation, vol. 5114/2008: Springer Berlin / Heidelberg*, July 18, 2008, pp. 258-267.

[10] M. Asim, H. Mokhtar, and M. Merabti, "A self-managing fault management mechanism for wireless sensor networks," *International Journal of Wireless & Mobile Networks (IJWMN)* vol. 2, no. 4, November 2010.

[11] F. Koushanfar, M. Potkonjak, and A. S. Vincentelli, "Fault tolerance techniques in wireless ad-hoc sensor networks," UC Berkeley technical *reports*, 2002.

[12] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol For Wireless Micro-Sensor Networks," in *Proc. of the 33rd Annual Hawaii International Conf. on System Sciences*, 2000, pp. 3005-3014.

Hla Yin Min is a Ph.D (IT) candidate from University of Technology (Yatanarpon Cyber City). She received master degree in computer technology from University of Computer Studies Mandalay. The field of her thesis is fault management for sensor network using cluster-based routing protocol. She is working as a teacher in Computer University (Pin Lon) and her research interested areas are wireless sensor network, routing protocols and clustering.