IJARESM
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING, SCIENCE & MANAGEMENT

SURVEY ON FAULT TOLERANT MECHANISMS IN WSN

Shalu Mishra[1], Prof.Dhiraj Patel[2], Prof.Pranav Lapsiwala[3]
Post Graduate student, E&C., S.N.P.I.T / GTU, Umrakh/Bardoli, Gujarat, India [1]
Assistant Professor, E&C., S.N.P.I.T. / GTU, Umrakh/Bardoli, Gujarat, India[2]
Assistant Professor, E&C., S.C.E.T. / GTU, Surat, Gujarat, India [3]

Abstract: ***The reliability of wireless sensor networks (WSN) is affected by faults that may occur due to various reasons such as malfunctioning of nodes, software issues, change in location, or environmental hazards. Clustering is an effective topology control and communication protocol in wireless sensor networks but if it is not prepared to deal with faulty situations it may suffer a reduction in overall lifetime. In this paper we present a survey of approaches to fault tolerance and detection techniques in WSNs. We provide taxonomy of faults and classify the surveyed approaches according to their methodology of detecting and recovering from faults.***

Keywords: **Clustering, Cluster Member Based Fault Tolerant Mechanism, Dynamic/Static Clustering Protocol, Fault-Tolerant Dynamic Clustering Protocol**

I. INTRODUCTION

Availability is one of the characteristic of WSN which mainly depends on fault tolerance to keep the system working as expected [2]. In WSN deployments, nodes provide functionality to its neighbors. Multihop routing is an example of such a service, where nodes forward messages on behalf of each other. Also in some cases nodes assume dedicated roles such as cluster head, which implies the responsibility of aggregating sensor data before it is forwarded to a base station, thereby saving energy. Nodes with stronger hardware capabilities can perform operations for other nodes that would either have to spend a significant amount of energy in performing these operations. So if a node fails it will affect working of other nodes in the network. These nodes, however, may fail due to various reasons, including radio interference, de-synchronization, battery exhaustion, or dislocation. Such failures are caused by software and hardware faults, environmental conditions, malicious behavior, or bad timing of a legitimate action.

To provide countermeasures in faulty situations two main actions must be performed:

Fault detection: The first step is to detect that a specific functionality is or will be faulty.

Fault Recovery: After the system has detected a fault, the next step is to prevent or recover from it.

A. Source of faults in real wsn applications

Wireless sensor networks are commonly deployed in harsh environment and are subject to faults in several layers of the system.

1) Node Faults:

Nodes have several hardware and software components that can produce malfunctions. For example, the enclosure can suffer impacts and expose the hardware of the sensor node to the extreme conditions of the environment. Organizing a network in clusters is an approach used in many applications, for example to extend the lifetime of the network. A small number of nodes are selected to become clusterheads. They are responsible for coordinating the nodes in their clusters, for instance by collecting data from them and forwarding it to the base station. If a clusterhead fails, no messages of its cluster will be forwarded to the base station any longer [2].

2) Network Faults:

Routing is one of the fundamental building blocks in a WSN. It is essential for collecting sensor data, distributing software and configuration updates, and for coordination among nodes. Faults on the routing layer can lead to dropped or misguided messages, or unacceptable delays [2].

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 is also subject to faults of its components. When this device fails, unless fault tolerant measurements are present, a massive failure of the network happens because the data from the sensor nodes cannot be accessed. 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 [2].

B. Fault detection techniques

The goal of fault detection is to verify that the services being provided are functioning properly, and in some cases to predict if they will continue to function properly in the near future. The simplest way to perform such a task is through visual observation and manual removal of incorrect values. In this technique human interaction leads to errors, it has a high cost and it is not efficient. Some fault detection techniques are self diagnosis, group detection and hierarchical detection. Through self diagnosis the node itself can identify faults in its components. With group detection, several nodes monitor the behavior of another node. Finally, in hierarchical detection the fault detection is performed using a detection tree where a hierarchy is defined for the identification of failed nodes. Often in a hierarchical detection the detection is shifted to a more powerful node such as the sink [2] .

1) Self-diagnosis

In many cases, nodes can identify possible failures by performing self-diagnosis.

2) Group detection

Here fault-tolerant can be applied by using clusters in WSNs. Here CH checks aliveness of the nodes in its cluster

3) Hierarchical detection

The definition of a detection tree enables a scalable fault detection algorithm in WSN. Each node forwards the status of the child nodes that it is monitoring to its parent node. Shifting

the fault detection task to a more powerful device is an alternative that can help to increase the lifetime of the WSN [2].

C. Fault recovery techniques

Fault recovery techniques enable systems to continue operating according to their specifications even if faults of a certain type are present. The most common technique is the replication of components. Although redundancy has several advantages in terms of high reliability and availability, it also increases the costs of a deployment. Recovery techniques for WSN can be classified into two major approaches: Active and Passive replication. Active replication means that all requests are processed by all replicas; while with passive replication, a request is processed by a single instance and only when this instance fails, another instance take over [2].

1) Active replication in wsn

Active replication in wireless sensor networks is applied in scenarios where all, or many, nodes provide the same functionality. One example is a service that periodically provides sensor data. Nodes that run this service activate their sensors and forward their readings to an aggregation service or to a base station. When some nodes fail to provide that information, the recipient gets the results from other nodes, which is often sufficient [2]. Some of these approaches are:

1) Multipath routing: Usually, it is desirable to avoid that a single failing node causes the partitioning of a sensor network. Thus, a network should be k-connected, which allows k – 1 nodes to fail while the network would still be connected [9].

2) Sensor value aggregation: Sensor value aggregation is a process where high level information is derived from a number of low-level sensor inputs. Here the inherent redundancy of sensor nodes can be used to provide fault-tolerant data aggregation. This ensures that despite of node failures, the resulting reading will contain the correct sensor reading of a region [2].

3) Ignore values from faulty nodes: A simple but efficient solution to not propagate a failure of one specific node to the entire network is to ignore the data that it is generating [11].

2) Passive replication in wsn

When passive replication is applied, the primary replica receives all requests and processes them [2].

D. Fault tolerance at different levels

Fault tolerance in WSNs can be classified into four levels hardware layer, software layer, network communication layer, and application layer [6].

1.) 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). There are three main reasons that cause hardware failure of sensor nodes. The first is that sensor networks are usually for commercial use and sensor nodes are cost sensitive. Therefore, design of a sensor node will not always use the highest quality components. The second is that strict energy constraints restrict long and reliable performance of sensor nodes. The third is that sensor networks are often deployed in harsh

and hazardous environments, which affect normal operation of sensor nodes. The wireless radios of sensor nodes are severely affected by these environment factors [6].

2) 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. An important component of system software is to support distributed and simultaneous execution of localized algorithms. Software bugs are a common source of errors in WSNs. One promising method is through software diversity where each program is implemented in several different versions [6].

3) Network Communication Layer:

Faults at network communication layer are the faults on wireless communication links. Assuming that there is no error on hardware, link faults in WSNs are usually related to surrounding environments. In addition, link faults can also be caused by radio interference of sensor nodes. For example, node a cannot successfully receive a message from node b if node a is within interference range of other nodes that are transmitting messages at the same time [6].

4) 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. However, an approach for fault tolerance in an application cannot be directly applied to other applications. On the other side, fault tolerance in application level can be used to address faults in essentially any type of resource [6].

E. Fault management architecture

Fault management architectures can be classified into centralized, distributed and hierarchical models [7].

1) Centralized model:

It is designed ideally for the centralized fault detection approaches. A central controller is usually responsible for fault maintenance of the overall network. In order to construct the global view of the network, central controller keeps updating nodes' states by message exchange. The central node identifies any faulty or suspicious nodes by comparing the current node states against those historical information models. It is accurate solution to identify fault. However, this centralized architecture is less efficient and more energy-expensive when large-scale sensor networks are considered [7]. The message flooding of such approach may greatly consume node energy because of frequent in-network message exchanges.

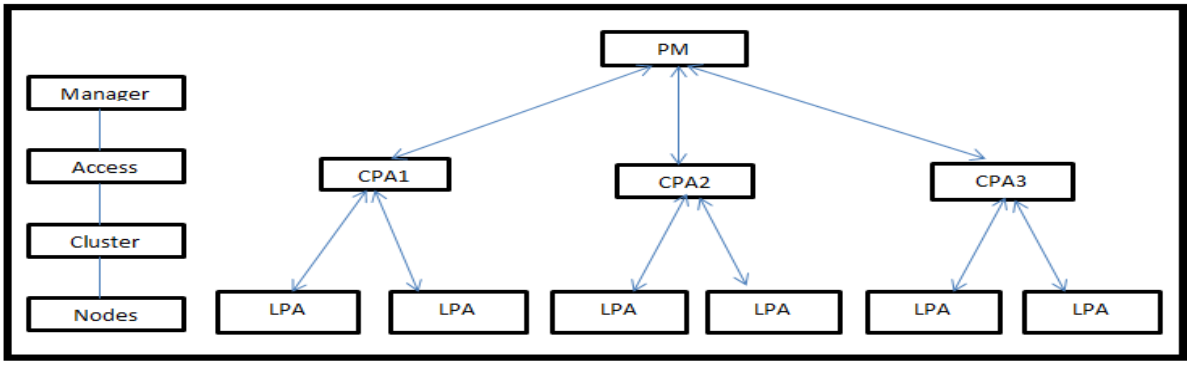
2.) Distributed model:

It splits the entire network into several sub-regions, and distributes fault management tasks evenly into these sub regions. Each region employs a central manager. Manager is responsible for monitoring and detecting failure in its region. It is also able to directly communicate with other managers in a coordination fashion for fault detection. As a result, the central controller of the overall network only needs to monitor a very small number of sensors in the network. This design conserves node energy by reducing in-network communication messages, and also enhances the system response time towards events

occurred in the network. Clustering can also be considered as one such approach [7]. In Clustering only CH needs to manage its cluster members locally.

3.) Hierarchical model:

It is a hybrid between the centralized and distributed approach. It uses intermediate managers to distribute manager functions. However, these intermediate managers do not directly communicate with each other. Each manager is responsible to manage nodes in its sub-network and report to its high-level central manager. In a three-layered hierarchical sensor network structure, cluster is adopted to reduce the number of sensor nodes monitoring the events occurred in the network. Sensors only send data of detected events to their corresponding cluster heads instead of transmitting to a far-away central fusion centre. The cluster head will make a decision about the fault events occurred within that sub-region. In order to accomplish fault management objectives in a reliable and energy-efficient way, Ying et al., proposed hierarchical mobile agent-based policy management architecture (as in Fig.1) for sensor networks. In which, Policy Manager (PM) at the highest level, Local Policy Agent (LPA) which manages a sensor node, Cluster Policy Agent (CPA) as an intermediate the highest level, Local Policy Agent (LPA) which manages a sensor component between PM and LPA. The management commands are always propagated from the PM to CPAs to LPAs [7].



PM: Policy Manager, CPA: Cluster Policy Agent, LPA: Local Policy Agent

Figure1 Fault Management Architecture [7]

II. CLUSTERING IN WSN

Clustering can be defined as the process in which nodes are placed in the form of cluster in order to achieve network scalability. It can be considered as an efficient way to aggregate and send data to the BS.

In 2002, Wendi Heizalman proposed LEACH. LEACH is a self-organizing, adaptive clustering protocol that uses randomization to distribute the energy load evenly among the sensors in the network. In LEACH, the nodes organize themselves into local clusters, with one node acting as the local base station or cluster-head. In LEACH there is random rotation of the high-energy cluster-head position such that it rotates among the various sensors in order to not drain the battery of a single sensor. In addition, LEACH performs local data fusion to "compress" the amount of data being sent from the clusters to the base station, further reducing energy dissipation and enhancing system lifetime. But this protocol has some drawbacks like in this protocol is that sensors always transmit data to the cluster head during their allocated TDMA slot. This consumes a lot of energy and dissipaiation of energy

of sensor nodes is more. Also in this protocol assumption is made that all nodes are within communication range of each other and the BS [11]. This assumption limits the scalability of the protocol. Here cluster-head aggregates data from all its members and send data to base station. In this protocol base station is located outside the network and cluster-head sends aggregated data to base station in one hop propagation which consumes lot of energy also this protocol offers no guarantee about the placement and/or number of cluster head nodes. So LEACH-C has been proposed in which central control algorithm is used to form the clusters. This produce better clusters by dispersing the cluster head nodes throughout the network [11]. To remove these drawbacks many protocols have been proposed like in 2006, Bo Huang, Fei Hao, Hui Zhu, Yuji Tanabe, Takaaki Baba proposed Energy Static Clustering Scheme for Wireless Sensor Network. It uses multi-hop propagation to send data to base station. As LESCS is a kind of static clustering protocol it removes the overhead of formation of cluster and selecting CH in each round because it forms cluster and CH once and never changed during the whole network. LESCS performs better than LEACH, in terms of system stability, energy consumption and network lifetime [1]. In 2008, Fuad Bajaber and Irfan Awan proposed Dynamic/Static Clustering Protocol for Wireless Sensor Network Static clustering owns high performance but the backbone sensors deplete energy faster and fail earlier than other sensors. Dynamic clustering is a good solution for hotspot problem but the dynamic clustering overhead is a heavy burden for limited energy sensors, and the stability of dynamic clustering is lower than that of static clustering. Both have some advantages and disadvantages so combining both techniques energy efficient Dynamic Static Clustering Protocol can be formed. In dynamic case DSC forms the clusters while in static case, the clusters are fixed for 10 rounds and cluster head position rotates among the nodes within the cluster [3]. DSC reduces communication overhead in setup phase. The first node death in DSC occurs later than the first node death in LEACH-C. DSC provides better performance than LEACH-C in terms of communication overhead, network lifetime and energy dissipated over time [3]. Here data is not sent based on occurrence of event, data is sent continuously so more energy is consumed.

In all these protocols there is no mechanism to detect the failure of CH because if CH fails it creates partition of node members with network for rest of the network life time. Nodes will not be able to send data to BS for rest of the network lifetime so these data are lost.

III. FAULT TOLERANT CLUSTERING IN WSN

In 2007, Yongxuan Lai and Hong Chen proposed Energy-Efficient Fault-Tolerant Mechanism for Clustered Wireless Sensor Networks. It views the cluster as an individual whole and utilizes the monitoring of each other within the cluster to detect and recover from the faults in a quick and energy efficient way. CMATO only needs the local knowledge of the network, relaxing the pre-deployment of the cluster heads and a k-dominating set ($k>1$) coverage assumptions [13]. CMATO deals with failures of multiple cluster heads, so it effectively recovers the nodes from the failures of multiple cluster heads and the failures of links within the cluster, gaining robust and fault-tolerant sensors. It builds multiple routing paths from the source to the destination, so transmissions can switch to another path when a path is failed. In CMATO, anti-cluster consulting mechanism is used to classify the type of the faults. The principle of the CMATO in-cluster consulting mechanism is: if more than α percents of the nodes in the cluster detect the failures of the links to the cluster head, then the

cluster head should be declared as a failure [13]. It improves the robustness of the clustered sensor network. When cluster members detect that the fault is a perpetual failure of the cluster head, they act cooperatively to select new cluster head to replace the failed one; when the cluster members detect the fault is a medium error, they just transfer themselves to the neighboring clusters or relay nodes [13]. So it is a distributed algorithm that does not need the *k*-dominated set coverage assumption or any global knowledge of the network. This mechanism does not use subscription method in which events are subscribed to the sensor nodes so data is sent continuously and there is more number of message exchanges which consumes more energy.

In 2011, Meikang Qui, Jianning Liu, Jiayin Li, Zongming Fei, Zhong ming proposed "A Novel Energy Aware Fault Tolerance Mechanism for Wireless Sensor Networks". Here the mechanism Called Informer Homed Routing (IHR) is used in which backup CH for each CH is selected. Nodes send data to PCH at each round, BCH checks weather PCH is alive or not by sending a small beacon message [8]. Here clusters are formed at each round, also number of exchange messages is increased so more energy is utilised for maintaining fault tolerance.

In 2013, PrasenjitChanak, TuhinaSamanta,Indrajit Banerjee proposed "Fault-Tolerant Multipath Routing Scheme For Energy Efficient Wireless Sensor Networks". In this protocol node can send data through multiple paths. Shortest path is selected for sending data other paths are used for duplicated data transmission also when neighboring node receives data it checks with its own data if data is same it does not forward that data [9]. In this method there is no subscription of event. Each node have to keep knowledge of its neighboring node and CH sends ack message to each node its cluster when it receives data which imply lot of message exchange.

In 2014, M. Hla Yin and Z. Win propose energy-efficient and fault tolerant routing LEACH (EF-LEACH) which is a modified version of the well known LEACH protocol; EF-LEACH proposes some fault related solutions of the pure LEACH. It provides network fault tolerant and achieves reliability and quality of service. After data transmission phase it performs fault detection phase and fault recovery phase where failure of CH is detected and network is recovered from that fault. Highest residual energy node will be selected as new CH [4]. Here in this protocol data is sent continuously in each round as there is no subscription of events so energy dissipation is more.

In 2009, Lutful Karim, Nidal Nasser and Tarek Sheltami proposed A Fault Tolerant Dynamic Clustering Protocol of Wireless Sensor Networks. Energy efficiency in the clustering protocols in highly desired in Wireless Sensor Network (WSN). Fault tolerant DSC (FT-DSC) protocol, provides reliability by a fault tolerance mechanism. In this protocol, the CH will be able to detect the failure of non-CH nodes and the BS will be able to detect the failure of CHs. Moreover, the CH and/or BS subscribes to non-CH nodes of a cluster to notify only when an event of interest occurs and so, the non-CH nodes do not sent data to CH in every time slot of a frame allocated to them, which reduces energy consumptions. CH will exclude the failure node from the allocated time slot (fault detection) by sending the special packet which is much smaller than that of the sensed event or data. Hence, sending a special packet consumes less energy as compared to that of a data packet. So fault detection of nodes will consume less energy. At the end of each round, the CH assigns the most remaining energy node as a new CH. If the BS is not aware of the failure of a CH, the new CH assignment at the end of around will not be performed. This will save energy by not making CH at the end

of each round. Hence this protocol provides more reliability compared to all above protocols because of its fault tolerant mechanism and also because base station subscribes message to all the nodes in the network so data is sent by nodes only when any event is triggered. This makes the protocol more practically applicable for real world applications. Energy dissipation in the DSC protocol over rounds is much more than FT-DSC and hence, the DSC protocol has less network life time than that of the FT-DSC protocol. However, the size of the special packet is much smaller than that of the data packet [5]. Hence, a special packet consumes less energy and has less communication overhead as well. So compared to all other protocols this protocol has high energy efficiency and is highly reliable. In this protocol data is send to BS according to subscription method and at the end of each round failure of CH is detected and new CH with sufficient energy is elected as CH for next rounds by BS.

IV. CONCLUSION

- To reduce energy consumption in forming clusters and selecting CH at the end of each round and to increase lifetime of backbone node, periodical changing of clusters is done by use of DSC protocol but it does not provide mechanism to detect failure of nodes.
- FT-DSC protocol provides the mechanism to detect the failure of any node or failure of CH.
- Better reliability and sustainability compared to other FT protocol as it saves energy because nodes send data only when subscribed events are triggered and small size packets are used for detection of failure of nodes.
- It uses hierarchical approach to detect failure of nodes and CH; this reduces the work load of all nodes and BS because BS needs to detect the failure of CH present in the network rather than detection of failure of all nodes in the network and failure of nodes is detected by CH due to this each node does not need to check aliveness of neighboring nodes so this protocol is efficient in terms of energy consumption for fault detection and recovery.

ACKNOWLEDGMENT

This work was supported by respective faculties and classmates. I express sincere thanks to Dr. H. R. Patel, Director, Dr. J. A. Shah, Principal, S.N.P.I.T. & R.C.,Umrakh, Bardoli, Gujarat, India for their motivational & infrastructural supports to carry out this research. I would like to give special thanks to HOD, Prof. V.N. Kapadiya, my guide Prof.Dhiraj Patel Assistant Professor, Electronics & Communication Engineering Department of S.N.P.I.T. & R.C. Umrakh, Bardoli and co-guide Prof. Pranav Lapsiwala Assistant Professor, Electronics & Communication Engineering Department of SCET, Surat, Gujarat, India whose timely and persistent guidance has played a key role in making my work a success.

REFERENCES.

[01] B. Huang, F. Hao, H. Zhu, Y. Tanabe and T. Baba, "Low-Energy Static Clustering Scheme for Wireless Sensor Network," Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006. International Conference on, pp. 1-4, 2006.

[02] De Souza, Luciana Moreira Sa, Harald Vogt, and Michael Beigl. "A survey on fault tolerance in wireless sensor networks." Interner Bericht. Fakultät für Informatik, Universität Karlsruhe: Karlsruhe, Germany (2007).

[03] F. Bajaber and I. Awan, "Dynamic/Static Clustering Protocol for Wireless Sensor Network," Computer Modeling and Simulation, 2008. EMS '08. Second UKSIM European Symposium on, pp. 524-529, 2008.

[04] Hla Yin Min, and Win Zaw "Energy Efficient, Fault Tolerant Routing LEACH (EF-LEACH) Protocol for Wireless Sensor Networks", International Conference on Advances in Engineering and Technology (ICAET'2014) March 29-30, 2014

[05] Lutful Karim and Nidal Nasser, Tarek Sheltami "A Fault Tolerant Dynamic Clustering Protocol of Wireless Sensor Networks"IEEE,2009.

[06] Lutful Karim "An Integrated Framework for Wireless Sensor Network Management" University of Guelph, 2012

[07] M. Hla Yin And Z. Win," Fault Management Using Cluster-based Protocol In Wireless Sensor Networks", International Journal Of Future Computer And Communication, Vol. 3, No. 1, February 2014.

[08] Meikang Qiu, Jianning Liu, Jiayin Li, Zongming Fei, Zhong Ming, Edwin H.-M. Sha, "A Novel Energy-Aware Fault Tolerance Mechanism for Wireless Sensor Networks" IEEE/ACM 2011

[09] PrasenjitChanak, TuhinaSamanta,Indrajit Banerjee proposed "Fault-Tolerant Multipath Routing Scheme For Energy Efficient Wireless Sensor Networks", IJWMN Vol.5.No.2, April 2013

[10] Rohan Chaudhari, Dharmistha Vishwakarma, Pranav Lapsiwala, " Energy Efficient LEACH Protocol for Wireless Sensor Network", International Journal of Advanced Research in Computer Science and Elecronics Engineering, Jan -13, Volume 2, issue -1, pp. 23-26. (ISSN NO: 2277-9043).

[11] Saurabh Mondal, Debajyoty Banik, "Energy Efficient Fault Tolerant Scheme for Wireless Sensor Networks (EEFSWSN)", IJCSET Vol 3 March 2013

[12] W. B. Heinzelman, A. P. Chandrakasan, and H.Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions on Wireless Communications Volume 1, No. 4, Oct 2002, pp.660 – 670.

[13] Yongxuan Lai, Hong Chen, "Energy-Efficient Fault-Tolerant Mechanism For Clustered Wireless Sensor Networks" 2007 IEEE.

