Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Fault Detection in WSNs

Vaishali Kalra, Ravi Kant Sahu
Computer Science Department, Lovely Professional University,
Punjab, India

Abstract: ***Information plays an important role in today's world. For transmitting this information, we use a lot of different kind of network system. Among this the most widely used medium is the wireless sensor network. But due to the high end traffic of the transmission of this information, some fault takes place. Detecting this wireless sensor node failure is very important. For detecting these faults, various approaches in wireless sensor network have been proposed. But due to the use of large numbers of portable sensor nodes in WSN, probability of sensor node failure gets increased. The objective of executing this project is to detect fault present in these sensor nodes. Here we are trying to detect the malicious node in order to reduce the data loss, thus enhancing the energy efficiency. By doing this, we can analysis the faulty nodes in a faster manner and and can ensure efficient data transmission.***

Keywords— WSN, Anomaly, Clustering, RTD, Data Recovery

I. INTRODUCTION

1.1 Wireless Sensor Networks

Wireless sensor network (WSN) comprises of huge number of tiny sensor nodes. Each sensor device has the capability to compute, communicate, sense and operate. Primarily, WSNs have been used widely in a variety of applications to perform tasks like environment monitoring and real time decision making. These tasks are purely dependent on the quality of data and information of the WSN.

Sensor nodes in the WSN are basically responsible for carrying up all the quality data and information. These sensor devices not only sense the situation but also cooperate with each other. So, sensing and communicating the data is the basic principle on which wireless sensor network works.

Besides sensor nodes, WSNs also contains sinks and sources. These all devices are connected with each other via wireless medium. This medium can be radio signals. These sensor devices are not expensive and are lower in energy. Moreover, these nodes have different memory capability. The sensor devices have functionality of sensing environmental and physical factors like pressure, temperature and sound in the field of network where they are actually deployed.

Hence, the nodes extract the data and information and then this is information is processed and is sent to the base station or central node via network. The nodes adjacent to a particular node are called its neighbor nodes. Every node passes the data to the next node. The next device then transfer the information to the neighbor node unless it arrives at the destination node.

To pass the information to the destination node, the sensor device should be aware about the direction of the destination node. While passing the data to the intermediate nodes in order to reach the destination node, the energy consumed is very high. Moreover, tasks like sensing the environment and collecting the data also requires high amount of energy. WSNs have numerous characteristics which are as following:

- Wireless sensor network is scalable in nature which means that any number of nodes can be deployed at any point of time; hence wireless sensor network can be enlarged.
- It is very easy to set up or configure a wireless sensor network because node deployment is done without any sort of installation.
- There are tons of sensor devices deployed in a wireless sensor network.
- Wireless sensor network has a feature of node mobility.
- It creates a scenario where human's physical presence is not required.

1.2 Sensor Node

Sensor node is the very important and main element of a wireless sensor network. Their functionalities include sensing the events, gathering and processing the data, and then finally forwarding the information to the destination node via neighbor nodes in the field. Besides sensing and other activities, sensor nodes also send back queries to the source nodes generated by sink or base station. In all, the sensor nodes act as communication channel between source node and sink. Every sensor node in a wireless sensor network has following subsystems:

- Sensor Subsystem
- Processing Subsystem
- Communication Subsystem

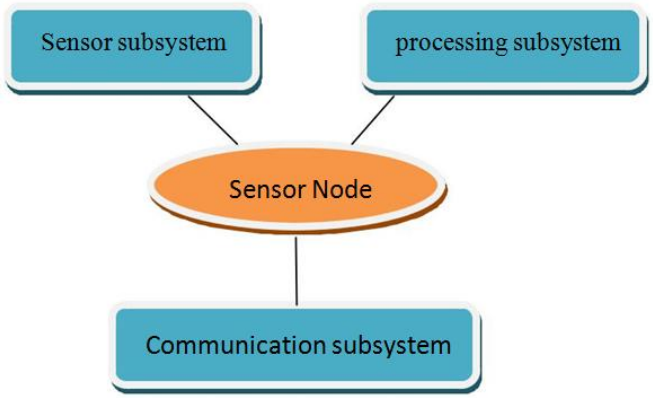

Fig.1 Subsystems of WSN.

Sensor Subsystem: The main function of this sensor component is to sense the environmental conditions or the events of the particular field.

Processing Subsystem: Processing basically comprises of all the computing, processing and storage related work **Communication Subsystem:** Communication is done between the sensor nodes, their immediate neighbors, source and the sink. Hence the information is communicated effectively with in the sensor network

1.2.2 WSN Hardware

As discussed above, a sensor device comprises of various units like sensing unit, processing unit, power unit and a transceiver unit. Sensing unit consist of further two units: analog to digital converter (ADC) and sensors. A small storage unit is associated with the processing unit. The function of transceiver is to connect the node with the network. WSN's hardware also includes batteries, CPU, power switch, antenna, external power connector, etc.

1.3 Architecture of WSN

The architecture of WSN explains the scenario that how field, source nodes, sensor nodes, sink are related to each other. It depicts how source node generates the message and then how this message is traversed through the network via neighbor nodes. In Fig. 1.3, it is shown that how source sends the announcement message to nearest dissemination node, how one dissemination node forwards the data to another dissemination node and finally the announcement message reaches to the sink.

The sink then sends the queries to the source and after receiving the response of those queries, it sends the complete information to the manager node through the internet. Manager node takes makes plans to take appropriate actions correspondent to the particular events that are sensed by the sensor nodes. The components that communication architecture of wireless sensor network includes:

- Sensor nodes
- Dissemination nodes
- Sink
- Manager node

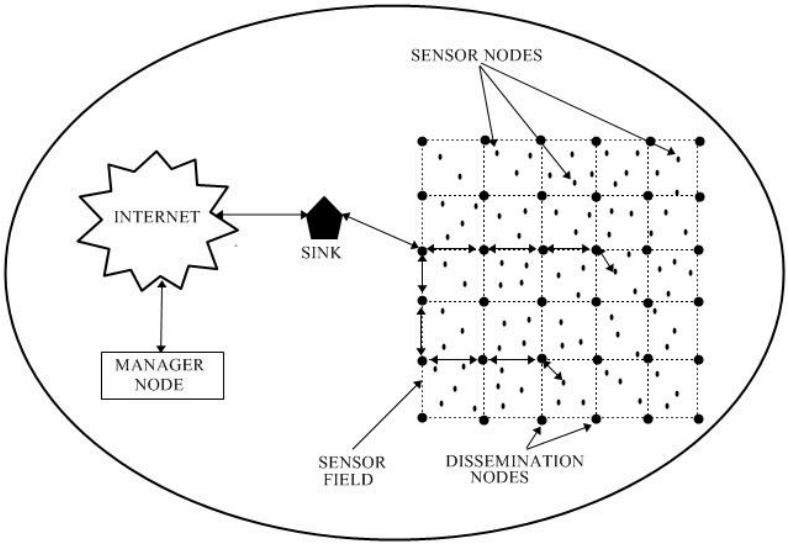

Fig.2 Wireless Sensor Network Communication Architecture

1.4 Fault Tolerance, Detection and Recovery in WSNs

Fault Tolerance: It is the property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components. If its operating quality decreases at all, the decrease is

proportional to the severity of the failure, as compared to a naively designed system in which even a small failure can cause total breakdown. Fault tolerance is one of the most important wireless sensor networks requirements. It ensures that the network continues to function correctly even when some components fail. In fact, fault tolerance is a need in this type of networks due to sensor node characteristics, radio communications and hostile environments in which these networks are deployed.

Fault Detection: Fault detection is an approach in wireless sensor network in which the fault occur are detected. Faults can be hardware faults or software faults. There are different approaches for finding faults in WSN.

Node Failure: Nodes in WSN are prone to failure due to energy depletion, hardware failure, communication link errors, malicious attack, and so on. Unlike the cellular networks and adhoc networks where energy has no limits in base stations or batteries can be replaced as needed, nodes in sensor networks have very limited energy and their batteries cannot usually be recharged or replaced due to hostile or hazardous environments. So, one important characteristic of sensor networks is the stringent power budget of wireless sensor nodes.

Fault Recovery: Recovery is the process in which the faults detected are treated so as to make system fine. There are various proposed methods for fault recovery as well. This process involves cost, effort and time. Once failure is recovered, the system starts working correctly.

1.5 Types of Sensing in WSN

- Event Sensing: It is the sensing technique where only events are being sensed.
- Periodic Sensing: In periodic sensing, the queries and events are being sensed in a periodic manner.
- Query sensing: Query sensing is the sensing process where only queries are being sensed not the events.

1.6 Issues of WSN

Although wireless sensor network has various unique characteristics but it also faces some challenges and issues. Some of the issues faced by wireless sensor network are:

Efficiency of Energy: Consumption of energy is a very vital factor for the lifetime of the network. As the traffic i.e. the transmissions of messages and queries between the source and the sink increases, more power is consumed. If power consumption is increases the lifetime of the wireless sensor network decreases. So high power consumption is an obstacle for the lifetime of the sensor node and the wireless sensor network.

Failure of nodes: Sensor nodes are prone to failure as the energy of the nodes continuously decreases. At the certain level the node run out of the energy and it fails.

Unparalleled power sources: When the sensor node is not left with energy, it dies and it cannot be replaced with another power source.

Failure of the whole network: When the nodes between the source and the sink fail, then the sink or the base station is completely separated from the whole network. So as the base station is isolated, it cannot receive or send messages and queries and the whole network fails.

Limited Storage: Sensor nodes are built with low memory. So limited data can be stored.

II. LITERATURE REVIEW

The reviewed literature describes the various fault detection techniques various research papers have been reviewed to analyze the detection techniques and various ways through which energy can be saved. The various others factors which are focused are data efficiency, fault prevention, energy efficiency etc. The reviewed research papers are explained in this section.

Sandeep Saurav Singh *et.al*[8] explains that using large number of sensors in an application increases the Quality of service (Qos). On the other hand using large number of sensors also leads to failure hence affecting the QoS. Sensor Node failure can happen due to many reasons such as failure of battery, environmental effects, hardware or software disorder.

For enhancing QoS it is important to detect the failure node and transfer the data associated with that sensor node. Existing system uses Round Trip Delay (RTD) time for selecting the failure node. RTD is the time taken to receive the packet at receiver's end and getting back the acknowledgement to the sender. If the RTD is exceeding its general value then it is expected that the node has failed.

This method does not lead to the failure detection at appropriate time. Hence, it can cause data loss in the network. To overcome this limitation, in this paper the Check Point Recovery Algorithm (CPRA) is used for fault detection. The CPRA calculates the energy level of each sensor node. At some time interval all the nodes will send a heartbeat which will lead to know that the node is working properly.

When the energy level of the node will decrease it will not send any heartbeat to the checkpoint which will let us know that the node is about to fail. So, the data associated with the node can be transferred to some other node which will lead to an increase in the reliability of the system. An approach of Check Point recovery algorithm (CPRA) is proposed.

This paper presents an AODV (Ad-hoc On Demand Distance Vector) protocol which is a reactive type of routing protocol to find the shortest path between two nodes.

The Check Point Recovery Algorithm is used for finding the malicious nodes. While transferring the data among the nodes, the nodes send a heartbeat message. If the heart beat messages are being received before time out, then the energy level of that node is high and that node can be selected for transmission.

If the heart beat is not received by a particular node, it means that that the energy level of that node is low and it is leading towards failure. When the low energy node is detected, it is replaced by another node. Dynamic sensor node is used for replacing the node whose energy level is about to drain with another node whose energy level is high to prevent the node from failure. The Network Topology Management (NTM) helps in maintaining the links of the node which replaces the failure node.

After the replacement of the nodes, the ID of the replaced node will be broadcasted to all the neighboring nodes. If the nodes are already replaced before failure, then the data associated with that node will not be lost. This decreases the data loss in the system and thus, increasing the efficiency of the system.

Ravindra Navanath Duche *et.al* [9] has presented a framework in which the Round Trip Delay (RTD) time of discrete round trip paths are used for the detection of faulty nodes and are compared with threshold value. The limitation of this scheme is that the detection of nodes happen after the expected RTD exceeds. By that time the node already use tobe in failed state. Hence, the data associated with that node cannot be retrieved again which leads to packet loss.

Sutharshan Rajasegarar *et.al***[1]** explains about Anomaly detection in wireless sensor networks which involves intrusion detection, fault diagnosis and monitoring applications. The main focus is on how to reduce or to minimize the energy consumption in sensor nodes and to maximize the lifetime of the network. Authors have further mentioned the two broad techniques of anomaly detection:

- Statistical Technique: In this technique, the prior knowledge about the distribution of the data is known. Disadvantage of this methodology is that it causes complexity due to large number of parameters which are to be estimated.
- Non parametric techniques: In this technique, the distribution of data set is not known. The Non Parametric approaches are further classified as:

Rule based approach– There are certain predefined rules .if the rules applied result in anomalous condition, then the anomaly is detected. Rules can be integrity rule, retransmission rule and repetition rule.

CUSUM Approach- This approach is used to detect change in the mean value of probabilistic or random process. Anomaly is detected by comparing the CUSUM value to the threshold value. The disadvantage of CUSUM approach is that a high value of threshold will result in longer detection delays. The other one is that it only focuses on features in isolation. The advantage is that it detects attacks like wormhole, sinkhole and jamming.

Data Clustering: Here the clusters of data points with similar properties are built. Points fall outside these clusters are termed as outliers. It detects routing attacks in sensor networks.

Density based approach: In this approach the population density distribution of the data is measured and data points lying in the low density regions are termed as outliers.

Support vector machine: In this method hyper sphere of the data vector is made. The data that lie outside the hyper sphere is termed as anomalous data. Here we have the problem of communication overhead.

Sirajul Ameen *et.al* [3], The focus of this paper is to minimize the task of cluster head. A group of nodes is called a cluster. Cluster head is chosen on basis of forte node and they pass data ultimately to sink node. These nodes sense the environment and cooperate with each other and generate a value as global consequence that will pass the status to sink node in the network. Fault tolerance: Nodes respond to the input without getting fail. Even if one of the nodes gets down, the system as a whole doesn't get affected. Fault diagnosis: Failures are of two type hardware and software faults. Fault can either occur if node gets out of range or some get down due to battery weaknesses. Problematic scenario: cluster nodes send their data to cluster head in order to send data ultimately to sink node, cluster head keep passing data to the nearest cluster heads and this may result early battery drain of cluster head. Model communication: burden is reduced by introducing the relay node between head and sink. Before transmission, record the Battery life, one with the highest is the cluster head. Features of relay node are as following:

- More battery strength
- 1 mb flash
- 64 mb SD Ram
- 400 mhz linux system
- Relay node is responsible for data packet fusion from sensor nodes.
- Communication is done by RCS (radio communication section), this section increases energy to do task.
- Similarly, IRS (information recording section), to store information received from previous node.
- CS (information conventional section), decides what to forward next.

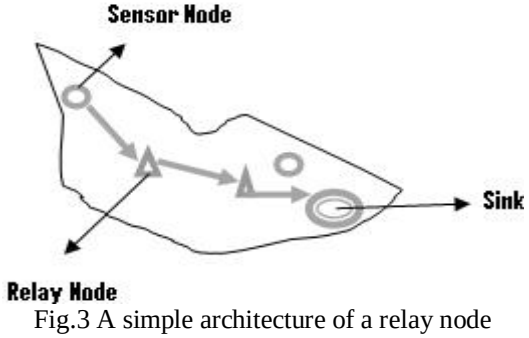

Fig.3 A simple architecture of a relay node

Ehsan Warriach *et.al*[5] explains about three detection approaches. While there are numerous methods for detecting faults, authors consider three qualitatively diverse methods Rule-based, Linear Least-Square Estimation (LLSE) and Hidden Markov Model (HMM - learning-based) to define heuristics rules for detecting and identifying faults dynamically. Rule-based methods are based on domain and expert knowledge to define heuristic rules for identifying and classifying faults. Estimation methods predict normal sensor behavior by leveraging sensor correlation. Finally, learning-based methods are able to statistically identify and classify classes of faults. The system heuristics rules built on expert and domain knowledge and data from activity recognition in smart office Lab.

III. CONCLUSION

This paper provides an overview of current approaches of fault detection in wireless sensor networks. It has also discussed the advantages, disadvantages of several approaches. Various issues of wireless sensor network have been mentioned. Along with that a clear architecture of the same has been described. Several techniques like rule based, cusum approach, support vector machine have been touched. It has also explained various ways for Qos enhancement and how it gets affected by node failure. moreover the issue of data recovery overhead has been addressed.

REFERENCES

[1] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," *IEEE Wirel. Commun.*, vol. 15, no. 4, pp. 34–40, 2008.

[2] Z. Wang, Q. Wen, Y. Sun, and H. Zhang, "A Fault Detection Scheme Based on Self-Clustering Nodes Sets for Wireless Sensor Networks," *2012 IEEE 12th Int. Conf. Comput. Inf. Technol.*, pp. 921–925, 2012.

[3] S. Ameen and M. A. A, "Fault Tolerance Using Cluster in Wireless Sensor Network," vol. 4, no. 4, pp. 351–356, 2014.

[4] C. A. Jerlin *et al.*, "Fault tolerance in wireless sensor networks," *Int. J. Innov. Res. Adv. Eng.*, vol. 2, no. 2, pp. 142–146, 2015.

[5] E. U. Warriach, K. Tei, T. A. Nguyen, and M. Aiello, "Fault detection in wireless sensor networks," *Proc. 11th Int. Conf. Inf. Process. Sens. Networks - IPSN '12*, vol. 3, no. 3, p. 87, 2012.

[6] C. Lo, M. Liu, and J. P. Lynch, "Decentralized Fault Detection in Wireless Sensor Networks," *Electr. Eng.*, vol. 2013, pp. 1–5, 2013.

[7] E. U. Warriach, K. Tei, T. A. Nguyen, and M. Aiello, "Fault detection in wireless sensor networks," *Proc. 11th Int. Conf. Inf. Process. Sens. Networks - IPSN '12*, p. 87, 2012.

[8] S. S. Singh, "Sensor Node Failure Detection using Check Point Recovery Algorithm," pp. 3–6, 2016.

[9] Ravindra Navanath Duche and Nisha P. Sarwade,Sensor Node Failure Detection Based on Round Trip Delay And Path In WSNs SENSORSJOURNAL, VOL. 14, NO. 2, FEBRUARY 2014.

