[Kumar *, Vol.5 (Iss.5): May, 2017]
ICV (Index Copernicus Value) 2015: 71.21

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)
InfoBase Index IBI Factor 3.86

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

SURVEY OF FAULT DETECTION ALGORITHM IN WSN

Vijay Kumar [*1]

[*1] Assistant Professor, Department of Computer Science, Central University of Haryana, India

DOI: https://doi.org/10.29121/granthaalayah.v5.i5.2017.1851

Abstract

In recent years, applications of wireless sensor networks (WSNs) have been improved due to its vast potential to connect the physical world to the virtual world. Also, a progress in microelectronic fabrication technology reduces cost of developed portable wireless sensor nodes. Faults occurring to sensor nodes are familiar due to the sensor device itself and the harsh environment where the sensor nodes are deploy. WSNs is mainly affect by the crash of sensor nodes. Possibility of sensor node failure increases with increase number of sensors. Wireless sensor networks have been recognized, at an early stage in their development, to be a useful measurement technology for environmental monitoring applications. Based on their independence from accessible infrastructures, wireless sensor networks can be deploy in virtually any location and provide sensor samples in a spatial and temporal resolution.

Keywords: WSN; Fault Model; BFRA.

Cite This Article: Vijay Kumar. (2017). "SURVEY OF FAULT DETECTION ALGORITHM IN WSN." *International Journal of Research - Granthaalayah,* 5(5), 207-213. https://doi.org/10.29121/granthaalayah.v5.i5.2017.1851.

1. Introduction

1.1. Wireless Networks

Today's Internet has been developed for more than thirty years. Recently many network Researchers are studying networks based on new communication techniques, in particular Wireless Communications. [1] Like traditional wired networks, wireless networks are created by routers and hosts. In a wireless network, the routers are dependable for forwarding packets in the network and hosts may be sources or sinks of data flows. People can deploy a wireless network very easily and speedily .The basic difference between wired and wireless networks is the way that the network components communicate. A wired network depends on physical cables to move data. As it is understood that in a wireless network, the communication among different network components can be either wired or wireless. As wireless message does not have the constraint of material cables, it allows a explicit freedom for the hosts and/or routers in the wireless network to travel. This is one of the advantages of a wireless network [2]. Wireless LANs present the follow productivity, convenience, and cost advantages over the wired networks: [3]

- Mobility: Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. Mobility supports efficiency as well as service opportunities which are not possible with wired networks.
- There are now thousands of hotels, universities and public places with public wireless connection. These free us from having to be at home or at work to get access the Internet.
- Reduced Cost-of-Ownership: Though the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, but overall mechanism expenses and life-cycle costs can be considerably lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
- Installation Speed and Simplicity: It is very easy and quick process to install a wireless LAN system and thus allows to get rid of the need to pull cable through walls and ceilings.
- Scalability: Wireless LAN systems can be configured in many different types of topologies to fulfil the needs of particular applications and installations. Configurations can be naturally changed and range from peer-to-peer networks suitable for a few numbers of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

In a wireless network the network components communicate with each other by the use wireless channels. Dissimilar radio frequency (RF) spectrum ranges are used in wireless networks, as for example, 2.5-2.7 GHz for the Multipoint Multichannel Distribution System ,27.5-29.5, correspondingly. The strength of the signal in a wireless medium decreases when the signal travels further [2].

When the signal travels beyond some distance, the strength gets reduced to the point where reception is not possible. The distance that a signal travels when it reaches to this point is called the radio range for the given signal. To simplify the transmission model regarding this property, people think that the wireless signal is strong enough for the receivers to receive the signal if the receivers are inside of the radio range [2]

2. Related Work

2015 Jie Wu, et al wireless sensor networks, named clustered agreement time synchronization (CCTS). This algorithm is developed on the base of the distributed consensus time synchronization (DCTS) algorithm. However, to obtain faster meeting in the clock synchronization of node and better energy efficiency, the clustering technique is included into the algorithm. The CCTS includes two parts: 1) intracluster time synchronization and 2) intercluster time synchronization. In the intracluster time organization, the better DCTS is applied. The cluster head is responsible for exchanging messages within the cluster. The standard value of skew costs parameters of intracluster virtual clock and the average value of intracluster virtual clocks are used to update the skew compensation parameter and offset compensation parameter, respectively. In the intercluster time synchronization, cluster heads replace messages via gateway nodes. To modernize the clock compensation parameters of the network virtual clocks, clock costs parameters of intracluster virtual clocks of every cluster head are assigned with corresponding weights based on the size of each cluster. The simulation results show that the future algorithm reduces the communication traffic compared with the DCTS algorithm, and improve the convergence rate suitable to the combination of clustering topologies

2014 Ravindra Navanath Duche et al the proposed method of fault detection is based on RTD time size of RTPs. RTD times of discrete RTPs are compared with threshold time to determine failed or malfunctioning sensor node. Initially this method is tested and verified on six wireless sensor nodes, implement by with microcontroller and Zigbee. In order to confirm the scalability of this concept, WSNs with huge numbers of sensor nodes are implemented and simulated in open source software NS2. Generalized model to establish the fault detection analysis time for WSNs by using discrete RTPs is suggested different experiments are performed in hardware and software based on RTD time measurements. Analysis time in every cases of fault detection is determined with the help of generalized model. Result scrutiny in hardware and software indicate that RTD time measurement results in both cases are quite the same, validating the real time applicability of this method.

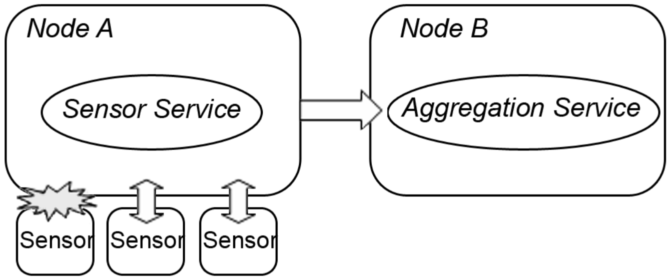
2013 Hong-Chi Shih et al purpose a fault node recovery (FNR) algorithm to enhance the lifetime of a wireless sensor network (WSN) when some of the sensor nodes shut down, either for the reason that they no longer have battery energy or they have reached their operational threshold. Using the FNR algorithm can result in smaller number replacements of sensor nodes and more reused routing paths. Thus, the algorithm not only enhances the WSN lifetime but also reduces the cost of replacing the sensor nodes. The conventional approaches to sensor network routing include the directed diffusion (DD) algorithm and the grade diffusion (GD) algorithm. The algorithm proposed is based on the GD algorithm, with the objective of replace fewer sensor nodes that are inoperative or have depleted batteries, and of reuse the greatest number of routing paths. These optimizations will ultimately augment the WSN lifetime and reduce sensor node replacement cost.

3. Failures in Wireless Sensor Networks

To comprehend fault tolerance mechanisms, it is significant to point out the difference between faults, errors, and failures different definitions of these terms have been used [9],

- A fault is any kind of defect that leads to an error.
- An error corresponds to an incorrect (undefined) system state. Such a state may direct to a failure

A failure is the (observable) manifestation of an fault, which occurs when the system deviate from its specification and cannot deliver its intended functionality. Figure illustrates the difference between fault, inaccuracy, and failure. A sensor service successively on node A is expected to periodically send the measurements of its sensors to an aggregation service running on node B. However, node A suffers a crash cause a loose connection with one of its sensors. While the code execute node A’s service is not designed to detect and overcome such location, an wrong state is reached when the sensor check tries to acquire data from the sensor. Due to this state, the service does not send sensor data to the aggregation service within the specified time interval. This results in a break down or omission failure of node A observed by node B.



In the scenario explained above, the fault is the loose connection of the sensor. The error is the state of the service after trying to read the sensor data and the failure occurs when the application does not send the sensor data within the specified time interval. To provide flexibility in faulty situations two main actions must be performed:

Fault detection: To provide any countermeasures, the first step a system must carry out 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 check or recover from it. The main technique to achieve this goal is to replicate the components of the system that are vital for its correct operation.

4. Exciting Fault Node Recovery Algorithm

4.1. Directed Diffusion Algorithm

The goal of the DD algorithm[2] is to reduce the data relay transmission counts for power administration. The DD algorithm is a query-driven communication protocol. The collected data is transmitted only if it matches the query from the sink node. In DD algorithm, the sink node provide the queries in the form of attribute-value pairs to the other sensor nodes by broadcasting the query packets to the whole network. Then, the sensor nodes send the data back to the sink node only when it fits the queries.

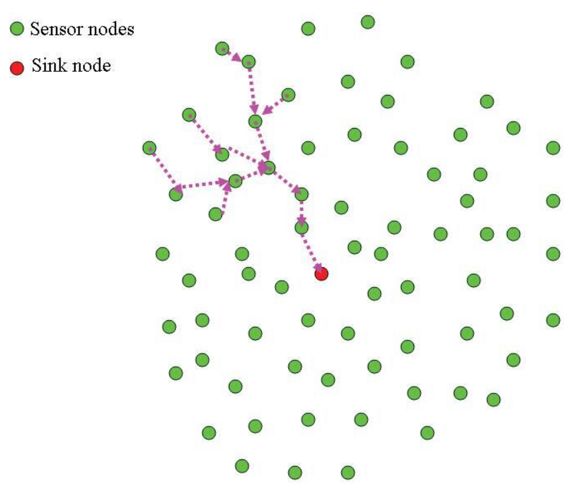


Figure 4.1: Wireless sensor node routing.

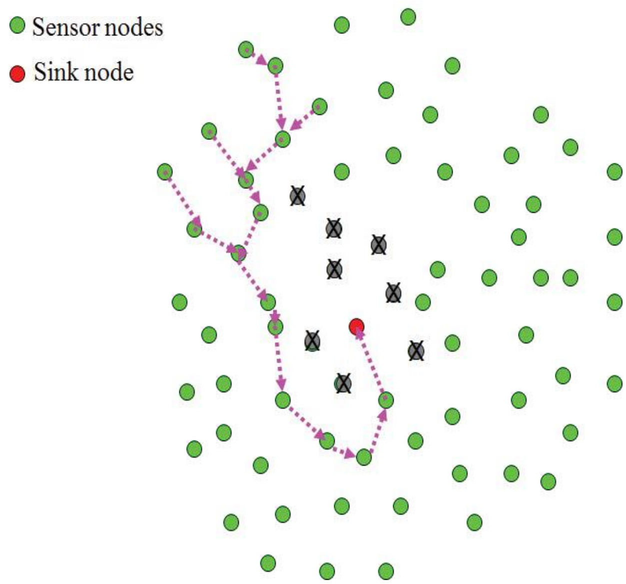


Figure 4.2: Wireless sensor node routing path when some nodes are not functioning.

4.2. Grade Diffusion Algorithm

The GD algorithm[2] not only creates the routing for each sensor node but also identifies a set of neighbor nodes to reduce the transmission loading. Each sensor node can choose a sensor node from the set of neighbor nodes when its grade table lacks a node able to perform the relay. The GD algorithm can also record some in order regarding the data communicate. Then, a sensor node can choose a node with a lighter loading or more available energy than the other nodes to perform the extra transmit operation. That is, the GD algorithm updates the routing path in actual time, and the event data is thus sent to the sink node quickly and right. Whether the DD or the GD algorithm is applied, the grade creating packages or concerned query packets must first be broadcast. Then, the sensor nodes move the event data to the sink node, according to the algorithm, when appropriate events take place. The sensor routing paths are shown in Fig. 4.1

The WSN may fail due to a range of causes, including the following: the routing path might experience a break; the WSN sensing area might experience a leak; the batteries of some sensor nodes might be depleted, requiring more transmit nodes; or the nodes wear out after the WSN has been in use a long period of time. In Fig. 4.2, the situation in which the outside nodes transfer event data to the sink node via the inside nodes (the sensor nodes near the sink node) in a WSN illustrate the accommodation measures for non-working nodes. The surrounded by nodes thus have the largest data communication loading, consuming energy at a faster rate. If all the surrounded by nodes deplete their energy or otherwise cease to function, the happening data can no longer be sent to the sink node, and the WSN will no longer task

5. Network Model and Faultmodel

We assume sensors are randomly deployed in the interested area and all sensors have a common transmission range. The area is assumed to be completely covered by the sensors. As shown in Figure 5.1, the shady circles represent faulty sensors and the light gray circles are good sensors. There could be a failure taking place in a certain area as illustrated in the figure. All sensors in the area go out of service. Since we are depending on majority voting, we assume that each sensor has at least 3 neighboring nodes. Because a large amount of sensors are cast into the interested area to form a wireless network, this condition can be simply obtain. Each sensor node is able to locate the neighbors within its transmission range through a broadcast/acknowledge protocol.

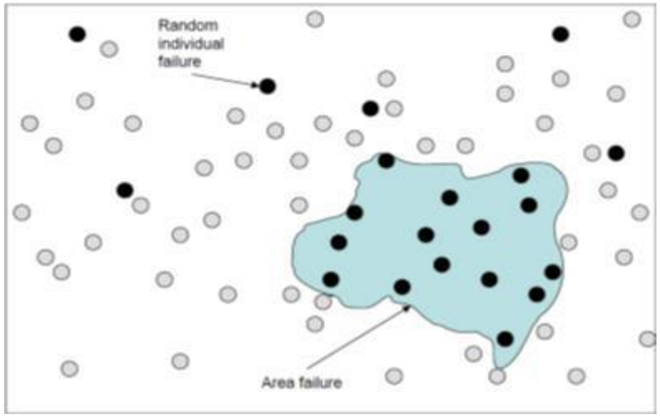


Figure 5.1: Sensor nodes randomly deployed over an area

6. Fault Detection Algorithm

In general the fault detection algorithms are categorized into two types namely centralized and distributed approach.

1) Centralized approach most existing approaches of fault detection in WSNs are centralized, in which each sensor reports its state information to the sinks by periodically transmitting specific control messages. Sinks parse the messages and detect the potential faults. In these approaches, they usually assume that data follow the same distribution. Thus they make use of the relation of data to detect the faulty measurements. For example, a correlation graph is used to characterize the internal correlations inside a node [4].
2) Distributed WSN: In distributed WSN each sensor node has the capability to identify its status (faulty or fault free) up to some extent as the biological component does. This capability is popularly known as self-monitoring approach. This approach delivers less information to either its neighbors or fusion center, which yields less energy consumption. A self-monitoring approach was discussed by authors in [16]. In this approach each sensor node sends an update message to its neighbors within a fixed time interval. Then the neighbor detects the existence of the node and sends the status to fusion center. If the neighbor does not found any update packet within that time interval then the neighbors declares the node may not exist and sends data to fusion center. Fusion center analyze the data received by each sensor to detect the fault status of all the nodes present in the network. This approach uses a static network as each sensor knows it's in neighboring co-ordination technique, each node identify its status based on neighbors data before communicating with the central. In [9] a neighboring coordination technique is used. Here each node decides its status based on the difference between its own sensed data and neighboring median reading.
3) Bayesian Fault Recognition Algorithms, BFRA: The algorithm can make a distinction between sensor faults and sensitive events. They pointed that fault nodes are spatially uncorrelated, while the measurements in the event region are correlated. In BFRA, every node exchanges their measurements with neighbors to get the statistical probability of event

detected by neighbors. Using the nodes' faulty probability and statistical probability of event, the algorithm estimates the conditional probability of event. Combined with the measurements from sensor node, BFRA can determine whether an event or error.

7. Conclusion

In this paper we provided a detailed study of faults that occurred in real WSN deployments. This concise study provides a valuable knowledge input for future application to prevent the same kind of issues from happening. In real wireless sensor networks, the sensor nodes use battery influence supplies and thus have incomplete energy resources. In adding to the routing, it is important to research the optimization of sensor node substitution, reducing the substitution cost, and reusing the most routing paths when some sensor nodes are nonfunctional.

References

[1] Ravindra Navanath Duche and Nisha P. Sarwade "Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs" IEEE SENSORS JOURNAL, VOL. 14, NO. 2, FEBRUARY 2014

[2] Hong-Chi Shih, Jiun-Huei Ho, Bin-Yih Liao, "Fault Node Recovery Algorithm for a Wireless Sensor Network" IEEE SENSORS JOURNAL, VOL. 13, NO. 7, JULY 2013.

[3] Marwa Saihi, Marwa Saihi, Ahmed Zouinkhi" Decentralized Fault Detection in Wireless Sensor Network based on function error" 2013 10th International Multi-Conference on Systems, Signals & Devices (SSD) Hammamet, Tunisia, March 18-21, 2013

[4] Meenakshi Panda, Pabitra Mohan Khilar "Distributed Soft Fault Detection Algorithm in Wireless Sensor Networks using Statistical Test" 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing

[5] Ehsan Khazaei, Ali Barati, Ali Movaghar" Improvement of Fault detection in wireless sensor networks" 2009 ISECS International Colloquium on Computing, Communication, Control, and Management IEEE.

[6] Zhaoxing Wang, Qiaoyan Wen, Teng Wang, Hua Zhang "A Fault Detection Method for Wireless Sensor Networks Based on Credible Sensor Nodes Set" 2012 Ninth IEEE International Conference on e-Business Engineering .

[7] Jianliang Gao and Jianxin Wang, Xi Zhang "HMRF-Based Distributed Fault Detection for Wireless Sensor Networks" IEEE JOURNAL, VOL. 12, NO. 2, 2012

[8] Jie Wu, Liyi Zhang, Yu Bai, and Yunshan Sun "Cluster-Based Consensus Time Synchronization for Wireless Sensor Networks " IEEE 2015.

[9] Luciana Moreira S´a de Souza, Harald Vogt" A Survey on Fault Tolerance in Wireless Sensor Networks" http://www.cobis-online.de/

*Corresponding author.
E-mail address: Vjkumar@cuh.ac.in