ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 4; Issue 6; November-December; 2016; Page No.. 75-79

Distributed Fault Detection Mechanism for WSN

Prakash Kawar Asawat[1], Girdhar Gopal Singh[2]

[1]Assistant Professor, Department of Computer Science & Engineering, Jodhpur Institute of Engineering and Technology, Jodhpur, Rajasthan, India

[2]B. Tech Scholar, Department of Computer Science & Engineering, Jodhpur Institute of Engineering and Technology, Jodhpur, Rajasthan, India

Conflicts of interest: Nil

Corresponding author: Prakash Kawar Asawat

Abstract

In recent days, WSNs are emerging as a promising and interesting area. Wireless Sensor Network consists of a large number of heterogeneous/homogeneous sensor nodes which communicates through wireless medium and works cooperatively to sense or monitor the environment. The number of sensor nodes in a network can vary from hundreds to thousands. The node senses data from environment and sends these data to the gateway node. Mostly WSNs are used for applications such as military surveillance and disaster monitoring. We propose a distributed localized faulty sensor detection algorithm where each sensor identifies its own status to be either "good" or "faulty" which is then supported by its neighbors as they also check the node behavior. Finally, the algorithm is tested under different number of faulty sensors in the same area. Our Simulation results will demonstrate that the time consumed to find out the faulty nodes in our proposed algorithm is relatively less with a large number of faulty sensors existing in the network.

INDEX TERMS:INTRODUCTION, FAULT CLASSICATION, FAULT DETECTION TAXONOMY, FAULT DETECTION TECHNIQ, APPLICATIONS OF WSN, CONCLUSION, REFERENCE.

INTRODUCTION

Wireless sensor networks consist of a large number of independent sensor nodes connected together to form a network. Each of these individual sensor nodes in a wireless sensor network has sensing and processing capability. Wireless communication is used as a medium for communicating between the nodes. It forms an ad hoc network with peer–peer communication. Wireless sensors are low power devices with limited computational power, memory, battery and storage. They are deployed in hostile and harsh conditions to report time-critical events such as landslide monitoring, agricultural monitoring, military operations, infrastructure monitoring, scientific data collection, intruder detection system, navigation, and environmental monitoring. Sensor networks are also used to monitor the health of patients in hospitals.

Since, sensor networks are deployed in hostile and harsh conditions, e.g., rain, snow, wind, thunder, etc., they are susceptible to frequent and unexpected errors. The faults may be due to hardware or software failure. These faults result in erroneous results in normal operation. The occurrence of faults during normal operation results inharsh consequences involving loss of human life, economic and environmental loss as sensor networks are used in safety catastrophic disasters. For example, if the wireless sensor detecting the activity of the volcano malfunctions and gives incorrect readings, it might result in unneeded panic or loss of lives due to the absence ofwarning.

The presence of faults in wireless sensor data, may increase the network traffic, decrease the fault detection efficiency of the base station and wastes the battery and power. They need to conserve battery as they are supposed to operate for periods of time ranging from hours to years. Moreover, replacing the battery is not feasible since sensors are normally deployed at inaccessible locations. The transmission of collected data from nodes to sink is an expensive processandresultsincongestion. The presence of faulty sensor nodes increases the congestion by transmitting unusable and misleading data. Therefore, fault detection techniques are required for proper management of the sensor network. Fault detection algorithms enhance bandwidth utilization and data reliability. However, the energy consumption by the nodes increases due to complex fault detection techniques. Hence, there is a tradeoff between conservation of energy versus maintaining a high Quality of Service. Fault detection techniques detect the faulty node in a wireless sensor network and create a record of all faulty nodes, which can be used for fault recovery of the node or replacement of the faulty node or isolate faulty sensor nodes from the network.

Fault Classification

Faults in WSN can be classified by two aspects: the time span of the fault and the locality of the fault. The timespan of the fault indicates the duration of the faults. Some faults are temporary faults and occur for a certain duration. Hence, based on the time span of the fault, faults can be further classified into two categories: (1) persistent faults and (2) transient faults. Transient faults are temporary faults that occur due to certain conditions such as network congestion, changing weather conditions, etc. These faults are not permanent and disappear after a short time. Persistent faults are the faults that are permanent; these faults exist until a fault recovery is performed. In a majority of cases, the faults are local to specific component of WSN. Faults are extremely local in the network and only affect a few components of the network. Generally, the entire WSN is not faulty. Faults only affect a small number of components of the network instead of the whole global network. Due to the increasing reliability of the networks, the growthof the faults is slower than that of network size.Hence,thedetectionhastobebasedonthelocalitythantheentireglobal system. Therefore, by fault locality, we classify the faults broadly into two categories: (1) data-centric and (2) system-centric. The fault classification is not disjoint and can overlap with each other.

2.1 DATA-CENTRICPERSPECTIVE

Data-centric perspective takes into consideration the characteristics of the sensed data in determining faults. They are also called as soft faults.

2.1.1 Offset Fault Off set fault refers to a deviation in sensed data by an additive constant from the expected data. This might occur due to improper calibration of the sensor. An offset fault can be modelled as $x' = \alpha + x + \eta$, where $x' \in f(t)$ and α is the constant value that get added to the normal reading.

2.1.2 Gain fault A fault is said to be a gain fault if the rate of change of sensed data does not match with expectation over an extended period of time. In gain fault, a constant value gets multiplied to the non-faulty sensor data. This also might be caused by improper calibration of the sensors. Again fault can be model ledas$x'=\beta x+\eta$, where$x' \in f(t)$andβ is the constant value that gets multiplied to the normal reading.

2.1.3 Stuck-at fault A fault is said to be a stuck-at fault when the difference or the variance of data from the data series of a node is zero which implies that the sensed data is constant. A stuck-at fault can be either transient or persistent. A stuck-at fault can be modelled as $x' = \alpha$, where $x' \in f(t)$ and α is the constant value that is sensed. Stuck at fault can be further classified as stuck-at-one and stuck-at-zero. When α is the maximum value that can be sensed by the sensor, it is called as stuck- at-one and when it is minimum, it is called stuck-at-zero.

2.1.4 Out of bounds A fault is said to be an out of bound fault if the sensed data lies beyond the thresholds defined by the problem requirement. A node is said to have out of bounds error if $x' > \theta$ or $x' < \theta_1$, where $x' \in f(t)$,θ and θ_1 are the application thresholds.

2.1.5 Spike faults If the rate of change of measured time series with the predicted time series is more than the acceptable changing trend, then the faults are said to be spike faults. If $|f(t) - f^P(t)|/t > \lambda$, where λ is the normal changing trend, and $f^P(t)$ is the predicted time series data at time t, then it is said to be spike fault.

2.1.6 Data loss fault A data loss fault occurs when sensed data is missing from the time series for a given node. If $f(t) = \Phi \;\&\; t > \tau$, where Φ is the null set and τ is the maximum time required for sensing, then it is called data loss error.

2.1.7 Aggregation/fusion error An aggregation error is said to occur when

$$(\sum |f(t) - f^P(t)|/t. > \lambda^*) \;\&\; (|f(t) - f^P(t)|/t < \lambda)$$

Where λ^* is the acceptable total error bound and λ is the normal changing trend.

2.2 SYSTEM-CENTRIC PERSPECTIVE The system-centric classification considers the characteristics and properties of the system that is used in the WSN. They are also known as hard faults.

2.2.1 Calibration fault Calibration is a major cause for faults in WSN. Many papers talk about the difficulty in calibrating the sensors. Calibration errors give rise to gain faults, drift faults and offset faults. Drift faults occur when the performance drifts away from original calibration formulas.

2.2.2Battery failure Battery failure is a major cause for faulty data. Depletion of the batteries leads to transmission of faulty data by the sensors. Most of the faults in the sensor data are caused by battery failures.

2.2.3 Hardware failure Communication and hardware failures occur due to the mal function of hardware components of WSN. These are mostly permanent faults that require the replacement of faulty hardware. As WSNs are deployed in harsh conditions hardware errors are quite frequent. One such instance of hardware fault is when the hardware short circuits due to the presence of water content

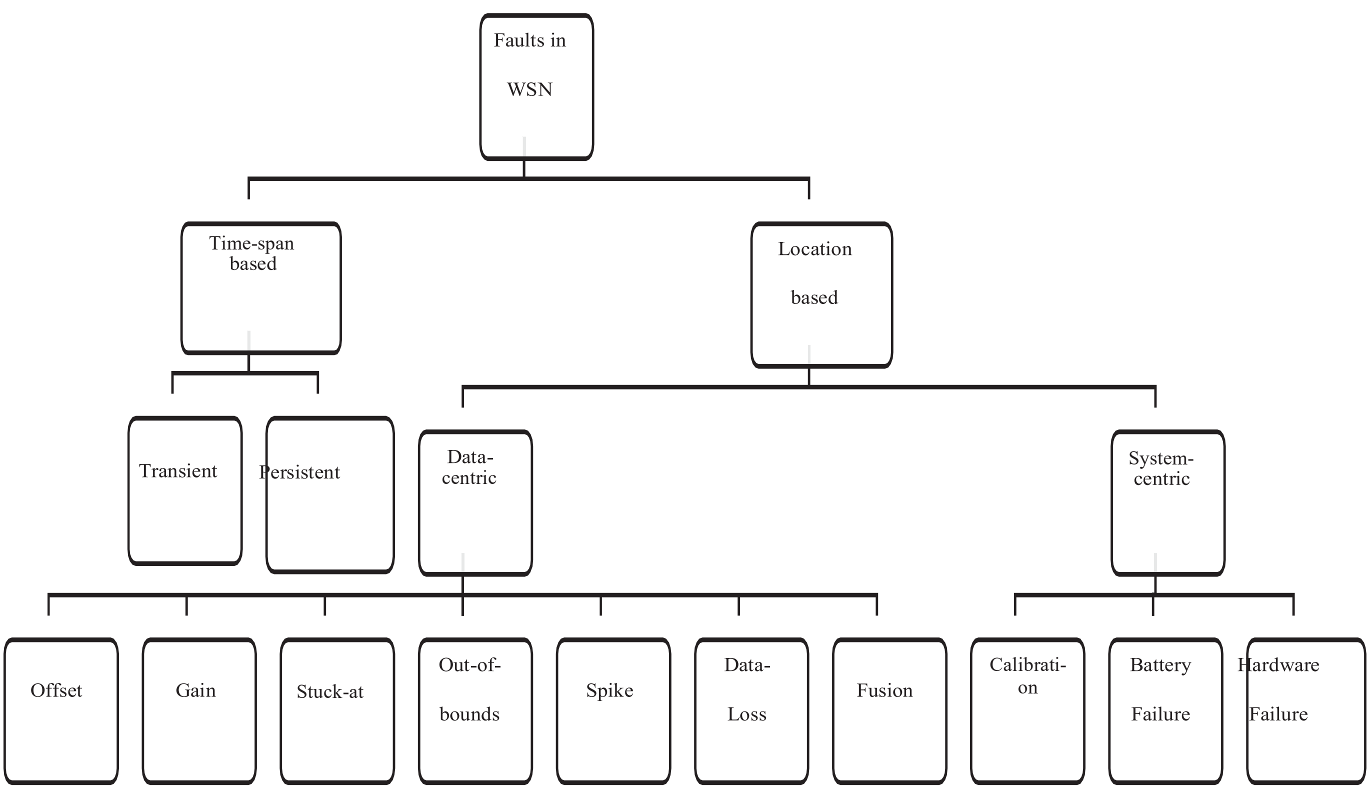

Fig.1: Taxonomy of faults in WSN.

FAULT DETECTION TAX

In recent couple of years, the popularity and use of wireless sensor networks have grown in leaps and bounds which ensued in the advancement of fault detection techniques. This provides us a motivation to develop a new taxonomy for wireless sensor network based on detection techniques. In this section, we discuss a new classification of fault detection techniques.

Fault detection techniques can be broadly classified into centralized, distributed and hybrid as shown in Fig. 5. The centralized approach consists of single central node or base station which monitors and analyses the condition of remaining nodes. Centralized approach increases the traffic in the network and ensues in network congestion, which resulted in Distributed approaches. In distributed approach, the task of monitoring and analysis is distributed among each node in WSN. A fault detection algorithm is run at each node to produce a localstatus of the node which is propagated throughout the network. Hybrid techniques combine both distributed and centralized approaches. These approaches create a multi-tiered WSN architecture which combines both centralized and distributed aspects.

Centralized approach can be classified into three categories: (1) statistics based and (2) soft computing based. Statistic based techniques use statistic techniques such as mean and sigma test. The soft computing-based algorithms are algorithms that are mainly based on machine learning techniques. Distributed approach can be further classified into six categories: (1) neighbourhood-based, (2) statistics-based, (3) probability-based, (4) soft computing-based, (5) self-detection and (6) cloud-based. Wireless sensor data are spatiotemporally correlated. The data obtained at an instance is related with previous and succeeding data. Similarly, there is a relation between sensor data from sensors in a geographically close proximity. Neighbourhood techniques use the spatial–temporal correlation between the nodes to detect faults in sensor reading. Neighbourhood techniques can be classified into Majority voting and Weighted Majority voting. Majority voting considers the majority of fault status of neighbouring nodes to determine the fault status of nodes. Majority weighted algorithm uses a weightfor each node in WSN and collects weighted votes from all the neighbouring nodes, and gives the prediction that has a higher vote.

Statistical algorithms are the algorithms that use statistical techniques to detect the outliers in the data. They can be categorized further into three categories namely Time-series analysis, Descriptive statistics, and Bayesian statistics. Time-series technique analyses time series data to detect similarities in the data and measure the amount of deviation. They use tests such as Komarov–Smirnov test and Kuiper testto detect outliers in wireless sensor data.

FAULT DETECTION TECHNIQUE

4.1 Distributed approaches

Feng et al. (2014) proposed a distributed fault detection algorithm based on weighted distance. In this algorithm, the weighted sensed value of a node is compared to original sensed value to judge faulty nodes. For a given node si, having neighbours sj, they compute the weighted distance from node si to node sj using the formula ρ = ∑ (1/ − 1)(1 − (( ) / M Es Es ∑ ( ))) i j M i j j M =1 =1 i j w where M is the number of neighbouring nodes of node si, E ( ) si j is the distance between the nodes si and sj and ρi is the weighted distance from node si and all of its neighbours sj. Then the weighted values for the nodes si is defined as x′ =i ρ xi j where xj is the sensed value of node sj and x′i is the weighted value. After that, they compare the weighted value of the node si and the original data at si with a fixed parameter. If the absolute difference between xi and x′i is less than the parameter, then the node si is assumed to be correct else it is declared faulty. The authors discuss the detection of data faults such as gain faults, stuck-at faults, and offset faults.

APPLICATION OF WSN:

1. **Area Monitoring**: It is a common application of WSNs. Here the WSN is deployed over a region where some event is to be monitored. A

military example is the use of sensors to diagnosis enemy intrusion. When the sensors detect the event being monitored, the event is reported to one of the base stations, which then takes relevant action. Similarly, wireless sensor networks may use a range of sensors to detect the presence/absence of vehicles ranging from motorcycles to train cars.

2. **Environmental Monitoring**: Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens. Wireless sensor networks can also be used to reduce the temperature and humidity levels inside greenhouses.
3. **Medical Application**: Sensor networks may also be broadly used in health care centres. In some modern hospital sensor networks are designed to supervise patient physiological data, to reduce the drug administration track and monitor patients and doctors inside the hospital.
4. **Structural monitoring**: Wireless sensors are used to monitor the movement within large buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc.
5. **Traffic Monitoring**: The sensor node has a built-in magneto-resistive sensor that measures changes in the Earth's magnetic field caused by the existence or passing of a vehicle in the proximity of the node. By placing two nodes a few metres apart in the direction of traffic, accurate individual vehicle speeds can be calculated and reported.
6. **Habitat Monitoring**: The intimate connection with its immediate physical environment allows each sensor to provide localized measurements and detailed report which is hard to obtain through traditional instrumentation.

CONCLUSION:

The outcome of the distributed localised faulty sensor detection algorithm is that each sensor node identifies its own status to be either “good” or “faulty” and the claim is then supported or reverted by its neighbours as they also evaluate the node behaviour. The outcome of the simulation results will show that the time consumed to find out the faulty nodes in our algorithm is relatively less than that of other approaches.

REFERENCE:

1. Z. Huang, et al., “A benchmark and comparative study of video-based face recognition on COX face database,” IEEE Trans. Image Process., vol. 24, no. 12, pp. 5967–5981 https://doi.org/10.1109/TIP.2015.2493448
2. F. Ciccozzi, I. Crnkovic, D. Di Ruscio, I. Malavolta, P. Pelliccione, and R. Spalazzese, “Model-driven engineering for mission-critical Iot systems,” *IEEE Software*, vol. 34, no. 1, pp. 46–53
3. F. Ciccozzi and R. Spalazzese, “MDE4Iot: supporting the Internet of things with model-driven engineering,” in *Intelligent Distributed Computing X. IDC 2016. Studies in Computational Intelligence, vol 678*, C. Badica, A. El FallahSeghrouchni, A. Beynier et al., Eds., pp. 67–76, Springer, Cham.
4. EARN project, http://www.crns.rnrt.tn/event/earn-2015.
5. A. L. S. Saabith, M. M. M. Fareez, and T. Vinothraj, “Python current trend applications-an overview,” *International Journal of Advance Engineering and Research Development*, vol. 6, no. 10.
6. A. S. Toor and A. K. Jain, “A survey on wireless network simulators,” *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 1, pp. 62–69.