Failure Node Detection in WSNs: A Survey

A. Sekar[1],
PG Scholar,
Department of Computer Science and Engineering,
P.S.R Engineering College, Sivakasi

R. Palanikumar[2]
Assistant Professor,
Department of Computer Science and Engineering,
P.S.R Engineering College, Sivakasi

Abstract:- **Wireless sensor network (WSNs) consist of large number of sensor nodes with monitoring and data transmission capabilities.WSN are used in military applications, positioning and tracking, localization of sensor nodes etc. These sensor nodes used to communicate with their neighbor nodes using radio signals. The QoS of such WSNs is mainly affected by the failure of sensor nodes. In order to maintain the QoS in wireless sensor network, identifying such failure nodes are essential. In this paper, various approaches of failure node detection were analyzed; advantages and disadvantage of each approach also were highlighted. Furthermore, new failure detection technique matrix calculus was discussed.**

Keywords- Monitoring Paths, Round trip delay, Round trip path

I. INTRODUCTION

Wireless sensor network with large numbers of portable sensor nodes has potential applications in a variety of fields, like surveillance, home security, military operations, medical, environmental and industrial monitoring. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication, and energy resources. WSNs are a trend of the past few years, and they involve deploying a large number of small nodes. The nodes sense environmental changes and report them to other nodes over flexible network architecture. Sensor nodes great for deployment in hostile environment or over large geographical areas, the sensor nodes leverage the strength of collaborative efforts to provide higher quality sensing in time and space as compared to traditional stationary sensors. Sensor nodes consists of processing capability (one or more microcontrollers or CPUs), may contains multiple types of memory (program, data and flash memory),have a RF transceiver(usually with single Omni directional antenna) ,have power source(batteries and solar cells),and accommodate various sensors and actuators.

Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external base station. A base- station may be a fixed node or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data. The data analysis based on such faulty sensor node will become incorrect or deviate from the mean value. This will eventually degrade the quality of service (QoS) of WSNs. The sensor node in the WSNs can become faulty due to various reasons such as battery failure, environmental effects, hardware or software malfunctions. In order to maintain the QoS in wireless sensor network, identifying such failure nodes are essential.

II. CHALLENGES IN WSNS

A. Reliability

WSNs are wireless networks and are therefore vulnerable to problems like packet loss. Nevertheless, they are used in areas such as chemical attack detection, in which these problems could easily lead to serious catastrophes.

B. Power Consumption

The nodes of WSN are usually battery powered because of their size. This limits the lifetime of node and raises the topic of energy-efficient in all aspects.

C. Mobility

Many applications urge the factor mobility into WSN challenges. For example, commercial applications, like vehicle tracking need networks that are able to constantly change its routing paths and infrastructure.

D. Node size

Miniaturization is the keyword in many studies about WSNs. Developing smaller nodes, with the same or even more efficiently than their bigger brothers is still a challenge, even present sensor nodes ,are hardly as big as a coin.

E. Privacy and Security

Unlike wired channels, wireless channels are accessible to both, legitimate and illegitimate users.

III. IMPORTANCE AND NECESSARY

Study the fault detection methods for nodes in WSNs for the following reasons.

- Massive low-cost sensor nodes are often deployed in uncontrollable and hostile environments. Therefore, failure in sensor nodes can occur more easily than in other systems;
- The applications of WSNs are being widened. WSNs are also deployed in some occasions such as monitoring of nuclear reactor where high security is required.
- It is troublesome and not practical to manually examine whether the nodes are functioning normally;

- Correct information cannot be obtained by the control center because failed nodes would produce erroneous data.
- Nodes are usually battery-powered and the energy is limited, so it is common for faults to occur due to battery depletion.

IV. A SURVEY OF DETECTION APPROACHES

A. Distributed Fault Detection (DFD)

DFD node fault detection scheme proposed by Jinran Chen determines the status of node by testing among neighbor nodes mutually. In this approach checks out the failed nodes by exchanging data and mutually testing among neighbor nodes in this network, but the fault detection accuracy of a DFD scheme would decrease rapidly when the number of neighbor nodes to be diagnosed is small and the node's failure ratio is high[1].

Neighbor node: The two nodes are neighbor nodes if the distance between them is within a single hop's communication scope. The set of all neighbors of node *Si* is *Neighbor* (*Si*) and the total number of neighbors of node *Si* is noted as *Num* (*Neighbor* (*Si*)).

B. Neighbor-Based Malicious Node Detection

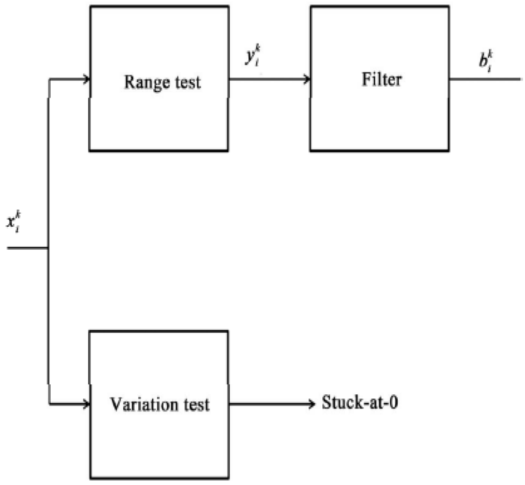

Fig. 1 Filtering

This approach has been proposed by Sung-ib Yim. Malicious nodes are modeled as faulty nodes behaving intelligently to lead to an incorrect decision or energy depletion without being easily detected. Each sensor node makes a decision on the fault status of itself and its neighboring nodes based on the sensor readings.

In detecting malicious nodes in the presence of faults and events, we employ a smoothing filter and confidence level evaluation to enhance the malicious node detection rate. A filter is used to correct some false readings due to transient faults [2].

C. Agent-based Fault Detection Mechanism

Agent-based approaches have been proposed for efficient dissemination in WSNs. The agent architecture consists of knowledge base and executable components. The knowledge base contains the information about the WSNs environment such as packet-store table and topology structure [3]. The packet-store table is composed of the received packets from target sensors; the agent maintains the topology structure of reverse multicast tree as well. The learning component provides the agent with the capability to monitor observations stored in its knowledge; thus to update agent routing mechanism. The scheduler component provides the agent with a time agenda to agent to exchange messages with other agents. Start and stop certain activities such as monitoring and aggregating.

The communication component allows the agent to exchange messages with other agents problem solver is an intelligent component of the agent. It includes fault-detection inference engine and fault-avoidance component. Fault detection inference engine utilizes the information in knowledge base to infer the working states of sensor nodes in tree.

D. Failure Detection Based on RTD

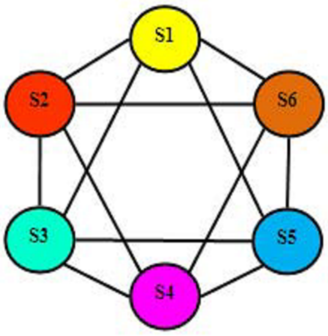

Fig. 2 Circular topology WSN with six nodes

RTD Estimation:

RTD time mainly depends upon the numbers of sensor node present in the round trip path and the distance between them. Selecting minimum numbers of sensor nodes in the RTP will reduce the RTD time. The round trip path (RTP) in WSNs is formed by grouping minimum three sensor nodes. Hence the minimum round trip delay time (τRTD) of RTP with three sensor node is given by

$$\tau\text{RTD} = \tau 1 + \tau 2 + \tau 3$$

Maximum Selection of RTPs:

Faulty sensor node is detected by comparing the specific RTPs to which it belongs. More numbers of sensor nodes in the round path will reduce the RTPs created. But due to this individual sensor node will be present in more RTPs. While detecting faults, comparisons of all such RTPs become necessary. This will delay the fault detection process. The numbers of RTPs formed with 'm' sensor nodes in maximum approach is given by

$$P = N (N - m)$$

Linear Selection of RTPs:

In order to reduce the RTPs in the fault detection analysis, instead of considering maximum numbers of RTPs, only few paths corresponding to the number of sensor nodes in WSNs are sufficient. We can select the RTPs equal to the numbers of nodes in WSNs to reduce the analysis time. RTPs selected in this way are called as linear RTPs because of the linear relationship between N and P. comparison of such linear RTPs is sufficient to detect the faulty sensor node. The linear RTPs in WSNs with N sensor nodes can be written as

$$P_L = N$$

Discrete Selection of RTPs:

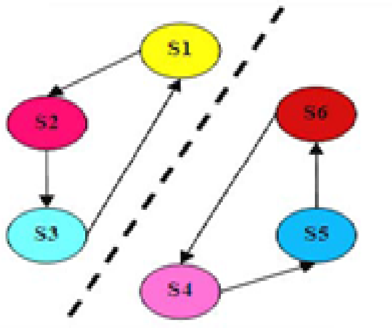

Fig. 3 Discrete RTPs

Discrete RTPs are selected by incrementing the source node value by three and their respective RTD times are measured by using the subroutine. The highest value of RTD time measured during the execution of first phase is selected as the threshold RTD time for all discrete RTPs in WSNs. In the second phase of fault detection, instantaneous RTD time of discrete RTPs is compared with the threshold time. Discrete RTPs whose RTD time is found to be greater than threshold time is then analyzed in detail. This particular discrete RTP is examined in three stages to locate the exact position of fault.

$$P_D = Q + C$$

Q and C in above equation are expressed as below

$$Q = \lfloor N/m \rfloor$$

$$C = \begin{cases} 0 & \text{if } R = 0 \\ 1 & \text{otherwise.} \end{cases}$$

Where Q is the quotient, m is the numbers of sensor nodes in RTP, R is remainder, N is numbers of sensor nodes in wireless sensor networks and C is correction factor to be added. Correction factor will be 0 if remainder is 0 otherwise it is 1.

Faulty sensor node is detected by measuring the round trip delay (RTD) time of discrete round trip paths and comparing them with threshold value. Algorithm is executed in two phases, first phase is used to decide the threshold value of RTD time and fault is detected in the second phase [4]. In the first phase all sensor nodes in WSNs are considered as working properly.

TABLE I

RTPs Comparisons for Maximum, Linear and Discrete Methods for Various WSNs

Round Trip Paths	Numbers of sensors nodes (N) in WSNs 6	10	20	40	60	80	100
P_M = N(N-m)	18	70	340	1480	3420	6160	9700
P_L = N	6	10	20	40	60	80	100
P_D =	2	4	7	14	20	28	34

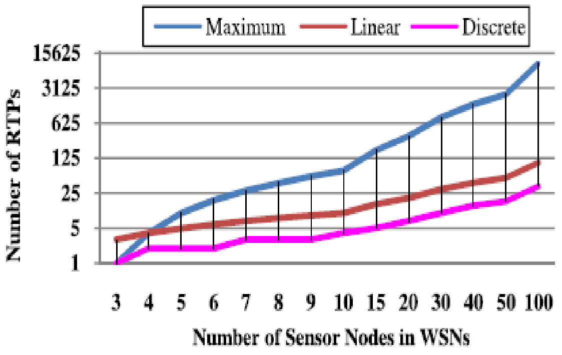

Fig. 4 Comparison Graph

V. A DISCUSSION OF NEW APPROACH PROPOSAL

A. *Matrix Calculus*

In matrix calculus, assuming the available node into matrix form and generate the RTPs by combining the nodes in order to row and column. Comparing RTD time of each RTPs with threshold value and find failure round trip paths. By comparing the failure RTPs nodes and find multiple failure nodes.

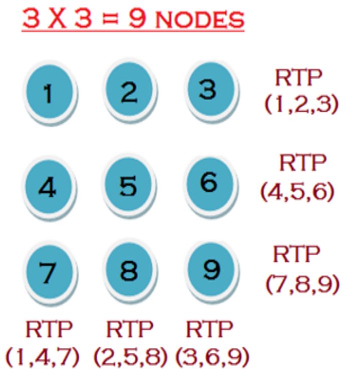

Fig. 5.Illustration of Matrix Calculus RTPs

Round Trip Delay:

The round-trip delay time (RTD) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received.

Round Trip Path:

The available nodes are combined as a group with minimum of 3 nodes and form a circular topology.

Threshold Time:

Initially all sensor nodes in WSNs are assumed as non faulty (working). The maximum round trip time of discrete RTPs is assigned as threshold time.

Formula for RTP Generation:

$$\text{RTP Generation} = \frac{N}{m} * 2$$

N- Number of Nodes, **m**- Nodes per RTP

2- Specifies *Column* and *Row* (2 sets of RTPs)

Advantages of Matrix Calculus:

- RTP generation is much easier.
- Detect multiple failure nodes from single RTP.
- Reduce the RTPs in the fault detection analysis

TABLE II Matrix Calculus Statistics

No of Nodes	No of RTPs	Failure Nodes
9	6	3
18	12	6
27	18	9
36	24	12
45	30	15
54	36	18
63	42	21
72	48	24
81	54	27
90	60	30
99	66	33

No of RTPs *Versus* Failure nodes

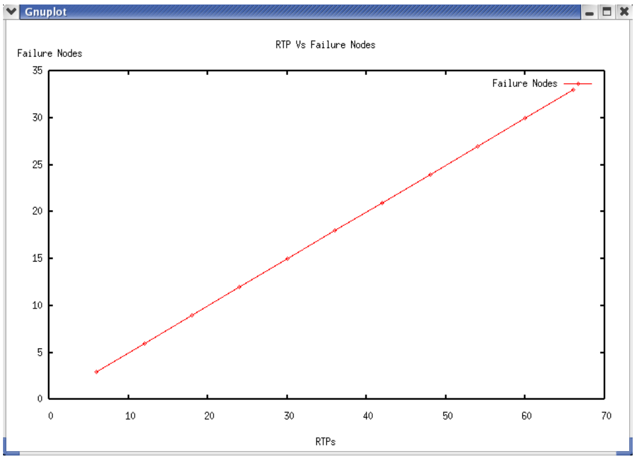

Fig 6. Statistics Graph

VII. CONCLUSION

In this paper, comprehensive surveys of failure sensor node detection approaches in WSNs which have been presented in the literature were described. They have a common objective of trying to find the failure sensor node and increase QoS of the network. Various approaches of failure node detection were analyzed; advantages and disadvantage of each approach also were highlighted. Furthermore, new failure detection technique matrix calculus was discussed. Compared to the discrete approach, matrix calculus method will find multiple failure nodes.

VIII. REFERENCES

[1] A New Method for Node Fault Detection in Wireless Sensor Networks, Peng Jiang , Sensors 2009, 9, 1282-1294; doi:10.3390/s90201282

[2] Neighbor-Based Malicious Node Detection in Wireless Sensor Networks, Sung-Jib Yim, Yoon-Hwa Choi, Wireless Sensor Network, 2012, 4, 219-225

[3] Agent-based Fault Detection Mechanism in Wireless Sensor Networks, Elhadi Shakshuki, Xinyu Xing, Haiyi Zhang

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

[5] R. N. Duche and N. P. Sarwade, "Sensor node failure or malfunctioning detection in wireless sensor network," ACEEE Int. J. Commun., vol. 3, no. 1, pp. 57–61, Mar. 2012.

[6] M. Lee and Y. Choi, "Fault detection of wireless sensor networks,"Comput. Commun., vol. 31, pp. 3469–3475, Jun. 2008.

[7] K. Sha, J. Gehlot, and R. Greve, "Multipath routing techniques in wireless sensor networks: A survey," Wireless Personal Commun., vol. 70, no. 2, pp. 807–829, 2013.

[8] P. Jiang, "A new method for node fault detection in wireless sensor networks," Sensors, vol. 9, no. 2, pp. 1282–1294, 2009

[9] Full Length Research Article, Efficient Way To Detect Fault Node Using Round Trip Delay, Sundaramoorthy, K., Kaviyarasi, G. and 3Dr. Srinivasa Rao Madhane, S. International Journal of Development Research,Vol. 4, Issue, 4, pp. 919-922, April, 2014