www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-3, June 2017

Research Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Detection of Faulty Sensor Node within Wireless Sensor Network for improving Network Performance

Tejashree Phatak[1*], S.D. Sawarkar[2]

[1*]Electronics Engineering, Datta Meghe College of Engineering, Airoli, India
[2]Electronics Engineering, Datta Meghe College of Engineering, Airoli, India

Corresponding Author: tejashreephatak786@gamil.com

Received 16th Mar 2017, Revised 30th Mar 2017, Accepted 26th Apr 2017, Online 30th Jun 2017

***Abstract*—**In most of application such as Habitat and Ecosystem- tem Monitoring, Seismic Monitoring, Civil Structural Health Monitoring, Monitoring Groundwater Contamination, Rapid Emergency Response, Industrial Process Monitoring, Perimeter Security and Surveillance Automated Building and Climate Control it is essential to observe or monitor the behavior of surrounding environment at a fine resolution over large spatial-temporal scales for this reason wireless Sensor Network (WSN) is used. WSN have high ability to connect physical world to the virtual world and sensor devices are tiny device and low battery devices due this use of wireless sensor network for monitoring surrounding behavior is increased time to time. Accuracy of WSN is enhanced by increasing the no of sensor within the network. As no of sensor increase this will increase the probability of failure of sensor within the network because WSN may be operated in unattended and hostile environment .If any of the sensor node is fails, this will lead to the change the network topology, also create network partitioning , increases distance between node pair and reduce the number of alternative available routes. In short it will degrade Network Performance of WSN, to improve network performance of WSN we have to find out faulty sensor node within the network. This paper will give one easy method for finding faulty sensor node within the network. This method measure Round Trip Time (RTT) of Round Trip Path (RTP) and compare the calculated RTT with threshold value(threshold value for RTT) if premeditated RTT is greater than threshold value or infinity then particular node from that respective path is declared as dead node or malicious node.

***Index Terms* —** Faulty sensor node, Network Performance, Round Trip Time, Round Trip Path

I. INTRODUCTION

WSN is made up of the tiny, low-power sensing element (sensor node). Sensor nodes within the WSN are used to sense the changes in surrounding environment such as temperature, sound, pressure and this sensor node sends the sense information to the observer for processing and analyzing. Sensor node is heart of WSN. Sensor node has to perform various functions like communication, storage, computation. Basic block diagram of typical sensor node is shown in fig 1. This sensor node normally consists of power supply unit, sensor, and analog to digital converter, processor, storage and mobilizer/actuator.

Some of the key general indicators of sensor network performance are connectivity, distance between node pairs, and number of alternative routes [10]. Such sensor node has to be operating in harsh and uncontrolled environment this may lead to make fault in sensor node. If any one of the sensor node in network became faulty then overall operation of WSN is suffers from erroneous result of faulty sensor node this will increase traffic and waste the limited energy.

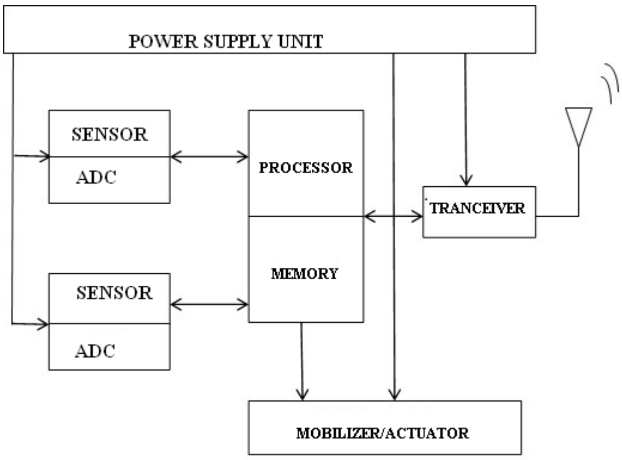

Fig.1. Typical sensor node

If any node in network is become faulty then distance between the nodes is increased as we know that for effective transmission of data in the network, required shortest path between source and destination. Average of all pairs of shortest path provides global measure of best connectivity across the whole network [10]. If node in the shortest path is become faulty then ultimately that shortest path is damage and this will affect the overall quality of the network and throughput. In fact faults in sensor node can affect quality of service of WSN. Effect of faults can be in form of human life, environmental impingement or economic loss. In military application WSN is most widely used for monitoring terrorist moment in remote areas and force protection. If faults exceed the margin level, then system may break down. In such application sensor node within the network are used to sense and discover the geographic region to forecast disasters before they occur. For example earthquake, tsunami, flooding. If one of the sensor node become faulty, then network may get divided and system oblivious of alarming situation. In medical application WSN used to sense the diseased persons condition and give that information to the doctor who is present at remote place, such a systems are most useful for person who is staying alone at home. In such an application sensor are attached to different part of body. If there is error in output of sensor might result in the misinterpretation of the daily extant activities of the person being monitored. In industry for monitoring operation of machines, machines are equipped with temperature, pressure and vibration sensors. Faulty monitoring sensors may not permit the system to activate the alarm which may lead to complete breakdowns and in turn economic burdens to industry. In target tracking application sensors are equipped on moving targets to track them in real time. For example VANET vehicular ad-hoc network in such application sensors are placed on vehicle for assurance to the secure and efficient transport system. In such an application if fault is occur that may lead to life-threatening events.

The basic sources of failure in sensor node are calibration error, malfunctioning hardware, hostile environment, low battery and link failure.

This section entails about introduction of WSN, sensor node faults and effects of fault in network. Detail existing methods are given in section II. Section III consists of methodology and design idea of proposed system. Section IV is conclusion.

II. LITURATURE SURVEY

To improve performance of WSN, it is essential to find faulty sensor node within network. So many methods are al- ready exits for finding faulty sensor node like watch-dog timer approach, centralized approach, Node-self detection approach, Cluster-based approach, Neighbor Co-ordination Approaches and Soft-computing approach. Watch-dog timer approach explain in paper [5] is Mitigating routing misbehavior in mobile ad hoc networks in this method watchdog timer concept is used to monitor the behavior of one hop neighbor. In this method watchdog tool is used to identify the faulty node. Here node obverses its one neighbor whether it is forwarding the packet just sent by overhearing, if neighbor node dose not forward the packet within predefined time period then consider that node is misbehaving. If misbehaving rate of that particular node is exceed above threshold then consider node is faulty. But this method is suffered from collision of data problem because information is transmitted in forward and reverses direction.

In paper [3] efficient tracing of failed nodes in sensor net- works explain centralized approach, in this one node is selected as base station or sink node and such node has to perform variety of operation. Base stations collect the information from each node of network regarding network topology. Once base station receive the network topology information it use those knowledge to find faulty node in network by using simple divide-and-conquer strategy based on adaptive route update messages[3]. Base station must know the near neighbors of each node. This method is dose not used in large area network because only one node has to perform variety of the operation due to this there is burden on single node this leads to rapid energy depletion in certain regions of the network.

Node-self detection approach explain in paper [11], in this method node itself finds its own fault by adding additional hardware and software. As we know that sensor node in wireless sensor network is low power device, because of additional hardware in the node will lead to increase hardware complexity, weight and energy requirement.

Fault Management Architecture for Wireless Sensor Net- work [7] and Cluster based failure detection and recovery Scheme [8] in wireless Sensor network those method uses cluster based approach. Each node has to send its energy update information to cluster head. In this method there is burden on the cluster head to perform fault finding operation this will lead to rapid depletion of its battery and require frequent re-clustering and this will affect network lifetime and scalability. This method is not applicable to the find malicious node.

Neighbor Co-ordination approach is explained in paper [2] in this method each node result is compare with its own neighbor. In this method time require to detect fault is much more and message complexity is also high because single fault finding process required more test round.

Soft-computing approach explained in paper [4] present an approach for detecting and identifying sensor node failure based on Principal Component Analysis (PCA), and wavelet decomposition. Complexity of this method is very high and this approach considers incorrect computation faults.

From the above mentioned methods, we studied that there is some limitations are present in every method. These limitations are in terms of complexity, energy consumption, time required for calculating faulty node, and some of method dose not calculate malicious node (attacker).

Proposed method uses round trip time (RTT), measurement of round trip path (RTP) and calculated RTT of RTP com- pare with threshold value .If calculated RTT is greater than threshold value then particular node of the respective path is declared as malicious node and if calculated RTT is infinity then particular node of the respective path is declared as crash node.

III. PROPOSED METHOD

In our proposed method our consideration is that system or network is symmetrical, means all nodes in the network are homogeneous node and they are operated in same environ- mental condition also they are placed at same distance. For given system we considered dual ring topology.

Main parameters of this method are Round trip time and Round trip path.

Definition of Round trip time: Round trip time (RTT) is the difference between time at which node transmit the information and time at which same node receive acknowledgement for that transmitted information. RTT is depends upon the no of hops present in the path. Relation between no of hop between path and RTT is proportional, if no of hop increases then RTT will increase.

1) Path selection.
2) Threshold round trip time calculation
3) Fault detection

Path5 = Node5-Node6-Node7

Path6 = Node6-Node7-Node8

Path7 = Node7-Node8-Node9

Path8 = Node8-Node9-Node10

Path9 = Node9-Node10-Node11

Path10 = Node10-Node11-Node0

Path11= Node11-Node0-Node1

Discrete path selection: for reducing no of RTP of linear path we adopt discrete path selection method. RTPs are selected in this method just by ignoring the two consecutive paths. Equation for path selection in this method are given by,

$$M_D = q + X \qquad (3)$$

Where,
M_D = Discrete RTP.
Q = quotient and given by,
Q=N/n (4)

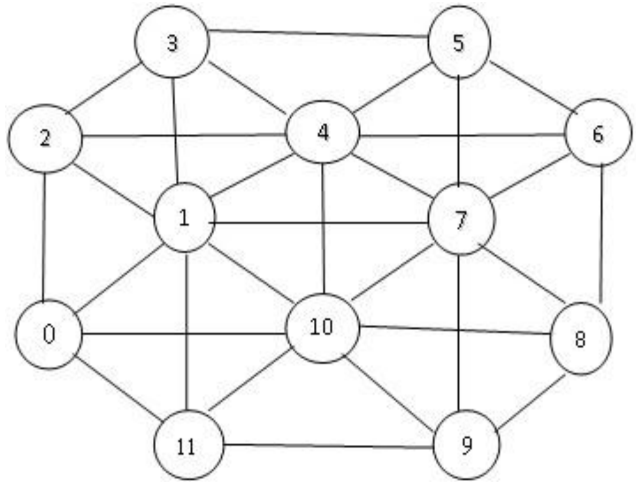

Fig. 2. Proposed topology

A. Path selection:

Where, N is number of sensor node and n is no of hop in RTP.
X = correction factor.

X = 0 if Remainder = 0 otherwise X = 1

Total no of Discrete paths are as follow

Path0 = Node0-Node1-Node2

Total no of path within topology can be calculated by equation shown below,

$$M = N(N - n) \qquad (1)$$

Where,

M = Total no of round trip path within topology.

N = Total no of sensor node within topology.

n = Total no node present in round trip path (no of hop). Topology shown in fig 3 has N=12, m=3 then RTP will be 108 by using equation(2) .If we consider RTP 108 for finding faulty node then this will increase overall time required for calculating faulty node in topology. Fault detection by analyzing RTT times of maximum numbers of RTPs will require substantial time and can affect the performance [1]. So that it is necessary to reduce the total no of RTP required for calculating fault and this can be achieve by using following method.

1) Linear path selection: In this RTPs are equal to no of node present in topology i.e.

$$M_L = N \quad (2)$$

Where,

M_L = Linear RTPs.

N = Total no of node presents in topology.

Given Topology has linear RTPs are 12 as follow.

Path0 = Node0-Node1-Node2

Path1 = Node1-Node2-Node3

Path2 = Node2-Node3-Node4

Path3 = Node3-Node4-Node5

Path4 = Node4-Node5-Node6

Path3 = Node3-Node4-Node5

Path6 = Node6-Node7-Node8

Path9 = Node9-Node10-Node11

B. Threshold round trip time calculation:

RTT time mainly depends upon the numbers of sensor node present in the round trip path and the distance between them [1].It is estimated by considering initially all sensor nodes in WSNs are working properly. Calculate RTT for discrete paths and highest value of RTT between all calculated RTTs set as threshold value.

C. Fault detection:

Fault detection is performed for two types of fault 1. Crash fault: This node is completely dead which does not take part in network activity 2.omission fault: This node adds some amount of delay in transmission of data.

Fault detection is performed by making any node in WSN as crash or omission node. And then compare calculated RTT with threshold value.

If RTT of particular paths is infinity then respective node of that path is declared as crash node.

If RTT of Particular paths are Greater than threshold value then declared that respective node of that path is omission node.

IV. RESULT

A. All nodes are working properly

Threshold value for round trip time is 20.25ms as shown in fig 3

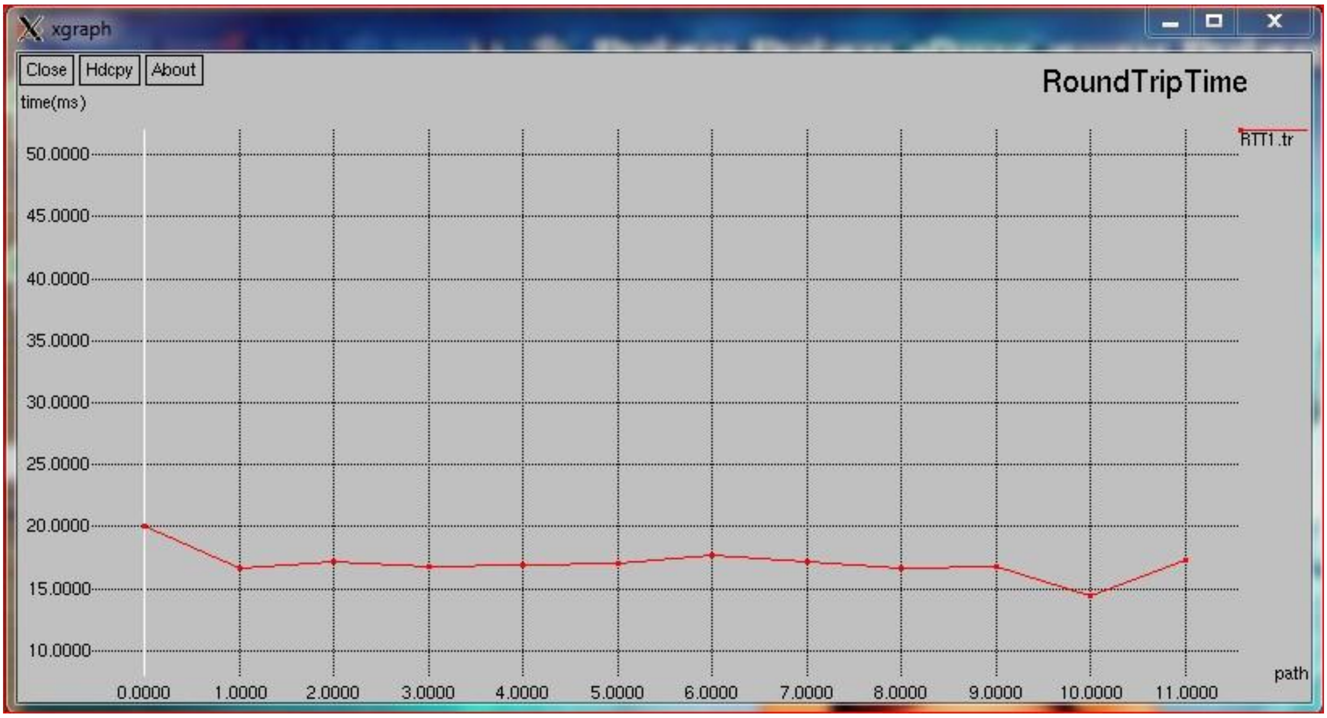

Fig. 3. All nodes are working properly

B. Node 7 is crash node

Due to node 7 is faulty Path5, Path6 and path7 has RTT which is equal to infinity as shown in fig 4

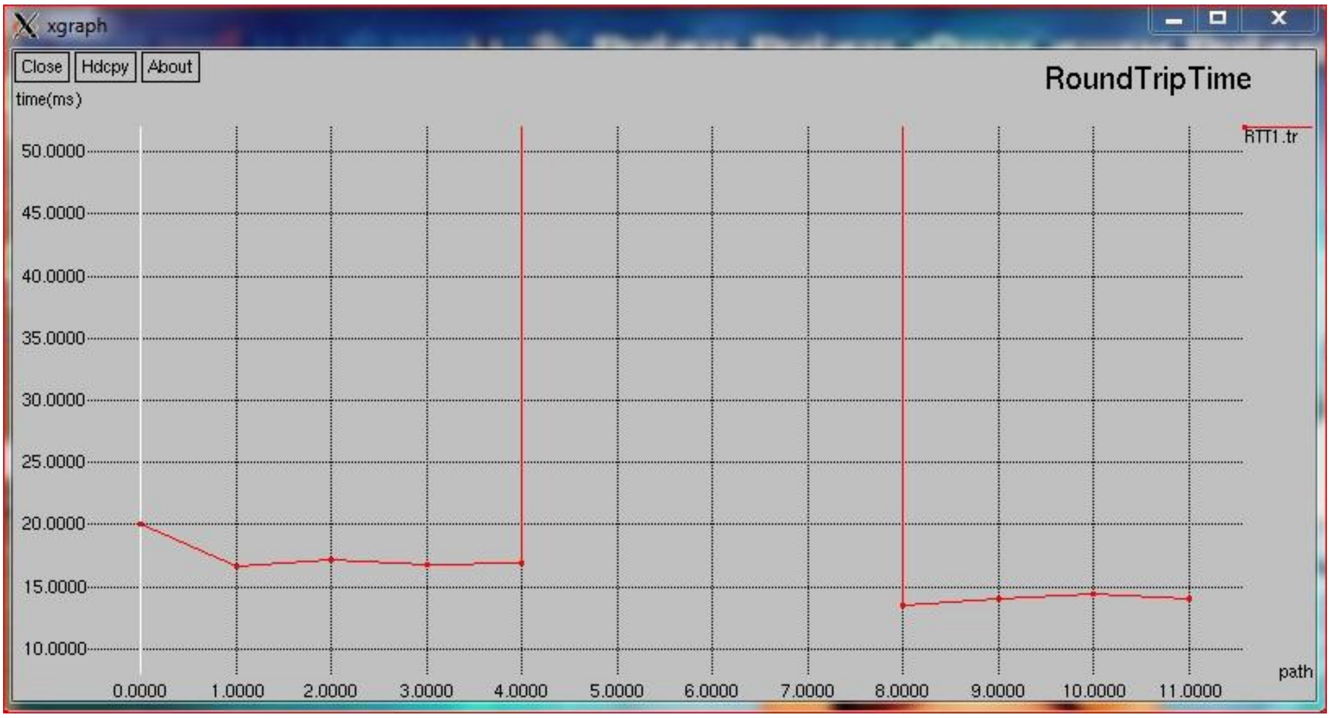

Fig.4 Node 7 is crash node

C. Node 7 is omission node

In this fault RTT value for Path5, Path6 and Path7 are 76.28 ms, 46.81 ms and 77.09 ms respectively which are greater than threshold value as shown in fig 5

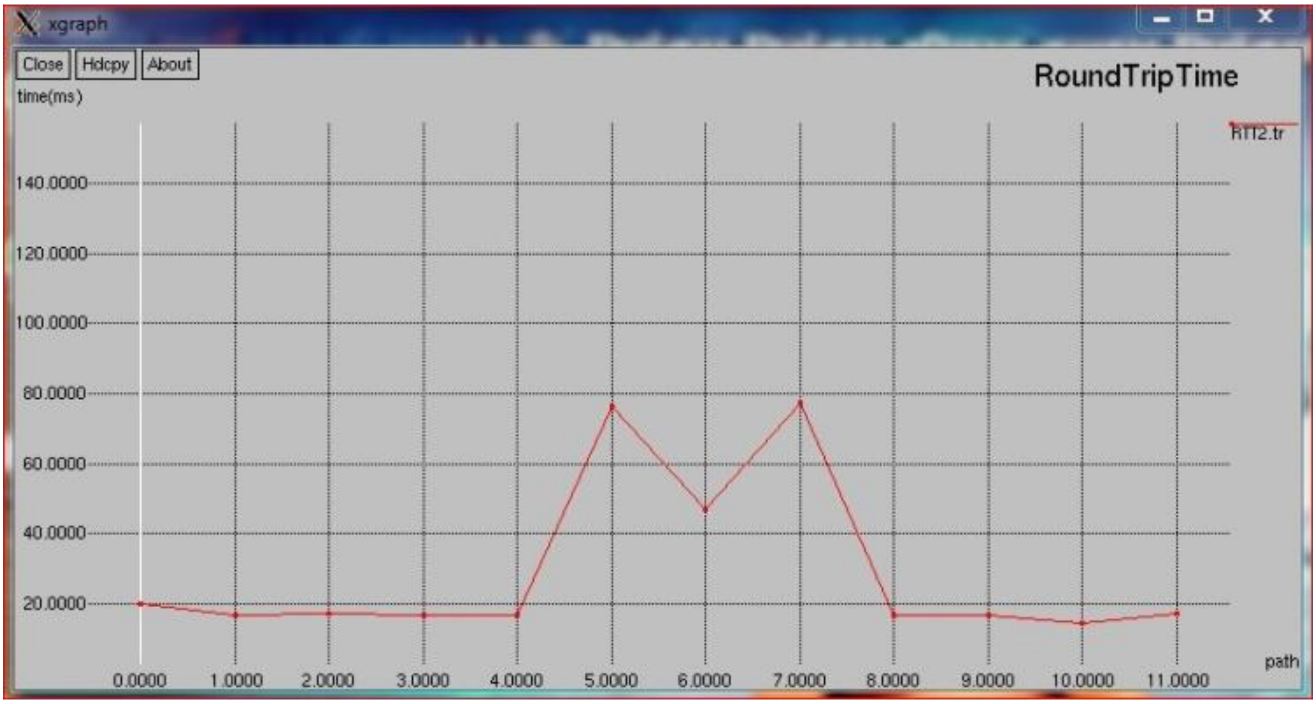

Fig.5 Node 7 is omission node

V. ANALYSIS

In proposed system fault calculation is performed on dual ring topology in which Round Trip Time is measure and measurement of RTT is sufficient for detection of faulty node. Because of considering discrete path mechanism, latency of proposed system is minimum as compare with other method and in this method there is no any extra burden on any signal node in the network for any calculation due to this reason there is no depletion of battery of any node so that scalability and lifetime of the network is not affected. As complexity of the system is very much less and does not require any extra hardware.

The proposed system find crash node which is dead due to hardware problem or node is completely damaged such a node does not take participation in transmission of data in network. This system also calculate omission node which takes the participation in network activity but does not transmits the data on given time such node introduce additional delay in network and such activity is done by attacker to disturb the network performance.

VI. CONCLUSION

This method improves latency which is required for finding fault. This method not only calculate crash node but also calculate omission node. Complexity of system is also less as compare with existing method. Scalability of the method is very much high. The use of discrete RTPs in the proposed method enhanced the efficiency of fault detection process.

REFERENCES

[1] RN. Duche, Nisha P. Sarwade, "*Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs*" IEEE SENSORS JOURNAL, VOL. 14, NO. 2, pp. 455-464, 2014.

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

[3] Enakshmi Nandi and Debabrata Sarddar, "*A Modified MapReduce-K-Means Clustering Based Load Distribution Method for Wireless Sensor Network in Mobile Cloud computing*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.8, pp.107-110, 2016.

[4] X.-L. Zhang, F. Zhang, J. Yuan, J. lanWeng, W. hua Zhang, "*Sensor fault diagnosis and location for small and medium-scale wireless sensor networks*", in Sixth International Conference on Natural Computation, China, pp.3628 3632, 2010.

[5] S. Marti, T. J. Giuli, K. Lai, M. Baker, "*Mitigating routing mis- behavior in mobile ad hoc networks*", in Proc. 6th annual international conference on Mobile computing and networking, USA, pp. 255265.

[6] A mahapatro, P.M. Khillar , "*fault Diagnosis in wireless Sensor Networks: A survey",* in IEEE communication surveys and Tutori- als, Vol.15, No 4, pp.1-4, 2013

[8] H. Redwan, G. Akele, K.H. Kim, "*Cluster-based failure detection and recovery scheme in wireless sensor network*", 2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN), China, pp. 407-412, 2014.

[9] 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, 2012.

[10] S. Sharma, D. Kumar, K. Kishore, "*Wireless Sensor Networks-A Review on Topologies and Node Architecture*", International Journal of Computer Sciences and Engineering, Vol.1, Issue.2, pp.19-25, 2013.

[11] S.Anusuya and S.Meenakshi, "*An Improved Dynamic Source Routing Protocol for Detection and Removal of Black Hole Attack in Mobile Ad-Hoc Network*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.12, pp.112-117, 2015.