



Emergency Node Based Fault Tolerance in Wireless Sensor Networks

T.Gobinath^{1*}, A.Tamilarasi²

¹Assistant Professor, IT department, Chettinad College of Engineering & Technology, Karur, Tamilnadu, India.

²Professor and Head, MCA, Kongu Engineering College, Erode, Tamilnadu, India.

*Corresponding Author Email: 1gobinath19@gmail.com

Abstract

In Wireless Sensor Network (WSN), fault occur due to node failure, malicious attack and link failure. Link failure causes the loss of sensitive data in a network leads to the emergency situation and influence generated and incoming data resulting in high probability of erroneous data, false packet transmission, wrong decision making and rigorous communication interruption. It leads to increase of traffic overhead and faulty node count in the network. In order to avoid this problem Emergency Node(EN) based process is proposed. Simulation clearly shows that the proposed method increased the packet delivery ratio and decreased the average delay, Energy consumption in WSN.

Keywords: Fault Tolerant, Wireless Sensor Network, Emergency Node, Link Failure.

1. Introduction

In Recent Days, To Attain a common task of WSN sensor devices work together and report the gathered information to a sink through remote interface like wireless channel . The devices are registered and equipped with advanced detecting and transmitting abilities to increase the performance of the network [9]. Basic working of Sensor nodes is to collect, summaries and transmitting data to the destination (Sink) through the interface, where the sink can received data from the Source and processed . After processing the data, sink can back up it for further processing. Sink can discard data once data is not up to level(threshold). Information are then conveyed to the sink either occasionally or on-request through the sinks[17]. The regions of utilizations of WSN's differ from common, social insurance and natural to military. Cases of uses incorporate target following in combat zones, living space observing, common structure checking, forest fire identification and, industrial facility support. Uncontrolled situations were created because of deploying vast number of sensors[3]. In sensor nodes, fault may happen because of, off base condition of equipment or a program as an outcome of a disappointment of a components. Adaptation to internal failure has been sketched out among the real difficulties in WSNs in the new research zone of Collaborative Signal Information Handling (CSIP) [11]. Fault Occurring results non-uniform network topology because of energy consumption are ceaseless and as the time advances .The issues that can happen because of sensor node failures are misfortune in availability, delay because of the connection failure and delay ,due to lost connection of the system because of the hole made by the failed sensors[3,10] . Different types of faults are represent, for example, hub deficiencies, organize blames and sink faults[16,8].

Sensor node gets adaptated to non-critical failure and convey a coveted level of usefulness within the sight of issues is the capacity

of a framework [1]. In real time sensor network application, the sensor hubs are inclined to disappointment and, being adapted to non-critical failure. In this manner, to beat sensor failure and to ensure framework availability, broken hubs ought to be distinguished and proper measures to get back availability must be taken to suit for the failed node. Due to increase in node, every sensor hub is restricted with the power supply , and visit substitution of the batteries regularly and it is not functional [12,6,13].Fault identification and fault recovery are the main stages in fault management. In fault identification stage, a surprising disappointment ought to be legitimately distinguished by the system framework. The fault recovery stage is the phase at which the sensor organize is to rebuilt , such that faults or faulty nodes don't affect encourage on arrange performance[6,4]. The primary issue of previous fault identification and healing is a normal energy loss throughout fault identification and recovery process. Battery can be depleted soon and affect energy efficiency in WSN due to increase of traffic overhead and faulty nodes in the network size . So these defective hubs must be stayed away from the system and furthermore lost information must be recouped. To solve the mentioned problems, we present Emergency Node based fault tolerant technique. In our proposed method, Source node send sensitive data to sink through EN rather than the faulty relay nodes.

2. Related Works

In [6],the paper proposed a decentralized strategy for fault identification and recovery in bunched WSN to be specific DFMC which can enhance the throughput of system by introducing is energy efficiency.

For fault identification and utilizations the new energy effective strategy is used to identify fault in network, DFMC is used to recover from fault, for which it consume less energy. [4] Comes with another strategy for effective fault management that perform fault identification and fault recovery in network. For Distributed management it distinguish, analyze and recover the traffic overhead according to the increase of WSN size. In particular, In distributed



manner, grid based design grants the execution of fault identification and permits the report to be sent crosswise over cells. To perform management task gateway nodes, cell director are selected by every cell. With least energy utilization by Cell manager and gateway node can detect a fault node in network. They agree a identical task network, where every nodes must having same assets. Nodes are of equivalent assets also, can without much of a stretch move down each other if there should arise an occurrence of recuperation. Be that as it may, a data loss amid transmission and results a right node to be proclaimed as fault. [23] came with CRINet algorithm, a safe furthermore, fault tolerant information accumulation plot with a mass key organizing system. In order to attain high availability, data sensed by sensors are exchanged to the sink using multi path technique. EBS system is associated in CRINet for assemble enter management keeping in mind the end goal to diminish re-key endeavors. The CRINet conspire is prevalent as far as information secrecy and accessibility. Nonetheless, the fault tolerant ability isn't powerful. [14] introduced a nonexclusive and proficient adaptation to internal failure computation for WSNs. Rather than existing approaches, the calculation introduced in this paper is completely decentralized and would thus be able to be utilized to help completely autonomic fault resilience in sensor arrange situations. The proposed plot offers profoundly dependable fault recognition, with negligible system overhead. Be that as it may, there is no difference in failure node increment when time utilization does not have enormous distinction [22] Introduced a various structure to appropriately convey fault administration assignments amid sensor hubs by presenting more 'self-overseeing' capacities. Moreover, they too consider a substitute answer for self-reconfigure blame management capacity of sensor hubs adjusting to different framework necessities. Resulting the capability of fault recognition is therefore called tapering. likelihood based fault recognition calculation to choose sensor nodes as test stations by taking into consideration of the likelihood dispersion of sensor nodes and the fault appropriation data. It showed that the proposal can delay the lifetime of sensor organize by just giving up not many fault distinguished rate. The Pareto rule that few bunches contain the enormous majority of the shortcomings has moreover been illustrated, and to test station this standard has been connected with it. On the other hand the battery life time isn't proficient. [16] introduced a fault tolerant clustering mechanism, in which sub-cluster group and small cluster group were divided from the entire system is to empowering an extensive decrease of correspondence and processing overhead. To provide rough sensor information of the fault node a matrix based proposal was used as fault tolerant method. The estimated code expectation contemplates different geographical parts of the issue. Be that as it may, there happen sensor disappointments. In [23], It shows LeDiR method relying upon the neighborhood perspective of a sensor node about the system to involved a minimal number of node moves to recover the network and ensure that to avoid from multiple path moves. [24] Came with fault tolerant system for the grouped conventions. At first every one of the nodes were bunched utilizing the EEDC convention. At that point, the Cluster Heads achieved FTS alongside information collection. Three stages were in FTS: fault identification, fault determination and fault recuperation. Fault identification in the FTS intention was communication trade. Repetition was viably used and, where a way to deal with choose the extra CHs in which they chose save CHs were sufficient near the CHs.

3. Fundamental of Fault Tolerance

A. Failure in Wireless Sensor Networks

To grasp adaptation to non-critical failure systems, it is vital to bring up the distinguish between failures, Errors, and faults in network. [7][18] have been used various meaning for the above terms. A fault may said as any sort of imperfection that prompts a mistake. A

fault compares to a mistaken framework state. It leads to failure in network. A failure is symbol of an error, occurs when the System strays from its determination and can't convey its expected usefulness. The error is the condition of the administration in the wake of endeavoring to peruse the sensor information and Node does not transmit data to the sink with in specific time interval the failure happens. Two major events must be performed to strengthen the failure circumstances:

- 1) Fault discovery: To give countermeasures, A framework must perform the initial step to distinguish that a particular operation will be/is faulty.
- 2) Fault Recovery: Once the fault is detected by framework, the following stage is used to recover or prevent from it. The main method to accomplish this task is to imitate(copy) the segments of the framework that are key for its right task.

B. Source of Faults in WSN Applications

Finally, The application process in the back-end which introduces the WSN information to the clients that endures a fault because of certain equipment failure or software defect and the whole framework is viewed as defective.

- 1) Node Faults: Nodes have a few equipment and programming parts that can deliver malfunctions. For instance, the walled in area can endure effects and uncover the equipment of the sensor hub to the outrageous states of the earth.
- 2).System Faults: In WSN routing is most important building block. It is fundamental for gathering information, conveying programming and update configuration in node, and for organization nodes in network. Moreover, Required protocol must be application-specific, for tracking an object and "following" mobile items. Fault on the directing layer can prompt dropped or misinformed messages, or inadmissible postponements.
- 3).Sink Faults: On a larger amount of the system a device (sink) that gathers every one of the information produced by the system and return to the back-end framework. At the point when this device comes up short, unless fault tolerant estimations are available, a massive failure of the system happens given that the information from the sensor hubs can't be gotten to. The zones where has no power supply the sink can be sent there, battery and solar panel system both are used in this kind of applications [15][19][20] to give the measure of vitality important.

C. Fault Tolerance

Fault recovery procedures empower frameworks to keep working as indicated by their details regardless of whether shortcomings of a specific kind are available. There are numerous potential sources for faults in WSNs. Adaptation to internal failure strategies have been proposed in different settings that expansion the unwavering quality of the usefulness of sensor hubs in their particular area. The most well-known of many strategies is the replication of segments. It is increased the expense of network deployment cost due to high dependability and accessibility. As an option, WSN can be reduced to a worthy level of configuration of project.

4. Assumptions and Network Model

In [6], fault identification and recuperation isn't performed, likewise there happens normal energy misfortune among fault discovery and connection failure.

In [5], According to increase in WSN, the quantity of defective nodes and the activity overhead is expanded. In [2], an information can be gone among transmission and result an exact node to be pronounced as broken. In [23] the group head account all key resources of each gathering, along these lines if assemble head in source gathering has been bargained, assailant can listen in the detecting information. Likewise there is no fault recovery or identification. In [14], traffic overhead of traffic results higher

energy utilization, which leads to depletion of battery life time. In [22], in any case, the viability of fault identification is decreased. In [21], fault discovery rate is diminished of the likelihood based fault location systems thought about with other basic sensor systems. In [16], the fault discovery and recuperation isn't performed.

In our proposed method, we assume the model definition and some important configuration that will used in the follow-up.

1). N sensor nodes are uniformly distributed over a rectangular field of area R. The nodes are in Static position and denoted by (x_n, y_n) where $n=1,2,...N$.

2). Each node has a limited communication range R_s .

3).Set of K source nodes are in the same region R. At time T, source node k transmit data to sink via intermediate node $i_1, i_2, i_3, \dots, i_n$.

4).At time T_n intermediate node i_n get fail to relay the data received from k to sink.

All assumptions are relatively common and practical for sensor networks.

5. Proposed Method

In this paper, Emergency Node(EN) based Fault tolerance mechanism is designed for Wireless Sensor Network. WSN consist of sensor nodes with unique Sensor ID, which are inexpensive and highly constrained in processing capacity and energy utilization, relatively Emergency Node(EN) have more onboard energy supply and richer computation capacity and, it is used to transferred data to sink in emergency situation. Fig.1 depict the working principle of WSN at normal situation ,Source node sensed threshold data from environment, by using relay node data reached sink node. EN always idle and act as backup node to provide fault tolerance in WSN. Fig.2 shows error and recovery model of our proposed system. Here, Sensed data of source node will not reach sink through relay node due to failure of link in the routing path. In case of non emergency situation source node identify alternate path and transmit sensed data to sink , it cause delay in a network to provide fault tolerant. This paper consider with emergency situation like sensed data from environment which is very sensitive and consist of threshold value readings. In routing path, link between source and relay node is failed, source node attempt to resend data through the immediate alternate routing path is also failed at time "T_n".

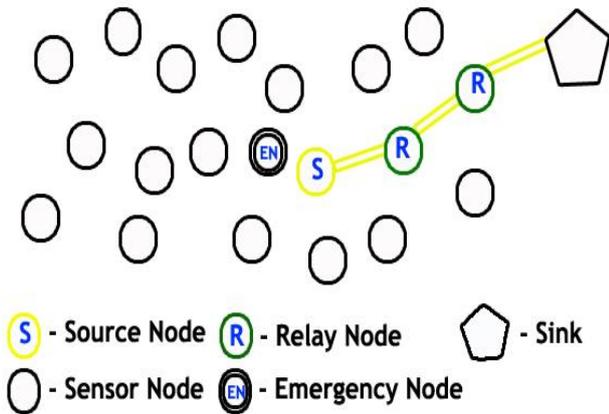


Fig. 1: Error Free WSN Scenario with Emergency Node

In this scenario, Source node send a request packet which consist of node ID, threshold Data and failure link information to the Emergency node. While deploying, EN Updated with threshold value of the sensing region. EN Received source node request and validate it by checking node ID, failure message and threshold value of the sensed data, after validate the data from source request packet and satisfied with all condition, EN transmit Source node data to Sink directly without delay, Once link failure validation failed, Emergency node rejects request from source node and add

node ID in malfunction table. EN validate link failure by sending and receiving beacon to the relay node.

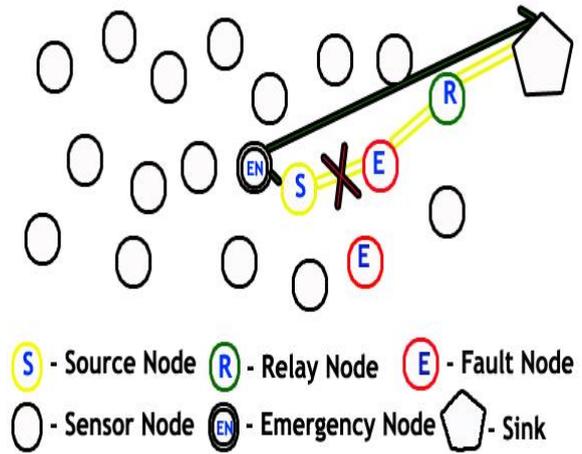


Fig. 2: Emergence Node based Fault Tolerant Method

Algorithm: Fault Tolerance by Emergency Node(EN) : Data Packets relayed from source and relayed by EN at Emergency situation

1. **Require :** Threshold Data(TD) from Source node , Route path Failure Confirmation(RFC) received by EN, Source request (Sr) consist of RFC and TD, En must have Threshold value (Tv)
2. **Ensure :** Ensure the data is sensitive or not
3. Source node transmit message to EN
4. Emergency Node Accept transmission to sink once following Conditions are satisfied ;
5. If $(Sr(ID)==1 \ \&\& \ En(Tv)==Sr(TD))$ continue;
6. If $(Sr(RFC)==1)$ continue;
7. Then
8. ENSendData of Sr(TD) to the Sink;
9. Else
10. Discard Sr;
11. Retransmit to Sr(ID);
12. Endif;
13. Else
14. DiscardSr;
15. AddSr(ID) in malfunction list;
16. Endif;
17. End;

6. Estimation of Metrics

A. Residual Energy: The residual energy (RE_j) of each node (N_j) after performing a data communication is expected using the subsequent formula:

$$RE_j = E_j - (E_{tr} + E_{re}) \tag{1}$$

Where nodes initial energy is E_j and E_{tr} and E_{re} are Energy utilization of nodes.

B. Average Distance: The average distance between the sensor nodes is characterized as transmission variety and hop count in network . It is represented by the following formula

$$D_m = T_{Rr} \times HpC \tag{2}$$

Where T_{Rr} represent transmission range of node ;hop count represent HpC; T_{Rr} is calculated using Friss Equation [10].

$$T_{Rr} = \frac{\eta}{4\pi} \times \sqrt{\frac{P_{tx} \times \alpha \times \beta \times (1 - |\epsilon Z|)}{P_{rx}}} \tag{3}$$

Where η represent wavelength of operation; P_{tx} denote transmitted power node; P_{rx} represent receiver sensitivity; α denote gain of the transmitter; β state receiver gain; ϵ represent receiving antenna's reflected power coefficient.

C. Burst loss limit (BL_m): It represent the mean burst length function and probability of packet loss. It is explained by following formula

$$BL_m = \sum XB + PB \tag{4}$$

$\sum XB$ represent burst length, $\sum XB = 1/\epsilon$, $PB = \sqrt{1 - \epsilon/\epsilon}$
 ϵ represent the probability of two repeated packet loss in network transmission.

D. Fault detection timer T_F : It is expressed using the subsequent formula:

$$T_{bl}T_F = T_{fw} + \alpha \tag{5}$$

T_{bl} represent tolerated burst loss; T_{fw} represent forwarding interval of sensor node; α is hop count[25].

E. Average Link quality: The arrangement of potency and/or the value of a packet received. It is directly related to RSSI.

$$LQT \propto RSSI \tag{6}$$

Logarithmic Ratio of P_{rx} - received power and P_{ref} -reference power denote RSSI. Constant value 1 mW is assigned to P_{ref} .

$$RSSI = 10 \cdot \log \frac{P_{rx}}{P_{ref}} \text{ (dBm)} \tag{7}$$

When increase of P_{rx} , results increase in the value of RSSI value and link quality improvement [6][25].

7. Simulation Results

A. Simulation parameters: Simulation is performed by NS-3 for the proposed Emergency Node based fault tolerant method. 20,30 and 50 are the node count and EN count is changed as 1,2,3,4 and 5. 100 m x 100 m square sensing region is used for 60 s simulation time. Constant bit rate is used as traffic in network. Table 1 represent settings and parameters of simulation.

Table 1: Simulation Parameters

Parameters	Values
Number of Sensor nodes	20,30 and 50
Number of Emergency Node	1,2,3,4 and 5
Sensing Area	100 x 100
Simulation time	60 s
Traffic model	CBR
Data Rate	250 kb
Propagation model	two-ray ground
Antenna used	Omni Directional antenna
Initial energy of each node	10.1 J
Transmission power of node	0.660
Receiving power of node	0.395

B. Performance Metrics: Following parameters were evaluated to analysis the performance of the proposed method 1). Packet Delivery Ratio: The ratio of successfully received packets and number of packets transmitted from source[25].

2). End-to-End delay: It is average time difference for data packets to transmitted from sources and received in the destinations.

3). Energy Consumption: Total Energy consumed by the network for transmission and reception

C. Results and Analysis: In simulation experiments, primary and Alternate Routing path Relay nodes fault were taken part into account. In this sensing scenarios, 20,30 and 50 are the number of nodes going to used for experiment.

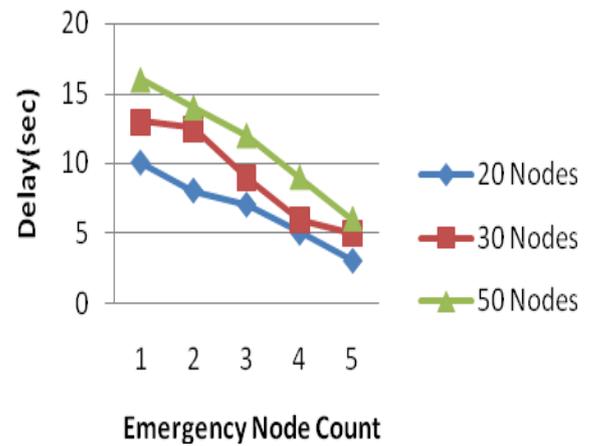


Fig. 3: Emergency Node Count Vs Delay

Fig. 3 shows the Experimental results of delay occurred for EN based operation by varying the EN. Delay is decreased in the network due to increase in EN count, more number of EN are concerned in routing and forwarding.

Fig. 4 represent the results of PDR obtained for Emergency Node based operation, by changing the Emergency nodes count. The PDR increases, when the count of Emergency node increased. Fig. 5 represent average energy consumption results for EN based operation by changing the EN count. Energy consumption decreased throughout the simulation, when Emergency node count is increased, due to number of EN and nodes are concerned in routing and forwarding.

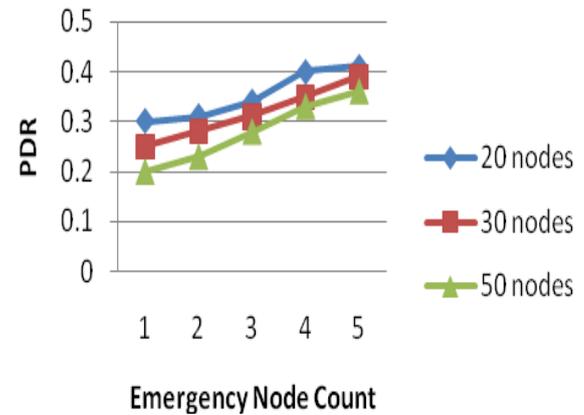


Fig. 4: Emergency Node Count Vs PDR

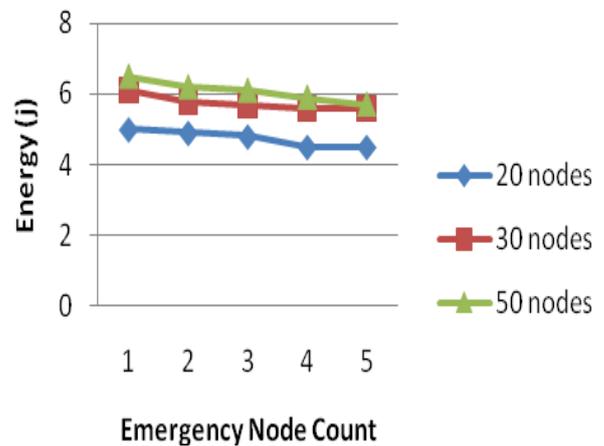


Fig. 5: Emergency Node Count Vs Energy Consumption

7. Conclusion

In this paper, an Emergency Node based fault-tolerant method has been proposed. This method provides effective solution where source node faced link failure due to fault in the nearest relay node's using Emergency Node. Our simulation result proves that, the proposed method minimizes the energy utilization with increased packet delivery ratio, reduced delay and increased the life time of network.

References

- [1] Akbari, A., Beikmahdavi, N.: 'Cluster-based and cellular approach to fault detection and recovery in wireless sensor networks'. Third International Conference on IEEE Advanced Computer Theory and Engineering (ICACTE), 2010, 2010, vol. 5, pp. V5-148
- [2] Asim, M., Mokhtar, H., Merabti, M.: 'A fault management architecture for wireless sensor network'. IEEE Int. Wireless Communications and Mobile Computing Conf., IWCMC'08, 2008, pp. 779-785 [15] Huang, J.M., Tai, S.C., Chen, K.H.: 'CRINet: a secure and fault-tolerant data collection scheme using 3-way forwarding and group key management in wireless sensor networks'. IEEE Wireless Telecommunications Symp., 2009, WTS 2009, 2009, pp. 1-6
- [3] Babaie, S., Rezaie, A.R.: 'DFDM: decentralized fault detection mechanism to improving fault management in wireless sensor networks', In (Eds): 'Digital information and communication technology and its applications' (Springer, Berlin Heidelberg, 2011), pp. 685-692
- [4] Babaie, S., Shojaiy, M.G.: 'Improving fault management using voting mechanism in wireless sensor networks'. Int. Conf. on IEEE Computational Intelligence and Communication Networks (CICN), 2010, 2010, pp. 359-362
- [5] Babaie, S., Shojaiy, M.G.: 'Improving fault management using voting mechanism in wireless sensor networks'. Int. Conf. on IEEE Computational Intelligence and Communication Networks (CICN), 2010, 2010, pp. 359-362
- [6] Bagheri, T.: 'DFMC: decentralized fault management mechanism for cluster based wireless sensor networks'. Second Int. Conf. on IEEE Digital Information and Communication Technology and its Applications (DICTAP), 2012, 2012, pp. 67-71
- [7] A. Birolini. Quality and Reliability of Technical Systems: theory, practice, management. Springer, 1997.
- [8] Chang, F.C., Huang, H.C.: 'A survey on intelligent sensor network and its applications', J. Netw. Intell., 2016, 1, (1), pp. 1-15
- [9] Choi, J., Hahn, J., Ha, R.: 'A fault-tolerant adaptive node scheduling scheme for wireless sensor networks', J. Inf. Sci. Eng., 2009, 25
- [10] Huangshui, H., Guihe, Q.: 'Fault management frameworks in wireless sensor networks'. Int. Conf. on IEEE Intelligent Computation Technology and Automation (ICICTA), 2011, 2011, vol. 2, pp. 1093-1096
- [11] S. Kumar, F. Zhao, and D. Shepherd, "Collaborative Signal and Information Processing in Microsensor Networks," IEEE Signal Processing Magazine, vol. 19, no. 2, pp. 13-14, Mar. 2002.
- [12] Liu, H., Nayak, A., Stojmenovi, I.: 'Fault-tolerant algorithms/protocols in wireless sensor networks', In (Eds): 'Guide to wireless sensor networks'(Springer, London, 2009), pp. 261-291 Information and Communication Technology and its Applications (DICTAP), 2012, 2012, pp. 67-71
- [13] Liu, T.H., Yi, S.C., Wang, X.W.: 'A fault management protocol for lowenergy and efficient wireless sensor networks', J. Inf. Hiding Multimed. Signal Process., 2013, 4, (1), pp. 34-45
- [14] Man, K.L., Chen, C., Hughes, D.: 'Decentralized fault detection and management for wireless sensor networks'. Fifth Int. Conf. on IEEE Future Information Technology (FutureTech), 2010, 2010, pp. 1-6
- [15] K. Martinez, P. Padhy, A. Riddoch, H. Ong, and J. Hart. Glacial environment monitoring using sensor networks. In REALWSN' 05, 2005.
- [16] Rehana, R.T., Maneesha, R.V., Sangeeth, K.: 'Fault tolerant clustering approaches in wireless sensor network for landslide area monitoring'. ICWN, 2008, pp. 107-113
- [17] Saleh, I., El-Sayed, H., Eltoweissy, M.: 'A fault tolerance management framework for wireless sensor networks', IEEE Innov. Inf. Technol., 2006, pp.1-5
- [18] A. S. Tanenbaum and M. van Steen. Distributed Systems: Principles and Paradigms. Prentice Hall, 2002.
- [19] G. Tolle, J. Polastre, R. Szewczyk, D. Culler, N. Turner, K. Tu, S. Burgess, T. Dawson, P. Buonadonna, D. Gay, and W. Hong. A macroscope in the redwoods. In SenSys '05: Proceedings of the 3rd international conference on Embedded networked sensor systems, pages 51-63, New York, NY, USA, 2005. ACM Press.
- [20] K. Langendoen, A. Baggio, and O. Visser. Murphy loves potatoes: experiences from a pilot sensor network deployment in precision agriculture. In IPDPS 20th International Parallel and Distributed Processing Symposium, 2006.
- [21] Ye, L., Qiu, X., Huang, R., 'Probability-based fault detection in wireless sensor networks'. Int. Conf. on Network and Service Management (CNSM), 2010, October 2010, pp. 218-221
- [22] Yu, M., Mokhtar, H., Merabti, M.: 'Self-managed fault management in wireless sensor networks'. Mobile Ubiquitous Computing, Systems, Services and Technologies, UBIComm'08, 2008, pp. 13-18
- [23] Abbasi, A.A., Younis, M.F., Baroudi, U.A.: 'Recovering from a node failure in wireless sensor-actor networks with minimal topology changes', IEEE Trans. Veh. Technol., 2013, 62, (1), pp. 256-271
- [24] Afsar, M.M.: 'Maximizing the reliability of clustered sensor networks by a fault-tolerant service'. IEEE 27th Canadian Conf. on Electrical and Computer Engineering (CCECE), 2014, pp. 1-8
- [25] Kasilingam Rajeswari, Subbu Neduncheliam., "Genetic algorithm based fault tolerant clustering in wireless sensor network", IET Communications, 2017, pp.1927-1932.
- [26] S.V. Manikanthan , T. Padmapriya "An enhanced distributed evolved node-b architecture in 5G tele-communications network" International Journal of Engineering & Technology (UAE), Vol 7 Issues No (2.8) (2018) 248-254. March 2018.
- [27] S.V. Manikanthan and K. srividhya "An Android based secure access control using ARM and cloud computing", Published in: Electronics and Communication Systems (ICECS), 2015 2nd International Conference on 26-27 Feb. 2015, Publisher: IEEE, DOI: 10.1109/ECS.2015.7124833.
- [28] T. Padmapriya and V. Saminadan, "Improving Throughput for Downlink Multi user MIMO-LTE Advanced Networks using SINR approximation and Hierarchical CSI feedback", International Journal of Mobile Design Network and Innovation- Inderscience Publisher, ISSN : 1744-2850 vol. 6, no.1, pp. 14-23, May 2015.