iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Fault Tolerance Review in Wireless Sensor Networks

Pamarthi Swapna[1], B.S.S.Tejesh[2], S.Neeraja[3]
[1, 2, 3]*ECE, SRK Institute f Technology, Enikepadu*

Abstract: ***Wireless sensor networks have diversified application like environmental monitoring, scientific data collection, and battlefield surveillance. In the Wireless sensor network, the sensor nodes are deployed in all possible environments. The wireless sensor network infrastructure comprises of a network and sensor nodes. Reliability is the prime issue in wireless sensor network. Reliability is affected by errors and faults that occurs due to various hardware and software issues. In both the wireless sensor networks and the traditional wireless networks occurrence of fault is persistent. If any node fails due to any abnormal condition then there will be a barrier in the communication. The failure of the communication in the wireless sensor networks may be caused by erroneous of nodes, breakdown in the links. The concept of fault tolerance enables the wireless sensor network to find and even out the errors. The self-healing capability in the wireless sensor network makes the nodes in the network more reliable.***
Keywords: Fault Tolerance, Reliability, Sensor Nodes, Wireless Sensor Networks.

I. INTRODUCTION

A Wireless sensor network comprises of sensor nodes, which are having the capability to sense, process and communicate data [1]. The applications such as military, industrial process are mainly involved in the enhancement of wireless sensor network. The wireless sensor nodes are of low cost so that large scale deployment of the sensor nodes is possible. Availability, Reliability, Maintainability are some of the promising characteristics offered by the Wireless sensor networks [2]. As the sensor nodes increases in the application the fault tolerance can only make the system work efficiently.

The sensor nodes are not affected by the faults and failures in the service level of the wireless sensor networks. The wireless sensor networks aim at eliminating the MTTR by employing the detection and recovery methodology [3]. Node to node communication is possible with the deployment made by the sensor nodes in the wireless sensor networks. The communication service employed by one node with the other node is based on multi hop routing.

Each and every node employs a dedicated task. The sensor nodes, which are having desired hardware capabilities are capable of performing the task for other nodes which are not having desired hardware functionalities [4].

The sensor nodes with efficient hardware functionalities may also fail and fault may occur due to radio interference, battery exhaustion. The hardware and software faults may lead to the above mentioned problems and make the system fault [5]. If any failure occurs in the sensor node, then the sensor node may not be in a condition to process any data. Sometimes a minor software bug may also drive the system to massive failure [6].

II. FAILURES IN WIRELESS SENSOR NETWORKS

Before coping with fault tolerance mechanisms, one must be able to understand the difference between faults, errors, failures.

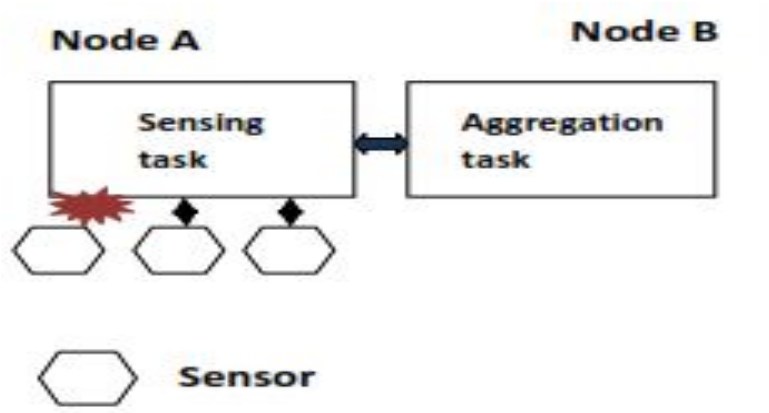
Fault is a type of defect which drives to error. An Error is an undefined state which drives to failure. Failure is a state where the system cannot implement its functionality [7]. The fault, error, failure is explained briefly with the help of the figure. In the Figure 1 there are two nodes they are node A and node B connected to a sensor.

Node A's task is to sense the data and transmit the measured data to the Node B which has an aggregation service running on it. Due to some disturbance caused between Node A and sensor.

The Node B may not receive any data because Node A is in Failure state.

The fault state occurred between the Node A and the Node B. The error state occurred when the sensor is not capable of pushing the data to the Node A. The Fault detection and Fault recovery are the two significant operations done to overcome in Faulty situations [8]. example of a web page in [7].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com



Fig, 1 Fault occurred due to lose connection between Node A and sensor.

III.SOURCES OF FAULTS IN WIRELESS SENSOR NETWORK APPLICATIONS

A. Node Faults

Single node and multi node faults are the two common types of faults that occur in the wireless sensor network. Single node fault corresponds that only one node is failed at a time. Multinode fault represents that multiple nodes are failed concurrently at a time. The malfunctions in the nodes are produced due to the hardware and software components. The nodes that are deployed in the external environment may lead to many issues because of enclosure impacts, environment conditions, short circuits [10]. In the packaging of the sensor node, if proper packaging is not done, then the components of the sensor nodes would become loose. Due to insufficient battery also the sensor node may fail to complete the task. The data acquisition application will not provide accurate results if the underlying components are not functioning properly [11]. Software bugs are also a prime cause for the faults in wireless sensor networks. To extend the lifetime of the network the nodes are transforming into cluster heads. The cluster heads take the lead in routing the data to the base station and maintaining proper coordination in the nodes within the cluster [12]. If the cluster head faces the failure state, then no information is transferred to the base station. In a tree like structure the nodes may be arranged at several levels. The base station performs the job of accumulating the information from the sensor nodes and does more processing on it and sends back the information to the sensor nodes. There are two approaches employed by the multi-tree aggregation one approach is rebuilding and another approach is local fixing. Rebuilding facilitates the topology to construct once again whenever any failure occurs. In the local fixing it performs the aggregate operation and uniquely identify the sensor nodes based on its address. The software bugs may also lead to processing incorrect information. If one node processes incorrect information in a cluster, then all the remaining nodes will aggregate the data and may subject to failure [13].

B. Network Faults

In a wireless sensor networks the fundamental role is routing of data. In a group of sensor nodes, a relay node is placed in between two sensor nodes. The information from a total of nine nodes is accumulated in the relay node. In a network if any new node is joined then a new unique address will be assigned to that node. In a network handling faults in single node are easier than handling faults in multiple nodes. For collecting data from the sensors it is essential to configure the software and also make coordination between the nodes [14]. The tracking of objects can be done by implementing specific routing protocols. Occurrence of faults in the routing layer can lead to delay in the messages, forwarding incorrect messages. The relay node maintains a routing table of all the available sensor nodes in its locality. In wireless sensor networks the links between one node and another node is highly volatile [15]. If the links between the nodes are not stable then routing paths may be changed. If one node is remote from the other nodes, then that node is in unreachable state and further communication with the nodes is not possible. The Radio interference, collision of messages, Software bug, link range coverage are some of the causes of faults in wireless sensor networks [16]. The network layer in the communication stack coordinates nodes. The network management monitors both the wired or wireless network. Enhancing the network to work efficiently, HSPREAD is the approach which will detect and reach the sensor node from the main base station.

C. Sink Faults

The sink main role is to collect the data from the devices and convey the data to the back end system. The sensor nodes are located near the sink node then more traffic issue arises. The sink node provide the network administrator with the necessary information so as the fault diagnosis can be done. If the fault tolerance scheme is not applied in the sink devices, then the data cannot be accessed

from the nodes if any fault occurs. If all the packets are routed into the sink node, then the issues like communication overheads and network latency occurs in the sink node. The sensor nodes that are far from the sink will consume more energy while processing information. The nodes which are malfunctioned their information must not be sent to the sink. With the employment of batteries and solar cells the sink devices can deployed in all the remote areas [17]. The sink deployed areas are monitored with the help of satellite connections. The satellite connections may also lost if there is any climate change in the environment.

IV. FAILURE CLASSIFICATION

The faults are transforming to failures in a wireless sensor network due to the following reasons as a node moving to remote area, link failure, power failure, malfunctioning [18]. The failure in the wireless sensor networks is classified into the crash, omission, timing, value, arbitrary.The failure by omission is determined by the radio interference which may lead to message loss. A crash failure occurs when the node stops responding to any request. In Timing scenarios, the failures may occur due to delay in the messages or early deliver of messages. Timing failure occurs whenever timing constraints are specified. If an incorrect value is sent by the device in a timely manner due to lack of accuracy, then the service is said to be failed. The incorrect data that is generated is caused by software malfunctioning, corrupt messages, hardware issues. The arbitrary failure is caused by malicious service that is integrated with the applications [19].

V. FAULT DETECTION TECHNIQUES

The need for fault detection techniques is to provide better functionality by overcoming the errors. Self-Diagnosis, Group Detection, Hierarchical Detection are some of the approaches for detecting Faults. The self-diagnosis is one of the approach for detecting faults by the nodes. The self-diagnosis of nodes based on the measurement of accelerometer it can be determined that some sort of hardware complications have been occurred. Whenever nodes are being moved to a new location, then also they are capable of detecting faults [20]. Based on the battery current, voltage measurements it can be predicted that the sensor node exhibits a fault due to battery exhaustion. The link connection between nodes must be reliable, if the connection is unreliable the nodes have the capability to detect the fault by Self –Diagnosis mechanism. The Group detection is another approach mainly based on the comparison between the generated value and the reference value. Some algorithms like are also used for the detection of faults. The boundary scheme represents that all the sensor nodes, which are in the boundary must have values. The misbehavior scheme makes the sensor nodes to communicate with each other and detect is made based on the messages received. The Hierarchial detection is a tree like structure provides a scalable approach in fault detection [21]. The network topology is a combination of child nodes, parent nodes, Sink nodes. The information from the child node is being transferred to the parent node. The results of the child nodes are aggregated in the parent node and for further processing the data has been transferred to the next level. Another hierarchial approach is that all in a network topology all the sensor nodes come under cluster node. All the cluster nodes information is grouped together and sent to the base station.

VI. FAULT RECOVERY TECHNIQUES

Even though faults occur in the system, the fault recovery technique enables the system to operate efficiently as per the specifications [22]. In the Wireless sensor networks there are two classifications in the fault recovery mechanisms. The Active and passive archetype are two approaches for the fault recovery techniques. In the active archetype, all nodes are involved in the processing of information. In the passive archetype, the processing of information is done by only one node. In the passive archetype if the node fails, then only the operation is taken by other nodes.

A. Active archetype in Wireless sensor network

The same functionality is provided by all the nodes in the active archetype. All the sensor which are dedicated to sense the data, perform their operation. The sensor nodes gather the sensed data and transfers the data to the next level that is to the base station. Even though one node fails, the other nodes are capable to transfer the information to the base station [23]. Multiple routing is used in active archetype. In a number of k nodes, even though if one node fails there will be k-1 nodes available to operate the functionality. The sensor value aggregation seeks to provide data from low-level sensors to the high-level sensors [24]. Identifying the malfunction sensor nodes provides an efficient solution by not transferring the failed sensor node data to the base station.

B. Passive archetype in wireless sensor network

In the passive archetype, the primary sensor node receives and processes all the requests. So as to maintain a link with the other nodes, the primary node data are transferred to the backup station.The fault recovery technique in the passive archetype consists of

node selection and service distribution [25]. In the node selection scenario, if the primary node is subjected to failure then new service provider will be selected. Based upon the chosen sensor node will take the operations to be done. In the probabilistic rotation system the sensor nodes keep changing their role. If the cluster head fails then the responsibilities are taken by another node based on the rotation period. In the group election a group of nodes called as a cluster. All the clusters will have a cluster head and these cluster heads will act as a gateway. The gateway consists the details of all the clusters and the nodes that are there in the cluster. When a gateway fails, then all the details of the failed gateway are handled by other gateways.

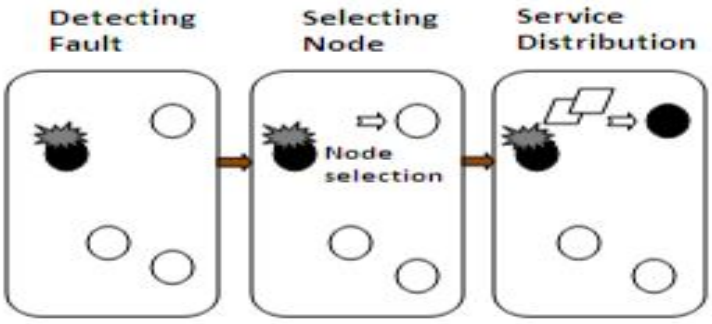


Fig. 2 Failure recovery in Passive archetype.

In the service distribution phase, for activating the service the sensor node serves as service providers. In some cases with little changes in the sensor node transform themselves as the service providers. The pre-copy scheme as described in [25] allows the sensor nodes to function according to the role assigned to them. Code distribution is another approach where service code is distributed through the network. In the [26] a middle ware programming for wireless sensor networks here the programming is done in such a way that the sensor node can be mobile and propagate through the network. The code migration makes the sensor nodes free of memory as all the nodes need not to have a pre-installed system. This remote execution makes the sensor node devices to transfer tasks to higher devices usually called as a base station.

VII. CONCLUSIONS

In this paper, a good understanding of faults that occur in wireless sensor networks is given. Our concise report can make the readers understand about wireless sensor networks. The paper discusses about the failures in wireless sensor networks, sources of faults in wireless sensor networks, Failure classification, different fault detection techniques and fault recovery techniques. This paper gives the readers a basic idea on what are the basic applications in wireless sensor networks

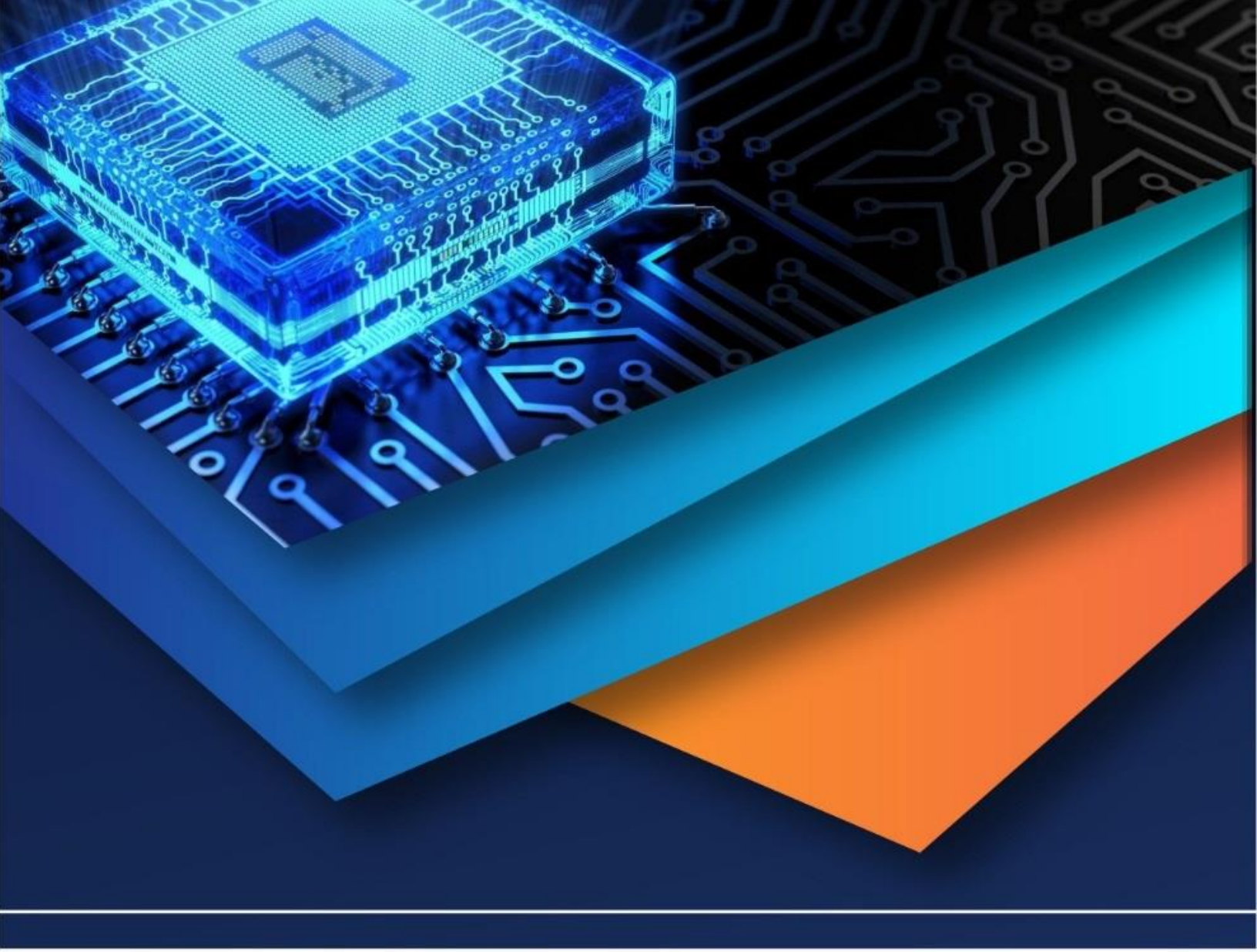
VIII. ACKNOWLEDGMENT

The Authors Pamathi Swapna, B.S.S.Tejesh, S.Neeraja are greatly thankful to the SRK Institute of Technology,Enikepadu authorities for providing necessary infrastructure facilities to carry out this research work.

REFERENCES

[1] F. Akyildiz, et al, “ASurvey on Sensor Networks”. IEEE Communications Magazine, 40:102–114, August 2002.
[2] D. Estrin,et al. “Next century challenges: scalable coordination in sensor networks. In MobiCom”99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pages 263–270, New York, NY, USA, 1999. ACM Press.
[3] A. Birolini. “Quality and Reliability of Technical Systems:theory, practice, management”. Springer, 1997.
[4] A. S. Tanenbaum and M. van Steen. “Distributed Systems: Principles and Paradigms”. Prentice Hall, 2002.
[5] 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.
[6] G. Tolle, et al. “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.
[7] W. R. Heinzelman, A. Chandrakasan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”. In Proceedings of the 33rd Hawaii International Conference on System Sciences, volume 8, page 8020, 2000.
[8] T. Schmid, H. Dubois-Ferri`ere, and M. Vetterli. “Sensorscope: Experiences with a wireless building monitoring sensor network. In REALWSN’ 05, 2005.
[9] R. Szewczyk, et al. “An analysis of a large scale habitat monitoring application”. In SenSys ’04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 214 226, New York, NY, USA, 2004.ACM Press.
[10] K. Martinez, et al. “Glacial environment monitoring using sensor networks”. In REALWSN’ 05, 2005.
[11] J. Thelen,et al . “Radio wave propagation in potato fields”. In First Workshop on Wireless Network Measurement, 2005.

[12] P. Levis and D. Culler. "Mat´e: A Tiny Virtual Machine for Sensor Networks". In ASPLOS-X: Proceedings of the 10th international conference on Architectural support for programming languages and operating systems, pages 85–95, New York, NY, USA, 2002. ACM Press.
[13] K. Langendoen, et al. "Murphy loves potatoes: experiences from a pilot sensor network deployment in precision agriculture". In IPDPS 20th International Parallel and Distributed Processing Symposium, 2006.
[14] A. Mainwaring, et al. "Wireless sensor networks for habitat monitoring". In WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 88–97, New York, NY, USA, 2002. ACM Press.
[15] C.-Y. Koo. "Broadcast in Radio Networks Tolerating Byzantine Adversarial Behavior". In Proceedings of the twenty-third annual ACM symposium on Principles of distributed computing, pages 275–282, 2004.
[16] S. Harte and A. Rahman. "Fault Tolerance in Sensor Networks Using Self-Diagnosing Sensor Nodes". In The IEE International Workshop on Intelligent Enviroment, pages 7–12, June 2005.
[17] L. Benini, et al. "A Discrete-Time Battery Model for High-Level Power Estimation". In Proceeding of the Design, Automation and Test in Europe Conference and Exhibition 2000, pages 35–39, 2000.
[18] B. Krishnamachari and S. Iyengar. "Distributed Bayesian Algorithms for Fault-Tolerant Event Region Detection in Wireless Sensor Networks". IEEE Transactions on Computers, 53:241–250, March 2004
[19] S. Marti,et al. "Mitigating Routing Misbehavior in Mobile Ad hoc Networks". In Proceedings of the 6th annual international conference on Mobile computing and networking, pages 255–265, 2000.
[20] G. Gupta and M. Younis. "Fault-Tolerant Clustering of Wireless Sensor Networks". Wireless Communications and Networking, 3:1579–1584, 2003.
[21] S. Rost and H. Balakrishnan. "Memento: A health monitoring system for wireless sensor networks". In SECON, 2006.
[22] L. B. Ruiz, et al. "Fault Management in Eventdriven Wireless Sensor Networks". In Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems, pages 149–156, June 2004.
[23] N. Li and J. C. Hou. "FLSS: A Fault-Tolerant Topology Control Algorithm for Wireless Networks". In Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, pages 275–286, 2004.
[24] P. Levis and D. Culler. "Mat´e: A Tiny Virtual Machine for Sensor Networks". In ASPLOS-X: Proceedings of the 10th international conference on Architectural support for programming languages and operating systems, pages 85–95, New York, NY, USA, 2002. ACM Press.
[25] J. L. Bredin,et al. "Deploying Sensor Networks with Guaranteed Capacity and Fault Tolerance". In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pages 309–319, 2005.
[26] D. Desovski,et al. "Linear randomized voting algorithm for fault tolerant sensor fusion and the corresponding reliability model". In IEEE International Symposium on Systems Engineering, pages 153–162, October 2005.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY