ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Evaluation of Some Fault Detection Techniques in Wireless Sensor Networks: A Review

Arezou Chehregosha, Mehran Emadi

Master Student [Computer], Dept. of CE, Yazd Branch, Islamic Azad University, Yazd, Iran

Assistant Professor, Dept. of EE, Mobarakeh Branch, Islamic Azad University, Mobarakeh, Iran

ABSTRACT: Wireless Sensor Network (WSN) consists of a set of inter-related elements called “nodes”. Due to the limitations with the node energy source, nodes may become faulty that will lead to the decrease in throughput and consequently reduction of output and efficiency of the network. Therefore, it is essential to have fault tolerability among network components in order to decrease damages. In reality, fault tolerability, fault identification, and fault resolving will lead to increase in reliability and validity of connections. Fault management in WSNs are divided into three sections: Fault detection, fault identification, fault optimization. As a matter of fact, fault detection is considered to be the first step towards fault management. So many techniques are proposed for fault detection in WSNs, each with different advantages and disadvantages. The aim of this article is to introduce some fault detection mechanisms in WSNs and the comparison of three algorithms as set forth.

KEYWORDS: Wireless Sensor Networks, Sensor Node, Fault Detection, Battery Power, Active Node.

I.INTRODUCTION

A wireless sensor network is a system consisting small nodes connected to each other without any cable or wire, and each node consists of several parts. In fact, a node includes a computation engine, power supply (battery), sub-systems for saving and connection, sensor devices, and in some cases actuating devices [3,17]. Power supply available for each node is relatively limited [17] and has to be replaced with new batteries repeatedly. However, this is time consuming and costly as there are so many nodes in such networks. As such, it is concluded that energy is a limiting factor for the performance of these networks [3].

Recently, wireless sensor networks received much attention due to their potential applications in the fields of military computations, wild nature tracking, traffic supervision, health care, environment supervision, and supervision on the building structures [6]. However, damages in one or more nodes may sometimes destroy the whole connection of that network. Hence, fault tolerability in wireless sensor networks is remarkably important. Fault tolerability is one of the system capabilities to provide optimal level of performance at the time of fault presence in system and somehow increases the system reliability [12].

There are so many factors that make fault tolerability as an important issue, and these factors are divided into the following three groups:

1) Technology
2) Vast application of these networks
3) Introducing of wireless sensor networks as a new scientific and engineering major

As stated in the above, the first reason for importance of tolerability of wireless sensor networks against fault occurrence is related to the technology and running aspects of these networks. Sensors and its actuators are the two most important parts in a node that have direct connection with the environment. Therefore, they interact with different factors as like physical, chemical, and environmental ones. As such, they have less reliability than some circuits available in a closed pack. In addition, thousands of nodes existing in sensor networks are individually very

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

complicated systems and each part acts with complicated process as like signal processing, connecting, sensing, computing, etc.

The second factor is related to the application of wireless sensor networks that may change and improve proportionate to their technology and structure. The most important point is that above-mentioned networks mostly work independently and far from human being's presence. In addition, those issues related to security and privacy will make prevention from testing of these networks. It must be noted that not only testing and fault tolerability is affected, but also other tasks like troubleshooting may face problems because it will be possible to recreate particular conditions under which faults have occurred. Another item as the most important factor in the widespread application of wireless sensor networks is that many of these applications in the field of safety are quire sensitive and are able to put unsuitable influences on human being and environment, especially when actuators are used. The third influential factor to pay attention to the wireless sensor networks and fault tolerability is the introduction of these networks as a new scientific field for research and examination, which is put under engineering majors group and few people are informed about diagnosis and troubleshooting of these networks. For this reason, precise forecast on the best and most effective strategy for being tolerable against faults in wireless sensor networks is considered to be a difficult job. Likewise, technology and applications concerning this type of network is changing and extending so fast. For instance, if we take energy consumption into account, each part depends mostly upon its relative consumption in other parts, especially when the required energy for connection is more than the required energy for computations; in this mode, improvement of localization algorithms is important, which may require more limited amount of connections [3].

Nodefailure

Wireless sensor networks consist of special distributed nodes for the observation of physical or environmental conditions as like temperature, sound, and pressure [14,15], through which they would be able to take their data from the source to destination. A wireless sensor network includes thousands of nodes, each connected to one or more sensors. Small size and low cost have made their wider application in networks creation. On the other hand, their reliability level is low and one of the main reasons is small amount of energy created by these nodes in a network. Electrical/mechanical problems, unsuitable environmental conditions, interference of external factors, and battery drain are amongst the main causes for nodes failure [15].

Nodes failure is a normal incident in wireless sensor networks [9,15], which is mainly due to their very limited energy and unsuitable environmental conditions. As the result of nodes failure, a set of nodes are separated from the others that is called failure, a set of nodes are separated from the others that is called "Cut" or separation. The above incident decreases the number of multi-hop routes and prevents from reaching the data to destination. For this reason, fault detection and diagnosis of fault-creating node is very important [15].

It has been tried in the present article to provide a definition of wireless sensor networks and their importance in modern world. Fault detection and relevant identification techniques are going to be described in section II. Some of the earlier studies in this respect are provided in section III in addition to a brief explanation on proposed algorithms for each case. Sections IV and V respectively include simulation of the algorithms and comparison of the results as a conclusion.

II.FAULT DETECTION

Reliability is the main topic for designing of tracking techniques in wireless sensor networks [1]. To design a comprehensive and reliable wireless sensor network, it is necessary to consider nodes failure and energy limitations by means of fault management techniques. Fault management in wireless sensor networks is divided into three parts: Fault detection, fault identification, and fault optimization (system restore). In fact, fault detection is the first step towards fault management in a network, in which this unexpected fault has to be identified correctly by network system [16].
Fault detection methods in wireless sensor networks are divided into five groups: Distributed, concentrated, battery power, self-diagnosis, and group diagnosis.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

1. Concentrated

Concentrated method is a standard technique for the identification and localization of faults in wireless sensor network. In this method, central node performs fault management techniques with an unlimited energy. This node usually integrates data inside the network through the active methods of fault detection by means of sending repeated messages and continual demands. The advantage of this technique is high efficiency and accuracy but resource limitations in wireless sensor network cannot pay the costs for the continual collecting of sensors since the nodes in this technique have to send extra costly messages [16].

2. Distributed

In this technique, nodes are allowed to make specific decisions before connection to the central node in order to prevent from plenty of transacted messages unless otherwise a fault may has happened in the system. Here we will have self-identification and self-correction of the nodes. Through making arrangements with the neighboring nodes and "Watchdog" technique, the nodes will perform fault detection [15,16].

3. Battery Power

As explained in the introduction, sensor networks are equipped with very limited energy sources and even it is practically impossible to replace these sources due the plenty of nodes and installation of these networks in inaccessible environments [8]. Battery power mechanism is based upon energy conditions of the sensor node. This model assumes that in case battery power level is sufficient for small jobs, that node will be active. It means a node will be able to act effectively when it can transmit data signals in its controlled area. As the battery power amount is progressively changing depending upon different factors, it is necessary to access a relatively fixed battery power in the time window. In fact, [2] states that each node at the beginning of time window has the most battery power amount (b_f) and the amount of battery power drain is specified by b_{drain} at the end of this time window. According to this mechanism, a time node exists in a specific time window in active mode for which the battery power should not fall under the threshold value of b_{th} [2].

4. Self-Diagnosis

In many cases, nodes are able to identify probable faults by means of their diagnostic mechanism [16]. In this method, computation through an accelerometer is applied for the diagnosis of failures due to hardware problems in the node. Through the above technique, nodes will be able to become aware of their displacement and other nodes. A similar method also consists of keeping the specifications of neighboring nodes, by which any alteration in any of these data indicates displacement of the node or its neighboring node [6,7].

5. Group-Diagnosis

In this technique, a group of nodes observe and evaluate other nodes behavior [7]. Fault diagnosis mechanisms are applied for the identification of destructed nodes. Both of the algorithms are provided based upon this idea stating that available sensors in homogenous areas must have similar values, unless otherwise the desired node stands at the boundary. Algorithms will compute probability of node failure through the measurement of values for all the neighboring nodes and comparison of the results [6,7].

II.RELATED WORKS

Myeong-Hyeon Lee and Yoon-HwaChoi assumed that all of sensor nodes have similar transmission amount [5]. The present study applies "distributed" method for fault detection. In this technique, the destructed sensor is taken into account as the sensor node without any fault and participate in network connections by the time it is able to transmit network data.

(1)

In Eq. (1), $\tilde{p}$ indicates node failure probability due to the application of fault diagnosis mechanism, *r* indicates probability of a node failure with the ability to participate in network connections, and *n* indicates number of diagnosed sensor nodes. When $0 \leqslant r \leqslant 1$, sensor node is not able to connect to its neighboring nodes.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

In this article, it is tried to perform fault detection mechanism by means of a graph. Connections graph with G(V,E) shows the connection between nodes, in which V indicates number of existing nodes and E indicates the graph edges. In this method of fault detection, two nodes i.e. V_i and V_j are compared to each other on the condition that $(V_i ,V_j) \epsilon E$. In case the difference value is less than the desired entry (C_{ij}) in attributed matrix is considered equal to zero.

In the proposed algorithm, each node Vi keeps a table including neighbors and their modes in attributed matrix. For each neighboring node, a single-bit called Fi is taken into account, which determines the fault condition of node Vi.

The aforesaid bit is initially followed with a value, assuming that desired node is faulty. Afterwards, their correctness is diagnosed through the following two conditions, in which is the threshold value.

- For each node V_i, Fi equals to 1 if $|C_i| \geq \theta$ (threshold test).
- For each node Vi, if there exists a neighbor like V_j for which F_j equals to zero, and $C_{ij} = C_{ji} = 0$, then F_i equals to zero too

By means of the above two conditions, faulty nodes are diagnosed through identification of the nodes without fault.

In the article proposed by Geetha D. D. et al. an active node model in wireless sensor network is applied for error detection that acts based upon battery power mechanism [2]. Performance of this algorithm is displayed in Fig. 1.

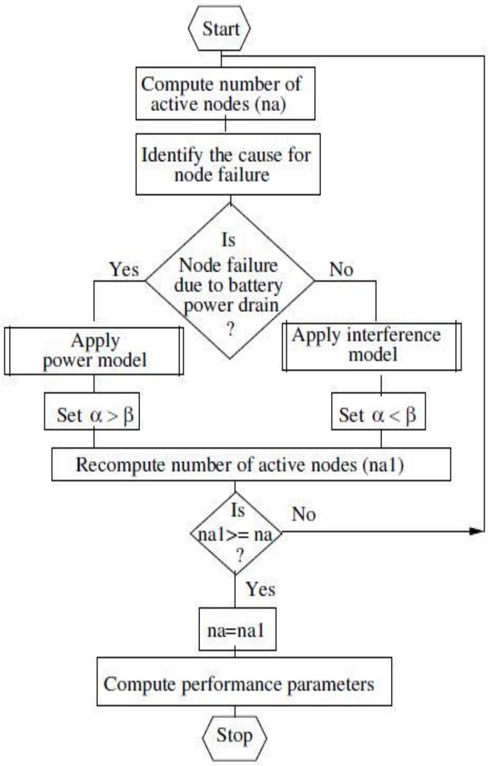


Fig. 1 Data flow for battery power and interference model

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

According to Fig. 1, a number of active nodes are identified and then failed nodes are detected. Afterwards, these failed nodes are examined to find out whether their failure will drain the battery or not. In case the answer is positive, battery power will be increased by means of a particular method that is going to be explained. Otherwise, interference model will be applied.

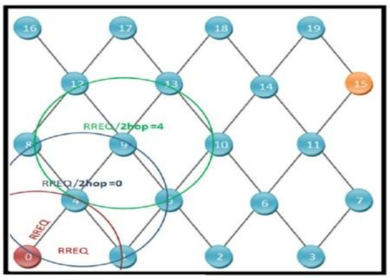


Fig. 2 Route detection

After passing the above procedures, a number of active nodes are identified, new values are compared to the values gained in earlier stages, and any set having more number of active nodes will be replaced with others. Finally, efficiency improvement parameters are computed. When there are many failed nodes, battery will be drained, while α will increase the battery power. When the main node has high interference, ß will increase the value.
In this method, a failed node transmits the source address, destination address, earlier hops, and next node address to the neighboring node with the highest power. This mechanism is called "Hand-off". The purpose of this technique is that plenty of nodes are going to be kept without battery drain.

Ahmed Roumane et al. use AODV-OFLES for fault tolerability in wireless sensor networks as the improved model of AODV algorithm [10]. Since data delivery in sensor networks is inherently faulty and unpredictable, a slight modification of the conventional routing has been proposed. This means that in case of node/link failure a second hop will be introduced. Selecting this second hop technique increases reliability, availability, energy-efficiency and maintainability of the network; thus the energy consumption of the network decreases. Only Failed Link Skipped (OFLS) is done in three general steps: Redefinition of the rout from (destination via next hop) to (destination via next hop via second hop), Exchanging the second hop information duringthe rout construction phase, and constructing a rout from the detecting node to its second hop toward the destination (in case of node/link failures).The rout selection mechanism acts as follows: First, source node sends an RREQ (Route Request) to all the other nodes and waits for the Route Replies (RREP) from the desired destination or intermediary node with the most up-to-dated route.

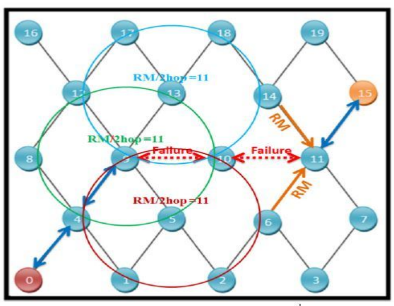


Fig. 3 Fault in the selected route

Optimal route is a route with its destination number equal or bigger than RREQ. The destination sequence number created by the destination determines the freshness of the route information; Since it contains any route information it sends to requesting nodes.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

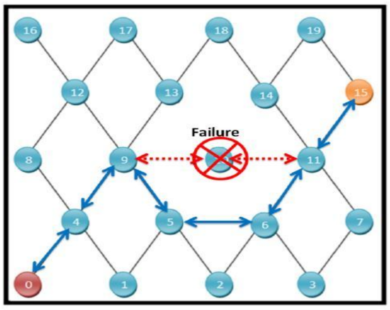


Fig. 4 Route restore by means of OFLS algorithm

In this case if there are two routs towards a destination, the one with the greatest sequence number is selected indicating most fresh route. Any node receiving this RREQ message will update its table and put the new data as the second hop. This procedure will continue by the time all data reach to destination. In case a fault occurs or no reply is received from the node during the time node is waiting for Replies packet from its consequent node, the node will perform a Route Maintain (RM) process with messages broadcasting to one of the neighboring hops. These packets consist of faulty node address and the next hop route.

Assuming Fig. 2 consider node 0 "source" tries to communicate with node 15 "destination" by broadcasting a RREQ (brown quarter circle in Fig. 2) to its neighbors at first. When they receive this message, each of them update its neighbor table by adding the address of the sending node. As this procedure continues, the node 0 can use nodes (4, 9, 10, 11) to achieve the goal. If a failure occurs to node 10, it should be omitted from the route and all of the neighbors tables.
First, node 9 runs a route recovery process by broadcasting a RM message within relevant information. This RM message is received by all its neighbors (green circle in Fig. 3). It should be pointed that a RM message is forwarded by a node only if it has a neighborhood relationship with either the second hop or the broken hop (brown and blue circles in Fig. 3). Finally, the node 11 sends RREP to node 9, which create the maintained rout (Fig. 4).

IV. COMPARISON

In this section, taking into account algorithms provided in section III, simulation is going to be performed and results will be analyzed.
Simulation results [5] are shown in Fig. 5. Mechanism efficiency depends upon various parameters as like number of nodes in the desired area, probability of node failure (shown by p), and θ threshold value.

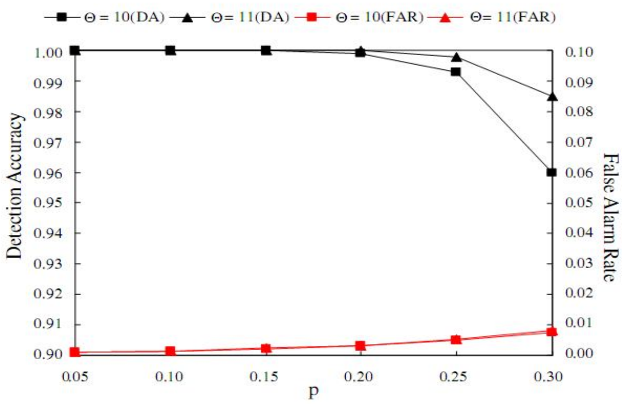


Fig. 5 Diagram for Detection Accuracy(DA) and False Alarm Rate(FAR)

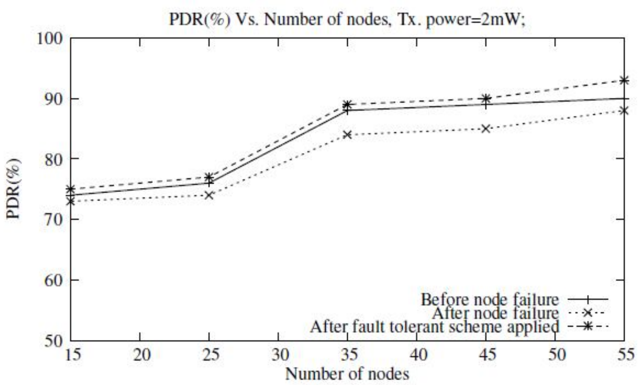
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

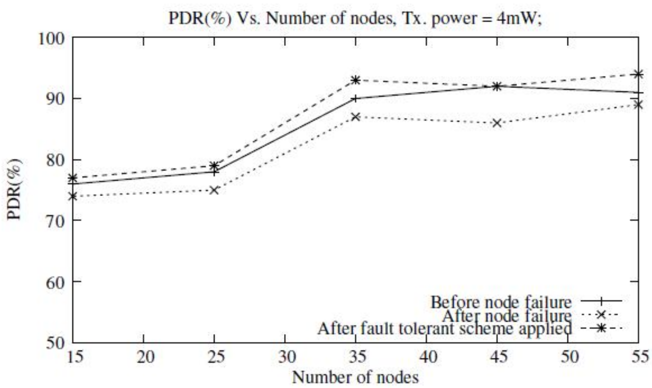
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Detection Accuracy (DA) is the ratio of number of detected nodes with failure to the total number of failed nodes and False Alarm Rate (FAR) is the ratio of number of safe nodes that are identified as failed nodes by mistake to the total number of correct nodes. For example, approximately 98% of the failed nodes have been detected accurately for p=0.3 and θ=8.



(a)



(b)

Fig. 6Diagram for Packets Delivery Ratio to the total number of nodes with transmission power of (a) 2mW, (b) 4mW

In Fig. 6 as provided according to the algorithm simulation indicated in [2], horizontal axe stands for the number of nodes and the vertical axe indicates PDR (Packet Delivery Ratio), which is in fact the ratio of packets delivery at destination.
There are three axes in this diagram, showing the situation of nodes relative to the packets delivered.

- First mode: before node failure
- Second mode: after node failure
- Third mode: after fault detected and fault tolerate scheme applied.

As stated in section III, fault detection is performed by means of algorithm [2] when the node follows with fault. As per the diagram, packets delivery rate at destination will increase after fault diagnosis.
In Fig. 6(a) the transmission power is 2mW. Fig. 6(b) is similar to Fig. 6(a); but the transmission power is 4mW. As evident in this diagram and a comparison to the first one, message transmission rate to destination is higher. As the result, the higher transmission power, message transmission speed will increase because voltage goes up by the time power increases.

In fact, message delivery rate to destination increases as the battery voltage (battery power) becomes more.
In [10], NS 2.33 Simulator is applied for the comparison of improved results of AODV-OFLS with AODV technique. Fig. 7 indicates that average amount of consumed energy by the network has failed against a number of main routes in simulation. Results of this simulation express that such routing with power improvement and delay reduction has improved system quality. This technique reduces network control overhead remarkably, which is one of the major problems in wireless sensor networks. Proposed algorithm also reduces energy consumption rate and this is considered to be a suitable alternative for wireless sensor networks.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

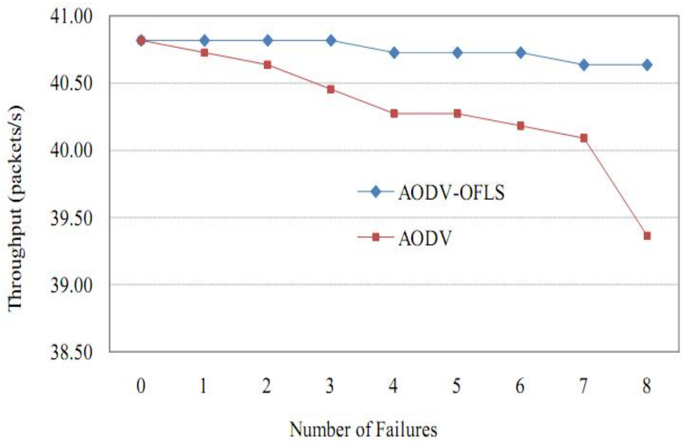


Fig. 7 Average energy consumption in the whole network

V. CONCLUSION

Due to unsuitable uncontrolled conditions around the network environment, wireless sensor networks are susceptible to various faults. The aim of this article is to express some error detection techniques and to compare the results out of their simulations. Each of the presented algorithms has made different results, depending upon which mechanisms among error detection, battery power, self-diagnosis, or distributed are applied. In the first technique based on distributed algorithm, it is initially assumed that all the nodes are faulty and then actual faulty nodes are detected through the above-mentioned algorithm. In fact, faulty nodes are diagnosed through the separation of those nodes without any fault.

REFERENCES

1. Chanak, P., Banerjee, I., “Energy efficient fault-tolerant multipath routing scheme for wireless sensor networks”, The Journal of China Universities of Posts and Telecommunications, Vol.20, Issue 6., pp.42-48, 2013.
2. Geetha, D. D., Nalini, N., Biradar, R. C., “Active Node based Fault Tolerance in Wireless Sensor Network”, India Conference Annual IEEE (INDICON) , Vol.12, pp.404-409, 2012.
3. Koushanfar, F., Potkonjak, M., Sangiovanni-Vincentelli, A., “FAULT TOLERANCE IN WIRELESS SENSOR NETWORKS”, IEEE Sensors, Vol.2, pp.1491–1496,2002.
4. Lau, B. C. P., Ma, E. W.M., Chow, T. W.S., “Probabilistic fault detector for Wireless Sensor Network”, Expert Systems with Applications, Vol.41, pp.3703-3711, 2014.
5. Lee, M. H., Choi, Y. H., “Fault detection of wireless sensor networks”, Computer Communications, Vol.31, pp.3469-3475, 2008.
6. Liu, H., Nayak, A., Stojmenovi´c, I., “Fault-Tolerant Algorithms/Protocols in Wireless Sensor Networks”, Guide to wireless sensor networks, Springer, pp.261-291, 2009.
7. Mishra, S., Jena, L., Pradhan, A., “Fault Tolerance in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 10., pp.146-153, 2012.
8. Paradis, L., Han, Q., “A Survey of Fault Management in Wireless Sensor Networks”, Journal of Network and Systems Management, Vol.15, Issue 2., pp.171-190, 2007.
9. Patheja, P. S., Waoo, A., Shrivastava, P., “Fault Tolerant, Energy SavingMethod for Reliable Information Propagation in Sensor Network”, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Vol.1, Issue 4., pp.34-38, 2012.
10. Roumane, A., Kechar, B., Kouninef, B., “Energy Efficient Fault Tolerant Routing Mechanism for Wireless Sensor Network”, Computer and Information Science, Vol.5, pp.68-76, 2012.
11. Salim, S., Javed, M., Akbar, A. H., “A Mobile Agent-based Architecture for Fault Tolerance in Wireless Sensor Networks”, 8th Annual Communication Networks and Services Research Conference, pp.276-283, 2010.
12. Somervill, K. M., “FAULT-TOLERANCE AND RECOVERY IN WIRELESS SENSOR NETWORKS”, Master Thesis Of Science Computer Engineering Old Dominion University, 2009.
13. Srikanth, V., Swathi, D., Tabassum, M., Babu, I. R., “Algorithms for Dynamic Node Events and Fault Tolerance in Wireless Sensor Networks”, IET International Conference on Wireless, Mobile and Multimedia Networks, Vol.7, pp. 235 – 239, 2008.
14. Sujae, P. R., Vigneshpandi, M., “A Cross Layer Fault Tolerant Communication Architecture for Wireless Sensor Networks”, Middle-East Journal of Scientific Research, Vol.20, Issue 10., pp.1292-1296, 2014.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

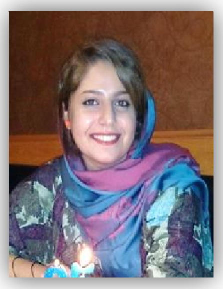
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

15. Tewani, N. N., Ithapu, N., Rao, K. R., Sami, S. N., Pradeep, B. S., Deepak, V. K., "Distributed Fault Tolerant Algorithm for Identifying Node Failures in Wireless Sensor Networks", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.2, Issue 5., pp.79-83, 2013.
16. Yu, M., Mokhtar, H., Merabti, M., "Fault management in wireless sensor networks", IEEE Wireless Communications, Vol.14, Issue 6., pp.13-19, 2007.
17. Yuan, T., Zhang, S., "Secure Fault Tolerance in Wireless Sensor Networks", IEEE 8th International Conference on Computer and Information Technology Workshops, Vol.26, pp.477-482, 2008.

BIOGRAPHY

.



Arezou Chehregosha is currently a M.Sc. student in Computer Engineering (Computer Systems Architecture) at Islamic Azad University, Yazd, Iran. Previous to that, she received her B.Sc. degree in Computer Engineering (Hardware) from University of Isfahan, Isfahan, Iran in 2012.Her researches include hardware implementations in herB.Sc. degree, and image processing and computer networks in herM.Sc. degree period.

Mehran Emadi received the B.Sc. degree in Electrical Engineering (Electronics) in 1995, the M.Sc. degree in Electrical Engineering (Electronics) in 1999 from Islamic Azad University,NajafAbad Branch, Iran, and the Ph.D. degree in Electrical Engineering (Image processing) from University Technology Malaysia (UTM), Malaysia in 2013. His researches include semiconductors in his M.Sc. degree and image processing, computer vision, biometric applications in his Ph.D. degree period. There have been more than 30 technical papers, published by him and he is an assistant professor in Azad University in Iran and now he is the head of Master students in Islamic Azad University, Mobarakeh Branch. He has been working as the program chair, and a committee member for someinternational conferences, and has been training several students in Universities by webinar