

Designing of fault management system for Wireless Active Guardrail System

Luca De Vito, Francesco Paolo Di Candia,
Francesco Picariello, Maria Riccio, Ioan Tudosa

*University of Sannio, Corso Garibaldi, 107, Palazzo dell'Aquila Bosco Lucarelli, 82100 Benevento, Italy
{devito, dicandia, fpicariello, riccio, ioan.tudosa}@unisannio.it*

Abstract- The paper offers a comprehensive study performed in order to design a fault management system, intended to be applied to monitor a Wireless Active Guardrail System (WAGS). An architectural overview of the WAGS sensing capabilities and a list of its possible faults are reported. Two stages of fault detection: (i) sensing node built-in fault detection, and (ii) server side built-in fault diagnostic, are argued and proposed for the future implementation.

I. Introduction

Integration of Wireless Sensor/Actuator Networks (WSNs or WSANs) to the transportation infrastructure (e.g. guardrails) represents a promising technology due to the WSN nodes characteristics (e.g. tiny size, cheap, scalable architecture and low power consumption). In [1] a practical approach of the application of WSN on the guardrails, forming a Wireless Active Guardrail System (WAGS), is presented. This project [1], briefly called "*Barriera Attiva*" - active guardrail, deals with the development and integration to the guardrail plates of WSN nodes in order to create an active role in traffic safety, by using distributed measurement systems along the monitored roads [2],[3]. This proposal is called "*Ideation and processing of a new innovative barrier based on an innovative concept of safety combined with structural function (passive function) and active function*", and it is financed by the Italian Ministry of Education, University and Research. Since these WSN nodes are intended to work in harsh environmental conditions (e.g. rain, snow, low or high environmental temperature), they are subjected by nature to unsatisfactory reliability. Usually, the main faults and failures of a WSN node can be produced by: (i) battery discharge or destruction, (ii) damage of radio transceiver, and (iii) various reasons (e.g. by an external unwanted event like strike, theft, etc.) [4]. From this point of view, in case of "*Barriera Attiva*" project, an investigation of typical faults and failures for the traffic safety WSN nodes was carried out.

This paper aims to: (i) present a list of possible main faults at the level of each type of traffic safety WSN node, (ii) propose a round trip approach of fault detection, diagnosis and solution, and (iii) investigate a possible software tool for fault management, designed to run on the server side. After the introductory Section, the paper is organized as it follows. The second Section describes several related works in the field of WSN fault management. Section III presents an investigation of possible hardware faults, in case of WAGS. The preliminary aspects, related to the architecture design of a software tool used for fault diagnostics and management, are presented in Section IV. Section V concludes the paper.

II. State of the art

Since now, many studies have been carried out regarding to the routing protocols, energy consumption and reliability of WSNs [5]. The current challenges in deploying of WSNs are focused to define and embed several software procedures for an intelligent detection of possible faults and failures. Since the sensors and actuators of the WSN nodes are in contact with the environment, they are prone to faults and failures. Usually, the environment working conditions produce anomalies on the hardware sensing/actuating capabilities and also to wireless connectivity of the nodes. In laboratory, these environmental conditions are hard to be emulated, and for this reason, one exiting challenge is to find an a priori evaluation of the possible faults of nodes. In the following, a short description of several surveyed papers related to the WSN fault diagnosis is firstly presented, and latter, few conclusions are discussed.

A survey of fault management in WSNs is presented in [6]. The paper presents a summary of the existing fault tolerant techniques and discusses several open research directions for practical implementation of such fault management systems. In [7] authors explore a comparative survey of diagnostic tools for WSNs. The paper presents the architectures and constraints of several diagnostic tools, used for post-deployment of WSNs. In this research, a couple of open research issues and a comparative analysis of the presented tools are discussed. In [8] a comparative analysis of fault detection and fault tolerance of WSNs, which is assessed by using: (i) a fuzzy inference system, and (ii) a neural network, in case of correlated temperature measurements, is presented. Authors in [9] present a work, where an intelligent instrument, based on an expert system used for fault diagnosis, is proposed. The presented diagnosis instrument consists of a hybrid inference engine combined with a

rule-based reasoning and a case-based reasoning. The knowledge base was optimally designed and assigned to a database server. Authors added the notion of certainty factor of a prescribed rule, which reflects the estimates of the confidence of the rule validity. The involved certainty factors represent a method of involving the uncertainty evaluation of the applied expert system, in case of using it for fault diagnosis. The authors have reported that the actual implementation of their fault detection and diagnosis system presents a higher efficiency. A fault detection system for WSNs, having online alerts capabilities, is presented in [10]. In order to cover several types of sensor faults, the authors have been focused their work on signal processing techniques (such as, temporal and spatial correlations, and self-organizing maps). A real-time fault diagnosis instrument using knowledge-based expert system is presented in [11]. This instrument uses a valuable knowledge database which was obtained with the help of technical experts and operators. The presented inference engine is built upon a fuzzy logic implementation. The fuzzy logic takes into account the parameters available in a knowledge database and uses also the real-time data provided by the real sensors. In [12] a novel self-diagnosis framework for fault diagnosis, in a large scale WSN, is presented. Authors designed a fault detection algorithm based on multiple nodes which cooperates among them in order to provide the final diagnosis result. This algorithm is based on a finite state machine implementation. A remote monitoring of a wireless network is presented in [13]. The authors have proposed a latent network diagnosis system which was tested in case of industrial sensor networks. The proposed tool employs a method based on packet sniffing, in order to evaluate instantaneously the performance of network and its efficiency. A propagation of fault-tolerant data packets in WSNs, using local additional network information, is proposed and described in [14]. In this study, the effect of failures and the communication protocol behavior are presented in detail. A large scale simulation was performed and, according to presented state of the art, the results were declared robust. Furthermore, in [15] a network fault model used to assess the dependability of networked embedded systems is presented. The proposed fault model and its possible applications are described in few scenarios. A novel strategy for sensor fault detection is described in [16]. In case of large WSNs, authors have presented a distributed fault detection algorithm. The faulty WSN nodes are being identified by taking into account the similarity of data, retrieved from the neighboring nodes. The faulty decision is done at the level of each node. The spatial and temporal correlations are used in this algorithm and the provided results for the faulty nodes are declared efficient. In [17] a classification of several debugging techniques of WSNs is presented. Authors divided the debugging tools, according to their usage in application life cycle, as: (i) pre-deployment, (ii) post-deployment, and (iii) deployment-time validation. Furthermore, they have classified the debuggers as: (i) software based, (ii) hardware-based, and (iii) hybrid. The key characteristics, which are required in case of implementation of an efficient debugging tool for WSNs, are described. From the works quoted above, the needs of fault management tools for the WSNs are summarized. A set of proposed fault management systems was presented and it was highlighted the relation between their capabilities and the used method of fault detection. In general, in order to carry out a centralized analysis of faults, the existing approaches of diagnosis of the WSNs for faulty nodes are sink-based (e.g. the root node). These procedures of fault management requires a large amount of data communication between sensing nodes and root nodes, and this represents the main disadvantage from the point of view of the traffic load on the network. In these multisensory measurement systems, special attention has to be paid to implement several additional capabilities of fault detection on each WSN node. If one or more sensors from a WSN node are faulty, it is necessary also to take into account a local test procedure, in order to test if this node can be used as a communication node in the network. If the RF transceiver is out of order (e.g. due to the electrostatic discharges phenomenon, [18]), from the networking capabilities point of view, the node will be in an offline state. According to the “*Barriera Attiva*” project development stages [1], it is necessary to design a WSN capable of fault detection. From the above observations, it should be highlighted the need of implementation of local fault detection capabilities for each WSN node.

III. Possible faults in a WAGS

In [2] and [3] the architectures of a modular sensor/actuator node, developed for the WAGS, are presented. One important component of the WSN node is represented by the IRIS module, which has embedded an Atmel ATmega1281 microcontroller (μC) and a compliant IEEE 802.15.4 radio frequency (RF) transceiver. The available sensors and actuators, embedded on the WSN nodes, are more prone to faults due to harsh environmental condition in comparison with the IRIS module. In Figure 1, the architectural overview of the WSN node designed for traffic safety measurements is depicted. This WSN node consists of: (i) two infrared sensors (S_1 and S_2) and an electronic interface which forms the speed measurement system, (ii) an 3-axis accelerometer sensor plus an electronic interface, forming the impact detection system; (iii) an ultrasonic transmitter (T) and receiver (R) sensor and an electronic interface which forms the proximity measurement system, and (iv) one buzzer and five RGB LEDs plus their electronic interface, which forms the actuators [3].

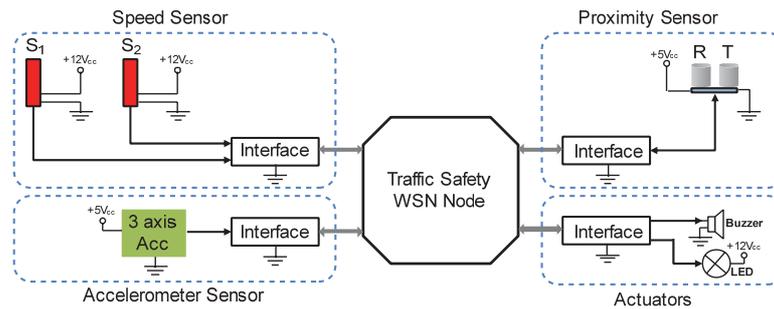


Figure 1. Architecture overview of the traffic safety WSN node.

In Figure 2, the architectural overview of the environmental monitoring WSN node is depicted. This WSN node consists of: (i) three gas sensors, (ii) one particulate matter (PM) sensor, (iii) one temperature sensor, and (iv) one humidity sensor. The concentrations of: (i) carbon monoxide (CO), (ii) nitrogen dioxide (NO₂) and (iii) sulfur dioxide (SO₂) gases will be measured. Each gas sensor (CO, NO₂ and SO₂) is mounted on a Digital Transmitter Board (DTB). These DTBs include some analog and digital circuitries which are used to convert the μ A output signal, generated by each sensor, into a 2-wire transmission line, and furthermore, the outputs of DTBs are connected through an analog interface to the IRIS module. The PM is a dust sensor which uses an optical sensing system and generates a proportional voltage to the particulate concentrations, available in the tested air. This sensor is connected via an analog interface to the IRIS module. The measurement of relative humidity is based on a capacitive sensing system and the measurement of temperature is based on the band gap effect in semiconductors. In Table 1, the list of: (i) sensor/actuator name, (ii) sensing/actuating types, (iii) input/output signal, (iv) the interface, and (v) power supply requirements, are presented.

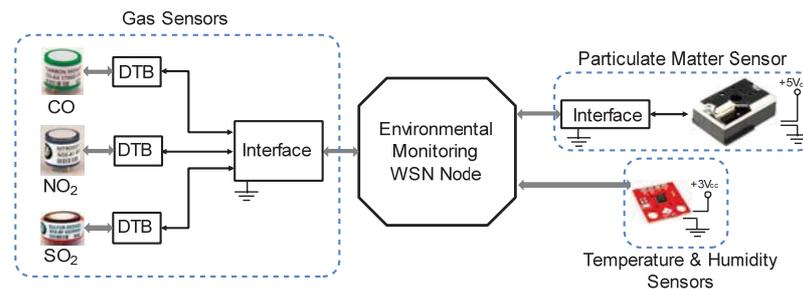


Figure 2. Architecture overview of the environmental monitoring WSN node.

In order to propose and design a fault management system for WAGS, an a priori list of possible faults of hardware components was investigated. According to the presented sensing and actuating principles from Table 1, the list of: (i) implemented measurement systems, (ii) number of sensors/actuators involved in each measurement system, and (iii) the possible faults of hardware components, is presented in Table 2.

Table 1. Sensors used in “*Barriera Attiva*” project.

No.	Sensor/Actuator name	Sensing/Actuating Type	Input/Output signal	Interface	Power supply requirements
1.	XUX1ANANM12	Infrared beam, use reflector;	Digital signal; level: 12V;	Transistor based;	12V, ~35mA
2.	Parallax PING)))	Ultrasonic burst;	Time modulated signal; level: 5V;	Dual supply digital level shifter;	5V, ~30mA
3.	ADXL326	Three axis capacitive accelerometer;	Analog signal; levels: 0÷3V;	Analog interface;	3V, ~350 μ A
4.	CO-AX, SO2-AF, NO2-A1	Electrochemical;	Current output; levels: 4÷20mA;	Trans-impedance amplifier; Digital Transmitter Board (DTB);	12V, ~25mA
5.	GP2Y1010AUOF	Optical;	Analog signal; level: 0.9÷3.4V;	Transistor based;	5V, ~20mA
6.	SHT25	Humidity - capacitive; Temperature – based on band gap;	I ² C interface; level: 3V;	Analog interface;	3V, ~300 μ A
7.	BlinkM LED	Programmable full-color RGB LED;	I ² C interface; level: 3V;	Dual supply digital level shifter;	3V, ~60mA
8.	KPEG122	Piezo buzzer;	Digital signal; level: 3V;	Transistor based;	5V, ~ 8 mA

Table 2. List of the possible hardware faults of the implemented sensing capabilities.

No.	Implemented system	Number of sensors/actuators	Possible faults of hardware components
1.	Speed measurement using two infrared beams	- two intelligent infrared sensors and two polarized reflectors, electronic interface;	- Obstruction of optical lens; - Internal power supply; - Transistor fault, short-circuits.
2.	Proximity measurement using ultrasound bursts	- one transmitter, one receiver, electronic interface;	- Ultrasonic transmitter fault; - Ultrasonic receiver fault; - Internal power supply fault; - Digital level shifter.
3.	Impact detection	- one 3-axis capacitive accelerometer;	- Internal power supply fault; - Incorrect acceleration values.
4.	Light and sound alerts	- five RGB LEDs, one buzzer;	- Internal power supply fault; - RGB LED fault; - MOSFET fault; - Buzzer fault; - Transistor fault.
5.	Gas measurement	- three electrochemical sensors (CO, SO ₂ , NO ₂), one digital transmitter board (DTB) for each sensor, one trans-impedance amplifier for each sensor;	- Internal power supply fault; - Trans-impedance amplifier fault; - Electrochemical sensing element fault; - Digital Transmitter Board (DTB) fault.
6.	Particulate matter measurement	- one LED, one light-sensing element;	- Internal power supply fault; - Internal led diode fault; - Internal light-sensing element fault; - Obstruction of the light-sensing element; - Transistor fault.
7.	Temperature and humidity measurement	- one humidity sensor based on capacitive type, one temperature sensor based on band gap;	- Internal power supply fault; - Internal humidity sensor fault; - Internal temperature sensor fault.

From the hardware architecture point of view of a WSN node, there are three major categories of faults/fails which can occur. These failures can be assessed by: (i) battery discharge, (ii) radio transmission, and (iii) sensors/actuators. The faults of sensors/actuators components were obtained by consultation of datasheets, application notes and hardware schematics by the experienced hardware engineers. In particular, the battery represents a crucial component of the each WSN node [2],[3],[16].

IV. Designing of fault management system for a WAGS

In Section II, a short survey of existing approaches for fault detection and diagnosis from different WSN applications was presented. By taking into account the state of the art and Table 2, in the following, a practical solution in order to design a fault management system is presented. Monitoring the WAGS health, by means of wireless data sets, provides a fundamental support for an efficient management of the entire network. A practical strategy of fault detection from WSN nodes should consist of two phases. A first phase of faults/failures diagnosis of a WSN node is represented by their built-in capabilities. In order to create a better management of faults/failures, on each WSN node it should be embedded some built-in fault detection possibilities. If the WSN node has detected a possible fault of its sensing/actuation systems, a message will be sent over the network to the server side to inform a Supervisor about the appeared problem. The second phase consists of providing a full diagnostic by the specialized software running on the server side, in order to offer a solution for the existing problem. In case of WAGS, these two main approaches of fault diagnostics were investigated and in the following, they are presented.

A. WSN node built-in fault detection

Since the WSN nodes are intelligent embedded systems, they should be able of on-line processing functions for the detection of faults. Such on-line processing functions could be [4]: (i) software built-in tests, (ii) hardware built-in tests, (iii) fault detection, identification and recovery, and (iv) fault tolerance and redundancy management.

In Table 3, a set of possible faults, which can be detected by using the built-in software/hardware procedures of each WSN node, are presented. These faults can be detected by designing of several built-in software/hardware procedures on each WSN node. The WSN nodes sensing/actuating capabilities are divided into two main categories: (i) traffic safety, and (ii) environmental monitoring. Each fault is coded as *Node ID sensor name*, where *Node ID* represents the identifier assigned to that WSN node, followed by the sensor name. These faults should be sent by each WSN node to the server in order to provide a diagnostic and to find a proper solution for solving the assessed faults. If a WSN node is faulty due to the battery discharge or radio transmission, in the following phase, by using the WAGS network capabilities a possible solution for such types of faults is provided.

Table 3. The sensors/actuators fault possibilities according to the implemented functionalities.

Node role	Implemented Functionalities	Sensor/Actuator	Fault code name	Index
Traffic safety measurement	Speed	S1	Node_ID_S1; fault of sensor S1;	1
		S2	Node_ID_S2; fault of sensor S2;	2
		S1, S2	Node_ID_S1S2; faults of sensors S1 and S2;	3
	Proximity	Ultrasound Transmitter	Node_ID_US_T; fault of ultrasonic transceiver;	4
		Ultrasound Receiver	Node_ID_US_R; fault of ultrasonic receiver;	5
	Impact detection	Accelerometer	Node_ID_ACC; fault accelerometer;	6
	Light flash	LED	Node_ID_LED; fault of LED;	7
Sound beep	Buzzer	Node_ID_B; fault of buzzer;	8	
Environmental monitoring	Gas measurement	CO, NO ₂ , SO ₂	Node_ID_GAS; fault of a gas sensor (or more than one);	9
	Particulate matter	PM ₂ , PM ₁₀	Node_ID_PM; fault of PM sensor;	10
	Temperature & humidity	Temperature, Humidity (T&H)	Node_ID_T_H; fault of T&H sensors;	11

B. Server side built-in fault diagnostic

According to the WAGS functionality, the monitoring of the entire network can be done in two ways: active and passive. Passive monitoring means that the fault event is reported when a WSN node goes offline from the radio communication point of view [6]. Beside this, active monitoring can be done by assessing probes (query or keep alive packets) for each WSN node, [6],[10]. By doing this type of interrogation with probes, the network traffic can be overloaded, and to avoid this, an optimization procedure of the frequency of query packets should be investigated. Since the radio communication capability of each WSN node has a possibility to failure, the network topology/links need to be changed dynamically (see Figure 3).

Due to different environmental conditions, the communication links between two adjacent WSN nodes may fail temporary or permanently [4]. Furthermore, packet losses, network attacks, traffic congestion, and so on, may occur [5],[6]. In case of a WAGS, the traffic congestion may appear due to the simultaneous communications of WSN nodes, when fault events or scheduled data, are required to be transmitted to the server side.

According to [2] and [3], the WAGS network architecture at the WSN node level is based on multi-hop communication. In Figure 3, a round-trip fault diagnostic and repair scenario for a WAGS is presented. For example, if a battery fails, the node automatically goes in off mode. This failure will be detected from the WAGS network by means of missing capability of link communication with the rest of the neighboring nodes.

One possibility of detection of the radio transmission failures can be assessed as it is described in the following: (i) the node N_n does not transmit data; (ii) if the nodes N_{n-1} or N_{n+1} wants to communicate with the node N_n and the acknowledgement link is not confirmed, then the nodes N_{n-1} and N_{n+1} will count the event; and (iii) the nodes N_{n-1} and N_{n+1} will establish between them a communication link, and in a latter phase, they will sent this event to the *Server* in order to highlight the communication failures with the node N_n (see Figure 3). The *Server* will alert the *Monitoring Service System* (MSS) about the existing problem, where a human *Supervisor* will pass the received fault to an engineer/technician.

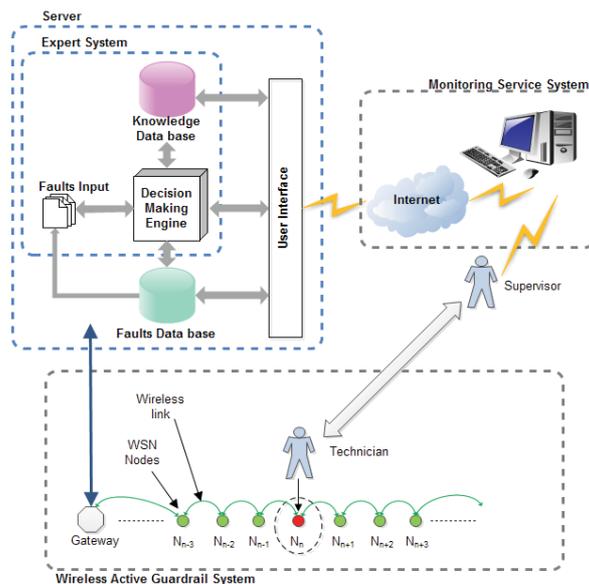


Figure 3. Round trip fault diagnostic and repair scenario.

Since the nodes N_{n-1} and N_{n+1} have been alerted the *Server* about the communication fault of the node N_n (forward trip), there will be a necessary second trip on field to be done, where the node N_n is located (backward trip). All the entire network status can be analyzed by the MSS which interacts with the *Server* according to [3]. According to the discussed ideas in [8],[9] and [11], in case of WAGS, an *Expert System* which will process the received fault symptoms from each faulty WSN node, can be implemented and tested for the future developments. This *Expert System* should consist of: (i) online *Faults input*, used to store all received fault symptoms; (ii) a *Knowledge Data base*, which will contain a list of possible faults of each measurement/actuation system; (iii) one *Decision Making Engine*, used to process the received faults and to provide an online diagnosis of each faulty WSN node; and (iv) an *User Interface*, used by the MSS to interact online with the *Expert System* and with *Faults Data base* from the *Server*. In general, there are a set of limitations of software

decisions (done by the *Expert System*) regarding to the faults/failures assessment [11]. Usually, on field, the technician investigates deeply the reason of the node N_n failure, by using the information provided by the *Server* in order to fix the assessed faults. Furthermore, all of the presented fault scenarios are worsened by the multi-hop communication of WSN nodes. In case of WAGS, for the nodes N_{n-1} and N_{n+1} tens/hundreds of hops are needed to reach the gateway node in order to deliver a data packet. Additionally, if traffic congestions appear in a local area, these can be propagated to all communication ways until the gateway node is achieved. This will affect the data delivery from one region to the other regions of the network. In case of the WAGS, by taking into account these issues, further investigations of the routing protocol should be carried out.

V. Conclusions

In the paper an investigation of the possible faults and failures which can occur in the sensing capabilities of WAGS has been discussed. The architectural overviews of the proposed traffic safety WSN nodes have been presented. A main outcome of this research is the realization of the lists of the possible hardware faults of the implemented sensing/actuating capabilities of each traffic safety WSN node. Further work is directed to develop a database which will contain the knowledge base for the WAGS fault management system.

Acknowledgment

The authors wish to thank Prof. Pasquale Daponte and Prof. Sergio Rapuano for their helpful suggestions during all the phases of the present work. The paper has been supported from Grant no. PON01_03100, "Ideation and processing of a new innovative barrier based on an innovative concept of safety combined with structural function (passive function) and active function", financed by the Italian Ministry of Education, University and Research.

References

- [1] Project PON01_03100, "Barriera Attiva". Available: <http://www.barrieraattiva.unisannio.it>.
- [2] L.De Vito, V.Cocca, M.Riccio, I.Tudosa, "Wireless active guardrail system for environmental measurements". Proc. of IEEE Workshop on Env., Energy, and Structural Monitoring Systems, Perugia, Italy, 28 Sept. 2012, pp.50-57.
- [3] P.Daponte, L.De Vito, F.Picariello, S.Rapuano, I.Tudosa, "Wireless sensor network for traffic safety". Proc. of IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems, Perugia, Italy, 28 Sept. 2012, pp.42-49.
- [4] A.Mahapatro and P.Khilar, "Fault diagnosis in wireless sensor networks: a survey". IEEE Communications Surveys & Tutorials, No.99, 2013, pp.1-27.
- [5] M.O.Farooq and T.Kunz, "Operating systems for wireless sensor networks: a survey". Journal Sensors 2011, vol.11, pp.5900-5930.
- [6] L.Paradis and Q.Han, "A survey of fault management in wireless sensor networks". Journal of Network and Systems Management archive, vol.15, Issue 2, June 2007, pp.171-190.
- [7] A.Rodrigues, T.Camilo, J.Sa'Silva and F.Boavida, "Diagnostic tools for wireless sensor networks: a comparative survey". Journal of Network and Systems Management, June 2012, Online, pp.1-45.
- [8] S.Abbas Khan, B.Daachi and K.Djouani, "Application of fuzzy inference systems to detection of faults in wireless sensor networks". Journal of Neurocomputing, vol. 94, 2012, pp.111-120.
- [9] Y.Lai, X.Li, Y.Xiong and P.Du, "Design of an efficient intelligent instrument fault diagnosis expert system". IMACS Multiconference on Computational Engineering in Systems Applications (CESA), 4-6 Oct. 2006, Beijing, China, pp.1756-1761.
- [10] M.Sarkis, D.Hamdan, B.El Hassan, and O.E.Aktouf, I.Parississ, "Online data fault detection in wireless sensor networks". Proc. of 2nd Int. Conf. on Advances in Computational Tools for Engineering Applications (ACTEA), 12-15 Dec. 2012, pp.61-65.
- [11] C.Nan, F.Khan and M.T.Iqbal, "Real-time fault diagnosis using knowledge-based expert system". Journal of Process Safety and Environmental Protection, vol. 86, Issue 1, January 2008, pp.55-71.
- [12] K.Liu, Q.Ma, X.Zhao and Y.Liu, "Self-diagnosis for large scale wireless sensor networks". Proc. of IEEE INFOCOM, 10-15 Apr. 2011, pp.1539-1547.
- [13] S.M.A.Zaidi, J.Jung, M.Kang, B.Song and K.H.Kim, "Remote industrial sensor network monitoring using M2M based ethical sniffers". Journal of Distributed Sensor Networks, Nov. 2012, pp.1-9.
- [14] I.Chatziannakis, A.Kinalis and S.Nikolsetas, "Fault-tolerant and efficient data propagation in wireless sensor networks using local, additional network information". Journal of Parallel and Distributed Computing, vol. 67, Issue 4, April 2007, pp.456-473.
- [15] F.Fummi, D.Quaglia and F.Stefanni, "Network fault model for dependability assessment of networked embedded systems". Proc. of IEEE Int. Symposium on Defect and Fault Tolerance of VLSI Systems, 1-3 Oct. 2008, pp.54-62.
- [16] C.Zhang, J.Ren, C.Gao, Z.Yan and L.Li, "Sensor fault detection in wireless sensor networks". Proc. of IET Int. Communication Conf. on Wireless Mobile and Computing (CCWMC 2009), 7-9 Dec. 2009, pp.66-69.
- [17] T.R.Sreedevi and S.Mary Priya, "A classification of the debugging techniques of wireless sensor networks". Proc. of Int. Conf. on Advances in Computing and Communications, 9-11 Aug. 2012, pp.51-57.
- [18] J.P.Carmo, P.M.Mendes, F.Ribeiro, C.Couto and J.H.Correia, "Effects of the ESD protections in the behavior of a 2.4 GHz RF transceiver: problems and solutions". Proc. of IEEE International Symposium on Industrial Electronics, June 30 2008-July 2 2008, Cambridge, UK, pp.935-938.