Modeling and Enhancing Reliability of Wireless Sensor Network – A Review

Mayurika JB

Lecturer

Department of Electronics, Government Polytechnic College, Jodhpur, Rajasthan, India

***Abstract*—Advancement in wireless sensor networks technology enables a wide range of applications such as health care, industrial automation, ambient conditions monitoring and security and defense systems. WSNs designers are facing many challenges in meeting application requirements e.g. reliability, fault tolerance, lifetime, throughput and responsiveness etc as application requirements and environmental conditions change over time. Failure of WSN may result catastrophic consequences like loss of life in the case of health care application and major disasters in the case of defense systems. Design of reliable wireless sensor network (WSN) need to address the failure of single or multiple network components and implementation of the techniques to tolerate the faults occurred at various levels. The issues and requirements of reliability improvement mechanism depend on the available resources and application for which the WSN is deployed. This paper discusses the different modeling approaches to evaluate the reliability and classification of the approaches to improve it. Also the paper analyzes reliability enhancement by existing fault tolerant methods in WSN and compares the performance of these techniques with the technique we developed.**

I*ndexTerms* — Component Reliability Modeling, Reliability Measure, WSNs, BS, QoS, GPS.

I. INTRODUCTION

A Wireless Sensor Network is a group of spatially distributed sensors to monitor the physical or environmental conditions so that data can be transferred from the source to the destination. Though Wireless Sensor Networks were initially motivated by the defense applications but nowadays they have been the preferred choice for the design and deployment of next generation monitoring and control systems. The WSN is buildup of hundreds and thousands of "nodes" where each node is connected to sensor(s). Small size and low cost of the nodes make them attractive for widespread deployment and also causes a disadvantage of low-operational reliability. Sometimes due to the failure of some of its nodes, the sensor network communication fails. Sensor nodes can fail, due to number of facts, such as exposure to harsh environments or simply energy depletion, and influence WSN dependability. In order to face this problem, and exploring the fact that WSN use several nodes, several fault tolerance measures proposed in the literature rely on the inherent node redundancy.

The reliability improvement process is an iterative process that is applied step by step in each stage of implementation of WSN. It can be improved one or multiple components like hardware, software or any ser- vice/functions of the network in order to achieve mini- mum required reliability. One of the approaches to improve the reliability of a system is fault tolerance (FT) defined as tolerating the faults which may occur during node placement, topology control, target or event detection, data aggregation, routing and information processing. Fault tolerance, is achieved by hardware or information redundancy. Usually redundancy can result in increased design complexity and increased costs but redundancy is an inherent property of the sensor network. Nodes in WSNs are prone to be failure due to energy depletion, hardware failure, communication link errors, malicious attack etc can be tolerated by hardware and software redundancy, which in turn improves the inherent reliability, and information redundancy and time redundancy will improve the operational redundancy.

Historically, WSNs have been characterized as wireless networks consisting of numerous small, energy constrained, low cost and autonomous nodes that are distributed over an area for the purpose of monitoring or sensing the physical entities such as temperature, light, motion and humidity. Communication or relaying of data typically occurs via wireless multi-hop routing. The majority of WSNs described in the literature exhibit a (source, sink) architecture, which may include any number of: **Source nodes:** which generate data, usually by using sensors to measure environmental factors such as temperature, humidity or radiation, **Sink nodes:** which collect the data gathered by source nodes and **Intermediate nodes:** which may include source nodes that aid the transmission from source to sink.

The generation of data at source nodes may occur either proactively or in response to some request. Sink nodes which are often referred to as base stations (BS), may be high powered, linked to databases via satellite links or have more resources than other nodes. WSN nodes are typically battery powered and the energy capacity of a battery is dependent on its size and since nodes are expected to be small, the batteries are unlikely to be of high capacity. Battery depletion is one of the key challenges in developing and working with WSNs, particularly since every operation performed by the node requires expenditure of energy. While other resources such as the CPU and memory may be immediately re-used when released, the same is not true of the battery. Unless a node has some means of energy replenishment, the capacity of batteries restricts both the maximum lifetime of nodes and the frequency with which the node can carry out particular actions. Beyond these characteristics, it is difficult to provide a formal definition of the exact capabilities of a WSN, particularly due to the increasing number of scenarios making use of the technology. It has been theorized that, with WSNs typically being application dependent, it is impossible to create a single architecture, which can be used in all applications.

Wireless technology has been traditionally used to connect people to each other or to devices. Cellular systems, wireless local area networks and broadband wireless access aim to provide voice and data communication. WSNs on the other hand have introduced a plethora of applications from traffic monitoring to health, from battlefield to surveillance and security by providing communication between devices. Recent developments in sensor technology and low power radios have enabled the widespread deployment of sensor networks consisting of small sensor nodes with sensing, computation, and communication and actuation capabilities. An individual sensor node collects data from the environment, performs local processing of data including quantization and compression, communicates its results to a data fusion center via a wireless medium and takes an action in response. Since a single sensor provides only limited information, a network of these sensors is used to manage large environments.

II. Literature Review

In WSN a large number of sensor nodes continually sense data from the environment and the critical event data need to be reliably delivered to the sink. The sink receives all the information from these sensor nodes, processes it and sends them to the end user. Therefore, given the nature of error prone wireless links, presence of moving nodes and failing nodes, ensuring reliable transfer of data from resource constrained sensor nodes to the sink is one of the major challenges in WSNs. There is extensive research done on reliable transport protocol and survey on existing data transport reliability protocols in wireless sensor networks is presented in some references. The network may be congested and sensor nodes may drop packet when the data packets generated by a large number of sensor nodes exceed the network capacity. In order to achieve reliability, the dropped packets must be re-transmitted which in turn leads to wastage of energy and bandwidth, very important stringent factors in WSN. Thus the reliability enhancement is achieved with the trade between reliable data transmission and network resources. In order to mitigate this problem, the reliable transport protocol consists of two essential mechanisms: congestion control (detection and avoidance), and loss detection and recovery with the minimum possible energy consumption. A Comparison between the protocols based on the method by which it recover the losses (End to End recovery, Hop to Hop recovery), messages to detect losses control congestion, type and level of reliability, energy efficiency, packet-driven reliability or event- driven reliability. Also a classification of reliability as Packet or event reliability is concerned with how much of information is required to notify the sink of an occurrence of something happening in the environment.

It is well accepted that a sensor network should be deployed with high density, in order to prolong the network lifetime. Sensor data collected from such network is likely to be highly correlated and redundant, so a function density control controls the density of the active sensors to certain level. At any instant of time only a subset of sensor nodes will be active, sensed and report to sink while other sensors are inactive must guarantee sufficient sensing coverage and connectivity reliabilities. The performance metrics of interest are 1) the percentage of coverage, i.e. the ratio of the covered area to the total area to be monitored; 2) the number of working nodes required to provide the percentage of coverage in 1); and 3) α-lifetime, defined as the total time during which at least α portion of the total area is covered by at least one node. The ability to report the Sink node is called as connectivity. A network is said to be fully connected if every pair of node can be communicated with each other either directly or via intermediately relay nodes. It is important to find the minimum number of sensors for a WSN to achieve the connectivity. The connectivity of a graph is minimum number of nodes that must be re- moved in order to portion the graph in to more than one connected component. Connectivity affects the robustness and throughput of the wireless sensor network. Both the coverage and connectivity are related to each other for improving the performance of Wireless sensor net- works. The issues in maintaining sensing coverage and connectivity by keeping a minimum number of sensor nodes in the active mode in wireless sensor networks are presented in. Various approaches to model the coverage are compared based on how they address the issues in coverage; some of them are coverage types, deployment strategy, sensing model, sensing area and nature of the algorithm. The system parameters, such as the initial energy of a node, the radio transmission rate, and the energy consumption rate, are assumed to same for all the nodes.

III. Reliability Modelling and Analysis Methods

Reliability is one of the most important performance measures and high level of reliability is a significant requirement for a wireless sensor networks using in Indus- trial and medical environments. Reliability level of the network can evaluated using the tool called as reliability modeling. Reliability modeling and analysis are key steps to the design and optimization of sensor network systems. The approach generally taken to investigate the reliability of a highly reliable WSN is

1) Develop a mathematical model of the reliability measure of the network;
2) Measure or estimate the parameters of the model;
3) Compute the network reliability based upon the model and the specified parameters.

During the deployment of WSN, reliability modeling can be used to predict the performance of the network elements to provide the information for the design of WSN suitable for an application in hand. For a network already deployed in the field reliability modeling combined with failure data analysis, can be used to identify the critical components, apply Fault tolerance and enhance reliability.

Reliability Measure

The There exist a number of reliability measures for a wireless network depending on the network and its applications. For a telecommunication network it is obviously communication issues that meet certain connectivity requirements. Whereas for the sensor network the focus is on information gathering, processing and communication issues to meet the coverage and connectivity requirements. Different criteria can be considered in order to express or measure the reliability of a network. The main ones are the following:

- Reliability measure of connectivity falls within any one of the categories, which are 2-terminal reliability, k-terminal reliability, all terminal reliability and many sources to terminal reliability. For example 2-terminal reliability can be computed using computationally efficient source to terminal path sets or cut sets enumeration algorithm;
- Hardware reliability measures are MTTR and MTTF;
- The coverage re liability measure is guaranteed de-sired level of coverage (at least k-coverage) of event or target at all times formulated by either Boolean sensing model or collaborative sensing model;
- Capacity/Max flow measure is defined as the probability that the maximum flow of the network is not less than the given demand.
- QoS reliability measure is guaranteed date transfer timely and guaranteed bandwidth data accuracy timely depends upon user/applications demand;
- Information reliability ensures that the nodes transmit to the sink only information concerning significant events or targets.

Each reliability measure is concerned with the ability of a network to be available to provide the desired service to the end user.

Classification of Reliability Modeling and Evaluation

Reliability of WSN, depends on combination of hard- ware, software and wireless link is modeled in many ways analogous to reliability modeling of hardware system. Reliability modeling aims at using abstract representation of the network as means for assessing their reliability. The basic reliability modeling techniques available in the existing work in WSN field are classified as shown in Figure 1.

Two of the most commonly used Deterministic reliability modeling and analysis methods are First Order Reliability Method (FORM) and the Second Order Reliability Method (SORM). The advantages of the techniques is less computational effort than Probabilistic models, but not suitable for modeling the reliability of real time applications of WSN. In a more restrictive sense, the term reliability is defined to be the probability that a wireless sensor network performs its mission successfully. Because the mission is often specified in terms of time, reliability is often defined as the probability that a system will operate satisfactorily for a given period of time. Thus reliability may be a function of time and can be estimated essentially using probability modeling. When the set of operating components and the set of failed components of a network are specified, it is possible to compute the probability that the system is operating and thus the reliability of the system. In probabilistic modeling, the concepts and methods of probability theory to compute the reliability of a complex system like sensor network.

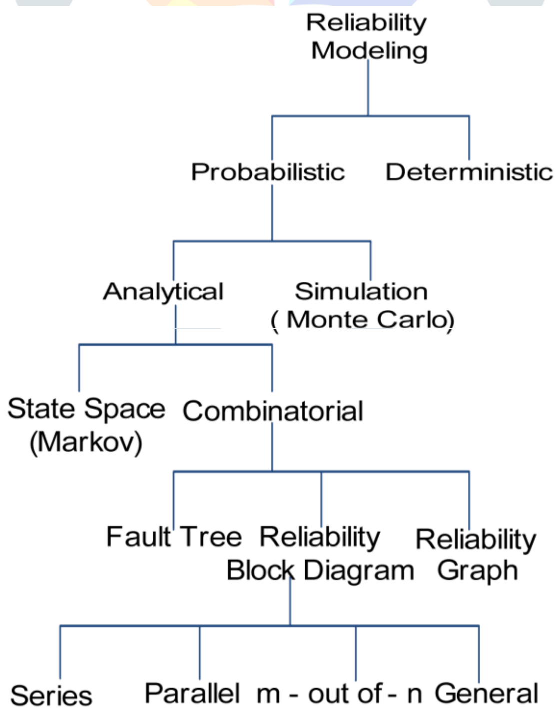

Figure 1: Classification of reliability models.

IV. RELIABILITY IMPROVEMENT IN WSN

The approaches proposed to reinforce the network reliability, provide a method for maximizing reliability under certain given constraints and WSN has sensor node constraints like battery power, transmission range, sensing range and processor capability. In addition network constraints are ad hoc nature, data rate, packet size, wireless link, scalability, security, dynamic topology and cost constraints. For WSN the focus is on sensing, processing and communication issues that meet some reliability measures and requirements. The communication issue has to meet the connectivity requirements so that the end user is able to access the network and receive the information sensed and processed by the sensor nodes. Achieving the overall network reliability of the communication process is to construct a network the minimum number of reliable links and each link must be economically feasible. The transport layer of WSN provides mechanisms for establishing a connection between sensor network and end users, while supporting Quality of Service (QoS) mechanisms to ensure the properties of the link lives up to a required quality of connection and reliability. In general, there are several approaches to achieve reliability against unreliable link, e.g., automatic repeat request, multi-path routing and source coding. On the other side the overhead increases and network be- come overloaded. That is, these traditional approaches are not suitable for WSN, many research works concentrate in improving the existing transport layer protocols or developing new efficient reliable data transfer scheme that satisfy the constraints and improve the performance. To cope with the above issues, many works has been proposed for efficient reliable data transfer scheme, some of them are network coding, cross-layer strategy that considers physical layer (i.e., power control), MAC layer (i.e., retransmission control) and network layer (i.e., routing protocol) jointly, hybrid method based on multipath data sending and behavior-based trust mechanism. Scalability is one out in WSN through efficient clustering. The cluster head node is used to receive data from other nodes in the cluster, aggregate it and then transmitting the processed information. Data aggregation is a process whereby data from sensors in an area is gathered for performing fusion to eliminate redundant data to provide the useful fused information to the base station and improve reliability and life time of the network. The clustering and cluster head selection process involves many issues of power efficiency, traffic distribution, link quality distance to sink etc to guarantee reliability. Aggregated values when transmitted to sink, aggregated values from other clusters can be fused using in the intermediate nodes to reduce traffic in WSN. Rule based Fuzzy logic, trust based, weight based, rough set theory are some of the secure and reliable techniques to tolerate faulty nodes and improve the credibility of the fused content in the presence malicious nodes.

V. FACTORS AFFECTING RELIABILITY IN WSN

A basic way to improve the reliability is to have redundant components; it may be hardware, software or information. Reliability analysis of the WSN provides a measure of the performance of the WSN. As the importance of reliability in WSN is discussed in the previous section, this section it is appropriate to investigate the factors affecting reliability so that the reliability can be improved by improving these parameters. In order to ensure that the network supports the application's requirements, it is important to understand how each of the categories of wireless sensor networking affects reliability. Challenges to achieving reliability on Wireless Sensor Networks can be divided to four main categories which are network elements, networking characteristics, conditions in which WSN is deployed and strategies used to design the network for an application are represented in Figure 2.

The first kind of problems comes from the limited resources of Wireless Sensor Networks nodes. A sensor node has a limited power without recharging capability affects the hardware reliability. The node is able to sense the environment using sensors and ADC used to convert to digital signal has low accuracy and low resolution will affect the information reliability. Similarly the processor with low computational power and memory space affects the Quality of Information (QoI).

Next kind of problems comes from software engineering point of view adds more challenges to achieve reliability of sensor network. In general, sensor networks software can be layered into levels: sensor node software, middleware and sensor network software. The sensor node software is the bottom layer contains sensor soft- ware and node software. The sensor software (Operating System) has full access to the sensor hardware, execute the process by which events occurred in the real world is sampled and converted into machine-readable signals. Malfunction or bucks in the software or programs will affect the QoS and information reliability. The node software process the raw data, receive and process the query and transmit the data to toe next node includes system software for network maintenance and application specific software related with packet reliability.

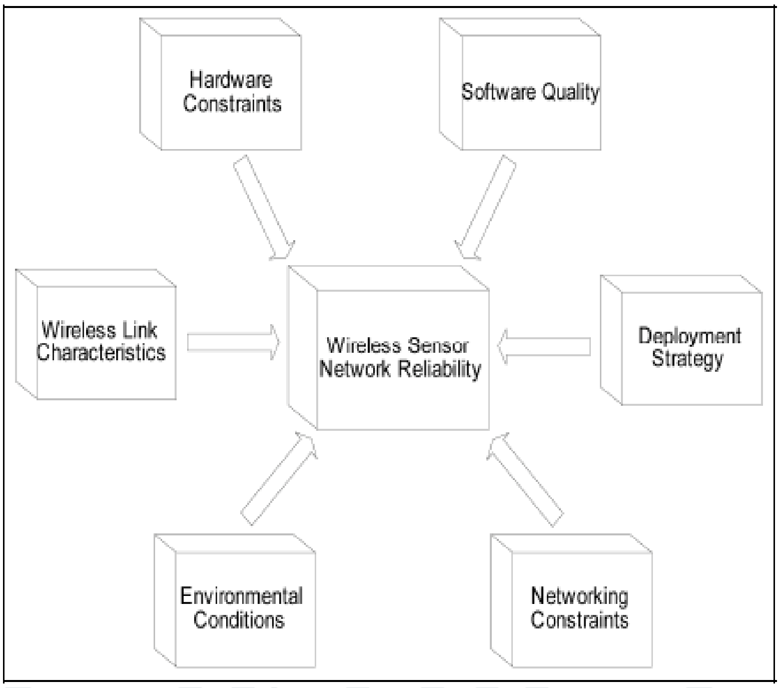

Figure 2: Factor Influence the reliability in WSN

Challenges in Wireless Sensor Networks

The characteristics of sensor networks and requirements of different applications have a decisive impact on the network design objectives and challenges in terms of network capabilities and performance. Sensor nodes are small-scale devices with volumes approaching a cubic millimeter in the near future. Such small devices are very limited in the amount of energy they can store or harvest from the environment. Furthermore, nodes are subject to failures due to depleted batteries or, more generally, due to environmental influences. Limited size and energy also typically means restricted resources (CPU performance, memory, wireless communication bandwidth and range). Extending lifetime and energy efficiency are also important objectives and challenges in WSNs [9].

Node mobility, node failures and environmental obstructions cause a high degree of dynamics in WSN. This includes frequent network topology changes and network partitions. Despite partitions, however, mobile nodes can transport information across partitions by physically moving between them. However, the resulting paths of information flow might have unbounded delays and are potentially unidirectional.

Communication failures are also a typical problem of WSN. Another issue is heterogeneity. WSN may consist of a large number of rather different nodes in terms of sensors, computing power and memory. The large number raises scalability issues on the one hand, but provides a high level of redundancy on the other hand. Also, nodes have to operate unattended, since it is impossible to service a large number of nodes in remote, possibly inaccessible locations. The design and development of a successful network must address many challenges dictated by WSN characteristics on one hand and the applications on the other. Few major challenges are as follows:

Small Node Size: Reducing node size is one of the primary design objectives of sensor networks. The advent in microelectronics technology made it possible to design miniaturized devices on the order of one cubic centimeter. Limited in energy and individual resources (such as CPU and memory), these tiny devices could be deployed in hundreds or even thousands in harsh and hostile environments. Reducing node size can facilitate node deployment and also reduce the cost and power consumption of sensor nodes.

Low Node Cost: Reducing node cost is another primary design objective of sensor networks. Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, it is important to reduce the cost of sensor nodes so that the cost of the whole network is reduced.

Low Power Consumption: Reducing power consumption is the most important objective in the design of a sensor network. Sensor nodes are powered by battery and it is often very difficult or even impossible to change or recharge their batteries. This constraint presents many new challenges in the development of hardware and software, and the design of network architectures and protocols for sensor networks. To prolong the operational lifetime of a sensor network, energy efficiency should be considered in every aspect of sensor network design.

VI. RESEARCH OBJECTIVES

Sensing the environment and sending the sensed data to a remote place via sink with greater reliability is the primary objective of WSNs. In many applications like battlefield surveillance and forest fire detection, reliability is the primary concern and cannot be compromised with cost of the network. So, there is need of using redundant sensor nodes as additional sensors to replace the faulty sensor nodes of the same type and thus to Provide fault tolerance for the communication backbone.

Many applications of WSNs require immediate and guaranteed actions like medical emergency alarm and fire detection. In these situations, packets has to be transported in a reliable way and in time through the sensor network and thus data reliability becomes very relevant for the proper functioning of the network. Most of the solutions available in literature address a specific reliability and fault tolerance problem but ignore other issues like fast delivery and successful transmission of packets in presence of some missing and mistaken bits due to noise, etc. in the communication channel.

Numbers of algorithms have studied the use of encoding techniques to enhance the reliability of the communications like Reed-Solomon encoding, data encoding to combat channel fading and distributed classification fusion approach using error correcting codes. There is still scope to enhance the reliability of communications by using neural network based encoding and clustering techniques.

There is a need of some mechanism to overcome the problems coming from wireless communication medium and limited resources. In WSNs, the medium of communication is wireless which is more unreliable than wired system as wireless channel is noisier. Because of disturbances/ noise, the information of interest may not be delivered successfully at the destination.

A sensor node is battery powered, so has limited power source and also it has small computational power and memory space. Therefore we can't play complicated algorithm to achieve the reliability. We can't send many control packets to tune the network, Nor can we run sophisticated algorithm in sensor nodes.

VII. Conclusions

Various design, deployment and functional aspects of a reliable WSN are analyzed in this paper. Also the necessity and requirements of reliability in WNS applications are discussed in detail. The existing research works with the notion of improving reliability are studied elaborately, compared based on their performance and reliability measures. Many of the works are available to improve the communication reliability of WSN by modifying the existing MAC, routing and transport protocols. Many methodologies to improve the sensing and coverage reliability are developed exceptionally for WSN by improving the aggregation and deployment techniques. On analyzing the works, it is shown that the reliability can efficiently improved by adopting fault tolerance in the de- sign of various functions especially event/target detection and data aggregation/fusion techniques. WSNs hold the promise of many applications in the area of monitoring and control systems. Many properties of the environment can be observed by the monitoring system with the advent of cheap and tiny sensors. All these applications are meant for the specific purposes, and therefore maintaining data transport reliability is one of the major concern and the most important challenge. To address the reliability, we survey the various existing techniques; each of them has its own unique working to ensure the reliability. Some of the techniques use retransmission mechanism while others use redundant information for insuring the reliability. Few of the above objectives may be considered in the future by the researchers.

References

[1] Hao Wen, Chuang Lin, Fengyuan Ren, Yao Yue, Xiaomeng Huang, "Retransmission or Redundancy: Transmission Reliability in Wireless Sensor Networks", in Proceedings of the IEEE 2007.

[2] Paulo Rogério Pereira, António Grilo, Francisco Rocha, Mário Serafim Nunes, Augusto Casaca, Claude Chaudet, Peter Almström and Mikael Johansson, "End-To-End Reliability in Wireless Sensor Networks: Survey and Research Challenges", in EuroFGI Workshop on IP QoS and Traffic Control, P. Pereira (Ed.), Lisbon, Portugal, December 6-7, 2007.

[3] Faisal Karim Shaikh, Abdelmajid Khelil and Neeraj Suri, "On Modeling the Reliability of Data Transport in Wireless Sensor Networks", in IEEE international conference in parallel, distribute and network based processing, pp. 395-402, 2007.

[4] Wenyu CAI, Xinyu JIN, Yu ZHANG, Kangsheng CHEN, Jun TANG, "Research on Reliability Model of Large-Scale Wireless Sensor Networks", in Proceedings of the IEEE 2006.

[5] V. Mhatre, C. Rosenberg, D. Kofman, R. azumdar, N. Shroff, "A minimum cost heterogeneous sensor network with a lifetime constraint", IEEE Transactions on Mobile Computing, Vol. 4(1), pp. 4 -15, 2005.

[6] D. Bein, V. Jolly, B. Kumar and S. Latifi, "Reliability Modeling in Wireless Sensor Networks", International Journal of Information Technology, Vol. 11 No.2 [2005].

[7] K. K. Sharma, R. B. Patel and H. Singh, "A Reliable and Energy Efficient Transport Protocol for Wireless Sensor Networks," International Journal of Computer Networks & Communications, Vol. 2, No. 5, 2010, pp. 92-103. Do i:10.5121/ijcnc.2010.2506

[8] J. J. Winston and B. Paramasivan, "A Survey on Connectivity Maintenance and Preserving Coverage for Wireless Sensor Networks," International Journal Reviews in Wireless Sensor Networks, 2011, Vol. 1, No. 2, pp. 11-18. [16] Z. ShuKui, G. ShengRong, C. ZhiMing and F. J. Xi , "A Reliable Collaborative Detection Scheme of Event-Rgion in Wireless Sensor International Symposium on Information Processing, 2009, pp. 021-024.

[9] G. J. Fan and S. Y. Jin, "Coverage Problem in Wireless Sensor Network: A Survey," Journal of Networks, Vol. 5, No. 9, 2010

[10] G. Campobello, A. Leonardi and S. Palazzo, "Improving Energy Saving and Reliability in Wireless Sensor Net- works Using a Simple CRT-Based Packet-Forwarding Solution," EEE/ACM Transactions on Networking, Vol. 20, No. 1, 2012, pp. 191-205.
[11] E. Cañete, M. Díaz, L. Llopis and B. Rubio, "HERO: A Hierarchical, Efficient and Reliable Routing Protocol for Wireless Sensor and Actor Networks," Computer Communications Vol. 35, No. 11, 2012, pp. 1392-1409. doi:10.1016/j.comcom.2012.04.003
[12] R. V. Kshirsagar and B. Jirapure, "A Survey on Fault Detection and Fault Tolerance in Wireless Sensor Net- works," International Journal of Computer Applications, Vol. 3, No. 1, 2011, pp. 130-138.
[13] S. Mishra, L. Jena and A. Pradhan, "Fault Tolerance in Wireless Sensor Networks," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 10, 2012, pp. 1
[14] L. Paradis and Q. Han, "A Survey of Fault Management in Wireless Sensor Networks," Journal of Network and Sys- terms Management, Vol. 15, No. 2, 2007, pp. 171-190. doi:10.1007/s10922-007-9062-0
[15] F. Koushanfar, M. Potkonjak, A. Sangiovanni-Vincentelli, "Fault Tolerance Techniques for Wireless Ad Hoc Sensor Networks," Proceedings of the IEEE Conference Sensors, Vol. 2, 2002, pp. 1491-1496. Do i:10.1109/ICSENS.2002.1037343