Optimal Node Deployment for Fault Tolerant Wireless Sensor Networks: A Survey

Ms. Vishakha Dhiman, Dr. T.P. Sharma

***Abstract* – Wireless Sensor Network consists of autonomous nodes which are deployed in harsh environments to collect data. WSNs are self-organizing systems with limited resources. WSNs should be reliable enough to carry out further work with the sensed data. But often it has seen that WSNs are prone to failures which degrade the reliability of the network. Hence a fault tolerant network is needed. Different approaches to fault tolerance are addressed. This paper summarizes the techniques of optimal deployment of nodes in WSN and ways of dealing with faults developing in the network. It also discusses various reasons of faults that occur in WSNs and to some extent given strategies to deal with such issues.**

I. INTRODUCTION

Wireless Sensor Network is a network of autonomous sensor nodes which is resource-constrained and self-organizing in nature. WSNs have multi-hop communication and hence are prone to failures. Fault tolerance is relatively less studied topic in WSNs as compared to VLSI. We surveyed on the frequent faults and the techniques used to overcome those faults that occur in real world WSNs deployments. Deployment of sensor network is not easy and needs a lot of effort as nodes can lead to innumerous failures. Various schemes exist in literature [21][24][26][28][30] for installation of large-scale sensor networks for real world applications. These nodes can be deployed over a wireless sensor networks in random or deterministic fashion. Present paper focuses on schemes that maximize the coverage and use minimum resources for communication while ensuring maximum fault tolerance. Also, we studied various methods of providing fault tolerance at the time of nodes deployment and ways to detect, diagnose and recover the faults. Also approaches of fault tolerance at the time of node deployment are covered. Existing approaches of fault management in are various in forms of architectures [34-36], protocols [31, 32], detection algorithm [33, 37-39] or detection decision fusion algorithm [40-41].

Fault tolerance techniques can be mainly divided into following categories: 1) Fault prevention: to prevent or avoid faults. 2) Fault detection: to detect failures in network by using different metrics. 3) Fault isolation: to correlate different types of fault indications received from the network and propose various fault hypotheses. 4) Fault identification: to test each proposed hypotheses in order to localize and identify faults. 5) Fault recovery: to treat faults and reverse the adverse effects.

In this paper, we concentrate on service availability in WSNs through the use of fault tolerance techniques. We present a survey of approaches to fault detection and recovery techniques in WSNs. We provide taxonomy of faults and classify the investigated approaches according to their ability to detect and tolerate faults.

This paper provides an overview of the relation of fault tolerance with other areas of research, described in section I, followed by types of deployment in section 2, design challenges, sources of faults and types of Faults in section 3 and fault tolerance in section 4 followed by conclusion in section 5.

II. TYPES OF DEPLOYMENT

A Wireless Sensor Network may be composed of homogeneous and heterogeneous sensor nodes which posses different computation and communication capabilities. The sensor nodes are usually scattered in the field. Each of these scattered sensor nodes has the capabilities of collect data and route data back to the base station. Random node deployment is preferable in most of the cases as it is not possible to deterministically add sensor nodes in most of the environments.

Designing and deploying sensor network by taking care of coverage (Area being monitored under node's range) and connectivity (Ability of active nodes to stay connected) will provide fault tolerance without need of fault detection and recovery techniques. Many applications require WSNs to exchange sensitive information or contain feedback processes that have high reliability requirements and they require a high

ISSN: 2278 – 1323

level of security to succeed. Even after all this, if failure occurs then safety measures can be taken.

Wang et al. [13] shows the relationship between coverage and connectivity. In k-coverage the network is said to be connected if network remains connected even if k-1 nodes fail. Two protocols are designed for the purpose Coverage Configuration Protocol (CCP) and SPAN connectivity maintenance protocol. CCP allows dynamic configuration of network by saving energy by putting nodes in sleep state when they are not required. The worst and best coverage is evaluated in [14].

Xue et al. [15] checks for one hop neighbors per node for connectivity. It concludes that neighbors has to grow as O (log n) with the network size n (where n is the number of nodes in the network).Neighbors per node is given as C log n, Where C is close to one, Asymptotic disconnectivity result for C = 0.074 and Asymptotic connectivity for C = 5.1774. Depending upon the environment and obstacles it is not always possible to deploy network a-priori as sensor nodes are often deployed in harsh environments so [16] proposed deployment techniques. Concurrent deployment (Number of nodes and location of nodes is known) and Incremental deployment (deployment of node is done and relatively other node is placed i.e. sensor node once placed is used to decide the location of next node).

Utkarsh et al. [42] studied different types of node deployment to get the topology with maximum coverage. They compared Regular Hexagon pattern, Octagon square pattern and tri-beehive node deployment pattern. In their study they found out that tri-beehive node deployment pattern is better opinion for wireless sensor networks in sense of average coverage performance. Different topologies are shown in figures 1, 2, 3, 4 and 5.

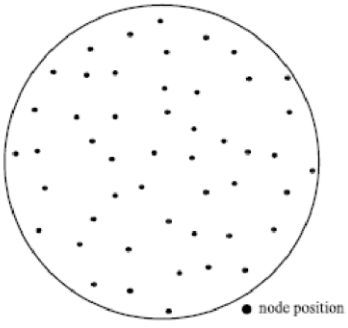

Fig. 1: Random Deployment pattern

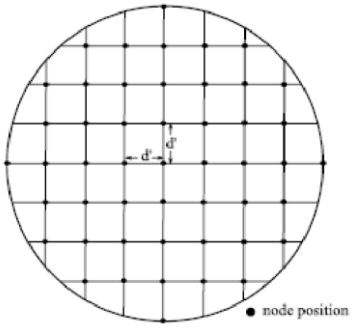

Fig. 2: Square Grid Based Deployment

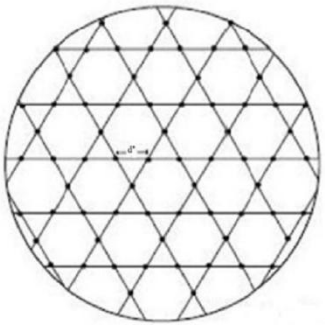

Fig. 3: Tri-beehive Based Deployment

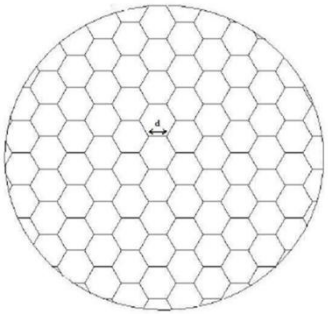

Fig. 4: Regular Hexagon Based Deployment

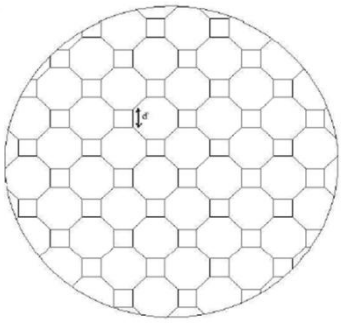

Fig. 5: Octagon Square Based Deployment

ISSN: 2278 – 1323

Fan et al. [43] proposed a deployment strategy of wireless sensor network to minimize the cost. Regular hexagon cell architecture is employed to build a network with minimum cost, coverage and connectivity. This paper formulated the energy consumption of sensor and sinks and provided an energy allocation theorem. By analyzing cost of network, an integer programming model is proposed to minimizing cost per unit area of network. A scheme of multi-sink network for large monitoring area is detailed. A uniform load routing algorithm is proposed to balance the energy consumption of sensors on the identical layer. A scheme of multi-sink network is proposed for large monitored area.

In order to avoid the uneven energy depletion and reduce the waste, many works have been reported [45]. Non-uniform node distribution strategy was proposed. In [44], some pure relay nodes were added to the network to reduce other nodes traffic burden. Y. Liu et al. [46] proposed a power-aware non-uniform node distribution scheme. They derived node distribution functions based on hop counts. Author of [47] explored the theoretical aspects of the non-uniform node distribution strategy and proposed a non-uniform node distribution strategy to achieve nearly balance energy depletion in network. Some works [48-49] focused on adjusting node different transmission range. H. Zhang et al. [50] formulates the energy consumption balancing problem as an optimal data transmission data distribution problem by combining the ideas of corona based network division and mixing routing strategy together with data aggregation and an energy balanced data gathering.

One of the ways to enhance lifetime of network is deploying sensor nodes within the network area so that energy flow remains balanced throughout the network. Hence results in reduction in energy holes.

III. DESIGN CHALLENGES, SOURCES OF FAULTS AND TYPES OF FAULTS

Fault tolerant techniques for distributed systems include tools that have become industry standard such as SNMP and TCP/IP, as well as more specialized and/or more efficient methods researched in [6-9]. Some of the challenges in designing the WSNs are mentioned in this section. First and main issue is the energy consumption. WSNs are concerned with reliable event detection unlike traditional network which is point-to-point reliable. They are concerned with services provided from one point to the other. Next main challenge faced in deployment of wireless sensor network is the monitoring of node's health i.e. is the node working correctly or has failed. If nodes are not monitored continuously then failures will occur which will add to the significant overhead and therefore will degrade the performance of the network. One other problem with WSNs is collision problem. Collisions in wireless sensor networks can only be mitigated not completely resolved as MAC layer has challenges such as coordinating a node's sleeping and active states. Network partitioning is the cause of failures as the communication links between WSNs break. With all these challenges there is one more challenge in deployment of WSNs and that is searching an optimal trade-off among coverage, lifetime, energy consumption, and connectivity

Data delivery in sensor networks is inherently faulty and unpredictable [1]. Sensor nodes are fragile, and they may fail due to depletion of batteries or destruction by an external event. Nodes may capture and communicate incorrect readings because of environmental influence on their sensing components. Links are failure-prone [2], causing network partitions and dynamic changes in network topology. Links may fail when permanently or temporarily blocked by an external object or environmental condition. Packets may be corrupted due to the erroneous nature of communication. In addition, when nodes are embedded or carried by mobile objects, nodes can be taken out of the range of communication. Congestion may lead to packet loss. Congestion may occur due to a large number of nodes' simultaneous transition from a power saving state to an active transmission state in response to an event-of-interest [5]. Fault scenarios are worsened by the multi-hop communication nature of sensor networks. It often takes several hops to deliver data from a node to the sink; therefore, failure of a single node or link may lead to missing reports from the entire region of the sensor network.

Faults associated with WSN are categorized into two major sections. They are either due to failure of individual node or due to failure in the network. Each of these two types of failures has been elaborately depicted in figure 6, figure 7 and figure 8.

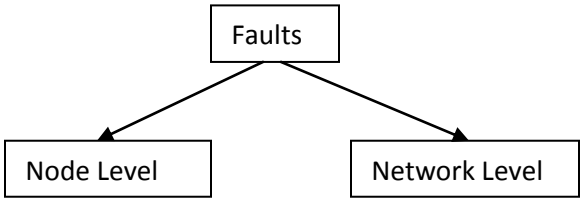

Fig. 6: Types of faults

ISSN: 2278 – 1323

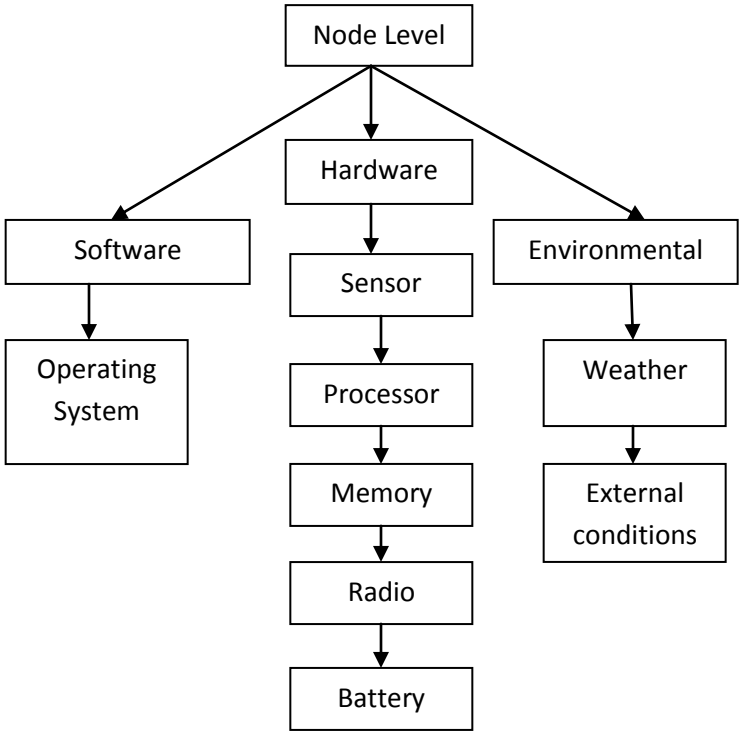

Fig. 7: Types of faults (Node level)

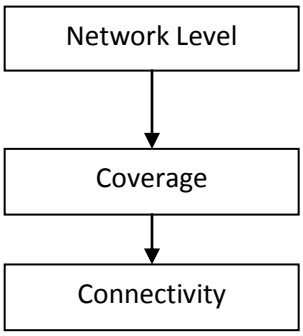

Fig. 7: Types of faults (Network level)

IV. FAULT TOLERANCE

Fault tolerance is the property that enables a system to continue operating properly in the event of failure of some of its components. Fault tolerance is the ability of a system to provide desired level of functionality in presence of faults.

A. Fault Tolerance at Different Levels

Five levels of fault tolerance were discussed by Ramakrishna et al. [59]. They are physical layer, hardware layer, system software layer, middleware layer, and application layer. On the basis of study, we classify fault tolerance in WSNs into four levels from the system point of view. More specifically, fault tolerance in a WSN system may exist at hardware layer, software layer, network communication layer, and application layer.

Hardware Layer

Faults at hardware layer can be caused by malfunction of any hardware component of a sensor node, such as memory, battery, microprocessor, sensing unit, and network interface (wireless radio).

Software Layer

Software of a sensor node consists of two components: system software, such as operating system, and middleware, such as communication, routing, and aggregation. Software bugs are a common source of errors in WSNs.

Network Communication Layer

Faults at network communication layer are the faults on wireless communication links. Link faults can be caused by surrounding environments or by radio interference of sensor nodes.

Application Layer

Fault tolerance can be addressed also at the application layer. For example, finding multiple node-disjoint paths provides fault tolerance in routing. The system can switch from an unavailable path with broken links to an available candidate path.

B. Fault prevention

Fault prevention is used to prevent fault occurring in WSN by following mentioned ways: By providing full coverage and connectivity between nodes in a WSN. By constantly monitoring network and reacting to some events which may cause faults in network such as changing the mode

ISSN: 2278 – 1323

of active node to sleep after its threshold energy level is crossed. Hence reducing the chances of information loss by depletion of energy of the node. Adding redundancy for delivery path so that the data is delivered even if some of the path failure occurs and hence makes network to be less prone to partitioning. Prevention role can be incorporated along with main concerned phases of WSN application design; they are i) Specification phase ii) design and development phase and iii) monitoring phase. Above mentioned are some of the things which should be taken care of while designing our network.

Sensor Network Monitoring

For quantitative understanding of communication patterns researchers did some experiments [1]. Performance of packet delivery at physical and MAC layers was measured. At physical layer the transmission with respect to distance is done. After certain distance the packet reception rate is highly unpredictable. At MAC layer two metric packet loss rate and packet delivery efficiency were used to see the density of deployment and work load. The results were 30% links were at low traffic load. 50% high traffic load, 50% or more had packet loss rate. Efficiency was 50% and 20% for low traffic load.

G. Zhaou et al. [4] found that links with very high and low reception are symmetrical while links with intermediate reception are asymmetrical. Efficient network management is provided by monitoring network health. Abnormal behavior can be predicted by administrators so that remedial actions can be taken. Monitoring techniques can be classified into two. Active monitoring (Performance measured is based on probing) and passive monitoring. Next the monitoring is discussed so as to get minimum overhead.

Monitoring Node Status

Energy is the scarcest resource for sensor nodes; residual energy level provides a good indication of possible node failures. eScan [17] is an active monitoring technique that monitors remaining energy levels using localized algorithms for in-network aggregation of local representations of energy levels. A prediction based approach has been proposed for generating an energy map [18]. Each node sends the parameters of the dissipation model to the sink.

Monitoring Link Quality

Tracking the quality of channels at the link layer may enable higher level protocols to adapt to changes in link quality by changing routing structures. One technique designed for link quality monitoring is based on snooping [2], by passively listening to the channel and inferring the loss and success rates via tracking of link sequence numbers.

Monitoring Congestion Level

Congestion can be one of the causes for packet loss. A straightforward policy is to evaluate the growth rate of the buffer length [19]. Alternatively, CODA [20] uses a combination of the present and past channel loading conditions, and the current buffer occupancy to infer accurate detection of congestion at each receiver with low cost.

Sensor network monitoring should not be limited to just one metric such as residual energy level, link quality, or congestion level. Other metrics such as buffer occupancy level, topology changes, etc., are equally important and should also be tracked.

Thomas et al. [51] proposed an integrated prototype of measurement setups which was built on Mica2 platform which could be directly plugged on Mica2 mote and allows the mote to monitor energy of the mote during runtime. Energy used can be determined by

$$E = \int_{t=0}^{T} u(t).i(t).dt$$

For discrete values:

$$E = \sum_{n=0}^{N} u[n].i[n].t[n]$$

$$E = K.\sum_{n=0}^{N} u[n]$$

Because i[n].t[n] has same size.

OK et al. [52] proposed an algorithm for distributed energy balanced routing(DEBR).It balances energy but can unnecessarily increase the delay in transmitting the data to the base station. In minimum hop routing model (MHRM) [53] every node finds a path to the base station such that hop count is minimized. Solutions to avoid hole [54-55] created due to failure of some Cluster Head Selection are presented in mentioned references. In [55] HAIR is proposed which is a routing protocol to avoid hole in advance by selecting next hop node from its neighbors based on smallest distance to base station without taking residual energy of the nodes into consideration as a result it may end up choosing node which has sufficient residual energy and hence may lead to increase in hole size.

In [56] Greedy approach is proposed to route data to base station based on maximum residual energy. But none of

ISSN: 2278 – 1323

the algorithm addresses energy efficient and fault tolerant routing issues together.

C. Multipath Routing

Multipath routing has been used in traditional wired networks to provide load balancing and route redundancy. Both of these notions are applicable to sensor networks: load balancing leads to a balance in energy consumption among sensor nodes, hence avoiding power depletion of a particular set of nodes; route redundancy increases the chances of messages to reach the destination, thus improving reliability of data delivery.

Meshed Multipath Routing such as Gradient Broadcast (GRAB) technique [22] creates a forwarding mesh from the source to the sink based on the "cost" of delivering the packet at each node. *Node-Disjoint Multipath* [23] relies on a number of alternate paths that do not share any nodes (other than the source and the destination nodes) with the primary path or other alternate paths. *Braided Multipath* [23] is a relaxation of node-disjointedness. It uses braided (or partially disjoint) paths. For each node on the primary path, an alternate path not including that node is found.

Multipath routing techniques discussed above utilize density of node deployment for reliable data delivery in different ways. GRAB provided higher reliability than disjoint paths because they use multiple interleaving alternate paths. Consider a scenario where two disjoint paths have failures at different hops. Disjoint multipath would not be able to recover from this fault without constructing a brand new path. Forwarding mesh would reliably deliver data if there was at least one complete forwarding path between source and destination. Forwarding mesh imposes higher overhead because the message is broadcast by more nodes irrespective of whether there are failures or not. On the other hand, under that scheme only one node generates a report about the event so fewer redundant packets are generated.

D. Fault Detection

Even with fault prevention mechanisms, failures will still occur, so fault detection techniques need to be in place to detect potential faults. Fault detection in sensor networks largely depends on the type of applications and the type of failures. Sensor nodes may also permanently fail. Tools such as "ping" or "traceroute" use ICMP messages to check whether a node is alive or not in wired networks. This approach can also be applied to evaluate the health of sensor nodes. In addition, since sensor nodes are energy-constrained and energy depletion often causes node death, remaining energy level can also be used as a warning of node failure [17, 18]. Other metrics such as interruption, delay or lack of regular network traffic are also considered as symptoms of faults [27, 28]. Alternatively, buffer occupancy level and channel loading conditions [19, 20] are used for fault detection (specifically, congestion).

Type of applications and the type of failures will be detected in wireless sensor networks. Packet loss can be an indication of faults. Geeta et al. [56] proposed a novel idea of an active node based fault tolerance using battery power and interference model(AFTBI) in WSN to identify faulty nodes using battery power of a node is low fault tolerance is designed through hand-off mechanism where faulty node selects the neighboring node with the highest power to transfer its services.

Laukik et al. [57] proposed a model that captures the essence of tree aggregation in heterogeneous networks and analyzed impact of using more reliable nodes such as Intel XScale – called Micro servers. Gaurav et al.[58] proposed the use of highly reliable long range black-haul-links in the form of wires between regions of the sensor network has been integrated and there was reduction in average energy expenditure per sensor node and also in non-uniformity in the energy expenditure of a node.

The existing failure detection approaches in WSNs can be classified into two types: centralized and distributed approach.

5. Conclusion

This paper reviewed different techniques for fault tolerance. Here first we discussed different reasons for failures in wireless sensor networks and then we mentioned different deployment techniques proposed for fault tolerant topology to prevent faults in network. We then discussed the algorithms that prevent, detect, and identify faults. The resource limitation and unattended feature of sensor networks renders the network very faulty, and this survey aims to help us further understand the challenges in designing fault tolerant protocols for distributed sensor applications.

REFERENCES

[1] J. Zhao and R. Govindan, Understanding packet delivery performance in dense wireless sensor networks. *Proceedings of ACM SenSys*, 2003.
[2] A. Woo, T. Tong, and D. Culler, Taming the underlying challenges of reliable multihop routing in sensor networks. In *Proceedings of ACM SenSys*, 2003.
[3] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, Impact of radio irregularity on wireless sensor networks. In *Proceedings of ACM MobiSys*, pp. 125–138, 2004.
[4] A. Cerpa, J. Wong, L. Kuang, M. Potkonjak, and D. Estrin, Statistical model of lossy links in wireless sensor networks. In *Proceedings of IEEE IPSN*, April 2005.

ISSN: 2278 – 1323

[5] S. Tilak, N. B. Abu-Ghazaleh, andW. Heinzelman, A taxonomy of wireless micro-sensor network models. *Mobile Computing and Communications Review*, Vol. 6, No. 2, pp. 28–36, 2002.

[6] A. L. Dos Santos, Jr., E. P. Duarte, and G. M. Keeni, Reliable distributed network management by replication. *Journal of Network System Management*, Vol. 12, No. 2, pp. 191–213, June 2004.

[7] X. Du, Identifying control and management plane poison message failure by *k*-nearest neighbor method. *Journal of Network System Management*, Vol. 14, No. 2, pp. 243–259, June 2006.

[8] J. W. Hong, S. Park, Y. Kang, and J. Park, Enterprise network traffic monitoring, analysis, and reporting using web technology. *Journal of Network System Management*, Vol. 9, No. 1, pp. 89–111, March 2001.

[9] H. L. Lutfiyya, M. A. Bauer, A. D. Marshall, and D. K. Stokes, Fault management in distributed systems: A policy-driven pproach. *Journal of Network System Management*, Vol. 8, No. 4,pp. 499–525, December 2000.

[10] C. Ensel and A. Keller, An approach formanaging service dependencies with xml and the resource description framework. *Journal of Network System Management*, Vol. 10, No. 2, pp. 147–170, 2002.

[11] W.Ye, J.Heidemann, andD. Estrin, An energy-efficientmac protocol forwireless sensor networks. In *Proceedings of InfoCom*, 2002.

[12] A. S. Tanenbaum and M. V. Steen, *Distributed Systems: Principles and Paradigms*. Prentice Hall, 2002.

[13] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, Integrated coverage and connectivity configuration in wireless sensor networks. *In Proceeding of the ACM Sensys*, 2003.

[14] S. Meguerdichian, F. Koushanfar,M. Potkonjak, and M. Srivastava, Coverage problems in wireless ad-hoc sensor networks. In *Proceedings of IEEE Infocom*, 2001.

[15] F. Xue and P. Kumar, The number of neighbors needed for connectivity of wireless networks. *Wireless Networks*, Vol. 10, No. 10, pp. 169–181, 2004.

[16] V. Isler, K. Daniilidis, and S. Kannan, Sampling based sensor-network deployment. In *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2004.

[17] Y. Zhao, R. Govindan, and D. Estrin, Residual energy scan for monitoring sensor networks. In *Proceedings of IEEE WCNC*, 2002.

[18] R. Mini, A. Loureiro, and B. Nath, The distinctive design characteristic of a wireless sensor network: the energy map. *Elsevier Computer Communications*, Vol. 27, No. 10, pp. 935–945, 2004.

[19] Y. Sankarasubramaniam, O. B. Akan, and I. F. Akyildiz, Esrt: Event-to-sink reliable transport in wireless sensor networks. In *Proceedings of ACM MobiHoc*, 2003.

[20] C. Y. Wan, S. B. Eisenman, and A. T. Campbell, Coda: Congestion detection and avoidance in sensor networks. In *Proceedings of SenSys*, 2003.

[21] K. Martinez, P. Padhy, A. Riddoch, H. Ong, and J. Hart. Glacial environment monitoring using sensor networks. In REALWSN' 05, 2005..

[22] F. Ye, G. Zhong, S. Lu, and L. Zhang, Gradient broadcast: A robust data delivery protocol for large scale sensor networks. *ACM WINET*, Vol. 11, No. 3, pp. 285–298, 2005.

[23] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *ACM Mobile Computing and Communications Review*, Vol. 1, No. 2, pp. 10–24, October 2002.

[24] J. Tateson, C. Roadknight, A. Gonzalez, T. Khan, S. Fitz, I. Henning,N. Boyd, and C. Vincent. Real world issues in deploying a wireless sensor network for oceanography. In RealWSN' 05, 2005.

[25] S. J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, A scalable approach for reliable downstream data delivery in wireless sensor networks. In *ACM MobiHoc Conference*, 2004.

[26] 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.

[27] J. Staddon, D. Balfanz, and G. Durfee, Efficient tracing of failed nodes in sensor networks. In *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, pp. 122–130, 2002.

[28] G. Tolle, J. Polastre, R. Szewczyk, D. Culler, N. Turner, K. Tu, S. Burgess, T. Dawson, P. Buonadonna, D. Gay, and W. Hong. A macroscope in the redwoods. In SenSys '05: Proceedings of the 3rd international conference on Embedded networked sensor systems, pages 51–63, New York, NY, USA, 2005. ACM Press..

[29] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, Tag: a tiny aggregation service for ad-hoc sensor networks. In *USENIX OSDI*, 2002.

[30] R. Szewczyk, J. Polastre, A. M. Mainwaring, and D. E. Culler. Lessons from a sensor network expedition. In EWSN, pages 307–322, 2004.

[31] Sergio Marti, T.J.Giuli, Kevin Lai, Mary Baker. itigating Routing Misbehavior in Mobile Ad Hoc Networks. in 6th International. Conference on Mobile Computing and Networking. 2000. Boston,Massachusetts.

[32] A.Perrig, R.Szewczyk, V.Wen, D.Culler, J.D.Tygar. SPINS: Security protocols for sensor networks. in ACM MobiCom'01. 2001. Rome, Italy: ACM Press.

[33] Chihfan Hsin, Mingyan Liu. A Distributed Monitoring Mechanism for Wireless Sensor Networks. in 3rd workshopo on Wireless Security. 2002: ACM Press.

[34] Linnyer Beatrys Ruiz, Jose Marcos S. Nogueira, Antonio A.F. Loureiro, MANNA: A Management Architecture for Wireless Sensor Networks. IEEE Communications Magazine, 2003. 41(2): p. 116-125.

[35] Ann T. Tai, Kam S. Tso, William H. Sanders. Cluster-Based Failure Detection Service for Large-Scale Ad Hoc Wireless Network Applications in Dependable Systems and Networks DSN ' 04. 2004.

[36] Winnie Louis Lee, Amitava Datta, Rachel Cardell-Oliver, WinMS: WSN-Management System, An Adaptive Policy- Based Management for WSN. 2006, UWA, aUSTRALIA.

[37] C. Hsin, Mingyan Liu, Self-monitoring of WSN. Computer Communications, 2005. 29: p. 462-478.

[38] Min Ding, Dechang Chen, Kai Xing, Xiuzhen Cheng. Localized Fault- Tolerant Event Boundary Detection in Sensor Networks. in INFOCOM 2005.

[39] Jinran Chen, Shubha Kher, Arun Somani. Distributed Fault Detection of Wireless Sensor Networks. in DIWANS'06. 2006. Los Angeles, USA: ACM Press.

[40] XuanwenLuo, Ming Dong, Yinlun Huang, Optimal Fault-Tolerance Event Detection in WSN.

[41] Thomas Clouqueur, Kewalk, Saluja, Parameswaran Ramanathan, Fault Tolerance in Collaborative Sensor Networks for Target Detection. IEEE Transactions on Computers, 2004. 53(3): p. 320-333.

[42] Utkarsh Aeron, Hemant Kumar, Coverage Analysis of Various Wireless Sensor Network Deployment Stratergies. IJMER, Vol.3, Issue2, 2013 :pp-955-961.

[43] Fan Tiegang, Teng Guifa and Huo Limin, Deployment strategy of WSN based on minimizing cost per unit area, Elsevier Computer Communications 38 (2014) 26–35.

[44] J. Lian, K. Naik, G. Agnew, Data capacity improvement of wireless sensor networks using non-uniform sensor distribution, Int. J. Distrib. Sensor Netw. 2 (2) (2006) 121–145.

[45] M. Younis, K. Akkaya, Strategies and techniques for node placement in wireless sensor networks: a survey, Ad Hoc Netw. 6 (4) (2008) 621–655.

[46] Y. Liu, H. Ngan, L.M. Ni, Power-aware node deployment in wireless sensor networks, in: Proceedings of International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 06), 2006, pp. 128–135.

[47] X. Wu, G. Chen, Avoiding energy holes in wireless sensor networks with nonuniform node distirbution, IEEE Trans. Parallel Distrib. Syst. 19 (5) (2008) 710–720.

ISSN: 2278 – 1323

[48] C. Song, J.N. Cao, M. Liu, Y. Zheng, H.G. Gong, G.H. Chen, Maximizing network lifetime based on transmission range adjustment in wireless sensor networks, Comput. Commun. 32 (11) (2009) 1316–1325.
[49] V. Mhatre, C. Rosenberg, Design guidelines for wireless sensor networks: communication, clustering and aggregation, Ad Hoc Netw. 2 (1) (2004) 45–63.
[50] H. Zhang, H. Shen, Balancing energy consumption to maximize network lifetime in data-gathering sensor networks, IEEE Trans. Parallel Distrib. Syst. 20 (10) (2009) 1526–1539.
[51] Thomas Trathning and Reinhold Weiss, A Runtime Energy Monitoring System for Wireless Sensor Networks,IEEE, 2008.
[52] Ok, C.-S., et al.(2009). Distributed energy balanced routing for wireless sensor networks. Compter and indusrial Engineering, 57, 125-135.
[53] Chiang, S.-S., Huang, C-H., &Chang, K-C.(2007). A minimum hop routing protocol for home security systems using wireless sensor networks. IEEE Transactions on Consumer Electronics, 53(4), 1483-1489.
[54] Jia, W.,Wang, T.,Wang, G., & Guo, M.(2007). Hole avoiding in advance routing in wireless sensor networks. In wireless communications and networking conference (pp.3519-3523).
[55] Hwang, S.-F., Lin, H.-H., & Dow, C.-R. (2012). An energy efficient routing protocol in wireless sensor networks with holes. IEEE Ubiquitous and future Network, 15(2), 551-591.
[56] D.D.Geeta, N.Nalini, Rajashekhar C. Biradar. Fault tolerance in wireless sensor network using hand-off and dynamic power adjustment approach. Elsevier, Journal of Network and computer applications 36, 2013.
[57] Laukik Chitnis, Alin Dobra, Sanjay Ranka. Fault tolerant aggregation in heterogeneous sensor networks. J. Parallel Distrib. Comput. 69(2009).
[58] Gaurav Sharma, Ravi Mazumdar, Hybrid sensor networks: A small world in: Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and computing Mobihoc05, ACM Press, New York, NY, USA, 2005, pp 366-377.
[59] Ramakrishna Gummadi, Todd Millstein, and Ramesh Govindan, "Declarative Failure recovery for Sensor Networks," AOSD '07, March 12-16 2007.

AUTHOR'S BIOGRAPHY

Vishakha Dhiman obtained her B.Tech degree in Information Technology from Institute of Engineering and Emerging Technology, Baddi, India in 2012 and pursuing her M.Tech degree in Computer Science and Engineering Department of National Institute of Technology, Hamirpur, India in 2015. Her research interest includes wireless sensor networks.

T. P. Sharma is an Associate Professor and Head in Computer Science and Engineering Department of National Institute of Technology, Hamirpur, India. He has done his Ph.D from Indian Institute of Technology, Roorkee (Electronics and Computer Engineering Department), India in the area of Wireless Sensor Networks. He has published numerous high quality research papers in International/ National journals and conferences, and has also contributed in various books of standard international publishers. His research interest includes distributed systems, wireless sensor networks, mobile ad hoc networks and wireless networks.

ISSN: 2278 – 1323