Issues and Challenges in Wireless Sensor Networks

Conference Paper · December 2013

DOI: 10.1109/ICMIRA.2013.18

1 author:

Sukhwinder Sharma
Baba Banda Singh Bahadur Engineering College

Issues and Challenges in Wireless Sensor Networks

Sukhwinder Sharma
CSE & IT Department
BBSB Engineering College
Fatehgarh Sahib, India
sukhwinder.sharma@bbsbec.ac.in

Rakesh Kumar Bansal
Department of ECE
GZSPTU Campus
Bathinda, India
drrakeshkbansal@gmail.com

Savina Bansal
ECE Department
GZSPTU Campus
Bathinda, India
savina.bansal@gmail.com

Abstract— **Recent advances in technology has made researchers quite optimistic towards the feasibility of Wireless sensor networks (WSNs). These are being deployed for various applications and have huge potential for research. However, owing to the multidisciplinary nature of this field, researchers have to face many a technical hitches. In this paper, an overview of the broad research issues and challenges involved in the design of WSNs are presented. Energy conservation emerges as one the most critical aspect in hardware and software related design issues, and puts a question mark on the overall practicability of WSNs. Besides, other related main issues include specialized hardware, software and operating system, synchronization, QoS, security, architecture and data collection related aspects with minimum communication and computation costs. This paper provides an insight into various such design issues for the better understanding of this field for the overall benefit of the research community working in this area.**

Keywords- WSN, issues, challenges, security, QoS, management

I. INTRODUCTION

In recent years, development and deployment of wireless sensor networks (WSNs) is growing on rapid pace. Wireless Sensor Network [1,2] consists of large number of sensor nodes (small and cost effective sensing devices with wireless radio transceiver) over a wide area mainly to monitor the environment that does not have infrastructure like power supply, wired internet connection and without human interaction. Each sensor node, having one or more sensors, is capable to collect, compute and communicate to other nodes. Sensor nodes are capable of sensing physical parameters like temperature, humidity, chemical composition etc. from the sensing field. The sensed data is then processed at node level or cluster level and communicated to sink or base station generally referred as collection points. Rapid deployment, self organization, high sensing fidelity, flexibility, low cost and fault tolerance characteristics of WSNs make them a very promising sensing technique for various applications. WSNs are very useful to collect information from those areas where it is difficult to reach and are seldom accessible. Promising applications of WSN include wide area monitoring for personnel/ vehicles, secure area intrusion monitoring and denial, environmental monitoring, animal habitats, migration, forest fires, natural disasters, subsea monitoring, building monitoring, vehicle traffic monitoring and control, remote site power substation monitoring, patient monitoring, smart home and inventory management and many other real life applications [3,4] for sensor deployments.

Wireless sense and control technology is being utilized to bridge the gap between the physical world of humans and the virtual world of electronics. WSNs hold the potential to provide low cost solution for the problems in military, medical and climatic conditions. The dream is to automatically monitor and respond to forest fires, avalanches, hurricanes, faults in countrywide utility equipments, traffic, hospitals and much more wide areas and with billions of sensors. However, owing to limited storage capacity and power of sensor nodes, numerous research issues and challenges are being faced by researchers while setting up a workable sensor network. This research paper presents an exploratory summary of these challenges and constraints for the overall benefit of researchers working in this challenging area in the following section.

II. RESEARCH ISSUES AND CHALLENGES IN WSNS

Major issues that affect the design and performance of a wireless sensor network are as follows:

- **Energy:** Sensors require power for various operations. Energy [5,6] is consumed in data collection, data processing, and data communication; also, continuous listening to the medium for faithful operation demands a large amount of energy by node components (CPU, radio, etc.) even if they are idle. Batteries providing power need to be changed or recharged after they have been consumed. Sometimes it becomes difficult to recharge or change the batteries because of demographic conditions. The most crucial research challenge for the WSN researchers is to design, develop and implement energy efficient hardware and software protocols for WSNs.

- **Self Management:** Wireless sensor networks once deployed should be able to work without any human intervention. It should be able to manage the network configuration, adaptation, maintenance, and repair by itself [7,8].

- **Hardware and Software Issues:** Sensor Networks consists of hundreds of thousands of nodes. It is preferred only if the node is cheap. Flash memory is advised to be used in sensor networks as it is

978-0-7695-5013-8/13 $31.00 © 2013 IEEE
DOI 10.1109/ICMIRA.2013.18

inexpensive. The central processing unit of sensor node determines energy consumption and computational capabilities of a node. In order to provide the flexibility for CPU implementation, large number of micro-controller, microprocessor and FPGAs (field programmable gate arrays) are available. For saving of power, microcontroller should have three states-active, sleep, idle. Further energy consumption for FPGA cannot be reduced; moreover separate block cannot be made for it. Deployment of FPGA to reduce power consumption is a great challenge. So, besides being cost effective, other issues are like the radio range of one sensor node has to be high ranging from 1 to 5 km. Radio range is critical for ensuring network connectivity and data collection in a network as the environment being monitored may not have an installed infrastructure for communication. Software in WSN should be hardware independent besides being light and less energy consuming. Algorithms and protocols should be designed in such a way that they should be less complex and be helpful in reducing energy consumption [9,10,11].

- **Operating System:** Operating System for WSNs should be less complex than the general operating systems. It should have an easy programming paradigm. Application developers should be able to concentrate on their application logic instead of being concerned with the low level hardware issues like scheduling, preempting and networking. Various Operating Systems developed for Sensor nodes include TinyOS [12], Mantis Operating System [13] and Nano-Qplus [13].

- **MAC Layer Issues:** Medium Access Control (MAC) solutions have a direct impact on energy consumption, as some of the primary causes of energy waste are found at the MAC layer: collisions, control packet overhead and idle listening [14]. Power saving forward error control technique is not easy to implement due to its high computing power requirements and the fact that long packets are normally not practical.

- **Quality of Service (QoS):** Quality of service [15,16] is the level of service provided by the sensor networks to its users. WSN are being used in various real time and critical applications, so it is mandatory for the network to provide good QoS. Though, it is difficult because the network topology may change constantly and the available state information for routing is inherently imprecise. Sensor networks need to be supplied with the required amount of bandwidth so that it is able to achieve a minimal required QoS. Traffic is unbalanced in sensor network since the data is aggregated from many nodes to a sink node. QoS mechanisms should be designed for an unbalanced QoS constrained traffic. Many a time routing in sensor networks need to sacrifice energy efficiency to meet delivery requirements. Even though multi-hops reduce the amount of energy consumed for data collection the overhead associated with it may slow down the packet delivery. QoS designed for WSN should be able to support scalability. Adding or removing of the nodes should not affect the QoS of the WSN.

- **Security:** Security is quite challenging issue as WSN is not only being deployed in battlefield applications but also for surveillance, building monitoring, burglar alarms and in critical systems such as airports and hospitals. Confidentiality is required in sensor networks to protect information traveling between the sensor nodes of the network or between the sensors and the base station; otherwise it may result in eavesdropping on the communication. In sensor networks, it is essential for each sensor node and the base station to have the ability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. A false data can change the way a network could be predicted. Integrity of data should be maintained. Data should not change and accurate data must reach at user end. Different types of threats in sensor networks are spoofing and altering the routing information, passive information gathering, node subversio, sinkhole attacks, sybil attacks, Denial of service attack and jamming [17,18,19].

- **Architecture:** Architecture [20,21] can be considered as a set of rules and regulation for implementing some functionality along with a set of interfaces, functional components, protocols and physical hardware. Lack of Sensor Network architecture is limiting feature and hampers the progress in this field. Sensor network architecture should be durable and scalable. As if number of nodes are increased QoS is not decreased, it must be flexible to meet the wide range of target application scenarios since the wireless sensor networks do not have a fixed set of communication protocols that they must adhere to. The architecture must decouple the data path speed and the radio transmission rate because direct coupling between processing speed and communication bit rates can lead to sub-optimal energy performance.

- **Data Collection and Transmission:** Data gathering is the main objective of sensor nodes. The sensors periodically sense the data from the surrounding environment, process it and transmit it to the base station or sink. Data gathering involves data collection and transmitting data to the sink node. Sometimes the sample of data collected is redundant and there is no need of transmitting such samples to the sink node as it will only consume energy. So care must be taken during data collection and transmission [22,23,24,25].

- **Calibration:** Calibration is the process of adjusting the raw sensor readings obtained from the sensors into corrected values by comparing it with some standard values. Manual calibration of sensors in a sensor network is a time consuming and difficult task due to failure of sensor nodes and random noise which makes manual calibration of sensors too expensive [26,22].

- **Deployment:** Deployment [27,28] means implementing the wireless sensor network in real world location. It is very laborious and cumbersome activity and depends on the demographic location of the application that how network will be deployed. At locations which are hard to reach, sensors are dropped from helicopter or may be in some locations sensors are placed according to some topology. Energy management issues like battery recharge and changing are challenges in real world scenarios. Deployment of sensor networks results in network congestion due to many concurrent transmission attempts made by several sensor nodes. Low data yield is a problem in real world scenario as network delivers insufficient amount of information.

- **Limited Memory and Storage Space**: A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type [29] has an 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. With such a limitation, the software built for the sensor must also be quite small.

- **Physical Attacks and Security:** The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network. Physical securities of the sensor nodes cannot be assured. Attackers may modify node hardware; replace it with malicious sensor or a dummy sensor [19,30].

- **In-network Processing:** To reduce communication costs some algorithms remove or reduce nodes redundant sensor information and avoid forwarding data that is of no use. As nodes can inspect the data they forward they can measure averages or directionality for example of readings from other nodes. For example, in sensing and monitoring applications, it is generally the case that neighboring sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires the techniques for in-network data aggregation and mining [31].

- **Decentralized Management:** The large scale and energy constraints of many WSNs make it infeasible to rely on centralized algorithms (e.g. executed at base stations) to implement network management solutions such as topology management or routing. Instead, sensor nodes must collaborate with their neighbors to make localized decisions, that is, without global knowledge. As a consequence, the results of these decentralized (or distributed) algorithms will not be optimal, but they may be more energy-efficient than centralized solutions. While the decentralization may lead to non-optimal routes, the management overheads can be reduced significantly.

- **Fault Tolerance:** Sensor network should remain functional even if any node fails while the network is operational. Network should be able to adapt by changing its connectivity in case of any fault. In that case, well- efficient routing algorithm is applied to change the overall configuration of network [18].

- **Robustness:** In order to support the lifetime requirements demanded, each node must be constructed to be as robust as possible. In a typical deployment, hundreds of nodes will have to work in harmony for years. To achieve this, the system must be constructed so that it can tolerate and adapt to individual node failure. Additionally, each node must be designed to be as robust as possible. System modularity is a powerful tool that can be used to develop a robust system. By dividing system functionality into isolated sub-pieces, each function can be fully tested in isolation prior to combining them into a complete application. To facilitate this, system components should be as independent as possible and have interfaces that are narrow, in order to prevent unexpected interactions. In addition to increasing the system's robustness to node failure, a wireless sensor network must also be robust to external interference. As these networks will often coexist with other wireless systems, they need the ability to adapt their behavior accordingly. The robustness of wireless links to external interference can be greatly increased through the use of multi-channel and spread spectrum radios [3]. It is common for facilities to have existing wireless devices that operate on one or more frequencies. The ability to avoid congested frequencies is essential in order to guarantee a successful deployment.

- **Interpreting Data and Formation of Knowledge:** Main challenges for data interpretation and the formation of knowledge include addressing noisy, physical world data, and developing new inference techniques**.** Uncertainty in interpreted data can easily cause users not to trust the system. It is necessary to develop techniques that convert this raw data into usable knowledge in an energy efficient manner [3].

- **Heterogeneity:** It is a group in which all the nodes are not identical and do not have same capability i.e. some node are more powerful than others. Example of heterogeneous group is cluster architecture in which node form a cluster head and gather data from less powerful node. Heterogeneity [32] arises when two completely different WSNs need to communicate with each other. Unified communication interfaces will be required to enable efficient information exchange across diverse systems and nodes.

- **Multimedia Communication:** Multimedia information is collected and communicated by the sensor network. In addition to data delivery modes typical of scalar sensor networks, multimedia data include snapshot and streaming multimedia content [33]. Processing and delivery of multimedia content are not independent and their interaction has a major impact on the achievable QoS. They demand high bandwidth for transmission.

- **Real Time Operation:** Many real-time wireless sensor networks must achieve real-time performance over extremely long lifetimes [3]. While energy harvesting has shown promise as an enabling technology for long-running wireless sensor networks, it also introduces new challenges to real-time processor scheduling due to fluctuating energy sources and limited capacity of energy storage.

- **Synchronization:** Time Synchronization in a sensor network aims to provide a common timescale for local clocks of nodes in the network. A global clock in a sensor system will help process and analyze the data correctly and predict future system behavior. Some applications that require global clock synchronization are environment monitoring, navigation guidance, vehicle tracking etc. Energy utilization in some synchronization schemes is more due to energy hungry equipments like GPS (Global Positioning System) receivers or NTP (Network Time Protocol). Sensors need to be synchronized with each other, as it may lead to inaccurate data estimation. Some synchronization protocols have high accuracy so they need more resources which results in energy loss. So, synchronization needs to be implemented correctly based on the application [34,35,36].

- **Secure Localization:** Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault [18]. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc.

III. CONCLUSIONS

Various research issues and challenges pertaining to WSNs that have been experienced by the researchers are presented in this work. Sensor networks have many challenges, but its vast number of applications lures researchers to investigate more into it. A thorough investigation reveals that WSN is a multidisciplinary field. On one side it demands scalable architecture from the hardware engineers to ensure good Quality of service; on the other end, it demands energy efficient algorithms and protocols from software engineers to make them practical and feasible. Energy saving is one of the main concern and various research issues ultimately boils down to minimize it by all means. Overall, a holistic approach and coordinated effort is desired from the research fraternity to make WSNs a reality. These efforts are worth as WSNs hold a vast potential for the overall benefit of mankind and to make pervasive computing a possibility in the coming times.

.

REFERENCES

[1] G. Anastasi, M. Conti, M.D. Francesco, and A. Passarella, "Energy Conservation in Wireless Sensor Networks: A Survey", Ad Hoc Networks, vol. 7, no. 3, 2009, pp. 537-568.

[2] G. Anastasi, M. Conti, M.D. Francesco and A. Passarella, "How to Prolong the Lifetime of Wireless Sensor Networks", Chapter 6 in Mobile Ad Hoc and Pervasive Communications, 2013, American Scientific Publishers, in CRC Press, to appear (January 2013), ISBN:1439846162 available at http://info.iet.unipi.it/~anastasi/papers/Yang.pdf

[3] J.A. Stankovic, A.D. Wood, and T. He, "Realistic Applications for Wireless Sensor Networks", Theoretical Aspects of Distributed Computing in Sensor Networks, Monographs in Theoretical Computer Science, An EATCS Series, Chapter 25, Springer-Verlag Berlin Heidelberg, 2011, pp. 835-863.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", Computer Networks, vol. 38, no. 4, 2002, pp. 393-422.

[5] M.H. Anisi, A.H. Abdullah, and S.A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", Wireless Sensor Networks, vol. 3, 2011, pp. 329-333.

[6] W. Dargie, and C. Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice. WileyBlackwell, 2010.

[7] K. Sohrabi, J. Gao, V. Ailawadhi and G.J. Pottie, "Protocols for self organization of a wireless sensor networks", IEEE Personal Communications, vol. 7, no. 5, 2000, pp. 16-27.

[8] S. Vaidyanathan and M. Vaidyanathan, "Wireless Sensor Networks- Issues & Challenges", Information Systems: Behavioral & Social Methods eJournal, 2011, pp. 7.

[9] P. Zhang, M. Sadler, A. Lyon and M. Martonosi, "Hardware Design Experiences in ZebraNet", Proc. 2nd International Conf. Embedded Networked Sensor Systems (SenSys), Nov. 2004, pp. 227-238.

[10] A. Crnjin, "Software Issues in Wireless Sensor Networks", Wireless sensor networks: concepts, multidisciplinary issues, and case studies, Belgrade, 2009, pp. 1-9.

[11] R. Sugihara and R.K.Gupta, "Programming Models for Sensor Networks: A Survey", ACM Transactions on Sensor Networks, vol. 4, no. 2, 2008, pp. 8:1-8:29.

[12] TinyOS, http://www.tinyos.net

[13] H. Abrach, S. Bhatti et.al., "MANTIS: System support for multimodal networks of in-situ sensors", Proc. 2nd ACM International Workshop Wireless sensor networks and Applications (WSNA), 2003, pp. 50-59.

[14] D. Puccinelli and M. Haenggi, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing", IEEE Circuits and Systems Magazine, vol. 5, no. 3, 2005, pp. 19-31.

[15] E. Troubleyn, I. Moerman and P. Demeester, "QoS Challenges in Wireless Sensor Networked Robotics", Springer Wireless Personal Communications, vol. 70, no. 3, June 2013, pp. 1059-1075.

[16] D. Chen and P.K. Varshney, "QoS Support in Wireless Sensor Networks: A Survey", Proc. 2004 International Conf. on Wireless Network (ICWN 2004), June 2004. pp. 227-233.

[17] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, vol. 13, no.1, 2005-2010, pp. 14-27.

[18] M.K. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, no. 1, 2011, pp. 62-67.

[19] A.K. Pathan, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. 8th International Conf. Advanced Communication Technology (ICACT'08), vol. 2, 2006, pp. 1043-1048.

[20] A. Jangra, Swati, Richa and Priyanka, "Wireless Sensor Network (WSN): Architectural Design issues and Challenges", International Journal on Computer Science and Engineering, vol. 2, no. 9, 2010, pp. 3089-3094.

[21] S. Duan and X. Yuan, "Exploring Hierarchy Architecture for Wireless Sensor Network Management", Proc. IFIP International Conf. Wireless and Optical Communications Networks, IEEE, 2006, pp. 6.

[22] J. Feng, S. Megerian and M. Potkonjak, "Model Based Calibration for Sensor Networks", Proc. of IEEE Sensors, vol. 2, Oct. 2003, pp. 737-742.

[23] Y. Xue, Y. Cui, and K. Nahrstedt, "Maximizing Lifetime for Data Aggregation in Wireless Sensor Networks", Mobile Networks and Applications: Special Issue on Energy Constraints and Lifetime Performance in Wireless Sensor Networks, 2005, pp. 853-864.

[24] R. Rajagopalan and P.K. Varshney, "Data Aggregation Techniques in Sensor Networks: A Survey", IEEE Communications Surveys and Tutorials, 4th quarter, vol. 8, no. 4, 2006, pp. 48-63.

[25] A. Boulis, S. Ganeriwal and M.B. Srivastava, "Aggregation in Sensor Networks: An energy-accuracy trade-off", Proc. 1st IEEE International Workshop Sensor Network Protocols and Applications, May 2003, pp. 128-138.

[26] V. Bychkovskiy, S. Megerian, D. Estrin, and M. Potknojak, "A Collaborative Approach to In place Sensor Calibration", Proc. 2nd International Workshop Information Processing in Sensor Networks (IPSN'03), Apr. 2003, pp. 301-316.

[27] A. Ahmed, J. Ali, A. Raza and G. Abbas, "Wired Vs Wireless Deployment Support for Wireless Sensor Networks", Proc. IEEE Region 10 Conf. (TENCON 2006), Nov. 2006, pp. 1-3.

[28] J. Li, Y. Bai, H. Ji and D. Qian, "POWER: Planning and Deployment Platform for Wireless Sensor Networks", Proc. 5th International Conf. Grid and Cooperative Computing Workshops (GCCW'06), IEEE, Oct. 2006, pp. 432-436.

[29] J. Polastre, R. Szewczyk and D. Culler, "Telos: enabling ultra-low power wireless research", Proc. 4th International Symp. Information Processing in Sensor Networks (IPSN'05), Apr. 2005, pp. 364 – 369.

[30] T. Zia and A. Zomaya, "Security Issues in Wireless Sensor Networks", Proc. International Conf. Systems and Networks Communication (ICSNC'06), Nov. 2006, pp.40.

[31] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly resilient, energy efficient multipath routing in wireless sensor networks", Proc. 2nd ACM International Symp. Mobile Ad Hoc Networking and Computing (MobiHoc'01), Oct. 2001, pp. 251–254.

[32] R. Mulligan and H.M. Ammari, "Coverage in Wireless Sensor Networks: A Survey", Network Protocols & Algorithms, vol. 2, no. 2, 2010, pp. 27-53.

[33] T. Melodia and I.F. Akyildiz, "Research Challenges for Wireless Multimedia Sensor Networks", Distributed Video Sensor Networks, Chapter 16, Springer-Verlag London Limited, 2011, pp. 233-246.

[34] J. Elson, and K. Romer, "Wireless Sensor Networks: A New Regime for Time Synchronization", ACM SIGCOMM Computer Communication Review, vol. 33, no. 1, 2003, pp. 149-154.

[35] S. Palchaudhuri, A.K. Saha and D.B. Johnson, "Adaptive Clock Synchronization in Sensor Networks", Proc. 3rd International Symp. Information Processing in Sensor Networks (ISPN 2004), Apr. 2004, pp. 340-348.

[36] F. Sivrikaya and B. Yener, "Time Synchronization in Sensor Networks: A Survey", IEEE Network, vol. 18, no. 4, July/August 2004, pp. 45-50.