Wireless Sensor Network – Theoretical Findings and Applications

Ashish Patel
SVM Institute of Tech.
Bharuch, India

Rutvij Jhaveri
SVM Institute of Tech.
Bharuch, India

Kruti Dangarwala
SVM Institute of Tech.
Bharuch, India

ABSTRACT

Wireless sensor networks (WSN) consist of tiny sensor nodes scattered on a relatively large geographical area. The nodes are cooperative in nature, that is, they can communication with one another or to a central control unit. The work of each such node is to collect the information from surrounding like pressure, temperature, humidity, magnetic fields, optical fields etc [2]. Actually they are ad hoc network with some additional constraints. The node should be capable enough for power consumption, collection of data, self healing, mobility, self configuration to name a few. These features of WSN node differentiate it from conventional ad hoc networks [14]. This survey paper aims at reporting wireless sensor network, its design, networking of nodes, and security in system. In this paper, fundamentals of wireless sensor network are discussed. Different component like sensor, microcontroller, battery require for sensor networks are explained in detail. We have tried to include all the aspects of WSN. The Protocols, Operating Systems, tools require for WSN node programming and some security issues are also discussed.

1. INTRODUCTION

The WSN node typically has a transceiver, a microcontroller, an electronic circuit for interfacing with the sensors, on board storage and an energy source. The size and cost of each such node may vary according to the complexity. Sometimes WSN nodes also comprise actuators which can act directly to control different types of objects. For example, actuator can control the flow of gas in chamber, it can open a value by sensing the pressure, and it can start or stop the motor. WSN is active research area because of unlimited potential for numerous applications like military, environmental, health, transportation, construction, water/waste water management, disaster management etc. [15] Though, the limitation of wireless bandwidth and problems of power consumption, recently the wireless sensor network has experienced exponential growth because of the necessity of the application areas mentioned earlier. [17] The main characteristics of wireless sensor networks are Ability to cope with node failures, Mobility of nodes, Communication failures, Heterogeneity of nodes, Scalability to large scale of deployment, Ability to withstand harsh environmental conditions, Ease of use, and Power consumption as shown in fig.1. [6] The paper describes history, fundamentals of wireless sensor networking, components used in WSN, followed by operating systems, tools, protocols and security measurements require for functioning of wireless sensor network. The choice of sensor depends on the requirement of data collection like emperature, pressure, humidity, light etc. Based on these equirements one can classify the sensors in the categories like gyroscope, diodes, thermostats, thermocouples, accelerometer, GPS, capacitive or resistive, magnetometers etc.

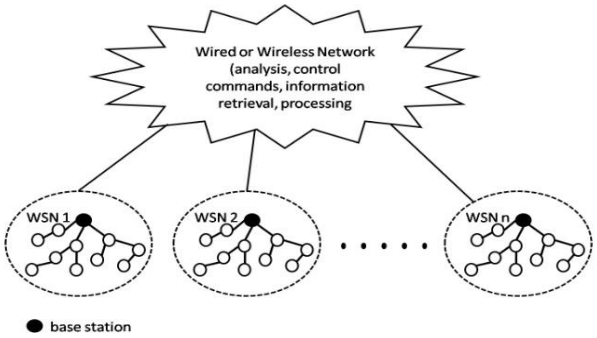
Wired or Wireless Network (analysis, control commands, information retrieval, processing
WSN 1
WSN 2
WSN n
• • • • •
base station

Fig. 1 Typical Wireless Sensor Network

The classification of sensors can also be based on the methods they apply and the electrical phenomena they utilize to convert physical properties into electrical signals like Resistive sensors, Inductive or piezoelectric sensor.

2. HISTORY

The distributed sensor network (DSN) program was initiated by the Defense Advanced Research Project Agency (DARPA) around 1980. [4] WSN technology started with the very early DARPA sponsored military project in 1978. During the 1990s DARPA was involved in search of the low power wireless integrated microprocessor (LWIM). In 1993 UCLA started research in WINS - Wireless Integrated Network Sensors. In 1998 a distributed military sensor system SenseIT was started with the help of 29 research projects involving 25 institutes and still working in the direction of new networking techniques and information processing. [2] The smartdust concept was introduced, developed, and funded by DARPA due to the potential military applications of the technology. [7] The PicoRadio (Berkeley Wireless Research Center) group is dedicated to advancing the field of Wireless Sensor Networks in all areas: RF circuit design, networking, positioning, low voltage digital design, antenna design, and low power analog design. Some tools are also invented like LEACH (Low-Energy Protocol Simulator for Wireless Networks) during these period. The Terminode project was there to develop a system approach to investigate wide area, large, totally wireless networks or mobile ad-hoc wide area networks (MANET). European Union Information Society Technologies (EU IST) is also working in wireless sensor networking area from 2003. [4] Technological advances in the past decade have completely changed the situation. MEMS technology, more reliable wireless communication, and low-cost manufacturing have resulted in small, inexpensive, and powerful sensors with embedded processing and wireless networking capability. Such wireless sensor networks can be used in many new applications, ranging from environmental monitoring to industrial sensing, as well as traditional military applications. [3] [11] [12] [21] The WSN time line is given below. [27]

1997	SMART DUST
1999	BERKELEY MOTES, TINYOS
2003	ZIGBEE ALLIANCE
2004	IEEE 802.15.4
2006	IEEE 802.15.4-2006 ZIGBEE PRO
2007	WIRELESS HART IETF RFC4944: IPV6 OVER 15.4
2008	ZIGBEE SMART ENERGY
2009	ZIGBEE GREEN POWER ANNOUNCED
2011	IEEE 802.15.4E IETF IPHC, ND, RPL, COAP, … ZIGBEE SE2.0

3. FUNDAMENTALS OF WIRELESS SENSOR NETWORKS

Although wireless sensor network shares many similarities with other distributed systems, it has some unique challenges and constraints. The advances in technologies such as very large scale integration (VLSI), microelectromechanical systems (MEMS), and wireless communications changed the whole scenario of wireless sensor networks. The desirable properties of WSN are energy efficiency, distributed sensing, wireless, multi-hop, distributed processing and low cost.

3.1 Sensor Network Applications

The main purpose of wireless sensor networks was military application during world war and later during the cold war. But today they are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, environment monitoring, target tracking, pipeline monitoring, structural health monitoring, precision agriculture, health care, supply chain management, active volcano monitoring, transportation, human activity monitoring, and underground mining, to name a few.

3.2 Sensor Network Design

The main part of sensor network is its node. Node, sometimes also known as mote is capable of sensing the data, processing of data and communication with other nodes using its own power source. Typical node consists of microcontroller, Transceiver, memory, power source and some sensors as shown in fig. 2. [10]

3.3 Microcontroller

It is a small integrated device generally used for embedded systems. Microcontroller provides real-time response in embedded environment. When certain event occurs, controller catches the interrupt and servers that interrupt. It is the main unit controlling the activities of other devices in the figure shown.

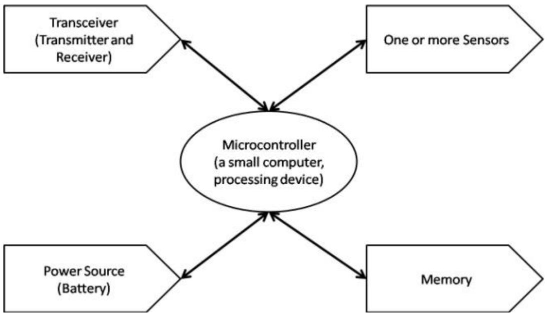

Fig. 2 Architecture of Wireless Sensor Node [10]

3.4 Transceiver

It is a unit containing both transmitter and receiver. Transceivers are called Medium Attachment Units (MAUs) in IEEE 802.3 documents and were widely used in 10BASE2 and 10BASE5 Ethernet networks.

3.5 Memory

The Sensor node must have onboard memory to store the data collected by different sensors. It can be on-chip or flash memory depending on the application requirements. Some portion of this memory is used to store system data and other portion is used for user data.

3.6 Power Source

The sensor node consumes power for sensing, communicating and data processing. Power can be stored in batteries or in capacitors. Life of sensor node depends mostly on the power source it is using. So power saving policies like Dynamic Power Management (DPM) or Dynamic Voltage Scaling (DVS) is used in sensor networks.

Sensor

Typical sensor converts the physical quantity such as temperature, humidity, pressure into a signal which can be further processed by some electronic device like microcontroller. Below is the list of some sensors by sensor type.

- Chemical
- Electric current, electric potential, magnetic, radio
- Environment, weather, moisture, humidity
- Automotive, transportation
- Acoustic, sound, vibration
- Flow, fluid velocity
- Ionizing radiation, subatomic particles
- Navigation instruments
- Position, angle, displacement, distance, speed, acceleration
- Optical, light, imaging, photon
- Pressure
- Force, density, level
- Thermal, heat, temperature
- Proximity, presence

Depending on the type of the sensor, it can sense different physical properties.

3.7 Sensor Network Topologies

Common sensor network topologies are Peer to Peer (also called Point to Point), Star, Tree and Mesh. There are many more network topologies that have not been discussed in this article.

3.8 Sensor Network Protocols

Network protocols decide, by which route on the network, node has to send packets for communications. [16] In wireless environment node announces its present by broadcasting the message and waits for the response from its neighbours. Routing protocols for wireless sensor networks are responsible for maintaining the routes in the network and have to ensure reliable multi-hop communication under the constraints like limited transmission range and low power consumption. [13] Table 1 shows some common routing protocols for WSN. [22]

There are other protocols like IMEP, TORA and W2LAN useful for routing in WSN.

Table 1 - LIST OF WIRELESS SENSOR PROTOCOLS

PROTOCOL	EXAMPLE
TABLE-DRIVEN (PRO-ACTIVE) ROUTING	HSR, DSDV, IARP, HSLS
REACTIVE (ON-DEMAND) ROUTING	AODV, ACOR, AORP, DYMO
FLOW-ORIENTED ROUTING	IERP, LUNAR, RDMAR, SSR
HYBRID ROUTING	HRPLS, HWMP, OON, ZRP
HIERARCHICAL ROUTING PROTOCOLS	CBRP, CEDAR, FSR
BACKPRESSURE ROUTING	DIVBAR
HOST SPECIFIC ROUTING PROTOCOLS	LANMAR
MULTICAST ROUTING	MRMP, ERAMOBILE, PUMA, AMRIS, LAM, TSMP
GEOGRAPHICAL MULTICAST PROTOCOLS (GEOCASTING)	MOBICAST, ABIDING GEOCAST
ON-DEMAND DATA DELIVERY ROUTING	MAODDP
OTHER PROTOCOLS	IMEP, TORA, W2LAN

3.9 Communication between nodes and BS

In other wireless domain network role is of data transport, compete for resources, high data rates, maximize network throughput. While in Wireless Sensor Network, network role is information collection, resource allocation, low data rates and maximizes network life time. Sensor nodes always require active connection for communicating with neighbour nodes as well as base station. Communication plays important role in designing wireless sensor network. Primarily, there are three types of communication techniques, Optical Communication, Infrared Communication and Radio-Frequency Communication. Optical communication can be disturbed by atmospheric conditions and requires line of sight. Infrared is having very limited range and RF communication is having a problem with antenna size, a good trade-off require for choice of communication technique. Ease of use, availability in market and integrity among the nodes makes RF communication a good candidate for testing in sensor nodes. [23]

4. OPERATING SYSTEM

Operating system in WSN enables the applications to interact with hardware resources to accomplish particular task. Moreover, Operating system is responsible for memory management, power management, file management and networking. Operating systems are of two types, single task and multi task. Multitasking operating system require large amount of memory. The choice of operating system for WSN depends on the factors like data types, scheduling, memory, multithreading, interrupt and so on.

TinyOS is the most widely used runtime environment in WSN. It is Event-Based operating system and uses static memory management system. Mate is design to work on top of TinyOS as one of its component. Other operating systems are SOS, Contiki and LiteOS and they are using dynamic memory management system. TinyOS and SOS not allow us to use system calls but Contiki and LiteOS supports system calls. [26] Generally, the field of wireless sensor networks is relatively young. The operation environments as well as the application requirements are likely to evolve and to be made more compact and refined. Subsequently, the tradeoff is between dynamic reprogramming and code replacement on the one hand, and code execution efficiency on the other. [2] Other useful environments are MagnetOS, MANTIS, OSPM, EYESOS, SENOS, EMERALDS and PicOS.

5. SENSOR NETWORK TOOLS

It is generally not feasible to develop a model to test the behaviour of a sensor node because of complexity of the networks. So simulation tools are necessary to study the behaviour of a node or to do research in this area. One can classify sensor network tools in two categories, General simulation packages and Specific WSN Framework. [5] NS-2 (Network Simulator), OMNET++ (Objective Modular Network Testbed), J-Sim, NCTUns2.0, JiST/SWANS, GloMoSim, SSFNet, Ptolemy II are some examples of general tools available for simulation. TOSSIM [25], EmStar /EmSim /EmTOS [24], ATEMU, SENS, Prowler/JProwler, SNAP are some examples of specific WSN tools.

6. WSN PROGRAMMING

In WSN constant communication requires with the nodes due to failure of node or changes in network topologies. So WSN programming differs in many ways with the traditional distributed programming. Sensor network programming approaches can be classified as either node-centric or application-centric. Node-centric approach generally deals with programming a single node, the entire network sensing application can be defined by considering the logic of all nodes of the system. nesC, TinyGALS (globally asynchronous and locally synchronous), SNACK (Sensor Network Application Construction Kit) and different thread based models are used for programming a WSN node. [18] The main advantage of the thread-based approach is that multiple tasks can make progress in their execution without blocking other tasks.

7. SECURITY IN WIRELESS SENSOR NETWORKS

The characteristics of wireless sensor networks, such as Resource constraints, Lack of central control, limited battery power and lack of infrastructure, make them more vulnerable to attack than conventional ad hoc networks. The security schemes for WSN should require less computational power and memory because sensor nodes are tiny and have more limited capacity. [9] WSN node is prone to active or passive attack. Some of the well known attacks on WSN are Denial of service (DoS) attack, Sybil attack, Hello Flood, Wormhole attack, Blackhole or Sinkhole attack etc. [20] However, developing solution to these attacks and making it efficient represents a great research challenge. Again, ensuring security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. [19] In a secure wireless ad hoc sensor network, a node is authorized by the network and only authorized nodes are allowed to access the network resources. The generic process to establish such a network consists of bootstrapping, pre-authentication, network security association establishment, authentication, and behaviour monitoring and security association revocation. Among these, authentication is of the utmost importance and is an essential service in network security. Other basic security services like confidentiality, integrity and nonrepudiation depend on authentication. Secret information is exchanged only after nodes are able to verify and validate one another [9].

8. CONCLUSION

Objective of WSN was stand-alone systems for monitoring and surveillance in military applications; they are becoming key component of next generation networks. Today, most of the sensor network solutions are under testing and implementation for better results. Networks of hundreds of sensor nodes are already being used to monitor large geographic areas for modelling and analyzing data. Still, Sensor networks are only a semi-functional prototype model for many applications. [8] The area requires great involvement from researchers, students, and practitioners for understanding the challenges of this exciting field. Despite their popularity, wireless sensor network systems are difficult to code. Developers of these systems need to deal with high-level application logics and low-level input/output operations simultaneously. The survey paper throws the light on most of the basic fundamental aspects of wireless sensor networks. While these topics are some of the key issues regarding WSN, there are many important topics not discussed in this paper. The author has tried to explain the WSN system for further study.

9. REFERENCES

[1] S. Kumar and D. Shepherd, "SensIT: Sensor information technology for the warfighter," in Proc. 4th Int. Conf. on Information Fusion, 2001, pp. TuC1-3–TuC1-9.

[2] Waltenegus Dargie, Christian Poellabauer, "Fundamentals of Wireless Sensor Networks, Theory and Practice", Wiley Series on Wireless Communication and Mobile Computing.

[3] Chee-Yee Chong, and S.P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," Proceedings of the IEEE, Vol. 91, No.8, August 2003.

[4] I. Khemapech, I. Duncan, and A. Miller, "A Survey of Wireless Sensor Networks Technology, in PGNET", Proceedings of the 6th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting, EPSRC, June 2005.

[5] E. Egea-López, J. Vales-Alonso, A. S. Martínez-Sala, P. Pavón-Mariño, J. García-Haro, "Simulation Tools for Wireless Sensor Networks", Summer Simulation Multiconference – SPECTS, 2005

[6] M.A.M. Vieira, C.N. Coelho. Jr., D.C. da Silva Jr., and J.M. da Mata, "Survey on Wireless Sensor Network Devices," IEEE, 2003.

[7] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Mobile networking for smart dust," in Proc. ACM/IEEE Int. Conf. Mobile Computing and Networking (MobiCom), 1999, pp. 271–278.

[8] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in Proc. Int. Conf. Mobile Computing and Networking (MOBICOM), 1999, pp. 263–270.

[9] Erdal Çayırcı, Chunming Rong, " Security in Wireless Ad hoc and Sensor Networks, A John Wiley and sons ltd, publication, 2009.

[10] J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, "System Architecture Directions for Networked Sensors", ASPLOS, November 2000

[11] J Rabaey, J Ammer, J Silva Jr., and D Pater. "Picoradio: Adhoc wireless networking of ubiquitous low-energy sensor/monitor nodes", In WVLSI, Orlando, Florida, USA, April 2000.

[12] D. Kotz, C. Newport, B. Gray, J. Liu, Y. Yuan, C.Elliot. "Experimental Evaluation of Wireless Simulation Assumptions." In Proc. of the 7th ACM/IEEE Int. Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM'04), Venice, Italy, pp. 78–82, October 2004.

[13] Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera, and Cláudia Jacy Barenco Abbas, "Routing Protocol in Wireless Sensor Networks", vol. 9, Sensors 2009, pp. 8399-8421.

[14] S. Misra, "Guide to Wireless Sensor Networks", Computer Communications and Networks, DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.

[15] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422

[16] Dai S, Jing X, and Li L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.

[17] Paolo Baronti, Prashant Pillai, Vince Chook, Stefano Chessa, Alberto Gotta, Y. Fun Hu,"Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards", PhD Seminar.

[18] David Gay, Philip Levis, Robert von Behren, MattWelsh, Eric Brewer, and David Culler, "The nesC Language: A Holistic Approach to Networked Embedded Systems", Proc. ACM SIGPLAN Conference on Programming

Language Design and Implementation (PLDI 2003), pp. 1-11, San Diego, CA, USA, June 2003.

[19] Chris Karlof, David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures” Ad Hoc Networks, 1: 293–315, 2003.

[20] John P. Walthers, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, “Wireless Sensor Networks Security: A Survey”, Technical Report MIST-TR-2005-007, July 2005.

[21] J. Zheng and M.J. Lee, “Will IEEE 802.15.4 Make Ubiquitous Networking a Reality?” IEEE Communication Mag., Jun 2004.

[22] Shio Kumar Singh, M P Singh, and D K Singh, “Routing Protocols in Wireless Sensor Networks – A Survey”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.

[23] Marcos Augusto M. Vieira, Claudionor N. Coelho. Jr., Diógenes Cecílio da Silva Junior, José M. da Mata, "Survey on Wireless Sensor Network Devices", Federal University of Minas Gerais, Brazil.

[24] Girod, L., Elson, J., Cerpa, A., Stathopoulos, T., Ramanathan, N., and Estrin, D., “EmStar: A software environment for developing and deploying wireless sensor networks”, Proc. of the USENIX Annual Technical Conference, Boston, MA, 2004.

[25] Levis, P., Lee, N., Welsh, M., and Culler, D., “TOSSIM: Accurate and scalable simulation of entire TinyOS applications”, Proc. of the 1st ACM Conference on Embedded Networked Sensor Systems (SenSys), Los Angeles, CA, 2003.

[26] Abdelzaher, T., Stankovic, J., and He, T. “The LiteOS operating system: Towards Unix-like abstractions for wireless sensor networks”, IPSN ’08: Proceedings of the 7th International Conference on Information Processing in Sensor Networks (pp. 233–244). IEEE Computer Society, Washington, DC, USA, 2006.

[27] Kris Pister, “Wireless Sensor Network Standards”, Founder & Chief Technologist, Dust Networks, EECS, UC Berkeley, 2011.