International Journal of Research in Engineering and Innovation (IJREI)
journal home page: http://www.ijrei.com
ISSN (Online): 2456-6934

Study of wireless sensor networks with its applications and security

P. Valarmathi

Lecturer (Senior Grade), Department of Electronics & Communication Engineering, Sakthi Polytechnic College, Erode, Tamil Nadu, India

Abstract

Wireless Sensor Networks (WSNs) are an emerging technology with a wide range of potential application areas such as monitoring, tracking and controlling. For several applications of Wireless Sensor Network, security is an important requirement. However, security solutions in Wireless Sensor Network are entirely different compared with traditional networks due to resource limitation and computational constraints. This paper presents the characteristics, security requirements, encryption algorithms and operation modes of Wireless Sensor Network to develop a security solution. Also, an overview of the applications of WSNs and different attacks and their countermeasures are to be discussed.
© 2018 ijrei.com. All rights reserved
Keywords: Wireless Sensor Network, Analog to Digital converter, Distributed WSN, Hierarchical WSN, Medium Access control, Transmission Control Protocol.

1. Introduction

A sensor network is a wireless network consisting of spatially distributed autonomous devices that use sensors to observe physical or environmental conditions [1, 2]. WSNs are becoming considerably very important to many applications and used by military for surveillance purposes. A WSN is a distributed network and it contains a large number of distributed, self-directed and tiny, low powered devices called sensor nodes. Figure 1 shows a typical Wireless Sensor Network.

WSNs are composed of sensor nodes which are closely deployed either inside a physical phenomenon or very close to it. The sensor nodes are transceivers usually scattered in a sensor field which has the ability to collect data and route data back to the sink and the end-users are connected through the sink. The sink communicates with the end-user through internet or satellite network or wireless network like WiFi, cellular systems, etc. However, in many cases the sink can be directly connected to the end-users.

The ever-increasing capabilities of these tiny sensor nodes, which include sensing, data processing, and communicating, enable the realization of WSNs based on the collaborative effort of a number of other sensor nodes

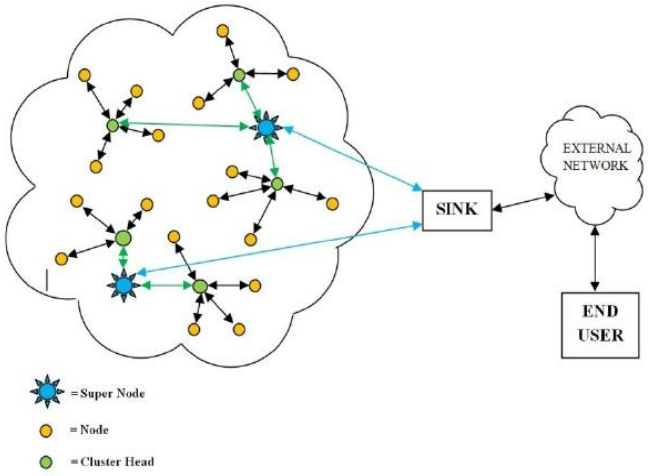

Figure 1: A typical Wireless Sensor Network [7]

Figure 2 shows the areas of WSN. It includes knowledge and technologies from wireless communications, networking and systems and control theory. In order to realize the existing and potential applications for WSNs, an extremely efficient communication protocols are required.

Corresponding author: P. Valarmathi
Email Id: rameshb4u@yahoo.com

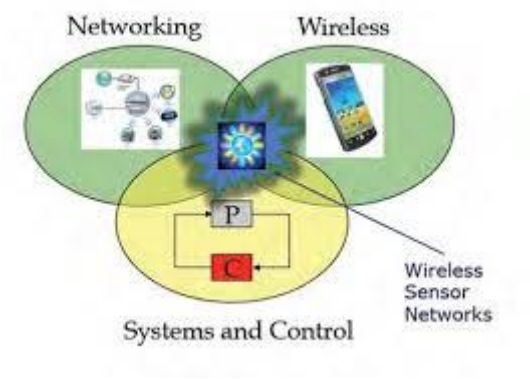

Figure 2: Areas of WSN [3]

1.1 Objectives for WSN Design

The following are the objectives of Wireless Sensor Network design. [4]

- Reducing node size
- Reducing node cost
- Low Power Consumption
- Self - Configurability
- Scalability
- Adaptability
- Reliability
- Fault Tolerance
- Security

1.2 Components of WSN system

The components of WSN system are sensor node, relay node, actor node, cluster head, gateway and base station.

1.2.1 Sensor node

Source node is having capable of executing data processing, data gathering and communicating with additional associated nodes in the network.

1.2.2 Relay node

It is a midway node used to communicate with the adjacent node. It is used to enhance the network reliability. It is a special type of field device that does not have process sensor or control equipment.

1.2.3 Actor node

Actor node is a high end node used to perform and construct a decision based on the application requirements.

1.2.4 Cluster head

It is a high bandwidth sensing node used to execute data fusion and aggregation functions. Based on the applications, there may be more than one cluster head inside the cluster.
Gateway: It is an interfacing between sensor networks and outside networks. The gateway node is most powerful in program memory and data memory, processor utilized, transceiver range and extension possibilities through external memory.

1.2.5 Base station

It is an extraordinary type of nodes having high computational energy and processing capability.
Generally, Fault Tolerance, Scalability, Production Costs, Hardware Constraints, Sensor Network Topology, Transmission Media and Power Consumption are the Design issues of a wireless sensor network.

1.3 *Node components of WSN*

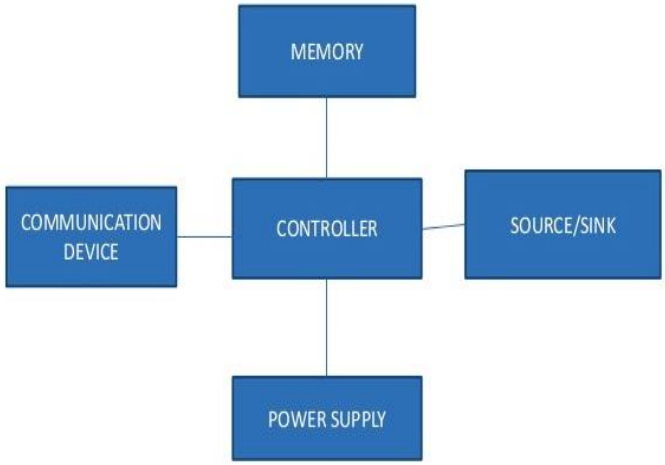

Figure 3: Node component of a WSN [33]

Each sensor node consists of a microcontroller unit, transceiver unit, power unit, memory unit and a sensor unit. The node component of a WSN is shown in figure 3.
The sensor unit is the main component of a wireless sensor node that differentiates it from other embedded system. It includes several sensor units of sensor nodes which integrate various sensors like thermal sensors, magnetic sensors, vibration sensors, chemical sensors, bio sensors, and light sensors.
The measured parameters from the external environment are fed into the processing unit by sensing unit of sensor node. The analog signal generated by the sensors are digitized by using Analog to Digital converter (ADC) and sent to controller for further processing.
The processing unit is the important core unit of the sensor node which executes different tasks and controls the function of other components. The required services for the processing unit are pre-programmed and loaded in the sensor node processor unit. The energy utilization rate varies depending

upon the nodes functionality. The variation in the performance of the processor is identified by the evaluating factors like processing speed, data rate, memory and peripherals supported by the processors. Mostly ATMEGA 16, ATMEGA 128L, MSP 430 controllers are used in commercial motes.

The computations are performed in the processing unit and the acquired result is transmitted to the base station through the communication unit. In communication unit, a common transceiver acts as a communication device and used to transmit and receive the information among the nodes and base station and vice versa. There are four states in the communication unit: transmit, receive, idle and sleep. A functional block diagram of a versatile wireless sensing node is shown in figure 4. A key aspect of wireless sensing node is to reduce the power consumption of the system and periodical measurement of power quality is done.

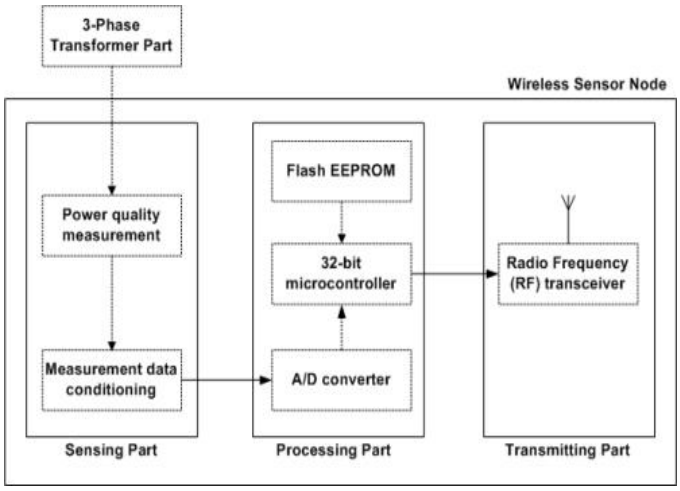

Figure 4: Functional Block Diagram of a Versatile Wireless Sensing Node [34]

Based on the node properties, the sensor networks are classified into homogenous sensor networks and heterogeneous sensor networks. If all the sensor nodes within the cluster are having the same properties or homogenous, it is called as Distributed WSN (DWSN), otherwise (heterogeneous) it is referred as Hierarchical WSN (HWSN). Figure 5 shows the hierarchical and distributed WSN.

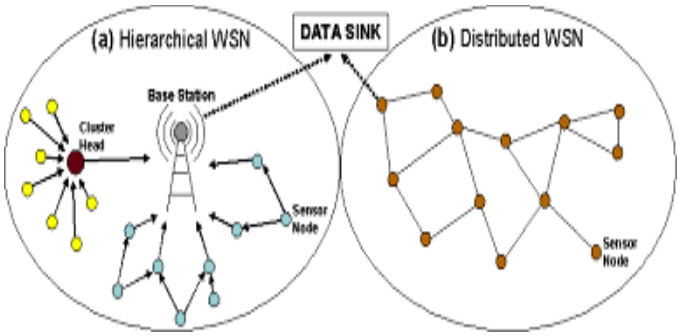

Figure 5: Hierarchical and Distributed WSN

The major characteristics of the sensor node used to evaluate the performance of WSN are [5],

- Fault tolerance
- Mobility of nodes
- Dynamic network topology
- No communication failures
- Heterogeneity of nodes
- Scalability
- Independency and programmability
- Utilization of sensors
- Impracticality of public key cryptosystems
- Lack of a prior knowledge of post-deployment configuration

2. Organization of WSN

Any WSN can be configured as a five layered architecture as,

1. The physical layer is responsible for frequency selection, modulation and data encryption.
2. The data link layer functions as a pathway for multiplexing of data streams, data frame detection, Medium Access Control (MAC) and error control.
3. The network layer is used to route the data supplied by the transport layer using special multi-hop wireless routing protocols between sensor nodes and sink nodes.
4. The transport layer maintains the data flow if the application layer requires it.
5. The application layer makes the hardware and software of the lower layers transparent to the end user.

2.1 Communication structure of a wireless sensor network

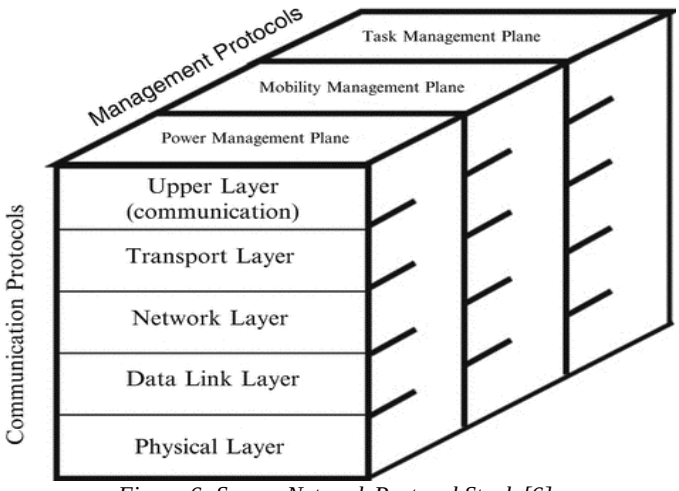

Figure 6: Sensor Network Protocol Stack [6]

The sensor network protocol stack shown in figure 6. It consists of physical layer, data link layer, network layer, transport layer, application layer and power management, mobility management, task management planes [7].

2.1.1 Physical layer

It is responsible for selection of frequency, generation of carrier frequency, signal detection, modulation and data encryption. Modulation depends on transceiver and hardware designing for simple operation, low power consumption and low cost. Binary modulation schemes are easy to implement and have more energy efficient. This layer addresses the needs of simple but robust modulation, transmitting and receiving techniques.

2.1.2 Data Link Layer

It is liable for multiplexing data streams, frame detection, medium access and error control. It ensures point-to-point and point-to-multipoint links in communication system. Medium Access Control protocols share communication resources between sensor nodes more efficiently. Since there is a noise, MAC must be power-aware and able to reduce collision with nearest broad cast.

2.1.3 Network Layer

It is responsible for routing the data supplied by the transport layer. It is designed by considering the following points.

- Power efficiency is an important concern.
- Sensor network is almost data centric.
- Data aggregation is useful only when it does not hinder the sensor node collaborative effort.
- An ideal sensor network has attribute-based addressing and location awareness.
- Clock synchronization and fault tolerance.

2.1.4 Transport layer

It helps to maintain the data flow if sensor network requires it. It is required when a system to be accessed through internet or other external networks. The Transmission Control Protocol (TCP) needs to be split into two parts in which one part connects the sensor network with other network like internet and another part connects the sink node to sensor nodes.

2.1.5 Application Layer

Based on sensing tasks, different types of application software can be built and used on application layer. These protocols make hardware and software of lower layers transparent so that system can be edited easily. The protocols are, Sensor Management Protocol (SMP), Sensor Query and Data Dissemination Protocol (SQDDP), Task Assignment and Data Advertisement Protocol (TADAP).

3. Power, Mobility and Task Management Planes

When the power level of a sensor node is low, it cannot participate in routing messages. This problem can be handled by power management plane. The mobility management plane identifies and registers the moving of sensor nodes. The task management plane balances and schedules sensing tasks given to a specific region.

4. Routing Protocols for WSN

Routing protocols for wireless sensor networks can be classified into data-centric, hierarchical and location-based. Figure 2 shows the wireless sensor network routing protocols. In these categories, source, shortest path, and hierarchical and geographical routing have been employed to develop all of the routing algorithms.

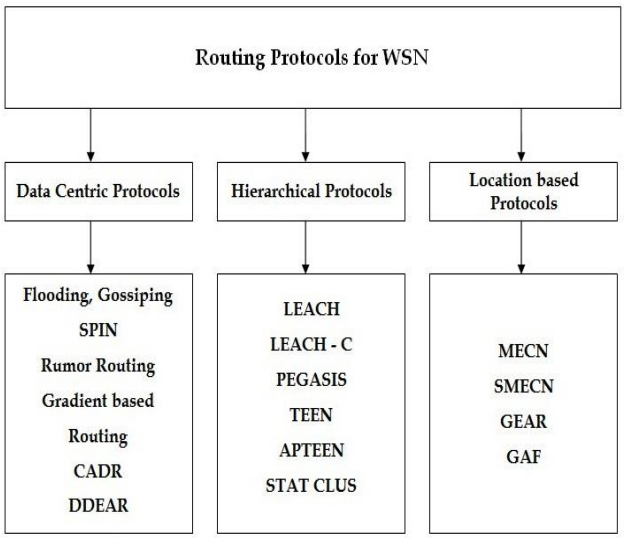

Figure 7: Wireless sensor network routing protocols [8]

In data-centric protocols, the sensor nodes transmit information for the available data and wait for a signal requisition from an interested sink. Flooding is one of the simplest techniques which may be used to broadcast information in WSN and a reactive technique which need not require costlier topology maintenance or complex route discovery algorithms. A gossiping is a flooding derivative, in which nodes do not broadcast. Instead of broadcasting, they send the incoming packets to a randomly selected neighbor.

Sensor Protocols for Information via Negotiation (SPIN) address the deficiencies of classic flooding by providing negotiation and resource adaptation [9]. SPIN employs a shortest path strategy based on three types of messages:

• ADV – New data advertisement.
• REQ – Request for data.
• DATA – Data message.

The popular algorithm for data-centric protocols is direct diffusion and it depends on its routing strategy on shortest path [10]. Rumor routing [11] is a direct diffusion variation that is proposed where geographic routing is not feasible. Gradient based routing is another variant of direct diffusion [12].

The key idea of gradient-based routing is to memorize the hops when the interest is diffused in the entire network. Constraint

Anisotropic Diffusion Routing (CADR) is a common form of direct diffusion [13] makes the network as a distributed one in which complex queries may be further classified into several sub queries.

4.1 Hierarchical protocols

These protocols are based on clusters because it contributes to more scalable activities like increase in nodes, improved robustness and more efficient resource utilization for many distributed sensor coordination tasks. Low-Energy Adaptive Clustering Hierarchy (LEACH) is a cluster-based protocol that minimizes energy dissipation in sensor networks by randomly selecting sensor nodes as cluster heads [14].

Power-Efficient Gathering in Sensor Information System (PEGASIS) [15] is a near optimal chain-based protocol. In Threshold-sensitive Energy Efficient protocol (TEEN) [16], sensor nodes continuously sense the medium, but data transmission is done less frequently. On the other hand, Adaptive Periodic TEEN (APTEEN) is a hybrid protocol which changes the threshold values in the TEEN protocol, as per the user needs and type of application [17].

4.2 Location-based protocols

Location-based protocols make use of position information to relay data to the desired regions. Existing location services can be classified according to how many nodes host the service. This can be either a specific node or all of the network nodes. Minimum Energy Communication Network (MECN) [18] establishes and maintains a minimum energy network for wireless networks by utilizing low-power geographic positioning system (GPS).

The Small Minimum Energy Communication Network (SMECN) [19] is an extension of MECN. The main advantage of SMECN is that it considers obstacles between pairs of nodes. Geographic Adaptive Fidelity (GAF) [20] is an energy-aware location-based routing algorithm which conserves energy by switch off the unnecessary nodes without affecting the routing fidelity. Finally, Geographic and Energy Aware Routing [21] uses energy-awareness and geographically informed neighbor selection heuristics to route a packet toward the destination region.

5. Measurement of power consumption in WSNs

In order to ensure the expected lifetime in a WSN, it is important to properly define the workflow of the nodes, evaluating and measuring their power consumption. Such evaluation may provide feedback during application design phase, consenting to improve the overall energy efficiency. The methods determining the power consumption are theoretical estimation, direct measurements and usage simulations tools.

Theoretical estimation relies on the network concept including the surrounding environment. Due to the difficulty of describing the environment, realistic models are not easily evaluated and even simplified models can be very complex, resulting impractical or not accurate [22].

Direct measurements, relying on physical sensor node, give the good accuracy on energy consumption estimation. Due to the availability of multiple platforms and environmental constraints, the implementing design and deployment of a sensor network application are complex tasks [23]. Thus it is often useful to simulate, at various stage of development, one or more components of the networks. Thus, accurate simulators may be a useful tool for the assessment of the WSN performance. Specific solutions have been proposed in recent years for various wireless systems.

For instance, some simulators have been developed for PAN network devices, such as Bluetooth. A Bluetooth device has been described as a finite state machine, each state being associated to link manager level activities, such as a scan/inquiry operation. The average power consumption was measured for each identified state transitions so that the results are more accurate [24].

A deep optimization of power consumption may require a simulation tool to profile the energy cost of the internal work of each node. This requires to model events with time constants that may be lower than a microsecond [25]. Thus, other WSN simulators have been recently developed, focused on the simulation of the protocol and MAC level, on processor profiling, on attempting to combine both features [26] [27].

6. Attacks and Security Mechanisms on WSN

The following are the types of attacks and the security mechanisms to counter the attacks on wireless sensor networks [28].

1. Common Attacks
2. Denial of service (DoS) Attack
3. Node compromise
4. Impersonation Attack
5. Protocol- specific Attack

6.1 Common Attack

The first common attack is eavesdropping i.e., an adversary can easily retrieve valuable data from the transmitted packets that are sent. The second common attack is Message modification i.e., the adversary can intercept the packets and modify them. The third common attack is message replay i.e., the adversary can retransmit the contents of the packets at a later time.

To counter common attacks like eavesdropping, message modification, message replay attacks, strong encryption techniques and time stamps are to be used.

6.2 DoS Attack

A DoS attack on WSN may take several forms.

- Node collaboration: A set of nodes act unkindly and restrict broadcast messages from certain sections of sensor networks.
- Jamming attack: An attacker jams the communication channel and avoids any member of the network in the affected area to send or receive any packet.
- Exhaustion of power: An attacker repeatedly requests packets from sensors to deplete their battery life.

6.3 Node compromise Attack

A sensor node is considered as compromised when an attacker gains control to the sensor node itself after it may be arranged. Different complex attacks can be easily started, since the subverted node is a full- fledged member of WSN.

6.4 Impersonation Attack

In this attack, a malicious node impersonates a legitimate node and uses its identity to mount an active attack like Sybil or node replication. In a Sybil attack, a single node takes on multiple identities to deceive other nodes. On the other hand, the node replication attack is the duplication of sensor nodes.
To counter Sybil attack proper authentication is a key defense. A trusted key server or base station may be used to authenticate nodes to each other and bootstrap a shared session key for encrypted communications.

6.5 Protocol- specific Attack

The attacks against routing protocols in WSN are:

- Spoofed routing information - Corruption of the internal control information.
- Selective forwarding - Traverse a malicious node depending on some criteria. To counter selective forwarding attack, Using multiple disjoint routing paths and diversity coding are used.
- Wormhole attack - Captures the information at one location and replays them in another location either unchanged or tampered.
- Hello flood attack - Creation of false control packets during network deployment.

7. Applications of WSN

The applications of wireless sensor network are as follows. [29, 30, 31]

7.1 Military or Border Surveillance Applications

WSNs are the essential part of military command, control, communication and intelligence systems. Sensors can be deployed in a battle field to monitor the presence of vehicles and track their movements, enabling close surveillance of opposite forces.

7.2 Environmental Applications

Environmental applications include tracking the movements and patterns of insects, birds or small animals.

7.3 Health Care Applications

Wireless sensor networks can be used to monitor and track patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care expenditures in the current health care systems.

7.4 Environmental Conditions Monitoring

WSN monitors the environmental conditions affecting crops or livestock, monitoring temperature, humidity and lighting in office buildings, and so on. These monitoring modules could even be combined with actuator control modules.
Home Intelligence
WSN provides intelligent living environments for human beings in a home like water, gas, electricity and then send the readings to a remote centre through wireless communication.

7.5 Industrial Process Control

In industries, WSNs are used to monitor manufacturing process or the manufacturing equipment. For example, chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. These sensors are used to alert in case of any failures occurred.

7.6 Agriculture

Sensors can be deployed on the ground or under water to monitor air or water quality. Gravity feed water system is observed by pressure transmitters to monitor water levels, pumps may be controlled using wireless I/O devices. Irrigation automation technique enables more efficient usage and reduces the wastages [32].

7.7 Structural Monitoring

Wireless sensors are used to monitor the movement within a buildings/infrastructure like bridges, flyovers, tunnels etc. and enabling engineering practices to monitor assets remotely. It is also far more accurate than any visual inspection that would be carried out.

8. Conclusion

Networking is one of the most important aspects in the design

of WSNs, which involves a variety of network architectural and protocol design issues. For designing a proper Wireless Sensor Network, we should consider the flexibility in operation, low cost, more energy efficiency, fault tolerance, high sensing reliability and fast deployment. When developing a security solution, the WSN characteristics, security requirements, modes and the current encryption algorithms are considered. The strategies of security protocols may help on the security issue in WSNs. Also, an overview of the applications of WSNs and different attacks and their countermeasures are discussed.

References

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

[2] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[3] An Introduction to Wireless Sensor Networks, Draft, version 1.8, Carlo Fischione September 2014.

[4] F. Koushanfar, M. Potkonjak and A. Sangiovanni - Vincentelli , " Fault - tolerance techniques for ad-hoc sensor networks ", Proceedings of IEEE Sensors, Vol. 2 , June 2002, pp. 1491–1496.

[5] Kavita Kumari, Inderdeep Kaur Aulakh and Amol P Bhondekar, "Structural Health Monitoring System using Wireless Sensor Network", Conference Paper, April 2015.

[6] Kazem Sohraby, Daniel Minoli and Taieb Znati, "Wireless Sensor Networks Technology, Protocols and Applications", Wiley Interscience A John Wiley & Sons, Inc., Publication.

[7] M.A. Matin and M.M. Islam, "Overview of Wireless Sensor Network", Chapter 1, Published by INTECH, http://dx.doi.org/10.5772/49376.

[8] Raúl Aquino-Santos, Luis A. Villaseñor-González and Víctor Rangel Licea, "Performance analysis of routing strategies for wireless sensor networks", Rev. Fac. Ing. Univ. Antioquia No. 52 pp. 185 – 195, March 2010.

[9] W. R. Heinzelman, J. Kulik and H. Balakrishnan, "Adaptive Protocols for information Dissemination in Wireless Sensor Networks", Proceedings of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM). 1999. pp. 174-185.

[10] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, "Next Century Challenges: Scalable Coordination in Sensor Networks", Proceedings of the 5th ACM/IEEE International Conference on Mobile Computing and Networking, 1999. pp. 263-270.

[11] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks", International Conference on Distributed Computing Systems (ICDCS-22), 2002, pp.22-31.

[12] C. Schurgers and M. B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks", Proceedings of the Communication for Network-centric operations: creating the information force, 2001, pp. 1-5.

[13] M. Chu, H. Haussecker and F. Zhao, "Scalable Information-Driven Sensor Querying and Routing for ad-hoc Heterogeneous Sensor Networks", International Journal of High Performance Computing Applications, Vol. 16, 2002, pp. 293-313.

[14] Heinzelman, W. R. Chandrakasan and A. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Vol. 2, 2000, pp. 1-10.

[15] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-Efficient GAthering in Sensor Information Systems", Proceeding of the IEEE Aerospace Conference, Vol. 3, 2002, pp. 1125-1130.

[16] A. Manjeshwar and D. P. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks", Proceedings of the 15th International Symposium on Parallel and Distributed Processing, 2001, pp. 2009-2015.

[17] A. Manjeshwar and D. P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks", Proceedings of the 16th International Symposium on Parallel and Distributed Processing, 2002, pp.195-202.

[18] V. Rodoplu and T. H. Meng, "Minimum Energy Mobile Wireless Networks", IEEE Journal on selected areas in communications, Vol. 17, 1999, pp. 1333-1344.

[19] L. Li and J.Y. Halpern, "Minimum-Energy Mobile Wireless Networks Revisited", IEEE International Conference on Communications, Vol. 1, 2001, pp. 278-283.

[20] Y. Xu, J. Heideman and D. Estrin, "Geography informed Energy Conservation for Ad-Hoc Routing", Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking, 2001, pp. 70-84.

[21] Y. Yu, R. Govindan and D. Estrin, "Geographic and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks", UCLA Computer Science Department Technical Report, UCLA/CSD-TR-01-0023, 2001.

[22] Abuarqoub, Abdelrahman, et. al., "Simulation Issues in Wireless Sensor Networks: A Survey", SENSORCOMM, The Sixth International Conference on Sensor Technologies and Applications, 2012.

[23] Hergenröder, Anton, Joachim Wilke and Detlev Meier, "Distributed energy measurements in WSN Test beds with a sensor node management device (SNMD)", Architecture of Computing Systems (ARCS), 23rd International Conference on. VDE, 2010.

[24] D. Macii and D. Petri, "An Effective Power Consumption Measurement Procedure for Bluetooth Wireless Modules", IEEE Transactions on Instrumentation and Measurements, Vol. 56, No. 4, August 2007.

[25] T. Laopoulos, P. Neofotistos, C. A. Kosmatopoulos, and S. Nikolaidis, "Measurement of Current Variations for the Estimation of Software-Related Power Consumption", IEEE Transactions on Instrumentation and Measurements, Vol. 52, No. 4, August 2003.

[26] Egea-Lopez, E., et. al., "Simulation tools for wireless sensor networks", Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS '05), 2005.

[27] Antonio Moschitta and Igor Neri, "Power consumption Assessment in Wireless Sensor Networks", Chapter 9, Published by INTECH, http://dx.doi.org/10.5772/57201.

[28] S. Prasanna, Srinivasa Rao, "An Overview of Wireless Sensor Networks Applications and Security", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[29] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey", Computer Networks, Vol. 38 (4), pp. 393–422, 2002.

[30] Bharathidasan, A., Anand, V. and Ponduru, S., "Sensor Networks: An Overview", Department of Computer Science, University of California, Davis, Technical Report. 2001.

[31] A. Boukerche, "Algorithms and Protocols for Wireless", Mobile Ad Hoc Networks, John Wiley & Sons, Inc., 2009.

[32] Jun Zheng and Abbas Jamalipour, "Introduction to Wireless Sensor Networks", Institute of Electrical and Electronics Engineers, 2009.

[33] Miguel Angel Erazo Villegas, Seok Yee Tang and Yi Qian, "Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring," Technical Report TR-NCIG-0501.

[34] Yujin Lim, Hak-Man Kim and Sanggil Kang, "A Design of Wireless Sensor Networks for a Power Quality Monitoring System," Sensors, Nov 2010.