

REVIEW ON WIRELESS SENSOR NETWORK

NIMISHA A RAI¹, JAYSHREE S SONAWANE²

¹Asst. Prof. Department of Electronics, Dr. D.Y. Patil ACS College, Pune University, Pimpri, Pune, India

²H.O.D, Department of Electronics, Dr. D.Y. Patil ACS College, Pune University, Pimpri, Pune, India
nimishaanilrai@gmail.com, jayshreesonawane@ymail.com

ABSTRACT

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. This has been enabled by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, and cost, hardware, and system constraints. This Paper represents a survey on types of network, Topologies, Characteristic of WSN, Design objective, Application Layer.

Keywords: WSN, adhoc, MANET, MAC

[1] INTRODUCTION

A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from a battery.

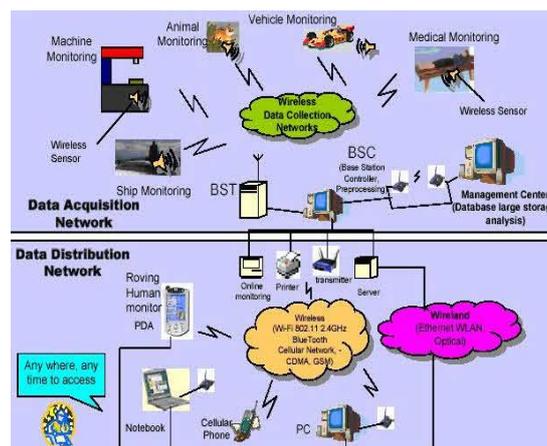


Fig 1. WSN Network

2. WSN Network Topologies

For radio communication networks, the structure of a WSN includes various topologies like the ones given below.

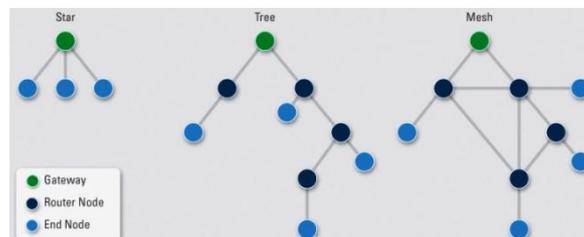


Fig 2. Wireless Sensor Network Topologies

2.1 Star Topologies

Star topology is a communication topology, where each node connects directly to a gateway. A single gateway can send or receive a message to a number of remote nodes. In star topologies, the nodes are not permitted to send messages to each other. This allows low-latency communications between the remote node and the gateway (base station). Due to its dependency on a single node to manage the network, the gateway must be within the radio transmission range of all the individual nodes. The advantage includes the ability to keep the

remote nodes' power consumption to a minimum and simply under control. The size of the network depends on the number of connections made to the hub.

2.2 Tree Topologies

Tree topology is also called as cascaded star topology. In tree topologies, each node connects to a node that is placed higher in the tree, and then to the gateway. The main advantage of the tree topology is that the expansion of a network can be easily possible, and also error detection becomes easy. The disadvantage with this network is that it relies heavily on the bus cable; if it breaks, all the network will collapse.

2.3 Mesh Topologies

The Mesh topologies allow transmission of data from one node to another, which is within its radio transmission range. If a node wants to send a message to another node, which is out of radio communication range, it needs an intermediate node to forward the message to the desired node. The advantage with this mesh topology includes easy isolation and detection of faults in the network. The disadvantage is that the network is large and requires huge investment.

3. Types of WSN

Depending on the environment, the types of networks are decided so that those can be deployed underwater, underground, on land, and so on. Different types of WSNs include:

3.1 Terrestrial WSNs

Terrestrial WSNs are capable of communicating base stations efficiently, and consist of hundreds to thousands of wireless sensor nodes deployed either in unstructured (ad hoc) or structured (Preplanned) manner. In an unstructured mode, the sensor nodes are randomly distributed within the target area that is dropped from a fixed plane. The preplanned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models. In this WSN, the battery power is limited; however, the battery is equipped with solar cells as a secondary power source. The Energy conservation of these WSNs is achieved by using low duty cycle operations, minimizing delays, and optimal routing, and so on

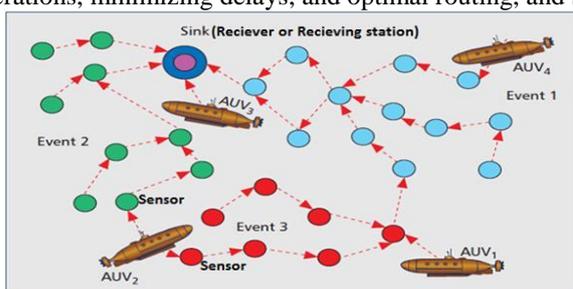


Fig3. Terrestrial WSNs

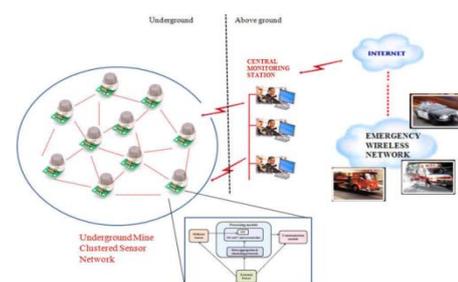


Fig 4. Underground WSNs

3.2 Underground WSNs

The underground wireless sensor networks are more expensive than the terrestrial WSNs in terms of deployment, maintenance, and equipment cost considerations and careful planning. The WSNs networks consist of a number of sensor nodes that are hidden in the ground to monitor underground conditions. To relay information from the sensor nodes to the base station, additional sink nodes are located above the ground. The underground wireless sensor networks deployed into the ground are difficult to recharge. The sensor battery nodes equipped with a limited battery power are difficult to recharge. In addition to this, the underground environment makes wireless communication a challenge due to high level of attenuation and signal loss.

3.3 Under Water WSNs

More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water. Autonomous underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a long propagation delay, and bandwidth and sensor failures. Under water WSNs are equipped with a limited battery that cannot be recharged or replaced. The issue of energy conservation for under water WSNs involves the development of underwater communication and networking techniques.

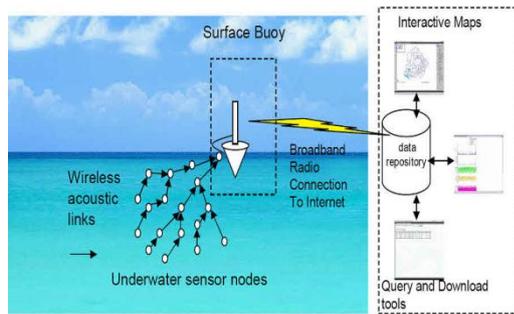


Fig 5. Under Water WSNs

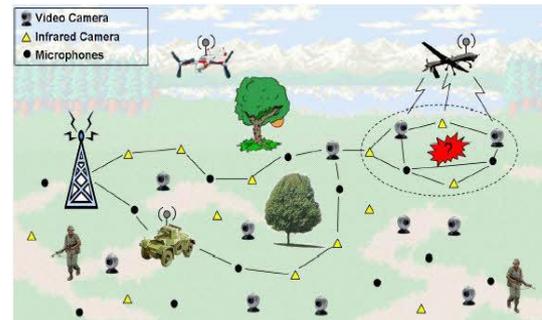


Fig 6. Multimedia WSNs

3.4 Multimedia wireless sensor networks have been proposed to enable tracking and monitoring of events in the form of multimedia, such as imaging, video, and audio. These networks consist of low-cost sensor nodes equipped with microphones and cameras. These nodes are interconnected with each other over a wireless connection for data compression, data retrieval and correlation. The challenges with the multimedia WSN include high energy consumption, high bandwidth requirements, data processing and compressing techniques. In addition to this, multimedia contents require high bandwidth for the contents to be delivered properly and easily.

3.5 Mobile WSNs

These networks consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sense and communicate. The mobile wireless sensor networks are much more versatile than the static sensor networks. The advantages of MWSN over the static wireless sensor networks include better and improved coverage, better energy efficiency, superior channel capacity, and so on.

4. Wireless Sensor Networks Applications

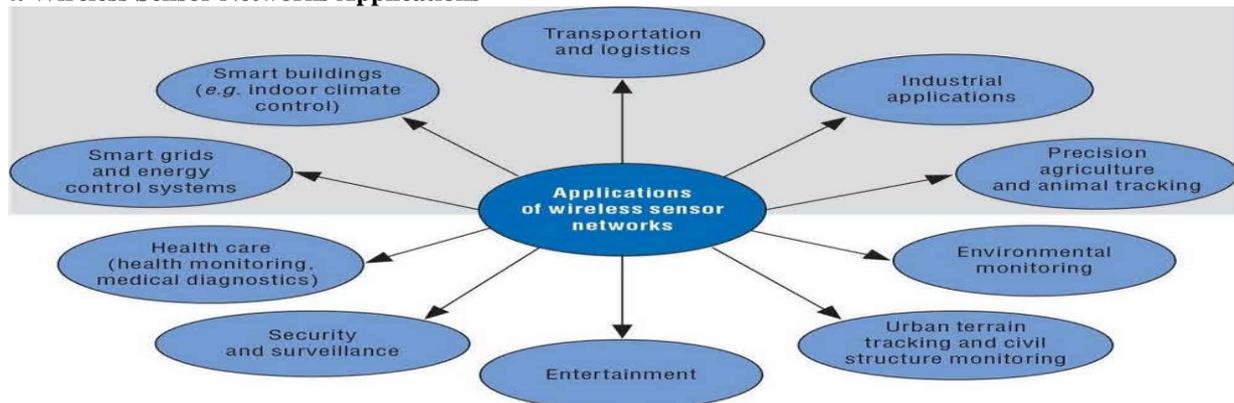


Fig 6. WSN Applications

5. Limitations of Wireless Sensor Networks

1. Possess very little storage capacity – a few hundred kilobytes
2. Possess modest processing power-8MHz
3. Works in short communication range – consumes a lot of power
4. Requires minimal energy – constrains protocols
5. Have batteries with a finite life time
6. Passive devices provide little energy

6. Network Characteristic

As compared to the traditional wireless communication networks such as mobile ad hoc network (MANET) and cellular systems, wireless sensor networks have the following unique characteristics and constraints:

6.1 Dense sensor node deployment: Sensor nodes are usually densely deployed and can be several orders of magnitude higher than that in a MANET.

6.2 Battery-powered sensor nodes: Sensor nodes are usually powered by battery and are deployed in a harsh environment where it is very difficult to change or recharge the batteries.

6.3 Severe energy, computation, and storage constraints: Sensors nodes are having highly limited energy, computation, and storage capabilities.

6.4 Self-configurable: Sensor nodes are usually randomly deployed and autonomously configure themselves into a communication network.

6.5 Unreliable sensor nodes: Since sensor nodes are prone to physical damages or failures due to its deployment in harsh or hostile environment.

6.6 Data redundancy: In most sensor network application, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.

7. Network Design Objectives

7.1 Small node size: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers, reducing node size can facilitate node deployment. It will also reduce the power consumption and cost of sensor nodes.

7.2 Low node cost: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, reducing cost of sensor nodes is important and will result into the cost reduction of whole network.

7.3 Low power consumption: Since sensor nodes are powered by battery and it is often very difficult or even impossible to charge or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.

7.4 Scalability: Since the number sensor nodes in sensor networks are in the order of tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes.

7.5 Reliability: Network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels.

7.6 Self-configurability: In sensor networks, once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

7.7 Adaptability: In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

7.8 Channel utilization: Since sensor networks have limited bandwidth resources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

7.9 Fault tolerance: Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self testing, Self-calibrating, self-repairing, and self-recovering.

Security: A sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.

8. Components of a WSN Node

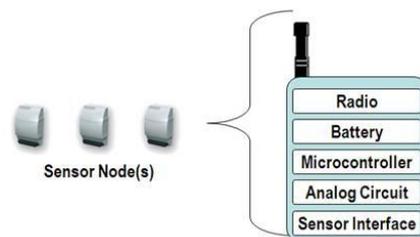


Fig 7. Components of WSN

A WSN node contains several technical components. These include the radio, battery, microcontroller, analog circuit, and sensor interface. When using WSN radio technology, we must make important trade-offs. In battery-powered systems, higher radio data rates and more frequent radio use consume more power. Often three years of battery life is a requirement, so many of the WSN systems today are based on ZigBee due to its low-power consumption. Because battery life and power management technology are constantly evolving and because of the available IEEE 802.11 bandwidth, Wi-Fi is an interesting technology. The second technology consideration for WSN systems is the battery. In addition to long life requirements, we must consider the size and weight of batteries as well as international standards for shipping batteries and battery availability. The low cost and wide availability of carbon zinc and alkaline batteries make them a common choice. To extend battery life, a WSN node periodically wakes up and transmits data by powering on the radio and then powering it back off to conserve energy. WSN radio technology must efficiently transmit a signal and allow the system to go back to sleep with minimal power use. This means the processor involved must also be able to wake power up, and return to sleep mode efficiently. Microprocessor trends for WSNs include reducing power consumption while maintaining or increasing processor speed. Much like your radio choice, the power consumption and processing

speed trade-off is a key concern when selecting a processor for WSNs. This makes the x86 architecture a difficult option for battery-powered devices.

8.1 Sensor Node Hardware Architecture

WSNs are composed of individual embedded systems that are capable of:

1. Interacting with their environment through various sensors
2. Processing information locally
3. Communicating this information wirelessly with their neighbor

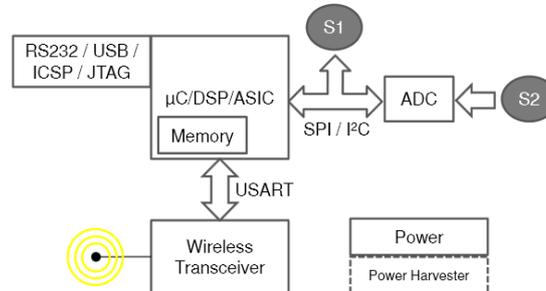


Fig 8. Hardware Architecture for Sensor Node

Commercial platforms typically consist of three components and can be either an individual board or embedded into a single system: Wireless modules or motes are the key components of the sensor network as they possess the communication capabilities and the programmable memory where the application code resides. A mote usually consists of a microcontroller, transceiver, power source, memory unit and may contain few sensors. A sensor board is mounted on the mote and is embedded with multiple types of sensors. Available sensor boards include the S300/400 and MDA100/300 that are used in the Mica family of mote. Alternatively, the sensors can be integrated into the wireless module such as in the Telos or the SunSPOT platform. A programming board, also known as the gateway board, provides multiple interfaces including Ethernet, WiFi, USB, or serial ports for connecting different motes to an enterprise or industrial network or locally to a PC/laptop. These boards are used either to program the motes or gather data from them.

9. WSN Protocol Stack for Wireless Sensor Networks (WSNs)



The protocol stack for WSNs consists of five protocol layers:

1. Physical layer
2. Data link layer
3. Network layer
4. Transport layer
5. Application Layer

9.1 Application Layer: The application layer includes a variety of application – layer protocols that perform various sensor network applications, such as query dissemination, node localization, time synchronization, and network security. For example, the sensor management protocol (SMP) is an application – layer management protocol that provides software operations to perform a variety of tasks, for example, exchanging location – related data, synchronizing sensor nodes, moving sensor nodes, scheduling sensor nodes, and querying the status of sensor nodes.

9.2 Transport Layer: In general, the transport layer is responsible for reliable end – to – end data delivery between sensor nodes and the sink(s). Due to the energy, computation, and storage constraints of sensor nodes, traditional transport protocols cannot be applied directly to sensor networks without modification. For example, the conventional end – to – end retransmission – based error control and the window – based congestion control mechanisms used in the transport control protocol (TCP) cannot be used for sensor networks directly because they are not efficient in resource utilization.

9.3 Network Layer: The network layer is responsible for routing the data sensed by source sensor nodes to the data sink(s). In a sensor network, sensor nodes are deployed in a sensing region to observe a phenomenon of interest. The observed phenomenon or data need to be transmitted to the data sink. In general, a source node can transmit the sensed data to the sink either directly via single – hop long – range wireless communication or via multihop short – range wireless communication. However, long – range wireless communication is costly in terms of both energy consumption and implementation complexity for sensor nodes. In contrast, multihop short

– range communication can not only significantly reduce the energy consumption of sensor nodes, but also effectively reduce the signal propagation and channel fading effects inherent in long – range wireless communication, and is therefore preferred. Since sensor nodes are densely deployed and neighbor nodes are close to each other, it is possible to use multihop short – range communication in sensor networks. In this case, to send the sensed data to the sink, a source node must employ a routing protocol to select an energy- efficient multihop path from the node itself to the sink.

9.4 Data Link Layer : The data link layer is responsible for data stream multiplexing, data frame creation and detection, medium access, and error control in order to provide reliable point – to – point and point – to – multipoint transmissions. One of the most important functions of the data link layer is medium access control (MAC). The primary objective of MAC is to fairly and efficiently share the shared communication resources or medium among multiple sensor nodes in order to achieve good network performance in terms of energy consumption, network throughput, and delivery latency.

9.5 Physical Layer

The physical layer is responsible for converting bit streams from the data link layer to signals that are suitable for transmission over the communication medium. For this purpose, it must deal with various related issues, for example, transmission medium and frequency selection, carrier frequency generation, signal modulation and detection, and data encryption. In addition, it must also deal with the design of the underlying hardware, and various electrical and mechanical interfaces.

10. Major Issue in WSN

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

10.1.1) The hardware design issues are

- 1) Radio Range of nodes should be high (1-5 Kilometers).
- 2) Use of Memory Chips like flash memory is recommended for sensor networks as they are non-volatile, inexpensive and volatile.
- 3) Energy/Power Consumption of the sensing device should be minimized and sensor nodes should be energy efficient since their limited energy resource determines their lifetime.
- 4) Sensor Networks consists of hundreds of thousands of nodes hence the node must be cheap.

10.1.2) an operating system framework for a sensor node should be able to provide memory management and resource management in a constrained environment. The various issues in designing an Operating System (OS) for sensor networks are:

- 1) An OS for sensor nodes should be hardware independent and application specific. It should support multihop routing and simple user level networking abstractions.
- 2) The OS should have inbuilt features to reduce the consumption of battery energy.
- 3) The OS should have an easy Programming paradigm.

10.2) Wireless Radio Communication Characteristics: Performance of wireless sensor networks depends on the Quality of wireless communication. But wireless communication in sensor networks is known for its unpredictable nature. Hence various issues are

- 1) Low power consumption in sensor networks is needed to enable long operating lifetime by facilitating low duty cycle operation, local signal processing.
- 2) Distributed Sensing effectively acts against various environmental obstacles and care should be taken that the signal strength, consequently the effective radio range is not reduced by various factors like reflection, scattering and dispersions.
- 3) Multihop networking may be adapted among sensor nodes to reduce communication link range and also density of sensor nodes should be high.
- 4) Long range communication is typically point to point and requires high transmission power, with the danger of being eavesdropped. So we should consider short range transmission to minimize the possibility of being eavesdropped.
- 5) Communication systems should include error control subsystems to detect errors and to correct them.

10.3) Medium Access Scheme: Communication is a major source of energy consumption in WSNs and MAC protocols directly control the radio of the nodes in the network. MAC protocols should be designed for regulating energy consumption, which in turn influences the lifetime of the network. The various design issues of the MAC protocols suitable for sensor network environment are

- 1) The MAC layer provides fine-grained control of the transceiver and allows on and off switching of the radio. The design of the MAC protocol should have this switching mechanism to decide when and how frequently the on and off mechanism should be done. This helps in conserving energy.
- 2) A MAC protocol should avoid collisions from interfering nodes, overemitting, overhearing, and control packet overhead and idle listening.
- 3) Scalability, Adaptability and decentralization is another important criterion in designing a MAC protocol.



- 4) A MAC protocol should have minimum latency and high throughput when the sensor networks are deployed in critical applications.
- 5) A MAC protocol should include Message Passing.
- 6) There should be uniformity in reporting the events by a MAC protocol.
- 7) The MAC protocols should take care of the well know problem of Information Asymmetry, which arises if a node is not aware of packet transmissions two hops away.
- 8) MAC Protocols should satisfy the Real-time requirements.

10.4) Deployment: Deployment means setting up an operational sensor network in a real world environment. Deployment of sensor network is a labor intensive and cumbersome activity as we do not have influence over the quality of wireless communication and also the real world puts strains on sensor nodes by interfering during communications. Sensor nodes can be deployed either by placing one after another in a sensor field or by dropping it from a plane. Various deployment issues which need to be taken care are

- 1) When sensor nodes are deployed in real world, Node death due to energy depletion either caused by normal battery discharge or due to short circuits is a common problem which may lead to wrong sensor readings. Hence problems affecting sink nodes should be detected to minimize data loss.
- 2) Deployment of sensor networks results in network congestion due to many concurrent transmission attempts Made by several sensor nodes. Another issue is the physical length of a link. Two nodes may be very close to Each other but still they may not be able to communicate due to physical interference in the real world.
- 3) Low data yield is another common problem in real world deployment of sensor nodes. Low data yield means a network delivers insufficient amount of information.
- 4) Self Configuration of sensor networks without human intervention is needed due to random deployment of sensor nodes.

10.5 Localization

Sensor localization is a fundamental and crucial issue for network management and operation. In many of the real world scenarios, the sensors are deployed without knowing their positions in advance and also there is no supporting infrastructure available to locate and manage them once they are deployed. Determining the physical location of the sensors after they have been deployed is known as the problem of localization.

Location discovery or localization algorithm for a sensor

Network should satisfy the following requirements [45]:

- 1) The localization algorithm should be distributed since a centralized approach requires high computation at selective nodes to estimate the position of nodes in the whole environment. This increases signaling bandwidth And also puts extra load on nodes close to center node.
- 2) Knowledge of the node location can be used to implement energy efficient message routing protocols in sensor networks.
- 3) Localization algorithms should be robust enough to localize the failures and loss of nodes. It should be tolerant to error in physical measurements.
- 4) The precision of the localization increases with the number of beacons. A beacon is a node which is aware of its location. But the main problem with increased beacons is that they are more expensive than other sensor nodes and once the unknown stationary nodes have been localized using beacon nodes then the beacons become useless.
- 5) Techniques that depend on measuring the ranging information from signal strength and time of arrival require specialized hardware that is typically not available on sensor nodes.
- 6) Localization algorithm should be accurate, scalable and support mobility of nodes.

10.6. 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.

Various Calibration issues in sensor networks are

- 1) A sensor network consists of large number of sensors typically with no calibration interface.
- 2) Access to individual sensors in the field can be limited.
- 3) Reference values might not be readily available.
- 4) Different applications require different calibration.
- 5) Requires calibration in a complex dynamic environment with many observables like aging, decaying, damage
- 6) Other objectives of calibration include accuracy, resiliency against random errors, ability to be applied in various scenarios and to address a variety of error models. Research includes designing various calibration techniques involving the various issues which we have discussed previously.

10.7 Network Layer Issue

Over the past few years sensor networks are being built for specific applications and routing is important for sending the data from sensor nodes to Base Station (BS).

Various issues at the network layer are

- 1) Energy efficiency is a very important criterion. We need to discover different techniques to eliminate energy inefficiencies that may shorten the lifetime of the network. At the network layer, we need to find various methods for discovering energy efficient routes and for relaying the data from the sensor nodes to the BS so that the lifetime of a network can be optimized.
- 2) Routing Protocols should incorporate multi-path design technique. Multi-path is referred to those protocols which set up multiple paths so that a path among them can be used when the primary path fails.
- 3) Path repair is desired in routing protocols whenever a path break is detected. Fault tolerance is another desirable property for routing protocols. Routing protocols should be able to find a new path at the network layer even if some nodes fail or blocked due to some environmental interference.
- 4) Sensor networks collect information from the physical environment and are highly data centric. In the network layer in order to maximize energy savings we need to provide a flexible platform for performing routing and data management.
- 5) The data traffic that is generated will have significant redundancy among individual sensor nodes since multiple sensors may generate same data within the vicinity of a phenomenon. The routing protocol should exploit such redundancy to improve energy and bandwidth utilization.
- 6) As the nodes are scattered randomly resulting in an ad hoc routing infrastructure, a routing protocol should have the property of multiple wireless hops.
- 7) Routing Protocols should take care of heterogeneous nature of the nodes i.e. each node will be different in terms.

10.8 Security

Security in sensor networks is as much an important factor as performance and low energy consumption in many applications. Security in a sensor network is very challenging as WSN is not only being deployed in battlefield applications but also for surveillance, building monitoring, and burglar alarms and in critical systems such as airports and hospitals. Since sensor networks are still a developing technology, researchers and developers agree that their efforts should be concentrated in developing and integrating security from the initial phases of sensor applications development; by doing so, they hope to provide a stronger and complete protection against illegal activities and maintain stability of the systems at the same time.

Following are the basic security requirements

- 1) Confidentiality is needed to ensure sensitive information is well protected and not revealed to unauthorized third Parties. 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.
- 2) Authentication techniques verify the identity of the participants in a 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.
- 3) Lack of integrity may result in inaccurate information. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function; for e.g., it is unacceptable to have improper information regarding the magnitude of the pollution that has occurred.
- 4) One of the many attacks launched against sensor networks is the message reply attack where an adversary may capture messages exchanged between nodes and reply them later to cause confusion to the network. So sensor network should be designed for freshness; meaning that the packets are not reused thus preventing potential mix-up.
- 6) Security and QoS are two opposite poles in sensor networks. Security mechanisms like encryption should be lightweight so that the overhead is minimized and should not affect the performance of the network.

CONCLUSIONS

A wireless sensor network is a very important wireless network which is used to monitor and control environmental, industrial and health condition. A sensor network is usually designed and deployed for a specific application. The design requirements of a sensor network change with its application. When using WSN radio technology, we must make important trade-offs for battery life and power management. In this paper we took a review on network design characteristic, objective, network protocol layer and various design objective.



REFERENCES

- [1] Swati Sharma and Dr.Pradeep Mittal(2013),International Journal of Advanced Research in Computer Science and Software Engineering, Wireless Sensor Network : Architecture and protocol, pp :303-308
- [2]Aamir Shaikh and Siraj Pathan (2012), International Journal of Information and Education Technology, Vol.2, Research on Wireless Sensor Network Technology, pp. 476-479
- [3] Kiran Maraiya, Kamal Kant, Nitin Guptar (2011), International Journal of Computer Applications Vol.21, Application based Study on Wireless Sensor Network
- [4] Shio Kumar Singh, M P Singh, and D K Singh (2010), Article in International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, India, pp. 63-83
- [5]Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar (2008), Article in Proceedings of the World Congress on Engineering 2008 Vol I, London, U.K pp.
- [6]Shio Kumar Singh, M P Singh , and D K Singh (2010), Article in International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, India, pp. 63-83

