WIRELESS SENSOR NETWORK

Hitesh Kumar*

Chesta Verma*

Pankaj Kumar*

Abstract: *Wireless Sensor Networks (WSN) are an emerging and very interesting technology applied to different applications. They are formed by small, self organized devices that cooperate to form a large scale network with thousands of nodes covering a large area. The independent operation of the devices and the self-organization feature of the network present some challenges related to security, particularly regarding the security of the processed and routed data over the network.*

Keywords: *WSN, ADC, GPS, ISM, CCR, WINS*

***Student (B. Tech. 5th Sem), Electronics and Communication Engineering Dronacharya College of Engineering, Gurgaon, India**

1. INTRODUCTION:

A wireless sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

Some of the application areas are health, military, and security. For example, the physiological data about a patient can be monitored remotely by a doctor. While this is more convenient for the patient, it also allows the doctor to better understand the patient's current condition. Sensor networks can also be used to detect foreign chemical agents in the air and the water. They can help to identify the type, concentration, and location of pollutants. In essence, sensor networks will provide the end user with intelligence and a better understanding of the environment. We envision that, in future, wireless sensor networks will be an integral part of our lives, more so than the present-day personal computers.

Realization of these and other sensor network applications require wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad hoc networks are outlined below:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.

- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

Since large numbers of sensor nodes are densely deployed, neighbor nodes may be very close to each other. Hence, multi hop communication in sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the transmission power levels can be kept low, which is highly desired in covert operations. Multi hop communication can also effectively overcome some of the signal propagation effects experienced in long-distance wireless communication.

One of the most important constraints on sensor nodes is the low power consumption requirement. Sensor nodes carry limited, generally irreplaceable, power sources. Therefore, while traditional networks aim to achieve high quality of service (QoS) provisions, sensor network protocols must focus primarily on power conservation. They must have inbuilt trade-off mechanisms that give the end user the option of prolonging network lifetime at the cost of lower throughput or higher transmission delay.

2. WIRELESS SENSOR NETWORK:

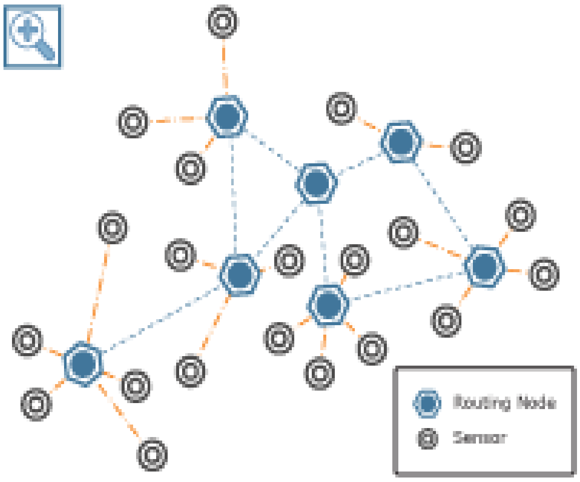

Figure 1:-wireless sensor network

Wireless sensor networks consist of clusters of devices using sensor technologies deployed in a specific area. They communicate data wirelessly to a central system. Sensor networks continuously monitor the physical, chemical processes or magnetic properties, using the existing communications infrastructure.

A software layer for processing and data management allows building industrial, government or military applications.

Wireless sensor networks based on emerging technologies such as wireless communication technologies, information technology, semiconductors, MEMS, microsystems technology and embedded micro-sensors.

Wireless sensor networks have the potential to revolutionize telecommunications in a way similar to what we call the Internet of things by offering a wide range of different applications some of which remain to be discovered. Sensor networks have a huge potential for applications in various fields, including:

- Environment and health: ocean temperature, collecting information on patients' conditions
- Management of critical industrial areas: monitoring of oil containers, checking the concentration of chemicals and gases
- Warehouse management and supply chain monitoring and historical states of the goods with the conditions of critical conservation
- Military applications: surveillance and recognition

A wireless sensor network consists of many tiny sensor nodes, each equipped with a radio transceiver, a microprocessor and a number of sensors. These nodes are capable of independently forming a network through which sensor readings can be propagated. Each node has an autonomous processing capacity, data can be processed as they pass through the network.

Given the limitations of the equipment and the physical environment and levels of high demands with which the nodes must operate, algorithms and protocols must be designed to provide strong and efficient energy consumption. The design of the physical layer and communication technologies and the information coding still represent significant challenges for this new technology

3. WSN SYSTEM ARCHITECTURE:

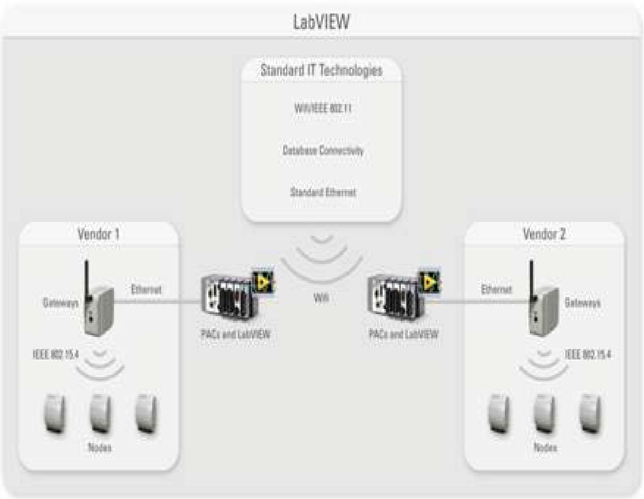

Figure 2. WSN System Architecture Combines Wired and Wireless

Wireless technology offers several advantages for those who can build wired and wireless systems and take advantage of the best technology for the application. To do this, you need flexible software architecture like the NI Lab VIEW graphical system design platform. Lab VIEW offers the flexibility needed to connect a wide range of wired and wireless devices (see Figure 2).

4. WSN NETWORK TOPOLOGIES:

WSN nodes are typically organized in one of three types of network topologies. In a star topology, each node connects directly to a gateway. In a cluster tree network, each node connects to a node higher in the tree and then to the gateway, and data is routed from the lowest node on the tree to the gateway. Finally, to offer increased reliability, mesh networks feature nodes that can connect to multiple nodes in the system and pass data through the most reliable path available. This mesh link is often referred to as a router (see Figure 3).

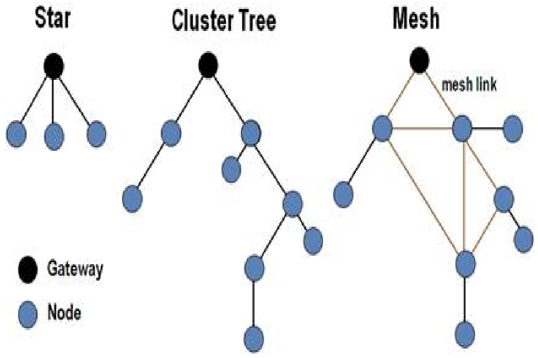

Figure 3. Common WSN Network Topologies

5. COMPONENTS OF A WSN NODE:

A WSN node contains several technical components. These include the radio, battery, microcontroller, analog circuit, and sensor interface. When using WSN radio technology, you 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, you 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 minimum 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.

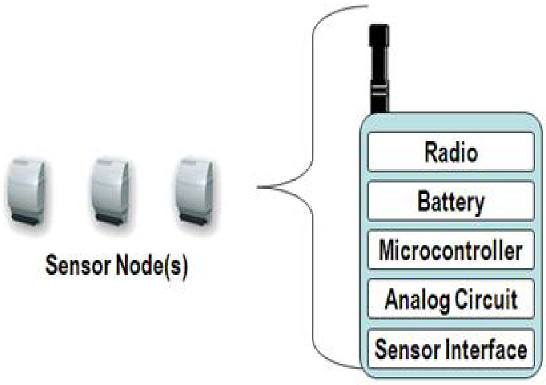

Figure 4. WSN Sensor Node Components

6. DELIVERING LAB VIEW CONNECTIVITY FOR WSN SYSTEMS:

Lab VIEW as a platform offers a broad range of connectivity options including Lab VIEW drivers for WSN. These drivers are available for WSN systems from Crossbow, Accsense, and Accutech, and drivers are currently being developed for Banner, MeshNetics, and Techkor WSN systems.

7. WHY USE SIMULATION IN WSNS:

Nowadays, the WSN is a hot research topic. Many network details in WSNs are not finalized and standardized. Building a WSNs test bed is very costly. Running real experiments on a test bed is costly and difficulty. Besides, repeatability is largely compromised since many factors affect the experimental results at the same time. It is hard to isolate a single aspect. Moreover, running real experiments are always time consuming. Therefore, WSNs simulation is important for WSNs development. Protocols, schemes, even new ideas can be evaluated in a very large scale. WSNs simulators allow users to isolate different factors by tuning configurable parameters.

Consequently, simulation is essential to study WSNs, being the common way to test new applications and protocols in the field. This leads to the recent boom of simulator development.

However, obtaining solid conclusions from a simulation study is not a trivial task. There are two key aspects in WSNs simulators: (1) The correctness of the simulation models and (2) the suitability of a particular tool to implement the model. A “correct” model based on solid assumption is mandatory to derive trustful results. The fundamental tradeoff is: precision and necessity of details versus performance and scalability. In the rest of this survey, several main-stream WSNs simulators are described and compared in more detail.

8. FACTORS INFLUENCING SENSOR NETWORK DESIGN:

A sensor network design is influenced by many factors, which include fault tolerance; scalability; production costs; operating environment; sensor network topology; hardware constraints; transmission media; and power consumption. These factors are addressed by many researchers as surveyed in this paper. However, none of these studies has a full integrated view of all factors that are driving the design of sensor networks and sensor nodes. These factors are important because they serve as a guideline to design a protocol or an algorithm for sensor networks. In addition, these influencing factors can be used to compare different schemes.

8.1. Fault tolerance

Some sensor nodes may fail or be blocked due to lack of power, have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures The reliability $Rk(t)$ or fault tolerance of a sensor node is modelled using the Poisson distribution to capture the probability of not having a failure within the time interval $(0,t)$: equation(1)

$$R_k(t) = \exp(-\lambda_k t)$$

where λk and t are the failure rate of sensor node k and the time period, respectively.

Note that protocols and algorithms may be designed to address the level of fault tolerance required by the sensor networks. If the environment where the sensor nodes are deployed has little interference, then the protocols can be more relaxed. For example, if sensor nodes are being deployed in a house to keep track of humidity and temperature levels, the fault tolerance requirement may be low since this kind of sensor networks is not easily damaged or interfered by environmental noise. On the other hand, if sensor nodes are being deployed in a battlefield for surveillance and detection, then the fault tolerance has to be high because the sensed data are critical and sensor nodes can be destroyed by hostile actions. As a result, the fault tolerance level depends on the application of the sensor networks, and the schemes must be developed with this in mind.

8.2. Scalability

The number of sensor nodes deployed in studying a phenomenon may be in the order of hundreds or thousands. Depending on the application, the number may reach an extreme value of millions. The new schemes must be able to work with this number of nodes. They must also utilize the high density nature of the sensor networks. The density can range from few sensor nodes to few hundred sensor nodes in a region, which can be less than 10 m in diameter The density can be calculated according as equation(2)

$$\mu(R) = (N \pi R^2)/A$$

where N is the number of scattered sensor nodes in region A; and R, the radio transmission range. Basically, $\mu(R)$ gives the number of nodes within the transmission radius of each node in region A.

In addition, the number of nodes in a region can be used to indicate the node density. The node density depends on the application in which the sensor nodes are deployed. For machine diagnosis application, the node density is around 300 sensor nodes in a 5×5 m^2 region, and the density for the vehicle tracking application is around 10 sensor nodes per region. In general, the density can be as high as 20 sensor nodes/m^3. A home may contain around two dozens of home appliances containing sensor nodes but this number will grow if sensor nodes are embedded into furniture and other miscellaneous items. For habitat monitoring application, the number of sensor nodes ranges from 25 to 100 per region. The density will be extremely high when a person normally containing hundreds of sensor nodes, which are embedded in eye glasses, clothing, shoes, watch, jewelry, and human body, is sitting inside a stadium watching a basketball, football, or baseball game.

8.3. Production costs

Since the sensor networks consist of a large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the networks. If the cost of the network is more expensive than deploying traditional sensors, then the sensor network is not cost-justified. As a result, the cost of each sensor node has to be kept low. The state-of-the-art technology allows a Bluetooth radio system to be less than 10$. Also, the price of a Pico Node is targeted to be less than 1$. The cost of a sensor node should be much less than 1$ in order for the sensor network to be feasible. The cost of a Bluetooth radio, which is known to be a low-cost device, is even 10 times more expensive than the targeted price for a sensor node. Note that a sensor node also has some additional units such as sensing and processing units as described in Section 8.4. In addition, it may be equipped with a location finding system, mobilizer, or power generator depending on the applications of the sensor networks. As a result, the cost of a sensor node is a very challenging issue given the amount of functionalities with a price of much less than a dollar.

8.4. Hardware constraints

A sensor node is made up of four basic components as shown in Figure. 5: a *sensing unit*, a *processing unit*, a*transceiver unit* and a *power unit*. They may also have application dependent additional components such as a *location finding system*, a *power generator* and a *mobilizer*. Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units may be supported by a power scavenging unit such as solar cells. There are also other subunits, which are application dependent. Most of the sensor network routing techniques and sensing tasks require the knowledge of location with high accuracy. Thus, it is common that a sensor node has a location finding system. A mobilizer may sometimes be needed to move sensor nodes when it is required to carry out the assigned tasks.

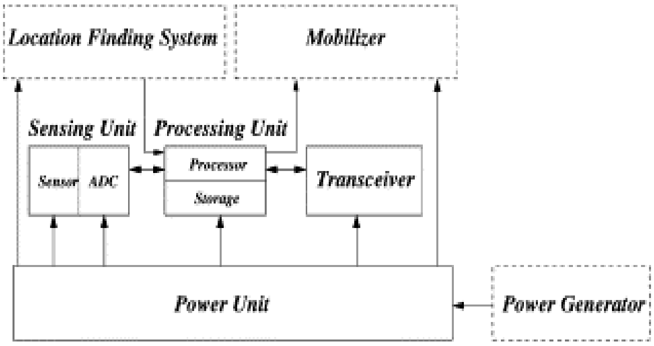

Figure. 5. The components of a sensor node.

All of these subunits may need to fit into a matchbox-sized module. The required size may be smaller than even a cubic centimeter which is light enough to remain suspended in the air. Apart from the size, there are also some other stringent constraints for sensor nodes. These nodes must

- consume extremely low power,
- operate in high volumetric densities,
- have low production cost and be dispensable,
- be autonomous and operate unattended,
- be adaptive to the environment.

Since the sensor nodes are often inaccessible, the lifetime of a sensor network depends on the lifetime of the power resources of the nodes. Power is also a scarce resource due to the size limitations. For instance, the total stored energy in a *smart dust mote* is on the order of 1 J. For wireless integrated network sensors (WINS), the total average system supply currents must be less than 30 μA to provide long operating life. WINS nodes are powered from typical lithium (Li) coin cells (2.5 cm in diameter and 1 cm in thickness). It is possible to extend the lifetime of the sensor networks by energy scavenging, which means extracting energy from the environment. Solar cells is an example for the techniques used for energy scavenging.

The transceiver unit of sensor nodes may be a passive or active optical device as in smart dust motes or a radio frequency (RF) device. RF communications require modulation, band pass, filtering, demodulation and multiplexing circuitry, which make them more complex and expensive. Also, the path loss of the transmitted signal between two sensor nodes may be as high as the fourth order exponent of the distance between them, because the antennas of the sensor nodes are close to the ground. Nevertheless, RF communication is preferred in most of the ongoing sensor network research projects, because the packets conveyed in sensor networks are small, data rates are low (i.e., generally less than 1 Hz) , and the frequency re-use is high due to short communication distances. These characteristics also make it possible to use low duty cycle radio electronics for sensor networks. However, designing energy efficient and low duty cycle radio circuits is still technically challenging, and current commercial radio technologies such as those used in Bluetooth is not efficient enough for sensor networks because turning them on and off consumes much energy.

Though the higher computational powers are being made available in smaller and smaller processors, processing and memory units of sensor nodes are still scarce resources. For instance, the processing unit of a smart dust mote prototype is a 4 MHz Atmel AVR 8535 micro-controller with 8 KB instruction flash memory, 512 bytes RAM and 512 bytes EEPROM. TinyOS operating system is used on this processor, which has 3500 bytes OS code space and 4500 bytes available code space. The processing unit of another sensor node prototype, namely μAMPS wireless sensor node, has a 59–206 MHz SA-1110 micro-processor. A multithreaded μ-OS operating system is run on μAMPS wireless sensor nodes.

Most of the sensing tasks require the knowledge of position. Since sensor nodes are generally deployed randomly and run unattended, they need to corporate with a location finding system. Location finding systems are also required by many of the proposed sensor network routing protocols. It is often assumed that each sensor node will have a global positioning system (GPS) unit that has at least 5 m accuracy. It is argued that equipping all sensor nodes with a GPS is not viable for sensor networks. An alternative approach where a limited number of nodes use GPS and help the other nodes to find out their locations terrestrially

8.5. Sensor network topology

Sheer numbers of inaccessible and unattended sensor nodes, which are prone to frequent failures, make topology maintenance a challenging task. Hundreds to several thousands of nodes are deployed throughout the sensor field. They are deployed within tens of feet of each other. The node densities may be as high as 20 nodes/m^3. Deploying high number of nodes densely requires careful handling of topology maintenance. We examine issues related to topology maintenance and change in three phases:

8.5.1. Pre-deployment and deployment phase

Sensor nodes can be either thrown in mass or placed one by one in the sensor field. They can be deployed by

- dropping from a plane,
- delivering in an artillery shell, rocket or missile,
- throwing by a catapult (from a ship board, etc.),
- placing in factory, and
- placing one by one either by a human or a robot.

Although the sheer number of sensors and their unattended deployment usually preclude placing them according to a carefully engineered deployment plan, the schemes for initial deployment must

- reduce the installation cost,
- eliminate the need for any pre-organization and pre-planning,
- increase the flexibility of arrangement, and
- promote self-organization and fault tolerance.

8.5.2. Post-deployment phase

After deployment, topology changes are due to change in sensor nodes

- position,

- reachability (due to jamming, noise, moving obstacles, etc.),
- available energy,
- malfunctioning, and
- task details.

Sensor nodes may be statically deployed. However, device failure is a regular or common event due to energy depletion or destruction. It is also possible to have sensor networks with highly mobile nodes. Besides, sensor nodes and the network experience varying task dynamics, and they may be a target for deliberate jamming. Therefore, sensor network topologies are prone to frequent changes after deployment.

8.5.3. Re-deployment of additional nodes phase

Additional sensor nodes can be re-deployed at any time to replace the malfunctioning nodes or due to changes in task dynamics. Addition of new nodes poses a need to re-organize the network. Coping with frequent topology changes in an ad hoc network that has myriads of nodes and very stringent power consumption constraints requires special routing protocols.

8.6. Environment

Sensor nodes are densely deployed either very close or directly inside the phenomenon to be observed. Therefore, they usually work unattended in remote geographic areas. They may be working

- in busy intersections,
- in the interior of a large machinery,
- at the bottom of an ocean,
- inside a twister,
- on the surface of an ocean during a tornado,
- in a biologically or chemically contaminated field,
- in a battlefield beyond the enemy lines,
- in a home or a large building,
- in a large warehouse,
- attached to animals,
- attached to fast moving vehicles, and
- in a drain or river moving with current.

This list gives us an idea about under which conditions sensor nodes are expected to work. They work under high pressure in the bottom of an ocean, in harsh environments such as a debris or a battlefield, under extreme heat and cold such as in the nozzle of an aircraft engine or in arctic regions, and in an extremely noisy environment such as under intentional jamming.

8.7. Transmission media

In a multihop sensor network, communicating nodes are linked by a wireless medium. These links can be formed by radio, infrared or optical media. To enable global operation of these networks, the chosen transmission medium must be available worldwide.

One option for radio links is the use of industrial, scientific and medical (ISM) bands, which offer license-free communication in most countries. The International Table of Frequency Allocations, contained in Article S5 of the Radio Regulations (Volume 1), species some frequency bands that may be made available for ISM applications. They are listed in Table 1.

Table 1. Frequency bands available for ISM applications

Frequency band	Center frequency
6765–6795 kHz	6780 kHz
13,553–13,567 kHz	13,560 kHz
26,957–27,283 kHz	27,120 kHz
40.66–40.70 MHz	40.68 MHz
433.05–434.79 MHz	433.92 MHz
902–928 MHz	915 MHz
2400–2500 MHz	2450 MHz
5725–5875 MHz	5800 MHz
24–24.25 GHz	24.125 GHz
61–61.5 GHz	61.25 GHz
122–123 GHz	122.5 GHz
244–246 GHz	245 GHz

Some of these frequency bands are already being used for communication in cordless phone systems and wireless local area networks (WLANs). For sensor networks, a small-sized, low-cost, ultralow power transceiver is required. A certain hardware constraints and the trade-off between antenna efficiency and power consumption limit the choice of a carrier frequency for such transceivers to the ultrahigh frequency range. They also propose the use of the 433 MHz ISM band in Europe and the 915 MHz ISM band in North America. The transceiver design issues in these two bands. The main advantages of using the ISM bands are the free radio, huge spectrum allocation and global availability. They are not bound to a particular standard, thereby giving more freedom for the implementation of power saving strategies in sensor networks. On the other hand, there are various rules and constraints, like power limitations and harmful interference from existing applications. These frequency bands are also referred to as unregulated frequencies.

Much of the current hardware for sensor nodes is based upon RF circuit design. The µAMPS wireless sensor node, uses a Bluetooth-compatible 2.4 GHz transceiver with an integrated frequency synthesizer. The low-power sensor device uses a single channel RF transceiver operating at 916 MHz. The WINS architecture also uses radio links for communication.

Another possible mode of internode communication in sensor networks is by infrared. Infrared communication is license-free and robust to interference from electrical devices. Infrared based transceivers are cheaper and easier to build. Many of today's laptops, PDAs and mobile phones offer an infrared data association interface. The main drawback though, is the requirement of a line of sight between sender and receiver. This makes infrared a reluctant choice for transmission medium in the sensor network scenario.

An interesting development is that of the smart dust mote , which is an autonomous sensing, computing and communication system that uses optical medium for transmission. In the former, the mote does not require an onboard light source. A configuration of three mirrors (CCR) is used to communicate a digital high or low. The latter uses an onboard laser diode and an active-steered laser communication system to send a tightly collimated light beam toward the intended receiver.

The unusual application requirements of sensor networks make the choice of transmission media more challenging. For instance, marine applications may require the use of the aqueous transmission medium. Here, one would like to use long-wavelength radiation that can penetrate the water surface. Inhospitable terrain or battlefield applications might encounter error prone channels and greater interference. Moreover, a sensor antenna might not have the height and radiation power of those in other wireless devices. Hence, the choice of transmission medium must be supported by robust coding and modulation schemes that efficiently model these vastly different channel characteristics.

8.8. Power consumption

The wireless sensor node, being a micro-electronic device, can only be equipped with a limited power source (<0.5 Ah, 1.2 V). In some application scenarios, replenishment of power resources might be impossible. Sensor node lifetime, therefore, shows a strong dependence on battery lifetime. In a multihop ad hoc sensor network, each node plays the dual role of data originator and data router. The disfunctioning of few nodes can cause significant topological changes and might require re-routing of packets and re-organization of the network. Hence, power conservation and power management take on additional importance. It is for these reasons that researchers are currently focusing on the design of power-aware protocols and algorithms for sensor networks.

In other mobile and ad hoc networks, power consumption has been an important design factor, but not the primary consideration, simply because power resources can be replaced by the user. The emphasis is more on QoS provisioning than the power efficiency. In sensor networks though, power efficiency is an important performance metric, directly influencing the network lifetime. Application specific protocols can be designed by appropriately trading off other performance metrics such as delay and throughput with power efficiency.

The main task of a sensor node in a sensor field is to detect events, perform quick local data processing, and then transmit the data. Power consumption can hence be divided into three domains: *sensing*,*communication*, and *data processing*.

The sensing unit and its components were introduced in Section 8.4. Sensing power varies with the nature of applications. Sporadic sensing might consume lesser power than constant event monitoring. The complexity of event detection also plays a crucial role in determining energy expenditure. Higher ambient noise levels might cause significant corruption and increase detection complexity. Power consumption in data communication and processing are discussed in detail in the following subsections.

8.8.1. Communication

Of the three domains, a sensor node expends maximum energy in data communication. This involves both data transmission and reception. It can be shown that for short-range communication with low radiation power (~0 dbm), transmission and reception energy costs are nearly the same. Mixers, frequency synthesizers, voltage control oscillators, phase locked loops (PLL) and power amplifiers, all consume valuable power in the transceiver circuitry. It is important that in this computation we not only consider the active power but also the start-up power consumption in the transceiver circuitry. The start-up time, being of the order of hundreds of micro-seconds, makes the start-up power non-negligible. This high value for the start-up time can be attributed to the lock time of the PLL. As the transmission packet size is reduced, the start-up power consumption starts to dominate the active power consumption. As a result, it is inefficient in turning the transceiver ON and OFF, because a large amount of power is spent in turning the transceiver back ON each time. The authors present a formulation for the radio power consumption (P_c) as equation(3)

$$P_c = N_T[P_T(T_{on} + T_{st}) + P_{out}(T_{on})] + N_R[P_R(R_{on} + R_{st})]$$

where $P_{T/R}$ is the power consumed by the transmitter/receiver; P_{out}, the output power of the transmitter;T/R_{on}, the transmitter/receiver on time; T/R_{st}, the transmitter/receiver start-up time and $N_{T/R}$, the number of times transmitter/receiver is switched on per unit time, which depends on the task and medium access control (MAC) scheme used. T_{on} can further be rewritten as L/R, where L is the packet size and R, the data rate. Today's state-of-the-art low power radio transceiver has typical P_T and P_R values around 20 dbm and P_{out} close to 0 dbm. Note that PicoRadio aims at a P_c value of −20 dbm.

A direct-conversion architecture is proposed for the transceiver circuitry. Based on their results, the authors present a power budget and estimate the power consumption to be at least an order of magnitude less than the values given above for P_T and P_R values.

8.8.2. Data processing

Energy expenditure in data processing is much less compared to data communication. Assuming Rayleigh fading and fourth power distance loss, the energy cost of transmitting 1 KB a distance of 100 m is approximately the same as that for executing 3 million instructions by a 100 million instructions per second (MIPS)/W processor. Hence, local data processing is crucial in minimizing power consumption in a multihop sensor network.

A sensor node must therefore have built-in computational abilities and be capable of interacting with its surroundings. Further limitations of cost and size lead us to the choice of complementary metal oxide semiconductor (CMOS) technology for the micro-processor. Unfortunately, this has inbuilt limitations on energy efficiency. A CMOS transistor pair draws power every time it is switched. This switching power is proportional to the switching frequency, device capacitance (which further depends on the area) and square of the voltage swing. Reducing the supply voltage is hence an effective means of lowering power consumption in the active state. Dynamic voltage scaling, aims to adapt processor power supply and operating frequency to match workloads. When a micro-processor handles time-varying computational load, simply reducing the operating frequency during periods of reduced activity results in a linear decrease in power consumption, but reducing the operating voltage gives us quadratic gains. On the other hand, this compromises on peak performance of the processor. Significant energy gains can be obtained by recognizing that peak performance is not always desired and therefore, the processor's operating voltage and frequency can be dynamically adapted to instantaneous processing requirements. the authors propose a workload prediction scheme based on adaptive filtering of the past workload profile and analyze several filtering schemes. The power consumption in data processing (P_p) can be formulated as follows:

equation(4) $$P_{\mathrm{p}} = CV_{\mathrm{dd}}^{2}f + V_{\mathrm{dd}}I_{0}\mathrm{e}^{V_{\mathrm{dd}}\,/\,n'V_{\mathrm{T}}}$$

where C is the total switching capacitance; V_{dd}, the voltage swing and f, the switching frequency. The second term indicates the power loss due to leakage currents The lowering of threshold voltage to satisfy performance requirements results in high sub threshold leakage currents. Coupled with the low duty cycle operation of the micro-processor in a sensor node, the associated power loss becomes significant

It is to be noted that there may be some additional circuitry for data encoding and decoding. Application specific integrated circuits may also be used in some cases. In all these scenarios, the design of sensor network algorithms and protocols are influenced by the corresponding power expenditures, in addition to those that have been discussed.

9. APPLICATIONS:

Area monitoring

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors detects enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.

Environmental/Earth monitoring

The term Environmental Sensor Networks has evolved to cover many applications of WSNs to earth science research.This includes sensing volcanoes, oceans,glaciers,forests, etc. Some of the major areas are listed below.

Air quality monitoring

The degree of pollution in the air has to be measured frequently in order to safeguard people and the environment from any kind of damages due to air pollution. In dangerous surroundings, real time monitoring of harmful gases is an important process because the weather can change rapidly changing key quality parameters.

- **Interior monitoring**

Observing the gas levels at vulnerable areas needs the usage of high-end, sophisticated equipment, capable to satisfy industrial regulations. Wireless internal monitoring solutions facilitate keep tabs on large areas as well as ensure the precise gas concentration degree.

- **Exterior monitoring**

External air quality monitoring needs the use of precise wireless sensors, rain & wind resistant solutions as well as energy reaping methods to assure extensive liberty to machine that will likely have tough access.

Air pollution monitoring

Wireless sensor networks have been deployed in several cities (Stockholm, London and Brisbane) to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas. There are various architectures that can be used for such applications as well as different kinds of data analysis and data mining that can be conducted.

Forest fire detection

A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.

Landslide detection

A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. Through the data gathered it may be possible to know the occurrence of landslides long before it actually happens

Water quality monitoring

Water quality monitoring involves analyzing water properties in dams, rivers, lakes & oceans, as well as underground water reserves The use of many wireless distributed sensors enables the creation of a more accurate map of the water status, and allows the permanent deployment of monitoring stations in locations of difficult access, without the need of manual data retrieval.

Natural disaster prevention

Wireless sensor networks can effectively act to prevent the consequences of natural disasters, like floods. Wireless nodes have successfully been deployed in rivers where changes of the water levels have to be monitored in real time.

Industrial sense and control applications

In recent research a vast number of wireless sensor network communication protocols have been developed. While previous research was primarily focused on power awareness, more recent research have begun to consider a wider range of aspects, such as wireless link reliability, real-time capabilities, or quality-of-service. These new aspects are considered as an enabler for future applications in industrial and related wireless sense and control applications, and partially replacing or enhancing conventional wire-based networks by WSN techniques.

10. CONCLUSION:

The flexibility, fault tolerance, high sensing fidelity, low-cost and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required.

REFERENCES:-

[1]. http://www.eetimes.com/document.asp?doc_id=1278992

[2].http://www.cse.wustl.edu/~jain/cse567-11/ftp/sensor/index.html

[3]. http://www.purelink.ca/en/technologies/related-technologies.php

[4]. http://www.ni.com/white-paper/7142/en/#toc3

[5]. http://www.sciencedirect.com/science/article/pii/S1389128601003024

[6]. http://en.wikipedia.org/wiki/Wireless_sensor_network