Application based Study on Wireless Sensor Network

Kiran Maraiya
Department of Computer
Science and Engineering
National Institute of
Technology Hamirpur,
Hamirpur (H.P.) INDIA

Kamal Kant
Department of Computer
Science and Engineering
ASET, Amity University,
Noida (U.P), India

Nitin Gupta
Department of Computer
Science and Engineering
National Institute of
Technology Hamirpur,
Hamirpur (H.P.) INDIA

ABSTRACT

A wireless sensor network is type of wireless network. Basically it consist a collection of tiny device are called sensor node, sensor node has a resource constraint means battery power, storage and communication capability. These sensor nodes are set with radio interface with which they communicated with one another to form a network. Wireless sensor network has very necessary application like remote has remote environmental monitoring and target tracking. The goal of our survey is to present a comprehensive review of the recent literature on various aspects of WSNs.And also discuss how wireless sensor network works and advantages and disadvantages over the traditional network

Keywords

Sensor network, layers, application, traditional network

1. INTRODUCTION

This wireless sensor networks is depends on a simple equation: Sensing + CPU + Radio = Thousands of possible applications. A wireless sensor network is type of wireless network. It is small and infrastructure less .basically wireless sensor network consist a number of sensor node, called tiny device and these are working together to detect a region to take data about the environment. Wireless sensor network has two types: structured and unstructured. if we talk about unstructured so is a collection of sensor nodes. And these deployed in adhoc manner into a region. Once deployed, the network is absent unattended perform monitoring and reporting functions. In other structured wireless sensor network, the all sensor nodes are deployed in pre designed manner. The benefit of structure wireless sensor network is that some nodes can be deployed with lower network maintenance and management cost. Fewer nodes can be deployed now since nodes are placed at specific locations to provide coverage while ad hoc deployment can have uncovered regions. Wireless sensor network aim is to provide efficient connection among the physical environmental condition and internet worlds. The sensor nodes of the wireless sensor network is allows random deployment in inaccessible terrains, this means protocol of the wireless sensor is self organized, another important feature of the wireless sensor network is cooperative effort of the sensor nodes. Sensor nodes are collecting data about environment, after collecting it they process it and then transmit to the base station. Base station provides a interface between user and internet. Basic characteristic of the wireless sensor network are limited energy, dynamic network topology, lower power, node failure and mobility of the nodes, short-range broadcast communication and multi-hop routing and large scale of deployment. In the wireless sensor network architecture includes both a hardware platform and an operating system designed. TinyOS is a component based operating system designed to run in resource constrained wireless devices. It provides highly well-organized communication primitives and fine grained concurrency mechanisms to application and protocol developers. Basically TinyOS is the use of event based programming in conjunction with a highly efficient component model. TinyOS enables system-wide optimization by providing a tight coupling among hardware and software. TinyOS has been designed to run on a generalized architecture where a single CPU is shared between application and protocol processing. Figure 1 show the basic architecture of the wireless sensor network in which sensor node deployed in the sensor fields and they communicate with each other for collect the information from the environment, or directly send to the base station basically base station act as a gateway. With the help of gateway data is transmitting to the internet. Because user is directly connect to the internet.
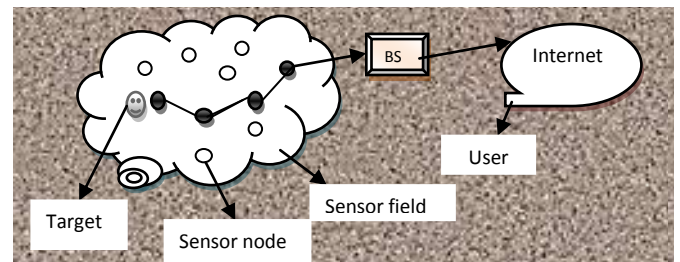

Figure 1 Architecture of the Wireless Sensor network

2. TYPES OF SENSOR NETWORKS

Wireless sensor networks are deployed on land ,underground, and underwater. A sensor network faces different challenges and constraints according to the environment in the sensor network deployed. There are five types of the wireless sensor network as discussed by Jennifer et at.[4].
1. Terrestrial Wireless sensor network.

2. Underground Wireless sensor network.
3. Underwater Wireless sensor network.
4. Multi-media Wireless sensor network.
5. Mobile Wireless sensor network.

Terrestrial WSNs [1] typically consist of hundreds to thousands of inexpensive sensor nodes deployed in a given region, either in

an ad hoc or in a pre-planned manner. In ad hoc deployment, sensor nodes can be dropped from a plane and randomly placed into the target area. In pre-planned deployment, there is grid placement, optimal placement, 2-d and 3-d placement models. In a terrestrial WSN, reliable communication in a dense environment is very essential. Sensor nodes must be able to successfully communicate with the base station in terrestrial WSN, while battery power is a limited. In any case, it is essential for sensor nodes to conserve energy. Energy of sensor nodes can be conserved with multi-hop optimal routing, short transmission range, in-network data aggregation, reducing data redundancy, minimizing delay and using low duty-cycle operations in terrestrial WSN.Underground WSNs in which sensor node covered underground, basically it used for detect used to monitor underground situation. And sink node are used for transmit information to the sensor node to the base station. This wireless senor network is more costly as compare to terrestrial WSN in terms of equipment, deployment, and maintenance. Underground sensor nodes are expensive because proper components must be used for reliable communication through soil, rocks, water, and other mineral contents. The underground environment makes wireless communication a challenge due to signal losses and high levels of attenuation. An underground WSN requires careful planning energy and cost considerations during deployment to increase network lifetime. Underwater WSNs consist of a number of sensor nodes and vehicles deployed underwater. Unlike terrestrial WSNs, underwater sensor nodes are more costly and less dense. independent underwater vehicles are used for searching or gathering data from sensor nodes. Sensor nodes communicate via acoustic waves in underwater WSN. Acoustic communication is a challenge in underwater due to limited bandwidth, long propagation delay, and signal fading problem. Underwater WSNs consist of a number of sensor nodes and vehicles deployed underwater. Unlike terrestrial WSNs, underwater sensor nodes are more costly and less dense. independent underwater vehicles are used for searching or gathering data from sensor nodes. Sensor nodes communicate via acoustic waves in underwater WSN. Acoustic communication is a challenge in underwater due to limited bandwidth, long propagation delay, and signals fading problem. And also node failure. Sensor node in wireless sensor network has a capability to take a harsh ocean environment condition. Sensor node have limited battery power which cannot be recharges and replace. For energy conservation, underwater WSNs involve developing efficient underwater communication and networking techniques. Multi-media WSNs are used to monitoring and tracking of events in the form of multimedia. Multi-media WSNs consist of a number of low cost sensor nodes equipped with cameras and microphones. These sensor nodes communicate with each other for data retrieval, process, correlation, and compression over a wireless connection. Multi-media sensor nodes are deployed in a pre-planned manner into the atmosphere for coverage guarantee. High bandwidth demand, high energy consumption, quality of service (QoS) condition, data processing and compressing techniques and cross-layer design are challenges in multi-media WSNs. Multi-media content such as video stream needs high bandwidth in order to content to be delivered. Therefore, energy consumption is high for high data rate. High bandwidth and low energy consumption transmission techniques have to be developed. QoS is difficult to preserve in a multi-media WSNs due to variable delay and variable channel capacity. It is essential to get a certain level of QoS for reliable content delivery. In-network processing, filtering, and compression of contents can significantly improve network performance by filtering and extracting redundant information and merging contents. Similarly, cross-layer interaction between the layers can improve the processing and the delivery process. Mobile WSNs is a collection of sensor nodes that can move on their own and interact with the physical environment. Mobile nodes have the ability of sensing, computing, and communication like static nodes. A key difference is mobile nodes have the ability to change the position and organize itself in the network. A mobile WSNs can start with some initial deployment and nodes can then spread out to gather information. A mobile node can communicate to another mobile node when they are within the range of each other and transfer gathered information. Another key difference is data distribution. In mobile WSNs, data can be distributed using dynamic routing while fixed routing or flooding is used in static WSNs. Sensor nodes deployment, localization, self-organization, navigation and control, coverage, energy, maintenance, and data process are challenges in mobile WSNs. Mobile WSNs applications include environment monitoring, target tracking, search and rescue, and real-time monitoring of hazardous material etc. Mobile sensor nodes can achieve a higher degree of coverage and connectivity compared to static sensor nodes.

3. HOW WIRELESS SENSOR NETWORKS WORKS

Wireless sensor networks is collection of the small tiny device called sensor nodes. It may be small and large. That's why construct the wireless sensor network is based on sensor nodes. So entire working of sensor network is depending on sensor nodes. These nodes are varying in size and totally depend on this because different sizes of sensor nodes work efficiently in different fields. Wireless sensor networking have such sensor nodes which are especially designed in such a typical way that they have a microcontroller which controls the monitoring, a radio transceiver for generating radio waves, different type of wireless communicating devices and also ready with an energy source like battery. The entire network worked simultaneously by using different dimensions of sensors and worked on the phenomenon of multi routing algorithm which is also termed as wireless ad hoc networking.

4. WIRELESS SENSOR NODE ARCHITECTURE

For better understanding of sensor network it is important to know about all the components of sensor node. Common sensor node architecture is shown in Figure2. The architecture of a generic wireless sensor node consists of four subsystems [5]. A computing subsystem consisting of a microprocessor, ALU and memory, a communication subsystem consisting of a short range radio for wireless communication, sensing subsystem that links the node to the physical world and consists of a group of sensors and actuators, and a power supply subsystem, which houses the battery and the (optional) DC-DC converter, and powers the rest of the node. Each subsystem plays an main role in the sensor node.
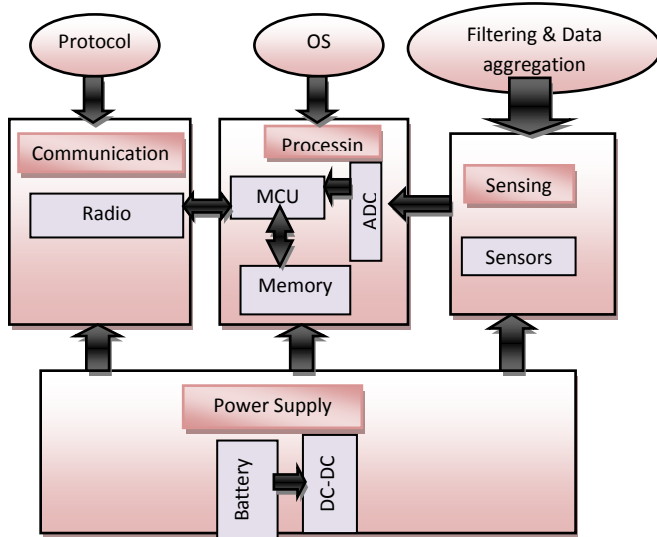
Figure 2 Sensor Node System

Radio: It enables wireless communication among sensor nodes and outside world. It consists of a short range radio which usually has a single channel, a low data rate and operates at unlicensed bands of near 2.4 GHz (global). For efficient energy consumption, it operates in four different modes: Transmit Receive, Idle and Standby modes. In case of most radios, it is observed that when radio operates in Idle mode it consumes energy almost equal to power consumed in Receive mode [6]. Thus, when it is not transmitting or receiving it is vital to completely shut down the radio rather than keep it in the Idle mode to save precious energy. Another influencing factor is that, when radio changes its operating mode, radio electronics causes a significant amount of power dissipation in this transient activity.

Microprocessor: It provides intelligence to the sensor node. The microprocessor controls the sensors, executes communication protocols and signal processing algorithms on the gathered sensor data [7]. To conserve energy, microprocessor works in four different modes: off, sleep, idle, and active. In sleep mode, the CPU and most internal peripherals are turned off, and can only be activated by an external event (interrupt). In idle mode, the CPU is still inactive, but other peripherals are active, for example, the internal clock or timer. In the active mode, multiple sub modes may be defined based on clock speeds and voltages. Within the active states, the CPU and all peripherals are active.

Sensor: It translates physical phenomena to electrical signals. There exists a variety of sensors that measure environmental parameters such as temperature, light intensity, temperature, magnetic fields, sound, image, etc. Due to the diversity of sensors, there is no standard power consumption figure. For a simple sensor we assume that only the states on and off are given, and that the energy consumption within both states can be measured by time. However, more powerful sensors operate in different states, comparable to the microprocessor. To reduce energy consumption low power components can be used at the cost of performance which is not required.

Battery: The battery is an important component in sensor node. It supplies power to all component of sensor node. Therefore, sensor nodes lifetime totally depends on battery and network's lifetime depends on lifetime of sensor nodes. The amount of power drained from a battery should be checked. Since Sensor nodes are usually small, light and cheap and the size of the battery is limited. (Advancement in Battery technologies much more slower than semiconductor technologies. For example, the energy densities of Li-ion batteries only increased 50% from 1994 to 1999. While in the same period of time, the number of transistors of Intel processors doubles every 24 months.). Sensor nodes are deployed in unattended environment where battery replacement is not possible in network which consists of thousands of nodes. Hence, energy consumption is vital factor to prolong sensor nodes lifetime.

5. SPECIAL FEATURES OF WIRELESS SENSOR NETWORKs

This section discusses some unique features of WSNs, which need to be taken into account when designing management architectures in WSNs

5.1 Different types of nodes

In the wireless sensor network are three types of sensor nodes: the normal nodes is reponsile for collecting information or sensor data. Sensor nodes have resource constraint. That's why sensor node have not storing capability for storing large amount of information or sensor data. It may take simply data processing if necessary; sink nodes responsible for receiving, storing, and processing (e.g. aggregation) data from normal nodes; and gateway nodes that connect sink nodes to external entities called observers. In addition, actuators can also be introduced to control or actuate on a monitored region in Wireless sensor networks.

5.2 Application-Specific

Wireless Sensor Networks are closely application-dependent. The constrained resources (e.g. processing, storage and transmission range) limit sensor nodes in WSNs to contain a wide variety of applications as the traditional network does. The designs of applications and management architectures in WSNs are also dependent on application semantics. As a result, application designers have to develop various complex and special program to execute node localization, data routing and data aggregation tailored to specific sensor applications. Thus, it is not likely that those programs can carry over directly from one application to another, since the application-specific requirements on WSNs are varied in terms of resource usage and communication patterns. Recent WSN research has focused increasingly on the solutions that can hold the diversity of various sensor applications by integrating the application knowledge with management architectures in WSNs.

5.3 Resource Constrains

Resource-constrains of sensor nodes is another unique feature of WSNs. Sensor nodes usually compose of four basic units as in Figure 2: a sensing unit, a processing unit, a transceiver unit, and a power unit. The power unit supports all the activities on a sensor node, including communication, local data processing, sensing, etc. The lifetime of a sensor node is mainly determined by the power supply since battery replacement is not an option in sensor networks, especially in dangerous environments as

battlefields or environment monitoring. The longer the lifetime of a sensor, the more stable the WSN. In order to save power, redundant activities should be reduced if not eliminated.

5.4 Network Topology

Network Topology represents the actual topology map and the achieve ability of sensor nodes in the network. Note that the topology in WSNs may be dynamic due to the nodes changes. For example, nodes may fail (either from lack of energy or from physical destruction), and new nodes may join the network. Therefore, the network must be able to reconfigure itself periodically.

5.5 Fault Tolerance

Failures are prone to happen in WSNs, which normally include sensor nodes failure, and communication failures etc. Although the sensor application may have already measured this in their design, there is still a need for WSN to have the ability to reconfigure and recover itself without too much human being intervene, especially in inaccessible environment condition.

6. PROTOCOL STACK FOR WIRELESS SENSOR NETWORK

The sensor network protocol stack is much like the traditional protocol stack, with the following layers: Physical, Data Link, Network, Transport, and Application as discussed by Elizabeth [8] and shown in Figure 3. The WSN must also be aware of the following management planes in order to function efficiently: Power, Mobility, and Task Management Planes. The Power Management Plane is responsible for minimizing power consumption and may turn off functionality to preserve energy. Mobility plane manages the movement of sensor nodes and maintains a data route to the sink. The task plane manages the sensing task assigned to sensor nodes so only those nodes which are necessary, are assigned sensing task and other node can focus their energy resource on routing and data aggregation.

Physical Layer: Physical Layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and encryption. The main work of this layer is to minimization of energy The minimum output power required to transmit over a distance d is proportional to d to a power of n, where n varies from 2 to 4 and is closer to four when the antennae are near the ground as is typical in WSNs. This is due to ground-reflected rays, which causes partial signal cancellation. This problem is overcome by multi-hop communication and high node density.
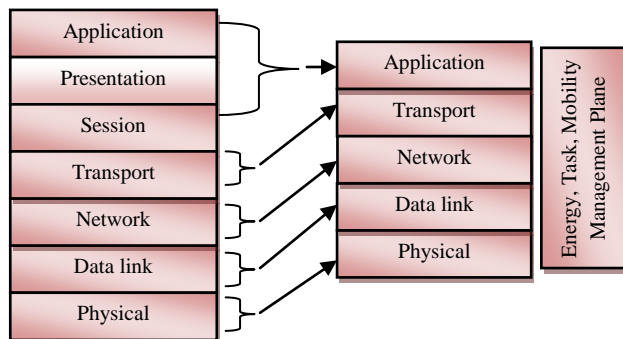

Figure 3 Protocol stack for WSNs

Data Link Layer: The Data Link is responsible for the multiplexing of data streams, data frame detection, medium access and error control. A WSN must have a specific Medium Access Control (MAC) protocol to address the issues of power conservation and data-centric routing. The MAC protocol must meet two goals. The first is to create a network infrastructure, which includes establishing communication links among nodes, and providing the self-organizing capabilities to the network. The second goal is to efficiently share communication resources (frequency) among all the nodes. Traditional MAC protocols fail to meet these two goals because power conservation is only a secondary concern in their development. Also, WSNs are controlled centrally and a much larger number of nodes than traditional ad-hoc networks. Any MAC layer protocol for WSNs must overcome the problem of changing topology of the sensor network due to node failure and redeployment.

Network Layer: The network layer is to provide internetworking with external networks like other sensor networks, In one scenario, the sink nodes can be used as a gateway to other networks. The network layer in a WSN must be designed with the following considerations in mind: Power efficiency, WSNs are data-centric networks WSNs have attribute-based addressing and Sensor nodes are location aware. The Link layer handles how two nodes talk to each other, the network layer is responsible for deciding which node to talk to.

Transport Layer: The transport layer comes into play when the system needs to communicate with the outside world. Transmitting data from sink to outside user is a problem because WSNs do not use global identification and attribute based naming is used for sending the data. Very little research has been done at the transport layer.

Application Layer: At the application layer, a Sensor Management Protocol (SMP), SMP is used to make the hardware and software of lower layers transparent to the sensor network management applications. The programmers and system administrators interact with the sensor network using SMP. Again at application layer the lack of global ids and infrastructure less nature of sensor networks must be taken into account. SMP provides the rules for the following to enable interaction between applications and sensor networks: Data aggregation, attribute-based naming, and clustering ,Time synchronization, Moving sensor nodes, Exchange data related to the location finding algorithms, Authentication, key distribution, and security, Turning nodes on or off, Querying WSN configuration status, reconfiguring the WSN. Different considerations must be taken when developing protocols for WSNs. Traditional thinking where main focus is on quality of service must be reversed. In WSNs quality of service must be compromised to conserve energy and preserve network lifetime. The thought process must focus on the functionality of the entire network rather than what is best for each individual node. Concern must be taken at every level of the protocol stack to conserve energy, allow nodes to reconfigure the network, and modify their set of tasks according to the resources available.

6. WIRELESS SENSOR NETWORK APPLICATIONS

Wireless sensor network has a lots of applications like security, monitoring, biomedical research, tracking etc.basically these application are used emergency services. The applications of the

sensor network are categorized into various classes such as Environmental data collection, Military applications, Security monitoring, sensor node tracking, health application, home application, and hybrid networks.

1. Environmental Data Collection

In environmental data collection application, are used collect various sensor data in a period of time. If a data to be meaningful so collecting sensor data at regular interval and the nodes would remain at known locations. In the environmental data collection application, a large number of nodes continuously sensing and transmitting data back to a set of base stations that store the data using traditional methods. In typical usage scenario, the nodes will be evenly distributed over an outdoor environment. In environmental monitoring applications , it is not essential that the nodes develop the optimal routing strategies on their own. Instead, it may be possible to calculate the optimal routing topology outside of the network and then communicate the necessary sensor data to the nodes as required. This is possible because the physical topology of the network is relatively constant. While the time variant nature of RF communication may cause connectivity between two nodes to be intermittent, the overall topology of the network will be relatively stable.

2.Military Applications

Most of the elemental knowledge of sensor networks is basic on the defence application at the beginning, especially two important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology form the Defence Advanced Research Project Agency (DARPA), sensor networks are applied very successfully in the military sensing. Now wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. In the battlefield context, rapid deployment, self-organization, fault tolerance security of the network should be required. The sensor devices or nodes should provide following services: like Monitoring friendly forces, equipment and ammunition, Battlefield surveillance, Reconnaissance of opposing forces, Targeting, Battle damage assessment Nuclear, biological and chemical attack detection reconnaissance.

3.Security Monitoring

Security monitoring networks are collected of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation. The immediate and reliable communication of alarm messages is the primary system requirement. These are "report by exception" networks. It is confirmed that each node is still present and functioning. If a node were to be disabled or fail, it would represent a security violation that should be reported. For security monitoring applications, the network must be configured so that nodes are responsible for confirming the status of each other. One approach is to have each node be assigned to peer that will report if a node is not functioning. The optimal topology of a security monitoring network will look

quite different from that of a data collection network. In a collection tree, each node must transmit the data of all of its decedents. The accepted norm for security systems today is that each sensor should be checked approximately once per hour. Combined with the ability to evenly distribute the load of checking nodes, the energy cost of performing this check becomes minimal. A majority of the energy consumption in a security network is spent on meeting the strict latency requirements associated with the signaling the alarm when a security violation occurs. In security networks, a vast majority of the energy will be spend on confirming the functionality of neighboring nodes and in being prepared to instantly forward alarm announcements. Actual data transmission will consume a small fraction of the network energy.

4. Node tracking scenarios

In which wireless sensor network is the tracking of a tagged object through a area of space monitored by a sensor network. There are many condition where one would like to track the location of important assets or personnel. Current inventory control systems attempt to track objects by recording the last checkpoint that an object passed through. However, with these systems it is not possible to determine the current location of an object. For example, UPS tracks every shipment by scanning it with a barcode whenever it passes through routing centers. The system breaks down when objects do not flow from checkpoint to checkpoint. In typical work environments it is impractical to expect objects to be continuously passed through checkpoints. With wireless sensor networks, objects can be tracked by simply tagging them with a small sensor node. The sensor node will be tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations. Instead of sensing environmental data, these nodes will be deployed to sense the RF messages of the nodes attached to various objects. The nodes can be used as active tags that announce the presence of a device. A database can be used to record the location of tracked objects relative to the set of nodes at known locations. With this system, it becomes possible to ask where an object is currently, not simply where it was last scanned . Unlike sensing or security networks, node tracking applications will continually have topology changes as nodes move through the network. While the connectivity between the nodes at fixed locations will remain relatively stable, the connectivity to mobile nodes will be continually changing.

5. Health Applications

Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital. In spring 2004 some hospital in Taiwan even use RFID basic of above named applications to get the situation at first hand. Long-term nursing home [9]: this application is focus on nursing of old people. In the town farm cameras, pressure sensors, orientation sensors and sensors for detection of muscle activity construct a complex network. They support fall detection, unconsciousness detection, vital sign monitoring and dietary/exercise monitoring. These applications reduce personnel cost and rapid the reaction of emergence situation.

6. Home Application

Along with developing commercial application of sensor network it is no so hard to image that Home application will step into our normal life in the future. Many concepts are already designed by researcher and architects, like "Smart Environment: Some are even realized. Let's see the concept "the intelligent home":After one day hard work you come back home. At the front door the sensor detects you are opening the door, then it will tell the electric kettle to boil some water and the air condition to be turned on. You sit in the sofa lazily. The light on the table and is automatically on because the pressure sensor under the cushion has detected your weight. The TV is also on. One sensor has monitored that you are sitting in front of it. "I'm simply roasting. The summer time in Asia is really painful." You think and turn down the temperature of the air condition. At the sometime five sensors in every corner in the room are measuring the temperature. Originally there is also sensor in the air condition. But it can only get the temperature at the edge of the machine not the real temperature in the room. So the sensors in the room will be detecting the environment. The air condition will turn to sleep mode until all the sensors get the right temperature. The light on the corridor, in the washing groom and balcony are all installed with sensor and they can be turned on or turn out automatically. Even the widows are also attached with vibratory sensors connected to police to against thief. How nice! You become nurse and bodyguard at the same time.

7. WIRELESS SENSOR NETWORK CHALLENGES

WSN is an emerging area. It offers wide variety of applications and these applications can be implement in real world. To implement them more efficient protocols and algorithms are needed. Design a new protocol or algorithm addresses challenges of this field. To design a better protocol or algorithm, it is necessary to first clearly understood challenges [9]. These challenges are summarized below.

Physical Resource Constraints: The most important constraint in sensor network is the limited battery power of sensor nodes. Sensor nodes are left in unattended environment where recharge and replacement of battery is not possible. Sensor node's lifetime dependents on battery power. Thus effective lifetime of sensor network is directly dependent on battery. Hence the energy consumption is main design issue of a protocol. Limited computational power and memory size is another constraint due to that individual sensor node can store and process less amount of data. So the protocol should be simple and light-weighted. Limited bandwidth is also a constraint due to this communication delay can be high.

Ad-hoc Deployment: Sensor nodes are randomly deployed in required monitoring field without any infrastructure. For an example, for fire detection in a forest the nodes are typically dropped in to the forest from a plane. Sensor nodes itself create connections with other nodes and form an infrastructure. Hence new protocol or algorithm should be able to handle this ad-hoc deployment.

Fault-Tolerance: Sensor nodes are prone to failure because of unattended environment. A sensor node may fail due to hardware or software problem or energy exhaustion. If few of sensor nodes fail, working protocol should handle all type of failures to maintain connectivity and prolong lifetime of network. For example, routing or aggregation protocol, must find suitable paths or aggregation point in case of these kinds of failures.

Scalability: In monitoring field, number of sensor nodes deployed could be in order of hundreds, thousands or even more. It depends upon the application. It may possible that initially deployed sensor nodes are not enough to monitor the environment. In this situation, protocol that is working upon network should be scalable and able to accommodate large number of sensor nodes.

Quality of Service: Some applications like multi-media or time critical needs QoS. Multi-media application requires enough good quality of contents (video, audio and image). In time critical application, the data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. New protocols which are designed for such applications should handle QoS.

Security: In sensor networks, security is another important and challenging parameter. An effective and efficient compromise should be achieved, between security demands for secure communication and low bandwidth required for communication in sensor network. Whereas in traditional networks, the focus is on maximizing channel throughput with secure transmission.

8. WIRELESS SENSOR NETWORKS VS TRADITIONAL WIRELESS NETWORKS

There are many existing protocols, techniques and concepts from traditional wireless network, such as mobile ad-hoc network, cellular network, wireless local area network and Bluetooth, that are applicable and still used in WSN, but there are lot of fundamental differences which initiate the need of new techniques and protocols [12]. Some of the most important characteristic differences are summarized below: In WSNs, number of nodes is much higher than any traditional wireless network. Depending on the application, nodes may be in order of even millions. Thus, it requires an extremely scalable solution to make sure sensor network operations without any interruption. WSNs have large number of sensor nodes due to this addresses are not assigned to them. Instead of address-centric sensor networks are data-centric. Operations of sensor networks are concentrated on data instead of individual sensor node. Thus, sensor nodes need collaborative efforts. Most of traditional wireless networks use point-to-point communications, whereas sensor networks use broadcast communications. Sensor nodes are much cheaper than nodes in ad hoc networks. WSNs are event-driven or environment-driven. Sensor networks generate or collect data when any event occurs or environment changes, while human generates data in traditional networks. Hence, traffic pattern changes significantly from time to time. Mobile ad hoc Networks (MANETs) are designed for distributed computing, while sensor networks are mostly used to gather information. Data collected by neighboring sensor nodes is highly correlated. It has also been observed that the environmental quantities changes very slowly and some consecutive readings, sensed by sensor nodes are correlated. It is a unique characteristic of sensor network, which gives an opportunity to develop energy efficient protocols for routing and aggregation. These protocols reduce traffic and redundant data in network and prolong network lifetime. Thus,

main focus of sensor network is to extend network lifetime, where traditional network try to maximizing throughput of a channel or minimizing node deployment in network.

9. THIS NETWORK HAS CERTAIN ADVANTAGES ALSO OVER THE TRADITIONAL NETWORKS

Advantages: The configuration of the wireless sensor network is nearly zero. Sensor nodes of the wireless sensor network have low cost as compared to GPRS modems. if we talk about energy so in which minimum energy consumption as compared to traditional network and the coverage area is easy to expansion and reduction. **Disadvantages:** Wireless sensor network has lower speed as compared to wired network. It is a less secure because hacker's laptop can act as access point. If you connected to their laptop, they'll read all your information. Affected by surrounding. Such as walls (blocking), microwave oven (interference), far distance (attenuation).

10. CONCLUSION

Wireless sensor network is very important wireless network because it able to monitor the physical and environment condition, where traditional network is not monitors it. In this paper we discuss overview of the wireless sensor network, how differ from the tradition network, and challenges, features, protocol stack of the sensor network. But wireless sensor networking has a bright future in the field of computer networking because we can solve the monitoring problems at an advanced level in the future with the help of such technology of networking.

10.1. Acknowledgments

11. REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey On Sensor Networks", IEEE Communications Magazine, Volume 40, Number 8, pp.102-114, 2002.

[2] Deborah Estrin, R.G., John Heidemann, Satish Kumar. Next Century Challenges: Scalable Coordination in Sensor Networks. In ACM/IEEE International Conference on Mobile Computing and networking. 1999.

[3] Eiko Yoneki, J.B., A Survey of Wireless Sensor Network Technologies: Research Trends and Middleware'S Role. 2005, University of Cambridge: Cambridge. p. 45.

[4] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey," Computer Networks Elsevier 52 (2008) 2292–2330.

[5] I.F. Akyildiz, E.P. Stuntebeck, Wireless underground sensor networks: research challenges, Ad-Hoc Networks 4 (2006) 669–686.

[6] J. Feng, F. Koushanfar, M. Potkonjak,"System-Architectures for Sensor Networks Issues, Alternatives, and Directions", IEEE International Conf on Computer Design (ICCD), Germany, 2002. pp. 226- 231.

[7] D. Culler, D. Estrin, M. Srivastava, "Overview of Sensor Networks", IEEE Computer, USA, vol 37, pp. 41-49, August 2004.

[8] A. M. Bratkovski, "Monitoring an environment using RFID assembly." vol. WO/2006/094085, W. I. P. Organization, Ed. USA: HEWLETT-PACKARD Development Company, L. P., 2006, p. 13

[9] I.F. Akyildiz, W. Su, A power aware enhanced routing (PAER) protocol for sensor networks, Georgia Tech Technical Report, January 2002, submitted for publication.

[10] P. Bonnet, J. Gehrke, P. Seshadri, Querying the physical world, IEEE Personal Communications (October 2000) 10–15.

[11] A. Cerpa, J. Elson, M. Hamilton, J. Zhao, Habitat monitoring: application driver for wireless communications technology, ACM SIGCOMM'2000, Costa Rica, April 2001.

[12] R. K. Ghosh , Vijay Garg , M. S. Meitei , S. Raman , A. Kumar and N. Tewari, "Dense cluster gateway based routing protocol for multi-hop mobile ad hoc networks," *Ad Hoc Networks*, Vol. 4, No. 2, p.168-185, March, 2006 .