Design Issues and Challenges in Wireless Sensor Networks

Khushboo Gupta
PhD Research scholar
Department of Computer Science Engineering
Uttar Pradesh technical university, Lucknow, India

Vaishali Sikka
M.Tech (Information Technology)
Department of Computer Science Engineering
Banasthali Vidhyapith, Jaipur, India

ABSTRACT
Wireless Sensor Networks (WSNs) are composed self-organized wireless ad hoc networks which comprise of a large number of resource constrained sensor nodes. The major areas of research in WSN is going on hardware, and operating system of WSN, deployment, architecture, localization, synchronization, programming models, data aggregation and dissemination, database querying, architecture, middleware, quality of service and security. This paper study highlights ongoing research activities and issues that affect the design and performance of Wireless Sensor Network.

General Terms
Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords
Wireless Sensor Network; Design Issues; Hardware; Operating System; Middleware; QoS; Architecture; Security

1. INTRODUCTION
Wireless sensor networks (WSN) are increasingly used in applications such as military, healthcare, environmental, biological, structural health monitoring, and condition based monitoring.With the great advancement in the field of embedded computer and sensor technology, WSN's consist of thousands of sensor nodes which are capable of sensing, actuating and relaying the collected information. The potential of Wireless Sensor Network is nothing short of revolutionary. This technology will affect all aspects of our lives in the near future.

2. VARIOUS DESIGN ISSUES
In addition to the unreliable wireless communication, nodes of a WSN have to work with limited resources such as limited memory, limited computation and processing capacity, limited storage, limited battery power, limited communication capacity. Related to design of wireless sensor network [33] different factors are discussed as:

2.1 Hardware of Wireless Sensor Network
Wireless sensor networks are composed of several thousands of micro devices called nodes. A Sensor and Mote together form a Sensor Node. The structure of the sensor node is as shown in figure1. A Sensor Node forms a basic unit of the sensor network [1, 2].A Sensor is a device which senses the information and passes it on to a mote. Sensors measures the changes in physical environment like pressure, sound humidity, vibration and changes to the health of person like blood pressure, stress and heartbeat. A Mote consists of processor, battery, memory, ADC for connecting to a sensor and a radio transmitter for forming an ad hoc network.

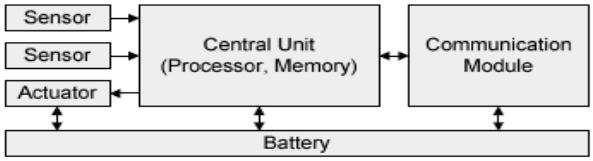

Figure 1. Structure of sensor Node

The nodes used in sensor networks are tiny and have energy constraints. The hardware design issues of sensor nodes are [3]:

1. Power Consumption of sensor should be minimized and nodes should be power efficient since their limited power resource determines the network lifetime. To conserve power the node should shut off when not in use. Battery type is significant since it can affect the design of sensor nodes. Battery Protection Circuit can be added to the sensor nodes to avoid overcharge or discharge problem.
2. Radio Range of nodes should be high of around 2-5 km. Radio range is crucial for ensuring network connectivity and data gathering in a network as the environment being examined may not have an installed infrastructure for communication.
3. Use of Memory Chips like flash memory is desirable for sensor networks as they are non-expensive, non-volatile and thus electrically erased and reprogrammed.

There are various hardware platforms that are already developed taken into account the above discussed design issues like MicaZ,Mica2,BT Node and Imotes and MIT µAMPS .Among theses the Berkeley Motes, which is commercially made available by Crossbow Technologies is very popular and is also for several research work.

2.2 Operating System of Wireless Sensor Network
Operating system architecture for a sensor node should be able to provide resource management and memory management in a constrained environment. The various design issues of an Operating System (OS) for sensor networks are:

1. In sensor network a sensor node is responsible for computation of the extracted data from the local environment. It processes that data and manipulates it as per the requirement of an application. A concurrency mechanism is required in sensor nodes as all the activities in sensor network require real time response like processing and routing of the data.

2. An OS for sensor nodes should not be hardware dependent instead it should be application specific and should support multi-hop routing.
3. The OS should have an easy programming paradigm. Application developers should be able to concentrate on the application logic instead of being concerned with the lower level hardware issues like preempting scheduling and networking.
4. The OS should have in-built features to minimize the battery consumption. Since motes cannot be recharged as and when wished so it should impose limitation on the amount of resources used by each application [4].
5. The OS need to be priority based by giving precedence for higher priority events.

Several Operating Systems like TinyOS [5] is designed on the principle of above design issues. TinyOS is an open source and most popular OS used by the researchers and industry. TinyOS has a component-based architecture which enables rapid innovation and implementation while minimizing the code size as required in sensor networks. The execution model of TinyOS supports complex yet safe concurrent operations. TinyOS's component library includes distributed services, sensor drivers, network protocols and data acquisition tools. TinyOS has been implemented in NesC language, which supports the TinyOS component and concurrency model.

2.3 Wireless Communication Characteristics

Performance of wireless sensor networks is determined by the quality of wireless communication. But wireless communication is well known for its unpredictable nature. Main design issues for Wireless communication in WSNs are:

1. Low power consumption is required to enable long operating lifetime by facilitating local signal processing and low duty cycle operation.
2. Distributed Sensing effectively acts against various environmental barriers and care should be taken so that the signal- strength and radio-range is not reduced by various factors like dispersions, reflection and scattering.
3. Multi-hop networking may be accommodated in the sensor nodes to reduce communication link range and density of sensor nodes should be kept high.
4. We should consider short range transmission as Long range communication is usually point to point and demands high transmission power, with the possibility of eavesdropping.
5. Communication systems should include flow control and error control mechanism to detect and correct errors.

2.4 Medium Access Schemes

Communication is a main source of power consumption in WSNs and MAC protocols directly control the radio of the sensor nodes in the network. Thus MAC protocols should be designed for controlling and regulating power consumption, which in turn influences the network lifetime .The various design issues of the MAC protocols suitable for sensor network environment are: [6, 7]:

1. The MAC layer can helps in conserving the power as it has control of the transceiver and allows on and off switching of the radio. The design of the MAC protocol can incorporate this switching mechanism to decide when and how frequently the on and off should be done.
2. A MAC protocol should also avoid collisions from interfering nodes, over-hearing, over-emitting, control packet overhead and idle listening. When a receiver node receives more than one packet at the same time, these packets collide and the information is lost, which need to be sent again thereby increasing power consumption. Over-hearing occurs if a node picks up packets that were destined for some other node. When a destination node is not ready to receive messages then it is called over-emitting. Idle listening is an important factor as the nodes often hear the channel for possible reception of the data which is not sent.
3. Scalability, Adaptability and De-centralization are important criterion in designing a MAC protocol. The sensor network should adapt to the changes in the node density, network size and topology. Also some nodes may die over time, some more nodes may join and some nodes may move to different locations. A good MAC protocol should able to adapt to these changes in the network.
4. A MAC protocol should have high throughput and minimum latency (high network efficiency) when the sensor networks are deployed in critical applications. The MAC protocols should also take into account the well-known problem of Information Asymmetry, which arises if a node is not aware of packet transmissions two hops away.
5. A MAC protocol should include Message Passing, which means dividing a long message into small fragments and transmit them in burst. Thus, a node which has more data gets more time to access the medium.MAC Protocols should also satisfy the Real-time requirements. Mac being the base of the communication stack; processing, timely detection and delivery of the information from the deployed environment are an essential requirement in a WSN application.
6. There should be uniformity in reporting the events by a MAC protocol. Since the nodes are deployed random manner, nodes from highly dense area may face high contention among themselves when reporting events resulting in high packet loss. Consequently the sink detects fewer events from such areas. Also the nodes which are nearer to the sink transmit more packets at the cost of nodes which are away from the sink.

Some popular MAC Protocols are for WSN are S-Mac (Sensor MAC), B-Mac (Berkeley MAC), Z-MAC (Zebra MAC), Time-MAC and Wise-Mac.

2.5 Deployment

Deployment means positioning an operational sensor network in a real world environment. Sensor nodes can be deployed either by placing one after another in a sensor field or by dropping it from a plane. 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. Several deployment issues which need to be taken care are [8, 9]:

1. During the deployment of Sensor Network, Node death due to power consumption (depletion) caused either by normal battery discharge or due to short circuits is a common problem which may lead to wrong sensor readings. Also problem affecting sink nodes should be identified to minimize data loss, as sink node store and forward the collected data thus act as a gateway.
2. Another common problem of real world deployment of sensor nodes is Low data yield, which means network is not delivering sufficient amount of information as required.
3. Due to multiple concurrent transmission attempts made by the sensor node, deployment may results in Network Congestion. Another issue is the physical interference in the real world due to which two close nodes may not be able to communicate with each other while nodes which are far away may communicate with each other.
4. Self-Configuration of sensor networks without human intervention is required for random deployment of sensor nodes.

A framework is proposed in [10] taken into account the above deployment issues. POWER is a software environment for planning and deploying WSN applications into actual environment.

2.6 Localization

Sensor localization is a primary and essential issue for network management and operation. In many real world scenarios, the sensors are deployed in ad-hoc manner so they do not have knowledge about their position. The problem of determining the physical location of the nodes is called localization. Also there is no supporting infrastructure available to locate and manage them once they are deployed [11, 12].

Localization algorithm for a sensor network should satisfy the following requirements:

1. Since Centralized localization approach need high computation. It also puts extra load on the nodes closer to the center node. Thus the localization algorithm distributed.
2. To implement an energy efficient message routing protocols in sensor networks, knowledge of the node location can be used.
3. Localization algorithms should be robust enough to localize the failures and loss of nodes. Localization algorithm should be scalable, accurate and support mobility of nodes.
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
5. Techniques that depend on measuring the ranging information from signal strength and arrival require specialized hardware that is usually not available on sensor nodes.

2.7 Synchronization

Time Synchronization provides a common timescale for local clocks of nodes in the sensor network. Clock synchronization is an important service in sensor networks. A global clock in a sensor system will help to analyze the data correctly and predict future system behavior. Some applications that require global clock synchronization are navigation guidance, environment monitoring, vehicle tracking etc. A clock synchronization service for a sensor network has to meet challenges that are different from those in infrastructure based networks [13].

1. Power utilization in some synchronization schemes is more due to energy hungry equipment like NTP (Network Time Protocol) and GPS (Global Positioning System) receivers.
2. The Network lifetime for the nodes which are spread over a large geographical area needs to be taken into account. Since Sensor nodes have higher degree of failures, the synchronization protocol needs to be more robust to failures and communication delay.
3. Sensor nodes need to coordinate and collaborate to achieve to data fusion. In data fusion the data gathered from different nodes are aggregated into a meaningful result. If the sensor nodes lack synchronization then the data estimation will be inaccurate.
4. For higher degree of accuracy, more resources are needed. Therefore we need to have tradeoff between synchronization accuracy and resource requirements based on the application.
5. Since the Sensor networks span multi hops with higher jitter, the algorithm for clock synchronization needs to achieve multihop synchronization even in the presence of high jitter.

Various synchronization protocols are Reference Broadcast Synchronization (RBS) and Delay Measurement Time Synchronization protocol.

2.8 Calibration

Calibration is the process of accommodating the raw sensor readings obtained from the sensors into corrected values by comparing it with some standard values. Manual calibration of sensors is a time consuming and tedious task due to failure of sensor nodes and random noise which makes it too expensive.

Various Calibration issues in sensor networks are [14]:

1. A sensor network consists of huge number of sensors usually with no calibration interface.
2. Reference values might not be readily available and Access to individual sensors in the field can be limited.
3. Different applications may require different calibration. Calibration in a complex dynamic environment requires many observables like aging, decaying, damaging etc.
4. 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.

2.9 Network Layer Issues

Over the past few years sensor networks are being built for specific applications and routing which is a very challenging task is important for sending the data from sensor nodes to Base Station (BS). Various issues at the network layer are [15]:

1. Power efficiency is a very important criterion. At the network layer, we have to find different techniques for discovering power efficient routes (route discovery) and for relaying the data from the sensor nodes to the BS so that the network lifetime can be optimized.
2. Routing Protocols should include multi-path design technique. Multi-path protocols are those protocols which set up multiple paths so that a path among them (alternative paths) can be used when the primary path fails.
3. Route Maintenance is required in routing protocols whenever a route breakage 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 if some nodes fail or blocked due to some environmental interference.
4. In the network layer in order to maximize power consumption we have to provide a flexible platform for performing Route Discovery and Management.
5. Sensor networks collect information from environment and are highly data centric. The data traffic that is generated will have significant redundancy among individual sensor nodes since multiple sensors may generate same data. The routing protocol should overcome such redundancy to improve power and bandwidth utilization.
6. Routing Protocols should be of heterogeneous nature i.e. each node will be different in terms of communication, computation and power. They should have multiple wireless hops so the nodes are scattered randomly resulting in an ad hoc routing infrastructure.

Various routing Protocols for WSNs are Rumor Routing, Direct Diffusion, (SPIN) Sensor Protocols for Information via negotiation, Low Energy Adaptive Cluster Hierarchy (LEACH), Geographic and Energy Aware Routing (GEAR), Threshold sensitive Energy Efficient sensor Network protocol (TEEN), Sequential Assignment Routing (SAR) and others

2.10 Transport Layer Issues

Transport layer provide End to End reliable communication. The various design issues for Transport layer protocols are [16]:

1. Transport layer is responsible for fragmenting the message into several packets at the transmitter and reassembled at the receiver. Therefore a transport protocol should ensure orderly transmission of the fragmented segments.
2. A transport layer protocol should be reliable for delivering data into large group of sensors under extreme conditions. Limited bandwidth results in congestion and may also lead to packet loss. Bit error rate also results in packet loss and also wastes power.
3. End to End communication may suffer due to various reasons: The placement of nodes is not predetermined and external obstacles may lead to poor communication between two nodes. Another problem is failure of nodes due to battery depletion.
4. In sensor networks the loss of data is tolerable when it flows from source to sink. But message loss is sensitive when the data that flows from sink to source.
5. Traditional transport protocols such as UDP and TCP cannot be directly implemented in sensor networks as flow control and congestion control mechanism cannot be applied for nodes which are far away from sink node.

One popular transport layer protocol is Pump Slowly, Fetch Quickly (PSFQ) [12].

2.11 Data Aggregation and Dissemination

Data collection involves collecting the sensed data from multiple sensors and transmitting the data to the BS for further processing. The sensors periodically sense the data from the environment, process it and transmit it to the BS or sink. The frequency of reporting the data and also the number of sensors which report the data is application specific. The data generated from sensors is often redundant and huge for the BS to process it. Thus a method is required for combining the sensed data into high quality information and this can be accomplished through Data Aggregation [17].

Data Aggregation can be defined as the process of combing the data from multiple sensors with the aim to eliminate redundant transmission and estimating the desired answer about the sensed environment.

Some design issues in data aggregation are [17]:

1. Sensor networks are unreliable in nature. Certain data may be unavailable or expensive to obtain for instance the number of nodes in the network and the number of nodes that are actually responding and also it is difficult to find complete and up-to date data of the neighboring sensor nodes.
2. Allowing few nodes to transmit data directly to the BS or to have less transmission of data to the BS to reduce power.
3. Eliminate redundant data transmission from nodes by using meta- data negotiations as in SPIN protocol.
4. Improving in-Network aggregation which means sending partially aggregated values rather than raw values, thereby reducing power consumption. Improving clustering techniques for data aggregation to conserve power of the sensors.

Data dissemination is a process by which data and the queries are routed in the sensor network [18]. Data dissemination is a two-step process. In the first step, if a node is interested in some data, like temperature or humidity, then it broadcasts its interests to its neighbors periodically and then through the whole sensor network. In the second step, the nodes that have the requested data will send the data back to the source node after receiving the request. The main difference between data aggregation and data dissemination is, in data aggregation data can be transmitted periodically, while in data dissemination data is always transmitted on demand. Flooding

is one important protocol which includes data dissemination approach.

2.12 Database Centric and Query

Sensor networks have the capability to spread and monitor a huge geographical area and to produce vast amount of data. So sensor networks should be able to accept the queries and respond with the accurate results. The following requirements and design issues of a sensor network make sensor database different from traditional database [19].

1. The nodes are volatile since they may get depleted and links between nodes may go down at any point of time but data collection should not be interrupted.
2. Sensor data is exposed to more errors than in a traditional database due to interference of signals and device noise.
3. Sensor networks produce data continuously in real time and on a large scale from the sensed phenomenon which require updating the data frequently; whereas traditional database is usually of centralized and static in nature.
4. Limited storage and energy scarcity is another important issue that requires attention in a sensor network database but a traditional database usually consists of plenty of resources and disk space is not an issue.

2.13 Architecture

The lack of an overall WSN architecture is the main factor for currently limiting the progress in sensor networks. Architecture can be considered as a set of rules and regulation for implementing some functionalities along with a set of interfaces, functional components, protocols and physical hardware. Software architecture is needed to bridge the gap between raw hardware capabilities and a complete system. The key issues that must be addressed by the sensor architecture are [20, 21]:

1. Several operations like continuous monitoring of the channel, encoding of data and transferring of bits to the radio need to be performed in parallel. Also sensor events and data calculations must continue to proceed while communication is in progress.
2. A durable and scalable architecture would allow dynamic changes to be made for the topology with minimum update messages being transmitted.
3. The system must be flexible to meet the wide range of target application scenarios since the wireless sensor networks to not have a fixed set of communication protocols that they must adhere to.
4. The architecture must provide precise control over radio transmission timing. This requirement is driven by the need for ultra-low power communication for data collection application scenarios.
5. The architecture must decouple the data path speed and the radio transmission rate because direct coupling between processing speed and communication bit rates can lead to sub-optimal energy performance.

The authors of [22] design a novel SP abstraction which promotes cooperation across the link and network layers to utilize limited resources efficiently. A unifying abstraction in SP leads to supporting a variety of link-layer technologies and network protocols while taking care that doing so will not lead to a significant loss of efficiency.

2.14 Sensor Network Programming Models

Today, researchers are too much concerned with low level details like sensing and node to node communication that raise a need for programming abstractions. There is need for designing programming models for sensor networks due to following issues [23]:

1. A reactive and event driven programming model is required, as the data gathered from the surrounding phenomenon is not for general purpose computing.
2. Programming models can help programmers in writing energy efficient applications. As even a typical embedded OS consuming hundreds of KB of considered too much.
3. Since the applications in a sensor network have to run for a long duration without human intervention, we have to reduce the run time errors and complexity.
4. A Programming model should be accompanied by runtime mechanism that can achieve bandwidth efficiency whenever possible.

Programming models like TinyOS with Nesc and TinyGALS with gals [24] are popular models and provides tremendous opportunities for research.

2.15 Middleware

WSN middleware is considered as a software framework that glues together the network hardware, operating systems, network stacks and applications. A middleware for wireless sensor network should facilitate development, deployment, maintenance and execution of sensing-based applications. Several issues in designing a middleware for wireless sensor networks are [25]:

1. Middleware should provide new programming paradigm to provide application specific API's rather than dealing with low level specifications. It should also provide interfaces to the different types of hardware and networks supported by primitive operating system abstractions.
2. Middleware should include technique to deliver real time services by dynamically adapting the environmental changes and providing consistent data. Middleware should also be adaptable to the devices being programmed depending on the hardware capabilities and application requirement.
3. Efficient middleware solutions should conceal the complexity involved in configuring individual nodes based on their capabilities and hardware architecture.
4. The Design of Middleware should be transparent. Middleware is designed for providing a general framework whereas sensor networks are designed for a particular application. Therefore a trade-off is required between generality and specificity.
5. Middleware design should include a real time priority that means message priority should be

assigned at runtime by the middleware. Middleware in sensor network should support scalability, mobility and dynamic network organization.

6. Middleware should also support Quality of Service (QoS) and Security Mechanisms. The importance of these in sensor networks is crucial in mission critical areas like military, aviation and in medical field.

A popular Middleware architecture for constructing application specific virtual machines is Mate [26] that executes on top of TinyOS.

2.16 Quality of Service

The level of service provided by the sensor networks to its users is known as Quality of Service. The authors of [27] describe Quality of Service (QoS) for sensor networks as the optimum number of sensors sending data to information-collecting sinks or a BS. Since sensor networks are implemented in huge number of applications which includes mission critical applications such as military applications and nuclear plant monitoring applications.

The Quality of Service issues in sensor networks are [29]:

1. The QoS in WSN is difficult because the network topology may constantly change. This dynamic nature of sensor networks makes availability of precise state information next to impossible.
2. Nodes in the sensor network may join, leave and rejoin and links may be broken at any time. Hence maintaining and re-establishing the paths dynamically is a problem in WSN. Sensor networks should be supplied with the required amount of bandwidth in order to achieve a minimal required QoS.
3. Traffic is uneven in sensor network as the data is aggregated from many nodes to a sink node. QoS technique should be designed to balance QoS constrained traffic.
4. Buffering in routing can be useful as it helps to receive packets before forwarding them. But a vast amount of data is buffered in multihop routing. This limitation in buffer size will increase the delay in packet delivery making it difficult to meet QoS requirements.
5. QoS designed for WSN should be able to support scalability that means adding or removing of the nodes should not affect the QoS of the WSN.

Sequential Assignment Routing (SAR) [24] is one of the first protocols which had QoS support.

2.17 Security

Security is as much an important feature as performance and power consumption in Wireless Sensor Network. Security in a sensor network is very challenging as WSN is deployed in battlefield applications, surveillance, building monitoring, burglar alarms and in critical systems such as hospitals and airport. Different types of threats in sensor networks are Spoofing and altering the routing information, passive information gathering, node subversion, sinkhole attacks, sybil attacks, Denial of service attack and jamming.

Following are the initial security requirements to which every WSN application should adhere to [30,31,32].

1. Confidentiality is needed to protect information traveling between the sensor nodes of the network or between the sensors and the BS; otherwise it may result in eavesdropping on the communication. It ensures sensitive information is well protected and not revealed to unauthorized third parties.
2. Authentication verifies the identity of the participants in a communication. In sensor networks it is essential for each sensor node and the BS to have the ability to verify that the data received was really sent by a trusted sender.
3. Lack of integrity may result in imprecise information. Many sensor applications rely on the integrity of the information to function.
4. One of the attacks 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.
5. In sensor networks secure management is required at the BS level, as communication in sensor network ends up at the BS. Issues like Key distribution to sensor nodes in order to establish encryption and routing information need secure management. Clustering techniques also require secure management as each group of nodes may include a large number of nodes that need to be authenticated with each other in order to exchange data in a secure manner.
6. Security mechanisms like encryption should be lightweight so that the overhead is minimized and should not affect the performance of the network.

3. SUMMARY

Wireless Sensor Networks have created wide range of challenges that still needs to be addressed to develop the WSN applications. In this paper we have discussed several issues associated with Wireless Sensor Networks. We have also implemented these issues in part or as a whole in some important protocols. The impact of wireless sensor networks on our day today life can be preferably compared to what Internet has done to us. WSN is emerging as a very important tool for making our life comfortable and safe. This field is surely going to give us tremendous opportunity to change the way we perceive the world today.

4. ACKNOWLEDGMENTS

We are highly indebted to Dr. Prof. K. P. Yadav for their guidance and constant supervision as well as for providing necessary information regarding the subject. Our thanks and appreciations to our family members and friends who have willingly helped us out with their abilities.

5. REFERENCES

[1] J. Wang, X. Ren, Y. Shen, and S. Liu, "A remote wireless sensor network for water quality monitoring," *Intl. Conf. on InnovativeComputing and Communication*, pp.7-12, 2010.

[2] Michał Marks "A Survey of Multi-Objective Deployment in Wireless Sensor Networks", Journal of telecommunications and information technology, published in 2010.

[3] P.Zhang, M.Sadler,A,Lyon and M.Martonosi, "Hardware Design Experiences in ZebraNet", In proceedings of SenSys'04, November 3-5, 2004, Baltimore, USA.

[4] A.Eswaran, A.Rowe and R.Rajkumar, "Nano-RK: An energy aware Resource Centric RTOS for sensor networks", In proceedings of the 26th IEEE International Real-Time Systems Symposium (RTSS'05) 2005, pp: 256-265.

[5] Tinyos Operating System for WSN www.**tinyos**.net/

[6] IlkerDemirkol, CemErsoy and FatihAlagoz, "MAC Protocols for Wireless Sensor Networks: A Survey", IEEE Communications Magazine, April 2006.

[7] Ying Liang, "Energy-efficient, Reliable Cross-layer Optimization Routing Protocol for Wireless Sensor Network", International Conference on Intelligent Control and Information Processing, August 13-15, 2010, Dalian, pp. 493-496.

[8] J. F. Martinez, M. S. I. Familiar, , Corredor, A. B. Garcia, S. Bravo, and L. Lopez, "Composition and deployment of e-health services over wireless sensor networks," *Mathematical and Computer Modelling*, vol. 53, no. 3-4, pp. 485-503, February 2011.

[9] J.Li, Y Bai, HaixingJi and D. Qian, "POWER: Planning and Deployment Platform for Wireless Sensor Networks", In proceedings of the Fifth International Conference on Grid and Cooperative Computing Workshops (GCCW'06), IEEE 2006.

[10] Xia Zhenjie, Chen Changjia,"A Localization Scheme with Mobile Beacon for Wireless Sensor Networks", In Proceedings of International Conference on ITS Telecommunications Proceedings 2006.

[11] SantashilPalChaudhuri, Amit Kumar Saha and David B.Johnson,"Adaptive Clock Synchronization in Sensor Networks", IPSN'04, April 26-27, Berkeley, California, USA.

[12] Kamin Whitehouse and David Culler,"Calibration as Parameter Estimation in Sensor Networks",In Proceedings of WSNA'02 September 28, 2002, Atlanta,Georgia,USA, pp 59-67.

[13] Deepak Ganesan et.al, "Networking Issues in Wireless Sensor Networks", Elsevier Science, 9th December 2005.

[14] C. Wang et.al, "A Survey of Transport Protocols for Wireless Sensor Networks", IEEE Network June 2006. Vol:20, Issue:3, pp:34-40.

[15] Chien-Yih Wan, L.Krishnamurthy, "Pump-Slowly, Fetch-Quickly (PSFQ): A Reliable Transport Protocol for Sensor Networks", IEEE Journal on selected areas in Communications, Vol 23, No 4, April 2005.

[16] Wensheng Zhang, G Cao and Tom La Porta,"Data Dissemination with Ring Based Index for Wireless Sensor Net.

[17] Yang wenguo and GuoTiande, "The Non-uniform Property of Energy Consumption and its Solution to the Wireless Sensor Network", 2nd International Workshop on Education Technology and Computer Science, March 6-7, 2010, pp. 186- 192.

[18] S.Duan and XiaobuYuan,"Exploring Hierarchy Architecture for Wireless Sensor Network Management", IEEE 2006.

[19] System Architecture for Wireless Sensor Networks by Jason Lester Hill, Ph.D dissertation, University of California at Berkeley.

[20] Joseph Polastre, Philip Levis, David Culler et.al,"A Unifying Link Abstraction for Wireless Sensor Networks", SenSys'05, November 2-4, 2005, San Diego, California, USA, ACM 2005.

[21] Ryo Sugihara and Rajesh K.Gupta,"Programming Models for Sensor Networks: A Survey", ACM Transactions on sensor networks 2006

[22] E.Choeng, J.Liebman,J.Liu and F.Zhao,"TinyGALS: A programming model for event-driven embedded systems", in SAC'03, pp 698-704.

[23] Kay Romer, Oliver Kasten and F.Mattern,"Middleware Challenges for Wireless Sensor Networks", Mobile Computing and Communications Review, Volume 6, Number 2.

[24] P.Levis and D.Culler,"Mate: A Tiny Virtual Machine for Sensor Networks", In Proceedings of the 10th International Conference onArchitectural Support for Programming Languages and Operating Systems, San Jose, CA, USA, October 2002.

[25] RanjitIyer and Leonard Kleinrock,"QoS Control for Sensor Networks", IEEE 2003.

[26] M.Younis, K.Akkayaet.al,"On Handling QoS traffic in Wireless Sensor Network", Procedings of the 37th Hawaii International Conference on System Science 2004.

[27] K.Shhrabi, J.Gao, V.Ailawadhi and G.J.Pottie,"Protocols for self organization of a wireless sensor networks",IEEE Personal Communications, October 2000, pp 16-27.

[28] Jai Xiangyu and Wang Chao,"The security routing research for WSN in the application of intelligent transport system", Proceedings of the 206 IEEE International conference on mechatronics and automation, June 25-28, 2006, Luoyang, China.

[29] Yong Wang, GarhanAttebury and ByravRammurthy,"A survey of security issues in wireless sensor networks", IEEE Communications survey, 2nd quarter 2006, Volume 8, No 2.

[30] KuthhadiVenuMadhav, Rajendra.C and Raja Lakshmi Selvaraj "A STUDY OF SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS", Journal of Theoretical and Applied Information Technology © 2005 - 2010 JATIT& LLS

[31] KaziChandrima Rahman, "A Survey On Sensor Network" , ISSN 2218-5224, Vol. 01,ISSUE 01, published in 2010