Analysis Of Wireless Sensor Networks (Wsns) And Routing Issues

P. R. Gundalwar
Asst. Professor, Smt. Bhagwati Chaturvedi College Of Engineering, Nagpur (MS), INDIA

Dr. V. N. Chavan
Professor, S. K. Porwal College, Kamptee, Nagpur (MS), INDIA

Abstract:

In recent years there has been observed a high demand in Wireless Sensor Networks (WSNs). WSNs are an enabling technology with the potential to revolutionize information and communication technology. This paper provides an overview of basic concepts on WSNs such as wireless network types: infrastructure based and infrastructure less, components of WSN node, motivation for Mobile Adhoc Network, OSI/RM, various topology, and routing etc. One must understand different designing issues for developing new routing techniques applicable exclusively for WSNs. This paper highlights a few number of routing issues in WSNs related with data, network, hardware/operating system, fault-tolerance, security, Quality-of-Service etc.

1 Introduction

The history of wireless networks started in the 1970s and the interest has been growing ever since. At present, sharing of information is vital and difficult too as the users need to perform administrative tasks and set up static, bidirectional links between the computers. Wireless Sensor Networks (WSNs) are rapidly emerging as an important new area in wireless and mobile computing research. Wireless networks can be broadly classified into two types: Infrastructure based and infrastructure less networks [1]. The first category is supposed to use some sort of means to establish communication after permission is granted, and the other without any means and permission grant system. This is shown in Figure 1. Today's need for accepting challenges in electronics and telecommunication disciplines is how to use effectively the existing infrastructure based and infrastructure less network for making every human being safety and reliable.

WSNs is an ad hoc wireless networks collection of wireless nodes forming temporary network. Due to the mobility of nodes, the status of a communication link is a function of the location and transmission power of the source and destination nodes and the channel interface from other links. WSNs consists of a large number of densely deployed miniature disposable sensor nodes in the region of interest to monitor and capture physical environmental conditions like temperature, humanity, pressure etc transmit environmental data in multi hop manner to the base station node or sink for further processing through a wireless link.

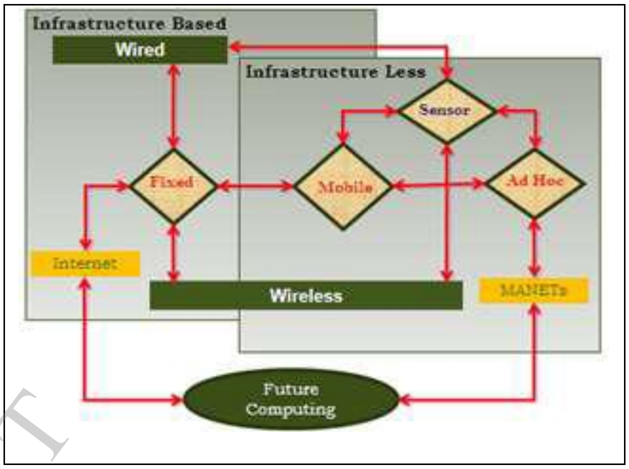

Figure1. Type of Wireless networks

Wireless sensor nodes are tiny light weighted sensing devices. Due to recent technological advances, the manufacturing of small and low cost sensors became technically and economically feasible. A large number of these disposable sensors can be networked in many applications that require unattended operations. A WSN contain hundreds or thousands of these sensor nodes. These sensors have the ability to communicate either among each other or directly to an external Base-Station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy.

Each sensor node comprises sensing, processing, transmission, mobilizer, position finding system, and power units [6]. This is shown in Figure 2.

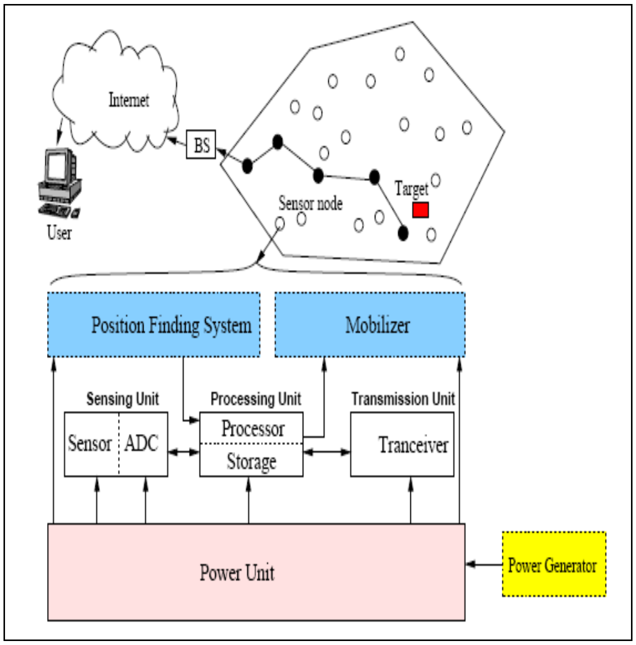

Figure 2. Components of WSN node

2. Mobile Ad Hoc Network

Wireless networks motivated the construction of temporary networks with no wires, no communication infrastructure and no communication intervention. Such interconnection between mobile computers emerged as Ad hoc Network and gradually referred as Mobile Ad Hoc Networks (MANET). MANET has several characteristics like dynamic topology, bandwidth constraints, energy-constrained operation, limited physical security etc. Therefore, the routing algorithms are difficult to formalize mathematically, instead they are tested using extensive simulation. A MANET topology can be defined as a dynamic multi-hop graph G = (N,L), where N is a finite set of mobile nodes and L is a set of edges which represent wireless links. A link (i,j) Є L exists if and only if the distance between two mobile nodes (MNs) is less or equal than a fixed radius r as shown. This r represents the radio transmission range that depends on wireless channel characteristics including transmission power. Accordingly, the neighborhood of node x is defined by the set of nodes that are inside a circle (assume that MN are moving in a two-dimensional plane) with center at x and radius r, and it is denoted by:

$$Nr(x)=Nx=\{nf|d(x,nf) \leq r, x \neq nf, \square\ j \in N, j \leq |N| \}$$

where x is an arbitrary node in graph G and d is a distance function. A path i.e. route from node i to node j, denoted by Rij is a sequence of nodes Rij = (i,n1, n2,…,nk, j) where (i,n1), (nk,j) and (ny,ny+1) for $1 \leq y \leq k-1$ are links. A simple path from i to j is a sequence of nodes with no node being repeated more than once. Due to the mobility of the nodes, the set of paths i.e. wireless links between any pair of nodes and distances is changing over time. New links can be established and existing links can vanish [3].

3. Wireless Sensor Network

The basic issue of communication network is to securely transmission of messages for achieving both quantity of service and quality of service. The WSNs, generally used in one environment, but for data acquisition and data distribution, which can be managed and monitored by a common management center using large number of BS controller. This is used simultaneously in both the areas of diversified application like machine/industrial, building automation, vehicle monitoring, medical facilities, environmental/animal conservation, disaster management etc monitoring and allowing access via PDA, notebooks, cellular phones etc using various wireless communication technologies like Bluetooth, WiFi, cellular network, CDMA, GSM etc on 24x7 basis from any location of globe [2]. This is shown in Figure 3.

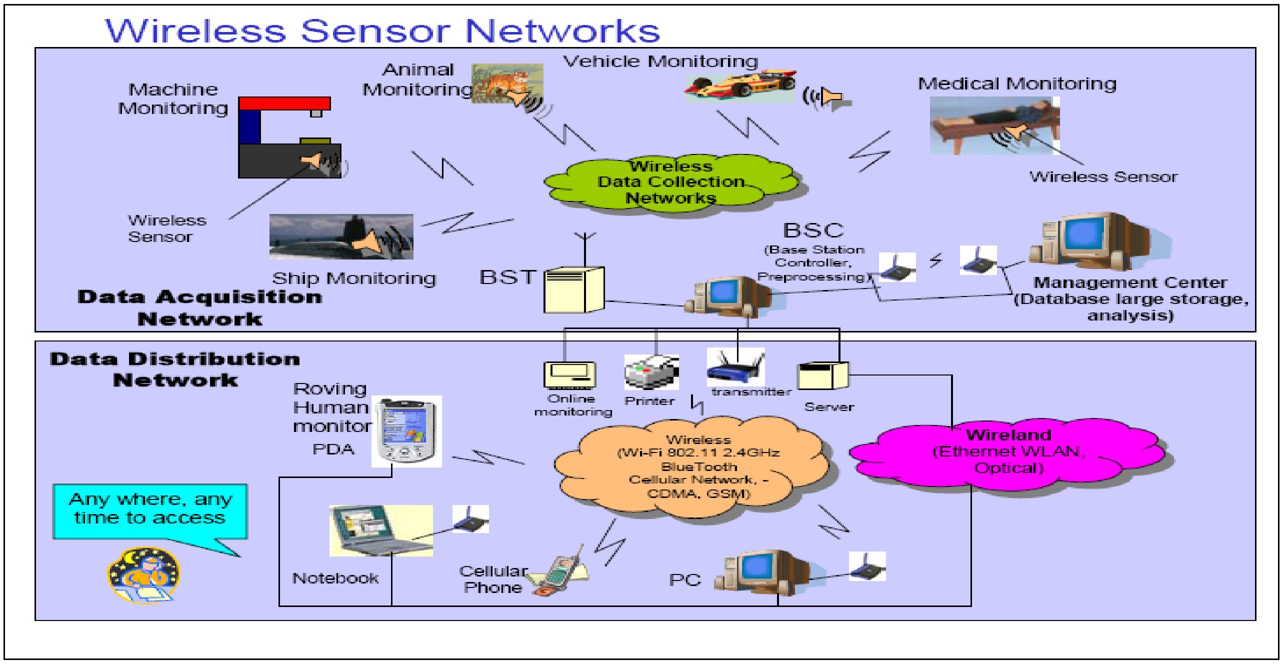

Figure 3: Scenario of WSN

4. Communication Network Essentials

To understand and be able to implement sensor networks, seveal basic sufficient primary concepts are required which are given below:

4.1 History and Recent developments

The Ethernet (Standard IEEE 802.3) was developed in the mid 1970's by Xerox, DEC, an Intel, and was standarized in 1979. It was officially adapted in 1995. Client-server networks became popular in the late 1980's with the replcement of large mainfrane computers by network of perssonal computers. In 1984 IBM introduced the 4 Mbit/s token ring (Standard IEEE 802.5) network. Peer-to-peer networking (P2P) architectures replaced by Peer-to-peer computing and has sparked a revolution for the Internet age and has obtained suceess in a very short time. IEEE ratified the IEEE 802.11 specification in 1997 as a standard for Wireless Local Area Network (WLAN), current verwsion supports transmission upto 11 Mbit/s. WiFi is useful , fast and esay network within the budget and capbility of small organization. Bluetooth was initiated in 1998 and standarized by the IEEE as Wirless Personal Area Network (WPAN) specifiaction IEEE 802.15 Bluetooth is a short range RF technology aimed at facilitating communication of electronic devices between each other and with the Internet, allowing for data synchronization that is transparent to the user. Supported devices include PCs, laptops, printers, joysticks, keyboards, mice, cell phones, PDAs, and consumer products. Mobile devices are also supported. Home RF was initiated in 1998 and has similar goals to Bluetooth for WPAN. Its goal is shared data/voice transmission. It interfaces with the Internet as well as the Public Switched Telephone Network. It uses the 2.4 GHz band and has a range of 50 m, suitable for home and yard. A maximum of 127 nodes can be accommodated in a single network. IrDA is a WPAN technology that has a short-range, narrow-transmission-angle beam suitable for aiming and selective reception of signals.

4.2 Open System Interconnection Reference Model (OSI/RM)

The OSI/RM computer network architecture delineates the basic functionality and services are offered by all seven layers of OSI RM to be interlinking heterogeneous computer systems toward accomplishing useful communication among several application procedures [2],[4]. This is shown in Figure 4. It specifies the relation between messasges transmitted in a communication network and application program run by the uses. Each layer is self contained , so that it can be modified without unduly affecting the seven layers.

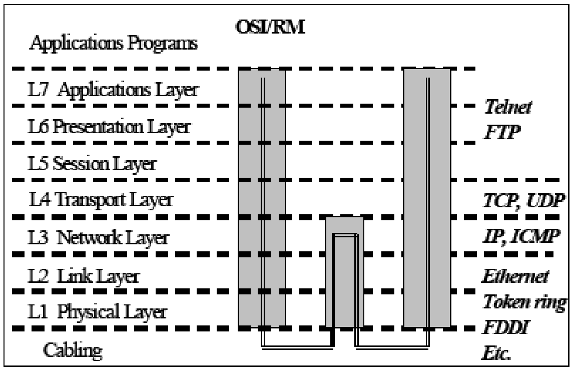

Figure 4. Open System Interconnection Reference Model

4.3 Basic Network Topology

The basic topologies include fully connected, mesh, star, ring, tree, bus which are shown in Figure 5. A single network may consists of several interconnected subnets of different topologies. Network are further classified as Local Area Networks (LAN), Wide Area Networks (WAN) etc. depending on geographical dimensions and other parameters [2].

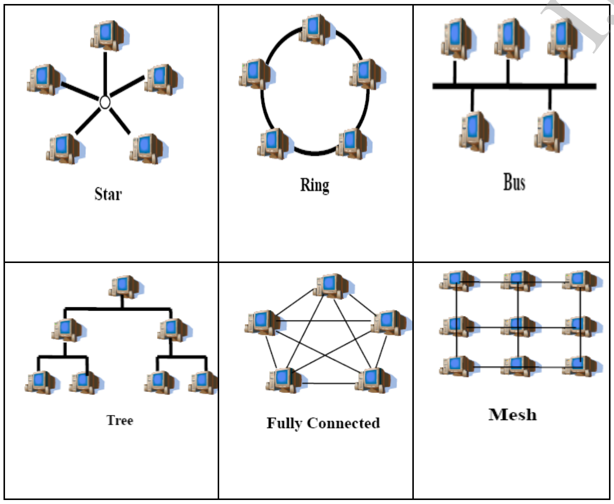

Figure 5: Basic Network Topologies

4.4 Routing

WSNs may require novel routing techniques for scalable and robust data dissemination. One of such routing techniqe from network structure based protocols category is Directed diffusion which incorporates data-centric routing coupled with application-specific in-network processing. Such techniques can help establish energy-efficient data dissemination paths between sources (sensors) and sinks (data processing or human interface devices). In addition, directed diffusion allows the design of localized algorithms for flexible path construction and recovery, enabling these systems to be robust to dynamics[5].

5. Routing Issues in WSNs

Design of routing protocols in WSNs is influenced by many burning issues. These issues must be resolved before efficient degree of communication can be achieved in WSNs. Following are some routing issues that affect routing mehcanisms in WSNs. The objective is that WSN must carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation.

5.1 Hardware and Operating System

Wireless sensor networks are composed of hundreds of thousands of tiny devices called Sensor Nodes (SNs). A SN is often abbreviated as a node. A Sensor is a device which senses the information and passes the same on to a mote. Sensors are used to measure the changes to physical environment parametr. A Mote consists of processor, memory, battery, A/D converter for connecting to a sensor and a radio transmitter for forming an ad hoc network. A Mote and Sensor together form a SN. The hardware of the SN and complete set of SN is as shown in Figure 6. There can be different sensors for different purposes mounted on a Mote. Motes are also sometimes referred to as Smart Dust. A SN forms a basic unit of the sensor network. The most preferable Operating Systems (OS) for SN are like TinyOS, Mantis Operating System, Nano-Qplus etc.

The various issues in designing an OS for sensor networks are (i) An OS for SNs should be hardware independent and application specific. (ii) It should support multihop routing and simple user level networking abstractions. (iii) It should have inbuilt features to reduce the consumption of battery energy. (iv) It should have an easy programming paradigm (v) Application developers should be able to concentrate on their application logic instead of being concerned with the low level hardware issues like scheduling, preempting and networking [8].

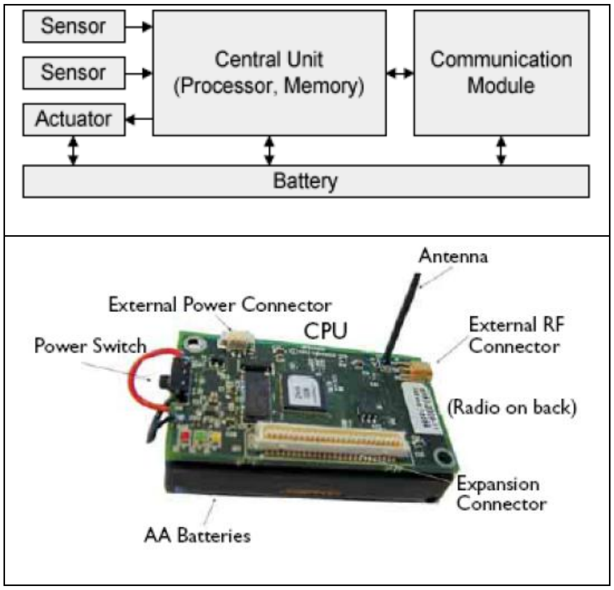

Figure 6: Hardware of SN and comlete set

5.2 Node Deployment

Node deployment in WSNs is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation. Inter-sensor communication is normally within short transmission ranges due to energy and bandwidth limitations. Therefore, it is most likely that a route will consist of multiple wireless hops.

Research has predominantly assumed that SNs are powered by a portable and limited energy source, viz., batteries. Once a sensor's power supply is exhausted, it can no longer fulfill its role unless the source of energy is replenished. Therefore, it is generally accepted that the usefulness of a wireless sensor expires when its battery runs out. Rapid technological progress has made available low-cost sensors and communication networks which led to the development of various other potential WSN applications. The solution suggested for this problem is to use harvested power supply to produce ambient energy e.g. solar, thermal, vibrational, wind, RF etc [1],[6],[7].

5.3 Energy Consumption

SNs can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy-conserving forms of communication and computation are essential. SN lifetime shows a strong dependence on the battery lifetime. In a multihop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some SNs due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network [1],[6].

5.4 Data Reporting Model

Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. Data reporting can be categorized as either time-driven i.e.continuous, event-driven, query-driven, and hybrid. The time-driven delivery model is suitable for applications that require periodic data monitoring. As such, SNs will periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest at constant periodic time intervals. In event-driven and query-driven models, SNs react immediately to sudden and drastic changes in the value of a sensed attribute due to the occurrence of a certain event or a query is generated by the BS. As such, these are well suited for time critical applications. A combination of the previous models is also possible[6].

5.5 Data Aggregation

Since SNs may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced. Data aggregation is the combination of data from different sources according to a certain aggregation function, e.g., duplicate suppression, minima, maxima and average. This technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols. Signal processing methods can be used for data aggregation [6].

5.6 Fault Tolerance

A failure or bloked state of SN may be resulted due to lack of power, physical damage, or environmental interference. It should not be propogated among other SNs wchich can affect the whole sensor network. If many SNs fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection BSs. Therefore, multiple levels of redundancy may be needed in a fault tolerant sensor network [5],[6].

5.7 Clock Synchronization

Clock synchronization is an important service in sensor networks. Time Synchronization in a sensor network aims to
provide a common timescale for local clocks of nodes in the network. A global clock in a sensor system will help process and analyze the data correctly and predict future system
behavior. A clock synchronization service for a sensor network has to meet challenges that are substantially different from those in infrastructure based networks [8].

5.8 Node/Link Heterogeneity

A SN can have different role or capability in terms of computation, communication, and power. The existence of heterogeneous set of sensors raises many technical issues related to data routing. Any sensor can be either deployed independently or the different functionalities can be included in the same SNs. Even data reading and reporting can be generated from these sensors at different rates, subject to diverse quality of service constraints, and can follow multiple data reporting models. The hierarchical protocols designate a clusterhead node different from the normal sensors. These clusterheads can be chosen from the deployed sensors or can be more powerful than other sensor nodes in terms of energy, bandwidth, and memory. Hence, the burden of transmission to the BS is handled by the set of clusterhead nodes [1],[7].

5.9 Scalability

The number of SNs deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of SNs. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality [6].

5.10 Coverage

In WSNs, each sensor node obtains a certain view of the environment. A given sensor's view of the environment is limited both in range and in accuracy; it can only cover a limited physical area of the environment. Hence, area coverage is also an important design parameter in WSNs [6].

5.11 Connectivity

High node density in sensor networks precludes them from being completely isolated from each other. Therefore, SNs are expected to be highly connected. This, however, may not prevent the network topology from being variable and the network size from being shrinking due to SN failures. In addition, connectivity depends on the, possibly random, distribution of nodes [6].

5.12 Network Dynamics

Most of the network architectures assume that SNs are stationary. However, mobility of both BSs or SNs is sometimes necessary in many applications . Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the BS [6].

5.13 Transmission Media

In a multi-hop sensor network, communicating nodes are linked by a wireless medium. In general, the required bandwidth of sensor data will be low, on the order of 1-100 kb/s. Related to the transmission media is the design of Medium access control (MAC). One approach of MAC design for sensor networks is to use TDMA based protocols that conserve more energy compared to contention based protocols like CSMA (e.g., IEEE 802.11). Bluetooth technology can also be used [6].

5.14 Quality of Service

In some applications, data should be very quickly accessed over the specified time, immediately after sensed, otherwise the data will be useless. Therefore, this is important for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime [6],[8].

5.15 Security

Security in WSNs is very important. Security in a sensor network is very challenging as WSN is not only being deployed in battlefield applications but also for surveillance. Different types of threats in sensor networks are Spoofing and altering the routing information, passive information gathering, node subversion, sinkhole attacks, Denial of service attack and jamming [8].

Conclusion

The growth of Internet has been phenomenal especially in the last two decades, far surpassing its original objective of providing connectivity to computers that support end user applications and information sharing. WSNs are responsible for increasing use of smart devices that interact directly with the physical world are added to the Internet turning it into a pervasive network.

Although many of previous research work focused on routing techniques, there are still many challenges that need to be solved in WSNs. We explored those burning issues that are actually challenges which must be considered for designing an algorithm for routing in WSNs. Our next work will pinpoint on different routing techniques based on these issues.

References

[1] A. K. Dwivedi, O. P. Vyas, “Network Layer Protocols for Wireless Sensor Networks: Existing Classifications and Design Challenges”, International Journal of Computer Applications (0975– 8887)Volume 8– No.12, October 2010

[2] F. L. LEWIS, Wireless Sensor Networks, Smart Environments: Technologies, Protocols, and Applications, ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004.

[3] Anuj K. Gupta, Dr. Harsh Sadawarti, Dr. Anil K. Verma, “Performance analysis of AODV, DSR & TORA Routing Protocols”, IACSIT International Journal of Enginerring and Technology, Vol.2,No.2,April 2010

[4] Ram Kr. Singh,Amit Asthana, “Traffic Flow Confidentiality Security Service in OSI Computer Network Architecture”, VSRD-IJCSIT, Vol. 1 (10), 2011, 744-749

[5] Deepak Ganesan, Ramesh Govindan, Scott Shenker, and Deborah Estrin, “Highly-Resilient, Energy-Ef_cient Multipath Routing in Wireless Sensor Networks ” Mobile Computing and Communications Review, Volume 1, Number 2

[6] Jamal N. Al-Karaki Ahmed E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey”, ICUBE initiative of Iowa State University, Ames, IA 50011.

[7] Winston K.G. Seah, and Alvin T.S. Chan “Challenges in Protocol Design for Wireless Sensor Networks Powered by Ambient Energy”, http://ecs.victoria.ac.nz/twiki/pub/Main/TechnicalReportSeries/ECSTR11-02.pdf.

[8] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H , Subir Kumar Sarkar, “Issues in Wireless Sensor Networks”, Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.