# Wireless Sensor Network –A Survey

Nirvika Chouhan[1], P.D.Vyavahare[2], Rekha Jain[3]
[1]M.E. Student, [2] Professor, [3]Assistant Professor
Department of Electronics & Telecommunication Engineering
Shri G.S. Institute of Technology and Science
Indore, India
[1]c_nirvika@yahoo.com, [2] prakashvyavahare@gmail.com, [3]rjain_me@yahoo.co.in

***Abstract*—Wireless sensor networks are the networks consisting of large number of small and tiny sensor nodes. The nodes are supplied with limited power, memory and other resources and perform in-network processing. In this paper, various issues are discussed that actually put the limitations in the well working and the life time of the network. In Wireless sensor network, nodes should consume less power, memory and so data aggregation should be performed. Security is another aspect which should be present in the network. Quality of service, routing, medium access schemes all are considered in designing the protocols.**

***Keywords— Wireless Sensor Network, In-network processing, Security, Data aggregation, Power Consumption.***

## I. INTRODUCTION

Wireless sensor network is a network consisting of large number of sensor nodes deployed in the particular region to sense and monitor the physical phenomena like temperature, humidity, pressure and so on. The sensors then process and communicate the sensed data and all together pass it to the head node, called Sink.

The following are the main characteristics of wireless sensor network-

- Wireless sensor network can perform its operation very well even in the remote environment without any human presence. They have the ability to withstand harsh environmental condition.
- The networks are designed so that they posses self-organizing and self-healing capabilities.
- Additional nodes can be placed at any time to replace any malfunctioning node or due to changes in the task to be done.
- Sensor nodes are very small, simple and are easy to use.
- Topology of sensor network does not remain same. It keeps on changing.
- ***In-network processing***- The main and unique feature of wireless sensor network is that it performs in-network processing. Data is processed not only when it completely reaches the sink, but instead along its way, when it is forwarded from one node to another i.e. hop by hop .It enables reduced packet transmission to the sink as data is processed earlier. Apart from reducing the burden of processing in sink node, it also provides the facility like data aggregation in each node, which helps in less consumption of the power, memory, energy in the entire network and thus having the larger lifetime of the network.
  Thus we can say that wireless sensor network possesses data-centric multi-hop communication and is different from the traditional route-centric multi-hop communication.

The important constraints in wireless sensor network are power, memory, computational resources, and bandwidth. Since nodes are supplied with the limited, irreplaceable power source, it is always required that they should consume as much low power as possible so as to have long life of network.
Also, nodes are very close to each other, so multi-hop communication is expected to consume less power than the single hop communication.
All the networks aim to achieve high Quality of Service but all of them provide it at the cost of high power consumption. But still, protocols should emphasize more on power conservation. Therefore all the protocols that are implemented should satisfy this particular condition.

## II. APPLICATIONS

The following are the main applications regions of wireless senor network-

- The simplest application includes the measurement and monitoring of physical phenomenon like temperature, pressure, humidity etc.
- *Area Monitoring*- The sensors are placed in the region to be monitored like in detecting the movement of vehicles.
- *Environmental sensing*- This includes the measurement of harmful gases in the atmosphere; to detect the forest fire by measuring temperature, humidity and gases which are produced which are produced by fire in trees or vegetation. Even the slight movements of soil can be detected.

- *Defense and Military Application*- In military they are used to monitor if there is any illegal entry of any person, arms etc. Network can be deployed in target area to gather the battle damage assessment data and also to watch for the activities of the opposing forces.
- *Societal Application*-It includes movement of school going children; allow end users to handle and manage home devices and appliances locally and remotely; tracking and doctors and patients inside a hospital etc.
- *Industrial monitoring*- Includes machine health monitoring and based on that maintenance is done. Also includes data logging which includes collection of data to monitor the environment condition like level of water in tank in nuclear plant to see well working of the system.

## III. DIFFERENCE FROM MANET

Even though wireless sensor network is considered as an ad-hoc network, but it is quite different from mobile ad-hoc network (MANET). And also the protocols that are used in the MANET cannot be used in the wireless sensor network.

Differences in both the network lie in the facts below-

- MANETs are usually close to humans, in the sense that most of the nodes in the network are the devices that are meant to be used by human beings (e.g., laptop computer, mobile radio terminals, etc.); conversely, wireless sensor networks do not focus on human interaction but instead focus on interaction with the environment.
- The number of nodes as well as density of deployment in the wireless sensor network are much larger than the ad-hoc network and may increase according to the applications. Thus sensor network requires different and more scalable solutions.
- The network size in case of MANET depends on the number of active users present in the deployment area. But in sensor network the number of nodes depends upon the extension of observed area, characteristics of node and on required redundancy.
- The traffic in MANET is generally higher owing to the use of well known service like Web, mail, video etc. But, the data rate of sensor network is very low owing to the interaction with the environment.
- Sensor nodes are deployed once in their life time and are stationary, except for the few nodes but, nodes in MANET move in an ad-hoc manner.
- Both the networks are designed for the self configuration but there solutions are different. Wireless sensor network has limited power and recharge is practically impossible. Therefore energy consumption is very important parameter to be considered in sensor network as compared to MANET.
- The QoS services in MANET are determined by the traditional applications but for sensor network entirely new QoS services are required which also takes the energy constraint into account.
- Sensor networks are application specific. We cannot have the solution that fits for all the problems.
- Nodes in sensor networks are small and power limited as compared to MANET. So, communicating and computing software should be of less size and more energy efficient than that of being used in MANET.

## IV. VARIOUS ISSUES

The following are the various issues which affect the design and performance of wireless sensor network-

- Power consumption
- Security
- Data aggregation
- Routing
- Quality of Service

### *A.* ***Power Consumption***

Since sensor nodes are very small in size so they are equipped with limited power source. They are generally run with batteries and in some scenarios it is practically impossible to replace power source. Therefore methods and algorithms should be made to have as much low power consumption as possible so that for the same power a sensor node can live for more time.

In wireless sensor network power, conservation and power management take on the additional importance and researchers are focusing to design power aware algorithms and protocols.

Since there are three main tasks of sensor node, power consumption is divided into three domains-

- *Sensing*- Sensing power depends upon the nature of application. Continuously monitoring requires more power than the time to time monitoring.
- *Communication*- Sensor node expends maximum power in the data communication. The components of receiver and transmitter consume the valuable power. Also the power required to make the transmitter on is also taken into consideration as it makes up the noteworthy affect on total power consumption.
- *Data processing*- Energy expenditure in this is less then communication but still taken into consideration.

The solutions can be provided either at hardware level or software level.
At *hardware level*, it is possible to add solar cell or scavenge energy from motion of winds. Improved batteries and microcontrollers are used. Most hardware level provides the multiple power saving states- ON, OFF, IDLE for each component of the device so that they remain active at a particular time, only when required.

- At *software level* , solutions are targeted as-

i) *Minimizing Communication*

Minimizing number of messages is a cross cutting solution. With good MAC protocol, routing algorithm, number of messages to be transmitted gets reduced and thus the power consumption.

ii) *Creating sleep/wake up schedules for nodes or particular components of nodes.*

Solutions to schedule sleep/wake-up patterns vary considerably. Many solutions attempt to keep awake the minimum number of nodes, called sentries, to provide the required sensing coverage while permitting all the others to sleep. To balance energy consumption a rotation is performed periodically where new sentries are selected for the next period of time.

So whatever implementation is done in wireless sensor network, power management is the prime concerned i.e. low power consumption should be there. For this, hardware and software solutions must be provided.

### *B.* ***Security***

Security is an aspect which is required in both wired and wireless network. However in wireless sensor networks, it is more important as their unique characteristics and purposes of the application, that they serve, make them attractive to intruders or attackers.

The following are the security properties which is required by sensor network-

a) *Authentication*- It is very important for receiver to make sure that the data, which it is using in the processing, originates from the correct source. Thus data authentication allows receiver to verify that data was sent from the claimed source only.
b) *Confidentiality*- Information should be revealed only to the authorized or intended entities. Other should not be able to get it from reading the memory or from eavesdropping.
c) *Data integrity*- It ensures that there is no manipulation, no alteration, and no damage in the received data during transmission.
d) *Availability*- This security mechanism ensures that the network and its applications are able to perform their tasks any time without interruption.
e) *Key establishment*- For sensor-to-sensor key establishment, a shared key is established by two communication nodes to protect communications. Thus, all sensed data transmitted between participants could be verified and protected even if an attacker eavesdrops on the communications between nodes or injects illegal sensed data into networks.This requirement still provides an adequate level of security.

The sensor nodes are prone to several attacks which can disturb the entire function of the network. The different types of attacks are-

a) *Sybil Attack*- It is the type of attack in which the attacker claims to have several identities in the network. It is defined as a malicious device claim to be at several locations simultaneously so that if a node finds this device to be its neighbor, it can forward the data to this malicious device and so security is violated.
b) *Denial of service Attack*- The type of standard of denial of service attack on wireless sensor network is jamming the node or set of nodes. The jamming can be constant or intermittent. In constant jamming, the entire network is jammed and no messages are able to be sent or received. In intermittent jamming, nodes are able to exchange messages periodically but not consistently.
c) *Physical Attack*- In this, sensors are destroyed permanently so the losses are irreversible. The attacker can extract the cryptographic secrets, modify the programming in sensors or replace them with the malicious nodes which are under the control of them.
d) *Node Replication*- In this, an attacker adds a node in the existing network by replicating or copying the existing node's ID .This replicated node can disrupt the network's behavior in the sense that they can change the routing, corrupt the packets. The attacker can even copy the cryptographic key to the replicated sensor if he has access to the entire network.
e) *Traffic analysis Attack*- this consists of monitoring the transmission and listening to the data. An increase in the number of transmitted packets between certain nodes give the signal that specific sensor has registered activity.

Keeping in mind all types of attacks, the encryption algorithm should be made and also following considerations are taken-

- Node Capture- The network infrastructure is made up of small, low cost nodes and is distributed over the hostile region. It is often impossible to prevent the physical attack of intruders on node also referred to *node capture*. It is reasonable to assume that an attacker can have full control on captured node i.e. it can read the

memory and influence its operation. So special secure memory devices would be needed to prevent this access. However it is rarely present in the cheap sensor node.

- For implementing the cryptographic algorithms, memory and computational capabilities are serious obstacles. For this reason, asymmetric key cryptography is considered to be too heavy to implement. So algorithms should be light weighted and consume less resources.
- Even in the end to end information transfer, there are involvements of the intermediate nodes or we can say the large no of parties that can access and modify the data.
- Limited energy constraint in the nodes make easy for the intruder to exhaust energy budget and let the nodes die.

To provide security, public key approach cannot be used in this network as this is quite heavy and computationally very expensive. Symmetric key cryptography can be used as this is much more energy and resource efficient. RSA and Elliptic Curve cryptography can be used but there arises the problem of the key distribution. So whatever protocol and encryption algorithm is designed, it should be light weight, more efficient and even resolve the problem of key distribution.

### *C.* ***Data Aggregation***

Wireless sensor network consists of a number of nodes that sense the data from environment process it and then communicate it to the sink or base station. The frequency of reporting the data depends on the application. It may be possible that many of the nodes sense the same or co-related data. It may also happen that the sensed data consists of much redundant information. So, instead of sending same type of data and irrelevant data to the base, some common, useful or some summarized form of the data is transmitted. This will have a huge advantage of power savings and communication cost saving.

All this can be achieved by data aggregation. *Data Aggregation* is the systematic collection of most critical data from the sensors nodes and makes it available to the sink in energy efficient manner with minimum delay latency. Thus the main goal of data aggregation is to enhance the lifetime of the sensor network.

Data aggregation thus –

- Improves bandwidth utilization
- Improves energy utilization
- Improves processor utilization
- Improves network lifetime
- Ensures end to end privacy

But data aggregation may not be useful in every scenario. It depends upon in which we are more concerned – to the quality of service or power consumption. It sometimes degrades the QoS metrics in wireless sensor network, which we require. This can be explained in following points-

- *Accuracy*-It is most important metric as most of the applications demand this. Since not all the data is transmitted to the sink node, there is always some difference between resulting value at sink and the true value.
- *Latency*- Data aggregation increases the latency as nodes have to wait for the data to come from others.
- *Bandwidth Utilization*-When data aggregation is used along a single path, bandwidth is utilized properly. However, when aggregation is carried out in multiple parallel paths, the delay may be reduced but use of bandwidth increases.

These show the tradeoff existing between data aggregation and energy efficiency, data accuracy and with other quality of services. Hence, protocols are designed keeping in mind all the issues.

Some protocols are Power Efficient Gathering in Sensor Information Systems (PEGASIS), Low Energy Adaptive Clustering Hierarchy (LEACH), Power Efficient Data gathering and Aggregation protocol (PEDAP).

### *D.* ***Routing***

Once the data is collected by a node, it is very important to find out how the data has to be travel from one node to other node in order to reach the sink node. The path may be single hop where there is direct communication with sink node.

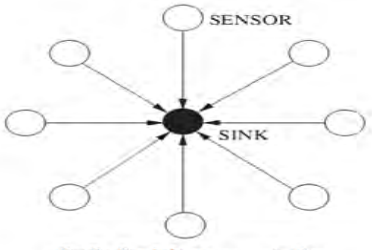


Fig B : Single hop communication

But practically wireless sensor network performs multi hop communication where the data has to pass through so many nodes to reach the sink node.

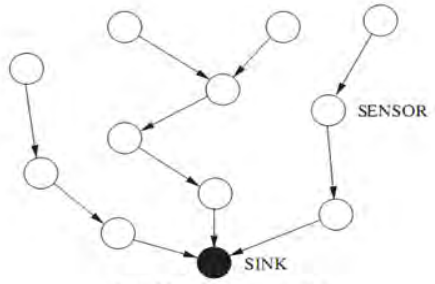

Fig C: Multi-Hop communication

The designing of the path travelled i.e. routing protocol is major issue. The following are the criteria which a routing protocol in sensor network must satisfy-

- *Energy efficient*- It is one of the most important criteria. Routing protocol should be such that it eliminates the energy inefficiencies and increases the life time of the network as we have seen all the sensor nodes have limited power in them. So protocols should consume less power in relaying data from sensor nodes to sink so the life time of the network is optimized.
- *Multi path design technique*- Routing protocols should incorporate multipath design technique. Multi path is referred to those protocols which provide multiple paths so that a path among them can be used when the primary path fails.
- *Fault tolerance* - Whenever any path break is detected, path repair is desired. Fault tolerance is another desirable property of the routing protocol. Routing protocol should be able to find out new path even if some nodes fail or blocked due to some environmental interference.
- *Reduce Redundancy*- Since it is possible that multiple sensors generate same data, there may be traffic generation and this will have significant redundancy among individual sensor node. Routing protocol should thus reduce such redundancy to improve energy and bandwidth utilization.
- *Scalability*- As wireless sensor network consists of large number of nodes, so routing protocol should work with this huge number of nodes.
- *Node heterogeneity*- Routing protocol should take care of the heterogeneous nature of the nodes, i.e. each will be different in terms of computation, power, and communication.
- *Quality of service*- It refers to various aspects or parameters which are actually used for measurement of performance in network including end to end delay, throughput, variations in delay The network application always ensure the quality of service which depends on the applications. Routing protocol should be designed to fulfill the different aspects according to the application and provide QoS.
- *Mobility*- Routing protocol must be able to deal if message source or destination or both are moving.

Routing protocols like Sensor Protocol Information via Negotiation (SPIN), Gradient Based routing, Ad-Hoc on demand Distance Vector (AODV), Geocasting are used but still have some limitations.
The routing protocols developed, till now, try to fulfill all these requirements, but still dealing with the large number of nodes and topology change. These are considered along with most important energy efficiency. Routing protocol should allow easy communication between the sensor networks and the external world i.e. Internet.

### *E.* ***Quality of Service***

Quality of service (QoS) is the level of service which is provided to the users by sensor network. It is also defined as the optimum number of sensor nodes sending information to the sink. As the applications of wireless sensor network are getting vast like in military, the information obtained from the network is very important and has to be intact. It is therefore necessary to maintain quality of service in many of the applications.
Quality of service is characterized by minimum delay, maximum throughput, and bandwidth utilization.
Various Quality of service issues in wireless sensor network are-

- Nodes in the wireless sensor network may join, leave and rejoin and links may be broken at any time. So maintaining and re-establishing the path and path information are big deals and hence affect the QoS routing algorithm.
- Traffic is not uniform in wireless sensor network as data aggregation occurs in many nodes. So, QoS mechanism should be able to deal with this unbalance traffic.
- Many times energy efficiency has to be sacrificed to meet the delivery requirements. Though multi-hop reduces energy consumption, overhead associated with the data collection slow down the speed of packet delivery.

- Wireless sensor network needs to be supplied with the sufficient bandwidth to achieve the minimal required QoS.
- In routing, buffering of packets is advantageous. But in multi-hop large amount of data need to be buffered. This much of buffer size actually increases the delay variations and is difficult to meet the QoS requirement.

QoS models are therefore designed application specific, to be able to support heterogeneous nature of nodes and to minimize tradeoffs.

## V. OPERATING SYSTEM

The operating system in the wireless sensor network is the layer of the software between the node's hardware and application. It provides the environment for programming to application developer. Its main functions include controlling and protecting the access to the resources, managing allocation to the users.

There are many operating systems that can be used in wireless sensor network –TinyOS, Sensor operating System (SOS), Contiki, Nano-RK, LiteOS.

We have many simulators available for sensor networks. The most popular are TOSSIM, NS-2, J-SIM, OPNET, GLOMOSIM, Qualnet and so on. TOSSIM is a simulator for TinyOS. One can directly compile the programs into TOSSIM instead of compiling TinyOS application for a mote. The languages that can be used for programming are – nesC, C and Lab VIEW.

## VI. CONCLUSION

Wireless sensor networks have large number of small sized and power limited nodes. Its flexibility, low cost deployment, in-network processing and other important characteristics find its applications in wide range of fields. The impact of this being the energy consumption, this network is having a large network on our day to day life is very much noticeable. Main being the energy consumption, this network is having a large number of other issues and challenges associated with them. All of these need to be overcome and researches are being made so as to have desirable results in more efficient way.

## REFERENCES


[1] I.F. Akyildiz, W. Su and Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey", *Elsevier Computer Network*, vol.38, pp. 393-422,March 2002.

[2] Gowrishankar S , T.G. Basavaraju , Manjaiah D.H and Subir Kumar Sarkar, "Issues in Wireless Sensor Networks", *Proceedings of the World Congress on Engineering*, vol 1, pp.978-988, London, U.K. , July 2 - 4, 2008.

[3] Waltenegus Dargie & Christian Poellabauer, "Fundamentals of Wireless Sensor Networks", *John Wiley and Sons Ltd. Publication.*

[4] Holger Karl and Andreas Willig, "Protocols and Architectures for Wireless Sensor Networks", *John Wiley and Sons Ltd. Publication.*

[5] R. Rajagopalan and P.K. Varshney,"Data-aggregation techniques in sensor networks:A survey", *IEEE Communications Surveys and Tutorials*",vol 8, pp. 48- 63, 2006.

[6] Ilker Demirkol, Cem Ersoy, and Fatih Alagöz, Bogazici University; "MAC Protocols for Wireless Sensor Networks: A Survey", *IEEE Communications Magazine*, April 2006.

[7] Shio Ku Singh, M.P Singh, D.K Singh; "Routing protocols in wireless sensor networks-A survey", *IJCSES*, November 2010.

[8] Jia Guo, Jian'an Fang and Xuemin Chen, "Survey on secure data aggregation for Wireless sensor network", *IEEE Wireless Communications*, vol 10, pp. 138-143, July 10-12, 2011.

[9] Yun Zhou, Yuguang Fhang, Yanchao Zhang,"Securing Wireless Sensor Networks",*IEEE Communcation Survey*,Volume 10, No.3, 3rd Quarter 2008 .