Pragmatics of Wireless Sensor Networks

Rashmi Vashisth
Department of electronics and communication
AMITY School of Engineering and Technology
IP University, New Delhi, INDIA

Ajay Jangra
Department of computer science and engineering
University Institute of Engineering and Technology
Kurukshetra University, Kurukshetra. INDIA

Abstract—**Wireless sensor network composed of infrastructureless, small, low-power, low cost, dynamic nature, application oriented, and multihoping wireless nodes, design for the purpose of collecting information by environment sensing, processing and communication. Designing of these networks become more complicated due to deploy nodes characterstics, maintenance of database, security, authentication and its functioning in open environment. This paper presents a general overview of WSN in detail and covers its applications and vulnerable aspects of WSN.**

Keywords- Wireless sensor network, Architecture, power unit, WSN design challenges

I. INTRODUCTION

Wireless Sensor Networks which is a type of wireless network consist of small distributed self-organized autonomous devices using sensors to cooperatively monitor physical or environmental conditions, (such as vibration, motion, temperature, sound, and Pressure) and send information wirelessly. A WSN node mainly consists of four main parts: - ***Processing unit***- to convert the sensed information into electrical signal**,** ***Sensor***-sense the data from environment**,** ***Transceiver***- to transmit and receive the signal and most importantly, and ***Energy Source Unit***- to supply the sufficient energy to the sensor nodes Depending on usage purpose there may be additional components such as localization unit, energy producer, position changer etc. Due to low energy sources and bandwidth, transmission range of nodes is restricted with about approximately 30 meters. Thus, dense deployment of nodes is required for more reliable data transmission. The processing capacity of WSN nodes is also low both because of data processed by WSN nodes are too small and energy is limited. [2, 3, 4, 5, 8, 9, 12]

II. NODE CHARACTERISTICS

A. Dynamic Network Topology

Due to the deployment of nodes in the infrastructure less area as a result the network topology always changes due to the addition of new nodes, failure of nodes, and mobility. So, it is a very challenging task to maintain the topology of sensor network. Thus, the topology is responsible for affecting the sensor network characteristics such as latency, capacity, robustness, complexity and processing of data.

B. Node Types

In sensor network, on the basis of sensing range basically two type of set or group of node are exist- *homogeneous group of node and heterogeneous group of node*. A Group in which all nodes are identical and have same capability is known as homogeneous group of node. Example of homogeneous group is layered architecture. On the other hand, a group in which all the nodes are not identical and do not have same capability i.e. some node are more powerful than others. Example of heterogeneous group is cluster architecture in which node form a cluster head and gather data from less powerful node. [10]

C. Multi-hop

As large number of sensor are deploying in WSN, so it is not feasible for each node to reach the base-station. It may be require intermediate node to reach the base-station. Thus, the solution is multi-hop.

D. Small Size node

Sensor nodes are generally small in size where range of each node is restricted about 30m.Due to small size of node; energy is limited which makes processing capability low.

E. Application-oriented

Due to the wireless nature of sensor network, they are used in major variety of application such as military, environmental and health care etc. Nodes are deployed randomly and spanned depending upon the type of application used [9, 11, 12]

III. WSN ARCHITECTURE

A sensor node consists of mainly five components as shown in fig.1. The main components of a sensor node are power source, transceiver, microcontroller, external memory and one or more Sensors can be used. Basically node is divided into four major blocks where each block has specific functionality.

Power-- Power supply consists of 2 components – battery and AC-DC converter .The goal is to supply the power to the sensor nodes to monitor the environment. So it is necessary to extend the lifetime of sensor nodes by refining energy from environment. So, a MEMS system is proposed by *Amirtharajah* that extracts electric energy from vibrations Life of sensor node depends upon battery. So battery is the important component that must be distribute properly. Batteries can be dividing into primary and secondary i.e. rechargeable or non-rechargeable battery will use. Non-rechargeable battery is good solution since it has high density. A power management layer is connected with the power supply block to control the main resource of a sensor node and its energy level. The power management layer uses the knowledge about the battery's voltage slope to adapt dynamically the system performance.

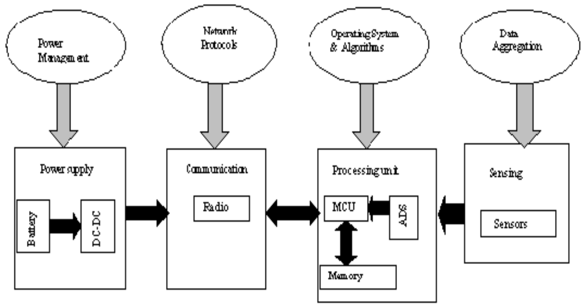


Figure 1 – shows the architecture of sensor node [15]

Communication- Communication is performed through communication channels. This phase provide some network protocol in order to perform communication. Three type of communication are discussed under this-optical, infrared, radio frequency (IR). ***RF (Radio-frequency)*** - It is based on electromagnetic waves. The main challenge in RF is size of antenna. In order to optimize communication, antenna must be at least λ/4, where λ is the wavelength of carrier frequency. Radio also plays an important role in power conservation. Because it has four operating mode- transmit, receive, idle, and sleep. In order to conserve power, it is necessary to shut down the radio when no needed since radios operating in idle mode take power equal to receive mode ***Processing Unit*** - It is responsible for collecting data from various source and then process, store and converting it. The central process unit of sensor node determines energy consumption and computational capabilities of a node. In order to provide the flexibility for CPU implementation, large number of micro-controller, microprocessor and FPGAS (field programmable gate arrays) are available. It provides flexibility for CPU implementation. FPGA can be reprogrammed and reconfigured so FPGA will be a good solution for sensor node monitoring with the development of ultra power FPGA has two disadvantages i.e. it can not reduce their energy consumption. Secondly, it is not feasible to make separate block for it. But it does not mean that it can not be used in sensor. In near future, if ultra-low power will be developed, it will eliminate the deployment cost due to reprogrammable and reconfigurable feature. MICROCONTROLLER not only consists of memory and processor but also non-volatile memory and interfaces. For saving of power, microcontroller should have three states-active, sleeps- idle. Low power X energy efficient is the capability of a device that consumes low energy per clock and energy efficient means a device that consumes low energy per instructions. ***Sensors -*** It helps in linking up the sensor nodes to the physical world and this block has a group of sensors and actuators that depend on the application of wireless sensor network. These nodes consist of several sensors and one can contains more than one sensor at the same time depending upon the application. There are different of sensors like acoustic sensor, resonant temperature sensor, magnetic field sensor etc. Each sensor has its specific functionality depending upon the application. [3, 4, 5, 13, 14, 15, 16]

IV. RELATED WIRELESS TECHNOLOGIES

A. 802.11 Wierless LAN

802.11 can be considered as wireless LAN in 1997. IT works in 2 modes: - infrastructure mode or Adhoc mode.

B. Bluetooth

It was initiated in 1998 and standardized by IEEE 802.15. It is a short range RF technology. Bluetooth supports a very short range i.e. approximately 10 meters and low bandwidth of 1-3 Mbps and designed for low-power network devices like handhelds. The low manufacturing cost of Bluetooth hardware makes it applicable or useful to the industry vendors but it is rarely used for general-purpose WLAN networking due to the low range and speed considerations.

C. Zigbee

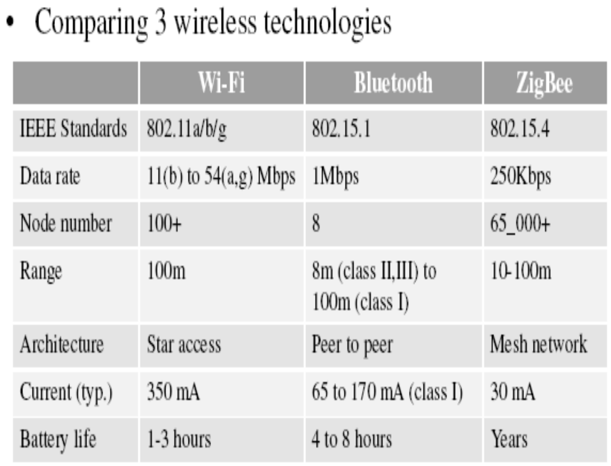
It was standardized by IEEE as wireless personal area network (WPAN) such as wireless headphones connecting with cell phones via short range radio.

D. Wi-Fi

WI- FI often used as a synonym for IEEE 802.11 technologies. Today IEEE 802.11 device is installed in many personal computers, video games and printers etc.

E. Wi-Max

The 802.16 standards are sometime referred to as "WI-MAX" (worldwide Interoperateability Microwave access), mobile "WI-MAX", "802.16d" and "802.16e". WI-MAX is a possible replacement candidate for cellular phone technology as GSM, CDMA or can be used as to increase capacity. It can be considered as a wireless technology for 2G, 3G and 4G networks in both developed and poor nation. [17, 18]



- Comparing 3 wireless technologies

	Wi-Fi	Bluetooth	ZigBee
IEEE Standards	802.11a/b/g	802.15.1	802.15.4
Data rate	11(b) to 54(a,g) Mbps	1Mbps	250Kbps
Node number	100+	8	65_000+
Range	100m	8m (class II,III) to 100m (class I)	10-100m
Architecture	Star access	Peer to peer	Mesh network
Current (typ.)	350 mA	65 to 170 mA (class I)	30 mA
Battery life	1-3 hours	4 to 8 hours	Years

V. DESIGN CHALLENGES

- *Fault tolerance* - Fault tolerance means to maintain sensor network functionalities without any interruption due to failure of sensor node because in sensor network every node have limited power of energy so the failure of single node doesn't effect the overall task of the sensor network. Adaptable protocols can establish new links in case of node failure or link congestion. Network can able to adapt by changing its connectivity in case of any fault. In that case, well- efficient routing algorithm is applied to change the overall configuration of network.
- I*nfrastructure*- Sensors network are infrastructure less in which nodes can communicate directly with base station. It utilizes multi-hop radio relaying and number of base station depends upon area covered by node and its radio range.
- *Real –time*- Achieving Real-time in WSN is difficult to maintain. It must support maximum bandwidth, minimum delay and several QOS parameters. This issue can affect time synchronization algorithm.
- *Dynamic changes*-As in sensor network nodes are deployed without any topology and they are adaptable to changes due to addition of new nodes or failure of nodes. Thus, unlike traditional networks, where the goal is to maximize the channel throughput or minimize the node deployment, but in a sensor network focus is to extend the system lifetime and the system robustness.
- *Power Consumption*- Wireless sensor node is microelectronic device means it is equipped with a limited number of power source. Nodes are dependent on battery for their power. Hence power conservation and power management is an important issue in wireless sensor network. Due to this reason researchers are focusing on the design of power aware protocols and algorithm for sensors network.
- *Quality of Service*- It means data should be delivered within time period. Some real time sensor applications are based on time means if data should not be delivered on time from the moment it is sensed; the data will become unusable for e.g. fire detection requires good quality of services.
- *Unattended operation*- In wireless sensor network, nodes is deployed randomly, without any topology. Once these nodes are deployed they don't require human intervention. Hence the nodes are responsible for reconfiguration in case of any modification i.e. addition of new nodes or failure of any node. Nodes are independent of each other so there maintenance needs to be autonomous.
- *Security*- Security is very important parameter in sensor network since sensor networks are data centric so there is no particular id associated with sensor nodes and attacker can easily inserted himself into the network and stole the important data by becoming the part of network without the knowledge of sensor nodes of the network. So it is difficult to identify whether the information is authenticated or not. [1, 4, 7, 8, 11, 12 19, 20, 21, 22,28]

VI. APPLICATION AREAS

Depending upon the requirement and characteristics of system, wide variety of applications are there which require constant monitoring and detection of specific event. *Military Applications*-Sensor networks are applied very successfully in the military sensing. WSN can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems, detection of mass destruction and explosion and enemy movement, Biological, nuclear and chemical attack detection reconnaissance and military situation Awareness. *Environmental Applications*- Nowadays sensor networks are also widely applied in habitat monitoring, agriculture research-include sensing of pesticide, soil moisture, PH levels, habitat Exploration of Animals, forest Fire and Flood detection, traffic control and ocean monitoring includes monitoring of fish.. *Health or Medical Applications*-Sensor networks are also widely used in health care such as monitoring patient physiological data such as blood pressure or heart rate, to control the drug administration, unconsciousness detection, exercise monitoring and non-invasive health monitoring. *Home Application*- Home application will step into our normal life in the future. In home application, sensor node can be embedded into furniture and home appliances, monitoring product quality, managing and monitoring inventory system and automatically control the temperature and airflow of the room. [5, 6, 14, 2, 20, 21, 23]

VII. SECURITY GOALS

As, wireless sensor network used in variety of applications so there must be provision for secure communication over sensor network. A large number of security issue exist in WSN as sensor network are used in mission critical environment such as military and healthcare application as these environment have demanding security requirement so in order to design appropriate security mechanism we consider some security goals that are:

A. Data confidentiality

Confidentiality is the ability of protecting message from passive attackers so that any message communicated through the sensor network remains confidential. This is the most important issue in network security. Establishing and maintaining confidential is extremely important when node identities and keys are being distributed to establish a secure communication channel among sensor node.

B. Data authentication

Authentication means that receiver should ensure that message come from right sender. Attacks in sensor network involve the alteration of packet but adversaries can insert fake packets. In other words, data authentication verifies or checks the identity of senders. Data authentication can be achieved through symmetric or asymmetric mechanism where sender and receiving nodes share secret key to compute the message authentication code but due to wireless nature of the media it is very difficult to ensure authentication.

C. *Data integrity*

Data integrity means to ensure the reliability of data that received data is not altered or changed while on network. [21, 26]

D. *Data availability*

It is of primary concern for maintaining an operational network. It determines whether a node has the availability to use the resources or whether network is available communicating. The failure of base station/cluster leader lead to failure of entire sensor network.

E. *Data freshness*

For determining the freshness of data a common method is used in which counter is added with every message that gives information about the freshness and staleness of the packet Data freshness is of 2 types:-Weak freshness and strong freshness. Weak freshness provides partial ordering but carries no information delay. Strong freshness provides total order on a request response pair and allow for delay estimation.

F. *Quality of service*

It means data should be delivered within time period. Some real time sensor applications are based on time means if data should not be delivered on time from the moment it is sensed; the data will become unusable for e.g. fire detection requires good quality of services**.** [5, 16, 24, 25, 26, 28, 29]

VIII. SECURITY ATTACKS

Sensor nodes are placed in a dangerous environment where they are not physically protected and because of the broadcast nature of the WSN it is more vulnerable to attacks of the WSN it is more vulnerable to attack**.** Basically there are 2 types of attacks in general. [19, 21, 24, 27, 28, 29]

A. *Passive attacks*

In this type of attack an unauthorized user or adversary monitor or listens the communication channel and collect the information, but does not modify the data this type of attack is known as ***passive attacks***. *Attacks against privacy:* Attacks against privacy falls under the category of passive attacks - Monitor & Eavesdropping, Traffic analysis, and Camouflage Adversaries

B. *Active attacks*

In this attack adversary listen, monitor or modify the data stream in the communication channel. The following are the active attacks. *Routing attacks* in sensor network- Spoofed, Altered and replayed routing information, Selective forwarding, Sinkhole attack, Sybil attack, Wormhole attack, Hello flood Attack. Other important type of attacks includes Denial of service attacks, Node Subversion, Node Malfunction, Node Outage, Physical attacks, Message Corruption, False Node, Node replication Attacks and Passive information gathering.

IX. CONCLUSION

This paper briefly discribe the functioning of wireless sensor network. Wireless sensor networks get huge popularity because of its wide range of applicaions areas and low desiging cost. Architectural design issues and related wireless technologies have been discussed. Performance and future of any network can be easy estimated by analyzing its security objectives and possible attacks. Although much work has been done in this direction and lot more is too required.

REFERENCES

[1] Pooja Sharma, Deepak Tyagi, Pawan Bhadana "A Study on Prolong the Lifetime of Wireless Sensor Network by Congestion Avoidance Techniques", Pooja Sharma et. al. /International Journal of Engineering and Technology Vol. 2(9), 2010, 4844-4849

[2] Chiara Buratti, Andrea Conti, Davide Dardari and Roberto Verdone"An Overview on Wireless Sensor Networks Technology and Evolution, *Sensors* 2009, *9*, 6869-6896; doi:10.3390/s9090686

[3] Pravin Shankar spravin@cs.rutgers.edu Rutgers University "Sensor Networks - A Survey"

[4] Archana Bharathidasan, Vijay Anand Sai Ponduru "Sensor Networks: An Overview"

[5] Kazi Chandrima Rahman "A Survey on Sensor Network", COPYRIGHT © 2010 JCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 01, ISSUE 01, MANUSCRIPT CODE: 100715

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

[7] Hetal Jasani, Kia Makki, Niki Pissinou, "On Wireless Sensor Networks" Second International Latin American and Caribbean Conference for Engineering and Technology "Challenges and Opportunities for Engineering Education, Research and Development" 2-4 June 2004, Miami, Florida, USA

[8] Neelam Srivastava "Challenges of Next-Generation Wireless Sensor Networks and its impact on Society", Journal of telecommunications, Volume1 , Issue in feb 2010

[9] Sasha Slijepcevic, Ranjit Iyer, Michael Panossian," A Survey of Wireless Sensor Networks"

[10] Kay Romer and Friedemann Mattern," The Design Space of Wireless Sensor Networks", partly supported by NCCR-MICS and centerly supported by Swiss science foundation under grant no.5005-67322, IEEE wireless communications.Dec 2004

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

[12] Raymond Mulligan, Habib M.Ammari :Coverage in Wireless Sensor Networks: A Survey"Network Protocols and Algorithms ISSN 1943-3581 2010, Vol. 2, No. 2

[13] Parveen Rentala, Ravi Musunuri, Shashidhar Gandhan Udit Saxena "Survey On sensor Networks", University Of Texas At Dallas, Richardson.

[14] I.F.Akyildiz, Y. SankaraSubramaniam, E. Cayirci "Wireless Sensor Network: A Survey", 2002 Published by Elsevier Science B.V.

[15] Marco Augusto M. Vieira, Claudionor, N. Coelho. JR. Diogenes Cecilio da Silva Junior, Jose M .Da Mata.

[16] T.Kavitha, D. Sridharan "Security Vulnerabilities in Wireless Sensor Network: A Survey", Journal of information Assurance and Security 5 (2010)031- 044

[17] http://www.webopedia.com/quick_ref/WLANStandards.asp

[18] http://compnetworking.about.com/cs/wireless/f/infrawireless.htm

[19] Thesis by Shriram Sharma "Energy-efficient Secure Routing in Wireless Sensor Networks

[20] Toh. C.K., 2002, "Ad-hoc Mobile Wireless Networks Protocols and Systems" , Prentice Hall, Inc

[21] Eiko Yoneki, Jean Becon," A Survey of Wireless Sensor Network Technologies: research trends and middleware's role", technical report published by university of Cambridge, September 2005

[22] Yi Qian and KejieLu, David Tipper, "A design for secure and survivable wireless sensor networks", IEEE Wireless Communications • October 2007

[23] Ying Miao, "Application of sensor networks", seminar on self-organization networks, Faculty of engineering Science, Delivered on Monday 02-05-2005

[24] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary "Wireless Sensor Network Security: A Survey", 2006 Auerbach Publications, CRC Press

[25] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti "A Survey on Wireless Sensor Networks Security", SETIT 2007 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications March 25-29, 2007 – TUNISIA

[26] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, “A Survey of Attacks, Security echanisms and Challenges in Wireless Sensor Networks”(IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009

[27] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti “A Survey on Wireless Sensor Networks Security”, SETIT 2007 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications March 25-29, 2007 – TUNISIA.

[28] Ajay Jangra, Rajesh Verma, Priyanka “Designing Robust Hybrid Wireless Sensor Network: Dual Technology Aspect” in International Journal of Computer Science and Technology (IJCSET) Volume 1. Issue 4. December, 2010. Londom UK

[29] Ajay Jangra, Swati, Richa, Priyanka “Wireless Sensor Network (WSN): Architectural Design issues and Challenges” in (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, PP 3089-3094