Wireless Sensor Network: An Overview

Kirti Kangra[1], Jaswinder Singh[2]
Department of Computer Science and Engineering
Guru Jambheshwar University of Science and Technology, Hisar, Haryana, India
kirtikangra98@gmail.com, jaswinder_singh_2k@rediffmail.com

Abstract: *-By the progression of the technology use of wireless sensor network has also gain popularity. Now these days WSNs are used in almost every field. In wsn network data is being collected by observing the surrounding with huge number of sensors deployed at place to send or receive data securely. The main functional unit of a wsn is sensor which gathers data and transmits that data to the base node by performing some data aggregation technique. These networks have the abilities of not being centralized, can maintain themselves and healing, dynamic topology, multi hop routing and provide the integrity and confidentiality of data. This paper provides an overview towards WSN.*

Keywords: WSN, Architecture, Protocols, Security Threats, Applications

I. INTRODUCTION

Day to day life of people has changed due to technological innovations. Telecommunication networking is one of them which affect the life of people by use of information technology [1]. Because of increasing use of electronic devices wireless communication is becoming more popular now these days. If we thought about wired communication firstly, we need to set a infrastructure to establish the communication, whereas wireless communication may or may not need any infrastructure [2].

Wireless network is made up of number of nodes which are connected to sensor or sensors. Every sensor node has radio transceiver with an antenna (internal or external), microcontroller or an electronic circuit for interfacing with sensors and a battery or any energy source. Sensors are present in different sizes from shoe size to grain of dust and cost also vary from few rupees to thousands of rupees according to their functionality and complexity. Apart from size and cost other constraints are also their like battery, energy, memory, computational power and speed etc.[3].The wireless sensor network's configuration might range from a straightforward star network to a sophisticated multi-hop wireless mesh network. Interaction between the nodes is achieved via flooding and routing.

Architecture

The structural design of wsn consist of: (A) Source nodes: that produce data, generally sensors to determine the environmental parameters like temperature, humidity etc., (B) Sink nodes: that collects the data stored by source nodes (C) Intermediate nodes: that may consist of source nodes which aid the data transmission from source to sink [5]. Figure 1 shows the architecture of wsn.

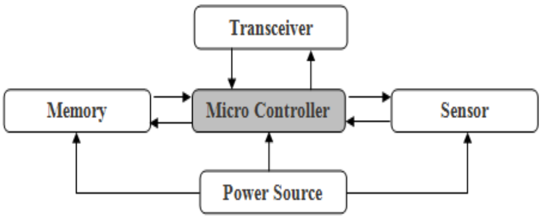

Figure 1: Structure of WSN[4]

In wireless sensor networks nodes are usually vary from hundreds to thousands of tiny cooperating with other wireless sensor nodes. The development of WSN has gain interest of various industries and used in various domains in which it is used as shown in Figure 2. The main job of a WSN is to observe the area concerned, gather data and transmission of that data to the sink node. Sink node is responsible for making decisions on the bases of collected data from the nodes.

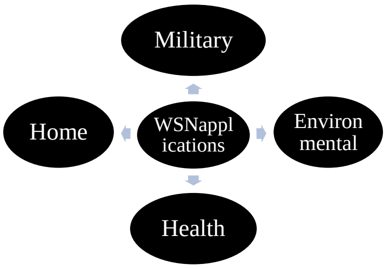

Figure 2: Applications of WSN

Sensors in wireless networks are typically deployed for harsh areas by aircrafts to get some specific quality of service. Limited battery energy and communication capacities sensors worked for a long time. Reliability is one of the main requirements for the sensor network for the applications. The objective of the wsn is to obtain and transporting the data required by distinct application having different needs on the reliability and timeliness of data transmission. The failures in the network affect the reliability over the time and become more difficult to attain the required reliability but the effective framework for the reliability of data transmission protocols in WSNs is at present absent.

A. Components of sensor nodes

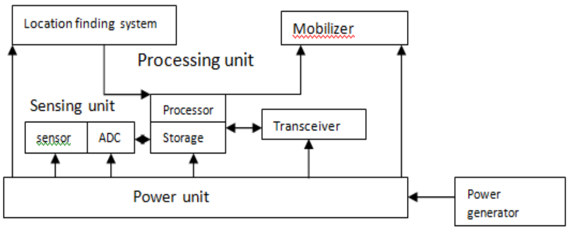

Figure 3: components of sensor node

C. Characteristics of WSN [5]

Ad-hoc: Wireless Sensor Network is formed at a time when they required, same as in a traditional Mobile Ad-Hoc Network. Network is not deployed in traditional centralized manner which manages the network. Nodes are the important part of the network with the help of adaptive protocol nodes communicate with their neighbour nodes in range. Multihop transmission is using for the distant nodes. With the help this feature of the Wireless Sensor Networks provides a straight forward and fast development.

Densely populated: Nodes are placed distinct from each other so sometimes number of sensors are needed for a small area. Reason behind to use large no. of sensor nodes are they provide redundancy if some of nodes die too early due to energy depletion or any physical damage. This will provide surety that the data is transmitted to the sink node. Another reason according to which if any node fails, due to this dense network data will not lost, it will transmit to the sink.

Limited power and limited resources: These are main problem of WSN that it has limited energy (battery life). If energy depleted, node will not be able to receive or transmit data it become useless. Sometimes it is impossible to replace all the drained energy nodes because of accessibility condition or more in number. Sensor nodes have restricted transmission range, not more than few hundred feet, or low CPU processing power.

Scalability: Wireless sensor network must be capable to manage number of nodes in the sensor which is an important characteristic of WSN and allow cooperating with other nodes present in network. As Wireless Sensor Networks have huge number of sensor nodes, this becomes much costly and impractical to retain distinctive node identifiers.

D. Applications [6]

Environmental Applications: -The sensor networks have an enormous environmental application. These nodes can be used to track and record animal movements, birds. These sensors can be used to monitor the terrestrial, soil, atmospheric context, irrigation and precision agriculture. They can also be used to detect fire, floods, earthquakes, chemical / biological outbreaks and so on.

Health care monitoring: -There are several types of sensor networks available for medical purposes, including embeddable in the environment, portable, and mountable. The devices you inject into a person's body are known as insertion medical devices. Portable technology is utilised on or close to a human body surface. Physically confined sensors are used in integrated systems. Possible Applications could involve tracking a person's whereabouts, body posture, and general surveillance of infected patients in clinics and at home. Physically placed implants use data collected by a network of depth cameras, a monitoring floor, or similar devices as input to track a person's physical status for ongoing health diagnosis. Physiological networks will collect data on the patient's spending on exercise and health. In smart healthcare, user's information integrity and security are of utmost importance.

Military Applications: -Since the WSNs can be positioned quickly and are self-organized; these networks are therefore very helpful for sensing and monitoring friendly or unreceptive motions in military operations. Observation of the battlefield can be done with the help of sensor nodes to watch everything if more equipment, forces, or ammunition is required in the war zone. Sensor nodes can also detect the chemical, nuclear and biological attacks.

Home Application: -As the technology advances, our household appliances are also making their way for their smart use and adequate performance. These sensors can be seen in refrigerators, microwaves, vacuum cleaners, security systems and water observation systems as well. Using the WSNs, the user can manage devices nearby and distantly.

E. Issues and Challenges in WSNs[7]

The primary concerns with a WSN's development and efficiency are:

Energy: Power is required by nodes for a variety of tasks. The medium for reliable function necessitates a significant amount of power from node components like the CPU, radio, etc. in order to obtain, process, communicate, and continuously respond to data, even if they sometimes fail to function. Batteries need power recharged after they have been consumed or needs to change battery. It is not always possible to recharge battery or to change battery due to surrounding situation. “Designing, producing, and implementing energy-efficient hardware and software protocols for WSNs is the key difficulty”.

Self-Management: Once deployed, wireless sensor networks must be capable to perform its function without the help of human. The network configuration, adjustment, preservation and restore should be managed by network itself.

Security: These days, deploy a secured WSN is a major issue not only in warzone, monitoring the condition of an area but also in healthcare and ir airports also. Confidentiality is main concern to wher information is travelling between the sensor networl or between the sensors and the base station; else data become infected or stolen. For every sensor networl node, it is important that it can differentiate betweer that data is being sent by a trusted or malicious node Data which is sent to user should not be modified and correct data must be transmitting to user end. Various attacks are possible in WSN like spoofing and modification in the routing information, passive information collection, sinkhole attacks, Sybil attacks, DOS attack and jamming etc.

Calibration: By comparing the raw sensor observation data obtained from the sensors with a small set of reference values, the calibration procedure transforms the raw data into precise values. Due to sensor node malfunctions and stochastic noise, manual calibration of sensors in a sensor network is a time-consuming and difficult task that is also quite expensive.

*Fault Tolerance:*It is crucial for a sensor network to continue operating even if one or more sensor nodes breakdown while it is in operation. Even in the event of an error, the network must have the capability to change its connectivity. In that circumstance, a capable routing algorithm should be modified to change the network's overall configuration.

MAC Layer Issues: Since some of the major roots of energy waste are found in the MAC layer—collisions, overhead data packet management, and inactive listening. Medium access control solutions directly affect energy usage. Power-saving forward error control algorithms are difficult to effectuate due to their high computational power requirements and the fact that extended datagrams propagation is typically not viable.

II. PROTOCOLS IN WSN

There are different types of protocols which are used to establish the communication between the sensors like routing protocols, data transmission protocols, energy saving protocols etc. Some of
them are: -

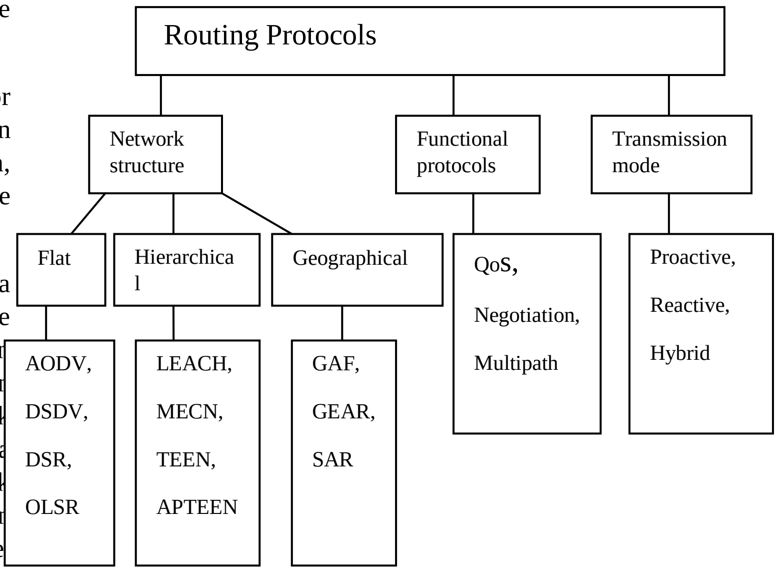

Figure no 4- Routingprotocol [8]

A. *Comparative analysis of some routing protocol*:[9]

Protocol Feature	**Distance Sequenced Distance Vector**	**Ad hoc On Demand Vector**	**Dynamic Source Routing**
Multi-cast Routing	N	N	Y
Uni-directional link support	N	N	Y
Periodic Broadcast	Y	Y	N
Multi-cast	N	Y	N
Routes maintained in	Table	Table	Cache
Route cache/table timer	Y	Y	N
Reactive	N	Y	Y

Table no.1 comparative analysis

B. *Features of some Authentication Protocols in WSNs* [10]

Protocols	Blocked Attacks	Main Features
SPINS (Security Protocol for Sensor Networks)	Message Replay Attack, Data and Information Spoofing	Provides data authentication, replay protection, Low communication cost
LEAP (Localized, Encryption and Authentication)	Information Spoofing, Data Attack	Provides authentication, Uses 4 keys
RKP (Random Key Pre- distribution)	Data and Information Spoofing, Data Attack in Transit	Provides resilience and authentication, Uses random pre-distribution key
TinySec	Data and Information Spoofing	Provides authentication, , integrity and confidentiality

Table no.2 comparative analysis

III. SECURITY THREATS

In wsn there are some attacks which are possible during the data transmission. As earlier mention that the security is the major concern of the WSN. Some of attacks are:

Threat	**Layer**
Jamming Tempering	Physical
Exhausting Collision Unfairness	Link
Neglect and Greed Homing Misdirection Black holes	Network
Flooding Desynchronization	Transport
Clone attack	Application

Table no .3 Security threats [11]

CONCLUSION

Wireless sensor network is gaining more popularity these days. The functional unit of wsn is sensors and combining these sensors the network which is formed is wireless sensor networks. These networks are used in almost every field whether its hospitals to diagnoses the patient condition, in battle area or to check the environmental condition of any specific area etc. But as discussed in the paper there are some constraints like energy, computation speed, bandwidth, and security etc. Different types of protocols are used to establish the connection between the sensors or between the sensors and sink node to transmit or receive the data.

REFERENCES

[1] V. J. Hodge, S. O'Keefe, M. Weeks, and A. Moulds, "Wireless sensor networks for condition monitoring in the railway industry: A survey," *IEEE Trans. Intell. Transp. Syst.*, 2015.

[2] J. Rigelsford, "802.11 Wireless Networks: The Definitive Guide," *Sens. Rev.*, 2014.

[3] J. A. Stankovic, "Research challenges for wireless sensor networks," *ACM SIGBED Rev.*, 2007.

[4] B.Ayyappan,Dr.P.Mohan Kumar "SecurityProtocols in WSN: A Survey" *International Conference on Science Technology Engineering &Management* (ICONSTEM),2017

[5] Z. Wang, M. Feng, T. Miao, W. Jiang, and J. Shen, "Energy efficient MAC protocol for wireless sensor networks: A survey," *in Lecture Notes in Computer Science*, 2017.

[6] Priyanka, P, Ayyappan, B, "Wireless sensor Net- -works -technologies, protocols, applications and simulators: Asurvey" *JCPS Journal*, 2015.

[7] Sukhvinder Sharma,Rakesh Kumar Bansal,Savina Bansal "Issues and Challenges in Wireless Sensor Networks "International Conference on Machine Intelligence Research and Advancement ,2013.

[8] A. Tiab and L. B. Medjkoune, "Routing in Industrial Wireless Sensor Networks: A Pages Survey," *Chinese Journal of Engineering, Vol. 2014*, 1-7, 2014.

[9] Divya Upadhyay, P. Banerjee, A.L.N Rao" Critical Performance Comparison of On-Demand Routing Protocols for Optimal Application in WirelessSensor Network " *IEEE International Conference Confluence The Next Generation Information Technlogy*, 2014.

[10] Aykut Karakaya, Sedat Akleylek"A Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks",*IEEE* ,2018.

[11] Manpreet Kaur , Amarvir Singh "Detection and Mitigation of Sinkhole Attack in wireless sensor Network" International Conference on Micro-Electronics and Telecommunication Engineering, 2016.