

# Wireless Sensor Network, Analysis On Its Application Types

Aketi Santhosh

Assoc. Prof.

Department of ECE

Siddhartha Institute of Technology and Sciences

Narapally, Hyderabad, Telangana, India

Bhookya Naveen

Professor

Department of ECE

Siddhartha Institute of Technology and Sciences

Narapally, Hyderabad, Telangana, India

**Abstract** - A wireless sensor network is a type of network that consists of a collection of small sensors called sensor nodes. Sensor nodes are resource constrained, which means that they have restricted battery power, storage, and communication capabilities. These sensor nodes have a radio range that they use to communicate with one another and form a network. Wireless environmental monitoring and object tracking are two applications where a wireless sensor network is quite useful. The main goal of this survey is to present a comprehensive evaluation of recent work on various elements of WSN and the operation of wireless detection networks, as well as the benefits and drawbacks of traditional wireless networks. Wireless sensor networks are made up of thousands of sensor nodes that communicate wirelessly with one another. Thousands of applications rely on it. In this study, we look at such WSNs from the perspective of applications, and we examine many application areas where these sensor networks are used, as well as their capabilities and requirements.

**Keyword:** WSN, Sensor nodes, battery power, storage, Environmental Monitoring

## 1.INTRODUCTION

Wireless sensor networks have emerged as a result of recent breakthroughs in electronics and wireless networks, and are regarded as one of the most important technologies for the future. Small battery-powered devices with minimal communication and compute capabilities are used in these networks. Every sensor in a wired sensor network has three subsystems: the sensor subsystem, the processing subsystem, and the communication subsystem. The sensor sub-system senses the environment, and the resulting sensed data is provided to the processor sub-system for local computation. Finally, the communication sub-system exchanges messages with surrounding sensor nodes to provide communication. Wireless sensor networks have advanced to the point

that they may now be used efficiently in health-care applications. Thousands of wired devices can be replaced with wireless devices using sensor-based technologies without sacrificing performance. Even in high-mobility situations, such technology has the ability to provide reliability. In the future, we'll look into integrating a large number of wireless sensor networks with traditional medical equipment. The current applicability of wireless sensor networks in health care systems was investigated in this research.

### 1. Wireless Sensor Architecture

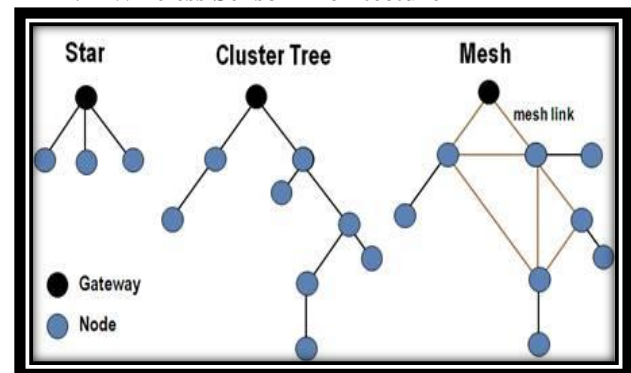


Figure 1 General Architecture of Wireless sensor network

The general design of wireless sensor networks is shown in Figure 1. Mesh topology, Star topology, and Tree topology are the three network topologies available in sensor networks. Each topology, that is, each network, must have a gateway node, as well as a network administrator and sensor nodes. Wireless sensor technology has emerged as a critical technology with substantial potential for improving a variety of recent applications in medical, transportation, agriculture, industrial, military, and home-based applications in recent years. It's also used to develop cutting-edge technologies in industries including worldwide environmental monitoring, precise agriculture, smart cities, medical care, and a variety of future military applications.

### **1.1 Medical Applications**

Several wireless technologies are used in medical applications, including Wireless Body Area Network (WBAN), Wireless Personal Area Network (WPAN), and Wearable Wireless Sensor Networks (WWSN), among others. WBAN technology necessitates the continuous operation of sensors that monitor a patient's physiological signals such as blood pressure, glucose level, heart rate, and movement. Wearable and implantable sensors are available in this WBAN technology. WWSN technology is used to demonstrate the review. Some performance measures, such as packet segmentation, packet loss, access delay, and security, are studied to assess the performance of wireless sensor networks in hospital environments or health care systems. It is important to monitor certain of the patients' periodic activities, such as EEG, ECG, and GSR, which can be done using WPAN technology. Each sensor in such a network collects data and talks with a personal server, which combines all of the sensor data. Recent advances in medical sensor technology have spawned a new field known as Wireless Body Area Networks (WBAN). The main goal of wireless sensor networks-based healthcare applications is to continually monitor patients' health conditions, which is in high demand, and various projects are in the development and implementation stages to accomplish this. Because a wireless body area network is used to collect sensitive patient data, it must be properly secured against unauthorized user access.

### **1.2 Environmental Related Information Applications**

The use of environmental data collection is necessary to collect data from multiple sensors over a period of time. If the sensor data is significant, it is collected at regular intervals, and the sensor nodes remain in the same place. The base stations hold all of the obtained data from thousands of sensor nodes that are continuously detecting the environment in the application of environmental data gathering using traditional methodologies. Sensor nodes would be uniformly dispersed throughout an outdoor environment in a traditional deployment scenario. Sensor nodes in environmental monitoring applications do not need to develop optimum packet routing algorithms on their own. Rather, the ideal packet routing topology outward of the sensor network may be computed and then the important sensor information could be transmitted to the sensor nodes as needed. It's possible because the sensor network's physical network topology is fairly consistent. Because of its time-varying nature, RF transmission causes irregular connectivity between

any two nodes, yet the overall network topology will be rather stable.

### **1.3 Home Application**

In addition to wireless sensor networks for business uses, home-based sensor applications will become a part of our daily lives in the future. Many ideas have been proposed by researchers and designers, such as a smart environment in which the room temperature is detected by installing five sensors in each corner. Initially, air conditions had sensors as well. However, it can only record the temperature at each machine's corner, not the room's initial temperature. As a result, the sensors detect the room's environment. Only the air conditioner will switch from sleep mode to active mode after each sensor has collected the room's original temperature. Some areas of the smart house, such as the corridor, the washroom, and the balcony, have automatic sensors that can turn on or off the lights. The smart home's windows are equipped with vibratory sensors to prevent theft.

### **1.4 Military Applications**

The fundamental knowledge of wireless sensor networks is the foundation of the defense application at first. The Defense Advanced Research Project Agency (DARPA) has two critical defense programs: Distributed Sensor Networks (DSN) and Sensor Information Technology (SIT) (DARPA). Wireless sensor networks are successfully implemented in military-based sensing. Wireless sensor networks have now become an important component of communications, control, computing, intelligence, investigative, military, surveillance, and targeting systems. Rapid network deployment, self-organization of nodes, fault tolerance, and network security are some of the needs of sensor networks in the military setting. Sensor networks or nodes should provide the following services: observing friendly forces, missiles, and tools. Battlefield surveillance, enemy force discovery, precise targeting, battle destruction computation, and analysis of chemical, biological, and nuclear attack detection

### **1.5 Node tracking scenarios**

Sensor nodes in wireless sensor networks tracked the tagged object across the monitored space. There are a variety of situations in which it is necessary to track the location of key resources workers. Current stock control systems attempt to monitor objects by recording the object's most recent entry point. However, using these frameworks, determining the current area of the object is impossible. It is impractical to expect objects to pass through checkpoints on a regular basis in a typical network setting. Object tracking in wireless sensor networks is accomplished by tagging the objects with a

lightweight sensor node. Because the sensor nodes are installed in an environment with established positions, only when things move through the area of sensor nodes can they be properly detected. Instead of monitoring ambient data, those sensor nodes will be set up to detect the RF messages sent by sensor nodes attached to various objects. The sensor nodes can act as dynamic tags, reporting the presence of any device. Furthermore, a database can be used to track the location of monitored items in relation to a group of sensor nodes in known locations. With this framework, it is possible to inquire as to where the tracked object is currently located, rather than just where it was last checked. Sensor nodes tracking applications, unlike detection or security systems, will have network topology changes as sensor nodes move through the system. While the connectivity between sensor nodes in permanent locations will be somewhat fixed, connectivity to moveable nodes will be constantly changing.

### **1.6 Security Monitoring**

In recent years, network monitoring for security purposes has become increasingly vital. These networks are made up of multiple sensor nodes that are placed in fixed locations throughout an environment and constantly monitor at least one sensor in order to detect an intruder or attacker. One of the most significant differences between security network monitoring and network environmental monitoring is that security solutions do not actually collect any data. This has a substantial impact on the network's ideal architecture. Every sensor node must promptly verify the state of its sensor nodes, but it only needs to send an information detail when a security breach occurs. The system's primary need is that warning signals be communicated quickly and reliably. "Report by special case" systems are what they're named. Every sensor node is confirmed to be present and operational. If a sensor node malfunctioned or failed, it would indicate a security breach that needed to be reported. The sensor network must be set up for these security monitoring applications, and only the sensor nodes are responsible for confirming each other's condition. One method is to assign each sensor node to a peer that will notify you if one of your sensors isn't working.

The optimum security monitoring system topology will look to be significantly different from that of an information gathering network. Every sensor node in a gathering tree must communicate the information of all of their decedents. Every sensor node in today's security networks must be verified around once every hour, according to the accepted norm. When

combined with the ability to distribute the task of reviewing sensor nodes equitably, the energy cost of performing this check becomes negligible. A large portion of the energy consumed by a security system is used to meet the stringent latency requirements associated with raising the alert when a security breach occurs. In security systems, a large portion of the node's energy is spent confirming the operation of nearby sensor nodes and setting up the node to relay alert statements instantly. The energy consumed by genuine information transmission will be a small fraction of the sensor node's total energy.

## **2. CONCLUSION**

Wireless Sensor Networks are made up of thousands of sensor nodes that are wirelessly connected and have the capability of sensing the environment or event and transferring information to the sink. This paper looked at some of the most recent sensor network applications that have been published. The need for sensor networks is rapidly growing due to the fact that these systems have made it possible to undertake critical activities that humans are unable to perform. Healthcare applications play an important role in everyday life and will continue to do so in the future. The applications of Wireless Sensor Networks in various sectors were investigated in this research. In addition, numerous studies involving healthcare monitoring applications, such as home administration, will be pursued. The application of Wireless Sensor Networks in medicinal services was divided into three categories: patient monitoring in a clinical setting, home and long-term care center monitoring of elderly patients, and the accumulation of long-term clinical databases. The current use of WMSNs in medical services has a few flaws that need to be addressed, according to this analysis. The wireless sensor network research group has done an exceptional job of overcoming a few limitations that now exist for human services applications; nevertheless, further progress is needed in terms of privacy and security challenges, as well as breakthroughs in wireless communication.

## **REFERENCE**

- [1] Andrew S. Tanenbaum, David J. Wetherall, "Computer Networks", Fifth Edition, ISBN -13: 978-0-13- 212695-3
- [2] William Stallings, "Network Security Essentials Applications and Standards", Second Edition, Pearson Education, Inc. ISBN 0-13-035128-8
- [3] William Stallings, "Wireless Communications and Networks", Second Edition, © 2005 Pearson Education, Inc., ISBN: 0-13-191835-4
- [4] Kiran Maraiya, Kamal Kant, Nitin Gupta, "Application based Study on Wireless Sensor Network", International

Journal of Computer Applications (0975 – 8887), Volume 21, Issue 8 May 2011.

[5] Th. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks", IEEE, Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 27-29, 2005.

[6] Long Zhaohua, Liu Jianfeng Jiang Guiquan, "Survey of Routing Protocols in Wireless Sensor Networks Based on Applications", IEEE, 2010 2nd International Conference on Industrial and Information Systems.

[7] Murtadha M. N. Aldeer, "A Summary Survey on Recent Applications of Wireless Sensor Networks", 2013 IEEE Student Conference on Research and Development (SCORED), 16 -17 December 2013, Putrajaya, Malaysia.

[8] IlkerDemirkol, CemErsoy, and FatihAlagöz, Bogazici University, "MAC Protocols for Wireless Sensor Networks: A Survey", IEEE Communications Magazine, April 2006.

[9] Manohar Potdar, Atif Sharif, VidyasagarPotdar, Elizabeth Chang, "Applications of Wireless Sensor Networks in Pharmaceutical Industry", IEEE, 2009 International Conference on Advanced Information Networking and Applications Workshops.

[10] Daniele Puccinelli and Martin Haenggi, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing", IEEE Circuits and Systems Magazine Third Quarter 2005

[11] X. Chengsheng Yuan, Sun. X, and Lv. Rui, "Fingerprint liveness detection based on multi-scale LPQ and PCA," China Communications, vol. 13, no. 7, pp. 60–65, 2016.

[12] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG cryptography and authentication in body area networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 6, pp. 1070–1078, 2012.

[13] Z. Zhang, H.Wang,A. V. Vasilakos et al., "Channel information based cryptography and authentication in wireless body area networks," in Proceedings of the 8th International Conference on Body Area Networks, pp. 132–135, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013.

[14] Z. Li and H. Wang, "A key agreement method for wireless body area networks," in Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOMWKSHPS), pp. 690–695, 2016.

[15] L. Shi, J. Yuan, S. Yu, and M. Li, "Mask-ban: movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," IEEE Internet of Things Journal, vol. 2, no. 1, pp. 52–62, 2015.