A Review Based On Study Of Wireless Sensor Network With References To The Technology And Applications

Dr. K. J. Praveen Kumar¹, Dr. K. Divya², Dr. T. K. Sumati³, Dr. M. Sathya Priya⁴

¹Assistant professor, Department of computer science Gobi Arts & science college Gobichettipalayam.

²Assistant professor of Information Technology, Bharathidasan college of Arts and Science Ellispettai, Erode.

³Associate professor of computer science, Gobi Arts & science college Gobichettipalayam.

⁴Assistant professor of computer science, Gobi Arts & Science college Gobichettipalayam.

Abstract

Wireless Sensor Networks, often known as WSNs, are playing a significant part in the ongoing transformation that is being brought about by sensing technologies. WSNs have evolved as a strong technology that may be utilised in a variety of settings, including but not limited to military operations, surveillance systems, Intelligent Transport Systems (ITS), and other similar settings. WSNs are made up of a variety of sensor nodes, all of which are responsible for gathering data from their surroundings and keeping an eye on the environment outside. The majority of the efforts put into this research are concentrated on finding ways to keep the energy requirements of the sensor network to a minimum. This will allow the network to function for a significantly longer period of time. The discharge of the batteries that the sensor nodes are powered by has been the key source of worry with regard to the conservation of energy. In addition to this, wireless sensor networks (WSNs) are being utilised for the security features they provide so that they can be employed in sensitive environments such as military battlefields. In this paper, the Wireless Sensor Network (WSN) is presented from a variety of perspectives, including applications, routing and data collecting, security considerations, and brief discussions of modelling platforms that are applicable to WSNs. This Paper makes a contribution in a roundabout way regarding implementing WSNs in a variety of various sectors of its operation and reflects the significance of doing so.

Keywords: Wireless Sensor Networks, technologies, conservation of energy, applications.

1. INTRODUCTION TO WSN

The creation of wireless sensor networks, which are comprised of individual devices referred to as sensor nodes, has been made possible by advancements in wireless communication. Sensor nodes are devices that are capable of sensing, wireless communication, and
computation. They have a low power consumption, a small size, and are inexpensive. As soon as the sensors are introduced into the network, they immediately begin to configure themselves, communicate with one another to facilitate data gathering, and then send that information on to the Base Station.

WSN can also be thought of as a network made up of small, simple devices called nodes that can sense the environment and send information from the monitored area. The information can be sent directly to the sink or through multiple hops to the sink, which can then use it locally or connect to other networks (like the internet) through gateway nodes. WSN can also be thought of as a network that can gather information about the environment and send it to other devices.

1. A sensing unit, a processing unit, a transceiver, and a power unit are the primary components that make up a sensor node.

2. The sensing device gathers information about the physical amount, which is then converted into a digital representation by an analogy-to-digital converter, or ADC for short. After then, the CPU is used to perform more computations, and the transceiver is used to send and receive data from either the Base Station or the other nodes in the network. The power unit is always the most noticeable component of a sensor node. In applications that require no human supervision, the battery cannot be changed once it has run out of juice. Mobilizers, power generators, and location finding systems are examples of the types of application-specific devices that are available.

![Fig. 2 Components of a sensor node](http://www.webology.org)
2. Challenges in WSNs

WSNs are designed with a number of different aims in mind, one of which is to carry out data communication while at the same time adopting aggressive energy management measures in order to try to extend the lifetime of the network and prevent connectivity deterioration. The regulation of the topology in WSNs is affected by a wide variety of problematic aspects. In order for wireless sensor networks (WSNs) to achieve effective communication, certain obstacles must first be cleared. In the following, we will provide a brief summary of some of the difficulties and design considerations that have an impact on the building and maintenance of topologies in WSNs.

a. Deployment of nodes: The performance of topology control algorithms is impacted by the deployment of nodes in WSNs, which varies depending on the application. Either a deterministic plan or a random one can be used for the deployment. Deterministic deployment requires the sensors to be manually positioned, and data to be transmitted along paths that have been predetermined. On the other hand, in the random node deployment method, the sensor nodes are dispersed at random in order to create an infrastructure in an ad hoc fashion.

b. Consumption of energy without a loss in precision: Sensor nodes can burn up their limited supply of energy by conducting computations and transferring information in an environment that is wireless. As a result, methods of communication and computing that require less energy are absolutely necessary. The lifespan of the sensor node has a significant correlation with the lifespan of the battery.

c. Data Reporting Model: The manner in which data is sensed and reported in WSNs is determined by the application being used and the urgency with which the data must be reported. Reporting on data can be arranged into one of four categories: time-driven (continuous), event-driven, query-driven, or a hybrid of the two. Applications that need to monitor their data on a
periodic basis are good candidates for the time-driven delivery approach. As a direct result of this, sensor nodes will, at regular intervals, power on their sensors and transmitters, take readings of the environment around them, and broadcast the data that is of interest at periodic intervals that are both consistent and periodic in nature.

d. Heterogeneity of Nodes and Links: In many studies, it was believed that all sensor nodes were homogenous, which means that they had the same capacity in terms of computing, communication, and power. On the other hand, the role that a sensor node plays or the capabilities it possesses can vary greatly depending on the application.

e. Fault Tolerance: In the event of a power outage, physical damage, or environmental interference, some of the sensor nodes may be rendered useless or blocked. The failure of individual sensor nodes is supposed to have no influence on the overall mission that the sensor network is accomplishing. The MAC and topology algorithms must be able to handle the construction of new links and routes leading to the data gathering base stations in the case of a large number of nodes failing.

f. Scalability: The number of sensor nodes that may be deployed in the sensing region can range anywhere from a few hundred to several thousand or even more. Any topology control technique must be able to function with such a massive number of sensor nodes in order to be considered viable. In addition, the routing control algorithms for sensor networks should be adaptable enough to be scalable in order to react to happenings in the surrounding environment. The vast majority of the sensors are able to remain in the sleep state until an event takes place, and the data provided by the few sensors that are still active is of a coarse quality.

g. Security: In certain applications, the communication between nodes is essential to be sufficiently secured in order to keep the confidentiality. When working with military applications like surveillance on the battlefield, military operations, and other similar tasks, it is almost always required.

3. APPLICATIONS OF WSN

For example, a wireless sensor network may comprise seismic and low sample rate magnetic sensors as well as optical and infrared sensors, as well as acoustic sensors. These sensors can keep tabs on a wide range of environmental variables, including air temperature and humidity, vehicle speed and direction, lightning activity and pressure, soil composition and noise levels, as well as the presence or absence of specific objects and the mechanical stress levels on attached objects. WSN applications can be broken down into the following categories:

a. Applications inside the Military:

b. Environmental applications:

c. Applications in the Healthcare Industry:

d. Home applications:

e. Traffic control:
4. SECURITY ASPECTS OF WSN

The use of WSN in a variety of applications, including those dealing with climate change, environmental monitoring, traffic monitoring, and home automation, has helped propel its popularity to an all-time high in recent years. As a result, maintaining the WSN is a difficult undertaking that has always existed. The use of symmetric key techniques, asymmetric key techniques, and the hash function all contribute to cryptography's capacity to provide security. It is necessary to use a lightweight cryptographic algorithm due to the severe limitations that WSN have in terms of compute, communication, and the amount of battery power available. Because of the limitations imposed by sensor nodes, the choice of cryptographic method is critically important in WSN. The following three aspects can be used to describe cryptography in wireless sensor networks (WSN):

symmetric, asymmetric, and hash function are all terms that are used.

5. SIMULATION PLATFORM IN WSN

When it comes to WSN testing, simulation is one of the most common methods of evaluating novel communication architectures and network protocols in addition to testing and validating current ones. Prior to investing a substantial amount of time and money into the system, researchers can benefit from simulation by gathering significant information about the system's feasibility and practicability. This knowledge is essential to its successful implementation. When it comes to WSNs, testing and validation that is based on simulation offers a number of benefits, some of which include ease of deployment, lower costs, flexibility, and the potential to test large-scale networks. Due to the enormous variety of simulation tools and the unique requirements of WSNs, it is difficult for a user to select a nearly perfect tool for his evaluation (such as energy-constraints and large-scale deployment). In order to solve this problem, a survey of some of the simulation tools that are currently considered to be the most advanced and commonly utilised for WSNs is offered below. The purpose of this project is to provide assistance to researchers in the process of selecting an appropriate simulation tool to evaluate their work and to achieve trustworthy results for large-scale WSNs.
6. Conclusion

WSNs have found extensive applications across a variety of domains of human existence. Because of advancements in sensing technology, it is now possible for any sensor node to communicate and react to a variety of various characteristics. This article provides an overview of several different WSN-related topics. Following the concise overview of the WSN, we moved on to explore some of the most pressing concerns. Along with the security features of WSN, applications have been brought to people's attention. Following that, a tabular comparison of the various simulation software's has been provided. Based on the findings of the research presented in this article, one can draw the conclusion that WSN has significantly impacted virtually every facet of the modern period. It possesses a vast potential for research in addressing a variety of facets of human existence.

REFERENCES


