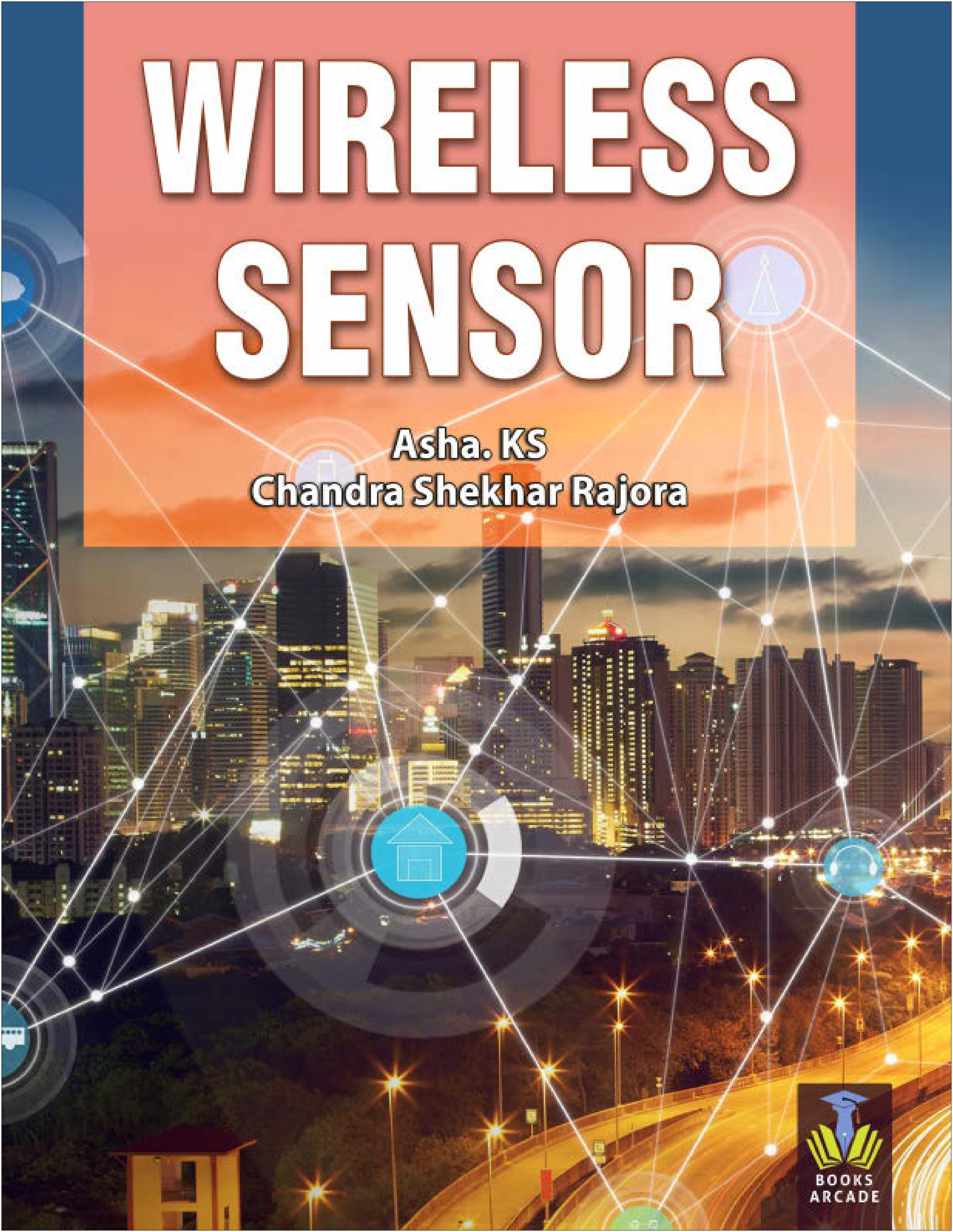
WIRELESS SENSOR

Asha. KS

Chandra Shekhar Rajora



BOOKS ARCADE

Wireless Sensor

Wireless Sensor

Asha. KS

Chandra Shekhar Rajora

BOOKS ARCADE
KRISHNA NAGAR, DELHI

Wireless Sensor

Asha. KS
Chandra Shekhar Rajora

This book contains information obtained from highly regarded resources. Copyright for individual articles remains with the authors as indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

BOOKS ARCADE

Regd. Office:
F-10/24, East Krishna Nagar, Near Vijay Chowk, Delhi-110051
Ph. No: +91-11-79669196, +91-9899073222
E-mail: info@booksarcade.co.in, booksarcade.pub@gmail.com
Website: www.booksarcade.co.in

Year of Publication 2023

International Standard Book Number-13: 978-81-962948-9-2

CONTENTS

CHAPTER 1

INTRODUCTION

Asha. KS, Associate Professor,
Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN
(Deemed-to-be University), Karnataka – 562112
Email Id- ks.asha@jainuniversity.ac.in

A new type of wireless networks known as wireless sensor networks (WSNs) is quickly gaining popularity with both military and commercial uses. A wireless sensor network (WSN) is a wireless network made up of several different sensor devices that are deployed across the network and are used to track environmental or physical parameters. A WSN is made up of a collection of interconnected, small sensor nodes that may exchange data and interact with one another. These nodes collect environmental data, including temperature, pressure, humidity, and pollution levels, and communicate it to a base station. Depending on the kind and volume of data being monitored, the latter communicates the information to a wired network or generates an alert or an action [1]–[3].

Common uses include tracking animal and human movement in woods and along borders, weather and forest monitoring, combat surveillance, and geomorphological conditions monitoring, such as humidity, temperatures, resonance, and pollution. They transmit wirelessly using the same air-based transmission channel as wireless local area networks (WLANs). Standard access protocols like IEEE 802.11 are available to provide appropriate communication between nodes in a local area network.

However, WSNs cannot be directly used with this protocol or the others. The primary distinction is that sensors are provided with a relatively tiny source of energy (often a battery), which depletes quickly, as opposed to showed an interest in local area networks. Therefore, it becomes necessary to develop new, energy-conscious MAC protocols.

A WSN has less resources than a standard WLAN, thus there are undoubtedly some differences between the two. A wireless sensor network (WSN), is a wireless computer network made up of several scattered independent sensor nodes to coordinate the physical or environmental factors, such as vibration, pressure, temperature, music, locomotion, and pollution, at various settings. WSNs are being utilised in a broad range of commercial and residential applications, including as traffic management, smart and digital houses, smart cities, monitoring of the environment and habitats, and monitoring of industrial processes.

Tiny general-purpose CPUs, actuators, and small sensors make up the construction of WSNs, which can only handle a limited amount of computing. Numerous low-cost, low-power, and conscience sensor nodes make up the WSN. One of the primary objectives of every WSN is to collect data or data center from the environment [4], [5].

Wireless sensor network limitations

The main factors that determine what protocols should be used are the hostile and isolated locations at which the wireless sensor nodes are often deployed, the constrained computing and energy resources, as well as the constrained file cabinets in the nodes. Because of the few resources, for instance, the schemes and protocols often employed to secure WSNs are lightweight solutions, while those used for routing are more emission and that it should need the least amount of execution time. Both the innovation and research communities have been attracted by wireless sensor networks (WSNs). WSN applications have proliferated in both the public and military spheres. Although military applications first spurred the development of wireless sensor networks, WSNs are currently used in a wide range of commercial and industrial settings. The vast majority of WSNs in use today assess scalar experimental results including pressure, elevation, movements, and pollution. The majority of WSNs are typically designed for low-bandwidth, delay-tolerant applications. Therefore, the majority of research has focused on the latter paradigm, also known as terrestrial sensor networks. The fundamental issue with any WSN application is the network's lifespan. A gateway in a WSN configuration provides wireless communication to the wired/fixed network.

Computer networks now play a crucial role in many aspects of our lives, including business, education, and everyday living. Regardless of the physical location of the resources or the users, networks make information and services accessible to anybody in the network. Various kinds of computer networks are split into. Applications include keeping tabs on ally troops, following enemy movements, maintaining equipment health, or spotting any biological, chemical, or nuclear attacks. Applications for the environment include monitoring animal movement, seeing fires in buildings or forests, and sensing or spotting chemical leaks. Applications in business and logistics include monitoring inventories, tracking cars and other items, and more.Remote monitoring applications of WSNs assess the specified environmental conditions regularly and communicate sample data or alerts primarily in three modes, as opposed to mobile object location tracking applications, which need real-time updating of the tracking results:

Periodically, at a certain length of time; in reaction to a specific occurrence, often when the value of a particular measurement surpasses a predetermined threshold; In response to user inquiry.The aforementioned WSN applications' capacity to quickly and easily deploy a large number of wireless sensor nodes is a key advantage. All of the typical wireless design and implementation issues are brought on by this functionality. The key ones include large-scale deployment, data management, security, interference, and energy efficiency. All of these problems must be addressed in the development and deployment of WSNs.

There are several approaches that may be used to solve the energy efficiency issue. One strategy is to optimise the hardware and embedded software, including routing algorithms, which reduces energy consumption and makes a WSN effective. The topic of energy efficiency is addressed in this book by enhancing power management at both the hardware component and network levels.

The performance of WSNs may be significantly impacted by interference from other wireless systems operating in the same area and using a comparable frequency range. Due to the limitations of WSNs, such as their limited computational capacity, standard interference avoidance mechanisms may not be effective for a large-scale WSN. This difficulty and a thorough explanation of such restrictions will be covered in this book. We'll provide some helpful advice for setting up wireless sensor networks. Because WSNs are wireless, security problems are inescapable. A proper defence system must be in place to thwart any attacks on data dissemination that is healthy. Data transferred through WSNs is often encrypted, and security management services are in place for WSNs. This book offers a way to guarantee system level security, concentrating in particular on remote Denial of Service (DoS) assaults.

The cost of sending all of this sensor data to a sink node is high when huge volumes of data are created over time. Techniques for data aggregation and compression help to minimise the quantity of data sent. For sensor networks to function, a reliable technique must be used to control dispersed data flow, query, and analysis. By using a local sensor node's storage space as a distributed database to which requests can be sent to retrieve data, rather than sending large amounts of raw data to the base station, this book will address the challenge to data management caused by both reducing the amount of data to be transferred and improving the distributed capability of in-network data processing.

In order to provide the necessary effective sensor field, a wireless sensor network often comprises of a high number of sensor nodes. They may conveniently cover a vast geographic region. Users are unable to manually manage the whole network due to this feature. In order to define network parameters, update systems, and monitor WSNs, a full management architecture is needed. When WSN sizes grow, scalability problems may cause system performance to suffer. The applications described in this book identify significant implementation flaws on a broad scale. Such implementations are only successful when the number of nodes is kept at around 100, beyond which the congestion and high routing costs cause the data transfer to substantially slow down and finally stop. The book's section on application technology addresses this problem.

This book is intended to serve as a textbook or reference for final-year undergraduate and graduate students as well as wireless communication technology researchers. Additionally, it is helpful for business managers, IT specialists, and software and system engineers who want to adopt WSNs. As a result, it sets out to investigate and analyse the conceptual, design, and implementation difficulties of WSNs, looking at relevant design methodologies and practical implementations. This book is distinct from previous publications in the area where the IEEE 802.15.4 standard and the ZigBee standard are extensively detailed but where there is a lack of explanation and demonstration at the system level .Additionally, this book differs from others in that it focuses on design and execution rather than just presenting theoretical study findings on a small number of isolated themes. Once they have finished reading this book, the readers should be able to build and implement WSNs for their own applications.

Local area network, metropolitan area network, wide area network, and personal area network (WAN). A PAN is a computer network built around a specific person, as the names suggest. Computers in a constrained space, such as a single building or a group of buildings, are connected through LANs. While a MAN is the name of the network that links computers inside a city or municipality. A wide area network (WAN) links a huge number of computers across a continent or nation. These network communication lines are often wired, which means that actual cables are used to connect the various network devices. Data transfer through wired computer networks is dependable, but installing the necessary wiring is expensive and often cumbersome. Although they have their own set of difficulties including interference, dependability, and others, wireless communication technologies provide the apparent option to get beyond these barriers.

Wireless networks use radio waves, infrared, or other wireless media to link any devices or computers. When it covers a vast region, it is referred to as a Wireless WAN. When it covers a small area or a building, it is referred to as a Wireless LAN (WLAN). Alternatively, it may link electronic devices within a person's range, in which case it is known as a wireless personal area network (PAN) (WPAN). A network called a low-rate wireless personal area network (LR-WPAN) is designed for extremely low-cost, short-range wireless communications.

These standards are divided into groups based on the throughputs, communication ranges, and application domains they support. High data throughput applications often employ standards like Wi-Fi, WiMAX, Ultra Wideband, and 802.11a/g/n, which typically need a main power source. Full mobility is intended to be attained by systems built on the General Packet Radio Service (GPRS), Enhanced Data Rate for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), and High-Speed Downlink Packet Access (HSDPA) platforms. The primary purpose of the Bluetooth standard was to eliminate computer connecting cords. Developed for wireless sensor networks, the ZigBee standard.

Networks of Wireless Sensors

In order to monitor and control physical or environmental conditions at various locations, wireless sensor networks (WSNs) are a collection of specialised autonomous sensors and actuators with a wireless communications infrastructure. WSNs are designed to cooperatively pass their data to a central location and/or pass their control commands to a desired actuator through the network.

Introduction rates and limited communication ranges, as well as physically compact, inexpensive, and low-power sensor nodes. A WSN is made up of several nodes, ranging in number from a few to thousands or even more, each of which is linked to one or more other nodes. Nodes may be created to perform one or more of the following tasks: sensing, data relaying, or data exchange with an external network. A sensor node is used for detecting, a router is used for relaying data, and a base station, also known as a sink node and analogous to a gateway in a conventional network, is used for exchanging data with other networks.

A transducer, a microprocessor, a radio transceiver, and a power source typically a battery are all included in every sensor node. Based on observed natural occurrences and changes in the environment, the transducer produces electrical signals. The sensor output is processed and stored by the microcontroller. A central computer issues orders to the radio transceiver, which has an internal antenna or is connected to an external antenna, and the radio transceiver responds by sending data to the computer. Finally, a programmer receives the gathered data through the satellite network and the Internet. The majority of sensor nodes are randomly distributed to keep an eye on a sensor field; they are not required to have a fixed position. Typically, a sensor node's on-board radio transceiver is how they connect with one another.

Applications include keeping tabs on ally troops, following enemy movements, maintaining equipment health, or spotting any biological, chemical, or nuclear attacks. Applications for the environment include monitoring animal movement, seeing fires in buildings or forests, and sensing or spotting chemical leaks. Applications in business and logistics include monitoring inventories, tracking cars and other items, and more.

Remote monitoring applications of WSNs assess the specified environmental conditions regularly and communicate sample data or alerts primarily in three modes, as opposed to mobile object location tracking applications, which need real-time updating of the tracking results. Periodically, at a certain length of time; in reaction to a specific occurrence, often when the value of a particular measurement surpasses a predetermined threshold; in response to user inquiry. The key ones include large-scale deployment, data management, security, interference, and energy efficiency. All of these problems must be addressed in the development and deployment of WSNs.There are several approaches that may be used to solve the energy efficiency issue. One strategy is to optimise the hardware and embedded software, including routing algorithms, which reduces energy consumption and makes a WSN effective. The topic of energy efficiency is addressed in this book by enhancing power management at both the hardware component and network levels.

The performance of WSNs may be significantly impacted by interference from other wireless systems operating in the same area and using a comparable frequency range. Due to the limitations of WSNs, such as their limited computational capacity, standard interference avoidance mechanisms may not be effective for a large-scale WSN. This difficulty and a thorough explanation of such restrictions will be covered in this book. We'll provide some helpful advice for setting up wireless sensor networks.

Because WSNs are wireless, security problems are inescapable. A proper defense system must be in place to thwart any attacks on data dissemination that is healthy. Data transferred through WSNs is often encrypted, and security management services are in place for WSNs. This book offers a way to guarantee system level security, concentrating in particular on remote Denial of Service (DoS) assaults. The cost of sending all of this sensor data to a sink node is high when huge volumes of data are created over time. Techniques for data aggregation and compression help to minimise the quantity of data sent. For sensor networks to function, a reliable technique must be used to control dispersed data flow, query, and analysis. By using a local sensor node's storage space as a distributed database to which requests can be sent to retrieve data, rather than sending large amounts of raw data to the base station, this book will address the challenge to data management caused by both reducing the amount of data to be transferred and improving the distributed capability of in-network data processing.

In order to provide the necessary effective sensor field, a wireless sensor network often comprises of a high number of sensor nodes. They may conveniently cover a vast geographic region. Users are unable to manually manage the whole network due to this feature. In order to define network parameters, update systems, and monitor WSNs, a full management architecture is needed. When WSN sizes grow, scalability problems may cause system performance to suffer. The applications described in this book identify significant implementation flaws on a broad scale. Such implementations are only successful when the number of nodes is kept at around 100, beyond which the congestion and high routing costs because the data transfer to substantially slow down and finally stop. The book's section on application technology addresses this problem.

This book is intended to serve as a textbook or reference for final-year undergraduate and graduate students as well as wireless communication technology researchers. Additionally, it is helpful for business managers, IT specialists, and software and system engineers who want to adopt WSNs. As a result, it sets out to investigate and analyse the conceptual, design, and implementation difficulties of WSNs, looking at relevant design methodologies and practical implementations. This book is distinct from previous publications in the area where the IEEE 802.15.4 standard and the ZigBee standard are extensively detailed but where there is a lack of explanation and demonstration at the system level. Additionally, this book differs from others in that it focuses on design and execution rather than just presenting theoretical study findings on a small number of isolated themes. Once they have finished reading this book, the readers should be able to build and implement WSNs for their own applications. The physical layer, the data link layer, the network layer, the transport layer, and the application layer make up the five layers of the WSN protocol stack. Each layer in the system is given a certain set of tasks to do without consulting the other levels stack of protocol.

The connections between various devices and their communication channel are defined and managed by the physical layer, the top layer of the protocol stack. Frequency selection, carrier frequency production, signal detection, modulation, and data encryption all fall within the purview of the physical layer. Additionally, the physical layer specifies the kinds of cables and connections that work with the communication medium. The data connection layer, the second tier of the protocol stack, is in charge of providing the services necessary for many nodes to properly access and share a communications medium. Medium access control, dependable delivery, error detection, and error repair are some of these services.

The network layer, the third tier of the protocol stack, is in charge of creating the communication routes between network nodes and effectively routing packets along these routes. Various routing protocols may have different needs, and the decision will have an impact on the communication pathways set up. Some routing procedures may favour communication channels that allow the WSN offer the greatest Quality of Service (QoS), while other energy-saving algorithms may choose for the path that gives the WSN the longest possible lifespan. Still other routing protocols will employ a combination of the two goals.

The fourth tier, the transport layer, is in charge of supplying a higher-level layer of the protocol stack and, as a result, supplying the users with clear and dependable end-user communications. The Transmission Control Protocol (TCP) and the User Datagram Protocol are two of the most well-known and disparate transport layer protocols (UDP). Transport layer protocols that focus on establishing connections, like TCP, provide robust error handling, transmission control, and flow control.

UDP, for example, offers an unstable service but with little error handling, transmission, and flow management. In contrast. The application layer is the last and fifth layer, which is used by the majority of WSN. The system's application layer is located nearby the system's users. There are several possible applications that might be implemented at the application layer, such as Telnet, HTTP, FTP, and SMTP (SMTP). Application layer programming is largely concerned with WSN.The application layer also examines the lower levels to see whether there are enough network resources and services to fulfil the user's network requests.

To guarantee that the network system operates on many hardware platforms, the embedded software architecture of wireless sensor networks must depend on a few standards. According to the intended use, current standards may be easily separated into two categories: public and private. The wireless modulation/demodulation module, MAC layer, network layer protocols, etc., will be developed by manufacturers of wireless sensor networks utilising the chosen standard. After buying the items from the producers, the developers will construct their own apps on top. The assertion that a single standard can include all the capabilities needed for wireless sensor networks is untrue. Actually, there isn't a single standard that applies to the idea of WSNs. The current standards, particularly private standards, sometimes concentrate on the designated applications, which may diminish the help offered elsewhere. For instance, the support for data throughput may be compromised if a standard permits the product to have an extended system lifespan.

As their goals are to adopt as much support from the manufacturers as possible, the public standards perform considerably more evenly on the aforementioned concerns than the private standards. In order to assure the greatest level of compatibility, any creation of a public standard will take into account a wide range of potential factors. Since they only need to enhance the substance of the standard for their own purposes, private standards evolve more quickly than public standards.

Private standards, on the other hand, could not be accessible to the general public, as their name suggests.The IEEE 802.15.4 standard from 2003 is specifically created as a new Low-Rate Wireless Personal Area Network (LR-WPAN) standard for applications with low data requirements and constrained power and processing resources. It tries to solve the issues with the current standards, such WiFi and Bluetooth. For the purpose of using LR-WPANs, the standard provides the physical (PHY) layer and media access control (MAC) layer. 2003 saw the release of IEEE 802.15.4's first version. Unless otherwise specified, the version of the IEEE 802.15.4 standard discussed in this chapter.

The radio transceiver and the related low-level control mechanism are the key components of the PHY layer. By gaining access to the PHY layer, the MAC layer offers the definitions for the data flow. A common method is defined by the service specific convergence (SSCS) and IEEE 802.2TM Type 1 logical link control (LLC) for the higher layers to access the PHY and MAC layers' services.

The wireless sensor network applications often demand the employed protocol to be as basic as feasible in order to minimise system overhead due to the feature of restricted resource availability. The IEEE 802.15.4 architecture is straightforward and enables programmers to create application software that directly interacts with data flow at a low level. Although more established standards that adhere to the Open System Interconnection Reference Model (OSI) may be capable of providing dependable and plentiful service, the model's 7-layer specification renders that kind of architecture too complex to be useful for the construction of WSNs.

Devices with Full Function and Reduced Function

A full-function device (FFD) and a reduced-function device are the two categories of devices that participate in the IEEE 802.15.4 system, according to the specification (RFD). An FFD is given the capacity to construct a full-featured IEEE 802.15.4 stack, enabling it to operate as a PAN coordinator (which may start and control the whole network). This involves setting up the network and accepting requests for association from other devices, among other things. It may also change into a coordinator (which performs similar duties to those of a PAN coordinator, with the exception of establishing networks) or a regular device. An RFD is a piece of equipment that can carry out the stack's fundamental operations, or a rudimentary implementation of the IEEE 802.15.4 protocol.

The RFD is often used to connect to sensors and periodically transmit sensor values to the network. A FFD is allowed to communicate with other FFDs and RFDs according to the IEEE 802.15.4 standard. This feature allows the upper-layer to establish a multi-hop network by implementing routing protocols. An RFD, however, can only communicate with an FFD since it lacks network management capabilities, making it unsuitable for taking part in complex network operations like sending out beacon signals to synchronise network devices. As a result, in the same setting, an RFD may persist longer than an FFD. Since certain wireless sensor network applications need long-term, independent monitoring, it is impractical to routinely replace the dispersed sensor nodes' power supplies. RFDs are more suited to carrying out the activities of such sensor nodes in order to save energy.

Application code running on FFDs may execute more complex applications than application code running on RFDs, for example, applications such as network creation, network maintenance, packet relay, and network device management. This RFD performs a sensing duty on a regular basis, transmits the sensor reading to a controller, and then sleeps for a predetermined amount of time before waking up to do the subsequent round of sensing. The peer-to-peer topology is used to create cluster tree and mesh networks, while the star topology is used to create star and tree networks.

In the star topology, an FFD acting as a coordinator is designated as the primary device, or PAN coordinator, and is responsible for launching and overseeing the whole network. The PAN coordinator must be associated with before other coordinators and network devices may join the network. All network communications are managed by the PAN coordinator. A PAN is also necessary for the peer-to-peer topology.

To initiate the network start-up process, the IEEE 802.15.4 Standard and Wireless Sensor Network 13 coordinator are used. The peer-to-peer architecture, however, underlies network communications, which are not constrained by the PAN coordinator. Any FFD device may freely communicate with any other FFD device as long as they are close enough to do so. Any RFD device cannot directly communicate with any other RFD device; it can only communicate with its parent FFD device. A tree topology is created by RFD devices and the parent FFD device.

A single cluster network or a network with several clusters might be the topology of a cluster tree. There is only one cluster-head in a single cluster network (CH). When there is just one hop between each node and the cluster head, the network topology changes to a star topology. More than one cluster-head may be found in a multi-cluster network. Only the cluster-head may be reached by each node in a cluster. An upper level sub-network made up of all the cluster heads may communicate with their head, which might be a sink node linked to an external network or the head of the cluster heads, directly.

Nodes in various clusters interact via their cluster leaders rather than directly speaking to one another. A hierarchical design with clusters at the bottom level and the cluster-head network at the top level is shown in the cluster tree topology in displays a more intricate cluster tree architecture where each cluster, represented by a dotted cycle, is connected to another cluster by a border node. Border nodes may either be cluster heads or regular nodes. To establish a border node connection with the network, a designated device (DD) is necessary. Cluster 0 is formed by the DD device and its border node with cluster-head CH0. With one serving as a cluster-head and the other as a border node, CH1 and CH3 each have two logical addresses. Wireless nodes in wireless systems must share a common medium for signal transmission, just as in all other networks. The IEEE 802.15.4 standard specifies Multiple Access Control (MAC) protocols that describe how the wireless media is shared by the participating nodes. This is accomplished in a manner that optimises system performance as a whole. For wireless networks, MAC standards may range from

The scientific band of the ISM band is divided into 79 channels with a 1 MHz bandwidth via frequency-hopping spread spectrum (FHSS). Each portion of the information is sent to a distinct channel after being divided by the transmitter. The action is referred to as frequency hopping. The receiver has already been informed of the channel order or hop sequence that the transmitters will utilise. Bluetooth transmits data via FHSS.

With direct-sequence spread spectrum (DSSS), each bit is separated into a chip-like pattern of bits. The chip is created by using a pseudo-random code to conduct an XOR (exclusive-OR) operation on each bit. The chip, which is the result of the XOR operation, is then sent. The receiver decodes the original data using the same pseudorandom code.

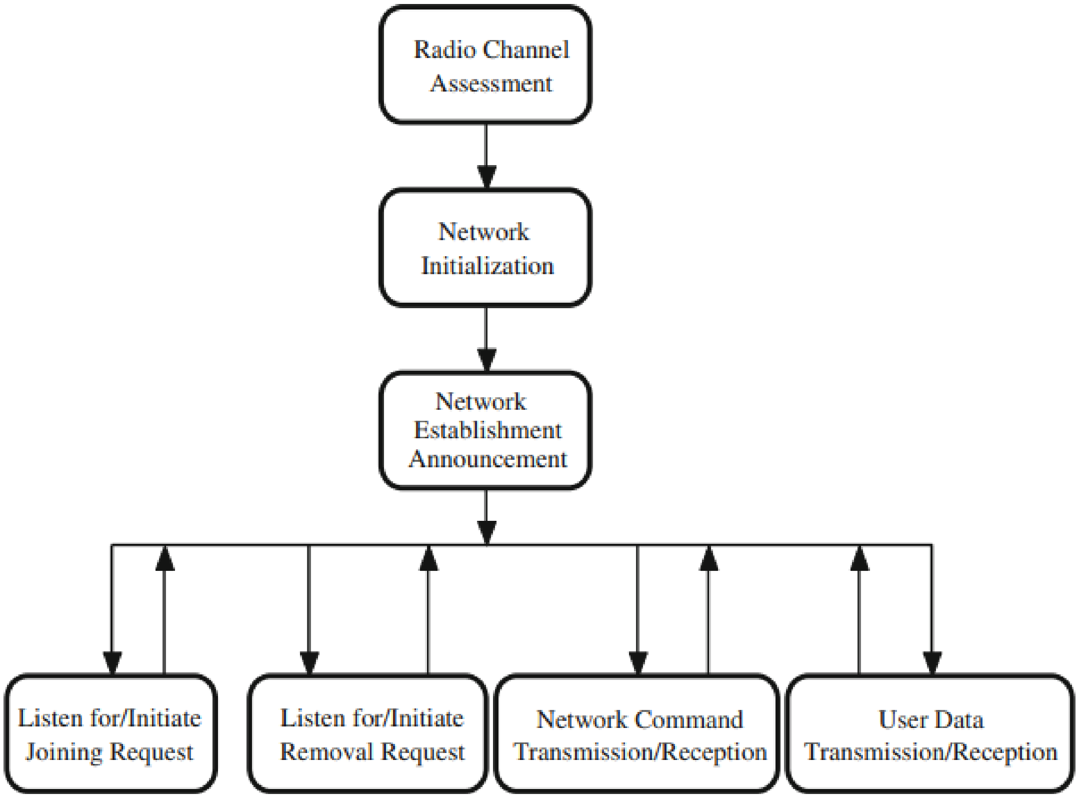

Radio Channel Assessment
Network Initialization
Network Establishment Announcement
Listen for/Initiate Joining Request
Listen for/Initiate Removal Request
Network Command Transmission/Reception
User Data Transmission/Reception

Figure 1: Discloses the Radio Channel assessment.

The spectrum that is accessible is split into subbands (i.e., channels) using frequency division multiple access (FDMA), where each channel is utilised by one or more users. Each user using FDMA is given a dedicated channel that has a distinct frequency from the channels allotted to other users. The dedicated channel is used by the user to communicate information. The inability of the channels to be extremely near to one another is the main issue with FDMA. Since transmitters that transmit on a channel's main frequency band also emit some energy on the channel's sidebands, a separation in frequency is necessary to prevent inter-channel interference.

Users may share the available bandwidth in the time domain, as opposed to the frequency domain, thanks to time division multiple access (TDMA). Each active node is given one or more time slots for the transmission of its data through TDMA, which splits a band into a number of time slots. Another method is code division multiple access (CDMA). It puts all nodes in the same bandwidth at the same time rather than dividing the available bandwidth into frequency or time slots. Each user has been given a unique code that serves as a barrier between their transmission and that of other users. Common names for CDMA include direct-sequence spread spectrum (DSSS). By utilising the illustration of several conversations occurring in the same space but in different languages, CDMA may be better understood. In this situation, those who can comprehend one language attend to that dialogue and ignore everything else that is being said in the other language. Figure 1 discloses the Radio Channel assessment.

They are implemented to monitor specific physical processes in almost all WSN applications. They are used to measure things like temperature, air pressure, human body radiation, chemical reactions, item movement, and bodily vitals, among other things. This allows us to get certain crucial details about the borders, also known as edges. Recognizing a border is essential for monitoring a physical technology's edge. The initial step in addressing the edge detection problem is generally seen to be identifying the border. There are various techniques for recognizing the edge in digital processing, but they are difficult to employ in the context of WSNs because the mobile nodes are not evenly spaced apart like pixels and because there is a shortage of computational and memory resources.

CHAPTER 2

WIRELESS SENSOR NETWORK TOPOLOGIES

K. Gopala Krishna, Associate Professor,
Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN
(Deemed-to-be University), Karnataka – 562112
Email Id- k.gopalakrishna@jainuniversity.ac.in

A key topic of study in recent years has been the effective design of wireless sensor networks. A sensor is a machine that reacts to and picks up input from environmental or physical factors, such as weight, heat, light, etc. An electrical signal is often transferred from the sensor's output to a microprocessor for further processing.

This article covers a general review of categorization, attack kinds, mobility, and routing protocols as well as several types of wireless sensor networks. An ADC turns the analogue data that the sensor obtains from the outside environment into digital data. Intelligent data transmission and manipulation are carried out by the primary processing unit, which is often a processor or a microcontroller. A radio system, often a short-range radio, is used in a communication system to transmit and receive data. A tiny battery, such as the CR-2032, is required to power the whole system since all of the parts are low-power gadgets.

Contrary to its name, a sensor node also includes processing, communication, and storage components in addition to the sensing component. Finally, a Sensor Node is now capable of collecting data from the real world, analysing networks, correlating data, and fusing data from other sensors and its own data thanks to all these characteristics, components, and improvements [5]–[8].

A network of gadgets that can wirelessly transmit the data obtained from a controlled field is known as a wireless sensor network. Multiple nodes are used to forward the data, and a gateway is used to link it to other channels like wireless Ethernet. Different sensors design, computer technology, and wireless system advancements have resulted from recent technology, transmission, and networking improvements. Such sophisticated sensors may serve as a link between the physical and digital worlds. Sensors are utilised in a wide variety of products, businesses, equipment, and environments and aid in preventing infrastructure failures, accidents, resource conservation, wildlife preservation, productivity growth, and security. Figure 2 discloses the WSN applications.

The development of VLSI, MEMS, and wireless communication systems has also led to the utilisation of networked embedded networks and systems. Therefore, you may create more potent microprocessors that are noticeably smaller in diameter than prior generation items with the aid of contemporary transistors. Tiny, low-cost, and low-power instruments, controllers, and actuators are now possible because to the shrinking of processing, computing, and sensing technologies.

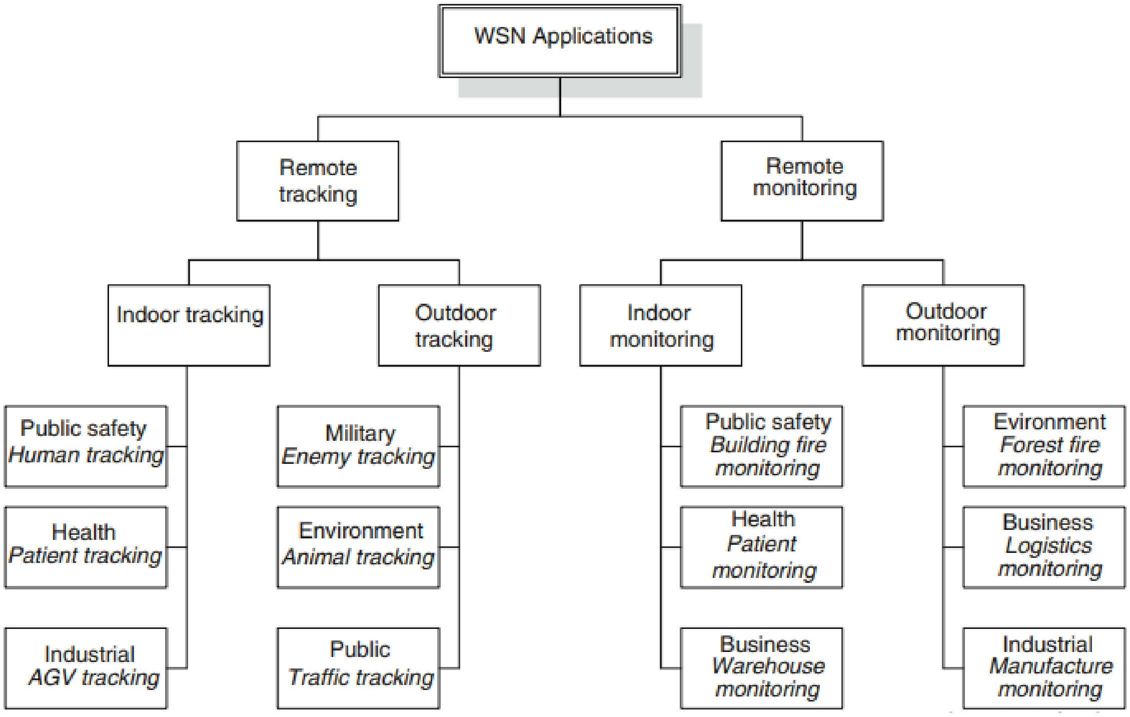


Figure 2: Discloses the WSN applications [9]**.**

Radio Channel Evaluation

Making sure the necessary transmission medium is always accessible is the first crucial step in building a wireless system. The specifics of this evaluation rely on the specifications for the wireless network that will be developed. For networks that use frequency hopping, the evaluation may concentrate on analysing all of the available channels before determining the hopping plan.

The evaluation performed for networks that employ frequency division multiple access is focused on finding the channel that is most suited for the network usage, such as the cleanest, that results in the fewest radio activities, etc. The number of nearby wireless frequency band-using systems is another crucial factor to consider during the channel evaluation phase. Multiple networks are quite likely to be active nearby since wireless sensor networks are simple to create. During the assessment stage, it is very important to try to prevent conflict with other networks. This book's Chapter 7 will go into depth on interference avoidance.

Energy detection, active scan, and passive scan are the three channel assessment functions that are specified by the IEEE 802.15.4 standard. Here is an explanation of these terms:Energy detection is precisely described so that the system can ascertain the energy level on the designated channels. Its energy level rises with any wireless signal activity in the selected channel. Consequently, any possible interfering sources may be found by employing energy detection. The best way to evaluate the channel is by energy detection, especially when the modulation and spreading properties of the undesired wireless signals differ from those of the IEEE 802.15.4 transceiver.

Passive and Active Scan: The system can determine how many comparable wireless networks are present nearby by using the active and passive scanning features. A FFD coordinator should implement at least one active scan before starting an IEEE 802.15.4 network. This function is carried out by transmitting a beacon request inside the FFD's personal operating area, which is a kind of synchronisation signal used to synchronise the network device and is often created by a network's PAN coordinator (POS).

The FFD coordinator will then record any more coordinators' answers, or named beacon frames, giving the network description, as illustrated. The present FFD coordinator may decide if it is feasible to launch the intended network in this region or on the given channel by comparing the output with the received descriptions.

As illustrated in a passive scan implementation enables the receiver of the present FFD to continuously scan the specified channel for network beacons. If more coordinators send out beacons with information about their networks, the beacons will be logged and handled in the same way as the current scan.

Network Initialization

The PAN coordinator implements network initialization. Before a network is really started, initialization of the network involves setting up several network settings. The working channel, the network identification, the assignment of the network address, and creating an IEEE 802.15.4 network beacon are some of the factors.

Setting of Network Parameters

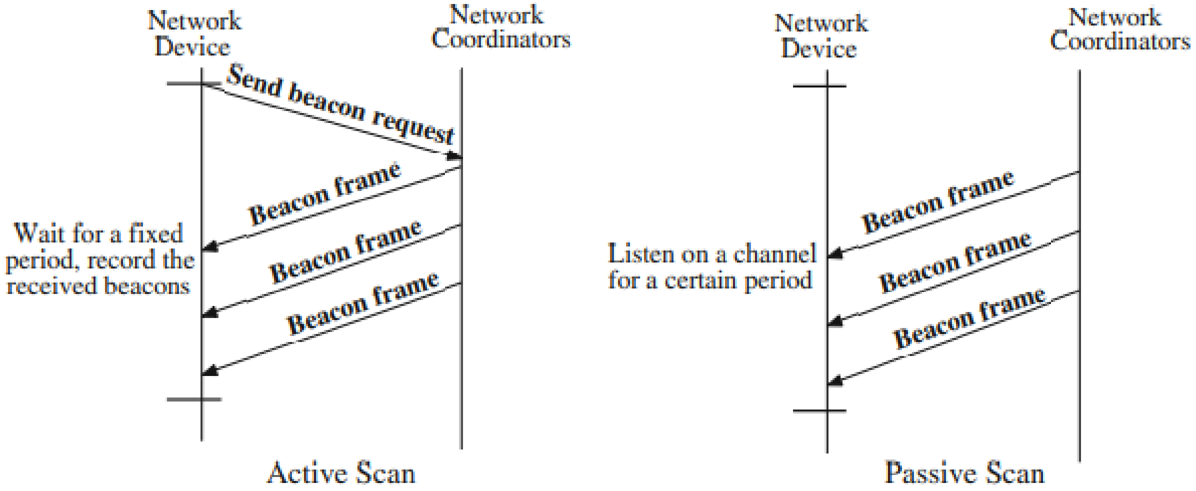


Figure 3: Discloses the network device analysis.

The working channel is chosen based on the findings of a channel evaluation that was previously mentioned. The usage of the radio frequency and the accompanying modulation methods are specified by the IEEE 802.15.4 standard. The frequency and modulation used are also used to specify the supported data rate. Over the three frequency bands specified in the standard, there are a total of 27 channels.

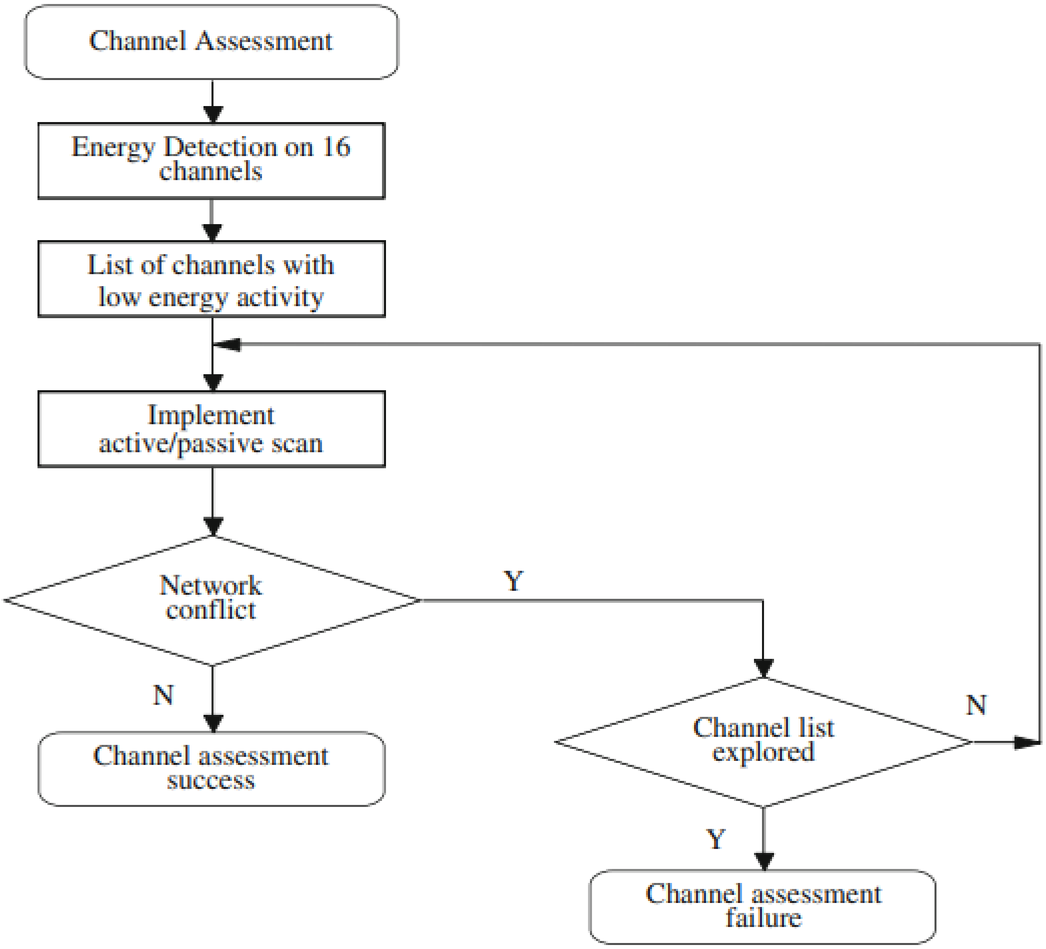

Channel Assessment
Energy Detection on 16 channels
List of channels with low energy activity
Implement active/passive scan
Network conflict
Y
N
Channel assessment success
Channel list explored
N
Y
Channel assessment failure

Figure 4: Embellishes the Channel assessment.

A strategy for frequency utilisation must be prepared in advance since the IEEE 802.15.4 standard does not permit dynamic data rate modification or frequency hopping.The choice of frequency band is also another problem at this point. It must abide with the regional radio laws in the area where the system is to be installed. Figure 3 discloses the network device analysis.

The system should choose a network identification so that other devices can recognise the network after the functional channel has been determined. The IEEE 802.15.4 standard as a network system includes a 16-bit network identifier (PAN ID) for identifying each network. Since the chosen PAN ID must be distinct from all other networks within the radio field of influence, it cannot be the same as any other network. As a result, information for the defined network may be usefully obtained from the active or passive scan.

The extended address mode and the short address mode are the two fundamental communication address modes as defined by the IEEE 802.15.4 standard. A 64-bit length number must be used in extended address mode; this requirement was specified in the device's firmware at the time of production. The device's uniqueness may be guaranteed by the 64-bit address.

The usage of extended address mode has the drawback of making any data packet's effective payload smaller. The usage of a 16-bit long integer is mandated by the short address mode. When the network is launched, the PAN coordinator is in charge of creating the 16-bit network address. A PAN coordinator may, for instance, establish its own network address to 0x0000. Frequency band assignment and data rate. Figure 4 embellishes the Channel assessment.

Band of frequency (MHz) Channel (Kb/s) Bitrate Modulation

The theoretical network capacity is determined by the short address mode length and cannot be more than 65,535 characters (i.e. 216). The effective payload size of a data packet in an IEEE 802.15.4 network may be increased by using the short address mode, however it must be correlated with the PAN ID. The short address's uniqueness cannot be guaranteed in any other case. There is no default short address allocation method in the standard; instead, network designers may create a suitable scheme depending on the needs of the application.

Super frame Construction

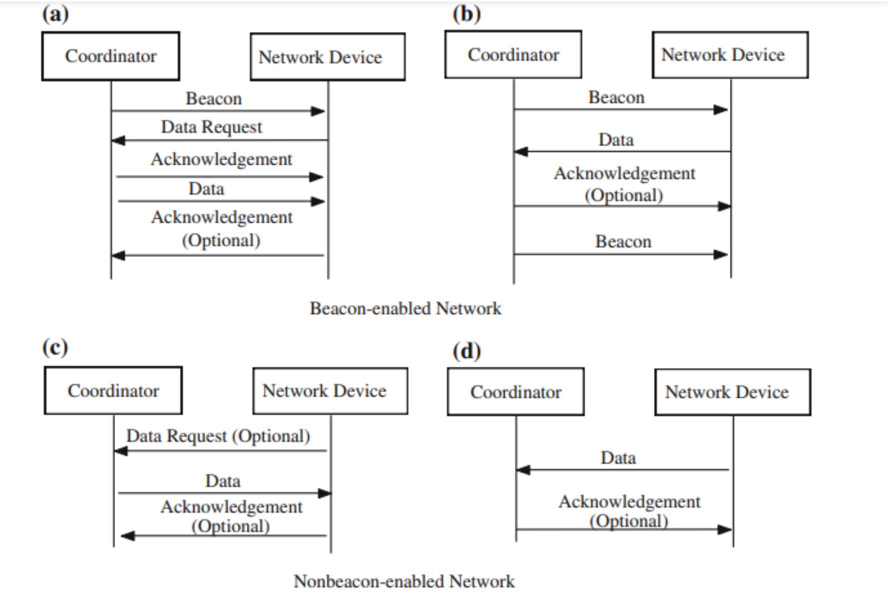


Figure 5: Discloses the Beacon enabled and non-Beacon enabled network.

Reduced duty-cycle settings enable the IEEE 802.15.4 standard's low power consumption capability. The transceiver is the part of a wireless system that uses the most power. An IEEE 802.15.4 transceiver's usual operating current ranges between 20 and 30 mA. If the transceiver is left on all the time, especially when the module is powered by batteries, this represents a large energy usage. The term "Superframe Structure" is defined in the IEEE 802.15.4 standard, which enables the system to use fewer transceivers while maintaining network functionality. Figure 5 discloses the Beacon enabled and non-Beacon enabled network.

Network Announcement of Establishment

The PAN coordinator may make the announcement that the network has been successfully established after the network parameters have been initialised. The network protocols in use dictate the specific process for announcing the creation of the network. The announcement's main objective is to let other gadgets know that the existing wireless system exists. There are two approaches to accomplish this goal: aggressively advertise or passively reply when a request is made. Some wireless protocols synchronise network processes using the regular beacon broadcasts. Beacon-enabled networks are this kind of network. It also provides information about the features of the present wireless networks, such as the operating channel, frequency band, geographical position, etc., to freshly started devices. The term "non-beacon-enabled network" refers to a network that is not beacon-enabled by the protocol. In this case, the PAN coordinator will continue to listen on the functioning channel and reply to any legitimate requests provided by the devices carrying out radio channel evaluations.

After the network's notification of its launch, a beacon signal will be periodically sent out for beacon-enabled networks in accordance with the SO and BO settings. The PAN coordinator must maintain persistent beacon transmission throughout the network's operational lifespan so that devices doing passive scans may detect it, and any active scans launched by other devices must also demand a response.

Start Joining Requests

When an IEEE 802.15.4 network is successfully initialised, the PAN coordinator takes over as the primary network management. To carry out the task of network management, the PAN coordinator's transceiver should always be listening on the chosen working channel, unless it is actively transmitting data.Any device that wants to join the network should carry out the following three steps:

To find the appropriate PAN coordinator, start an active scan (FFD only) or passive scan, synchronise with the network beacons if necessary (0 SO BO 14), and then ask to join the network by sending an associate request to the found PAN coordinator. The PAN coordinator may put the created process into action after receiving the joining request to verify it. The device receives a response including the network information (i.e., the network address) and decision after the PAN coordinator, if the request is approved, decides how to assign a network address to the device. The

PAN coordinator must react with appropriate comments if the joining request is denied. The network device may utilise the assigned address to execute network communication after receiving a response from the PAN coordinator, or it can use a predetermined procedure to handle the response of "joining failure."

Pay attention to/start a removal request

The procedure for handling a request for removal is the same as for a request for membership. The PAN coordinator has the ability to remove a device address from the list of authorised devices and inform the affected device of the removal. As an alternative, the PAN coordinator may carry out operations after receiving the network device's request to disconnect. The gadget is able to guarantee that the removal request is approved after receiving the notice from the PAN coordinator.

Transmission and reception of Network Commands

The primary uses of network command transmission and reception are for network administration. Without any user involvement, they are often invisible to users. A command that requires user input may, on occasion, wait for the user's instructions before continuing. As a result, the system architecture must include a processing module for this sort of usage. For instance, a network device should send a conflict notification command to the PAN coordinator if it discovers that another IEEE 802.15.4 network is active nearby and is using the same network ID. The PAN coordinator should then begin an active scan and broadcast the coordinator to find a new PAN ID. Using the IEEE 802.15.4 25 realignment command to build WSNs. In this instance, user involvement is necessary to complete the new PAN ID selection. Another instance is when a network system begins to raise the bar for adopting new devices; in this case, the higher layer management system must examine the specifics of every device that requests to be included.

Transmission and Reception of Data

According on the usage of a beacon, the IEEE 802.15.4 standard classifies data transmission and reception. The communication strategy .From a coordinator to a network device and from a network device to a coordinator are the two communication paths.The network beacons define a certain time that the superframe structure falls inside.The transceivers of the network devices become synchronously functional and begin to carry out the intended functions within the superframe's range as soon as they receive the beacons. The duration of the transceivers' active time is defined by the superframe structure. When an active time is over, the transceivers should cease operating and be silent until the next inactive period begins and the next beacon appears. The synchronisation method gives the system an opportunity to save energy without compromising communication. The PAN coordinator, which must be powered on for the duration of the network, sends the network beacons to guarantee that all devices synchronise with the same source.

The developers may not have had access to the actual implementation of the mechanisms stated or described in the standard since the majority of the functions used in data transfer are wrapped inside the stack. Despite this, it is still important to understand what the system accomplishes. Particularly given that a large number of stacks will deal with the issues found and send them back to the apps for manual processing by the users. For instance, the coordinator is unable to permanently keep the pending data in the local buffer owing to hardware limitations. The stack will send an event of type "TRANSACTION EXIRED" to the application after a certain amount of time. If there isn't enough room, the stack will additionally produce an event of "TRANSACTION OVERFLOW" when the coordinator wishes to store fresh pending data. Successful transmission, missing acknowledgement, and CCA failure are all intended to return a matching event to the application for the CSMA-CA implementation. It is crucial for the embedded software architecture to properly handle the event returning from the stack in the function block of "Network Command Transmission/Reception."

ZigBee stack structure

A method to accomplish wireless communication with a low data rate and low power consumption is defined by the IEEE 802.15.4 standard. It only supports peer-to-peer and star topologies. The term "complete network system" is not defined. Technically speaking, the IEEE 802.15.4 standard is more suited for usage in wireless communication than in large-scale network applications since it concentrates on the development of the PHY and MAC layers. In order to build large-scale wireless networks on top of the IEEE 802.15.4 standard, which only specifies the PHY and MAC layers, for low-rate wireless personal area networks, the ZigBee specification was developed in 2004 by the ZigBee Alliance (LR-WPAN). The honeybee, which employs a zigzag-style dance to communicate with other individuals, is where the term ZigBee originates. Developers of the ZigBee protocol seek to mimic this behaviour so that LR-WPAN may easily handle complicated communication duties.

The network (NWK), security, and application layers are all defined in the stack profile provided by the ZigBee standard. It is the responsibility of developers to either create their own application profiles or integrate with the open profiles offered by the ZigBee Alliance. Smart energy, building automation, home automation, home and hospital care, telecom applications, consumer electronics control, and industrial process monitoring and control are all covered by the publicly accessible ZigBee profiles.

Topologies of Stars

Each node in a star topology communication system attaches directly to a gatekeeper. Multiple distant nodes may receive or deliver messages from a single gateway. The nodes are not allowed to communicate with one another in instar topologies. As a result, the gateway and the distant node are able to communicate with minimal latency (base station).The gateway must be close to all of the nodes' radio transmission ranges since it relies on only one node to control the network. The benefit includes the capacity to keep the electricity consumption of the distant nodes at a minimal and just under control. The total number of connections transmitted to the hub determines the length of the network. Figure 6 discloses the ZingBee Alliance.

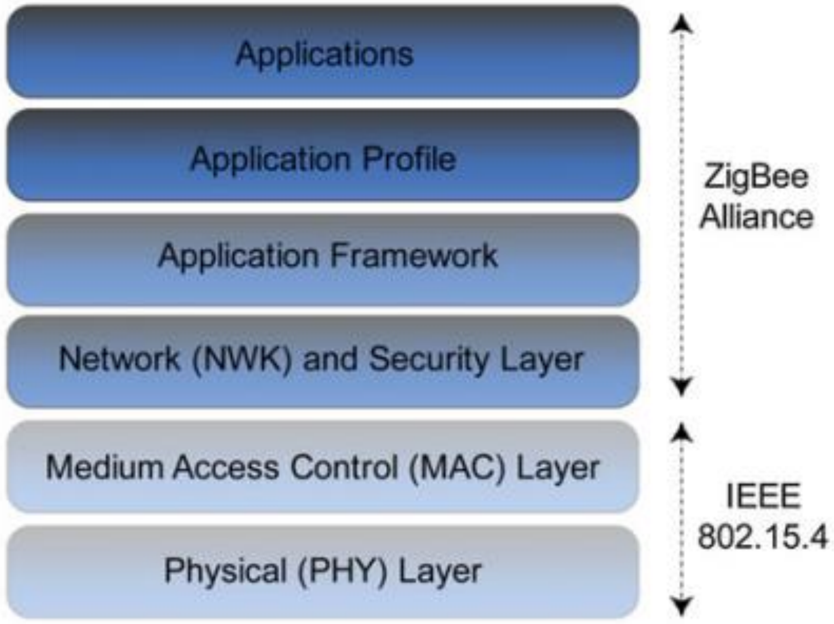


Figure 6: Discloses the ZingBee Alliance.

Adds the packet's metadata, such as the destination address, to the beacon frame's "address awaiting list." The network device will be aware whether a packet is waiting on the coordinator upon receipt of the beacon frame. The network device has two ways to go forward: The network device should automatically transmit the data request command to the coordinator utilising the slotted CSMA-CA (carrier sense multiple access with collision avoidance) if the network device's macAutoRequest, an indication for the MAC response mode, is set to TRUE. The stack should offer the application layer with a primitive of "Beacon Notify" if the macAutoRequest is set to FALSE, and allow the application choose whether it needs to submit a data request command. The coordinator will initially choose how to acknowledge the network device after receiving the data request instruction. The coordinator transmits the acknowledgment within the predetermined time frame of macAckWait.Duration if it can access the local buffer and detect that the pending packet for that network device is there. The coordinator shall send the acknowledgment with the data pending field, an indication of the pending status, set to 1 if it is unable to finish the acknowledgement transmission within the specified time frame. If the data pending filed was set to 1 in the previous acknowledgment frame, the coordinator should transmit the data packet to the network device after sending the acknowledgement. If there is no data waiting, the length of the data payload will be 0. If the data pending field in the acknowledgment is set to 1, the network device will activate its receiver upon receiving it for a maximum of aMaxFrameResponseTime. To confirm the successful receipt, the network device may be needed to send back an acknowledgment. The slotted CSMA-CA transmission method should be used for data frame transfer from the coordinator to the network device. Figure 7 discloses the application layer.

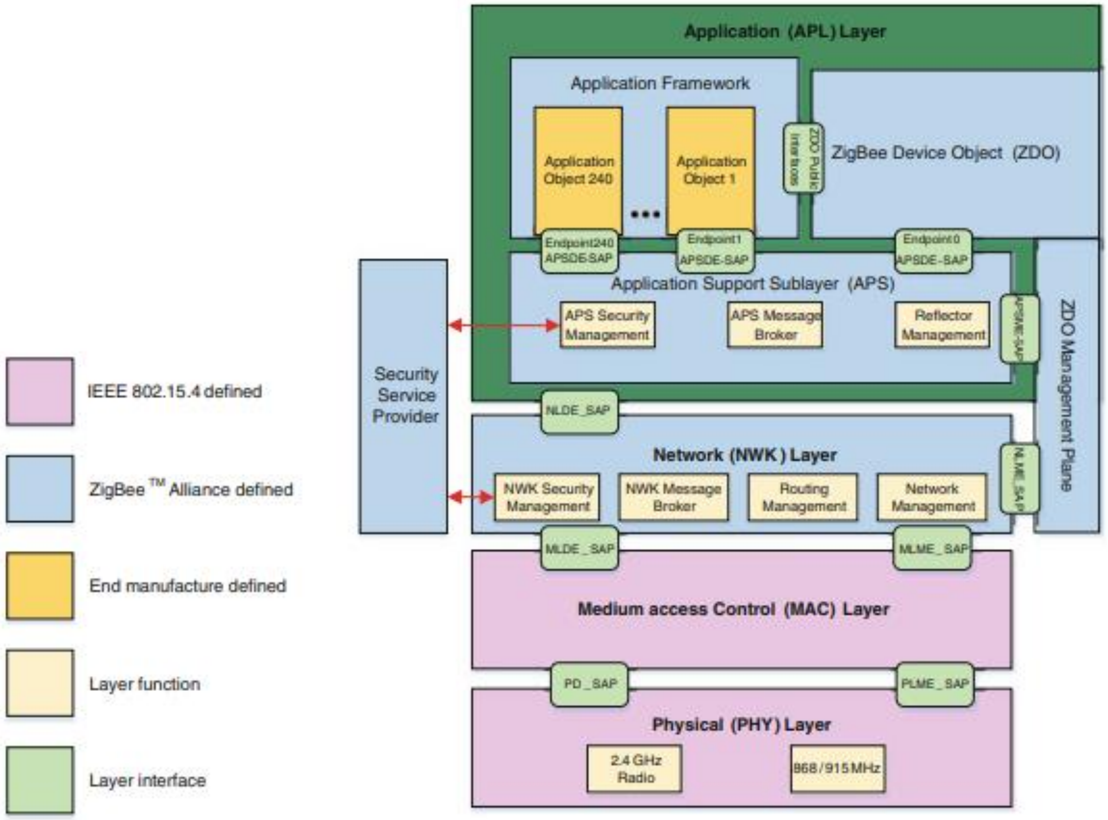


Figure 7: Discloses the application layer.

If a coordinator in a network without beacons wants to send a data packet to a network device, it has two options: either send the packet directly to the device using unslotted CSMA-CA, or store the data in the local buffer and wait for the network device to send the coordinator a data request command after a predetermined amount of time has passed.

The procedure for polling information from the coordinator in a network without beacon support is the same as it is in a network with beacon support. However, as there is no superframe structure at the moment, the CSMA-CA mechanism should utilise its unslotted form.

Network apparatus Coordinator

If the network device has a packet to broadcast to the coordinator after receiving the conventional beacon, it may start the conversation using the slotted CSMA-CA. It must make sure that the transmission and acknowledgment can be completed before the active time expires. If not, the operation will be put on hold and start again at the beginning of the following active period. If a network device has a data packet to send to the coordinator in a non-beacon network Indirect transmission is the process of keeping the data on the coordinator and sending it out until a request is received from the network device. Low power consumption is the goal of the indirect transmission. The radio receiver is usually off to save energy, and the network devices are often in a sleep mode. By storing data on the coordinator, it will be easier for network devices to access the data without constantly turning on the receiver. When a time slot opens up, the network device may transmit the data request command. Figure 8 discloses the different types of topologies.

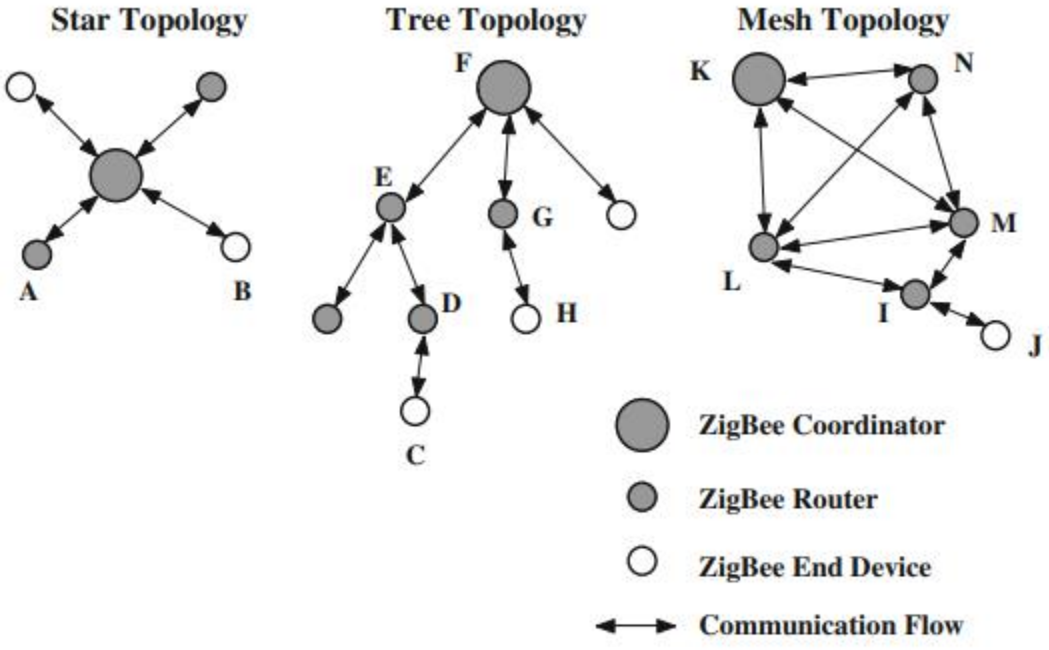


Figure 8: Discloses the different types of topologies.

Topological Tree

Cascaded star topology is another name for tree topology. Each node in a tree topology links to a node higher up the tree before connecting to the gateway. The primary benefit of a tree topology network is that it is simple to expand a network and to identify errors. This network's weakness is that it is largely dependent on the network segment; if it breaks, the whole network would come to an end [10]–[12].

The star topology is the most straightforward to realise. The ZigBee coordinator serves as the network's hub, and in order to create a network, additional ZigBee devices, such as ZigBee routers and ZigBee end devices, must connect to the coordinator. Due to the ZigBee coordinator's limitations, the star topology is not appropriate for large-scale applications. Devices that are outside of the coordinator's radio range cannot be networked because every device must connect to the network through the coordinator's ZigBee radio. The primary drawback of the star topology is that the whole network would be impacted if the central node (the ZigBee coordinator) fails. A star network prohibits direct communication between devices. For instance, in the initial topology, if Device A needs to send a message to Device B, the message will first be routed to the ZigBee coordinator before being forwarded to the target.

Comparatively speaking, the tree topology is more adaptable than the star topology. Its distribution is not limited by the coordinator and may be expanded by adopting auxiliary devices utilising ZigBee routers. An end device must join the tree through a router device, and a router device must join the tree via another router device in order for a tree network to be formed (the ZigBee coordinator can be used as a router device as well). The distinction is that a router device has the ability to adopt end devices or other router devices as its offspring, also known as sub-devices. End devices are not allowed to have kids. Consequently, a parent device cannot be an end device. These guidelines must be followed by the network communications in a tree network. For instance, if device C is to transmit a message to device H, the message should first go via devices D and E before returning to device F. Device F then transmits the message to device H via device G. The message must leave the ZigBee Router in order to meet the requirement.

Wireless sensor networks and ZigBee 35 source nodes ascend the tree to the closest common ancestor, then descend it to the destination node. The drawback is that, should one of the route's connections fail, there is no backup path to take. The routing protocol may, however, be implemented rather easily since each device just has to keep a tree table and send messages to the parent or descendant node that leads to the destination.

The mesh topology has a similar structure to the tree topology, but it offers more flexible network connections. No router is required to transmit a message to the parent device before communicating with another router. When some of the possibilities fail, the network routing algorithm would choose an alternate route from the available choices.

ZigBee Hybrid Network

ZigBee networks may create a variety of architectures by properly combining mesh, star, and tree topologies. Among these, the mesh topology is the most well-liked network topology due to its adaptable network setup and network communication's capacity to self-heal.

Network configuration that is adaptable

Mesh topology and tree topology are equivalent in terms of logic relationships. The mesh topology may be seen as a modified variation of the tree topology since it uses the same criteria to construct the network.

A mesh topology is a star topology that has been magnified. Since the router nodes may initiate contact with one another, if the application calls for it, the communication flows can be programmed to aggregate at a single point. Consequently, the mesh topology allows for variable network construction.

A mesh network, however, cannot be connected to a star or tree network.

- The power to cure oneself

As was said above, both the star network and the tree network share the same crucial flaw: if the centre node or any link on the route fails, the whole network would come apart. By navigating around the broken connections or nodes, the mesh network may use the dynamic routing protocol to fix the issue.

Hybrid building

Instead of one of the three topologies mentioned above, ZigBee networks often have a hybrid structure. The ZigBee coordinator and ZigBee router components make up Layer 1. The router components build the framework of the network where the routing protocols may be used. The layer 2 ZigBee end devices join 36 other end devices. Principle of Wireless Sensor Networks 2 The parent ZigBee router devices connect to the network. A ZigBee end device can only communicate with its parent device, according to the ZigBee standard. Therefore, the network communication relay does not include the ZigBee end devices. Any network communications that take place between a ZigBee end device and other ZigBee network devices must first be transmitted to the matching parent device before being sent to the intended recipient. A star topology is formed by the parent ZigBee router device and any linked ZigBee end devices.

Topologies of Mesh

Within its radio broadcast range, the Mesh topologies provide data transfer from one node to another. A node requires an intermediary node to transfer the message to the target node if it wishes to send a message to another node that is beyond the radio communication range. This mesh architecture has the benefit of making network failure isolation and detection simple. The network's size and high investment requirements are a drawback.

CHAPTER 3

TYPES OF WIRELESS SENSOR NETWORK

Shweta Gupta, Associate Professor,
Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN
(Deemed-to-be University), Karnataka – 562112
Email Id- shwetagupta832000@gmail.com

The kinds of networks are chosen in accordance with the environment, allowing for their deployment beneath water, underground, on land, etc. Various WSN types include:

1. Terrestrial WSNs
2. Underground WSNs
3. Underwater WSNs
4. Multimedia WSNs
5. Mobile WSNs

A sensor is a device that is used to capture data about a physical process or a physical occurrence and convert it into electrical signals that can be processed, measured, and analysed from the viewpoint of an electronics engineer. Any kind of information from the actual environment, including temperature, pressure, light, sound, motion, location, flow, humidity, and radiation, may be considered a physical process in the description of a sensor given above. In order to record, observe, and respond to an event or a phenomena, a sensor network is a structure made up of sensors, processing units, and communication components. The controlling or observing body may be a consumer application, a governmental body, a civil organisation, a military organisation, or an industrial entity, and the events may be connected to anything, including the physical world, an industrial environment, a biological system, or an IT (information technology) framework.

Such sensor networks may be used for data collecting, surveillance, monitoring, medical telemetry, and remote sensing. Researchers and engineers believe that Wireless Sensor Networks are a significant technology for the twenty-first century as a whole. Recent advancements in MEMS sensors (Micro Electro Mechanical System) and wireless communication have made it possible to deploy inexpensive, low-power, small, and smart sensors across a large area and connect them through wireless networks and the internet for a variety of civic and military purposes. A Wireless Sensor Network is made up of Sensor Nodes, which are installed in high density and often in huge numbers and enable connection, embedded computing, data processing, and sensing.

Driving Forces behind Wireless Sensor Networks

New sensor designs, information technologies, and wireless systems have been made possible by recent advancements in engineering, communication, and networking. Such sophisticated sensors may serve as a link between the physical and digital worlds. Sensors are employed in a wide range of products, businesses, equipment, and environments and aid in preventing infrastructure failures, accidents, resource conservation, wildlife preservation, productivity boosts, security, etc.

The development of VLSI, MEMS, and wireless communication technologies has also led to the utilisation of distributed sensor networks and systems. You may create more potent microprocessors that are noticeably smaller in size than prior generation items with the aid of contemporary semiconductor technology. Tiny, low-cost, and low-power sensors, controllers, and actuators are now possible because to the shrinking of processing, computing, and sensing technologies.

Components of WSN

It is possible to separate a typical wireless sensor network into two components. As follows:

Structure of a sensor node network

Input Node in a WSN, a sensor node is made up of four fundamental parts.
Power Source Sensor Processing Unit Wireless Sensor Networks Sensor Node Communication System. An ADC turns the analogue data from the physical environment that the sensor has collected into digital data. An intelligent data processing and manipulation is carried out by the primary processing unit, which is often a microprocessor or a microcontroller.A radio system, often a short-range radio, is used in a communication system to transmit and receive data. A tiny battery, such as the CR-2032, is required to power the whole system since all of the parts are low-power gadgets.

Contrary to its name, a sensor node also includes processing, communication, and storage components in addition to the sensing component. A Sensor Node is in charge of gathering data from the physical world, network analysis, data correlation, and fusion of data from other sensors with its own data thanks to all these characteristics, components, and improvements.

Network Structure

The networking of these sensor nodes is similarly critical when several sensor nodes are distributed across a vast region to cooperatively monitor a physical environment. A sensor node in a WSN uses wireless communication to connect not only with other sensor nodes but also with a Base Station (BS).

Network Architecture for Wireless Sensor Networks

The sensor nodes cooperate with one another to complete the job after receiving orders from the base station. The sensor nodes deliver the required data back to the base station after gathering it.

A base station may connect to other networks over the internet as well. A base station processes the data it receives from the sensor nodes in a straightforward manner before updating the information and sending it over the internet to the user. Single-hop network architecture is used when every sensor node is linked to the base station. Long distance transmission is technically feasible, but it will need substantially more energy than data gathering and calculation.

Wireless Sensor Networks Single Hop Sensor Architecture

As a result, multi-hop network design is often used. The data is transferred across one or more intermediary nodes rather than a single connection between the sensor node and the base station.

Wireless Sensor Networks Multi-Hop Network Architecture

Two methods may be used to do this. Network architecture types include flat and hierarchical. The base station transmits orders to all of the sensor nodes in a flat design, however the sensor node that matches the query will react utilising peer nodes through a multi-hop network.

Wireless Sensor Networks Multi-Hop Flat Network Architecture

A cluster of sensor nodes is created in a hierarchical topology, and the sensor nodes communicate data to matching cluster leaders. The data may then be sent to the base station via the cluster heads.

Multi-Hop Hierarchical Wireless Sensor Networks Network Architecture

Networks of Wireless Sensors are categorised
Wireless Sensor Networks are installed in accordance with the needs of the application and are very application-specific. As a result, one WSN's characteristics will vary from those of another WSN. Regardless of the application, the following categories may be applied to wireless sensor networks in general. Mobile and Static Determined and Nondeterministic WSN Single and many base stations for WSN Mobile Base Station and Static Base Station for WSN WSN Multi-hop and Single-hop Self-Configuring and Non-Self-Configuring WSN both heterogeneous and homogeneous WSN Mobile and Static. Many applications use static networks, where all of the sensor nodes are permanent and immobile. Certain applications, particularly those involving biological systems, need for mobile sensor nodes. We refer to them as mobile networks. Animal monitoring is a kind of mobile network.

WSNs that are deterministic and nondeterministic

The location of a sensor node is computed and fixed in a deterministic WSN. Only a few applications allow for the deployment of sensor nodes that have been designed in advance. Due to a number of reasons, such as hostile operating conditions or severe environments, it is often not feasible to determine the location of sensor nodes. Such networks need a sophisticated control mechanism since they are nondeterministic.

Both single and multiple base stations WSN A single base station that is near to the sensor node area is all that is used in a single base station WSN.

In the case of a multi base station WSN, more than one base station is employed, and a sensor node may send data to the nearest base station. All sensor nodes connect with this base station.

Mobile Base Station WSN and Static Base Station

Even base stations may be stationary or mobile, much like sensor nodes. A static base station is permanently located, often not far from the sensing area. To balance the load on the sensor nodes, a mobile base station travels around the sensing area.

Multi-hop and Single-hop WSN

The sensor nodes of a single-hop WSN are directly linked to the base station. Peer nodes and cluster heads are used to transmit the data in multi-hop WSNs in order to save energy.

WSNs that are both self-reconfigurable and not self-configurable

The sensor networks of a non-self-configurable WSN are unable to organise into a network on their own and must depend on a control unit to gather data. The sensor nodes in the majority of WSNs are able to organise and maintain the connection and cooperate with other sensor nodes to complete the mission.

WSNs that are heterogeneous and homogeneous

All sensor nodes in a homogeneous WSN have comparable levels of energy consumption, computing power, and storage. When using a heterogeneous WSN, the processing and communication activities are separated in accordance with which sensor nodes have greater computing demands?

WSN network topologies

A WSN might be a single-hop network or a multi-hop network, as we have previously seen. The various network topologies that are used in WSNs are listed below.

Skyline Topology

Each node in the network is linked to the hub, which serves as the network's single centre node and is also referred to as the switch in star topology. Star topology is relatively simple to use, create, and grow. The hub plays a crucial function in the network since all data passes through it, and if the hub fails, the whole network may also collapse.

Star Topology Wireless Sensor Networks

Topology of trees

In a tree topology, there is a single root node at the top of the network, and this node is linked to several nodes at the next level, and so on. The root node has the greatest processing and energy usage, which decreases as we go down the hierarchical hierarchy.

Networks of Wireless Sensors and Tree Topology

Mesh Topography

Each node in a mesh topology works as a relay for the data of other linked nodes in addition to delivering its own data. Fully Connected Mesh and Partially Connected Mesh are further categories for mesh topologies. A node is linked to one or more of its neighbours when a mesh topology is partly connected, while in fully connected mesh topology, every node is connected to every other node.

Wireless sensor network applications

The potential uses for wireless sensor networks are, theoretically, limitless. The following is a list of some of the most popular uses for wireless sensor networks.HVAC (Heating, Ventilation, and Air Conditioning) in Air Traffic Control (HVAC)

1. Factory Assembly Line
2. Vehicle Sensors
3. Management and surveillance of the battlefield
4. Health Applications
5. Highway and Bridge Monitoring
6. Disaster Preparedness
7. seismic detection
8. Managed Electricity Load
9. Control and observation of the environment
10. Inventory Control Industrial Automation

Health Care Security Systems for Individuals
Systems for Tsunami Alerts
Monitoring and Sensing of the Weather

Address Management for ZigBee

The bottom layer (PHY and MAC) of the ZigBee stack is built using the IEEE 802.15.4 standard, making the 64-bit extended address and the 16-bit network address both usable by ZigBee networks. They are insufficient to distinguish between different things that have the same physical location. To resolve the issue, the idea of Endpoint addressing is given in the ZigBee standard illustrates how addresses are used in a ZigBee network when two ZigBee devices, A and B, must interact with one another. The three terminals on device A correspond to the three sensors on device B. Using either its IEEE 802.15.4 64-bit extension address or its 16-bit network address, terminal 1 on device A may ask device B to create a wireless communication channel in order to initiate connection with the temperature sensor on device B.

How can device B be made to understand that the communication is for the temperature sensor and not for any of the other two sensors? To aid the system in differentiating between the many items present on a single physical device, the ZigBee standard includes a sub-level addressing mode called Endpoint. Endpoint is a classification that essentially exists in the stack.
Up to 240 virtual objects may be supported by a single ZigBee device (endpoint 0 is used for endpoint management). Each virtual item is unique and has the ability to exist independently of other things. The ZigBee stack operating on the destination ZigBee device may quickly find the intended item if the communication's initiator specifies which endpoint it is seeking. Particularly for wireless sensor networks, the ZigBee specification's Endpoint notion is helpful. Typically, a sensor node has numerous sensors to perform various sensing activities.

The ZigBee specification's communication foundation is profile management. It contains of well-defined agreements on messages, message formats, and processing actions that allow system collaboration. The many components may build an interoperable, distributed application by adhering to the same profile. Additionally, there is no need to worry about compatibility as the items from various manufacturers may connect with one another without issue.

The Profile ID in is an 8-bit number that identifies the current profile's attribute. Public profiles are those that have been defined by the ZigBee Alliance and include Home Control Stack Profile, Building Automation Stack Profile, Plant Control Stack Profile, etc. Private profiles are those created by the makers specifically for the designated applications. Developers may request a profile ID by submitting an application to the ZigBee Alliance. Due to administrative requirements, the profile ID must be distinct. Users do not need to request permission if the profile is defined for research purposes. The ZigBee public profiles and accompanying IDs are shown in Figure 9 discloses the zigBEE devices.

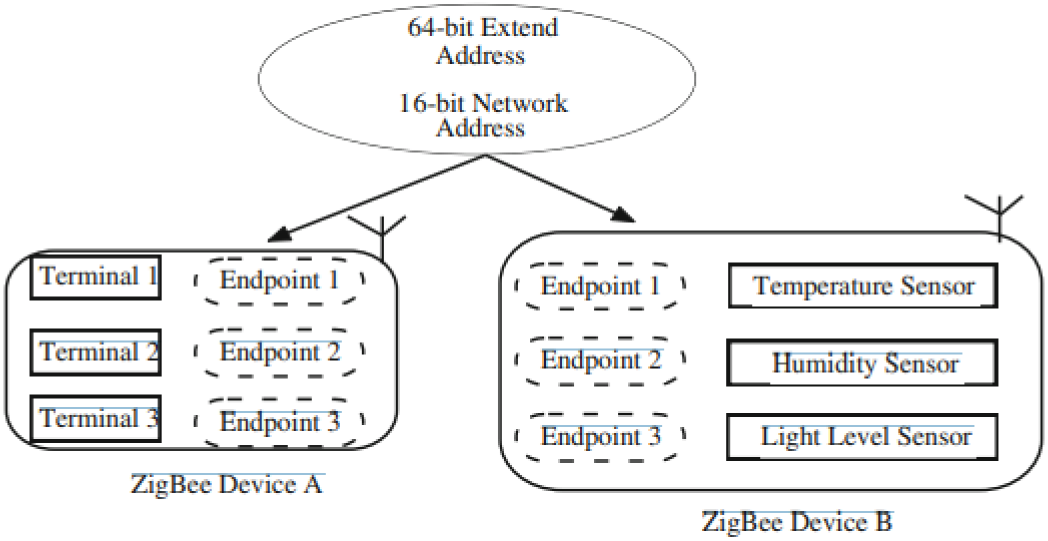


Figure 9: Discloses the zigBEE devices.

Terrestrial WSNs

Terrestrial WSNs, which are composed of "hundreds to thousands of wireless sensor nodes deployed either in an unstructured (ad hoc)" or organized (pre-planned) way, are capable of effectively interacting with base stations. The sensor nodes are randomly scattered around the target region that is dropped from a fixed plane in an unstructured manner. The preplanned or structured mode takes into account grid layout, 2D and 3D placement models, and optimum placement [11]–[13]. The battery power in this WSN is limited, however as a backup power source, the battery is fitted with solar cells. These WSNs' energy saving is accomplished by the use of low duty cycle functions, minimalizing delays, effective routing, and other techniques.

Terrestrial sensor networks and underwater sensor networks have different characteristics.

These are how the two communication technologies vary from one another:

Cost and Size: While water is used for communication in underwater networks, air is used for communication in terrestrial networks. While underwater sensors are costly gadgets, terrestrial sensor nodes are less expensive because of their smaller size. This is because underwater transceiver gear is expensive and has to be shielded from the harsh underwater environment.

Deployment: While terrestrial sensor networks are widely used, underwater sensor deployment is less common because of the high cost and technical difficulties. Power: Due to the longer distance and more intricate signal processing required at the receiver, acoustic underwater communication requires more power than terrestrial communication. Because of the challenging channel conditions, better signal processing is needed underwater. Underwater networks demand more energy usage, which raises the need for larger batteries.

Memory: The storage capacity of terrestrial sensor nodes is very constrained. Due to the intermittent channel need, underwater sensor nodes need to collect more data.

Subterranean WSNs

In terms of deployment, upkeep, equipment costs, and careful design, subterranean wireless sensor network are more costly than terrestrial WSNs. The WSNs networks are made up with several sensor nodes that are buried in the ground to track conditions there. Additional sink nodes are positioned above the ground to transmit data from the nodes to the base station. The wireless sensor networks buried underneath are challenging to recharge. It is challenging to recharge the sensor energy nodes since they have limited battery power. Additionally, the significant amount of attenuation and signal loss in the subterranean environment that make wireless communication difficult.

Water-based WSNs

Water covers more than 70percent of the total of the surface of the globe. These networks are made up of submerged vehicles and several sensor nodes. Data from these sensor nodes is gathered by autonomous underwater vehicles. Broadband and sensor failures, as well as a high propagation latency, provide difficulties for underwater communication. WSNs have a constrained battery that can't replace or recharged underwater. The evolution of underwater networking and communication methods is a factor in the problem of energy saving for underwater WSNs.

Multimedia WSNs Multidisciplinary wireless sensor nodes have been suggested to allow for the tracking and observation of events that take the form of multichannel, including audio, video, and image. These networks are made up of inexpensive sensor nodes with cameras and microphones. For data compression, retrieval, and correlation, these nodes are linked to one another through a wireless connection.

Discovery of Devices and Services

The ZigBee specification offers a system for finding devices and services in the network, which streamlines and standardises service delivery. The device discovery command may be issued as either a broadcast message or a unicast message, and it supports both the IEEE 64-bit and 16-bit network addresses. For storing node descriptors of the devices that are in sleep mode, a network needs have a major discovery cache device, which may be a router or a coordinator. Any device transfers its descriptor data to the main discovery cache before entering sleep mode. When the requested device is in sleep mode, it is the main discovery cache device that answers. Light Switch Profile really carries out the implementation (0x01)

For instance, if a ZigBee device that has just joined the network wants to know the network address of the coordinator but only has access to the coordinator's 64-bit extend MAC address, or if the device wants to know the network address of devices that can control lights, the ZDO can assist in sending out formatted broadcast queries to the network or a unicast query to a particular device and getting the results once the discovery is complete. One of the protocols included in the ZigBee stack is the ZDO. Every ZigBee device that is using a ZigBee stack has its own ZDO instance, which may handle information processing under ZDO administration without any user input. The developers should think about how to structure the query submission and handle the results.

ZigBee Binding

Support for the idea of binding, which is a logical relationship between two endpoints situated in distinct devices, is one of the ZigBee specification's important features. It is common in the creation of sensor network applications to transmit control messages from one point to many destinations, from several destinations to one point, or from one point to one destination. Depicts the scenario, which includes the following three circumstances:

1. More than one light may be controlled by a single switch.
2. One light switch controls one light, which is a common occurrence when a central switch is intended for usage in a warehouse. This is a typical occurrence in everyday life: many light switches controlling a single light. The design of the light control in the hallway or on the stairs often uses this.

Lighting Switch

Because utilising the usual way to handle the scenarios in would result in a significant amount of work being repeated, the binding mechanism may make the processes considerably, the coordinator is chosen to store the binding table since it is meant to be powered on throughout the duration of the network. The table now has two entries: the first element lists the source address and endpoint of Switch 1, as well as the corresponding addresses and endpoints of Lights 1 and 2. The address and endpoint of Switch 2 and Light 3's corresponding address and endpoint are also noted in the second entry. Switch 1 may transmit the coordinator the command and its own address if it needs to switch on Lights 1 and 2. The coordinator will look through the table after receiving the directive to identify Lights 1 and 2's addresses. The coordinator then substitutes Lights 1 and 2's addresses for the instruction's target addresses before sending it out automatically. Switch 1 may thus control Lights 1 and 2 thanks to their binding. Additionally, the instruction may be processed fast, increasing the efficiency of execution as a whole.

Wireless Sensor Network

The Internet Engineering Task Force (IETF) created 6LowPAN, which stands for IPv6 over IEEE 802.15.4 low-power wireless personal area networks (L-WPAN), in 2007. The most recent iteration of the Internet Protocol is IPv6. IPv6 is natively supported by IEEE 802.15.4 low-power wireless sensor networks thanks to 6LoWPAN. As a result, any wireless node in a wireless sensor network based on 6LoWPAN may now be accessed over the Internet. By means of an adaption layer and the optimization of associated protocols, 6LoWPAN standards allow the effective use of IPv6 across low-power, low-rate wireless networks on basic embedded devices, according to Shelby and Bormann's 2009 technical description.

Source for ZigBee Coordinator: Switch The first stop is Lights 1 and 2.Switch 2 is the source. Light 3 is the destination. 2 Switches 1 ZigBee Device One switch, two lights 1 light, 2 lights, and 3 ties ZigBee networks' use of binding.

Wireless Sensor Networks Basics

1. Because it permits the use of current network infrastructure built on IP-based protocols, it promotes interoperability.
2. Without the use of gateways, wireless devices may be quickly and simply linked to the Internet.
3. Enabling IP also makes it possible for the network to employ all IP-based technologies, including proxies, which are well-known and have a track record of success when used for higher-level services in expansive networks.
4. HTTP, SNMP, DPWS, and other well-known application protocols and data types may be utilised.
5. In a network with shaky connections, transport protocols may provide some level of dependability.
6. The availability of all standards and associated materials thanks to IP technology encourages creativity.
7. There are currently a lot of protocols available for administering and commissioning IP-based networks.

The protocol architecture for 6LoWPAN is shown in, where a LoWPAN layer an adaptation layer is inserted between the MAC layer and the IPv6 network layer. The following tasks are carried out by the adaption layer:

Fragment the IPv6 payload, compress the IPv6 header, and compress the UDP header.The 6LoWPAN standard has the details. 6LoWPAN employs the UDP (user datagram protocol) and ICMP (Internet control message protocol). Routers at the edge of 6LoWPAN, also known as edge routers, adapt IPv6 and IEEE 802.15.4.The location of edge routers during the fusion of WSN and the Interne. An edge router, a number of LoWPAN routers (R), and a number of LoWPAN hosts make up each LoWPAN (H). A remote server is also available through the Internet. By effectively reducing headers and streamlining IPv6 needs, 6LoWPAN makes IPv6 available for simple embedded devices over low-power wireless networks. There are a number of things to take into account while connecting a LoWPAN to the Internet or another IP network. Figure 10 discloses the server network of the system

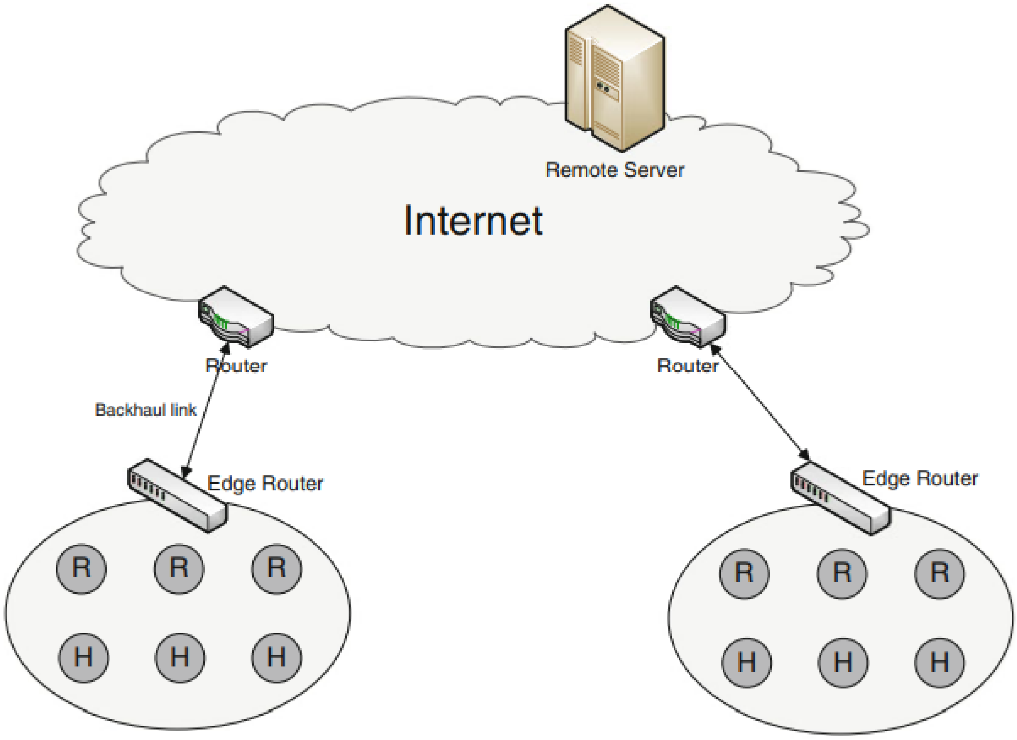


Figure 10: Discloses the server network of the system

High efficiency, high bandwidth needs, data processing, and compression methods are some of the difficulties faced by the multimedia WSN. Additionally, high bandwidth is needed for the correct and efficient delivery of multimedia materials. One of the prospective application areas for the newly established wireless sensor networking technology is Wireless Underground Sensor Networks (WUSNs). WUSN is a specific subset of WSN that focuses on the usage of sensors in the soil's subsurface area [14]–[17]. Although lacking wireless communication capacity, this area has long been utilised to bury sensors, mostly aimed at hydrology and ecological monitoring applications. WUSNs promise to close this gap and provide the framework for cutting-edge applications. The communication method is the fundamental distinction between WUSNs and terrestrial WSNs. In reality, a thorough evaluation of the subterranean wireless channel wasn't accessible until recently because of how differently electromagnetic (EM) waves propagate in soil compared to in air.

Architecture for Wireless Sensor Nodes in General

The development of the sensor nodes, which must satisfy the demands imposed by the particular applications, is the first step in the establishment of any WSN. WSNs employ a lot of sensor nodes, thus they need to be tiny, inexpensive, energy-efficient, and equipped with enough storage, processing power, and communication capabilities. Because of the size restriction, the sensor nodes are unable to be powered by long-lasting, high-capacity batteries or the main power supply. The sensor nodes should employ low power CPUs and compact radio transceivers with a constrained bandwidth and transmission range due to the requirements for low cost and energy efficiency.

As a result, the requisite calculation and transmission capabilities place limitations on sensor node design. The sensor nodes typically have four main subsystems: sensing, computing, communication, and power supply. The sensing subsystem typically consists of one or more sensors and actuators to monitor the physical environment. The computing subsystem typically consists of a microcontroller or microprocessor with memories to store and process the data collected by the sensing subsystem. If energy-harvesting methods are used, the power supply subsystem may also comprise a generator shows a typical wireless sensor node topology. There are two sections to the sensor subsystem. The first is a simple sensor that consists of sensor components that gather data from the environment surrounding the node and convert it into an analogue signal known as an

This analogue signal is subsequently transformed into a digital value using an ADC. The second component is an intelligent sensing system that may provide further features like data pre-processing and measurement error correction. The sensor system has to provide an interface that works with the microcontroller's calculation job. All computer tasks, including processing sensor data, performing data fusion, maintaining system battery life, configuring sensor settings, and executing high-layer protocols, such the ZigBee standard, are carried out by the computing subsystem. Here, the CPU is mostly to blame for power usage. One way to reduce power usage is to operate at a lower operating voltage. Another technique to make sure the microprocessors always operate in a power-saving mode is to split the subsystem's work time into several modes and transition between them.

It is the job of the communication subsystem to send and receive data frames. It is commonly known that transmitters use the majority of the energy used for wireless communication, and that the transmitting power determines how far a signal may travel. To make better use of the energy, the majority of radio frequency (RF) modules provide a way for a programme to dynamically alter the transmitting power. The direct current to direct current (dc-dc) converter with an auxiliary control circuit and a battery make up the power supply subsystem. The dc-dc converter offers multiple voltages to support all of the system's components and allows them to operate in various modes to cut down on power usage.

Component-based and System-on-Chip Design

With regard to the RF modules that are currently on the market, there are two approaches to create wireless sensor nodes. The other is based on a component-based design, whereas the first is based on a System-on-Chip (SoC) solution. Numerous RF module suppliers, including Chipcon, Microchip, Freescale, and others, provide SoC RF modules, which combine an RF module with a microprocessor, flash memory, RAM, ADC, and other specialised electrical circuits on a single chip. The sensor node design in thanks to these SoC RF modules. Hardware Design for WSNs There are only a few more components that need to be added, making the hardware design of wireless sensor nodes rapid, simple, and dependable. Lack of flexibility is a flaw with SoC systems, which makes it difficult to satisfy certain unique needs. The component-based design gives designers a wide range of freedom since they may choose all the necessary components, such as RF modules, microprocessors, and other electrical components, and create various layouts for the sensor node depending on the components selected. As a result, it may provide better performance at cheaper cost. It could, however, be difficult and time-consuming. Since it may greatly reduce the time it takes to bring the design to market, this chapter concentrates on the ZigBee compatible SoC design. Figure 11 discloses the power management system.

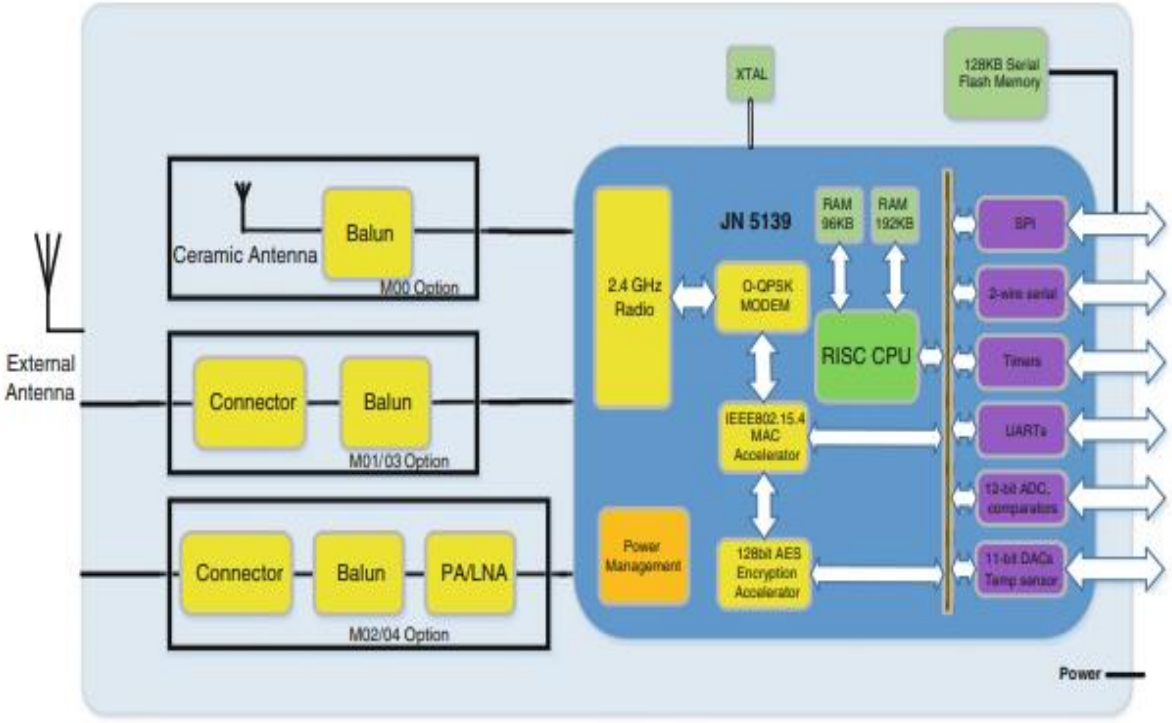


Figure 11: Discloses the power management system.

This chapter's design case study uses the Jennic JN5139 microchip as an example of one of these chips. The JN5139 modules include all necessary 2.4 GHz RF components as is common for SoC solutions. A JN5139 microcontroller, 1Mbit of serial flash memory, and peripheral circuitry make up this device. The application code that is put into the microcontroller during the boot process is stored in the 1Mbit serial flash memory.

The pricey RF design and testing are no longer necessary thanks to this Jennic module. By simply powering the Jennic module and attaching switches, actuators, and sensors to the module's IO pins, sensor nodes may be created displays a block schematic of the Jennic module.The module has a memory system, a 32-bit RISC (Reduced Instruction Set Computer) CPU, a wealth of analogue and digital peripherals, and an integrated 2.4 GHz transceiver that complies with IEEE 802.15.4 standards.

Cellular WSNS

These networks are made up of a number of mobile sensor nodes that may interact with their physical surroundings. Mobile nodes are capable of computation, sensing, and communication. Compared to static sensor networks, mobile wireless networked sensors are far more adaptable. Better and enhanced coverage, more energy economy, greater channel capacity, and other benefits distinguish MWSN from static wireless sensor networks.

CHAPTER 4

ROUTING IN WIRELESS SENSOR NETWORK

Hari Krishna Moorthy, Associate Professor,
Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN
(Deemed-to-be University), Karnataka – 562112
Email Id- harikrishna.moorthy@jainuniversity.ac.in

A mechanism called the routing protocol is used to choose an appropriate route for data to go from source to destination. When choosing the route, which relies on the network type, channel characteristics, and performance indicators, the procedure runs into a number of problems. In a wireless sensor network (WSN), the data gathered by the sensor nodes is normally sent to the base station that links the sensor network to other networks (perhaps the internet), where it is evaluated and appropriate action is taken.

Single-hop communication occurs in very small sensor networks where the base station and motes (sensor nodes) are in close proximity to one another. However, in the majority of WSN applications, where the coverage area is much larger and millions and millions of nodes must be deposited, multi-hop communication is necessary because the majority of the sensor nodes are located too far from the sink node (gateway) to be willing to speak also with core network directly. Direct communication is another name for single-hop communication, whereas indirect communication is another name for multi-hop communication [17]–[19].

In multi-hop communication, the sensor nodes act as a conduit for other sensor nodes to get to the base station in addition to producing and delivering their own content. Forwarding is the process of selecting an appropriate route from a source node to a destination node, and it is the network layer's main job. Because WSNs vary from wireless transport systems networks in a number of ways, designing routing protocols for them is a difficult issue. There are several kinds of routing difficulties in wireless sensor networks. The following are a few significant difficulties:

Allocating a universal IDs system for a large number of sensor nodes is virtually impossible. Therefore, wireless sensor motes are incapable of using traditional IP-based protocols. It is necessary for detected data to flow out of a number of different sources to a particular base station. However, conventional communication networks do not experience this. Most of the time, the produced data traffic contains a lot of redundancy because several sensing nodes might provide identical data at the same time. Therefore, it is crucial to take advantage of this redundancy using the network parameters and to make the most use of the bandwidth and energy that are available.

Furthermore, wireless motes are severely constrained in terms of transmission power, bandwidth, storage capacity, and on-board power. A variety of novel routing techniques have been proposed as a result of these differences in order to address the routing issues in the wireless sensor networks.

- **Lifetime:** In a lot of applications, sensor nodes are positioned in places that are difficult, if not impossible, for people to reach. As a result, it is not practical to constantly replace the batteries used by WSNs, and the sensor node's limited initial energy supply plays a significant role in determining how long it will last. To optimise the overall network lifespan, each node's local power consumption must be managed in the hardware design of WSNs. Each circuit should be designed to use the least amount of electricity possible. The lifespan of WSNs may also be extended by any energy-scavenging device installed on the sensor node.
- **Coverage:** According to the application criteria, WSNs must provide coverage of the region of interest. The needed coverage should be taken into account while deciding on the transmission power and the placement of sensor nodes.
- The sensor nodes will need more power to gather and transmit data as the coverage increases, which will reduce the lifespan of the WSNs due to a finite power source.
- **Robustness:** The wireless sensor nodes may need to operate under challenging or unpredictable conditions. The WSNs must be built in such a way that it can withstand individual node failures and adjust to them while still functioning as a whole.
- Communication: Sensor nodes should have low data rates and power requirements for communication.
- **Time Synchronization:** Sensor nodes should be able to wake up regularly or on demand and should be maintained in sleep mode after their duties are finished in order to save energy.
- **Security:** Some WSN applications, such as numerous military purposes, need data secrecy and a security method must be provided by the WSNs. Precise time synchronisation will allow various sensor nodes to cooperate with other network members.Hardware Design for WSNs Each sensor node's CPU must be able to execute sophisticated encryption and authentication methods.
- **Price and Size:** Depending on the application, the deployment of WSNs may call for thousands of sensor nodes. To keep such deployments feasible, individual sensor nodes should be as small and inexpensive as possible.

Based on the aforementioned factors, the design of a wireless sensor node may be broken down into the following steps: choosing a microcontroller, choosing an RF communication device, designing sensing devices, and designing power supply devices.

Choosing a microcontroller

The microcontroller, which serves as the brain of the sensor node, is in charge of collecting, analysing, compressing, recording, and storing data. On a single chip, a SoC microcontroller typically includes a CPU, flash storage, RAM, as well as analogue and digital peripherals. It is thought that using a SoC microcontroller in the sensor node architecture decreases the expenses associated with design and testing and is the best option for WSNs. When selecting the proper sort of microcontrollers, there are a few practical considerations that should be kept in mind.

- **Performance:** The power dissipation characteristics of the sensor node may be considerably influenced by the microcontroller's performance level. This is due to the fact that a microcontroller with greater performance consumes more power. The performance of an optimal microcontroller for the WSN system should satisfy the desired performance level of the application rather than selecting the best one since the degree of microcontroller performance needed for various applications differs.
- **Operating Mode:** Microcontrollers often have a variety of operating modes, such as Active, Idle, and Sleep modes, with each mode being defined by a distinct level of power consumption. This helps microcontrollers save energy. The sensor nodes' overall power consumption may be calculated by taking into account the transition periods for entering and leaving the sleep state. A microcontroller may utilise the sleep state more often and use less energy overall if it can enter and exit the sleep mode quickly. Thus, the overall energy consumption of the sensor node is significantly influenced by the power consumption levels of various modes, the transition time, the transition power, and the length of time the microcontroller spends in each mode.
- **Voltage Requirements:** The microcontroller's operating voltage range may significantly affect the system performance and sensor choice.
- It is decided to use a conventional low voltage microcontroller with an operating voltage range of 2.7 to 3.3 V.
- **CPU Speed:** Since the microcontroller's power consumption grows linearly with frequency, the amount of data analysis and in-network processing that must be carried out on a sensor node will decide the best CPU speed.
- **Support for the periphery:** The microcontroller should feature general-purpose digital I/O pins, Analogueto-Digital Converters (ADC), Comparators, and certain digital communication interfaces like RS-232, UART, I2C, or SPI since it is especially designed to connect with external devices.
- **Recall:** The microcontroller should have adequate memory to house the application programme, depending on the size of the WSNs' application programmes. Programs are often stored in flash memory, which the microcontroller may write to in boot mode.
- **Software Provided:** The choice of microcontroller might also be influenced by the software base that is available. For instance, many scientists and engineers like using C or C++ when writing their programmes. Consequently, a microcontroller that supports various settings for writing software may be thought of as being perfect for them.

Cost and Dimensions another factor to take into account when choosing a microcontroller is its low cost and small size. Typically, a chip with an integrated MCU and radio is selected because to its affordability, compact design, and simplicity of development.

Choosing a Communication Device

To share information between sensor nodes, a communication tool is utilised. A communication device typically consists of a low power radio system, which contains a digital baseband, a power amplifier, and an RF transceiver (antenna). Since the radio system often consumes the most power in WSNs, reducing its power consumption may significantly extend the lifespan of the whole system. The decision on which radio system to choose is influenced by a number of things.

- **Wi-Fi Technologies:** For business purposes, a number of wireless technologies, including Wi-Fi, Bluetooth, and ZigBee, are available. Table 3.2 provides a quick comparison of these three methods. Typically, ZigBee-based technology is used for WSNs in order to enable straightforward wireless communications with short-range distances, restricted power, low data throughput, cheap cost, and compact size.
- **Transmission Range:** The radio transmission range establishes the shortest possible distance between any two sensor nodes, and therefore, the WSNs' coverage.

The range is influenced by a number of variables, including the transmission power, the transceiver's range, the receiver's sensitivity, the antenna's gain and efficiency, and the channel encoding algorithm. Energy may be saved at sensor nodes considerably by optimising the transmission power. SNR (signal-to-noise ratio) and BER will both increase with increased transmission power (bit-error rate). Additionally, a signal should go farther the more energy it receives, expanding coverage and decreasing interference from other wireless systems.

Modulation Type: One of the purposes of RF communication devices is to transform a digital signal into an analogue signal for transmission. Modulation is the term for this action. Amplitude modulation, such as amplitude-shift keying (ASK), frequency modulation, such as frequency-shift keying (FSK), and phase modulation, such as phase-shift keying, are examples of common modulation processes (PSK). ASK employs amplitude changes to symbolise 0 and 1. To represent 0 and 1 in FSK, frequency changes are used. The binary data in PSK is represented by the signal's phase. For WSNs, quadrature phaseshift keying (QPSK) modulation is often used, in which each signal is phase-shifted by 90-degree increments.

- **Bit Rate:** WSNs do not need large bit rates for communication, in contrast to many other high performance data networks. Raw network bandwidth of 10–200 kbps is often enough for the majority of applications.
- **Turn-on Time:** For a radio to operate well in WSNs, it must be able to enter and leave low power sleep states fast. It rapidly becomes difficult to accomplish the requisite duty cycle of less than 1% if a radio's turn-on-to-receive time is more than a few tens of milliseconds. The duty cycle is defined as the percentage of time that a system is in an active state.

Design of Sensing Devices

A sensor is a device that measures an electrical signal that can be read by other electronic devices from a physical amount it is measuring. It acts as a bridge between the physical world and technological apparatus. Sensors may be categorised in a variety of different ways. From the perspective of the power supply, all the

Design Recommendations There are two types of sensors: passive and active, totaling. A passive sensor responds to an external stimulus, such as a photodiode, by producing an electrical signal without the need for an extra power source. An active sensor, like a temperature-sensitive resistor, needs external electricity to function. Sensors may be divided into digital sensor and analogue sensor based on the kind of sensor output singles. Binary values are output via digital sensors to the microcontroller. Analog sensors respond to an external variable by producing an analogue signal, often a voltage. The sensors may be divided into thermal sensors, mechanical sensors, chemical sensors, magnetic sensors, radiant sensors, and electrical sensors based on their measuring characteristics, which is the third categorization of sensors. The sensing concepts employed in WSNs are summarized.

The ideal sensor would have high sensitivity, precision, and repeatability as well as low power dissipation, cheap cost, and ease of use. These sensors may be positioned within or next to the phenomena to be studied. Sadly, we often cannot combine all of these characteristics into a single sensor and must make a decision.

One of the most used industrial thermometers is the thermocouple device, which Thomas Seebeck discovered in 1822. It is made up of two different metals that are fused together to create a tiny, distinct voltage at a certain temperature. Thermocouples are often regarded as the smallest, quickest, and most reliable temperature measuring technology (Swanson 2010). It may be utilised in difficult climatic circumstances and a very broad temperature range. However, there are three drawbacks to thermocouples. First, two temperatures must be measured in order to measure temperature using a thermocouple. Second, there is a nonlinear correlation between process temperature and thermocouple output voltage. Thirdly, the poor precision necessitates the use of a particular compensatory approach.

A resistor in an RTD sensor changes value in response to temperature changes and is a positive temperature coefficient sensor. It has earned a reputation for having good linearity, high repeatability, minimal drift, and excellent precision. RTD sensors are not suitable for high temperature applications, and they are also less sensitive to slight temperature fluctuations. When very steady and accurate readings are the most crucial criterion, an RTD is the sensor of choice.

Another form of resistor whose resistance changes depending on temperature is the thermistor sensor. However, thermistors and RTDs vary in that thermistors often employ ceramic or polymers as their material of construction whereas RTDs only use pure metals. The most typical thermistors have a negative coefficient of resistance for temperature. Moderate temperature range, cheap cost, and subpar but predictable linearity are all characteristics. Thermistors are perfect for measuring tasks that call for very precise sensitivity across a constrained range of temperatures.

IC temperature sensors are entire silicon-based sensing circuits with either analogue or digital outputs. They are manufactured in the form of ICs. Applications where the temperature falls between -55 and 150 C are the only ones where IC temperature sensors may be used. But when compared to other kinds of temperature sensors, they offer a number of benefits. First off, IC temperature sensors are regarded as being a class of tiny, precise, and reasonably priced temperature sensors with outstanding linearity. Second, they have simple interfaces for connecting to other devices like microcontrollers and amplifiers.

The Maxim IC temperature sensor DS18B20 was used as the temperature sensor in this design due to the benefits of IC temperature sensors. The DS18B20 digital thermometer offers measures from 9 to 12 bits in Celsius and has an alert function with non-volatile user-programmable higher and lower trigger points. One data line is necessary for the DS18B20 to communicate with a central microcontroller. The attributes are shown below: 2008 Dallas Semiconductor

1. Measures temperatures from -55 to 125C;
2. Accuracy: 5C from -10 to 85C;
3. Power supply range: 3.0-5.5 V;

60 3 WSN Hardware Design

Thermometer resolution may be set to 9 or 12 bits by the user, and it converts temperature to a 12-bit digital word in 750 milliseconds. It is also available in 8-pin SO, 8-pin SOP, and 3-pin TO-92 packages.

The design opts for the 3-Pin TO-92 packaging, and Table 3.6 lists the DS18B20's pin descriptions. An external power source is connected to the VDD pin to power the DS18B20 chip. The microprocessor's DIO pin is joined to the DQ pin.

Design of CO Sensors 3.4.2

As part of the detection of dangerous and combustible gases in the air, gas sensors are often utilised. They engage with different gases and provide an electrical output as a result. When choosing gas sensors, the following process should be taken into consideration:

1. Identify the target gas and any background gases that could be present in the monitoring region. Failure of the gas sensor might result from the presence of background gases.
2. Establish the target gas's concentration. The concentrations of the gases to be detected should typically be 3-5 times higher than the concentrations actually used for monitoring.
3. Establish the operating temperature range where the gas sensor will be mounted.
4. Establish the allowed power consumption since numerous gas sensors need a lot of electricity.
5. As many gas sensors have a lengthy reaction time, ascertain the necessary response time for gas sensing.
6. Choose a size and price that are reasonable.

DS18B20 (TO-92) (TO-92) Function Name

1 GND Ground

Data Input/Output 2 DQ.

3 VDD VDD is optional. For functioning in parasite power mode, VDD must be grounded.

DS18B20 application schematic (Dallas Semiconductor, 2008)

Design Case 3.4 No. 61

Electrochemical, semiconductor, catalytic, and infrared gas sensors can all be categorised. Typically, two or three electrodes are in contact with an electrolyte in electrochemical gas sensors. By oxidising or reducing the target gas at an electrode, they can determine its concentration. An electric current flows across an external circuit as a consequence of the electrochemical process. The desired gas concentration may be determined by measuring this electric current, which calls for an external amplifying circuit. Compact package size, resilience, the need for little to no external power, and cost effectiveness in large-scale manufacturing are all advantages of electrochemical sensors. Electrochemical sensors have a reaction time of around 30 s and a lifespan of often less than 3 years. Replacement sensors are expensive, particularly for large-scale deployments. Toxic gas detection is the major use for electrochemical sensors.

At a gas-detecting device, a semiconductor gas sensor is used. By monitoring changes in a semiconductor's electrical property, a specific gas may be identified. The increased demand for semiconductor gas sensors is a result of its many benefits, including their compact size, extended lifespan, rapid reaction times, and excellent sensitivity in detecting extremely low gas concentrations. However, they often need an additional 5 V power source to maintain the sensors' operational state.

A ceramic pellet and a filament made of platinum-iridium alloy make up the catalytic gas sensor. The target gas is burned by heated bare platinum wire coils in catalytic gas sensors, and the heat from the burning causes a change in the filament's resistance. Using a simple wheatstone bridge circuit, this change is measured. The sensor itself has a very straightforward design and is simple to produce. This approach has the benefit of measuring the gas directly. Battery-powered sensors cannot be used because the sensors need extra electricity to heat the bare coils. Combustible gas detection is the main application for catalytic gas sensors.

A "non-reactive" gas sensor is one that uses infrared technology. The target gas absorbs some of the infrared wavelengths of the light travelling through it, while other wavelengths pass through unabated. This is the foundation of the operating concept. The quantity of absorption that takes place when a volume of gas is illuminated by an infrared light source for an infrared gas sensor is linked to the concentration of the target gas. The main benefits of this technique are thought to be its long lifespan, lack of interaction with the target gas, excellent precision, and dependable concentration readings. However, utilising infrared gas sensors has limitations, including expensive cost and high power consumption.

The Figaro TGS5042 electrochemical CO sensor was selected as the sensor node design for the safety-monitoring example since it does not need electricity for the sensor itself. Below is a summary of the TGS5042 CO gas sensor's features: (2010) (Figaro)

- Battery-powered
- Linear connection between CO gas concentration and sensor output; high repeatability and selectivity to CO
- Target gases: carbon monoxide; typical detection range: 0-10,000 ppm; output current in CO: 1.2-2.4nA/ppm; operating temperature range: -40 to +70 C; response time: less than 60 s

The TGS5042's fundamental measuring circuit is seen in combination of an op-amp and resistor converts the sensor's little electric current into the sensor output voltage. The Jennic 5139 module receives the output through an ADC pin.

Design of Sensor Node Circuits

A microcontroller and a CO sensor may be combined into a single circuit using the temperature sensor shown in and the CO sensor shown in. The schematic design of a sensor node containing a temperature and a CO sensor is. The circuit for both the CO sensor and the temperature sensor is illustrated on the top right, and the Jennic 5139 module, which serves as both the microcontroller and the communication device, is shown on the left. A circuit that serves as a power source for two AAA batteries can be found at the bottom right. This schematic model may be transformed into a printed circuit board (PCB) design, allowing for the production of a wireless sensor node with temperature and CO sensors.

Power Administration

When a sensor node is powered by batteries, power management is one technique to extend its lifespan. By shutting off the electricity whenever feasible or changing the sensor system, it seeks to reduce energy waste and increase energy efficiency. Schematic for a temperature and CO gas sensor hardware planning for the low-power condition of WSNs. A sensor node's energy consumption may be divided into "useful" and "wasteful" sources. The usable energy consumption may be employed for environmental sensing, data processing, data transmission or reception, query processing, and forwarded queries and data to nearby nodes. Data transfer, processing, and acquisition are three areas where WSNs might waste energy. As a result, power management should address how much energy is used for these three tasks. Please take note that this section solely discusses chip level power management during the data collecting stage as it relates to hardware design. The subsequent chapters of the book will cover power management at both the data processing and data transmission phases.

The voltage of the power supply, the current consumption of the different components, and their operating duration all work together to determine how much power each component uses. Once the electrical components are chosen, the first two elements are fixed. Working time and idle time are the two components' running times, respectively. Equivalent amounts of energy are used by components in both their working and idle states. Only after receiving an acquisition instruction from the microcontroller does the node turn on the sensor power during the data collection stage, and it is shut off when the sensor reaches the idle state.

The DS18B20 temperature sensor, for instance, has a sleep mode that consumes 0.003 mW of power and is intended to work with the CO and temperature sensors shown. The temperature sensor is kept in standby mode until it is needed for a sensing duty by the sensor driver, which will be explained in the next chapter. The TGS5042 CO gas sensor is the component of the sensor node that consumes the most power, using 4 mA while it is operational. By turning the device off, you may prevent the use of power by idle sensors. A controlled switch on the sensor power supply line is necessary for this unconventional arrangement. As a result, the CO gas sensor circuit uses a P-channel switch J177, as illustrated, to turn the CO gas sensor off while it is in idle mode. When the CO gas sensor circuit is in an idle state, a control signal from the microcontroller shuts it off, and as a result, the current consumption in this condition is zero. The CO Power control of sensor nodes energy consumption. Power Administration Without a P-channel switch, the 65 gas sensor operates at 2,640,000 lc each cycle; this may be lowered to 240,000 lc.

<u>Use of less energy</u>

Most wireless sensor networks run on batteries. In these sensor networks, energy constraint is a significant problem, particularly in hostile conditions like a battlefield. When battery levels drop below a certain battery threshold level, sensor node performance suffers. When creating sensor networks, energy is a major problem for designers. There are countless numbers of motes in wireless sensor networks. Due to the network's intermittent power supply, each node has limited energy resources. Because of this, the routing protocol has to be energy-efficient.

Complexity:

The performance of the whole wireless network may be impacted by the architecture of a routing system. The cause of this is that we have little hardware expertise and that wireless sensor networks have severe energy limits [20], [21].

Scalability:

Since sensors seem to become cheaper every day, it is simple to deploy tens or even hundreds of sensors in a wireless sensor network. Therefore, network scalability must be supported by the routing protocol. The routing protocol shouldn't be interrupted if more nodes are ever added to the network.

Delay:

Some applications, like temperature sensors or alarm monitoring, need an immediate response or one without a significant delay. Therefore, the routing protocol need to have a low latency. In the aforementioned WSN applications, it is necessary to communicate the detected data in the shortest amount of time feasible.

Energy Scavenging Energy scavenging, also called energy harvesting, is another way to prolong the lifetime of a sensor node. Most people do not realize that there are abundant energies constantly around us such as solar, thermal, wind, and radio frequency energies. If these energies could be scavenged and transferred into electrical energy they can then be used to power the wireless devices, then the previously crucial battery limitations of WSNs could be removed. Depending on the different sensors and different environments these sensors are deployed in, various energy scavenging methods have been utilized including:

1. Light energy: sunlight or man-made light, which can be captured via solar panels, photo sensors;
2. Thermal gradient energy: waste thermal energy from heaters, furnaces and engines.

Radio Frequency energy: from satellites, TV base stations, mobile phones transmission stations, and other wireless electronics,

1. **Mechanical energy:** vibration, mechanical stress, strain and wind; CO gas sensor with a P-channel switch 66 3 Hardware Design for WSNs
2. **Human body:** a combination energy generated from bio-organisms or through body movements;
3. **Other energy:** chemical and biological sources. Power densities of commonly used power scavenging sources are compared.

The most accessible energy source is solar energy, which can be harvested through Photovoltaic (PV) conversion and has the higher power density of those compared. Therefore, a solar energy harvesting system is chosen as an example in this section to illustrate how localized energy harvesting systems can be designed to supplement battery supplies to prolong the lifetime of wireless sensor networks. Solar is the most powerful source of nature light, and an inexhaustible source of energy. Photovoltaic (PV) technology is used to convert solar energy directly into electricity. In practice, a solar cell is commonly used to harvest solar power.

Depicts the functional architecture of a solar energy harvesting system, which comprises three subsystems: an energy harvesting unit, a maximum power point tracking (MPPT) unit, and a power management unit.Solar Energy Harvesting Unit A solar cell is commonly used to harvest light intensities. Numerous types of commercial solar cells are available. The trade-off between price, dimensions and the efficiency of solar cells needs to be considered and two Centennial Solar MC-zSP0.8-NF-GCS, connected in parallel, were chosen as the main solar panel in the energy harvesting unit as a single solar cell would not be not sufficient to power the whole sensor node. Power densities of energy harvesting resources Energy source Power density (uW/cm3) 1 year lifetime Solar (outdoors) 15,000-direct sun 150-cloudy day Solar (indoors) 6-office desk Vibrations 200 Acoustic noise variation 10 Temperature gradient 15 @ 10 K gradient Shoe inserts 330 3.6 Energy Scavenging 67 3.6.2 Maximum Power Point Tracking Unit The main function of the MPPT unit is to deliver the maximum power from the solar panel to the energy reservoir.

The MPPT unit consists of a Pulse Width Modulation (PWM) DC/DC converter and the MPPT peripheral circuit. Because solar energy varies over time with the change of light intensity, an energy harvesting interface circuit with high power transfer efficiency is required to convert the scavenged power into a smooth value before storage in an energy reservoir. The type of DC/DC converter used, is determined by both the strength of the power harvested and the operating voltage of the energy reservoir. LTC3401 DC/DC converter is chosen here as its conversion efficiency is over 85 % in the 10–50 mA output current range while its output voltage is set to 4.1 V. There are two advantages in using the PWM DC/DC converter rather than charging the energy reservoir by directly connecting a diode with the solar panel. Firstly, this PWM DC/DC converter enables energy harvesting to continue even when the open circuit voltage of the solar panel is lower than the voltage of the energy reservoir. Secondly, using a diode to block the reverse current flow from the reservoir to the solar panel causes a 0.7 V drop in the output voltage, but the PWM DC/DC converter can avoid this voltage drop. The MPPT peripheral circuit consists of a miniaturized PV module and a comparator.

There exists a linear relationship between the open-circuit voltage of the miniaturized PV module and the maximum power point of the main solar panel when both of them are exposed to the same light radiation. Therefore the comparator with an input from the main solar panel and a feedback from the miniaturized PV module can be used to perform MPPT in terms of the above linear relationship. In the design here, we have chosen a Hamamatsu S1087 (Hamamatsu 2002) as the miniaturized PV module and use it as a radiance sensor. There is no need of any additional power supply for this radiance sensor.

Power Management Unit

A power management unit is used to store the scavenged energy and ensure its effective use. The power management unit consists of a primary buffer, a secondary buffer and a control charger circuit. There are two reasons for the use of multiple buffers in the power management subsystem here. As the light intensity in the environment changes, the generating voltage would vary over time, and consequently it is hard for the energy-harvesting unit to power the target system directly. Therefore, a high-density energy storage element such as a rechargeable battery must be employed to accumulate the available energy delivered by the energy-harvesting unit. On the other hand, the rechargeable battery has limited recharge cycles and lifetime, which limits the lifespan of the whole system. In order to prolong the system’s lifespan for as long as possible, the 68 3 Hardware Design for WSNs access to the rechargeable battery must be minimized and consequently, the target system should be directly powered by the energy-harvesting unit most of the time. Therefore another energy buffer is required. The two-buffer design here is in the same spirit as the design by Prometheus.

A primary buffer, a super-capacitor, which is directly charged by the harvesting panel, powers the target system when enough power is available. Otherwise, the target system draws current from the secondary buffer, a rechargeable battery. Furthermore, if a sufficient light source is available, the primary buffer charges the secondary buffer and powers the target system simultaneously. The primary buffer is directly charged by the energy-harvesting unit and its main purpose is to minimize access to the secondary buffer in order to prolong solar energy harvesting system Energy Scavenging 69 lifetime of the energy harvesting system. The primary buffer must have the capability to handle high levels of energy throughput and frequent charge cycles but does not need to hold energy for a long time. Basically, super-capacitors have a much longer lifetime, higher efficiency, higher power density, fast and simpler charging circuit than rechargeable batteries. This means that super-capacitors fit all the requirements for the primary buffer.

Therefore, two 22F super-capacitors have been chosen as the primary buffer in this design. The secondary buffer is used only when the energy in the primary buffer is exhausted, and needs to hold energy for a long period of time, i.e. have low current leakage. Rechargeable batteries have higher energy density, lower breakdown voltage, and lower leakage current. For these reasons, rechargeable batteries are the ideal option for the secondary buffer. A control charge circuit is needed to optimize the use of the harvested power for the sensor node. We adopted the Ambimax design for the control charge circuit. By comparing the terminal voltage of the super-capacitors with a pre-defined threshold voltage, the control charge circuit determines which power source, either the primary buffer or the secondary buffer, should power the target system at any moment. When the rechargeable batteries are not fully charged and the voltage of the sup-capacitor is higher than a second pre-defined threshold voltage and the rechargeable batteries are replenished by the supercapacitor.

Furthermore, overcharging and undercharging of the rechargeable battery is protected by software installed in the ZigBee chip. 3.6.4 Design Case a complete circuit for a solar energy- harvesting system. In the schematic diagram, a solar panel with the DC–DC converter circuit is shown at the bottom left side to harvest solar energy from environment. The MPPT circuit, shown at the top left side, is employed to keep the solar cell working. A complete solar energy harvesting circuit 70 3 Hardware Design for WSNs maximum power point. The right hand side is the power management circuit, which is used to maximize the lifetime of the system. It consists of a LTC1441 dual comparator, a charge control chip Max890L, two 22F super capacitors, and two rechargeable batteries. A ZigBee temperature and CO sensor node is connected with the solar energy harvesting system and the whole system was tested in an outdoor environment for one week. The sensor node worked autonomously as expected without any additional power requirement. During the daytime, the node was powered most of the time by the super-capacitor and the super-capacitor charged the battery when they had sufficient power. During the night, the node switched to use the batteries. The list of components and parameters is given in.

List of components and their parameters Designator Description .Conclusion Hardware design is one of the most crucial steps in the design of WSNs, where energy consumption is the most critical concern. This chapter groups the basic structure of sensor nodes into a sensing part, a microcontroller part, a RF transceiver part, and a power supply part. Many wireless electronics manufacturers provide microcontroller, RF transceiver, and their peripheral circuits on an integrated circuit board, discussed above as the SoC solution. Sensor node designs based on the SoC solution are quicker, easier, and more reliable than the components based design. Various considerations on microcontroller selection, communication device selection, sensor device design, and power supply device design, have been summarized in this chapter and the use of them have been illustrated by a temperature and CO sensor node design. Power management and energy scavenging are two ways to overcome the constraints caused by the energy consumption and prolong the lifetime of WSNs. Switching the power supply when the sensor node is not in an active mode can help in the reduction of the energy consumption. A complete solar energy harvesting system has been designed in this chapter, showing the promising future of using this type of technologies in the design of WSNs.

The most crucial and challenging step in developing a wireless sensor network is embedded software design. In this context, the word "embedded" really means "built-in." There are embedded systems everywhere. Mobile phones, microwaves, digital cameras, etc. are common examples. Computer software that is integrated into a device's circuits is referred to as embedded software.

A typical application-specific microprocessor used in embedded software has a modest compute capacity, is inexpensive, has a small amount of memory, and uses little power. Real-time operating systems (RTOS) are often used to run embedded software, and communication protocols developed specifically for embedded systems are offered as closed source by chip manufacturers. After its design is finished, embedded software must be uploaded to, tested on, and operated on the proper microprocessor before being incorporated in the electronics. Ideally, embedded software should be developed after the release of the relevant hardware.

The creation of multiple embedded software simulation environments has allowed for the concurrent or even prior design of embedded software. Using an environment like COOJA, a WSN simulator running the Contiki operating system (OS), embedded software development may be carried out concurrently with or even before hardware development. An embedded system for a certain application is made up of embedded software and the accompanying hardware. Before they are merged, software design and hardware design are carried out in parallel, starting with a list of system requirements before moving on to system architecture design and CPU selection

Design of Embedded Software for WSNs

Because embedded systems employ different microcontrollers and communication protocols, the architecture of embedded software differs from one system to the next. A WSN protocol stack, which also serves as the WSN software architecture, was shown. The hardware layer, the MAC (medium access control) layer, the network layer, and the application layer are listed in order from bottom to top. The baseband hardware is placed above the 802.15.4 stack, which is itself positioned above an application. There are specified entry points for the 802.15.4 stack that may be used to initiate and register callbacks for the application as well as request 802.15.4 actions. The Board API, Integrated Peripherals API, and Application Queue API are conceptually separate from and independent of the 802.15.4 stack. Application programming interfaces (APIs) may be used to accomplish activities including scheduling, operating the system, and accessing sensors (API). To put it another way, a user's application is made up of a number of calls based on these APIs. The communication services are offered by contacting the IEEE 802.15.4 stack API; the integrated peripherals API is used to provide sensor access and local PC connectivity; and the system requirements API is used to initiate hardware interruption.

Ten preconfigured operations, including user activities and BOS/Stack tasks, are available. The latter are actions that fall within the Basic Operating System (BOS) and don't need human input. Implementing these 10 preset functions is the responsibility of embedded software development.

The software launches when a sensor node is turned on by calling the method "AppColdStart," which initialises the system. This method may initialise any user variables or system extras like timers or UART ports.

To further allow sensor nodes to join the appropriate WSN, key ZigBee system settings including the radio channel and network identifier are defined here. Finally, the sensor node is forced to handle the hardware events while the BOS is setup and launched. The user application may register any new tasks with the BOS by invoking the method "JZA vAppDefineTasks" once the BOS has completed certain internal tasks to initialise the system. The registered ZigBee device may operate as a ZigBee Coordinator, Router, or End device via a call to the ZigBee stack by performing another initialization method called "JZA boAppStart."

Software architecture

Design of Embedded Software for WSNs

Following the activation of the BOS and ZigBee stack, the BOS transfers control to the user application using the following features:

1. JZA vAppEventHander: The user application function is called periodically by the BOS. Any user application code that has to be executed often should go here.
2. JZA vStackEvent: This function is used to manage a variety of events from the stack's lower tiers.
3. JZA vPeripheralEvent: This function is invoked whenever a system peripheral, such as a timer or a DIO line, generates an interrupt. While the CPU is operating in an interruption mode, it is termed. JZA vAppEventHandler will eventually retrieve the information about the interrupt from a simple FIFO queue that has been created ().
4. JZA bAfKvpObject: This function is only invoked when another node has sent a Key Value Pair (KVP) command packet over the radio. This function should have included the application code to process the incoming command and, if required, provide a response.
5. JZA bAfMsgObject: This method is only invoked after a radio-received MSG frame from another node. This function should be expanded to include the application code in order to process the incoming message.

Generic ZigBee embedded software framework,

1. 76 4 Designing Embedded Software for WSNs
2. JZA vAfKvpResponse: This function is used when another node sends a KVP response frame. To receive and process the response frame, the application code has to be included in this function.
3. JZA vZdpResponse: This method is used when a ZigBee Device Profile object responds.

The design of the embedded code for a sensor node is finished when these functionalities are implemented. The embedded code should then be compiled and downloaded to the hardware.

Development of the LowPAN Application

Another embedded software environment for WSNs. Every Contiki application is referred to as a process, which is a piece of code that the Contiki operating system executes on a regular basis. When a module containing a process is loaded into the system or when the system boots, Contiki processes are normally launched. When an event, such as the start of a timer or some external event, occurs, a process begins to execute.

One of the two execution contexts available to embedded programmes in Contiki is cooperative or pre-emptive. The cooperative execution context allows for the sequential execution of code alongside other context-specific programmes. Before any other collaboratively scheduled code may execute, cooperative code must run completely. The cooperative code may be interrupted at any moment by pre-emptive code. When cooperative code is halted by pre-emptive code, cooperative code will not start again until pre-emptive code has finished running. Processes always operate in the cooperative scheduling context, which is one of Contiki's two scheduling contexts. Interrupt handlers in device drivers and real-time jobs with set deadlines both make use of the pre-emptive context.

A process control block plus a process thread make up a Contiki process. The process control block, which is kept in RAM, includes a reference to the process thread as well as other run-time details about the process, such as its name and status. It may be quite little in size and just need a few bytes of RAM. The code for the process is kept in ROM as the process thread.

The PROCESS macro is used to declare or define a process control block instead of explicitly doing so. This macro accepts two inputs: a textual name for the process, which is used for debugging and for publishing lists of running processes to users, and the variable name of the process control block, which is used to access the process. Below is a description of the process control block used in the Hello World example.

Robustness:

Wireless sensor networks are widely used in very important and risky areas. A sensor node may sometimes expire or leave the wireless sensor network. As a result, the routing protocol has to be able to handle various types of settings, even harsh and lossy ones. The routing protocol's functioning should also be satisfactory.

CHAPTER 5

TRANSPORT PROTOCOL IN WSN

Sunil. MP, Assistant Professor,
Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN
(Deemed-to-be University), Karnataka – 562112
Email Id- mp.sunil@jainuniversity.ac.in

As we recall from the concept of general network layers, the main responsibilities of the Transport Layer are to ensure the dependable transmission of packet header using end-to-end retransmissions or other techniques, and minimise or completely avoid network congestion caused by excessive traffic flowing through routers or other relay points. The Internet utilises TCP. TCP, however, is incompatible with WSN transport layer architecture. This chapter will outline the specifications for the WSN transport layer design and provide some useful protocol examples.

Driver Development for Sensors

A typical wireless sensor network is made up of sensors and wireless transmission modules from the perspective of the hardware parts. Embedded software is required to make these components operational, and its constituent parts are often referred to as "drivers." The "quiet" hardware might become "active" to carry out the assignments thanks to the particular drivers. Drivers for two wireless transmission modules are given by the makers of microcontrollers and are part of peripheral hardware drivers. Only the development of sensor drivers is covered in this section.

The real tools for gathering environmental data are the linked sensors. Numerous frequently used sensors may be contained into a compact device and managed by a particular micro control unit. Developers of embedded software do not need access to the physical layer of the sensors. The control units will be in charge of carrying out the sensors' intended capabilities and coordinating with the external control system.

The sensor driver development uses embedded software to allow the wireless sensor node to either receive user commands from the desired sensors or to collect sensor data from those sensors. Although the operating principles of individual sensors may vary greatly, there are two basic types of sensor interactions (i.e., output and input interfaces): digital interface and analogue interface. The binary signals "1" and "0" are expressed utilising a certain duration of high level and low level voltages to enable communication across the digital interface.

ADC in the internal microprocessor

Digital sensor parts Developers of embedded software for WSNs may transmit and receive data that is understandable by both the sensor control unit (sensor microprocessor) and the external control system (wireless chip). The CPU collaborates with an inbuilt ADC (analog-to-digital converter) to produce digital signals through a digital interface. For creating the digital interface (i.e., communication rules), there are numerous digital communication standards available, including the serial communication protocol, the SMBus protocol (System Management Bus, defined by Intel), the I2C protocol (Inter-Integrated Circuit), the Universal Asynchronous Receiver/Transmitter (UART), and the 1-Wire interface (defined by Maxim Incorporated).

Compared to a digital interface, an analogue communication interface is easier to use.

Normally, the voltage level that the analogue sensors produce corresponds to a change in the sensing phenomenon after being transformed into a digital signal by an ADC, it may be utilised by the external control system.

Some analogue sensor types deliver a sequence of pulses to an external controller that are associated with the strength of the sensing phenomenon (speech, light, temperature, etc.). The outside control system will sample the number of pulses for a certain amount of time, turn it into a useful value by using a predetermined formula, and then give it to the consumers.

General Sensor Driver Procedure

A sensor driver should provide the external controllers the capacity to receive sensor data and communicate user commands to the sensors. The phases of sensor startup, sensor parameter setup, sensor data gathering, and sensor power management generally make up a comprehensive sensor driver design (sleep, wait, and standby).

Below, we provide a more thorough explanation of these procedures:

The first procedure, called "Sensor Initialization," is in charge of setting up all the sensor's default settings. This entails turning on the sensor, configuring the communication link, and resetting the sensor to its factory settings. The parameter settings of several sensors are saved in a linked non-volatile memory, such as an Electrically Erasable Programmable Read-Only Memory (EEPROM), where the user setups or particular manufacturer calibrations may be kept secure and are simple to retrieve in the event of a failure.

Reporting errors: The sensors may not respond appropriately during the startup phase, which indicates that various types of mistakes may have taken place. Some corresponding error handling method is required at this point to safeguard the external control system from a malfunctioning sensor.

Sensor Driver Development

User Guidelines: After the sensors have been correctly initialised, the driver need to be prepared to carry out the user commands. The sensor driver may be in one of the five possible stages before its working time is up: reading the sensor, standby, sleep, waking up, and parameter setting. The qualities and applications of the sensors depend on the needs of the application. It is not feasible to describe every sensor driver architecture in detail. No matter whatever sensors are used, the fundamental units the five described above should be present.

Reading the Sensor: The most crucial aspect of a sensor driver is its ability to read the sensor. The outside controller will send a request instruction to start the reading processes in order to get the sensor data. The sensor data will be generated after the reading operations have been completed. Many sensors temperature sensor, vibration sensor, humidity sensor, etc.) need a particular amount of time, also known as a sample period, to execute the sensing duty since the nature of the detecting material varies. Figure 12 discloses the lifecycle of the request data set of the set.

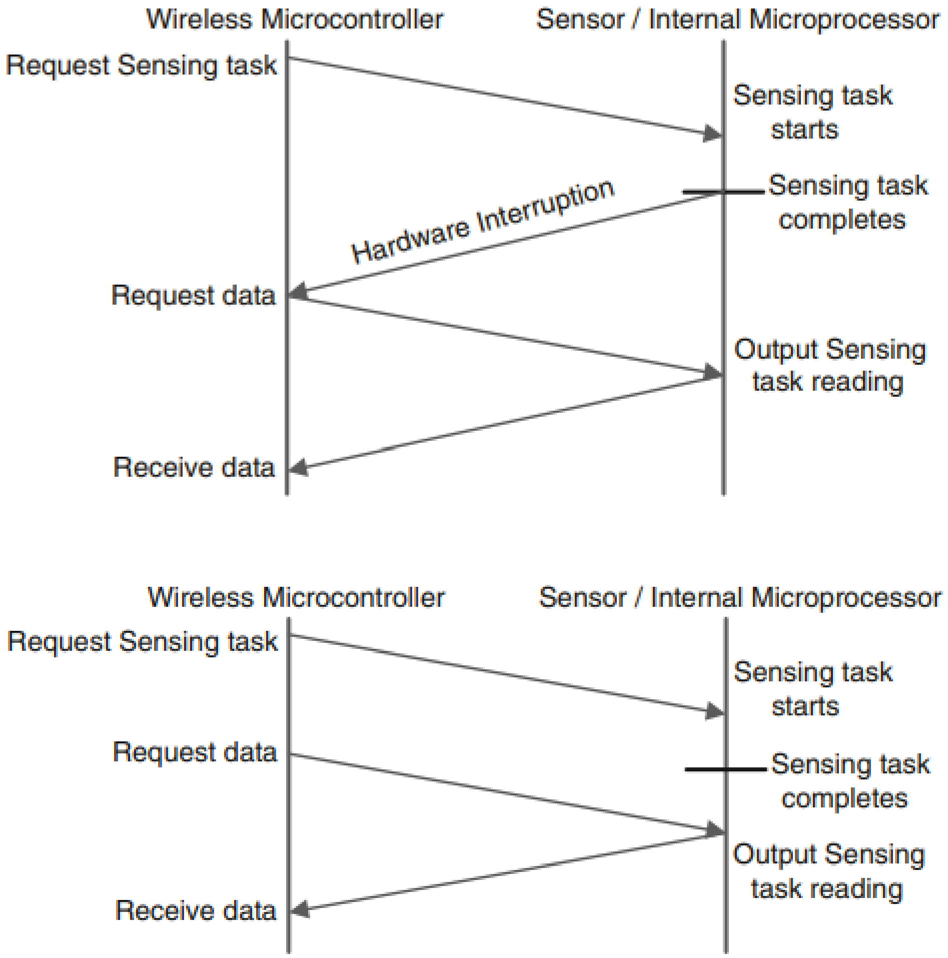


Figure 12: Discloses the lifecycle of the request data set of the set.

There are two ways for the driver to process the sensor:

Generic style:

The application, network, and MAC layer protocols should not be reliant on the WSN transport layer protocol. A transport layer may not be appropriate for certain applications that employ a flat topology if it substantially relies on network topology considerations such as a tree-based design.

Support for heterogeneous data flow:

In the same network, a transport protocol should be able to accommodate both continuous and event-driven flows. Fast response rate control techniques must be used with continuous (i.e., streaming) data to restrict the watershed speed and ease congestion. The rate control sensitivity criteria are less strict for event-driven flows. But it needs a very trustworthy event capturing system (i.e. no data loss) [22]–[24].

A routing protocol is a piece of software that runs at the network layer and determines which output path an incoming packet should take in order to be sent. It is an algorithm for determining a data transmission channel from a source node to a destination node, to put it another way. In WSNs, the destination node is often referred to as a base station or a sink node. It can be beyond the source node's broadcast range or even some distance away. As a result, before the data reaches the sink node, it may need to make many hops. A transmission channel from a sensor to a sink node. However, the routing protocols created for wired networks and other wireless networks like MANET are often unsuitable for WSNs owing to their particular characteristics and limitations. Following is a description of the usual characteristics and restrictions of WSN routing:

1. While conventional networks' routing protocols are developed to achieve excellent Quality of Service (QoS) during data transmission, one of the key goals of the routing protocol in WSNs is energy conservation and lowering power consumption.
2. A WSN may have a high number of sensor nodes.
3. The wireless sensor nodes have several restrictions, including restricted power supply, memory size, compute capacity, and bandwidth for the wireless channels connecting the wireless sensors. As a result, it could be impossible to contact each particular node using a global identifying address.
4. Different application criteria may apply to a WSN. As a result, the WSN's architecture should be application-specific.
5. A routing system should reduce data redundancy caused by several wireless sensor nodes sensing the same environmental condition things happening at once. To minimise duplication, data aggregation is necessary, including duplicate suppression, data fusion, and other techniques.
6. Due to their cheap cost and battery-powered nature, the sensor nodes in WSNs are more susceptible to faults or failure. Therefore, even in networks with node failures, the routing protocol should continue to perform well. This fault tolerance feature necessitates that the routing protocol be able to find and maintain an alternative path for data transmission in order to circumvent any network outage.

Routing Protocol Classification in WSNs

Depending on how the route is chosen, routing protocols may typically be categorised as either proactive or reactive. Routing protocols that are proactive determine routes before they are required and update them as the topology of the network changes.

When a request for transferring data is made, the route may be discovered in the route table that is now accessible and can be used without additional calculation. There is hence no need to introduce extra delay for data transmission. Proactive routing methods, however, are inappropriate for ad hoc networks, as the topology of the network is continually changing. Conversely, reactive routing systems only use a route discovery process when necessary. For dynamic networks, reactive routing techniques are appropriate. However, choosing a route might take some time and may result in increased data transmission delay.

There are several other classification schemes for routing protocols based on various factors. Another categorization of routing protocols, where each routing protocol is categorised as either protocol operation-based or network structure-based. There are three subcategories of network structure: flat, hierarchical, and location-based routing methods there are five subcategories of routing technologies used in WSNs: query-based, negotiation-based, multipath-based, quality of service (QoS)-based, and coherent-based. Since various routing protocols may fall under more than one of these categories and subcategories, they are not mutually exclusive. Only the routing protocols based on network structure are reviewed briefly in this section.

There are three types of network structures: flat, hierarchical, and location-based. All of the sensor nodes in the flat network are equally functional and responsible. Without taking the network architecture into account, they send the data to their neighbouring nodes. In contrast, sensor nodes in a hierarchical network have various functions to perform and are logically situated at various levels. Wireless sensor networks use a variety of routing protocols.

1. Network structure-based
2. Routing in a flat network
3. Routing in Hierarchy
4. Routing based on location and protocol operations
5. Routing strategies include query-based, negotiation-based, multipath-based, QoS-based, coherent-based, and others.

Hierarchical networks are separated into distinct clusters in accordance with Classification of Routing Protocols in WSNs 103, and each cluster names a cluster head to collect and relay inter-cluster traffic. The physical placement of the sensor nodes affects the location-based routing methods.

Flat Routing Protocols

When transporting data, flat routing techniques employ data-centric routing protocols, in which a base station is in charge of contacting other nodes and waiting for their reply. The network may be made more energy efficient by using data removal and negotiation. Without taking into account any topology modifications, a route discovery process may be started by flooding or broadcasting data to all of the neighbouring nodes. The most well-liked flat routing protocols are covered in this section.

Protocol for Flooding

The flooding protocol is the simplest flat routing protocol and is simple to implement over WSNs since no complicated algorithm programming is required. Without taking into account the network's architecture or structure, the flooding protocol simply broadcasts data to every neighbouring node. The identical broadcasting procedure may then be repeated to transmit the data to the target node. Although this protocol is straightforward and simple to use, it has several serious flaws. The production of several duplicate messages by numerous nodes is one of these issues.

Flooding procedure with implosion issue, each node sends the received data to its neighbours without knowing whether those neighbours have already received the data or not, routing technologies in WSNs get the same data twice.

Negotiated Sensor Protocol for Information

SPIN is a different flat routing protocol that uses information negotiation. The SPIN protocol is a modernization of the flooding protocol. The protocol gains a negotiating mechanism with SPIN. Instead of immediately transmitting data to every neighbouring node, SPIN first asks whether any node is interested in the data before sending it to those nodes exclusively. Data advertising (ADV), data request (REQ), and data (DATA) packets are the three different kinds of packets.

A sensor node transmits an advertising packet (ADV) to each of its neighbours once it has data. This ADV contains details on the sensed data. If a node that received the ADV packet has previously received the data, it will disregard the ADV packet. If not, it will return the REQ request packet to the originating node. Finally, the source node will transmit a data packet containing the data solely to these nodes (DATA). Until the recipient receives the data packet, this procedure is repeated. The duplicate data packet and implosion concerns are being addressed by this routing technology. The SPIN protocol comes in a variety of improved forms

The rates of data dispersion are comparable, however. In order to save energy usage, SPIN does not utilise neighbouring distance information. The duplicate data generated is reduced by half thanks to SPIN's negotiating technology. The nodes closer to the source node may not be interested in these data when the destination nodes are at some distance from the source node. So, with WSNs, sending an advertising packet (ADV) does not ensure that the data would reach distant, interested nodes.

Directed Diffusion Protocol

Another data-centric routing system utilised in flat network design is directed diffusion. A sink node or a base station may start the data collection process in the Directed Diffusion routing protocol.

1. Step 1: The sink node broadcasts an interest packet to all of its neighbours, who then broadcast it to all of their neighbours, and so on, until the interest message reaches the

source node that has this kind of data. A gradient value with value and direction characteristics is part of the interest message.

2. Step 2: Using several pathways based on the gradient, the source node, which holds the required data, transmits the data packet to the sink node.
3. Step 3: As illustrated in the sink node strengthens the optimal pathways.

Choosing the optimum route based on the gradient value depends on the application; for instance, some applications call for the shortest path, while others call for the path that uses the least amount of energy. Data is transmitted from Source to sink, while Interest is conveyed from Sink to Source. c best route from the source to the sink.The Directed Diffusion routing technology used in WSNs differs from the SPIN or floods routing protocols.

In Directed Diffusion, the wireless sensor nodes always receive data request packets from the sink node, but in SPIN, the wireless sensor nodes advertise that they have data to transmit and enable any interested nodes to request it. On the other hand, in the Directed Diffusion, every transaction is a neighbor-to-neighbour communication, and every node has the capacity to do data aggregation and caching. In addition to not requiring a specific network architecture, the Directed Diffusion routing protocol may not be appropriate for applications that demand continuous data delivery.

Protocols for Hierarchical Routing

Data routing in wired networks was first suggested to use hierarchical routing. However, with certain improvements in terms of network scalability and communication efficiency, it is also suited for data routing in wireless networks. The fundamental idea behind hierarchical routing protocols is based on categorising wireless sensor nodes into many levels. The majority of hierarchical routing protocols have two routing layers; the first layer is in charge of choosing the cluster heads, while the second layer deals with routing choices. Hierarchical routing protocols, for instance, may separate the sensor nodes based on their amount of energy and demand for extremely low power consumption. While nodes with lower energy levels may only be used to detect events, nodes with higher energy levels can be assigned to analyse and transfer data. The efficiency and scalability of the sensor nodes may be increased by cluster creation inside the network nodes. Numerous hierarchical routing techniques exist. Only a small selection of the most popular protocols are included in this section.

Low Energy Adaptive Clustering Hierarchy

Low Energy Adaptive Clustering Hierarchy (LEACH) focuses on energy conservation and lowering the amount of electricity used for communication. A small number of wireless sensor nodes are chosen at random to serve as cluster-heads in LEACH. The wireless sensor nodes will share the energy usage by repeating this cluster-head selection procedure. Because they use more energy than regular nodes and cannot be joined by other connected nodes, cluster-heads that are fixed will rapidly perish. LEACH operates in two distinct stages. The setup step, which involves specifying the cluster-heads, is the initial stage. The steady state phase, which involves transmitting the data, is the second stage. A collection of nodes (P) choose to take up the role of cluster chiefs during setup. These nodes must choose a value at random between 0 and 1. The node n cannot serve as a cluster head if this random number exceeds a threshold value T (n). The number of nodes G that didn't serve as a clusterhead during the previous rotation (1/P) determines the threshold T (n), which is computed as follows.

The non-cluster head nodes will decide which cluster head they wish to join after getting this advertising. The intensity of the signal from the clusterheads that have reached the node is the primary factor considered in this choice. Therefore, the cluster head that consumes the least amount of communication energy will be selected by the non-cluster head. Following that, the non-cluster nodes will inform the other cluster heads of their decision on the selection of the cluster-head.

For every node in its cluster, each cluster-head will create a Time Division Multiple Access (TDMA) schedule. According to the timetable, each node will send data to the cluster head. After that, the cluster-head aggregates the data to make it smaller. The aggregated data will then be sent to the sink node. The cluster-head role cannot be uniformly distributed across the network's sensor nodes in LEACH. Additionally, LEACH makes the assumption that all energy levels inside the network are uniform. LEACH further presupposes that each node has information to communicate at a certain moment.

Another nested routing technique is the Threshold Sensitive Energy Efficient Sensor Network (TEEN) protocol. The network design of TEEN is built on multilayer hierarchical grouping, as opposed to LEACH, which only has a single tier of hierarchy. The two-tier hierarchical depicts communication between the sensor nodes and their first-level cluster heads and between these first-level cluster heads and their second-level cluster heads. Direct communication between the second-level cluster heads and the sink node. Each level goes through this procedure. Each cluster's CH gathers data from its members, aggregates it, and then delivers it to another CH at a higher level or the sink node. As a node does not have to directly contact the sink node, this layered design increases the coverage of sensor networks and lessens the impact of the power and transmission range restrictions on the sensor nodes. Before reaching the sink node, the data from low-level clusters may pass through many CHs.

For applications monitoring physical events, such as detecting temperature and pressure, TEEN (Manjeshware and Agrawal 2001) is helpful. TEEN is also appropriate for real-time uses like fire alarms. In TEEN, the sensing process occurs instantly, however the data transmitting process occurs sporadically. TEEN sends data through cluster formation. The cluster head will communicate two threshold values to the non-cluster head nodes in its cluster. One is referred to as the hard threshold, and it is the attribute's threshold value over which the sensing node must activate its transmitter and relay the sensing data.

Classification of Routing Protocols in WSNs, paragraph 109 to it the second is known as the soft threshold, and it includes the little variation in the detected attribute's value that causes the node to turn on its transmitter and send the sensed data to the CH.

The Adaptive Threshold sensitive Energy Efficient sensor Network routing protocol (APTEEN) is an improved version of TEEN. APTEEN attempts to proactively gather regular data collections and retact to time-sensitive occurrences. To all the wireless sensor nodes in their cluster, the cluster-heads broadcast the hard and soft thresholds and set the transmission time. When the data values are higher than the strict threshold, these nodes are permitted to communicate the detected information. When the change in attribute value is equal to or larger than the soft threshold, the wireless sensor node will additionally communicate the data. The count time is the maximum amount of time for each node between two consecutive reports. Each node's time to communicate the detected data is assigned using this count time. A TDMA schedule will be utilised to allocate each sensor node a time slot and compel them to detect and send the data if they don't do so throughout the count time. Three main query types are supported by APTEEN:

Analyzing historical data, taking a snapshot of the network on demand, and keeping track of an event over time are all examples of persistent monitoring. When it comes to extending network lifespan and conserving energy, TEEN and APTEEN perform better than LEACH. On the other hand, both protocols still incur additional cluster overhead. The threshold operations and count time calculation add network overhead and implementation complexity. Controlled variable reliability while certain applications call for 100 percent uptime, others can live with occasional packet loss. This feature should be taken advantage of by the transport layer protocol in order to save energy at the nodes. For instance, we may not use a packet retransmission mechanism if the system doesn't need a 100% packet arrival rate.

Congestion detection and avoidance:

The most crucial component of a transport protocol is its congestion detection and avoidance mechanism. Because congestion only occurs in a small number of isolated "hot spots" where traffic volume is noticeably greater than at other locations, congestion identification with WSNs is not as simple.

Base station managed network:

Since sensor nodes have limited energy resources and processing power, the base station should handle the bulk of functions and computationally demanding activities. Since the sensors must lower their transmission rates to lessen the traffic, if we could share certain duties among them, we could be able to achieve a greater congestion avoidance impact.

Scalability:

Since there may be a huge number of nodes in sensor networks, the protocol needs to be scalable. Unfortunately, finding all sensors with memory management is difficult. Future improvements and performance enhancements the protocol need to be flexible enough to accommodate future adjustments that boost network efficiency and enable new applications.

Congestion recognition and avoidance:

In a WSN, certain sensors that relay data will become congested when multiple sensors send out data at once. It's critical to recognise such clogged sensors and use effective measures to stop further clogging.TCP, the most widely used transport protocol, has been used on the Internet for many decades. A communication channel must first be established through the 3-way handshake procedure used by the TCP protocol stack. The transmitting pace is then managed by a sliding glass door video content protocol that runs continuously. It assumes packet loss and rebroadcast the data when it detects timer-out or three duplicate Acknowledgement (ACK) packets. It strives for 100 percent dependability [25], [26].

Protocols for Location-Based Routing

The location-based routing protocols make up the third group of WSN routing protocols depending on the network architecture. The major goal of routing protocols in this category is to use the advantages of wireless sensor node locations in data routing. Based on each node's precise location, an address is generated for it. The Global Positioning System (GPS) or other positioning methods may be used by satellites to pinpoint the locations of each node. Depending on the signal strength, it is possible to compute the distance to the neighbours. In this section, two common location-based routing techniques will be discussed.

Geographical Flexibility

The main focus of Geographic Adaptive Fidelity (GAF) is energy awareness. Although GAF was first created for wireless ad hoc networks, it is equally appropriate for WSNs. GAF reduces energy use without compromising the reliability of routing.

WSN Routing Technologies

The primary idea of GAF is to partition the sensors field into predetermined virtual grid zones. Each node in the same zone will have a symmetric routing cost. As a result, by placing some of these nodes in the same zone into sleep mode, more power may be saved. Each node in the same zone may have its location determined using GPS shown to be separated into a sensor field. Node 1 is situated in zone A, followed by nodes 2, 3, and 4 in zone B, and node 5 in zone C. The dimensions of the virtual grid are r. Nodes 1 and 5 can interact with nodes 2, 3, and 4, but because they are in different zones (A and C, respectively) and are separated by zone B, they are unable to directly connect with one another.

The discovery stage, the active stage, and the sleep stage are the three phases of GAF. Discovering each node's neighbours inside the grid is a part of the discovery step. Nodes engage in data routing during the active stage. The transmitter of the node is turned off, and the node is put into sleep mode at this stage. Two of nodes 2, 3, and 4 in zone B may be simultaneously shut off, with one of them remaining awake for communication. It is clear that the positioning of the wireless sensor nodes in this routing protocol rely on the GPS technology, which is not always accessible, particularly for interior applications. In addition, this routing technique adds additional memory cost in order to store each node's neighbours' addresses.

Geographical and Energy-Aware Routing Protocol

In data-centric WSN applications, the Geographic and Energy-Aware Routing protocol (GEAR) aims to send data to every node within a designated area. The GEAR protocol routes data to a specific region of the network using the geographic data. The GEAR relies on energy and geographical information about the surrounding areas while routing data to a target location. By distributing interest packets to specific areas or directions inside the network as opposed to the whole network, GEAR's major goal is to decrease the amount of interests in Direct Diffusion.

The anticipated cost is determined by the target region's distance in addition to the energy that is still available. A network hole is produced when a node is the only one in its immediate vicinity on a path to the target area. The learnt cost is the modification to the predicted cost brought on by navigating network flaws. If there are no gaps in the network, the anticipated cost will be identical to the learnt cost. Every time a data packet arrives at the target area, the learnt cost is sent back one hop. GEAR chooses the next hop neighbours with intelligence to route the data to the target location in an energy-efficient manner based on the energy-aware information. GEAR distributes the data to all the nodes in the target area once it has arrived there.

The GEAR algorithm includes two steps,. Forwarding packets in the direction of the target location is the first step. The second stage involves spreading the packet throughout the intended area. The wireless sensor node that got the data initially checks to see whether there is at least one neighbour node that is closer to the intended location. The sensor node will choose the neighbour node that is closest to the target area if there are many neighbours. This node is designated as a network hole if there are no neighbours along the route to the target area. After the data packet has arrived at the target area, it may be spread via controlled flooding or recursive geographic forwarding in the second phase.

Protocols for AODV Routing

One of the most talked-about and sophisticated routing protocols is AODV, or Ad hoc On Demand Distance Vector. Charles E. Perkins (Nokia) and Elizabeth Belding-Royer are its principal creators (UCSB). The Motorola Cluster-Tree routing system and the AODV routing protocol are both implemented in the ZigBee standard, making them both extensively utilised in industry. This section explains the AODV idea and provides implementation specifics for a condensed form of AODV.

A dynamic, self-starting, multi-hop routing protocol called the Ad hoc On-Demand Distance Vector (AODV) algorithm allows participating mobile nodes to create and sustain an ad hoc network. With AODV, mobile nodes may rapidly receive routes for new destinations and are not required to keep up routes to locations with which they are not currently in contact. A further benefit of AODV is that mobile nodes can quickly adapt to network topology changes and connection breaks.

When a route to a new destination is required, the node broadcasts an RREQ to discover a route to the destination. AODV defines three sorts of messages: Route Requests (RREQ), Route Replies (RREP), and Route Errors (RERR).

In order for the RREP to be unicasted from the destination via a backward path to that originator, each node receiving the request stores a route back to the request originator in a backward table. When the RREQ reaches the destination or a node that provides reachability to the destination, a route may be established. By unicasting an RREP back to the source of the RREQ and establishing a routing table at each node, the route is made accessible. A HELLO message is routinely sent out by nodes that keep track of the link status of upcoming hops for active routes to detect a link break; if no ACK is received, the broken connection is invalidated. As a result, an RERR message is often sent to inform other nodes that the connection has been lost.

In a paper produced by the Internet Engineering Task Force (IETF) Mobile Ad hoc Networking Working Group, the forms of the messages RREQ, RREP, and RERR have been established. The specifics of these forms are shown in provides a list of the fields' definitions Application of an AODV Simplified Version

This section shows how a condensed version of AODV was implemented in sensor nodes running the Contiki Operating System (OS). Depicts a WSN with four sensor nodes in which node S must communicate certain detected information to node R. S and R nodes cannot communicate with one another. Two routers called transmitter nodes T1 and T2 are used to transport messages that have been received. The last node is Node R.

Software Architecture Design Two different software applications must be developed, one for the sender and one for the routers and receiver; the sender software application will be responsible for reading data, routing and forwarding, and the receiver software application will receive the data and forwards or displays it. The receiver software application should fit on both the routers and the receiver node as both kinds of nodes receive the same types of packets. Shows the flowchart for the sender application where two timers have been set. Timer 1 is set for determining the time interval of sensor reading.

When a route discovery is required, the route request message (RREQ) must be broadcasted to the neighbours and wait for route response message (RREP). Afterwards, the sender program will figure out the best path to the destination. When the best path is calculated, the routing table will be updated and the sensor readings will be forwarded to the next hop as a unicast connection. The criteria used in selecting a route here is to use the node with a higher battery level first and then choose the node with a higher RSSI level. The detail of each component is omitted for the sake of the simplicity. The router can receive a broadcast message (RREQ) or two types of unicast messages, RREP and Data Transmission (DATATX). If the packet is RREQ and the current node is not the destination node, the RREQ will be rebroadcasted. If the current node is the destination node, a RREP will be sent back. If the packet is DATATX, the packet will be forwarded to its receiver. If the packet is RREP, it will be forwarded to the sender node. The backwards table and the routing table should be updated as necessary. If the broadcast limit has been reached, it must discard the current message in order to avoid useless bandwidth occupation; otherwise the broadcast counter will be increased by 1. 118 5 Routing Technologies in WSNs 5.4 Cluster-Tree Routing Protocol the cluster-tree routing protocol is another routing protocol implemented in the ZigBee stack, and also has been widely used in industry.

It is a self-organised protocol that supports network redundancy in order to achieve fault tolerance in the network. The cluster-tree protocol uses packets negotiation to form either a single cluster network or a multi-cluster network. The cluster formation Start System Initialization Set Timer 1 Timer 1 expires Route Request

Set Timer 2 Timer 2 expires Route Table Available Sensor reading Sending out Sensor reading. Flowchart of the sender application Cluster-Tree Routing Protocol 119 process consists of two stages; select the cluster-heads of the WSN and subsequently, the non-cluster-head nodes in the WSN join the cluster-heads in order to form the clusters. Single Cluster Network a single cluster network contains only one cluster-head. All the nodes are connected to this cluster-head with one hop, and the network topology becomes a star Request route Broadcast route request Abstract sender's Battery and RSSI Battery > average level RSSI > existing RSSI Update route table Battery > existing battery End Route response.

Flowchart of route request in the sender application 120 5 Routing Technologies in WSNs topology. Each node in the network is waiting to receive a HELLO packet from the node that acts as a Cluster-Head (CH). The HELLO packet includes the clusterhead MAC address and the cluster-head ID number, which is equal to zero (0) in the single cluster network. If any node fails to receive a HELLO packet after a certain period of time, this node will be converted to act as a cluster-head. Then, it will distribute a new HELLO packet to all its neighbouring nodes, and waits to receive the CONNECTION REQUEST (CON REQ) packet from the neighbours. If it does not receive any CON REQ packets, it will turn back into regular node and wait again to receiving a HELLO packet.

The cluster-head can also be selected based on some features such as the transmission range, power level, computing ability, or location information. As shown in, once the cluster-head receives a CON REQ packet from a neighbour node, it will reply with a CONNECTION RESPONSE (CON RES) Processing Unicast message Broadcast message N Reach destination Y Re-broadcast N END Y RREP N Data Transmission Return RREP through unicast Y Locate the request node Y Send RREP N of router/destination nodes Cluster-Tree Routing Protocol 121 packet. The CON RES packet includes the node ID of the non-cluster-head node. Finally, the non-cluster-head, that receives the node ID, will send an Acknowledgment packet (ACK) to the cluster-head node.

If the cluster-head reaches the maximum limit of the node IDs, or reaches any other defined limitations, it would reject any new node connection request. This rejection is signalled by assigning a special ID to that node. The list entry of all neighbours and the routes would be updated periodically by sending HELLO packets. A node could receive an HELLO packet from node that belongs to other clusters. Consequently, the node saved the Cluster ID (CID) of the transmitting node in its neighbours list. After that, it would transmit the CID with the neighbour node ID inside the LINK STATE REPORT to its cluster-head. Subsequently, the cluster-head would know those clusters with which it has an intersection. The LINK STATE REPORT packet also allows the cluster-head to identify any existing problems in the network. If the cluster-head wants to update the topology of the network, it can be achieved by sending a TOPOLOGY UPDATE packet.

If the cluster-head stops working, then the transmitting of the HELLO packet would also be stopped. Therefore, all nodes would know that they have lost the cluster-head. Subsequently, a new cluster-head will be reconfigured by repeating the same process. Multi-Cluster Network A multi-cluster network consists of many single clusters. Multi-cluster networks need a Designated Device (DD) to give a unique Cluster ID to each cluster-head, and to calculate the shortest path from the cluster to the designated device. After the designated device has joined the network, it would act as a cluster-head, and would send HELLO packet to its neighbours. If the clusterhead receives the HELLO packet, it would send a CON REQ and would join the designated device to form the top-level cluster (Cluster 0). If the cluster-head is connected directly to the designated device, the cluster-head will become a border Establish a link between a cluster head and a node Routing Technologies in WSNs node with two logical addresses.

As shown in, if a regular node received the HELLO packet from the designated device instead of its cluster-head, it would act as a border node to its parent. The cluster-head would send a NETWORK CONNECTION REQUEST (NET CON REQ) packet to setup the connection with the designated device. Subsequently, the border node would send a CID REQUEST (CID REQ) packet to the designated device. If the designated device sent a CID RESPONSE (CID RES) packet, that contains the new cluster ID (CID), to the border node, the border node would send a NETWORK CONNECTION. Multi-cluster network consists of many single clusters Link CH with DD by border node Cluster-Tree Routing Protocol 123 RESPONSE (NET CON RES) packet to the cluster-head with the new CID. In addition, the cluster-head would inform its nodes about the new CID. Energy-Aware Routing Protocols AODV is not an energy-aware routing protocol. AODV uses the same route to send all of the data from the source to the destination until this route dies.

Therefore, the intermediate nodes on this route between the source and the destination nodes quickly expended their energy and die. As a consequence, the lifetime of the whole network will be effected, especially if the dead nodes are vital to the network such as being the coordinator or the router nodes. The clustertree protocol also does not consider the energy levels of the wireless sensor nodes in choosing the cluster head or determining the number of the clusters required in each network. It uses static nodes to act as cluster-heads during the whole lifetime of the network, which makes these nodes die quickly. This section considers the energy levels of the wireless sensor nodes, which can be applied in both AODV, and cluster-tree routing protocols. In order to maximize the lifetime of the PAN coordinator, the routers, and the whole network, it is necessary to balance power consumption and distributing the responsibilities of routing among the wireless sensor nodes especially the routers and the PAN coordinator. Therefore, it will be better to fully exploit the wireless sensor nodes to participate in the communication process and share data transmission. Firstly, the energy model of the wireless sensor network is presented. This energy model consists of several formulas.

ConsSpeed ¼ InitEng RemEng TimePeriod ð5:2Þ where, RemEng is the current energy level of the node and InitEng is the initial level of the node energy when this node joined the network. TimePeriod is the period of time that the node takes to consume the energy. ConsSpeed is the energy consumption rate for the node. The next formula is related to the lifetime of each node, LifeTime. This lifetime is the period of time for which the node can be kept running before dying or stopping transmitting and receiving signals. The lifetime of a node can be measured by Eq. LifeTime ¼ InitEng ConsSpeed Routing Technologies in WSNs This remaining lifetime means the period of time left for the node to keep running and serving the route. RemainTime ¼ RemEng ConsSpeed The remaining energy of the node indicates the level of energy left in the node and can be measured, RemEng ¼ IniEng ððPktT rxPowerÞÞ ð5:5Þ where PktT is the count of packets transmitted by this node. txPower is the transmission energy required to transmit each packet. PktR is the count of the received packets. rxPower is the energy consumed by receiving one packet. The lifetime of WSNs can be increased by distributing the role of routing and balancing the energy consumption among the whole collection of nodes.

Lifetime maximization can be achieved by taking into account the changes in the energy level of the wireless sensor node batteries simultaneously with the path discovery process and the packet forwarding process. In the energy-aware routing protocol, most of the nodes will act as intermediate nodes between the source and destination nodes. A new route will be established if an intermediate node along the pass to the destination has a lower energy level or a higher energy consumption rate. The energy cost of establishing a new route, EstRouteCost, can be obtained by EstRouteCost ¼ HopsNo Time ð5:6Þ where HopsNo is the number of hops between the source and destination node, txPower is the transmission power for one packet, and Time is the time needed to transmit these discovery packets. Because of the very short time needed to establish a new route, the whole energy cost of establishing a new route could be insignificant. In addition, the energy-aware routing will aim to keep most of the nodes running for their maximum lifetime. Each node, which has a high energy consumption rate and a short remaining lifetime, should be turned off for a period of time. A high energy consumption rate is determined by comparing the node’s energy consumption rate with other nodes. Turning off a node will make the energy-aware routing protocol choose an alternative node or change the whole route to the destination node. Repeating this process can distribute the routing role among most of the nodes; therefore balance the power consumption in the network as a whole. The additional steps necessary for the energy-aware routing within the existing routing protocols such as AODV or Cluster-tree routing. These steps are as follows:

At first, Node S must broadcast an RREQ message since it is unable to determine a path to Node R. The message will be received by Nodes T1 and T2, but since they are not the target nodes, they will resend it to Node R. Due to the possibility of simultaneous transmission from Nodes T1 and T2, a collision may occur. The transmitters wait for a random amount of time before delivering the message as part of a very basic collision avoidance technique. Node R unicasts an RREP message to the two transmitters T1 after receiving the message shows the format of the RREQ message in WSNs and T2 before going to Node S. Node S might choose the path based on two factors. The router with the highest battery level or the one with the highest RSSI is chosen. Node S will utilise the route once it has been found to deliver the sensed values in a unicast message.

A 20-byte header used by TCP is used to store congestion management and other data. With tiny packet sizes, the overhead from headers may use quite a lot of resources. Sensor data in WSNs are often numerical numbers. Such data may be represented with a few bytes. The TCP overhead is thus rather high.

The base station often the receiver side is made as simple as feasible via TCP. The base station merely sends an acknowledgement back to the sender of the packet if the data is right, it sends an ACK; if not, it doesn't respond at all. The sender must carry out a number of difficult rate control actions. In contrast, the base station in WSNs has infinite energy whereas the transmitter sensors has relatively restricted resources. More weight should be placed on the base-station side.

CHAPTER 6

LOCALIZATION IN WSN

Chandra Shekhar Rajora, Assistant Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University, Jaipur, India
Email Id- chandra.shekhar@jnujaipur.ac.in

In wireless sensor networks (WSNs), the phrase "localization" refers to pinpointing a device's position in the lack of external infrastructure, such satellites. So, the movement information service makes it possible for a device to be aware of its location. Due to the electricity nature of such endpoints, using extra devices is not recommended for wireless networks, particularly those with limited resources.

For instance, the global positioning system (GPS) locates a gadget by using distance readings from satellites. Additionally, indoor localisation is not possible with GPS. The need to find robots in the area of robotics is the traditional source of the localization challenge. It is crucial to have access to location data when a robot has to navigate a terrain.

Wireless sensor networks' (WSNs') information is closely connected in both space and time. The positioning of information-generating sensors is crucial in applications such target tracking, geographic routing, pollution management, structure health monitoring, and forest fire monitoring. For instance, in apps used to monitor forest fires, it is necessary to track the position of the fire in position to obtain precautions [27]–[29].

Additional uses include the enhancement of location-based regional routing techniques and medium access optimization. However, the localization issue for WSNs is considerably different from that of other networks since it is a network of tiny, low-powered devices. Additionally, the geolocation of the clusters is crucial for associating sensor data with node position data.

Localization: For data collecting and sensing, sensor nodes are dispersed all over the area. The knowledge of sensor node locations is often beneficial.

Localization offers the following benefits:

1. Some applications, including those used to monitor objects, heavily rely on position. Location-based Routing is activated, which might potentially lead to energy reduction.
2. Locations are useful for managing and monitoring sensor networks, which generally improves security.

Centralized System: In this scheme, sensor nodes communicate with a known central node by sending control messages to it. The central node then determines each sensor node's position and notifies the nodes of it.

MDS-MAP:

This system has the benefit of requiring neither anchor nor beacon nodes at the outset. Even without anchor nodes, it creates a relative map of the nodes; after adding three or more anchor nodes, the relative map is converted into absolute coordinates. When the number of anchor nodes is modest, this approach performs well. The fact that MDS-MAP needs centralised computation and network-wide information is a disadvantage.

A centralised localization method based on RSSI has the benefit of being a useful, self-organizing method that can handle any outside situation. The drawback of this system is that it uses a lot of power since it has to generate a lot of information and send a lot of it to the control centre.

Distributed System:

Each sensor node pinpoints its precise position on its own. Additional categories for distributed localization include range-based systems and range-free techniques. The range-based technique needs some ranged information, such as arrival time, arrival angle, or arrival time difference. Estimations of the absolute point-to-point distance is used to determine the location [30]–[32].

The signals from the individual sensors of WSNs are often transported to the Internet or other terminals through a number of sink nodes, despite the fact that WSNs may have different topologies, such as star, ring, mesh, or tree. A sink node is a special device that connects to regular sensor nodes but is more powerful than them, connecting a sensor network to the end consumers. The sink nodes may be thought of as a laptop computer that receives data from the network or as a much more compact micro-controller that serves as the gateway. Each sensor node has the ability to gather data and route it back to the sink node and the end users. The sink node is used to transport data back to the final user.

Depending on what the application requirements need, a sensor network may have several sink nodes operating at once. Two sink nodes X and Y the same level of interest in an event happening in sensor node B. When two sink nodes are deployed, sensor node A is many hops from sink node X and just one hop from its closest sink node, Y. As a result, sensor node A will use fewer hops and less electricity to relay its signal to a sink node when using two sink nodes as opposed to one sink node. We are aware that the energy required to route a message from any sensor node to the closest sink node is inversely correlated with the number of hops the message must make. Utilizing numerous sink nodes efficiently lowers the energy use for each message sent. The route length from a sensor node to a sink node becomes shorter and the sensor node's lifespan gets longer as the number of sink nodes rises. However, due to the sink node's higher cost than the sensor node, the number of sink nodes is restricted financially. Additionally, there may be times when using numerous sink nodes is not physically feasible.

Performance of the network may be affected by the sink node's location. Through the use of experimental data, showed that sensor nodes that are one hop away from a sink node use energy more quickly than other nodes in the sensor network. This is due to the fact that nodes that are one hop away from a sink node must also transmit messages produced by many other nodes in addition to their own. These nodes' burden is much greater than that of nodes further away from the sink node. As a result, these sensor nodes exhaust their energy more rapidly and stop functioning. The sensor network ceases to function if there are too many dead or nonoperative sensor nodes around the sink node, preventing other surviving sensor nodes from connecting directly to the sink node.

Sink Node Positioning Challenges

Finding the best sink node placements in wireless sensor networks is not without its difficulties. These include the presence of a sizable, if not infinite, solution space, an excessive number of related parameters, varying routing algorithms, varying application requirements, the presence of a sizable number of sensor nodes, and varying sensor node capabilities.

1. Vast, if not limitless, solution space: sink nodes are not catalogued and may be found everywhere in the environment. When there are no constraints, there are a lot of potential solutions.
2. A significant number of sensors are involved: Sensor networks may include thousands of sensor nodes. The sink node location issue becomes NP-complete when there are many sensor nodes involved.
3. Dynamic topological changes: The deployed sensor nodes may malfunction owing to manufacturing flaws or energy depletion, necessitating a change in the topology of the sensor network and the position of the sink node.
4. Node capability variations: Not all sensor nodes are created equal, for example, some have variable transmitters while others do not. In this situation, reducing the communication distance in sensor networks made up of sensor nodes with fixed transmitters and different communication ranges results in improved energy usage, but no energy savings are possible if only sensor nodes with a fixed range transmitter are utilised.
5. Differences in network architecture: There are two kinds of conventional sensor networks: flat and hierarchical. In contrast to hierarchical sensor networks, which disseminate data to the sink node via cluster-heads, flat sensor networks distribute data in several hops through network intermediate nodes.
6. Variations in routing algorithms: Different routing algorithms use various strategies to maximise data transmission tasks in sensor networks. When transferring data to the sink node, every routing algorithm provides a different data delivery structure. Different energy models are the result of these variations.
7. Differences in sampling modes: Periodical data sampling is required for wireless sensor networks, or they may function in an event-driven manner. The ideal sink node location issues become more challenging due to the need to accommodate both sampling modes. Choosing to optimise for a certain data sampling method, however, may require various considerations.

Sink Node Positioning Methods Categories

The majority of sink node placement research has concentrated on carefully choosing the sink node location, which may impact a variety of performance measures including energy consumption, latency, and throughput. They focus on structural quality indicators such network connection and distance, and/or they base their research on a predetermined topology. We categorise them as static techniques as a result. The optimality of the initial position for the sink node may become vacant throughout the operation of the network, due to changes in the state of the network or numerous external circumstances. However, dynamically altering the sink node placement may further boost the dependability of WSNs. For instance, it makes sense to put the sink node near to where targets are found and where there is a lot of traffic in a target monitoring application. We refer to these techniques as dynamic approaches.

The sink node has no ability to move while it is in a static position.Throughout the functioning of the network's existence, its position stays constant. The location of a single or many sink nodes in WSN, as well as optimization during network setup, have both been the subject of much study. The assumptions used, the network model taken into consideration, the information on the network state that is accessible, and the metrics that should be optimised may all be used to categorise the published studies.

The main goal of static sink node location is to increase network longevity. The location of the sink node was experimented with in various ways .Either the network lifespan specification, the network operation mode, or the network state parameters that are part of the optimization aim are to blame for the discrepancy. Although some users define the network lifespan as the period of time until the first sensor node fails, many others define it as the failure rate of a portion of installed sensors. Other research attempts to maximise network longevity by lowering the overall power used to get data from all sensors.

Additionally distinguishing aspects are the system model taken into account and the network architecture.

The sensors in a flat network architecture are uniform in their starting energy and often construct several paths to transmit their data to the sink node. Sensor nodes are arranged into clusters with a defined cluster leader in a hierarchical structure. The inter-cluster head network becomes the primary focus of the sink node location challenge in this scenario. The two-tiered hierarchical design of WSNs is shown in, where SN stands for sensor node and AN stands for upper and lower sensor nodes. Head Cluster for the Sink Node Cluster (a) (b)

132 Application Node, a cluster head, and BS, a different term for sink node, are used in the phrase "Optimization of Sink Node Positioning." The sink node is positioned to minimise either the maximum distance between cluster heads or the sink node or the amount of electricity used to transport data from the cluster head to the sink node.

Dynamic Sink Node Positioning

When sink nodes are installed in their initial positions, static sink node placement does not relocate them since it does not take into account dynamic changes that occur during network operation. Examples of dynamic changes include traffic patterns that can alter in response to events being monitored, load imbalances that can lead to bottlenecks, changes in application-level interest over time, and changes in the resources that are available on the network brought on by nodes running out of energy.

While the network is running, the sink nodes may be moved dynamically to enhance network performance. For instance, it could be prudent for the sink node in a target tracking programme to maintain a certain distance from a dangerous target. Maintaining a safe distance is important. Sensors in a disaster management programme may spot fires, falling structures, gas leaks, and other hazards. In these circumstances, it would be dangerous to approach these alleged incidents too closely.

Another instance is when multiple sensor nodes close to the sink node stop functioning as a result of their batteries running out. It is preferable for the sink node to relocate itself so that data sources may more quickly and reliably access it. According to, the sink node in an event-driven sensor network should be moved adaptively depending on the timing of the events.

When should the sink node move, where should it go, and how will the data be routed while the sink node is moving? These are the three steps suggested. Three example heuristics for dynamic relocation of the sink node were provided by, and they may help the network operate better in terms of energy consumption, data delivery latency, and sink node safety. They are moving to improve the lifetime of the network, speed up time-constrained traffic, and safeguard the sink node.

Positioning of Mobile Sink Nodes

A sink node may move as needed or would remain immobile without the use of dynamic sink node placement. A sink node might be created as a movable object that can move continuously inside a sensor field as opposed to just when necessary. By travelling toward sensor nodes where data originated, a mobile sink node may be utilised to gather data from a poorly populated sensor network. The sink's motionIf the sink node has a flying capability, random movement within a sensor field may be effective for large-scale applications like monitoring forest fires but is not recommended for time-sensitive applications.

By placing a sink node at a predetermined location at a predetermined time, predictable sink node mobility aims to maximise energy usage deployed a mobile sink node that travels along a predetermined route and collects data from the sensors as it approaches them.

This predicted mobility strategy makes it possible to gather data with a limited amount of transmission delay. Only calling nodes when they are scheduled to send data will result in the greatest power savings.The system model is created using the following assumptions about the WSNs for the purpose of simplicity:

- All sensor nodes have equal initial energy;
- The transmission range of each sensor node is fixed and equal to the distance between two adjacent nodes in the grid, i.e. a hop is of one grid cell side length;
- Multiple sink nodes are fixed on the grid;
- Data transmission and reception are the major energy consuming activities;
- All sensor nodes have equal initial energy;
- Sensor nodes communication
- Area that the sensor network covers Sensor Node for Mobile Sink Nodes
- Sensor network with a moving sink node.
- Sink Node Positioning Optimization
- Sink nodes may only be placed at certain locations in the grid, known as viable sites, and their quantity is set and predetermined.
- A sensor node uses the same amount of energy to send a bit as it does to receive a bit, hence the energy use is constant.

Formally, a sensor network is represented as a graph G (V, E), with V standing for sensor nodes and E for one-hop communication between two neighbouring nodes (i, j). Given the sensor network's mesh structure, a sensor node I may directly connect with its four neighbouring nodes (left, right, upper and lower).

Data packets created at the sensor node must be routed across many hops in order to reach the sink node if one-hop connection between the sensor node and sink node does not exist.

The notations and mathematical formulation used here to represent the power consumption at each sensor node were taken from 2005, and they are extended to include the scenario of numerous static sink nodes.

1. e0: initial energy (Joules) of each node less the threshold energy needed for node functioning; e: energy consumption coefficient for sending or receiving one bit (Joules/bit);
2. r: The rate (in bits/s) at which data packets are created; for homogeneous sensor nodes, r is constant across all nodes;
3. Ck I The amount of energy used to send and receive packets at node I while the sink node is at node k (Joules/s).
4. Network lifetime: z (seconds).

Lifetime of Node I allocated to Sink Node KJ (zij) (seconds).Simplified Routing Protocol, A streamlined routing protocol is taken into consideration in the WSN with the mesh topology as illustrated in

- A specific shortest route is adopted between a sensor node and a sink node when they are located on the same horizontal or vertical line, respectively shows a mesh-based WSN. Locating Static Multiple Sink Nodes for Maximum Efficiency
- If not, equal amounts of the two pathways will be taken along the edges of the rectangle with the sensor node and sink node as its opposing corners is an illustration of three scenarios b, a data package must be sent from node I to the sink node via two hops on a specific route four hops in two symmetric paths are needed.

Model for Energy Consumption,

Each node's location is expressed using an ordered pair of its column and row numbers, as seen in WSN's streamlined routing technique for mesh networks. 136 6 Improvement of the Sink Node the nodes connected to the row and column of the sink node are surrounded by horizontal and vertical dotted lines. These lines divide the sensor field into nine subsets: Upper Left (UL), Upper Right (UR), Lower Left (LL), Lower Right (LR), Vertical Above (VA), Vertical Below (VB), Horizontal Left (HL), Horizontal Right (HR), and the node K that houses the sink node.

As an example, consider node I in subset UR. Node I broadcasts its own created data packets to nodes j2 and j4, in that order. These packets are sent to sink node k by nodes j2 and j4. Node I also gets a portion of the packets produced at nodes j1 and j3, as well as a portion of the packets produced at nodes l1 and l2. The packets from nodes j3 and l2 are then retransmitted to node j2, while those from nodes j1 and l1 are sent to node j4. In conclusion, node I has power consumption of ck I 14 and sends and receives data packets at rates of 2r and 3r, respectively. 5 re: \sVA

The sensor field may be further divided if there are many sink nodes present. The division of the sensor field with two sink nodes, k1 and k2, is shown in are the designations for the subgroups. Some of the subsets will overlap depending on where the two sink nodes are located. If all of the sensor nodes are allocated to the closest sink nodes and there is no double assignment, that is, each node is assigned to one and only one sink node, the energy consumption calculation The lifespan of a sensor node is specified as max is the period until the first sensor node in the network runs out of battery power.

The positions of the various sink nodes should be optimised in order to maximise the lifespan of the sensor network and the shortest lifetime of all the sensor nodes. Thus, according to Yang A constraint may be added to the above optimum problem to express the case where sink nodes cannot be put at any obstacle in the sensor field, where / is the set of obstacles.

The issues posed by are optimum location problems that may be solved using a variety of optimization techniques. The majority of the evolutionary computation techniques may be used to solve the location issues due to the nature of the multi-variables in the aforementioned optimization. The ideal location issue is modelled by as a GA search issue. The implementation of the following three definitions is done in detail:

A fitness function described in terms of the problem's chromosomal representation; a set of manipulation operators, such as crossover, mutation, and reproduction; and a problem representation in the form of a chromosome that may be symbolically altered. The coordinates of N sink nodes, which are N pairs of integer coordinates Locating Static Multiple Sink Nodes Most Effectively

The chromosome is represented as an integer string of length 2N, which is equal to the double of the number of sink nodes. Equation shows that it is impossible to locate two separate sink nodes in the same place. Sink nodes cannot be placed in the same area as the set of barriers, according to equation. The goal function indicated in Eq is used to choose the fitness function in the GA.

The largest value of for all conceivable combinations of N sink nodes will be the desired value of the fitness function. The chromosome described in Eq. is updated using the three GA operators of crossover, mutation, and reproduction while satisfying the restrictions stated. In this work, an easy simulation has been performed sensor network having three forbidden locations and is created with two sink nodes

GA begins with multiple chromosomes that describe a variety of random solutions to the optimum placement issue since these two sink nodes are first chosen at random. The settings of GA are set at a mutation probability of 0.08, a crossover probability of 0.6, and a population size of 20. The parameters of the 8 9 8 sensor network are set to have the following values: r = 1 bit/s, e = 0.62 lJ/bit, and e0 = 1.35 J. The search results show that the two sink nodes are best placed in the top left corner (0, 0) and the bottom right corner (7, 7). This conclusion agrees with the findings for mobile sink nodes in study.

In this chapter, we simply take into account the multiple sink node locations optimum issue in terms of a streamlined routing method. The system model is likely to be far more complicated if the sensor network uses any other routing technique. We assume, in particular, that all sensor nodes are fixed, distributed in a bi-dimensional square grid with cells of the same size, and that the transmission. Improvement of the Sink Node Each sensor node's positioning range is fixed and equal to the space between its next two neighbours in the grid. The system model is the simplest with these two presumptions, although it is improbable that they are accurate. Given that the sensor nodes' locations may vary and their communication ranges, additionally, we assume that the number of sink nodes is predetermined and known. The number of sink nodes must be added as an extra optimum variable in the optimization if this supposition is false. However, the approach presented and the formulations of the search problem are often relevant to any challenging sink node location issues.

More costly and more precise.

Following is how the range-free algorithms operate: In WSNs, several grain nodes are dispersed. Seed nodes regularly broadcast http broadcast messages with current location information and are aware of their own positions. After receiving these control signals, sensor nodes may determine their own placements. Distributed algorithms based on beacons: divided into three sections:

Diffusion: In diffusion, a node's centroid at its nearby known nodes is where it will most likely be located. For APIT to provide a reliable location estimate, a high ratio of lighthouses to nodes and longer range beacons are necessary. This approach will not provide reliable results for low beacon density. Bounding box: Bounding box creates a zone around each node before attempting to adjust their placements. By employing distance measurements to nearby nodes and recognized beacon destinations that are many hops distant, collaborative multilateration allows sensor nodes to precisely estimate their positions. Additionally, it raises the computing cost at the same time.

CHAPTER 7

TOPOLOGY MANAGEMENT IN WSN

Lokesh Lodha, Associate Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University,
Jaipur, India
Email Id- lokesh.lodha@jnujaipur.ac.in

Wireless sensor networks (WSNs) operate with a mostly "autocratic" operating strategy. To sustain their autonomy, such networks must really be capable of self-configuration. The sensor nodes' temporal coordination and coordination fulfil the demands of WSN-specific applications. Naturally, it is required of these nodes to maintain a sound intra-network architecture. They have a limited communication range, minimal processing capability, and are power restricted. As a result, network infrastructure-related concerns should be effectively managed dynamically. For both connectivity and fault management, topology is an essential component of WSNs that requires attention. Two elements of topology topology control and topology management are the main topics of this chapter.

For effective operations inside a network contour, topology management entails the process of defining the inter-nodal linkages and virtual relationships to derive a simple graph of node connectivity. The goal of topology management is to maintain network connection while also saving energy on the nodes to increase the network's lifespan. A WSN's topology control is a gauge of its internode connection and network coverage. It could seem that topology management and control are similar.

The signals from the individual sensors of WSNs are often transported to the Internet or other terminals through a number of sink nodes, despite the fact that WSNs may have different topologies, such as star, ring, mesh, or tree. A sink node is a specific device that connects to regular sensor nodes but is more powerful than them, bridging a gap in the network end users and the sensor network. The sink nodes may be thought of as a laptop computer that receives data from the network or as a much more compact micro-controller that serves as the gateway. Each sensor node has the ability to gather data and route it back to the sink node and the end users, as shown in .The sink node is used to transport data back to the final user.

Depending on what the application requirements need, a sensor network may have several sink nodes operating at once. Two sink nodes X and Y may be shown in Figure showing the same level of interest in an event happening in sensor node B. When two sink nodes are deployed, as shown in, sensor node A is many hops from sink node X and just one hop from its closest sink node, Y. As a result, sensor node A will use fewer hops and less electricity to relay its signal to a sink node when using two sink nodes as opposed to one sink node. We are aware that the energy required to route a message from any sensor node to the closest sink node is inversely correlated with the number of hops the message must make. Utilizing numerous sink nodes efficiently lowers the energy use for each message sent. The route length from a sensor node to a sink node becomes shorter and the sensor node's lifespan gets longer as the number of sink nodes rises. However, due to the sink node's higher cost than the sensor node, the number of sink nodes is restricted financially. Additionally, there may be times when using numerous sink nodes is not physically feasible.

Performance of the network may be affected by the sink node's location. Through the use of experimental data, showed that sensor nodes that are one hop away from a sink node use energy more quickly than other nodes in the sensor network. This is due to the fact that nodes that are one hop away from a sink node must also transmit messages produced by many other nodes in addition to their own. These nodes' burden is much greater than that of nodes further away from the sink node. As a result, these sensor nodes exhaust their energy more rapidly and stop functioning. The sensor network ceases to function if there are too many dead or no operative sensor nodes around the sink node, preventing other surviving sensor nodes from connecting directly to the sink node.

Sink Node Positioning Challenges

Finding the best sink node placements in wireless sensor networks is not without its difficulties. These include the presence of a sizable, if not infinite, solution space, an excessive number of related parameters, varying routing algorithms, varying application requirements, the presence of a sizable number of sensor nodes, and varying sensor node capabilities.

- Vast, if not limitless, solution space: sink nodes are not catalogued and may be found everywhere in the environment. When there are no constraints, there are a lot of potential solutions.
- A significant number of sensors are involved: Sensor networks may include thousands of sensor nodes. The sink node location issue becomes NP-complete when there are many sensor nodes involved.
- Dynamic topological changes: The deployed sensor nodes may malfunction owing to manufacturing flaws or energy depletion, necessitating a change in the topology of the sensor network and the position of the sink node.
- Node capability variations: Not all sensor nodes are created equal, for example, some have variable transmitters while others do not. In this situation, reducing the communication distance in sensor networks made up of sensor nodes with fixed transmitters and different communication ranges results in improved energy usage, but no energy savings are possible if only sensor nodes with a fixed range transmitter are utilised.
- Differences in network architecture: There are two kinds of conventional sensor networks: flat and hierarchical. In contrast to hierarchical sensor networks, which disseminate data to the sink node via cluster-heads, flat sensor networks distribute data in several hops through network intermediate nodes.
- Variations in routing algorithms: Different routing algorithms use various strategies to maximise data transmission tasks in sensor networks. When transferring data to the sink

node, every routing algorithm provides a different data delivery structure. Different energy models are the result of these variations.

- Differences in sampling modes: Periodical data sampling is required for wireless sensor networks, or they may function in an event-driven manner. The ideal sink node location issues become more challenging due to the need to accommodate both sampling modes. Choosing to optimise for a certain data sampling method, however, may require various considerations.

Sink Node Positioning Methods Categories

The majority of sink node placement research has concentrated on carefully choosing the sink node location, which may impact a variety of performance measures including energy consumption, latency, and throughput. They focus on structural quality indicators such network connection and distance, and/or they base their research on a predetermined topology. We categorise them as static techniques as a result. The optimality of the initial position for the sink node may become vacant throughout the operation of the network, due to changes in the state of the network or numerous external circumstances. However, dynamically altering the sink node placement may further boost the dependability of WSNs. For instance, it makes sense to put the sink node near to where targets are found and where there is a lot of traffic in a target monitoring application. We refer to these techniques as dynamic approaches.

Throughout the functioning of the network's existence, its position stays constant. The location of a single or many sink nodes in WSN, as well as optimization during network setup, have both been the subject of much study. The assumptions used, the network model taken into consideration, the information on the network state that is accessible, and the metrics that should be optimised may all be used to categorise the published studies.

The main goal of static sink node location is to increase network longevity. The location of the sink node was experimented with in various ways. Either the network lifespan specification, the network operation mode, or the network state parameters that are part of the optimization aim are to blame for the discrepancy. Although some users define the network lifespan as the period of time until the first sensor node fails, many others define it as the failure rate of a portion of installed sensors. Other research attempts to maximise network longevity by lowering the overall power used to get data from all sensors.

Additionally distinguishing aspects are the system model taken into account and the network architecture. The sensors in a flat network architecture are uniform in their starting energy and often construct several paths to transmit their data to the sink node. Sensor nodes are arranged into clusters with a defined cluster leader in a hierarchical structure. The inter-cluster head network becomes the primary focus of the sink node location challenge in this scenario.

The performance of the whole network is heavily influenced by the communication topology. Many scholars have studied topology management using power control to achieve improved resource efficiency by lowering the sophistication of the routing protocols. These protocols' primary method of energy saving is the use of low processing power levels. This characteristic makes their suitability for use in sensor networks just as appealing as that of other wireless ad hoc network types. However, the majority of earlier methods did not take into account different wireless sensor network data flow patterns (WSNs). To accommodate various data traffic patterns, we provide a topology management system that dynamically modifies distribution power levels. The simulation findings demonstrate that the resulting wholeheartedly tree-like topologies provide an effective trade-off seen between complexity of the network architecture and the resources that are available.

Dynamic Sink Node Positioning Static sink node positioning does not consider dynamic changes during the network operation and therefore does not move the sink nodes once they are deployed in their original locations. Examples of dynamic changes are: traffic patterns which can change based on the monitored events; load many not be balanced among the nodes, causing bottlenecks; application-level interest can vary over time; and the available network resources may change due to the depletion of energy in some nodes. Dynamically repositioning the sink nodes while the network is operational can further improve the performance of the network. For example, in a target tracking application, it may be wise for the sink node to keep a certain distance from a harmful target. A safe distance should be maintained. In a disaster management application, sensors can detect fires, collapsing buildings, gas leaks, and so on. Moving too close to these reported events in such scenarios would be risky.

Another example is that when many sensor nodes in the vicinity of the sink node become dysfunctional due to the exhaustion of their batteries. It is better for the sink node to reposition itself to become easily and reliably reachable by data sources suggested that the sink node should be repositioned adaptively in an even-driven sensor network based when the events happen. proposed a three-step approach: when would it make sense for the sink node to relocate to, where should it go, and how will the data be routed while the sink node is moving, presented three sample heuristics for dynamic relocation of the sink node that can improve the network performance in terms of energy consumption, data delivery delay and safety of the sink node. They are repositioning for increased network longevity, enhancing timeliness of delay-constrained traffic, and protecting the sink node. 6.3.3 Mobile Sink Node Positioning Dynamic sink node positioning considers that a sink node can move on-demand or otherwise would stay stationary.

A sink node might be designed as a mobile device, which is able to move constantly within a sensor field rather than on-demand. A mobile sink node can be used to collect data from a sparsely populated sensor network by moving itself closer to those sensor nodes where data originated. The movement of sink 6.3 Categories of Sink Node Positioning Approaches 133 nodes can be random, or pre-defined. Randomly moving around within a sensor field is not suitable for time-sensitive applications but can work well for large-scale applications such as forest fire monitoring, provided the sink node is equipped with a flight capability. Predictable sink node mobility attempts to achieve optimum energy utilization by positioning a sink node at a pre-specified position at a specific time used a mobile sink node that moves along a pre-defined path, and pulls data from the sensors when it arrives close to them, as shown.

Such a predictable mobility approach enables the collection of data to be done in a bounded transmission delay. The maximum power saving could be realised by invoking nodes only when they are scheduled to transfer their data. 6.4 Optimizing Locations of Static Multiple Sink Nodes System Assumption Here we restrict the WSN to a mesh topology. For the sake of simplicity the following assumptions about the WSNs are made in establishing the system model:

1. All sensor nodes are stationary and located in a bi-dimensional square grid composed of cells of the same size;
2. Multiple sink nodes are fixed on the grid;
3. Data transmission and reception are the major energy consuming activities;
4. All sensor nodes have equal initial energy; the transmission range of each sensor node is fixed and equals to the distance between two adjacent nodes in the grid, i.e. a hop is of one grid cell side length.
5. Sensor nodes communicate with the sink nodes by sending data via multiple hops along the shortest path; Area covered by the Sensor Network Mobile Sink Node Sensor Node.

Optimization of Sink Node Positioning the number of sink nodes is fixed and known in advance;

1. Sink nodes can be located only at certain places in the grid, called feasible sites.
2. The energy consumed in a senor node when transmitting a bit is constant, and is the same as the energy consumed for receiving one bit.

Formally, a sensor network is represented as a graph G(V, E), where V are the vertices representing sensor nodes and E edges representing one-hop connectivity between two adjacent nodes (i, j). Considering the mesh topology in the sensor network, a sensor node i can communicate directly with its four adjacent nodes (left, right, upper and lower). If the sensor node is not linked with the sink node through one-hop connectivity, then data packages generated at this sensor node have to be relayed through multiple hops in order to reach the sink node. The notations and the mathematical formulation of power consumption at each sensor node here is adopted from work, and extend into a multiple static sink node case.

1. e: Energy consumption coefficient for transmitting or receiving one bit (Joules/bit);
2. e0: Initial energy (Joules) of each node minus the threshold energy required for node operation;
3. r: Rate at which data packets are generated (bits/s); for the homogeneous sensor nodes r is the same for all sensor nodes;
4. Ck i : Power consumption for receiving and transmitting packets at node I when the sink node is located at node k (Joules/s).
5. z: Network lifetime (seconds).

6. zij: Lifetime of Node i assigned to sink node kj (seconds). Simplified Routing Protocol in the WSN with the mesh topology a simplified routing protocol is considered.
7. When a sensor node lies on the same horizontal or vertical line of the sink node, a unique shortest path between the sensor node and the sink node is taken.

Otherwise, the two paths along the perimeter of the rectangle with the sensor node and the sink node as the opposite corners will be taken in equal proportions. Two hops in a unique route are required for transmitting a data package from node i to the sink node. Four hops in two symmetric routes are required in. Energy Consumption Model Following notation, each node's position is represented using the ordered pair of the node's column and row numbers ðx; yÞ; x ¼ 0; 1; ...; L 1; y ¼ 0; 1; ...; L 1: L is the numbers of column and row in the grid. A pair of i Route Sink Node Sink Node Route i (a) (b) (c) Sink Node i Route Simplified routing protocol for a WSN with the mesh topology 136 6 Optimization of Sink Node Positioning horizontal and vertical dotted lines is drawn enclosing the nodes associated with the row and the column of the sink node.

These lines partition the sensor field into nine subsets as shown in .Upper Left (UL), Upper Right (UR), Lower Left (LL), Lower Right (LR), Vertical Above (VA), Vertical Below (VB), Horizontal Left (HL), Horizontal Right (HR), and the node K ð6:1Þ Using node i in subset UR as an example, Node i transmits its own generated data packets to node j2 and j4, successively. Nodes j2 and j4 relay these packets to sink node k. In addition, node i receives half of the packets generated at nodes j1 and j3, and half of the packets generated at nodes l1 and l2. Then, node i retransmits the packets originated at nodes j3 and l2 to node j2 and those originated at nodes j1 and l1 to node j4. In summary, node i receives data packets at a rate Optimizing Locations of Static Multiple Sink Nodes 137 If there are multiple sink nodes in the sensor field, the sensor field can be further partitioned.

The partition of the sensor field with two sink nodes k1 and k2. The subsets are denoted as UL1, UR1, LL1, LR1, VA1, VB1, HL1, HR1, and UL2, UR2, LL2, LR2, VA2, VB2, HL2, HR2. Depending on the locations of the two sink nodes some of the subsets will be overlapped. The formulas of calculating the energy consumption will still be suitable for the multiple sink node cases, if all the sensor nodes are assigned to their nearest sink nodes and there is no double assignment i.e. each node is assigned to one and only one sink node.

Optimal Locations of Multiple Sink Nodes Assume there are N sink field with two sink nodes 138 6 Optimization of Sink Node Positioning The lifetime of a sensor node i which is assigned to the nearest sink node is given as max e0 c kj i !; j ¼ 1; 2; ... ; N The lifetime of the sensor network can be defined as the time till the first sensor node in the sensor network runs out of battery capacity, i.e. min i max j e0 c kj i ( ). In order to maximize the lifetime of the sensor network the shortest lifetime of all the sensor nodes should be maximized by optimizing the locations of the multiple sink nodes. Therefore the objective of optimal locations of multiple sink nodes. The situation where sink nodes cannot be placed at any obstacle in the sensor field can be formulated into the above optimal problem with a constraint, where / is the set of the obstacles. Solving Optimal

Location Problems Many optimization approaches can be used to solve the optimal location problems represented in Eqs. Because of the nature of multi-variables in the above optimization, most of the evolutionary computation algorithms can be applied to solve the location problems

A chromosome representation of the problem which is amenable symbolic manipulation;

- A fitness function defined in terms of this representation;
- A set of manipulation operators such as crossover, mutation, and reproduction.

The variables to be optimized in the objective function shown in Optimizing Locations of Static Multiple Sink Nodes 139. The fitness function in the GA is chosen from the objective function shown in for all possible combinations of N sink nodes. The three operators of GA, crossover, mutation, and reproduction are applied to update the chromosome with satisfaction of the constraints represented. A simple simulation has been done in this study. Two sink nodes are designed for a 8 9 8 sensor network with three prohibited locations In the initial stage, these two sink nodes are selected randomly, so GA starts with several chromosomes that describe a number of random solutions to the optimal location problem. The parameters of GA are chosen, as the probability of mutation being 0.08, the probability of crossover 0.6, and the size of the population.

The values of the parameters of the 8 9 8 sensor network are chosen as r = 1 bit/s, e = 0.62 lJ/bit, e0 = 1.35 J. The search results illustrate that the upper left corner (0, 0) and the bottom right corner (7, 7) are the optimal locations for the two sink nodes. This result is consistent with the results in Wang et al. (2005) work for mobile sink nodes. We only consider the optimal problem of the multiple sink node locations with respect to a simplified routing algorithm. If any other routing algorithm is employed in the sensor network the system model is likely to be much more complex.

In particularly, we assume that all sensor nodes are stationary and located in a bi-dimensional square grid composed of the same size-cells and the transmission 140 6 Optimization of Sink Node Positioning range of each sensor node is fixed and equals to the distance between two adjacent nodes in the grid. These two assumptions make the system model the simplest, but are unlikely to be realistic. As the sensor nodes may be randomly distributed and they may have different communication ranges. We also assume that the number of the sink nodes is fixed and known in advance. If this assumption is untrue the number of the sink nodes has to be included as an additional optimal variable in the optimization. Nevertheless, the methodology introduced and the formulizations of the search problem are, in general, applicable to any complex sink node positioning problems

A network's topology, or physical configuration, influences how the network interacts with various devices. Network topology diagrams display both the logical and physical configuration of nodes and links in a network.IT managers should utilise network topology tools to establish each node's ideal configuration and to improve traffic flow. A well-planned network architecture helps a company to swiftly focus on problems, fix them, and ensure that the network is operating at the highest data transfer rate possible.

Topology of a network is important affects how a network operates. A good network architecture assures that perhaps the network will operate with enhanced data transmission rates and at maximum efficiency aids IT administrators in comprehending the structure of the overall network architecture. The IT operations staff can better view the network and comprehend the interdependencies of each device thanks to a network topology tool enables a dispersed network to be seen geographically. This guarantees that an IT administrator can efficiently map the company's international network explains the effects that devices and programmes have on other network users. Network topology information may be used to determine which device or application may be influencing other devices and generating a network bottleneck helps identify and fix system-wide problems. The correct network topology map makes it simpler to diagnose issues, solve issues, and allocate resources for the network.

Network Topology Types

There are two categories of network topologies: logical and physical. Physical topologies display the network's real physical wiring topology, demonstrating where and how each connection is made. The logical network route that data takes to go from one extremity to the other is shown by logical topologies. Bus, ring, star, and mesh topologies are a few of the most common network topologies. The most widely used topology system is called star topology. In this configuration, each node is connected to a hub, switch, or computer that serves as the hub of the network. Because star topology is centralised, it is user-friendly, dependable, and simple to maintain. Star topology, however, is expensive and needs ongoing maintenance.

Every workstation is linked in series toward the main central wire using the bus topology. It is perfect for small networks because of its straightforward linear architecture and low cost. However, bus topology is often sluggish for bigger networks, and in the case of a network breakdown, issue identification is difficult with this architecture.

Network devices are linked by cables in a ring topology, where the last network device is wired to the first. A continuous ring is created by each device connecting to precisely two other devices. Ring topology has a low likelihood of packet collision and is cost-effective. Ring topology, however, is reliant on a single wire, difficult to debug, and costly to maintain.

Mesh topology in mesh topology, nodes are connected with connections such that there are at least some pathways accessible between the network's points. All nodes in a "completely meshed" network mapping are linked to every other node, but in a "partially meshed" network, only certain nodes have numerous connections to other nodes. Multiple pathways are mated to increase network resilience. For dedicated connections, more space is required, which is expensive.

CHAPTER 8

PERFORMANCE EVALUATION OF WIRELESS SENSOR NETWORKS

Dr.Sudhir Kumar Sharma, Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University, Jaipur, India
Email Id- hodece_sadtm@jnujaipur.ac.in

The fast growth of wireless sensor networks in recent years has made this technology the focus of research in the embedded area as well as one of the foundational elements of industry 4.0 and the Internet of Things. Although there are many advantages to using wireless sensor networks, there are also many drawbacks. For example, since wireless sensor nodes are typically placed in harsh environments, they will continue to use energy even when idle, making it difficult to regulate the network's operational conditions. Therefore, in order to efficiently monitor and enhance the network's quality, it is required to assess the network's entire performance and condition. This will enable the user to quickly regulate the network's operational status [32]–[34].

Currently, objective assessment and subjective evaluation are used to compare the performance of wireless sensor networks. The authors of present a mathematical analytical approach for the study and assessment of the average queue length and processing times of the data streams in wireless sensor networks with multiple pathways and admission control methods. This method is intended to be objective. The wireless sensor network depending on 802.15.4 IEEE performed a preliminary evaluation of the quality management indicators, including the network speeds and the incoming signal strength, in literature, where the author created a realistic environment. According to, the author's assigned weights to three indicators based on their subjective judgment and monitored the number of nodes with residual energy, node survival, and latency during various time periods.

This allowed them to assess the performance of wireless sensor networks. In, the author presents many performance indices, defines an acceptable threshold value, classifies network performance assessment on humans, divides the four scales, and analyses the four performance rating indicators of packet loss rate, switching frequency, load balancing, and latency. In the chapter, the author uses AHP to resolve the issue of wireless sensor network gini index weight distribution, evaluate the storage overhead, communication overhead, connectivity, and other aspects. However, the method will be biassed because it heavily depends on experience and has a lot of subjective factors.

It is challenging to harmonise the numerous methodologies indicated above with the usage of the evaluation indicators because of their stark variances. In order to address this issue, a type of quantitative and qualitative weighting method which is based on the decision has been proposed. This method does not solely depend upon this subjective decision factors, but also takes into account the characteristics of the gathered information, uses the information entropy principle from information theory to explore the data's characteristics, and conducts a thorough performance analysis on the performance of WSNs. It has apparent application value and research relevance since the performance assessment of WSN may provide judgment call reference for node redeployment, route selection, and prospective node failure assessment.

By eliminating the limitation imposed by wires, the fast advancement of wireless technology has resulted in substantial advancements for numerous applications. Unfortunately, wireless interference severely limits the development of wireless devices since the air, the channel for communication, is exposed to possible wireless interferencers, and as a result, unlike wired systems, these systems lack any reliable interference-resistance. Wi-Fi, Bluetooth, ZigBee, microwave ovens, cordless phones, and other common wireless devices all operate in the 2.4 GHz ISM band. Due to the fact that these technologies were primarily created for consumer electronics, it is typical for people to utilise two or more of these devices at once. If many wireless devices are operating in the same frequency range, their performance may be impacted.

The IEEE 802.15.4 protocol, which serves as the industry benchmark for low-cost, low-data-rate wireless solutions, is often used in the development of wireless personal area networks, or WSNs. The capabilities required for the development of low-cost wireless communication allowing monitoring and control operations in the fields of residential, commercial, and industrial applications are provided by the IEEE 802.15.4 standard. There are numerous situations when many wireless systems are active at the same time in the same place due to the mobility and widespread deployment of WSNs. The likelihood of interference affecting the wireless connections formed between IEEE 802.15.4 WSNs might grow significantly. The modest broadcast power (usually 1 mW) and relatively small bandwidth (2 MHz for each channel) of 802.15.4 WSNs make its receivers susceptible to interference from more potent wireless systems. IEEE 802.11b WiFi systems and IEEE 802.15.4 WSNs are often used in conjunction in real-world circumstances and scenarios.

The elements that may interfere with the functioning of WSNs have been identified by new advances in theoretical analysis and certain basic wireless system experiments. Commonly utilised interference mitigation techniques include providing for dynamic frequency agility, implementing effective routing protocols, and maintaining physical and frequency separations between the victim systems and the interferers. This chapter examines wireless interference in the functioning of WSNs, including its definition, causes, and effective mitigation measures.

Wireless Coexistence and Interference in WSNs

The capacity of one system to complete a job in a certain shared environment while other systems may or may not be employing the same rules is referred to as coexistence.For instance, if a ZigBee-based home automation system is to be installed in a residential setting, ensuring that the ZigBee system and any existing WiFi system in the house can coexist would be a key deployment concern. The cohabitation of the WSN and other wireless systems will assure the WSN's excellent performance for a large-scale WSN deployed for forest fire detection, environment or traffic monitoring, etc.

When discussing interference in the context of wireless communications, one of the following two definitions is often used: Packet collisions at the receiver are caused by (1) many simultaneous packet transmissions.The receiver won't be able to abstract any relevant information if numerous wireless signals arrive to it at once since the intended signal and the competing signal will overlap.

Another obstacle to the functioning of wireless communication systems is the physical component of the radio propagation channel. When designing the radio system, several physical obstacles like multipath propagation should be taken into account.

When a signal is broadcast, it may take multiple alternative pathways to reach the receiver for example, by reflecting off of buildings, windows, or walls). This is known as multipath propagation.

A multipath propagation example is shown in radio signal from WSN interference with IEEE 802.11b systems may be reflected and take a "reflected route" to the receiver. A basic receiver just puts the multipath signals together since it cannot discriminate between them. As a result, there is interference between the "signal on direct route" and the "signal on reflected path".

The interference analysis in this chapter primarily discusses and evaluates the impact that other wireless systems, notably IEEE 802.11b WiFi networks, which prioritise simultaneous packet transmissions, have on IEEE 802.15.4 WSNs.

Performance Measures

WSNs, the Physical (PHY) layer and the Media access control (MAC) layer may be distinguished as the two components of the performance measure used to assess wireless communication. Typically, these measurements are used to gauge the intensity of interference.

Performance Measures for the PHY Layer

Signal-to-noise ratio (SNR), which measures the ratio of average signal power to average noise power in decibels, is a frequently used statistic in the PHY layer of a wireless system (dB). A modulated signal must be sent by a radio system at a certain frequency. Only by continuing to listen at the same frequency can the receiver side accomplish any successful reception. The receiver won't be able to receive the required signal if the SNR is below a certain threshold, meaning that the amount of noise is higher than the usable signal (Chandra et al. 2007).

The bit error rate (BER), which compares the number of wrongly received bits on the receiver side to the total number of bits sent during a transmission, is another crucial measure. Certain wireless systems have varied SNR and BER requirements for obtaining an acceptable level of performance due to the usage of various modulation techniques. The simulation results of BER at varied SNR for various wireless standards.

A low bit error rate may often be attained with a rise in SNR. The associated SNR should be higher than 3 dB, for instance, if the IEEE 802.15.4 system is needed to achieve a bit error rate of 1.0E-

09. In other words, the quantity of accurately recovered bits will decrease as noise levels increase. This often occurs when a potent IEEE 802.11b (i.e., Wi-Fi) signal interferes with an IEEE 802.15.4 signal.

Interference and Wireless Coexistence in WSNs

Measures of the MAC Layer Performance

Even though it's crucial for developers to comprehend how the PHY layer measures like SNR and BER perform when the system is subject to interference, it may be challenging to test these metrics without specialised equipment. The majority of evaluations employ more detailed exams. The Packet Error Rate (PER), for instance, is used to quantify how resilient a wireless system may be under certain settings. At the MAC layer, this kind of measurement may be used.

The channel access and sharing mechanism is governed by regulations at the MAC layer. Additionally, it is in charge of putting together and taking apart data packets that have travelled through the PHY layer. The system-level analysis of the impact of interference on WSNs should take into account the metrics of PER, transmission latency, and throughput (Shin et al. 2007).

Rate of packet errors: The ratio of packets that are not successfully received by the receiver to all of the packets created by the source node is the packet error rate, which measures the proportion of packets lost (Cuomo et al. 2007). An increase in the packet error rate is one of the effects of interference in WSNs. Additionally, it is the most significant measure that may be enhanced by the use of anti-interference design.

Throughput and Delay the quantity of data sent from one station to another within a certain length of time is known as the throughput (Shin et al. 2007). The results of the BER through SNR simulation for IEEE 802.11b and IEEE 802.15 asterisk (IEEE Std 802.15.4 2003). 146 7 WSN interference with IEEE 802.11b systems would inevitably result in a growth in transmission delay and a decrease in throughput, which might be reduced by a successful anti-interference design at the system level.

Over the last 15 years, research in wireless sensor networks (WSN) has become one of the most fascinating areas in computer science. According to reports, sensors built inside processors are getting close to particle size. Military surveillance, environment monitoring, structural monitoring, and freight tracking are a few uses for WSN. In research papers made by eminent individuals and institutes in computer science research, the development of the discipline may be observed. This study surveys a broad range of subjects from those publications and evaluates their assessment methods. Storage, navigation, real-time communication, power management, and architecture are among the subjects covered [35], [36].

The sections that follow cover these subjects. Each of the five portions of the debate will concentrate on a research article that describes an implementation relevant to the subject. A basic introduction to the subject is provided in each section. An overview of the assessment of the implementation as it is described in the study paper comes after the introduction. Experimental set-up and findings will be covered in two separate subsections. The criticism that follows examines the assessment methods using the four criteria of data, workloads, factors, and metrics.

CHAPTER 9

WIRELESS ENERGY HARVESTING

Chandra Shekhar Rajora, Assistant Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University, Jaipur, India
Email Id- chandra.shekhar@jnujaipur.ac.in

A method called Wireless Energy Harvesting (WEH) makes it possible to extract energy from radio frequency (RF) transmissions. Information and energy are concurrently carried by all RF signals. Most of the time, receivers just process the data that signals carry. Receivers can extract some energy from the RF waves using wireless energy harvesting technology. This energy is perfect for low-power sensor networks, IoT, RFID, and a variety of other applications since it may be utilised to power devices or recharge batteries.

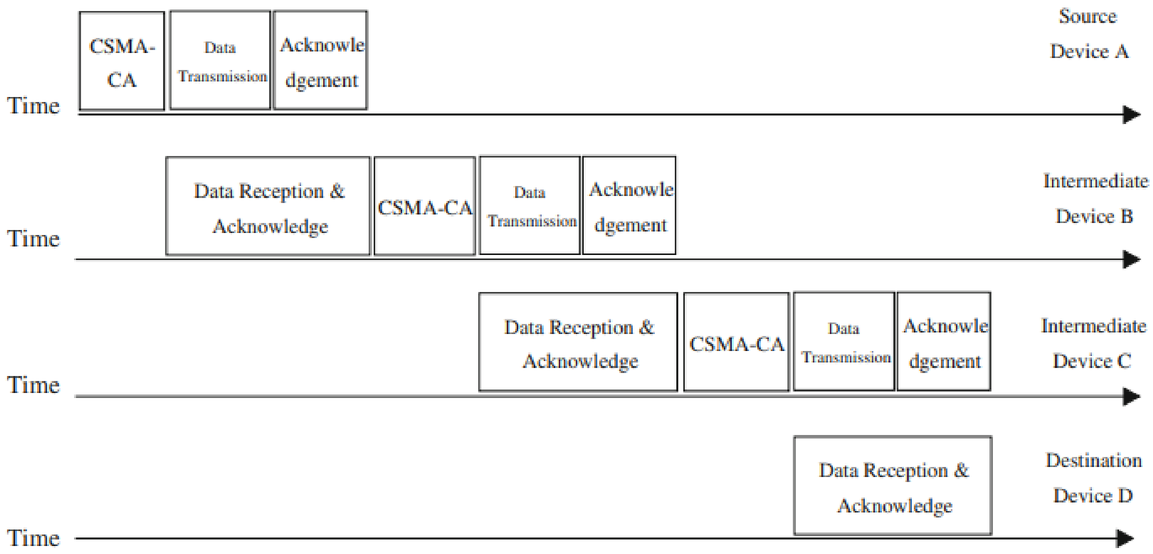
An antenna, a transceiver, a WEH unit, a power management unit (PMU), a sensor/processor unit, and maybe an onboard battery are the typical components of a WEH-enabled sensing device. The two most crucial energy harvesting equipment are the WEH unit and PMU. With the aid of an antenna, the WEH unit picks up the radio waves being sent and transforms them into a steady direct current (DC) energy supply that may be used to run a device or recharge a battery [37]–[39]. There is some power loss during the transmission of the received RF power to a useable DC supply between the matching circuit and the power converter's internal circuitry. The ratio of the produced useable DC output power to the input RF power is known as the converter's power conversion efficiency (PCE). A WEH unit may reach high PCE values, up to 70% or higher, by using cutting-edge RF-to-DC converters, commonly known as rectifiers. The PMU regulates how the gathered energy is stored. In order to optimize the lifespan of the gadget and maintain a high level of service, it also controls the allocation of the available energy among various customers.

Spread spectrum using direct sequence

The industrial, scientific, and medical (ISM) bands without a licence are essential to the Wi-Fi embedded technology is seeing rapid growth. a limited number of potential.Users include those who utilise IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n networks cordless phones, Bluetooth Pico-Nets, IEEE 802.15.4 networks, and homes

watching the WiMax networks, microwave ovens, and webcams.Therefore, any of these might potentially disrupt other systems. The direct sequence spread spectrum technique is adopted by the IEEE 802.15.4 standard (DSSS) to improve the chances for peaceful coexistence among various ISM band users. Spread spectrum modulation is a technology used in radio communications resilience and capacity of a system to coexist in the midst of interference.

Spread spectrum technology aims to disperse the transmission across a wide bandwidth.In the beginning, spread spectrum technology was used in military applications. It is employed due to a variety of appealing qualities, such as performance against jamming,communications with a minimal chance of interception and multiple access.Generally speaking, even despite narrow band's core frequencies signals (signals that encode and transport information by employing a narrow bandwidth) (signals that encode and transmit information by using a small bandwidth are not precisely the same, signal collision and data packets are nevertheless conceivable loss. Regulators like the limit and oversee the frequency distribution.



Federal Communications Commission of the USA. However, nothing is required is necessary in the ISM bands. Therefore, anybody might experience wireless interference a wireless network using narrowband signals.

Collisions between two narrowband transmissions are seen in the information conveyed by the information carried by the overlapping. Parts may get distorted as a result of interference. To prevent unwelcome meddling. The effective area of the overlapping regions between narrowband signals should be limited. This issue was addressed by the spread spectrum approach.

Indicating a narrowband interference signal, are the two narrowband signals shown by the solid line and narrowband intended signal (represented by the dotted line). The The "spread spectrum" strategy's goal is to employ more bandwidth to transmit the proposed narrowband signal initially contained bit information. After Only a tiny portion of the targeted initial narrowband signal is impacted by spreading.

WSN interference with IEEE 802.11b systems: 148 7 'signal' after it has been processed by the receiver filter, whose primary goal. Only responsive to signals on the designated frequency. although certain portions.

It is also possible that the receiver filter might allow the narrowband interference signal to pass extremely likely that the intended narrowband signal is successfully acquired, since only. The interference only affects a tiny percentage of the dispersed signal. In principle, if the spread signal is sent using additional bandwidth, interference may increase.

Tolerated. In spread spectrum, the processing gain G is a frequent metric when the terms "bit rate" and "chip rate" are used interchangeably. DSSS systems use before being sent, each bit is disassembled into a chip, which is a pattern of bits. Each bit is subjected to an XOR (Exclusive-OR) operation to create a chip. Using a fake random code. The chip bit, which is the result of the XOR operation, is then transferred and modulated the receiver employs the same pseudo-random code. Decipher the first information. Processing gains have the advantage that the pseudo-random the required narrowband signal is broadened out by code, making it less vulnerable.

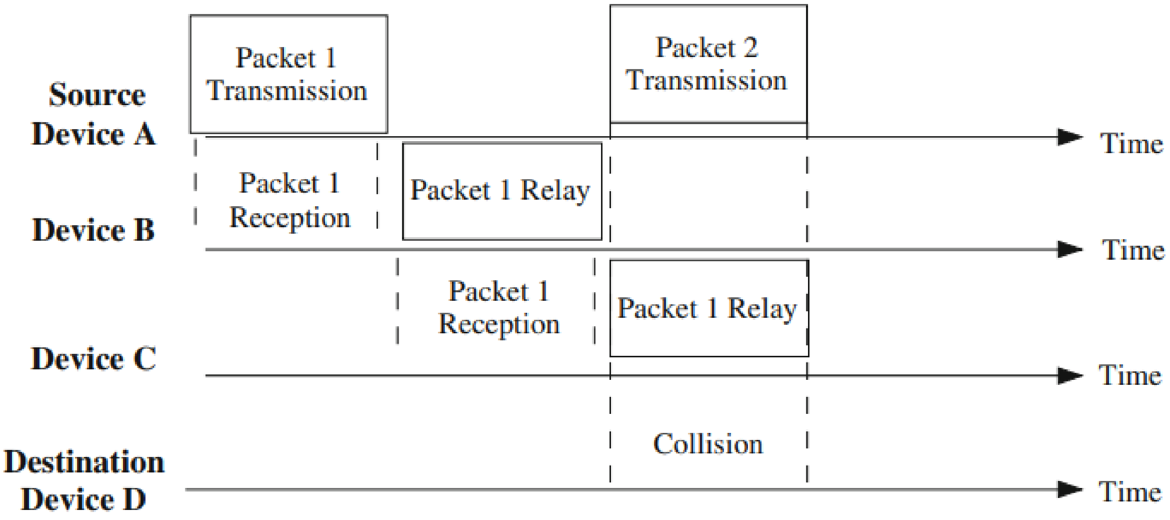
The used bandwidth to the narrowband interference signal. The ratio of signal to interference at the receiver may be thought of as the processing gain. After the dispensing operation. For instance, a wireless system calls for the normalised form of SNR is 10 dB Eb/N0, where Eb stands for energy per bit to provide an adequate performance, one must minimise the noise power spectral density (N0) having a respectable BER. The system can continue to operate if the process gain is 4 dB when the intended signal is 6 dB (10-4 dB) exceeds the necessary performance Interference. The chip rate of an IEEE 802.15.4 system operating in the 2.4 GHz band. Is 250 kb/s, and the chip rate is 2,000 kchip/s.

According to Eq, the IEEE 802.15.4 device is 9 dB. (7.1). Utilization of DSSS in IEEE Systems based on 802.15.4 add the ability to successfully coexist with a narrowband. Bluetooth is one example of a wireless communication technology whose bandwidth is less than IEEE 802.15.4 signal bandwidth. At the receiver, direct spread spectrum IEEE 802.15.4 Coexistence Mechanism 149. Although the IEEE 802.15.4 device improves the radio system architecture, when the interference power is smaller than the intended signal power, the capacity to tolerate the interference to a certain level is not feasible. Interference is overcome, especially when the unwanted signal is much stronger than the interfering signal.

Multiple Access with Frequency Division

In an IEEE 802.15.4 network, frequency division multiple access (FDMA) system creates 16 non-overlapping channels out of the 2.4 GHz ISM band and is .The channels are 5 MHz apart and are broad. Non-overlapping channel configuration enables several IEEE 802.15.4 users to operate independently on various frequencies without being concerned about overlapping. In light of this, if the intervening.

Currently, radio frequency is near the communication channel.The system may transition to a different channel whose centre frequency is.Any disruptive energy cannot interfere with frequency. A few further wireless systems use the radio frequency using the same or comparable processes. For the same FDMA approach is used, for instance, in the IEEE 802.11b/g technology to specify. The nto 79 channels with a 1 MHz bandwidth and makes use of



1. Wireless communication is accomplished via frequency hopping (FH). This system alternates between the designated channels continuously. The channels' or hops' order
2. The receiver has been informed in advance of the transmitter's predetermined and utilised sequence. A transmitter stays in each channel for no more than 400 ms and 1 W of maximum transmitter power are the recommended values. As a
3. Bluetooth devices may simply avoid the impact of interference as a result of FH by routinely changing channels.
4. Channel distribution of 2.4 GHz IEEE 802.15.4
5. Band 150 7 WSN-IEEE 802.11b System Interference
6. Carrier Sense Multiple Access with Collision, 7.4.3
7. Due to the likelihood that IEEE 802.15.4 devices may coexist with several wireless networks,
8. The Carrier Sense Multiple Access (CSMA) technique is used in the IEEE 802.15.4 MAC protocol using Collision Avoidance (CSMA-CA) to handle unforeseen situations
9. While the IEEE 802.15.4 devices are in use, interference or signal collision
10. Other network protocols have made extensive use of the CSMA-CA method.
11. Ethernet and Wi-Fi, for example. It uses a straightforward "listen before"
12. You speak" approach. A device listens on the wireless channel before starting a wireless transfer.
13. Puts channel assessment into practice the broadcast will start if the channel is open. The gadget will wait for a random interval if the channel is congested.
14. Reevaluating the channel. As channel assessment increases
15. In case of failure, the wait period lengthens exponentially to prevent interference.
16. The aforementioned techniques are all helpful in maintaining the coexistence.

The IEEE 802.15.4-based WSNs, however they achieve their effectiveness in various ways. The radio transmission's chance of being received is improved thanks to the DSSS technology. The IEEE 802.15.4 is provided by the FDMA after being correctly processed by the receiver. System with a higher likelihood of collaborating with other wireless systems by switching tithe signal on a separate radio frequency channel, and CSMA-CA tries to handle it before the radio signal really starts to spread, collisions. When WSNs are active be applied in real applications, the diverse circumstances brought on by various circumstances might emerge, necessitating more thought when creating interference prevention techniques.

According to the research currently available, interference only happens when two circumstances are satisfied: a minimal or zero radio frequency offset and strong interfering signal. Energy. The difference between the centre frequencies is referred to as frequency offset here comprises two connected channels of communication 7.5.1 Offset in Frequency. Devices compliant with IEEE 802.15.4 and IEEE 802.11b operate on the designated communication channels. The 2.4 GHz ISM band's constrained range makes it feasible to get the two wireless systems to operate at a similar frequency. A radio typically, transmission power congregates around the chosen frequency's central.

Channel, therefore if the frequency offset is large enough, it may easily result in interference. IEEE 802.11b and 802.15.4 operate in the 2.4 GHz ISM band. IEEE 802.11b contains fourteen. Channels with a 2.412 to 2.473 MHz central frequency range. Every channel 5 MHz apart from the neighbouring channels and 22 MHz broad. Due to multiple IEEE 802.11b communication channels overlap due to the high bandwidth one another. Enabling simultaneous operation of several IEEE 802.11b networks the frequency separation between any IEEE 802.11b communication channels must be at least 30 MHz when they coexist in the same space (So 2004). Consequently, If more than one IEEE 802.11b network is needed, the 802.11 specification advises. Three non-overlapping channels may be used to run near together. These three non-overlapping channels' parameters vary depending on the device. In China and North America, channels 1, 6, and 11 are suggested.

The source device is Device A. The target device, Device D, is awaiting data from Device A. Arrival Rate (AR) is the statistic used to gauge how well multi-hop transmissions work. The AR measures the proportion of data delivered from the source device that successfully reaches the target device. Device A must follow three standard procedures specified by the IEEE 802.15.4 standard in order for the transmission to be successful.

1. Use the CSMA-CA protocol to determine if the channel is open for data transmission.
2. Send data to the next hop.
3. Watch for a response from the next hop.
4. The relaying process for devices B and C, which serve as intermediary devices along the path, has four stages.
5. Receive data transmitted from the route's preceding node and, if necessary, send back an acknowledgment.

6. Use the CSMA-CA protocol to determine if the channel is open for data transmission.
7. Send data to the next hop.
8. Watch for a response from the next hop.

The data sent from device C must be received by device D, the target device of the multi-hop transfer, and acknowledged if necessary. A description of multi-hop transmission based on the same time line. On the same timeframe, compares the activities done by each device engaged in a multi-hop transmission. The source node, device A, may theoretically initiate a fresh data transmission for the subsequent data packet once the data have been successfully transmitted from device B to device C. However, if the transmissions are poorly timed or the transmission interval is too short, packet collisions will occur. If numerous radio transceivers are present in the same region, wireless communication is severely restricted such that only one transceiver may transmit radio signals at a time.

Multi-hop transmission simplified model 162 7 WSN interference with IEEE 802.11b systems during wireless communications is categorised as "hidden node" and "exposed node" concerns .To guarantee dependable connection, the wireless devices are placed near to one another. Additionally, routing protocols often examine a number of variables while choosing a route, such as signal strength, device response time delay, and distance between the candidate and the destination device. As a result, it is feasible that the intermediate devices chosen for a route are in close proximity to one another. For the condensed model we assume that the communication distance between devices A and C is one hop. By using the same procedure, it is feasible that both of these two packet transmissions will collide if device A begins to transmit the second packet while the first packet is being transported from device C to the destination device D.

Welcomeis that channel conflict will result from the actions "Packet 1 Relay," commencing from device B to device C, and "Packet 2 Transmission." One of them should then postpone channel access and wait for a chance delay before attempting again. The succeeding packet transfer might result in an even longer delay if the source device A's control of the transmission interval is improper (for example, if the interval is too short). The IEEE 802.15.4 standard's default retransmission method, which was designed for the case when an anticipated acknowledgment was not received after data transfer, is less successful in this situation. In multi-hop transmission, channel congestion and collision grow more complex and unpredictable as there are more intermediary devices involved. The design of the transmission protocol must take the unpredictability of multi-hop transmission into account.

The source device should set the time interval between each packet transmission to a minimal level, which should be equivalent to the amount of time needed for a packet to travel from the source device to the destination device, in order to assure the success of multi-hop transmission. There won't be much of a risk for a collision or channel congestion if a subsequent data transmission only begins after the prior data has been received on the target device. Here is how the minimum interval is described specifies the length of time needed to transmit an L-byte packet across a single hop from one device to another device. L is the packet's size. The number of hops in a multi-hop transmission is known as NHops. The MAC layer, in collaboration with the corresponding higher layers such as the network layer and the application layer, may be used to define the minimum time gap between each transmission of two consecutive source packets.

Interference Reduction in Multi-hop Transmission

If interference occurs, setting up 802.15.4 networks with a mesh architecture will provide you the most flexibility. If an existing route becomes unavailable, the routing protocol may be used as an alternative to retrying a multi-hop data transfer. It may be useful to switch to a different clear channel when the majority of wireless nodes are experiencing interference under certain circumstances. However, if the 802.15.4 network's coverage expands, channel switching implementation issues would worsen since it would be expensive to maintain the whole network synced show how interference may be reduced by finding a different path that avoids the interference region. Every node will keep a list of its close neighbours to make the task easier. Every neighbour has a corresponding interference bit that specifies whether or not that node is thought to be experiencing interference. Every node meticulously records the 164 missing acknowledgement packets for every neighbour. Interference of WSNs with IEEE 802.11b Systems The neighbour is deemed to be within the interference region and the associated interference bit is set to one if the number of lost ACKs exceeds a certain threshold. The nodes that are thought to be in the interference region won't take part in the phase of finding a new route.

Sending a message back to the source node to let it know about the connection break is still beneficial for the intermediate node. As a result, the source node will enter the phase of new route discovery following interference detection. After waiting for a certain period of time, it will cease transmitting any further data packets. Depending on the size of the network, this time might be extended or shortened. It will only send an RERR message back to the source node if the intermediate node is unable to locate a new route to the destination, allowing the source node to restart the route discovery process from scratch. The source node will begin delivering data packets to the previous next hop if an RERR message is not received because it will presume that a new route to the destination is open. When many interference zones are found, the aforementioned concept may also be used.

Wireless energy sources in the context of the Internet of Things (IoT), wireless sensor networks (WSNs), radio-frequency identification (RFID) tags, etc. may be divided into two categories: dedicated and ambient sources. The WEH unit is often tailored to collect energy from dedicated RF sources, which are installed to provide a reliable energy supply to the device. The WEH sensor cannot be adjusted to gather energy from particular sources since ambient sources are communicators that may emit consistent power over time regularly or arbitrarily. An intelligent WEH system that continuously scans the channel for potential harvesting opportunities is necessary to collect energy from various sources. Harvesting wireless energy in many frequency bands complicates the requirements for antenna architecture and necessitates a complex power converter because different ambient sources communicate at various frequency bands. WEH systems are often set up to exclusively utilise ambient energy harvesting as a backup supply.

The goal of IoT's intelligent architecture is to connect as many devices as possible to a network and allow them to communicate wirelessly. IoT transceivers must be built into a number of tiny devices in order for this to be practicable, which adds the additional difficulty of installing a power supply for numerous transceivers inside the same device. Therefore, considering low consumption of electricity is crucial while developing IoT devices. These gadgets can now be powered by smaller batteries thanks to WEH, and they can recharge their batteries by using the RF energy they receive. By providing appropriate power for a considerable durations, this greatly lengthens the recharging cycle of these gadgets. The usefulness of these devices may be increased by using WEH technology to combine additional sensors in a single package.

Contradiction Detection. The data flow is continuously monitored by each IEEE 802.15.4 node in the mesh network, and interference is detected using the default energy detection, or clear channel assessment, function. The node will start a group creation operation to create a temporary group in a clean channel after a rapid drop in throughput is identified and the energy detector returns a high level result.

In order for a group to form, the node that initiates the process must tell its nearby neighbours of the channel it intends to switch to. The neighbour node will switch to acting as a border node upon receiving this message, creating a link between the original mesh network and the nodes within the interference region. The border node will respond to the node from whom it got the group creation message on the new channel. The reply message verifies that the border node is informed of the change in circumstances. The border node then returns to the earlier channel. Immediately switching to the channel used by the temporary group, the border node delivers any new data intended for the nodes that have joined the temporary group to the targeted node. The border node returns to the original channel and keeps listening there when the data transfer is finished. The nodes in the temporary group continue to occasionally check the prior channel. They will notify all close neighbours, notably the border nodes, to break down their structures if it is judged that the channel is clear. When the interference has totally subsided, the whole group will be destroyed. Device A must follow three standard procedures specified by the IEEE 802.15.4 standard in order for the transmission to be successful.

9. Use the CSMA-CA protocol to determine if the channel is open for data transmission.
    1. Send data to the next hop.
    2. Watch for a response from the next hop.
    3. The relaying process for devices B and C, which serve as intermediary devices along the path, has four stages.
    4. Receive data transmitted from the route's preceding node and, if necessary, send back an acknowledgment.
    5. Use the CSMA-CA protocol to determine if the channel is open for data transmission.

6. Send data to the next hop.
7. Watch for a response from the next hop.

The data sent from device C must be received by device D, the target device of the multi-hop transfer, and acknowledged if necessary shows a description of multi-hop transmission based on the same time line. On the same timeframe, compares the activities done by each device engaged in a multi-hop transmission. The source node, device A, may theoretically initiate a fresh data transmission for the subsequent data packet once the data have been successfully transmitted from device B to device C. However, if the transmissions are poorly timed or the transmission interval is too short, packet collisions will occur. If numerous radio transceivers are present in the same region, wireless communication is severely restricted such that only one transceiver may transmit radio signals at a time (Golmie 2006). It is well acknowledged that the A C D

Multi-hop transmission simplified model 162 7 WSN interference with IEEE 802.11b systems during wireless communications is categorised as "hidden node" and "exposed node" concerns To guarantee dependable connection, the wireless devices are placed near to one another. Additionally, routing protocols often examine a number of variables while choosing a route, such as signal strength, device response time delay, and distance between the candidate and the destination device. As a result, it is feasible that the intermediate devices chosen for a route are in close proximity to one another. For the condensed model, we assume that the communication distance between devices A and C is one hop. By using the same procedure, it is feasible that both of these two packet transmissions will collide if device A begins to transmit the second packet while the first packet is being transported from device C to the destination device D. Device A transmits packet 1 from source device B to destination device D and acknowledging data

Device A as the source, Device B as the intermediary, Device C as the final device. Another scenario is that channel conflict will result from the actions "Packet 1 Relay," commencing from device B to device C, and "Packet 2 Transmission." One of them should then postpone channel access and wait for a chance delay before attempting again. The succeeding packet transfer might result in an even longer delay if the source device A's control of the transmission interval is improper (for example, if the interval is too short). The IEEE 802.15.4 standard's default retransmission method, which was designed for the case when an anticipated acknowledgment was not received after data transfer, is less successful in this situation. In multi-hop transmission, channel congestion and collision grow more complex and unpredictable as there are more intermediary devices involved. The design of the transmission protocol must take the unpredictability of multi-hop transmission into account.

The source device should set the time interval between each packet transmission to a minimal level, which should be equivalent to the amount of time needed for a packet to travel from the source device to the destination device, in order to assure the success of multi-hop transmission. There won't be much of a risk for a collision or channel congestion if a subsequent data transmission only begins after the prior data has been received on the target device. Here is how the minimum interval is described:

Specifies the length of time needed to transmit an L-byte packet across a single hop from one device to another device. L is the packet's size. The number of hops in a multi-hop transmission is known as NHops. The MAC layer, in collaboration with the corresponding higher layers (such as the network layer and the application layer), may be used to define the minimum time gap between each transmission of two consecutive source packets.

Interference Reduction in Multi-hop Transmission

If interference occurs, setting up 802.15.4 networks with a mesh architecture will provide you the most flexibility. If an existing route becomes unavailable, the routing protocol may be used as an alternative to retrying a multi-hop data transfer. It may be useful to switch to a different clear channel when the majority of wireless nodes are experiencing interference under certain circumstances. However, if the 802.15.4 network's coverage expands, channel switching implementation issues would worsen since it would be expensive to maintain the whole network synced show how interference may be reduced by finding a different path that avoids the interference region every node will keep a list of its close neighbours to make the task easier.

Every neighbour has a corresponding interference bit that specifies whether or not that node is thought to be experiencing interference. Every node meticulously records the 164 missing acknowledgement packets for every neighbour. Interference of WSNs with IEEE 802.11b Systems The neighbour is deemed to be within the interference region and the associated interference bit is set to one if the number of lost ACKs exceeds a certain threshold. The nodes that are thought to be in the interference region won't take part in the phase of finding a new route. Sending a message back to the source node to let it know about the connection break is still beneficial for the intermediate node. As a result, the source node will enter the phase of new route discovery following interference detection.

After waiting for a certain period of time, it will cease transmitting any further data packets. Depending on the size of the network, this time might be extended or shortened. It will only send an RERR message back to the source node if the intermediate node is unable to locate a new route to the destination, allowing the source node to restart the route discovery process from scratch. The source node will begin delivering data packets to the previous next hop if an RERR message is not received because it will presume that a new route to the destination is open. When many interference zones are found, the aforementioned concept may also be used.

Although still in its infancy, wireless energy harvesting technology is anticipated to have a broad variety of future applications in wireless networks, Machine-to-Machine (M2M) communications, RFID devices, and other areas. Wireless networks and devices are using much more energy as a result of the wireless communication sector's tremendous expansion. On the other hand, it is either impossible or prohibitively costly to replace batteries for low--cost devices in energy-- limited networks such as wireless sensor networks. Energy harvesting looks to be a developing option that has drawn significant attention to address these problems, since it fuels mobile devices by scavenging energy from the natural atmosphere (solar, wind, vibration, thermoelectric effects, ambient radio power, etc.). A possible strategy to further enhance the energy-efficiency of wireless networks for communications is the usage of energy collecting nodes. The effective design of data transmission, however, is also faced with additional difficulties as a result of the many theoretical and practical unresolved issues that are involved.

CHAPTER 10

SECURITY ISSUE IN WIRELESS SENSOR NETWORK

Anil Agarwal, Associate Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University,
Jaipur, India
Email Id- anil.agarwal@jnujaipur.ac.in

It could be extremely difficult to secure wireless sensor networks since they must be protected against harm, loss, assaults, and risks. A wireless cluster head furthermore has constrained bandwidth, “processing, and I/O capabilities”. Upholding confidentiality and preventing penetration are the traditional security concerns that are often taken into account in wireless sensor networks. Compared to fixed/wired networks, passed by congress to wireless networks may be challenging since they employ wireless as their primary communication method. WSN access control is more difficult to secure than it is for conventional wireless networks. This is mostly caused by the WSNs' constrained resources and, in most instances, their hostile operating environs.

In order to gather data from nearby points of interest, analyse it, and then send it to the sink, "wireless sensor networks (WSNs) are" made up of a lot of low-cost, small sensors nodes that are dispersed, self-organizing, unattended, and low processor speed contained . Industries for commercial and military usage of WSNs include traffic monitoring, inventory management, and tactical observation. In order to stop terrorism and the illicit trafficking of weapons and narcotics, they also offer border security. These networking provide sociopolitical advantages, such as weather forecasting, mission-critical capabilities, based on the identified mapping, vertical farming, and clinical services; they also offer a means of communicating in disaster-affected areas. Figure 13 discloses the attack in the wireless sensor network.

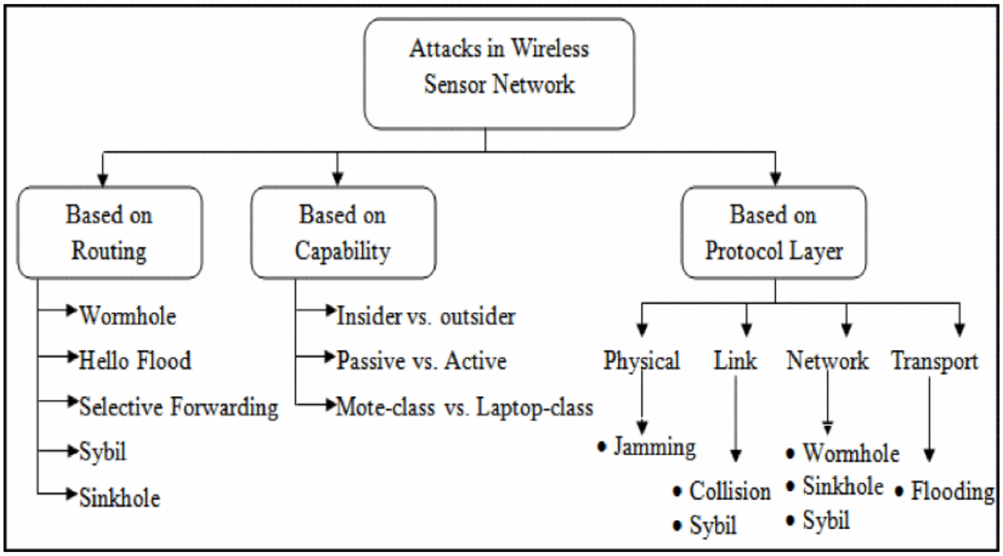


Figure 13: Discloses the attack in the wireless sensor network [42]**.**

Another of the main purposes of (WSNs) is to gather data about the outside environment. In contrast to infrastructure-based networks already in use, wireless networks may practically operate everywhere, particularly in locations where cable connections are not feasible. WSNs are frequently used gather, analyse, and distribute data on specific physical settings. A base station is subject to several limitations, particularly in terms of size and price, which should be maintained. These limitations lead to relatively tiny memory sizes, constrained energy sources, and a narrow channel capacity. Throughout the end, the sensor node is unable to perform encryption, decryption, or authenticating. The two words used in security the most often are onslaught and intruder. Attackers are those who attempt to manipulate information or have illegal access to a network's data. Attacks occur when an intruder uses the broadcaster's services.

WSNs include systems that gather data in the form of felt material from either the natural setting, such as weather, elevation, precipitation, level, movement, etc. The sink has access to this data through the gateway. Numerous monitors are used, and since they are wireless, they may readily function in any setting. Even when sensor nodes are scattered across the network, proper deployment is still necessary. A network may become inefficient due to increased incidence and interference when there are too many nodes deployed or when there are too few nodes deployed due to coverage concerns [40], [41], [43].

Infrastructure is applied to several indoor and outdoor settings. It's crucial to provide confidentiality while transferring data across a network. The far more difficult job in a WSN is security since it is difficult to constantly monitor the sensor nodes and internet. However, it must be protected in order to stop a hacker from assaulting the data flow.

Wormhole assaults

Several and more malicious nodes are present on the network at various points throughout this assault. Yet another blackhole tunnels communication towards another malicious node when a sender node provides it. The malicious node that received the information then communicates with its nearby neighbours. In this manner, the attackers deceives the sender and recipient nodes into believing that they are separated by only one or several hops while, in reality, there are several hops involved and, in most cases, both networks are out of range. Wormhole attacks and selectively forwarding are often combined [43]. It makes it harder to identify an attack if Sybil attack is used in conjunction with it.

CHAPTER 11

WIRELESS SENSORS AND CROWDSOURCING

Puneet Kalia, Associate Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University, Jaipur, India
Email id- puneet.kalia@jnujaipur.ac.in

Creative expression and capacities for detecting, gathering, processing, reporting crunching numbers from innumerable sources and surroundings have emerged as a result of the networking of more sophisticated and networked devices. Since the devices (nodes) in (WSNs) are typically assumed to be present in significant amounts and or the nodes are postulated to be as cost effective as feasible, the nodes in WSNs implicate severely restricted storage and compute resources, a lack of data integrity resistance to direct attacks, and minimal power sources. As a result, WSNs embody the greatest challenge among the different sorts of these so Internet of Things (IoT) implementations (usually batteries). Therefore, such devices often have to depend on stream cipher as their primary method (similar to inexpensive payment systems and other limited hardware)

Our research focuses on WSNs (or networks in principle) that use link keys and symmetry authentication. Due to resource constraints, this is the security option that WSNs use the most often. The connection keys formed between nearby WSN nodes serve as a fundamental building element for more complex network security applications as well as for secure communication. Link keys may be created in a variety of methods, such as by using a single master key for the whole network, deterministic pre-distribution, plaintext set an appropriate, or pairwise common belief. In our hypothetical situation, we suppose that each pair of neighbors has a link key that is shared by them both so that this key is applied to encode all communications sent back and forth between them.

No matter how link keys are created, attackers will always be able to discover them in some manner, spanning block ciphers techniques to physically capturing nodes and extracting the keys from them. The main goal of our study is to improve the total security of an interrelated group of nodes in the event that a non-trivial part of the linkage keys were penetrated (a compromised key is one that has been obtained by an attacker, independent of the moment of compromising). Through it too stealth amplification (SA) techniques, we deal with this problem.

As it is difficult, and sometimes even problematic, to determine such a compromising given the limited capacity of the nodes of the network or the manner of the assault, SA protocols do not depend on any information of whether a specific bridge has been attacked. New hardware infrastructures' cyber security should always be assured as they grow more crucial for the secure convenience of traveling on land, sea, and in the air. The technologically networks utilised by core vital infrastructures like air traffic control (ATC) or vessel traffic services have a lot of vulnerabilities, as shown in latest years both by academic sector and hacker communities. Number of factors make it difficult to quickly and effectively replace current solutions with safe ones; as a result, new protection strategies are needed. Figure 14 discloses the satellite positing and the broadcast system [41].

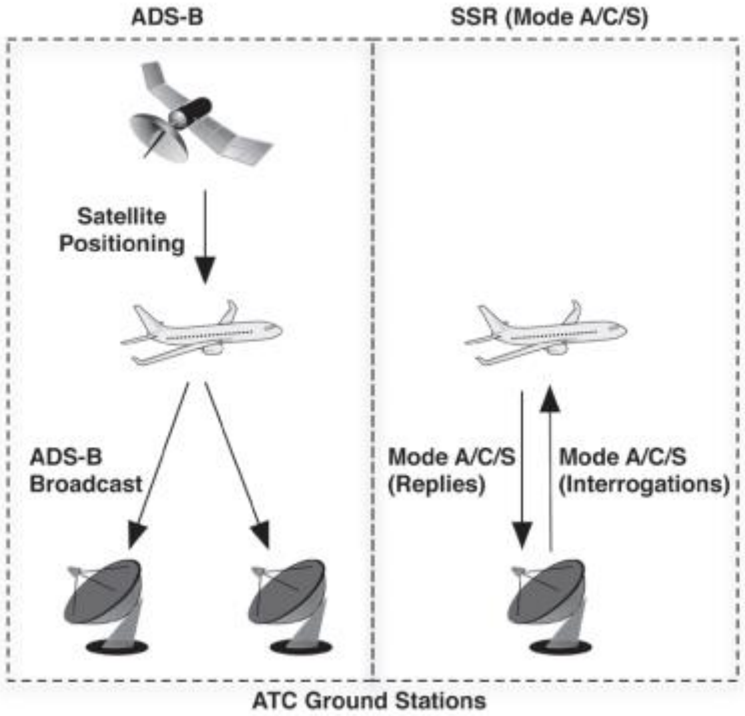


Figure 14: Discloses the satellite positing and the broadcast system [41]**.**

In this research, we suggest using crowdsourcing to secure key essential infrastructures instead of time-consuming and expensive technology implementation. We introduce the open-source monitoring system OpenSky and describe how it may be used to boost the security of ATC networks right away. In the past, the concept of crowdsourcing has been used to try to solve a variety of significant scientific issues, including protein structure and function and galaxy classifying. In recent times, a large number of commercial businesses have begun to monitor the positions of ships and aeroplanes all over the world using crowdsourcing platforms. Organizations and major industrial players are frequently requesting the systems' services as the apparatus for collecting data on them expands [42]–[45].

Traditional sensor nodes are being replaced with social monitoring. Sensors may be installed on commonly used items, like vehicles or cellular telephones, to capture crucial data in this method of crowdsourcing data collecting. The capacity to develop larger internet of things that are useful for gathering more comprehensive and complicated data is made possible by the growing advancement of information, such as the affordable sensors that are being incorporated into mobile phones. This paper's goal is to draw attention to issues in the sector and provide solutions. Instead than using social media to gather data, the usage of accelerometers is the main emphasis. Based on actual or hypothetical helps marketing technologies, research articles were examined. The flaws that have been discovered are compared to potential fixes in order to consider the field's future. When deploying a widespread network of sensors, we discovered that difficulties with privacy, noise, and trustworthiness existed. Additionally, we developed algorithms for assessing the veracity and integrity of collected data that may successfully address these issues.

CHAPTER 12

WIRELESS MULTIMEDIA SENSOR NETWORKS

Dr.Sudhir Kumar Sharma, Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University, Jaipur, India
Email Id- hodece_sadtm@jnujaipur.ac.in

Throughout the networked scientific world and as an interdisciplinary area of study, Wireless Sensor Networks (WSNs) are attracting a lot of attention. Due to developments in "micro-electro-mechanical systems (MEMS)", low power and highly integrated digital circuits, and the growth of wireless communications, WSNs are becoming increasingly affordable, low-power, multi-functional, and feasible.

A great number of intelligence battery-powered sensor nodes with the ability to sense, analyse, and wirelessly communicate make up wireless sensor nodes (WSNs). The sensing circuitry converts basic environmental factors, such as air temp, humidity, or light, that are connected to the area around the sensor into an electronic circuit. Understanding such a signal shows certain characteristics of things present and/or events occurring close to the sensor. The sensor either transmits such gathered data known as scalar data directly or through a series of electromagnetic hops to a command centre (sink), often via radio transmitter. WSNs have a broad range of uses, including real-time item tracking, environmental monitoring, health structure monitoring, setting up a ubiquitous computer environment, etc.

The design of WSNs is subject to several limitations as a result of the aforementioned features, including those relating to fault patience, scalable, direct labor, network architecture, operational environment, hardware limitations, battery life, etc. These difficulties have prompted much study on the possibility for detector coordination in data collection and processing during the last several years. In the majority of applications, there is no energy or communication connectivity in the placement region [44], [46].

In order to function properly, sensor nodes must be able to subsist on a modest amount of energy, which is often provided by a battery. Depending on the use of the installed network, the network should remain live and operational for a period of time that might range from a few weeks to a few years. Notwithstanding, the emergence of so-called multi-media wireless sensor networks was made possible by the quick improvement and progress of sensors, MEMS, encapsulated programming, as well as the accessibility of low-cost (Complementary Metal Oxide Semiconductor) CMOS cameras and microphones. These developments were also aided by the significant advancement in distributed remote sensing and multimedia source coding techniques.

As a consequence, Wireless Multimedia Sensor Network (WMSN) is a community of continuously networked sensor nodes that can collect scalar sensor data as well as both audio and video streams as well as multimedia devices like mics and cameras. WMSNs hold great promise for a variety of potential uses in both service member and military contexts that call for visual and aural data, such as command and control sensor networks, crime control reports, systems for traffic control advanced health care transportation, algorithmic additional help to elderly mhealth, and process plant control. Multimedia support in these applications has the ability to increase the amount of data gathered, expand the area covered, and provide non - linear and non-views i.e., in comparison to the observations of scalar data [40], [43], [47].

Groups of geographically scattered sensors are used in wireless sensor networks (WSNs), a special usage of the Internet of Things, to keep track of environmental changes in a specific region. A WSN is created up of discrete nodes that may connect to help of sensors to gather information on environmental variations in temperature, noise, pollution levels, humidity, wind, and other factors. In order to cooperate promote the passage of sensor data via the network and to a central place where operators receive it, sensor nodes interact with other adjacent nodes in the network. Although bigger implementations where monitors are far spread may employ a non - linear and non-connectivity ring topology because data travels in numerous stages between sensor nodes eventually arriving at the main site, wireless sensor networks may be built using the typical "wheel-and-spoke" or "star" architecture. In the network, sensor nodes serve three basic purposes:

1. In order to get data from sensors
2. To send sensor data through a network to the central location
3. To transmit sensor information from additional sensor nodes throughout the network to the central site

A low-powered battery or other power source, a microcontroller, an electrical circuit connecting the microcontroller to the instruments and power source, and a radio transceiver to enable network communications make up each sensor node and help it achieve its fundamental goals.

CHAPTER 13

UNDERWATER SENSOR NETWORKS

Chandra Shekhar Rajora, Assistant Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University,
Jaipur, India
Email Id- chandra.shekhar@jnujaipur.ac.in

Wireless sensor networks (WSN) have a lot of promise for use in environmental as well as armed services investigations. The majority of the time, the base station (BS), intermediate networks, and wireless sensor nodes where the data is gathered, maintained, and analyzed need to be situated distant from each other. There are two strategies to deploy the nodes: one requires that the sensor nodes' positions and networking configurations be specified, while the other does not. Due to its flexibility in implementation, sensor network may be placed at random in hospitable locations or employed in disaster relief efforts. High power BS, or sinks, do not connect with sensor nodes. They solely use broadcasting to converse with their nearby peer. In response to topological changes brought on by performance degradation or connection to new nodes, sensor networks modify. This internet of things has a number of additional nodes linked to it as a result. Modules are seamlessly reconstituted using the improve public in the event of a node failure.

Every time a node detects data in a WSN, it sends the data to the next sensor node. Each node determines its closest neighbour in order to execute data transmission to a certain source nodes, which uses less energy than other methods of data transport. Following the discovery phase, also known as the nearest node finding transition stage, there is a network transmission procedure where information is sent between the closest sensor nodes. The third step involves forwarding or transferring this information to the server or BS. Third phase is carried out in a single-hop way, which implies that each sensor node communicates its perceived data straight to the next member nodes in a single-hop manner.

Significant improvements have been made in underwater network protocols, interfaces, and telecommunication since 2000, which has attracted a lot of interest to research on underwater wireless sensor networks (UWSN). The tiny detectors that are placed at various depths of water to detect activity that occurs in an underwater environment and have limited memory, bandwidth, and energy. Many clusters have the ability to gather information, analyse it, and then send it through acoustic signals to the surface sink.

Via enabling endpoints or terminals in a transmission line to cooperate through each new information delivery, cooperative communications enable such a well utilisation of communication resources. The diversity of proficiency and performance of the system may also be significantly advanced via cooperative communications. Additionally, it is built on transmitted nodes, which have emerged as a promising method for the quality characteristics known as spectrum and economic proficiency, internet backbone exposure, and to lessen the likelihood of outages.

Underwater cooperative communication can be divided into two categories: single and multihop, and the multihop communication method has proven to be the most effective at transmitting data between sources and destinations when the following factors are carefully considered: limited bandwidth, multipath fading, limited battery, biased information capability, and propagation delay. networks of wireless communication Underwater includes sensors and autonomous marine engineering that connect, organise, and divide data among one another to extract information and evaluate utility. The nuclear sub uses an underwater telephone network that functions similarly to an amplitude modulated wireless signal, except that instead of using radio waves during transmission and receiving, sound waves are disseminated and received instead. Underwater telephone networks use transducers and acoustic speaker, much as land-based communication methods.

The initial research issues are those that arise while using UWSNs in harsh situations where the fracture thickness is less than 100 mm. The working frequency of the sensor nodes should be in the Gigahertz or Terahertz range, with a millimetre magnitude. Second, a "radio signal of GHz frequency range and THz range will incidence" severe intermediate assimilation due to route loss and lack of transmission radius occurring in non-invasive transmission medium such as water and liquid materials. Thirdly, when UWSNs are deployed in areas with complicated settings, they often have significant energy challenges because the tiny sensors can only store a very little amount of power with extremely limited power delivery. Fourth, due to the ineffective renewable energy production techniques, a constellation collective communication network is required to increase the dependability of the quality of service. The aforementioned WUSN characteristics and the challenging problems they pose call for the development of new, power-efficient cyclotron resonance forms and techniques.

One of the enabling technologies for the creation of future ocean-observation systems and sensor networks is wireless information transmission over the water. Applications of underwater sensing include instrument monitoring, pollution management, climate recording, and prediction of natural disturbances, search and survey missions, and the study of marine life. They span from the oil sector to aquaculture.

In addition to supporting cabled networks, autonomous underwater vehicles (AUVs) will be controlled via underwater wireless sensing systems. To instal a vast fiber-optic network of sensors (cameras, wave sensors, and seismometers) spanning kilometres of ocean bottom, for instance, cabled ocean observatories are being created on undersea cables. Similar to how cellular base stations are linked to the phone network, these cables may enable communication access points, enabling users to roam about and interact from locations where wires cannot.

Cabled submersibles, commonly referred to as remotely controlled vehicles, are another example (ROVs). These potentially heavier than 10 metric tonne vehicles are linked to the mother ship via a cable that may span several kilometres and transmit high power and high-speed communication signals to the far end. The Alvin/Jason pair of vehicles, used by the Woods Hole Oceanographic Institution (WHOI) to find Titanic in 1985, is a well-known example of a ROV/AUV tandem. These kinds of machines also played a key role in the discovery of hydrothermal vents, which are hot water sources on the ocean floor that revealed living forms not before known. The first vents were discovered in the latter part of the 1970s, and more are continually being unearthed. Only space missions can compare to the significance of such discoveries, and the technology that makes them possible.

The notion of underwater sensor networks is now encouraged by the development of both the vehicle and sensor technologies. However, one must deal with the communication issue if one wants to make this concept a reality. Acoustic technology is still the mainstay of modern underwater communication systems. For short-range networks (usually 1–10 m), where their very large bandwidth (MHz or more) may be used, complementary communication methods have been suggested. These include optical, radio-frequency, and even electrostatic communication. These signals need either high-power or big antennas since they attenuate extremely quickly, within a few metres (radio) or tens of metres (optical). Longer ranges are offered by acoustic communications, but they are restricted by three things: a small and distance-dependent bandwidth, time-varying multi-path propagation, and a slow sound speed. Together, these limitations provide a communication channel with a high latency and low quality, combining the worst features of terrestrial mobile and satellite radio channels into a very challenging communication medium.

The submarine communication system, created in the USA around the close of World War II, was one of the earliest underwater acoustic systems. In the 8–11 kHz frequency, analogue modulation was used (single-sideband amplitude modulation). Since then, research has progressed, bringing digital modulation-detection methods to the forefront of contemporary acoustic communications. Several different kinds of acoustic modems are now marketed and can communicate at speeds of up to a few kilobits per second (kbps) at distances of up to a few kilometres. Significantly greater bit rates have been shown, however these findings are still in the experimental research stage.

The development of acoustic modem technology has prompted study into networks. The main difficulties have been outlined throughout the last ten years, once again emphasising the basic distinctions between acoustic and radio transmission. For instance, acoustic signals may have propagation delays of up to a few seconds across a few kilometres since they move at a rate of 1500 m s1. In contrast to radio-based networks, propagation delays are not insignificant at bit rates on the order of 1000 bps, which is a fundamentally different scenario. Acoustic modems can often only operate in half-duplex mode. These limitations suggest that acoustic-aware protocol design may provide higher efficiency than the straight implementation of protocols created for terrestrial networks (such as 802.11 or transmission control protocol (TCP)). Energy efficiency will also be crucial for anchored sensor networks since recharging batteries hundreds of metres below the sea's surface is challenging and costly. Last but not least, underwater equipment (including sensors, robotics, modems, and batteries) is neither inexpensive nor disposable. This phenomenon, which radically alters many well accepted network design paradigms, may be the most significant characteristic that at least for now separates underwater sensor networks from their terrestrial equivalent.

Although underwater sensor networks are not yet frequently in use, their development is near. Fleets of cooperative autonomous vehicles (where vehicles are able to respond to one another, rather than only to supervisory commands from a central authority that essentially amount to "switch from mission A to mission B") and long-term deployable bottom-mounted sensor networks are included in the underlying systems. The primary focus of our study is the ongoing research that supports this evolution. As a result of reexamining conventional presumptions and using cross-layer optimization across the whole protocol stack, from the application to the physical connection. We also talk about testbeds, modelling and simulation tools, and the hardware that is presently on the market.

Uses for underwater sensing

Underwater sensor networks are being developed in response to the necessity to feel the underwater environment. Applications may have a wide range of needs, including stationary or mobile, brief or long-lived, best-effort or life-or-death, which can lead to a variety of designs. Next, we go through various deployment types, application categories, and a few particular, both real-world and hypothetical, instances.

Deployments

Two factors that change across various deployments of underwater sensor networks are mobility and density. Although there has been substantial progress in cabled underwater observatories, from the military sound surveillance system networks in the 1950s to the most current Ocean Observatories Initiative, our emphasis is on wireless underwater networks in this article.A network of underwater sensors may be set up in a variety of ways. Individual nodes tethered to docks, moored buoys, or the seabed make up static underwater networks (as in the cabled or wireless seafloor sensors .Instead, temporary buoys that are placed by a ship, utilised, and then left in situ for hours or days might support semi-mobile underwater networks. (The moored sensors may be deployed for a brief period.)

These networks' topologies remain static over extended periods, which allows engineers to construct the topology in a way that encourages connection. However, due to small-scale movement (such as a buoy precession on its anchor) or ocean dynamics, network connection may still alter (as currents, surface waves or other effects change). Static deployments powered by batteries may have energy limitations. AUVs, low-power gliders, or unpowered drifters with sensors connected to them may be used to create mobile underwater networks. Mobility helps to increase sensor coverage while using less technology, but it presents problems with localisation and keeping a network linked. AUVs have enough of energy for communications, while gliders or drifters struggle with this issue.

Network density, coverage, and node count are interconnected criteria that define a deployment, much as with surface sensor networks. Compared to terrestrial sensor networks, underwater installations often have fewer nodes, a greater range, and a lower density. With a median of five neighbours per node, the 2000 Seaweb deployment, for instance, had 17 nodes dispersed across a 16 km2 region.

Domains for applications

Similar categories apply to the applications of underwater sensor networks as they do to terrestrial sensor networks. The environment is observed through scientific applications, which range from counting or photographing animal life to observing geological processes on the ocean bottom and water properties (temperature, salinity, oxygen levels, bacterial and other pollution content, dissolved matter, etc). (micro-organisms, fish or mammals). Industrial applications keep an eye on and manage commercial operations like commercial fisheries, undersea pipelines, or equipment used for extracting oil or minerals. Control and actuation parts are often used in industrial applications. Applications for the military and homeland security include demining, communication with submarines, and safeguarding or monitoring port facilities or ships at foreign ports.

Although the application classes are comparable, underwater activities often need a lot more resources than terrestrial sensors. Commodity weather stations may be purchased for between $100 and $1000 USD, however the cost of establishing a simple underwater sensing system today begins at the high end and rises due to packaging and deployment expenses. Increasing the amount of information returned is necessary to reduce the cost of acquiring data on-site, hence scientific practise today often involves sample collection and return for laboratory analysis. Several research initiatives (covered in 3f) are now investigating low-cost underwater solutions, although the fixed costs rapidly climb for detecting in deeper water. These efforts are inspired by low-cost terrestrial sensor networks.

Finally, compared to the days to months or years that are typical in terrestrial sensing, deployments for underwater sensing take place over shorter times (a few hours). The main causes are battery restrictions and deployment costs paired with a broad region of interest. When compared to surface sensing, underwater deployments might be more demanding because of biofouling, which calls for regular upkeep. AUVs that are powered or glider-based may be deployed with buoys or anchored structures.

Wireless communications lower deployment costs, interactive data show whether sensing is operational or prompt corrective actions during collection, and data analysis during collection allow attendant scientists to modify sensing in response to interesting observations. These factors are also driving factors for underwater sensor networks. Although there are many short-term or experimental deployments of underwater sensing or networking, we only discuss a select few illustrative cases here. An early example of a large transportable network with possible military uses is Seaweb. Its primary objective was to research technologies suited for undersea detection and communication. Long-term deployments were place in coastal water zones.

MIT and the Commonwealth Scientific and Industrial Research Organisation of Australia investigated the collecting of scientific data using both stationary nodes and mobile autonomous robotic vehicles. Deployments have only lasted a few days in Australia's and the South Pacific's coastal regions. Large-scale cabled underwater sensing is being investigated by the Ocean Observatories Initiative in contrast To enable long-term observations in this static, scientific application, cables must not only offer power but also communications.

Technology for underwater networking and communications

Several technological challenges pertaining to the conception, evaluation, application, and testing of underwater sensor networks are covered in this section. The difficulties of acoustic communication are discussed at the physical layer, followed by the communications and networking layers, applications, hardware platforms, testbeds, and simulation tools.

Physical layer

Since radio or optical means provide long-distance communication (from metres to hundreds of kilometres) with huge bandwidths (kHz to tens of MHz), even at low power, the electromagnetic spectrum predominates in communication outside of water. Acoustic waves are the favoured option for underwater communication beyond tens of metres since water absorbs and scatters practically all electro-magnetic frequencies.

There are various phases to the propagation of acoustic waves in the communication-relevant frequency range. The power loss a tone at frequency f undergoes when it moves from one place to another is known as fundamental attenuation. This fundamental loss, which happens across a transmission distance of d, is taken into account in the first (basic stage). The second stage gives a more precise estimate of the acoustic environment around a particular transmitter by accounting for the site-specific loss caused by surface-bottom reflections and refraction that happens when sound speed varies with depth. The third step handles the sluggish fluctuations in the propagation medium that seem to be random changes in the large-scale received power (averaged over some local period of time) (e.g. tides). These phenomena are important for figuring out how much transmission power is required to shut a particular connection. Addressing the small-scale, quick fluctuations of the instantaneous signal strength necessitates a separate modelling step.

The number calculated using the fundamental (ideal) propagation loss A(d,f) and a typical power spectral density N(f) of the background noise, which decays at 18 dB per decade is shown in to show the combined impact of attenuation and noise in acoustic communication. The signal-to-noise ratio (SNR) seen at a small range of frequencies close to f is described by this property. The picture strongly argues that there is an ideal frequency for a certain transmission range by demonstrating how fast high frequencies attenuate over long distances, forcing the majority of kilometer-range modems to operate below several tens of kHz. Additionally, it demonstrates that as the distance grows, the available bandwidth (and hence the useful data rate) decreases .This frequency and a certain bandwidth are assigned before designing a large-scale system can proceed.

Download PowerPoint Signal echoes produced by multi-path propagation arrive with different delays. Depending on where the system is located, delay spreading may last anywhere from a few milliseconds to many hundreds of milliseconds. This results in a frequency selective channel transfer function in a wideband system since various frequency components may have significantly varying attenuation. Small-scale, quick changes often appear in the channel response and the instantaneous power, which are generally brought on by scattering and the system's own rapid motion or that of the sea surface (waves). Small-scale changes have an impact on the design of adaptive signal processing algorithms at the receiver while large-scale variations have an impact on power management at the transmitter.

The Doppler effect, which is a result of directional motion, results in extra temporal variation. AUVs typically travel at speeds of just a few metres per second, while freely hanging platforms may drift with the currents at rates comparable to this. The relative transmitter/receiver velocity to the speed of sound ratio may be as high as 0.1 percent due to the sluggish sound propagation, an extreme figure that suggests the necessity for specialised synchronisation. In contrast, radio systems often just need to consider the centre frequency shifting in these systems and the related values are orders of magnitude less.

Early systems concentrated on frequency modulation (frequency-shift keying) and non-coherent (energy) detection in order to avoid the lengthy delay spread and time-varying phase distortion. Although these techniques do not effectively utilise the available bandwidth, they are preferred for reliable communication at low bit rates (typically of the order of 100 bps over a few kilometres) and are used in both research prototypes and commercial modems, such as the micro-modem created by the WHOI and the Telesonar series manufactured by Teledyne-Benthos.

After coherent detection was shown to be possible on acoustic channels, the development of amplitude or phase modulation-based bandwidth-efficient communication techniques (quadrature amplitude modulation, phase-shift keying) gained impetus in the 1990s. Early work on single-carrier wideband systems with adaptive equalisation and synchronisation led to real-time implementations that currently provide 'high-speed' communications at multiple kbps across various link topologies (horizontal, vertical), as well as with AUVs.

The physical layer is the subject of intense research Multi-carrier modulation/detection is being examined as an alternative while single-carrier modulation/detection is being enhanced utilising strong coding and turbo equalisation Bit rates of many tens of kbps have been experimentally shown for both sorts of systems when they are expanded to multi-input multi-output setups that provide spatial multiplexing (the capacity to deliver concurrent data streams from different transmitters).

Successful signal processing depends on respecting the physical elements of sound propagation, and effective network design depends on comprehension of its consequences. The available bandwidth diminishes with distance, as seen in, and this fact strongly supports multi-hopping, exactly as with radio-based networks on land. A lengthy connection may be broken up into many shorter trips in an acoustic environment, which not only allows for power saving but also for the utilisation of more bandwidth .As measured in seconds for a certain amount of bits per packet, a larger bandwidth results in a higher bit rate and shorter packets. Shorter packets also reduce the likelihood of collisions over lines with various, non-negligible delays, even if shorter bits imply less energy per bit. If the interference can be controlled, both facts have positive effects on network performance (and longevity).

The design of medium access and upper layer protocols is influenced by these properties of the physical layer. The same network protocol, for instance, might operate differently depending on the frequency allocation. Moving to a higher frequency region will result in more attenuation of the desired signal, but will also result in more attenuation of the interference, potentially improving overall performance. Since a channel that is seen to be free may nevertheless include interfering packets, propagation delay and packet duration are important. Their length will impact the likelihood of collisions and the effectiveness of re-transmission (throughput). Finally, we can significantly reduce interference by using power control in conjunction with intelligent routing.

Resource sharing and medium access control

Systems with many users need a reliable method for allocating communication resources among the participating nodes. The frequency spectrum is naturally shared in wireless networks, therefore interference has to be effectively handled. To separate the signals that coexist in a single channel and give guidelines to enable various stations to effectively share the resource, many approaches have been developed.

The unique properties of the acoustic channel must be taken into consideration when developing resource-sharing plans for underwater networks. Long delays, frequency-dependent attenuation, and the comparatively long range of acoustic signals are the factors that are most pertinent in this situation. Also important to take into account are the bandwidth limitations of the acoustic gear, particularly the transducer.

Signals may be deterministically divided into frequency or time (time division multiple access, or TDMA) (FDMA). In the first scenario, users alternate between accessing the media, preventing interference by preventing temporal overlap between signals. FDMA, on the other hand, achieves signal separation in the frequency domain; although they may overlap in time, the signals inhabit separate regions of the spectrum. These methods have also been taken into consideration for underwater networks and are widely employed in the majority of communications systems. For instance, FDMA was selected for the early deployment of SeaWeb due to the restrictions of the acoustic modem, despite the fact that the usage of guard bands for channel separation results in considerable inefficiency and that this sort of frequency channel allocation has very little flexibility (e.g. to accommodate varying transmission rates). Although TDMA may be more adaptable, it requires synchronisation between all users to ensure that they all access different time slots. Such an underlying time-division structure is the foundation of many systems and protocols, but it needs coordination and guard times to account for irregularities in handling propagation delays.

Code division multiple access (CDMA), which separates signals that overlap in both time and frequency using specially created codes in conjunction with signal processing methods, is another quasi-deterministic method for signal separation. Since the acoustic channel has a small bandwidth (20 kHz or less for standard gear), the cost in this situation is a bandwidth extension. Underwater networks have been suggested for CDMA-based medium access protocols with power control, which offer the benefits of not needing slot synchronization and being resilient to multi-path fading.

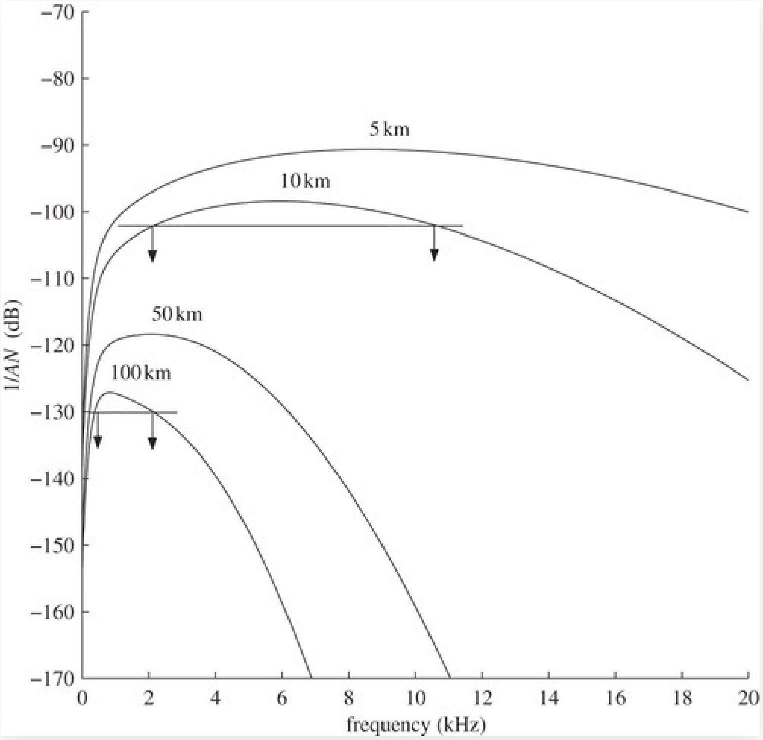


Figure 15: Discloses the frequency band and the dB ratio.

The data communication nodes often employ contention-based protocols that specify the guidelines by which nodes choose when to transmit over a shared channel, even though these deterministic approaches may be used directly in multi-user systems. The most simple protocol, ALOHA, allows nodes to simply broadcast whenever they need to (random access), and end-terminals may correct faults caused by overlapping signals (known as collisions) by retransmitting. In order to prevent transmission on a channel that is already in use, more sophisticated methods use carrier-sense multiple access (CSMA), a listen-before-transmit strategy, with or without collision avoidance (CA) algorithms. CSMA/CA has proved quite effective in radio networks, but underwater latencies (up to several seconds) render it exceedingly ineffective (even worse than ALOHA). ALOHA is indeed a possibility for underwater networks when coupled with basic CSMA capabilities, despite the fact that it is seldom taken into consideration in radio systems due to its low throughput. Figure 15 discloses the frequency band and the dB ratio.

The transport, routing, and network layers

It is unusual for any two nodes in a vast network to be able to interact directly, therefore multi-hop operation in which messages are sent via intermediary nodes to their intended recipient is frequently utilised. Furthermore, multi-hop operation is advantageous given the distance-bandwidth dependency covered in 3a.

Routing protocols are employed in this situation to choose a flexible path for a packet to go via a topology. While ad hoc routing for wireless radio networks has been the subject of several studies, research into routing design for underwater networks is currently ongoing work on underwater routing can be found in, where distributed protocols are suggested for both delay-sensitive and delay-insensitive applications and permit nodes to choose the next hop with the aim of minimising energy consumption while taking into account the application requirements and the specifics of acoustic propagation. Theoretical research has shown that it is feasible to determine an ideal advancement that the nodes should locally aim to accomplish in order to reduce the overall route energy consumption, leading to suggest a geographical strategy a similar concept was given, in which power control is also included into a cross-layer technique. Alternative methods include pressure routing, where choices are made based on depth, which is quickly and readily ascertainable locally using a pressure gauge.

A method for data broadcasting has been put out by who suggest an adaptive push system for the dissemination of data in underwater networks and demonstrate its viability in spite of the significant latencies present in this setting. Another crucial challenge is the design of the transport protocols for underwater acoustic networks. Large fractions of a second, which are often found in underwater networks are not what protocols like TCP are meant for, and a lack of capacity and substantial loss indicate that end-to-end retransmission would function badly.

To successfully transmit segmented data blocks through multi-hop pathways, for instance, suggest a novel transport protocol that makes use of erasure codes with varying block sizes. To deal with losses caused by lengthy delays, network coding and forward-error correction may also be used; coding benefits from optimized coding and feedback By eliminating end-to-end retransmission and enabling very sparse and often disconnected networks, other technologies like delay tolerant networking may be a better fit for many underwater networks. Underwater upper layer data-dissemination techniques have received little attention, and each deployment has traditionally used a unique approach present one system and provide procedures for synchronisation and data collection, storage, and retrieval for environmental monitoring.

Finally, topology control, where nodes sleep to save energy while preserving network connection, is a significant concern. Although coordination and scheduling algorithms may be used for this purpose, made the surprising discovery that, unlike radios, acoustic devices can really be awakened by an incoming acoustic signal without the need for extra hardware. This feature makes it feasible to wake up nodes when needed and to have a topology control system that is almost flawless. Such a low-power wake-up circuit is implemented in the media access protocol (MAC) layer of the sensor networks for undersea seismic exploration (SNUSE) modem and the Benthos modem also contains a wake-up mode.

Network services

Due to their widespread application among the various network services that are feasible, geolocation and time synchronisation have attracted the most attention. In a way, localization and time synchronisation are mirror images of one another since time synchronisation calculates clock skew whereas localization often guesses transmission time-of-flight while assuming correct clocks. Both present the difficulty of dealing with lengthy communications delay and noisy, time-varying channels underwater.

A decade later, wireless sensor networks spurred a resurgence of research with a focus on message and energy conservation through one-to-many or many-to-many synchronisation and integration with hardware to reduce jitter. Time synchronisation in wired networks dates back to the network time protocol in the 1990s. These concepts have been expanded upon in underwater time synchronisation and updated to handle issues with sluggish sound transmission. Clock drift occurring during message transmission dominates the error for acoustic channels longer than 500 m, according to time-synchronization for high latency network. Doppler-shift estimate was more recently included to D-Sync to account for inaccuracy brought on by node mobility or water currents.

The two main techniques for locating devices in wired and radio-based wireless networks are node-to-node ranging (based on communications time-of-flight) and beacon proximity (reachability due to attenuation). Localization techniques are often paired, similar to time synchronisation, or a beacon may broadcast to a large number of possible receivers. Since each microsecond of timing delay only causes a 15 mm loss in position, slow acoustic transmission enhances localization; yet, bandwidth restrictions make message counts much more crucial than in radio networks.

The technique presented by and sufficient distance map estimation are two underwater-specific localization systems with experimental validation. In order to lower message counts utilising an otherwise conventional approach based on all-pairs, broadcast-based, inter-station range, SDME uses post-facto localization (similar to post-facto time synchronisation of reference-broadcast synchronisation .At ranges of 139 m, they record localization accuracy of roughly 1 m. The technique developed by localises a moving AUV using a single moving reference beacon whose location is determined by the global positioning system. AUV position estimations using inertial navigation are integrated post-facto with an extended Kalman filter as part of their localization strategy, which is based on acoustic range between vehicles with synchronised, high-precision clocks. Their system calculates location with a standard variation of roughly 10-14 m in sea trials monitoring an AUV at 4000 m depths.

Techniques for sensing and application

The scope of this study does not allow for comprehensive examination of sensor technologies utilised in underwater applications, although we do briefly discuss certain difficulties in this section.

Some underwater sensor types are simple and affordable, but many quickly become complex and costly, costing anything from a few dollars to thousands or more. Affordable sensors include photo-diodes and thermistors, which monitor ambient light and temperature, as well as pressure sensing, which may provide an approximation of depth More specialised sensors include sonar, which can detect things beneath water, devices to monitor water CO2 concentrations or turbidity, and flourometers, which estimate chlorophyll concentrations .Such complex sensors may cost a lot more than simpler sensors. Traditional approaches to biology and oceanography focus on collecting samples from the natural world and taking them to a lab for examination. The cost of returning the sample is quite low when compared to the expense of transporting the scientist to the spot since conventional underwater research has relied on staff being there. We anticipate that the costs of sample-return compared to in situ sensing will compel a review of these assumptions as sensor networks and AUVs become more affordable.

The development of algorithms to control underwater sensing, sensor fusion, and coordinated and adaptive sensing is still in its early stages. Sonar has been utilised for analysing single sensor and sensor-array data for more than 60 years, and nowadays, offline pre-mission planning of AUVs is commonplace. We anticipate studies including online, adaptive sampling employing conversing AUVs as the field develops.

Hardware platforms

Over time, a variety of acoustic communication hardware platforms have been created with commercial, military, and academic success. These platforms are necessary to facilitate field usage and testing. Commercial devices with a large user base include Teledyne/Benthos modems. With vendor-supported changes, they have been widely deployed in SeaWeb, but since their firmware is not available to ordinary users, their usage is restricted for new physical layer and MAC research. In addition to the WHOI micro-modem, which is covered in 3g, the Evologics S2C modems enable the transmission of short packets, which are entirely programmable by the users and may be sent quickly without any medium access protocol rules. This capability may provide some extra flexibility. Even if the degree of reprogrammability of commercial devices is generally still quite restricted, there is some opportunity for designing and testing protocols by utilising such packets. These modems can transmit data at speeds of a few hundred to a few thousand bits per second (bps) across distances of up to tens of kilometres while using just a few tens of watts of power.

More options are available with research-specific modems, but they lack commercial backing. The WHOI micro-modem, which has a data rate of 80 bps (non-coherent) or roughly 5 kbps (coherent) and a range of a few kilometers, is perhaps the most popular device in this category. Other research modems have concentrated on straightforward, affordable designs, like the SNUSE modem at the University of Southern California (USC) and a cheap hydrophone at the University of California, San Diego in the United States, or on reconfigurable, frequently FPGA-based hardware to support higher speed communications or experimentation, like in Aqua Node at MIT a software-defined platform was suggested. This platform offers a robust way to test protocols in an underwater network and to customise them at runtime by adapting tried-and-true wireless radio tools (like GNU Radio and TinyOS) to operate with acoustic devices.

A low-power receive mode is supported by a number of modems, including Teledyne/Benthos, the SNUSE modem, and others, and may theoretically be used to provide wake-up modes for topology control .But whether or not the firmware is available typically determines how this wake-up capability is integrated with upper layer protocols.While there isn't a single operating system or development environment for all undersea research, platforms are often big enough to support conventional embedded operating systems. For instance, several organisations employ embedded Linux variations.

Test beds

The wide range of interest in underwater networks has led to a tonne of work in the lab and in modelling, but field tests are still challenging and expensive to instal offshore and charter boats for. In 2000, however, it was solely accessible to its creators, much as other modern field testing. A testbed that may be used by many projects at once or possibly be made available to the general public has recently been investigated by at least two organisations. A buoy-based, ocean-deployable testbed has been prototyped by WHOI while a modest, harbor-based testbed has been created by USC and made accessible to other parties. The ocean-deployable testbed can be transported to multiple sites and accessed over surface wireless for temporary deployments, but the USC testbed, which is internet-accessible, can only be utilised in one place and at any time. Giving more consumers the option to explore is a common objective of these programmes. The University of Connecticut, the National University of Singapore, and the North Atlantic Treaty Organization (NATO) Undersea Research Centre, among others, have installed medium-to-large-scale internal testbeds in addition to these moves toward shared testbeds.

Models and simulations

Alternatives are necessary because underwater hardware is expensive (a complete, watertight node can easily cost more than US$1000) and expensive to deploy (testing in a public pool can cost US$40 per hour due to the mandatory presence of a lifeguard, and deep sea deployments can easily cost tens of thousands of dollars per day). This contrasts with radio frequency wireless sensor networks, where experimentation is relatively accessible and affordable. The need for quick, controlled, repeatable testing under various situations is also crucial. To solve both of these issues, simulation and modelling are the best options. Unfortunately, networking simulators often have subpar accuracy when simulating the physical layer and the effects of propagation, which severely limits the predictive potential of such tools.

Many academics create unique simulators to answer their particular questions, while others create unique additions to already-existing tools like the network simulator .These technologies' generality and availability, however, are often limited, limiting their usage to their creators.

Building underwater modelling tools for the broader research community has been the focus of many recent initiatives, with a focus on capturing the essential aspects of sound propagation in adequate depth. For instance, the World Ocean Simulation System (WOSS) combines ns-2 with Bellhop, an acoustic propagation ray-tracing programme capable of forecasting the dispersion of sound in a given volume. This method combines an accurate acoustic propagation model in the tens of kHz frequency range with a potent and commonly used network simulation tool to get findings that may be considered to be somewhat realistic. While not a replacement for testing, these simulation frameworks are a highly helpful tool for initial research and for swiftly navigating a wide design area. An alternative strategy that is also being considered is to directly link a simulator to acoustic modems (rather than modelling propagation and the physical layer), fusing simulation and hardware to imitate a whole system.

To analyse acoustic propagation, a number of advanced modelling methods (including both analytical and computational techniques, such as ray tracing) have been created. However, in most cases, the complexity of such models renders them unsuitable for use in the analysis of communication systems and networks, where the time scales involved call for lightweight channel/error models and where many lower-level details may have a less significant impact on the performance as a whole. Because of this, there is presently a lot of interest in the creation of alternative models that may be used to simulation or analytical systems investigations. We anticipate that despite the fact that this is still an open subject, the current interest in underwater communication systems and networks will encourage study in the area, allowing for the development of inquiry tools that are both accurate and practical. Underwater sensing and networking are constantly evolving due to applications. In the last few decades, affordable computing, sensing, and communications have made it possible to network terrestrial sensors. We anticipate that underwater sensor applications will soon be made possible thanks to affordable computing, lower cost advanced acoustic technology, communications, and sensing.

While there has been substantial progress in the study of underwater sensor networks recently, there are still a number of problems that need to be resolved. Effective analysis, integration, and testing of these concepts is crucial given the flood of new communication, media access, networking, and application paradigms; the discipline must generate basic insights as well as comprehend what holds up in practise. This work will support more accurate performance analysis and system characterization, which will feed into the next generation of underwater communications and sensing, leading to the development of new theoretical models (both analytical and computational), as well as increased use of testbeds and field experiments. The seams that are sometimes overlooked in more specialised laboratory research, such as total system cost, energy needs, and general resilience in various environments, will also be stressed through integrating and testing existing concepts.

We are also encouraged by the field's expansion to take into account many possibilities, ranging from high-performance and cost to low-cost (but lower performance), as well as mobile (human-supported or autonomous), deployable, and fixed configurations.Distance aware collision avoidance protocol (DACAP) and tone-Lohi (T-Lohi) are two examples of protocols developed particularly for underwater networks using the CSMA/CA method. The DACAP is built on a preliminary signalling exchange to reserve the channel, lowering the likelihood of a collision. T-Lohi uses CA tones to provide lightweight signalling at the expense of increased sensitivity to the hidden-terminal issue Nodes that wish to transmit express their intention by transmitting narrowband signals, and they continue with data transmission if they do not hear tones transmitted by other nodes. Additionally, T-Lohi uses high acoustic latency to count competitors in ways that radios cannot, enabling very quick convergence [49]–[51].

While explicit coordination might enhance efficiency at the expense of collecting and keeping a time reference, unsynchronized protocols are easier. While inefficient long propagation still exists, synchronisation enables protocols to take use of the space-time volume by purposefully overlapping packets in time while they are still separate in space. In contrast to near-instantaneous radio communications, large acoustic latency allow concurrent packets to be successfully received, and packets delivered at various times may collide. Local synchronisation may be established and exploited to increase efficiency, even though it is often quite difficult to run such protocols in big networks. A number of protocols have been put out that rely on the system's multiple nodes having access to a single slotted structure. Early research took use of this issue by totally avoiding collisions by employing centralized scheduling rather than random access, but only for static topologies and with extra signaling. A decentralized, CSMA-based technique called slotted floor acquisition multiple access (FAMA) employs synchronization to lower the likelihood of a collision but is similarly prone to prolonged guard durations. Another protocol with this goal is the underwater wireless acoustic networks media access protocol, which uses local synchronization and sleep modes to reduce energy usage [52]–[56].

The purpose of this article is to examine the electricity consumption for the proposed cooperative data transmission in the cooperative transmission settings for Underwater WSNs that use clusters as their primary component. For Underground WSNs, efficient cluster-based communication methods include to investigate the realistic communication range for diverse subsurface issues among cooperative communications sensors. To propose a novel cooperative communication model that takes into consideration EM wave propagation properties in subversive situations.

CHAPTER 14

DATA GATHERING PROTOCOLS AND METHODS FOR WSN

Lokesh Lodha, Associate Professor,
Department of Electronics and Communication, School of Engineering & Technology, Jaipur National University,
Jaipur, India
Email Id- lokesh.lodha@jnujaipur.ac.in

Lightweight and compact sensor nodes are dispersed across the environment in wireless sensor networks (WSNs). These sensors and actuators are used to detect environmental characteristics. These characteristics include things like motion, strain, heat, motion, temperature, and humidity. Wireless communication is used to link the sensors to the "base station (BS)" or plunge to transmit data that has been detected. As a result, WSNs are being used for data gathering in several IoT-based activities, including residential applications, vehicle able to monitor, military implants, structure monitoring, ecology shriveling, detection systems, following for weapons systems, etc.

Due to the difficulties in designing sensor nodes, also including multipath routing, network congestion, and resource limitations (battery, communication, and computational resources), ad hoc and cell migration network routing methods are not appropriate for wireless sensor network. Because global addressing in WSNs is too challenging to maintain, several sensor nodes are installed for specialised applications. This huge number makes it possible for nodes in the same location to produce redundant data and send it to BS. This cause's network traffic and transmission waste, both of which increase energy usage. Due to the fact that more and more WSN applications do not allow for battery replacement or recharging, a sensor node's limited battery power is another major resource limitation. Because WSN uses a wirelessly backchannel, there is a higher chance of data transmission collisions, which affects network performance.

Wireless sensor networks (WSNs) consist of tiny, light sensor nodes that are dispersed across the surroundings. These sensors and actuators are used to detect environmental data. These characteristics include things like vibration, pressure, sound, motion, temperature, and humidity. The sensors are carefully synchronised and wirelessly linked to the base station (BS) or sink to forward detected data. As a result, WSNs are being used for data gathering in several IoT-based activities, including residential applications, vehicle monitoring, military implants, structure management, wildlife controlling, intrusion detection, tagging for military purposes, etc.

The Internet of Things (IoT) is a subject of study and discussion that is expanding quickly. IoT helps in monitoring operations for the military, healthcare, and the environment that need real-time data collection and distribution. Time synchronisation is crucial for the data collecting and information dissemination of collaboration wireless sensor network (WSN) networks when dealing with morning application. In this chapter, a temporal synchronisation function-based ad hoc navigation and data gathering protocol is proposed. The introduction of a hybrid bandwidth time synchronisation method in which reference time is derived from both the sink node (centralised) and the nearby nodes distributed. Since it reduces expenses and transfer exchanges, time synchronisation is incorporated into routed and communication communications in the network, which is advantageous for large-scale WSN.

Small hardware (HW) modules that are capable of sensing, monitoring, or measuring their surroundings make up wireless sensor networks (WSN), which are networks for data measurement and collection. The detected data are sent to some sink, server, or base station either directly or through relay via additional sensors. Such a configuration's main goal is to provide control or exploration powers over the region where the network is installed. The monitored terrain can range from a small coverage area (such as the human body) to a vast realm (such as a forest area for fire detection), the sensed variables of interest of the surroundings are varied (such as weather or health parameters, acceleration, or pollution), and the sensors can have different characteristics. These WSN characteristics can vary significantly (e.g., size, computational power, energy source).

The goal of the Internet of Things (IoT) is to make daily living better. Smart homes, smart cities, ubiquitous health care, assisted living, environmental monitoring, surveillance, and other technologies are all included in the notion. The Internet of Things (IoT) paradigm depends on connecting numerous devices (things) connected to the Internet via heterogeneous access networks so they can communicate with one or more Internet gateways and exchange information. These gateways can process the data, take action, and forward the information to another location if necessary.

IoT systems will heavily depend on WSN technology since many IoT devices are anticipated to be wireless and because sensing is one of the primary jobs and tools employed by the IoT paradigm. There are many different circumstances where WSN are used nowadays. Traditional classifications of WSN included terrestrial, subterranean, and multimedia. Given that WSNs and IoT are closely related, modern classification often reassigns the notions of the WSN domain to the IoT domain and categorises them according to their primary goals, such as smart cities, healthcare retail and leisure utilities (such as smart home energy control, water metering and leak detection, and other general infrastructure monitoring networks), agriculture and environmental safety (such as smart farming and harvesting) and others

Data gathering and dissemination are important functions of both WSN and IoT systems, as was previously mentioned. Device reports are gathered, and updates and operating responsibilities are transferred. Additionally, maintenance and functional evaluations are gathered and shared. It is difficult and receives significant attention from both the industrial and academic communities to collect and disseminate data in very dense networks like WSNs and IoT networks that span heterogeneous devices, many of which are anticipated to be small, with very constrained processing, storage, and energy resources, and with minimal network capabilities.

Several of these difficulties include: Information management there is a tremendous amount of data being gathered or that needs to be distributed to the relevant parties, and some of it is anticipated to be redundant, both in terms of the data sent by each device, which can be compressed, and in terms of the data that is received by various entities but is the same data. In order to minimise the amount of data broadcast via wireless channels, novel strategies for data compression and aggregation that take use of information redundancy supplied by many organisations are needed. To allow prompt decision-making and prompt action-taking, it is necessary to process and analyse data in real-time or very close to real-time due to the anticipated huge data interchange and the low latency requirement (at least for part of the information acquired).

The capacity to properly transmit, receive, and analyse immense amounts of data originating from an increasing number of devices and sensors in order to automatically operate a far wider range of daily living systems is directly tied to the issues associated with Big Data. Additionally, using cloud computing platforms allows for considerable improvements in data analysis skills .It opens up new possibilities for the growth and development of WSN/IoT networks in terms of the quantity of data that can be gathered as well as the number of sensing device.

Connectivity one of the main obstacles for the IoT in the future will be gathering and distributing data from and to many devices, perhaps across large, dense, heterogeneous networks. To meet this difficulty, new MAC protocols and coding schemes need be developed. In this regard, the MAC layer protocol design places a high priority on energy economy and air time usage. Any MAC layer protocol should make sure that gadgets use the wireless channel sparingly and with the least amount of energy possible. Security and privacy – The IoT network is vulnerable to major security flaws as a result of the massive number of devices that are connected to the Internet. More so considering the small number of relevant entities. As a result, concerns like authenticity, data encryption, and attack susceptibility such as device impersonation are crucial for the ongoing development of the IoT paradigm Additionally, the gathering and sharing of this information presents substantial issues in terms of data security and privacy since the information communicated across WSN and IoT networks might be extremely personal (e.g., health reports, device tracking).

In the aforementioned WSNs and IoT contexts, this review will examine the most recent developments in data gathering and dissemination techniques. Despite placing a heavy emphasis on current publications, we will discuss significant turning points and provide the most recent trends and research directions. Using the keywords from this article, we mostly used Google Scholar, IEEE Xplore, and the university library databases. Additionally, we consulted significant references from the biographies of the original publications and the papers that mentioned them. From the actual implementation of delivering bits through a communication media to the application layer, data gathering encompasses all networking tiers. We won't be able to address every facet of the subject due to its extensive nature (for example, in this paper, we will not discuss the critical topic of security and privacy).

More detail will be given to some of the topics than others. On some of the topics, we will provide a more thorough background and describe protocols that are aimed at a wider domain than data-gathering, though some of the topics we discussed rely on general wireless communication technology and on broad setup protocols that are not data-gathering oriented per se. For instance, several wireless routing and medium access control (MAC) protocols are created to support a variety of topologies, traffic patterns, and quality of service needs. They may be used, but they are not specifically designed for data collection. In our survey, we will also include a few more fundamental yet generic research. In certain situations, we will go into the relevant history and veer off into some ancillary areas to get the whole picture and better comprehend some data-gathering-related challenges. All of the protocol stack's layers will be addressed in detail. Classification based on a stack is not always straightforward since some problems require numerous stacks.

The platform of the device, which houses the sensing unit, can have a significant impact on how well an application uses it, particularly a data-gathering application. In turn, the platform architecture can have an impact on an application (such as data gathering) when it is designed in an application-oriented manner or when some of the platform's key features and requirements are taken into consideration. The WSN infrastructure and the network design have the same reciprocal impact (e.g., topology, system organization). We begin by evaluating research relating to innovations in the platform and architecture of the device as a whole .We present new options for algorithm creation in such networks by addressing new areas that have just lately been exposed to WSN and IoT networks. Some of these cutting-edge technologies have completely changed how applications use individual devices and the common network. They have also opened up new possibilities for algorithms and posed significant design difficulties for the whole protocol stack, which we detail in this study.

A concentrated description of recent developments in compressed sensing, a signal processing approach that may benefit from the sparsity and redundancy of the data, is given in Section 3 after that. Compressed sensing is used in data collection techniques to minimise report payload on many levels, including the quantity of sensed data and communicated reports, the number of devices that need to transmit reports, and the compression of combined relayed data before it is forwarded to its destination (the sink). We lay out the fundamentals of compressed sensing and evaluate the state-of-the-art in terms of data collection in WSNs.

Channel usage is crucial for wireless communication and has a significant impact on a number of performance factors, including throughput, latency, power consumption, delivery ratio, and more. Many different wireless channel access algorithms and protocols, as well as WSNs with their own characterisation, have been proposed throughout the years. We only cover a tiny portion of the several MAC protocols created specifically for WSNs in Section 4. We analyse some of the most recent MAC protocols used in data collecting in WSN and IoT networks, which handle new issues such very dense networks, crowded channels, and very restricted resources. Our major focus is on protocols that show a conceptual approach or trend.

As we go up the protocol stack, discusses components of routing. Routing methods in multi-hop wireless networks have also been thoroughly investigated, similar to the MAC sublayer. We begin by outlining a number of benchmarks for data collection in WSNs. We go on to discuss more current research, which mostly focus on improvements to the aforementioned procedure while also addressing fresh difficulties including scaling requirements and energy-related advancements that both provide new possibilities and place fresh restrictions. We keep looking at works that implement a network-coding approach by taking use of the multi-hop topology. Finally, we describe a novel paradigm that replaces the conventional configuration in which sensed data must be sent to a stationary central monitoring station (sink) with a mobile sink (or sinks) that may help gather the devices' reports and travel the terrain. We examine a number of cutting-edge plans for this mobile sink paradigm.

The last component of this study is devoted to wearable technology, which includes smart gadgets that are affixed to people's bodies and monitor their surroundings and themselves. Wearable technology presents difficulties in all the areas covered in the preceding sections, but they also open up new possibilities for high-demand applications with particular performance limits and needs. We stress this important application layer and cover many applications in Section 6 even if we do not try to offer a thorough assessment of the numerous applications that have been proposed over the years.

As previously stated, we ordered the parts depending on how broadly we divided the survey's issues into the communication levels. We point out that this division is somewhat fictitious since many advances in data collection use many layers. Additionally, several technical developments and research fields have an impact on numerous sectors at various tiers and are covered in more than one section. The paper's conceptual framework is shown in Figure 1. The primary study areas addressed in the article are represented by the ovals in the picture. The most notable data-gathering methods and developments, which are addressed in the article, are represented by hexagons. The arrows show how they are related to one another. Innovations, from platform hardware to the application layer, use technology like energy harvesting (EH), machine learning (ML), and artificial intelligence (AI), for instance. The network layer, however, is primarily responsible for using network coding. Both the MAC and the Network layers make use of Unmanned Aerial Vehicles (UAV).

WSN Architecture: Emerging Platforms and Innovative Infrastructure Concepts

In this study, data collection in the context of wireless communication networks is our main emphasis. The devices that provide the data (usually sensors) depend on the application and may be used in a wide range of contexts, including health, the environment, activity tracking, etc. Despite the fact that the sensing unit is the essential component, we will just briefly touch on it while addressing applications and their unique needs. However, the term "sensor" usually refers to the entire platform or device, of which the sensing unit is merely one part among many others, including the processing unit, transceiver unit, power unit, antenna, and others, some of which can be integrated into the device depending on the requirements of the specific application. The sensing device itself has needs and limitations, and in many circumstances cannot be changed. The platform design and integrated unit architecture may also be subject to a number of strict limitations. For instance, size limits may place severe restrictions on the design of the device; other restrictions may include low power consumption, low manufacturing costs, and self-operation. As a result, the device architecture is crucial and has an impact on several other system components. The transmission range, memory, and processor unit are just a few of the factors that the power supply may influence. These factors can then have an impact on the algorithms that the device is capable of executing, etc.

The architecture and design of the infrastructure as well as the end device have been the subject of much investigation. We leave it beyond the purview of this study to describe in detail the fundamental parts, such as the sensing unit, transceiver, antenna, processing unit, etc. The goal of the next paragraphs in this section is to discuss how data collection goals may affect both the design of particular sensors and the WSN architecture.

The latter includes topology, the way the data collection system is set up, and the algorithms used to carry out the data collection. It is important to highlight that the topology and, therefore, the data aggregation techniques are also determined by the properties of the sensors. In the follow-up, we discuss a number of platform architectural ideas as well as a number of network-wide architectures, most of which are current. The survey contains other, comparable research, however they are arranged in chapters according to the subject matter where they provide the most uniqueness. A schematic representation of the portion is shown in .The description is general and only focuses on the main topics covered in the section because many of the papers presented in this section cover more than one topic, and because, as was already mentioned, this section is not presumed to provide an exhaustive list of all papers or topics covered by the scope of WSN architecture. Some of the topics are not covered at all or are covered by only a few representative papers.

Application-Oriented

Application-focused sensor systems are common. Although their proposed architecture may sometimes be applicable to various applications, its design and assessment are often focused on a particular one. As a result, technical advancements in both hardware and software are often made for efficient operation. The obvious duty of monitoring a landscape is one of the most frequent ones for WSN. The monitoring of WSNs comes in a variety of forms. Monitoring every point in the Field of Interest (FoI), for instance, vs monitoring a small number of specified sites or targets (also known as target coverage), versus just keeping an eye on a region's boundary to look for invaders are all possible requirements (aka barrier coverage). In order to satisfy the monitoring goal while retaining network connection, a subset of sensors must often be chosen to solve the coverage challenge. The network architecture is determined by the capability of the sensors and the goal of the monitoring.

We provide a number of current examples that primarily focus on connection and data collection while adhering to the monitoring objective's limitations. In the target coverage issue, where a n sensor WSN has to monitor T distinct targets concentrate on energy-efficient data collecting since there is a path (multi-hop) from each source to the sink. The study addresses the forwarding of these packets to the sink and makes the assumption that the source nodes that detect targets and send data packets into the network are known. The study suggests a distributed data collection mechanism in which each node, after learning about its neighbours and their hop-count to the sink, forwards data packets to its neighbour with the most energy left and the fewest hops to the sink as necessary (the remaining energy is assumed to be known). According to Ammari , the k-coverage issue requires that every location in the field of interest (FoI) be covered by at least k sensors at any one moment, and that every active sensor engaged in the monitoring job be linked to the sink (possibly via a multi-hop route).

The paper makes the assumption that the sensors are mobile and heterogeneous (they don't all have the same characteristics), so they can move to any area of interest in the deployment field to participate in any area with insufficient k-coverage. The sensors can also serve as mobile proxy sinks, gathering sensed data from the sensors and sending it to the sink divides the issue into two issues that are resolved one after the other. Specifically, the mobile k-coverage problem, which chooses a minimal subset of active sensors to solve the k-coverage problem and the data gathering problem, and designs a forwarding scheme from the active sensors to the sink so as to minimise the energy consumption due to sensor mobility and communication.

The source of energy is one of the primary design considerations for the sensor platform. Usually, the sensor platform's battery serves as the energy source. It is used to power all necessary processes, including memory, computing, and wireless transmission. The longevity and a number of other characteristics, including the transmission range, of the battery may be affected by its qualities (such as the technology and size employed). The battery is a problem in many systems since it raises the price, limits the size of the platform, and—most importantly—needs to be changed from time to time. Saving energy is a difficulty that affects the whole protocol stack; in this survey, energy concerns are addressed in each section. PHY layer advancements have also been proposed as a means of maximising battery power, similar to the other layers.

To get around the battery problem, an alternate strategy is to include an energy-harvesting system. To increase the battery's longevity, such a mechanism may be integrated alongside it. More often, though, it will replace the battery entirely, taking over all of the operations. Batteryless WSNs that only use energy-harvesting (EH)-WSNs run the risk of having poor performance due to factors like reduced transmission range, limited awake time, and so on. Finding the ambient resource from which the energy may be gathered is one of the biggest obstacles. Numerous research have investigated various sources of supplementary energy, including sun, vibration, wind, motion, electromagnetic, and others. For instance, have several in-depth technology overviews with their benefits and drawbacks, energy harvesting models, challenge expectations, and future possibilities. An updated system design assessment on battery-free, energy-aware WSNs that rely on wireless energy transfer or ambient energy is provided. The strategies for energy supply are covered, together with information on energy management techniques and opportunities for energy savings at the node and network levels.

An RFID chip, a circulator (which permits power flow between three specified ports), a capacitive sensor, a circulator that enables power to flow between three defined ports, and an antenna make up proposed zero-power wireless sensor design (batteryless). According to the underlying principle, the sensor should reflect the RFID signal with a phase shift that relates to the value being measured propose the design and implementation of an energy independent WSN platform for ambient monitoring in indoor spaces. The suggested self-powered autonomous sensor node platform makes use of a microprocessor, an RF transceiver with a connected antenna, and integrated photovoltaic (PV) panels to capture energy. Experimental prototyping and validation of the proposed architecture was done. A floating wireless device with energy-harvesting capabilities is suggested the floating object may run for a longer period of time on its own energy. When installed over water, it enables long-distance communication between wireless sensor nodes and a gateway using LoRa technology.

To remotely gather data on the weather and water quality, the floating gadget may be utilised as an environmental monitoring station. The architecture of a solar-powered wireless sensor node that gathers environmental data and can send it over great distances is directly to the cloud. The architecture described therein uses LPWAN protocols, which provide a long-distance communication system with less data to transmit and good energy efficiency. Sigfox technology is used by the writers in their proof-of-concept design. There are surveys and tutorials addressing many facets of energy harvesting in WSN, as has been described in multiple works (a sliver of which we present herein). When we explore other data aggregation topics, such as routing improvement for EH-WSN (under EH restrictions), which we go into detail about in or when we talk about wearables in we will bring up EH once again the topology

The interplay between WSN and IoT will appear in many circumstances throughout the study. While the majority of the data in this study was collected through wireless devices, an IoT device would likely use a higher-level entity to collect data locally. The most current study by, for instance, where the authors list the IoT data management frameworks, problems, and concerns, is recommended for the reader to consult in order to evaluate the relationship between these two ideas. The three levels of data management in IoT networks communication, storage, and processing—are the main topics of this chapter. The implementation of IoT Data management for smart cities and smart homes is also explained.

A bi-directional WSN platform, where the sensors are expected to be able to act in response to control messages received from a sink, must be distinguished from a one-directional WSN platform, where the sensors merely gather the data and activate a particular infrastructure and set of technologies to send it to a sink. In the latter scenario, a higher-level object may be the sink (e.g., a cloud-based server). Although the control direction is often irrelevant to the main data collection procedures, extra restrictions could be put in place. Some requirements to take into account are reaction time, latency, BW utilisation effectiveness, security, and privacy. Social sensor clouds (SSC), which link a social network with a sensor network through a cloud architecture, are another illustration of a bi-directional platform for instance, who give a scenario of a smart village and explore a variety of topics, such as energy problems, green design, and the speed of data collection and exchange. A platform for on-demand WSN is created by.

The authors propose a data-gathering technique that reduces the number of queries to save resources while addressing bandwidth usage and delivery delay. A unique scenario is a sensor infrastructure where sensors form groups that belong to private owners. This may be the case in a smart city setting, in which case privacy and/or security issues need to take precedence. This is the subject that discuss. Although throughput constraints are taken into consideration, the authors provide a trust-assisted cloud for WSN. A WSN-based IoT infrastructure is suggested by that offers a dependable link between field sensors and the online database. The suggested platform is based on the time-slotted channel-hopping protocol and supports heterogeneous applications with resource-constrained devices. The time-slotted channel-hopping protocol calls for a clock synchronisation that may be maintained by using a technique that adjusts for clock drift for each timeslot.

Edge computing, as stated by enables sharing the workload of data collection among many cloudlets, which may be very advantageous for big WSN. This platform paradigm seeks to enhance a number of crucial factors, including decreased data delivery latency, greater bandwidth, scalability, resistance to potential cloud failures, and privacy management. The platform, however, demands an initial capital outlay and ongoing upkeep presented a virtual sensor network. A appropriate collection of sensors is identified for the job when a user-initiated sensing request is sent to the cloud.

The cost function, which considers factors such as the specific (e.g., monetary) cost of using sensors from the designated set, the potential benefit of using these sensors, and their efficiency in terms of distances and delays (calculated, for example, in terms of the number of hops from sensor to sink/gateway), also expressed as virtual links, is used to make the decision. While a generic virtualization issue is posed and a method is offered, the cost may be adjusted discuss the integration of unmanned aerial vehicles (UAVs) with WSN for crop monitoring in precision agriculture. The authors propose a down-up method in which the data is gathered and then provided to the cloud for analysis and potential feedback after being processed hierarchically from the ground level to the cluster head (CH) level.

Outlier data from certain sensors are given special attention since they may portend either a sensor failure or an impending uncommon occurrence in the agricultural field. Consensus algorithms were used to process the measured data. In addition, it suppressed outlier data that were still available for the cloud-based analysis's subsequent investigation. This research also concentrated on arranging the UAV trajectory to gather the WSN data. Actual deployment is shown and examined with many tens of sensors and multiple CHs. Please take note that is devoted to data collection facilitated by a mobile unit. an implementation of a ubiquitous consumer data service for sending brief messages to any computer platform. The authors provide a data cycle model that enables any device having a sensor or sensors to transmit data in the form of brief messages. The unstructured raw data is sent to a central or distributed computing platform, where it is transformed into rich, useful information for higher-layer applications. The large-scale crowd-sensing-based IoT scenarios and smart cities are the target markets for the proposed data cycle model and DataTweet architecture.

Application-Oriented Networking Architecture,

We proceed by discussing customised application-driven architecture types and unique WSN platform kinds for data collection. For situations where animals display sparse mobility, resulting in occasional wireless connectivity, propose an IoT network architecture for wildlife monitoring systems (WMS). Additionally, they propose a data forwarding improvement that applies the flood-store-carry-and-forward paradigm proposed in the groundbreaking in which the nodes distribute data among themselves until it reaches the sink in order to transfer it to the sink. In further detail, each node stores the information that needs to be sent, waits for connection with other nodes, and then distributes the information to them. The process is then repeated. The data is thus dispersed over the whole network (i.e., flooding) and will finally reach the sink. By controlling the data replication choice, the authors of propose using locally accessible routing parameters to enhance opportunistic data forwarding methods increasing the number of bits transmitted per symbol and, more specifically, relying on a quaternary interconnect scheme in which each transmitted symbol modulates two bits, will lengthen the lifespan of a wireless sensor network used in mobile healthcare applications. To cut down on energy use during data transmission and storage, a complementary neural network, static RAM-based architecture is proposed.

Numerous applications have used wireless sensor networks. Data collection is one of their most crucial uses, which involves the continuous gathering of sensing data at each sensor node and transmission of those data through wireless communication to a centralised base station for further processing. Each sensor node in a WSN employs wireless communications and is powered by a battery. A sensor node's modest size is the consequence of this, which makes it simple to attach to any surface while causing minimal disruption to the surroundings. With such flexibility, wireless sensor networks are far less expensive and labor-intensive to build and maintain than their wired counterparts, making them a more promising data collecting method overall.

But WSNs' distinctive characteristics also provide a host of brand-new difficulties. To further decrease the costs of maintenance and redeployment, the consideration of energy efficiency is often chosen in a WSN design. For example, the battery linked to a sensor node limits its lifespan, and the network's lifetime relies on the lifetime of sensor nodes. Additionally, these difficulties are made more difficult by wireless losses and collisions that occur when sensor nodes connect with one another.

Additionally, the demands put forward by data gathering apps present additional concerns that must be taken into account during network design. First of all, several sensors with various sample rates may be installed at various places in order to precisely collect various sorts of data (such as temperature, light, and vibration). More and more sensing data will be gathered along the delivery course as it is sent back toward the base station. If not handled appropriately, these problems might result in uneven energy consumptions throughout a WSN and severely reduce the network lifespan.

We first emphasise the unique characteristics of data collecting in WSNs in this research. We then address problems and earlier studies on the data collection protocol design while keeping these qualities in mind. Additionally, we go through several data collection protocols including Direct Transmission, Binary Scheme, LEACH, PEGASIS, and TREEPSI, which are essential for energy-efficient data collection and have a significant impact on a data collection WSN system's overall performance.

COLLECTION OF DATA

Each sensor node in a sensor network has a sensing capacity. The sensor nodes are dispersed at random to gather data at a predetermined place. First of all, once deployed, a sensor node is anticipated to continue operating on its own for many days, weeks, or even years. In contrast to the Internet, wireless mesh networks, and mobile ad hoc networks, where either constant power sources are available or the expected lifetime is several orders of magnitude lower than it is for WSNs, it is powered by the attached battery, necessitating high efficiency energy utilisation.

After gathering the data, it is sent back to a central base station for processing. Traditionally, cables used for power supply and data transfer have linked these sensors. The wired technique, on the other hand, is proven to need significant deployment and upkeep work. The placement of the cables must be carefully planned in order to minimise interference with the surrounding environment. And if a wire breaks, the whole network may become inoperable, requiring a significant amount of time and effort to locate and replace the damaged line. Additionally, the wiring deployment and its maintenance may be very challenging, if not impossible, due to the sensing environment itself. For instance, areas near volcanoes or wildfire scenes, where the hot gases and steams may quickly harm a wire. In fact, rodent hazards persist even in less hostile environments like a structure or a natural habitat, making the security of cables considerably more challenging than that of sensors.

As wireless sensor networks become more prevalent due to technological advancements, all these problems make them a good option .Since processing these data involves knowledge of the whole world and is complex, data gathering demands that all sensory data be reliably and correctly captured and sent to the base station far more intricate than that in other applications, such as target tracking. Therefore, the reported data from each sensor to the base station constitutes the majority of data gathering traffic. If such a "many-to-one" traffic pattern is not managed appropriately, it will result in a high level of imbalanced and ineffective energy usage over the whole network.

In reality, the message distribution protocol is used to distribute network setup/management and/or collection command messages from the base station to all sensor nodes when a data collection WSN is installed. Sensing data are then acquired from various sensors and sent to the base station through the data collection protocol in accordance with the information provided by the messages that were broadcast. It is important to note that the aforementioned procedure may operate repeatedly in a data collection system, meaning that after one round of data collection, fresh setting/command messages are broadcast, thereby beginning a new cycle of collection.

DISSEMINATION OF DATA

Data and requests for data are directed via a mechanism called data dissemination in a sensor network. A source is the node that produces the data in the context of data dissemination, and an event is the information that has to be reported. The term "sink" refers to a node that is interested in data, while "interest" is a descriptor for an event the node is interested in. Therefore, the event is sent from the source to the sink once sink gets an interest from source. As a consequence, disseminating data involves two steps. The node that is initially interested in certain occurrences, such as temperature or air humidity, periodically broadcasts its interests to its neighbours. The whole sensor network is then informed of new interests. After receiving the request, nodes that have requested data transmit it back in the second phase. A cache of incoming interests and data is also maintained by intermediate nodes in the sensor network. There are many different ways to distribute data. In this essay, additional in-depth discussion is given on floods, gossiping, and SPIN.

Flooding

When using the flooding approach, any sensor node that gets a packet broadcasts it to its nearby nodes, supposing that node is not the packet's destination and that the maximum number of hops has not been reached. This makes sure that the data and data-related requests are transmitted over the whole network. Flooding is a pretty straightforward procedure, but it has a number of drawbacks. Implosion occurs when many messages are sent to the same node during flooding. When a node gets the same message from many neighbours, this happens. Additionally, if many nodes detect the same event utilising flooding, neighbours will get repeated reports of the same event, which is referred to as overlap. Finally, flooding generates a large number of duplicated transmissions and does not account for the energy supply at sensor nodes. This substantially shortens the network's lifespan and wastes a lot of its resources.

Gossiping

Flooding is the foundation of the gossiping approach, except the receiving node only passes the packet to one randomly chosen neighbour as opposed to all of the neighbours. The benefit of gossiping is that it doesn't cause implosion and doesn't use up as much network capacity as flooding. The main drawback of gossiping is that since the neighbour is chosen at random, some nodes in the extensive network could not even get the message. So, gossiping is not a trustworthy way to spread information.

SPIN

Negotiation and resource adaptation are used by Sensor Protocols for Information through Negotiation (SPIN) to alleviate the drawbacks of simple flooding. With SPIN's data-centric routing, nodes advertise their data and transfer it once they hear back from interested nodes.ADV, REQ, and DATA are the three message kinds used by SPIN. After gathering some data, the sensor node delivers an ADV message with meta-data detailing the actual data. The neighbour responds with a REQ message if one of the node's neighbours is interested in the data. The sensor node transmits the real DATA message after receiving the REQ message. Data is distributed around the network as a result of the neighbour sending ADV message forward to its neighbours as well.

Node A uses an ADV message to announce its data, Node B responds with a REQ message, and Node A then transfers the requested data to B. Additionally, Node B transmits ADV messages to its neighbours. An enhanced version of SPIN, SPIN-2 utilises a resource or energy threshold to limit node involvement. As a result, only nodes with an adequate quantity of resources take part in ADVREQ-DATA exchange.

Flooding is less effective than SPIN because of the negotiation's reduction of implosion and overlap. The network's lifespan is extended by resource adaptation in SPIN-2 because sensor nodes with less resources are able to gather data for longer periods of time since they are not required to participate in the ADV-REQDATA exchange.

Data transmission from the sensor nodes to the base station is the goal of data collection. The goal of data collection algorithms is to maximize the number of rounds. All Rights Reserved One round in the 44-round communication process between nodes and the base station denotes the base station's collection of data from all sensor nodes. Data collecting algorithms thus aim to reduce power usage and collection process lag. Although acquiring data and disseminating it may appear comparable, there are key distinctions. While all data is delivered to the base station during data collection, additional nodes besides the base station might request data during data dissemination. Additionally, although data is usually sent on demand when it comes to data distribution, it might be delivered regularly for data gathering. We'll go into greater depth here about various data collection techniques such direct transmission, PEGASIS, and binary scheme.

Transmission Direct

All sensor nodes transmit data directly to the base station when using the direct transmission mode. Direct transmission is a straightforward technique, but it is also quite inefficient. Some sensor nodes may be located quite distant from the base station, resulting in very high energy consumption. In order to prevent collision, sensor nodes must alternate while sending data to the base station. As a result, the delay is also extremely great. Since the goal of data collection systems is to reduce both the energy consumption and the delay, direct transmission method performs extremely badly overall.

A data collecting protocol called Pegasis Power-Efficient Gathering for Sensor Information Systems (PEGASIS) makes the assumption that every sensor node is aware of the network's topology.PEGASIS seeks to reduce the transmission lengths over the whole sensor network, as well as the broadcast overhead, the number of messages delivered to the base station, and the energy consumption split evenly among all nodes. In PEGASIS, a chain of sensor nodes is built beginning with the node that is farthest away from the base station using a greedy algorithm. This chain is built before data transmission starts and is rebuilt if nodes fail.

Nodes aggregate the data during transmission, and just one message is delivered to the next node. The leader node then sends a single message to the base station including all the data. O(N), where N is the number of sensor nodes in the network, is the latency in messages arriving to the base station. Data is sent from the chain's two ends to the leader, who then transmits it all to the base station.

PEGASIS succeeds in its objectives: Since practically every node will transmit and receive only one message, transmission lengths throughout the whole network are short, overhead is low, just one message is forwarded to the base station, and energy is allocated fairly evenly among all nodes.

High latency, extremely lengthy chains in big sensor networks, and a lot of hops are needed to transmit data from the chain's end points to the base station are all drawbacks of PEGASIS. Additionally, PEGASIS makes the assumption that each node has access to network topology information, which isn't necessarily true in sensor networks.

Describe a WSN devoted to home deployment for geriatric healthcare and early health emergency alert. The authors initially voice privacy concerns over the monitoring and, as a result, support the use of just sound-based surveillance designed to simply alert people to potentially dangerous circumstances. They concentrate on a distributed architecture (rather than a centralised one) where each of the WSN sensors delivers encrypted IDs of their measurement in order to further adhere to the privacy needs. The foundation for event identification is feature extraction. The incoming signal is first divided into blocks using a Hamming sliding window, and then transformed into the frequency domain using a Discrete Fourier Transform (DFT) to determine the relative contributions of each spectrum band. After the discrete cosine transform, the final coefficients are obtained (DCT). The algorithm's concluding sections categorise the coefficients and input those classes into support vector machines, which then classify the predicted audio event. The scientists claim that by introducing a deep artificial neural network (ANN) into their system, the classification results might be significantly enhanced.

A similar technique was used for urban noise measurement by to be specific, convolutional neural networks classified noise levels and events while STFT was used for the noise preprocessing (CNNs). See the sources for further information on the networks the authors utilised. Similar techniques for noise monitoring WSN were presented. Analysis in the frequency domain was done. After that, categorization using statistical techniques was completed (Gaussian mixture model was used). Additionally, the authors in provide a complex WSN design in which energy-harvesting solar panels lengthen the sensors' useful lives while central, more potent nodes broadcast and monitor the sensors' state of charge.

Numerous self-powered smart devices are used by many data-gathering apps to capture real-time data and transmit it wirelessly to a central entity or entities (such as the cloud) for further processing and action. Sensing and wireless communication are the two fundamental tasks that these gadgets are anticipated to carry out. Given that many of these devices are typically simple with limited computation power and battery lifetime, there are two significant performance-impairing factors that arise from these two operations that must be taken into account: I energy consumption associated with these two operations; and (ii) airtime utilisation, which can also impair performance by causing high delays, jitter, battery consumption, etc.

Reducing the report payload, which has an impact on each report's transmission time and channel use, is thus one of the primary obstacles in overcoming these restrictions. At various stages, the payload of the sensed data can be reduced. For example, during the sensing stage, the size of the sensed data can be reduced; during the report preparation stage, the report size can be compressed; and during the transmission stage, the devices that must send reports can be chosen, reducing the amount of redundant data. Reports may be pruned, unified, and compressed during the relay stage to reduce the number of hops necessary for them to reach their destination. The next section talks about compressed sensing (CS). This innovative paradigm may decrease the report payload at the various levels stated above, reducing the transmission time and energy use of the sensing operation.

Compressed sensing is a signal-processing method that works best when the subject signal is sparse in one or more domains and can be represented by a minimum non-zero vector of coefficients. A high-quality reconstruction is made feasible by the signal sparsity, and this is done by solving a linear system of equations with a minimal number of non-zero values. As a result, in order to conduct the recovery, a convex minimization problem must be addressed. It should be noted that the CS approach samples the data signal non-uniformly, and its average sample rate is typically lower than the minimum rate required by the Nyquist-Shannon sampling theorem. both provide a thorough overview of the method. Compressed sensing may be used in a variety of networking areas.

For instance, illustrate several CS applications across networks and explain the relationship between CS and conventional information-theoretic approaches in source coding and channel coding. As a result of its ability to take advantage of the anticipated high spatial and temporal correlation between sensing reports sent by nearby sensors at various times in order to achieve the desired sparsity of the CS paradigm, CS is particularly well suited for sensed data gathering in wireless sensor networks (e.g., physical phenomena or a scenery). The next section reviews a few of these CS-based data collection methods is a densely distributed monitoring sensor network in which reports go via many hops before arriving at a sink. These research are predicated on the notion that the detected signals may be sparsely represented in a transform domain since the sensor readings are spatially linked. Both suggest a compressive data-gathering (CDG) method in which sensors project their reports on a random space basis utilising random coefficients to distributely encode their data.

Compressive sensing methods may be used at the sink to decode these encoded reports. In particular, CDG is designed for multi-hop networks where messages must pass through many hops to reach their final destination. At each sensor, distinct multiplications and additions are used to carry out the sampling procedure that defines the CS compression process. In particular, CDG proposes that each sensor utilise each of its reports (measurements) to create and deliver M distinct messages, each of which consists of a weighted sum of the sensor's own report with reports from other sensors crossing it, rather than forwarding individual sensor readings (relaying). The measurements (readings) acquired by all the sensors are symbolically represented by the vector.

The measurement matrix (coefficients matrix) should be a complete random matrix with i.i.d. Gaussian random numbers generated in accordance with N. (0,1M). In order to avoid the burden and expensive overhead necessary to gather these coefficients by the sink if they are generated randomly, the study proposes that each weighted sum coefficient be chosen pseudo-randomly based on each sensor's ID. The random coefficient selection proposed in Reference is extended to a partially random matrix in which the entries of a sub-matrix are still selected using (0,1M). The identity matrix or an upper triangular matrix with non-zero elements generated using N(0,1M) are the two alternatives recommended for the remainder of the matrix. The sink will be able to precisely recover the reports when the sensor readings are compressible, even if the number of weighted sums (messages) each sensor generates for each report (M) is much lower than the number of reporting sensors, according to CDG, which uses the compressive sampling theory to demonstrate this (N). For instance, on a route with N sensors, the sink only has to gather MN messages to encode the data sent by all N sensors [73]–[79].

A number of studies go into further detail about the sparsity of the detected signal, its projection matrix, and the recommended number of messages (M) to be sent to the sink. The majority of natural signals, according to are nonstationary and typically variable in the temporal and spatial domains. These have a direct impact on the reconstruction process and the number of measurements needed in CS; as a result, a fixed measurement set with a fixed transform basis (coefficient matrix) can lead to subpar performance (inaccurate measurement reconstruction). To take advantage of the local spatial correlation between sensed data from nearby sensor nodes, Ref. proposes an adaptive data-gathering scheme based on CS and an autoregressive (AR) model. By modifying the AR parameters, the proposed reconstruction system adjusts to the variance of sensed data. By assessing the recovery result and roughly estimating the number of measures needed to fulfil the accuracy need, the number of measurements is adaptively modified using the sensed data.

The compressed sparse function (CSF) approach is suggested by Xu et al. [64] to decrease the transmission overhead. The fundamental idea behind CSF is to compress felt data into sparse functions before sending them to the source, as opposed to encoding the sensed data by projecting it onto a basis on which it may be represented sparsely, as is the case with most CS-based systems. Using methods from polynomial approximation/interpolation theory, the source may recover the function and utilise it to derive data values that weren't supplied.

In particular, CSF only transmits this function to the sink because it discovers a function that maps the IDs of the sensors and their readings in a fairly simple manner. The sink can retrieve all N sensor values after it has recovered the function. the CSF technique can significantly lower message overhead while offering high recovery accuracy (better than the CDG scheme proposed by describe a generic CS framework for WSNs and the Internet of Things and demonstrate how to use the suggested framework to reconstruct the compressible data. The proposed framework is divided into three phases:

1. Information sensing to identify and compressively sample event signals;
2. Compressed sampling, in which the system collects data from networks; and
3. Reconstruction algorithms, in which the system precisely reconstructs the original signal from the compressed samples.

Different studies address the sampling problem and provide various methods to decrease the volume of data delivered, allowing just a portion of the sensors to detect the item or phenomena at once. With the understanding that the compression is at least achieved along the way to the sink, and is thus impacted by it, many research investigate how sensed data is sent to the sink. For instance, demonstrate that a random-walk-based sample may be employed for phenomenon awareness either at a sink or at other sensors without a sink, with little extra sampling, as opposed to the traditional uniform-sampling-based CS for function recovery. Offers an upper limit for the likelihood of a successful recovery with a certain error percentage since the distribution of the samples has a substantial impact on the recovery.

The calculated bound is an estimate of how many samples might be needed to recover a function using a certain basis and sampling strategy. In addition, analyse the sparsity of collecting non-uniform measurements while sampling along numerous random pathways and contend that random walk offers a more realistic solution for the data-gathering application in WSNs. According to the study, M independent random walks will define the MN measurement matrix. Particularly, each row of the M matrix corresponds to the set of vertices that the corresponding random walk visited. In order to implement the suggested random walk method, the article examines the necessary number of random walks (M) and their related lengths (the number of non-zero entries in each row).

In a cluster-based data-gathering technique proposed by the terrain is split into cells, and in each cell, a randomly chosen node serves as the cell head, collecting data from the cell members and transmitting it to the sink. Two forwarding strategies are suggested by one using centrally specified tree-based forwarding and the other using a gossip-based method. The projection method is based on random coefficients, much as propose HDACS as a further clustering-based hierarchical data aggregation approach that makes use of CS. To reduce the quantity of data communicated, HDACS specifically builds a multilayer hierarchical structure and adaptively establishes several compression thresholds depending on cluster sizes at various levels of the data aggregation tree. The encoding process is based on in which each cluster-head recovers (decodes) the messages it has received from its offspring (retrieves the original data), before compressing and transmitting it to its parent cluster-head.

Also recommend a compressibility-based clustering technique for hierarchical compressive data collection, driven by the need to use less power. Instead of using a random clustering method, the network in this research is broken down into a logical chain, and sensor nodes are categorised according to how compressible their data are. By picking a collection of nodes using greedy criteria depending on the compression ratio, this clustering method seeks to reduce the average compression ratio of all clusters. Then, using a mode threshold that depends on the number of nodes and the number of hops between a cluster head and a sink, it attempts to maximise the number of compressible clusters in order to choose the best transmission mode for each cluster.

Large-scale wireless sensor networks (WSNs), taking advantage of the spatial-temporal properties in the sensory data, in order to decrease the number of sensors involved in each CS measurement. The main argument made in this paper is that the measurement matrix should be created based on the representational framework and sensory information rather than the network environment. a multi-hop topology in which the sink node adaptively modifies the measurement formation according to the reconstruction of received measurements at each data-gathering period by fusing compressed sensing and network coding in the data-gathering method. The data aggregation carried out to balance the energy usage across sensor nodes is determined by the sink node in particular, makes use of the fact that, typically, only a small subset of network entities, such as links or nodes, are accountable for anomalies or degradation in network performance, as a small subset of congested links can be accountable for significant delays or high packet drop rates, and proposes using CS theory to identify these few entities based on end-to-end measurements. An investigation of the capacity and latency of data collection using compressive sensing in wireless sensor networks is provided by.

For both single-sink and multi-sink situations, the research takes into account a random topology and defines the capacity and delay performance enhancement that the CS paradigm may provide for data collection. A straightforward routing system for data collection with CS is specifically given for the single sink, and a constrained capacity in the order sense is offered. The proposed single-sink transmission scheme can achieve a capacity gain of (nM) over the baseline transmission scheme, and the delay can be decreased by a factor of (nlognM), where M is the number of random projections needed to reconstruct a snapshot and n is the number of randomly deployed nodes. This is demonstrated in particular by the suggested routing scheme with pipelining scheduling algorithm for data gathering. Their architecture demonstrates that the per-session capacity of data gathering with CS for the multi-sink case is (nnWMndnslogn), and the per-session delay is (Mnlogn), where W is the data rate. The number of source nodes chosen at random is ns, whereas the number of sinks in the network is nd. They use simulations to test the theoretical findings for the capacity scaling rules in single-sink and multi-sink networks.

Medium Access Control (MAC)

The medium access control (MAC) mechanism, which has a significant effect on various performance factors like reliability, latency, channel use, and power consumption (which impacts the lifetime of a sensor in particular and the network in general), is the next layer that we proceed to. Despite the fact that several access protocols for shared-channel networks wired and wireless have been proposed over the years owing to their distinct characteristics and needs, a great deal of research has been done on MAC protocols specifically designed for WSN. Numerous WSN MAC protocols were created to conform to different traffic patterns. As a result, in the follow-up, we provide a brief description of the WSN-MAC protocol for those who can support it but aren't particularly focused on data collection. We just examine a small portion of the extensive body of literature on the subject and the different MAC protocols developed throughout time [91]–[96].

One of the key issues with WSN is energy consumption, which must be taken into account while designing protocols and algorithms at all tiers of the protocol stack, as was already mentioned. The transceiver is the component of a sensor or Internet of Things device that uses the most power, whether it is sending data or is just awake and monitoring current traffic [97]–[104]. Adopting a duty-cycle method, in which the device sleeps the most of the time (its transceiver is in low power mode), and is awake just briefly to send or receive data, is one of the more popular ways to save power. Another critical element of wireless sensor networks (WSNs) is channel usage. In a typical WSN, airtime is a valuable network resource when numerous devices are attempting to deliver reports concurrently.

Fundamental challenges include coordinating amongst users to minimise accidents and preventing users from consuming the channel for extended periods of time, especially when the network is congested with several devices in the same area. Be aware that these problems, even when they are not often reported, may have a significant impact on performance in a dense network architecture. In light of this, an essential element of the functioning and effectiveness of any such system is making effective use of the channel (air time). The importance attributed to the creation of medium access control (MAC) protocols that are unique to WSNs is justified by these two crucial factors. To address the various WSN aims and needs, several alternative protocols have been proposed .In particular, duty-cycled-based MAC protocols for WSNs are the subject of this work.

Duty-Cycle MAC Protocols

Duty-cycle MAC techniques are often categorised as synchronous or asynchronous. The awake time interval in synchronous protocols is synchronised such that all devices are awake (or sleeping) at the same intervals .The relatively short waking time periods may be quite crowded and vulnerable to accidents because of this. In order to reduce this congestion and enable more devices to transmit in each cycle, many synchronous protocols have developed methods. One such protocol is DW-MAC which allots the awake period for transmission reservations that will be carried out during the sleep phase.

Each device in asynchronous protocols has a different wake-up schedule. Setting a rendezvous time when both the transmitter and the receiver are awake and creating a signalling method that lets both parties know they are awake and able to talk are thus the key challenges. The two subcategories of asynchronous MAC protocols are transmitter- and receiver-initiated. In protocols involving transmitters, the transmitter starts the transmission by snatching the channel while it waits for the designated receiver to awaken. For instance, in B-MAC before transmitting the data, the transmitter sends a lengthy preamble to capture the channel while it waits for the target receiver to awaken and respond. In the protocol, the transmitter sends a series of brief preambles that enable the target receiver to interrupt and signal that it is awake. In the transmitter discovers the receiver's wake-up time and begins the preamble broadcast just before that wake-up time.

The second strategy, known as the receiver-initiated paradigm, depends on the receiver to start the data exchange whenever it is awake and prepared to receive data. In RI-MAC the fundamental receiver-initiated MAC idea was first established. Under this concept, once a receiver wakes up, it sends a specified preamble to prospective transmitters to let them know that it is awake and prepared to receive data. A number of protocols adopted the RI-MAC paradigm and proposed improvements. Some protocols made an effort to minimise the energy used when a sender is awake while waiting for their intended recipient to awaken.

As an example, and AP-MAC proposed that each transmitter would learn its receiver's anticipated wake-up time and, rather than remaining awake while waiting for its designated receiver to wake up, will awaken immediately before its intended receiver's wake-up instance which aims to reduce the amount of time a receiver and, consequently, its potential transmitters stay awake, suggests another receiver-initiated improvement. It does this by trying to ascertain whether there are any pending packets for transmission and whether it needs to stay awake or if it can go back to sleep after probing the channel. The improvement depends on an extra frame called a "auto-ack" that is delivered by pending transmitters and follows the receiver's probing packet before the data transfer may continue. A receiver can determine whether there is traffic being sent by decoding a superposition of several "auto-ack" frames.

Even though the energy saved per cycle is insignificant, the total savings per day can be sizable because a device wakes up frequently to probe the channel. Two improvements are suggested by RIVER-MAC, one to shorten the amount of time a sender must wait for the intended receiver to awaken, and the other to enhance the RI-MAC collision resolution mechanism by allowing an active receiver to continue controlling the channel even after the collision resolution mechanism has been invoked, more specifically during the silent backoff interval. In order to deal with the persistent collisions that are prevalent in dense networks and under severe traffic loads when several devices are attempting to transmit to the same entity, MAR-RiMAC proposed an adjustment to the receiver-initiated method, and in particular RI-MAC (sink or relay). The reservation-based approach used by MAR-RiMAC uses brief signals that may be broadcast concurrently as reservations. The selected receiver makes a communication request and polls the devices consecutively, with no idle periods, after decoding the devices' identities [105]–[109].

Depending on EH necessitates modifications that often have to do with the energy source that was gathered. One important consideration in determining whether or not a scheme or protocol can be adopted by a network that relies on EH, and can be the main factor affecting their performance, is how to balance the harvested energy and the consumed energy. The whole network stack must be modified to handle EH-based sensors, including the MAC sublayer provide an adaptation of the receiver-initiated duty-cycle MAC protocol for energy-harvesting-powered wireless sensor networks, where in addition to the typical MAC difficulties, both the transmitter and the receiver must have enough power for successful transmission.

MAC Protocols for Other Setups

Next, we look at a few MAC protocols and MAC modifications for a variety of setups, including multi-channel, multi-radio, busy-tone utilisation, and other approaches than the duty-cycle method. In order to avoid interference from hidden terminals, adopts the conventional busy-tone scheme and allots a sub-channel for control. While receiving data on the data channel, a busy signal is transmitted on the control channel to inform nearby nodes of the ongoing transmission. Without the use of a control channel, employs multiple orthogonal radio channels and enables devices to dynamically choose the channels for their transmissions based on the channel conditions they sense. As a result, EM-MAC can avoid using channels that are currently jammed, interfered, or heavily loaded. The traffic load sent by a node is typically erratic in both space and time. Due to their tasks, topological location, and the amount of traffic they must relay, various nodes must send varying traffic loads. Furthermore, different traffic loads caused by events or requests can cause the same node to experience different loads at different times. A variety of studies have thus investigated an adaptive duty-cycle approach. For instance, have created a self-adaptive sleep/wake scheduling method based on reinforcement learning. Each node (device) in the proposed method divides the time into time-slots, which are not always synchronised between adjacent nodes. In each time slot, each node chooses whether to sleep or wake up, and while awake, it chooses whether to listen or transmit. The choice is made via Q-learning and is based on the system's assessment of its present condition and the circumstances of its neighbours.

create a different duty-cycle strategy that makes use of two radios: the main radio transceiver and an auxiliary wake-up When necessary, the wake-up radio, a low-power receiver that is activated by an outside event, may activate the primary transceiver. Through physical tests and measurements, give a thorough assessment of a particular Modulation assessing it for several performance metrics and contrasting it with other wake-up radio-based systems. The WuR hardware architecture that the authors describe and simulate is compared against four popular MAC protocols for WSN under three actual network A wake-up receiver with extremely low power consumption (1.3 W), high quick response (wake-up time of 130 s), and selective addressing is designed and prototyped by and described in relation to a wireless sensor node. The authors describe ALBA-WUR, a cross-layer method for data collection in wireless sensing systems, by leveraging their WRx. Similar to duty-cycled MAC protocols, wake-up radio-based protocols distinguish between receiver-initiated), which adopts the RI-MAC paradigm so that when a receiving node is ready to collect data, it wakes up all the nodes in its neighbourhood by broadcasting a wake-up call, and transmitter-initiated), which wakes up its potential receivers

Propose an energy-harvesting-based MAC protocol for cognitive radio networks (CRNs), in which secondary users (SUs) harvest energy from primary users' (PUs') broadcasts. As a result, the recommended protocol interlaces data transmissions from SUs within the transmission holes of these PUs. The mismatch between the little quantity of energy harvested for each PU's transmission and the energy needed for each SU data transfer is taken into account in the suggested energy-harvesting/data-transmission schedule.

Next, we discuss a number of WSN MAC protocols that were created specifically to take advantage of certain data-gathering configurations seen in WSN and IoT networks (e.g., that the traffic patterns are always from sensors to the sink, or that there exists a set of predefined messages that need to be sent). A data gathering technique is designed and examined by using information theoretic concepts. Each sensor in the proposed protocol must send one of a bank of predetermined messages to a sink. The protocol makes the assumption that there are many sensors in use and develops a method for a sink (or relay) to simultaneously gather messages from up to K sensors without knowing in advance which sensors will transmit and without the need for any synchronisation, coordination, or management overhead. develops a wake-up that may dramatically decrease end-to-end latency by taking use of the fact that traffic in data-gathering applications travels in a certain direction (towards a single or many sinks). The awake schedule of communication nodes is laid out in detail in D-3 so that packets may be delivered progressively toward their destinations without a node having to wait for its next-hop relay to wake up (i.e., the wake-up schedule is such that a relay wakes up in time to receive a packet just received by its predecessor).

WSN Data Collection Routing

As we continue to ascend the levels, we talk about Network layer-related concerns in this part. A brief overview of WSN routing protocols comes first. We observe that other sections of this survey also made reference to aspects of routing. We concentrate primarily on the well-known and more recent protocols. We focus on routing methods appropriate for data collection rather than giving a thorough analysis of routing protocols in multihop WSNs. A schematic grouping of the articles that were addressed into major issues. The subjects are selected such that the theme on each one may be covered by several articles, similar to the schematic division in the other sections to avoid having too many. The division of the papers is a little arbitrary: some articles may be found in more than one subject, while others are solely associated with that topic.

Mobile sensors are used by to obtain area coverage. After the first random deployment, these mobile sensors may be moved and repositioned to fill up gaps. The authors recommend a two-phase strategy. According to the first, the monitoring area is recognised (by the BS) after the first random deployment, and mobile nodes are moved to fill up any monitoring gaps that were found. This is done in an effort to guarantee that the AoI is completely covered by the static and relocated sensors. The suggested method schedules the sensor activities (awakening and transmission timings) in the second stage to reduce the nodes' energy usage while collecting and transmitting data to the base station. The research makes a distinction between cluster chiefs and "regular" nodes to achieve this. Boukerche and provide a survey that examines the algorithms and methods linked to the connectivity-coverage problems in WSN.

WSN architectures and designs may sometimes be more application-focused. For instance, suggest a sensor node architecture for energy-efficient trash management in the context of smart cities that employs low-cost and low-power components. The design suggested in uses LoRa LPWAN (low-power wide-area network) technology for real-time data transmission to gather the measured data in a distant data collection center. It also recommends a node architecture for sensing the fill level of garbage bins. Propose a concept for a sensor node that can identify water on house floors and provide early notice of water breaches. The network components (flood sensing nodes, actuator nodes, and a control centre are shown in the study, along with their software implementations. Communication within the sensor network is based on the standard. A low-cost system focused on agriculture is presented by .A farmer may get all the data required to manage crop irrigation effectively in real time with the help of the recommended system, which is based on LoRa technology and can gather numerous parameters, including humidity, ambient temperature, soil moisture, and temperature. The created wireless sensor node has very low power consumption thanks to hardware and software optimization.

Due to the difficulties in designing IoT devices, such as multipath routing, network congestion, and resource limitations (charging, connectivity, and computational resources), ad hoc and commercial data transmission methods are not suited for sensor networks. Because global trying to address in WSNs is too challenging to maintain, several sensor nodes are installed for specialised applications. This considerable number may cause nodes in the same location to produce duplicated data and send it to BS. This causes network traffic and transmission waste, and this in turn increases energy usage. Because replacement part or replenishment is not achievable in the majority of WSN applications, limiting rechargeable battery is another major resource that a sensor node must contend with. Because WSN uses a wireless communication channel, there is a higher chance of data transmission collisions, which affects data transmission. The aforementioned concerns must be taken into account while developing a new collection of data scheduling algorithm in order to meet its criteria for coverage area, greater accuracy, and low latency.

CHAPTER 15

FUTURE OF WIRELESS SENSOR NETWORK

Asha. KS, Associate Professor,
Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka – 562112
Email Id- ks.asha@jainuniversity.ac.in

Today, we can observe that the WSN have been effectively applied into the many areas where in certain circumstances, the human involvement is also not required. This is due to improvements in electronics, routing protocols, and security problems. Therefore, the development of sophisticated functionality in wireless sensor networks demonstrates that they have a very broad range of uses. Additionally, it seems that there are very few fields in which all the wireless sensor network should be used. The numerous applications for wireless sensor networks in today’s use patterns [110], [111].

Military:

Today's new and growing technologies, including networks, enable military actions by reliably and quickly getting crucial information to the correct people or organisations at the right moment. This is a very difficult assignment. Combat actions are more effectively conducted as a result. To satisfy the demands of today, the latest technologies must be swiftly incorporated into a complete architecture [61], [112], [113].

It is essential that situation awareness be improved applications in the military that are crucial include tracking enemy unit movements on land or at sea, detecting intrusions on bases, identifying chemical or biological threats, and providing logistics for urban combat roles in medical facilities and home care. BWSN development is necessary to address security management, better signal integration, and visualization.

E-services for healthcare, often known as health, have lately drawn a lot of interest from the scientific community and the business community since using the Internet has become a daily activity for people. The initiatives listed below are some of the ongoing ones that use WSN in healthcare:

1. A suggested structure for patient tracking and supervision.
2. A low power wireless personal area internet backbone system designed for detecting residential and extended care facilities.
3. Research wearable personal health systems that track and analyse human vital indicators via WSN.

Controlling: changing items depending on use patterns and operational circumstances. It has been revealed how the sensors included into the structures allow for circumstance monitoring of these investments. When sensors flag a potential issue, assets may be evaluated thanks to wireless sensing. As a result of avoiding dangerous failure, maintenance expenses will be lower. These implementations include sensors embedded in large structures, heavy-duty railways, and polymer and encapsulation.

Commercial and industrial:

Wireless sensor networks (WSNs) have successfully been used in systems like administrative information and information collecting, demonstrating their ability to meet the demands of industrial applications. Monitoring temperature, flow-level, pressure, and saturation indicators, which may also be applied in smart water and smart gas pipe systems, is one of the essential and indispensable applications of WSNs in manufacturing.

Smart home/Smart office: Korea will do research on smart houses. It is clear that a smart house might provide unique behaviours for a particular person. And building a smart house will undoubtedly need much planning and labour. There are several examples of goods available today that can carry out certain tasks that are seen as being a component of a smart home, such as: Smart metre and Smart dustbin [114], [115].

Traffic management and maintenance: To effectively manage rush hour traffic, a real-time automated traffic data gathering system must be used. They defined ITS (ntelligent Transport System as the surface transportation industry's use of computer, information, and sensor technologies. The purpose of the vehicle tracking programme is to find a certain vehicle or moving item, analyze it as it moves, and ensure that traffic flow and safety are improved.

Questions for Revision

1. What are the Wireless sensor network limitations?
2. What is wireless sensor?
3. How wireless sensor is useful?
4. How the sensor plays major important role in the life?
5. How the connectivity is working in the sensor?
6. How wireless sensor is used in the embedded system?
7. How the WSN is useful in the data allocation?
8. How WSN is effective in the day to day life?
9. How WSN is important in the signal processing?
10. How WSN is used as a primary signal development?

Bibliography

[1] J. C. López-Ardao, R. F. Rodríguez-Rubio, A. Suárez-González, M. Rodríguez-Pérez, and M. E. Sousa-Vieira, "Current Trends on Green Wireless Sensor Networks," *Sensors*, vol. 21, no. 13, p. 4281, Jun. 2021, doi: 10.3390/s21134281.

[2] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," *Procedia Comput. Sci.*, vol. 183, pp. 486–492, 2021, doi: 10.1016/j.procs.2021.02.088.

[3] A. P. Atmaja, A. El Hakim, A. P. A. Wibowo, and L. A. Pratama, "Communication Systems of Smart Agriculture Based on Wireless Sensor Networks in IoT," *J. Robot. Control*, vol. 2, no. 4, 2021, doi: 10.18196/jrc.2495.

[4] T. Kim, L. F. Vecchietti, K. Choi, S. Lee, and D. Har, "Machine Learning for Advanced Wireless Sensor Networks: A Review," *IEEE Sensors Journal*. 2021. doi: 10.1109/JSEN.2020.3035846.

[5] Q. Liu *et al.*, "Cluster-based flow control in hybrid software-defined wireless sensor networks," *Comput. Networks*, 2021, doi: 10.1016/j.comnet.2020.107788.

[6] D. Pásztor, P. Ekler, and J. Levendovszky, "Energy-Efficient Routing in Wireless Sensor Networks," *Acta Cybern.*, 2021, doi: 10.14232/ACTACYB.288351.

[7] S. Nashwan, "AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment," *Egypt. Informatics J.*, 2021, doi: 10.1016/j.eij.2020.02.005.

[8] M. A. Alharbi, M. Kolberg, and M. Zeeshan, "Towards improved clustering and routing protocol for wireless sensor networks," *Eurasip J. Wirel. Commun. Netw.*, 2021, doi: 10.1186/s13638-021-01911-9.

[9] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: An up-to-date survey," *Applied System Innovation*. 2020. doi: 10.3390/asi3010014.

[10] Y. Deng, C. Han, J. Guo, and L. Sun, "Temporal and spatial nearest neighbor values based missing data imputation in wireless sensor networks," *Sensors*, 2021, doi: 10.3390/s21051782.

[11] C. Y. Wang, C. H. Tsai, S. C. Wang, C. Y. Wen, R. C. H. Chang, and C. P. Fan, "Design and implementation of lora-based wireless sensor network with embedded system for smart agricultural recycling rapid processing factory," *IEICE Trans. Inf. Syst.*, 2021, doi: 10.1587/transinf.2020NTI0001.

[12] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni, and Y. Yang, "MSCR: multidimensional secure clustered routing scheme in hierarchical wireless sensor networks," *Eurasip J. Wirel. Commun. Netw.*, 2021, doi: 10.1186/s13638-020-01884-1.

[13] A. Al Guqhaiman, O. Akanbi, A. Aljaedi, and C. E. Chow, “A Survey on MAC Protocol Approaches for Underwater Wireless Sensor Networks,” *IEEE Sensors Journal*. 2021. doi: 10.1109/JSEN.2020.3024995.

[14] J. Lloret, S. Sendra, L. Garcia, and J. M. Jimenez, “A wireless sensor network deployment for soil moisture monitoring in precision agriculture,” *Sensors*, 2021, doi: 10.3390/s21217243.

[15] L. I. Peng, Y. U. Xiaotian, X. U. He, and W. A. N. G. Ruchuan, “Secure Localization Technology Based on Dynamic Trust Management in Wireless Sensor Networks,” *Chinese J. Electron.*, 2021, doi: 10.1049/cje.2021.05.019.

[16] S. Wang, H. You, Y. Yue, and L. Cao, “A novel topology optimization of coverage-oriented strategy for wireless sensor networks,” *Int. J. Distrib. Sens. Networks*, 2021, doi: 10.1177/1550147721992298.

[17] S. J. Bhat and K. V. Santhosh, “A Method for Fault Tolerant Localization of Heterogeneous Wireless Sensor Networks,” *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3063160.

[18] A. Jamil, M. Q. Ali, and M. E. Abd Alkhalec, “Sinkhole attack detection and avoidance mechanism for RPL in wireless sensor networks,” *Ann. Emerg. Technol. Comput.*, 2021, doi: 10.33166/AETiC.2021.05.011.

[19] Y. Yue, H. You, S. Wang, and L. Cao, “Improved whale optimization algorithm and its application in heterogeneous wireless sensor networks,” *Int. J. Distrib. Sens. Networks*, 2021, doi: 10.1177/15501477211018140.

[20] J. Zhang and H. Mao, “Multi-factor identity authentication protocol and indoor physical exercise identity recognition in wireless sensor network,” *Environ. Technol. Innov.*, 2021, doi: 10.1016/j.eti.2021.101671.

[21] Q. Ding, R. Zhu, H. Liu, and M. Ma, “An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks,” *Electronics (Switzerland)*. 2021. doi: 10.3390/electronics10131539.

[22] A. Zhang, M. Sun, J. Wang, Z. Li, Y. Cheng, and C. Wang, “Deep reinforcement learning-based multi-hop state-aware routing strategy for wireless sensor networks,” *Appl. Sci.*, 2021, doi: 10.3390/app11104436.

[23] M. L. Borham, G. Khoriba, and M. S. Mostafa, “Data collection protocols for wireless sensor networks,” *Int. J. Electr. Comput. Eng. Syst.*, 2021, doi: 10.32985/IJECES.12.4.4.

[24] L. Hamami and B. Nassereddine, “Factors Influencing the Use of Wireless Sensor Networks in the Irrigation Field,” *Int. J. Adv. Comput. Sci. Appl.*, 2021, doi: 10.14569/IJACSA.2021.0120382.

[25] R. S. Raghav, U. Prabu, M. Rajeswari, D. Saravanan, and K. Thirugnanasambandam, “Cuddle death algorithm using ABC for detecting unhealthy nodes in wireless sensor networks,” *Evol. Intell.*, 2022, doi: 10.1007/s12065-021-00570-5.

[26] P. K. Kodoth and G. Edachana, “An energy efficient data gathering scheme for wireless sensor networks using hybrid crow search algorithm,” *IET Commun.*, 2021, doi:

10.1049/cmu2.12128.

[27] N. Ajmi, A. Helali, P. Lorenz, and R. Mghaieth, "MWCSGA-Multi weight chicken swarm based genetic algorithm for energy efficient clustered wireless sensor network," *Sensors (Switzerland)*, 2021, doi: 10.3390/s21030791.

[28] H. Yang, X. Zhang, and F. Cheng, "A Novel Algorithm for Improving Malicious Node Detection Effect in Wireless Sensor Networks," *Mob. Networks Appl.*, 2021, doi: 10.1007/s11036-019-01492-4.

[29] S. Shukry, "Stable routing and energy-conserved data transmission over wireless sensor networks," *Eurasip J. Wirel. Commun. Netw.*, 2021, doi: 10.1186/s13638-021-01925-3.

[30] T. N. Jones, G. N. E. Roland Christian, and P. Felix, "Wireless sensors network for monitoring linear infrastructures using MQTT protocol on raspberry Pi with nRF24l01 and node-red," *Instrum. Mes. Metrol.*, 2021, doi: 10.18280/i2m.200501.

[31] S. Karimi-Bidhendi, J. Guo, and H. Jafarkhani, "Energy-Efficient Node Deployment in Heterogeneous Two-Tier Wireless Sensor Networks with Limited Communication Range," *IEEE Trans. Wirel. Commun.*, 2021, doi: 10.1109/TWC.2020.3023065.

[32] F. fei Wang and H. feng Hu, "Multi-path data fusion method based on routing algorithm for wireless sensor networks," *Int. J. Comput. Appl.*, 2021, doi: 10.1080/1206212X.2019.1652786.

[33] F. Wu, X. Li, L. Xu, P. Vijayakumar, and N. Kumar, "A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks with IoT Notion," *IEEE Syst. J.*, 2021, doi: 10.1109/JSYST.2020.2981049.

[34] I. A. A. E. M. And and S. M. Darwish, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3098933.

[35] J. Qin, J. Wang, L. Shi, and Y. Kang, "Randomized Consensus-Based Distributed Kalman Filtering over Wireless Sensor Networks," *IEEE Trans. Automat. Contr.*, 2021, doi: 10.1109/TAC.2020.3026017.

[36] E. Alzahrani and F. Bouabdallah, "Qmmac: Quorum-based multichannel mac protocol for wireless sensor networks," *Sensors*, 2021, doi: 10.3390/s21113789.

[37] A. Jabbari and J. B. Mohasefi, "Improvement of a User Authentication Scheme for Wireless Sensor Networks Based on Internet of Things Security," *Wirel. Pers. Commun.*, 2021, doi: 10.1007/s11277-020-07811-3.

[38] A. Aghaei, J. Akbari Torkestani, H. Kermajani, and A. Karimi, "LA-Trickle: A novel algorithm to reduce the convergence time of the wireless sensor networks," *Comput. Networks*, 2021, doi: 10.1016/j.comnet.2021.108241.

[39] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks," *IEEE Trans. Eng. Manag.*, 2021, doi: 10.1109/TEM.2019.2953889.

[40] T. Q. Z. Cesar, P. A. M. Leal, O. C. Branquinho, and F. A. M. Miranda, "Wireless sensor network to identify the reduction of meteorological gradients in greenhouse in subtropical conditions," *J. Agric. Eng.*, 2021, doi: 10.4081/jae.2020.1105.

[41] Z. Zeng, F. Zeng, X. Han, H. Elkhouchlaa, Q. Yu, and E. Lü, "Real-time monitoring of environmental parameters in a commercial gestating sow house using a zigbee-based wireless sensor network," *Appl. Sci.*, 2021, doi: 10.3390/app11030972.

[42] S. Karim, F. K. Shaikh, K. Aurangzeb, B. S. Chowdhry, and M. Alhussein, "Anchor Nodes Assisted Cluster-Based Routing Protocol for Reliable Data Transfer in Underwater Wireless Sensor Networks," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3063295.

[43] S. Arockiaraj, K. Makkithaya, and N. Harishchandra Hebbar, "Energy-Efficient Hybrid Protocol for Wireless Sensor Networks," *Int. J. Comput. Networks Appl.*, 2021, doi: 10.22247/ijcna/2021/210728.

[44] A. Rajput and V. B. Kumaravelu, "FCM clustering and FLS based CH selection to enhance sustainability of wireless sensor networks for environmental monitoring applications," *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-020-02159-9.

[45] A. Panchal and R. K. Singh, "EHCR-FCM: Energy Efficient Hierarchical Clustering and Routing using Fuzzy C-Means for Wireless Sensor Networks," *Telecommun. Syst.*, 2021, doi: 10.1007/s11235-020-00712-7.

[46] S. Mukase, K. Xia, and A. Umar, "Optimal base station location for network lifetime maximization in wireless sensor network," *Electron.*, 2021, doi: 10.3390/electronics10222760.

[47] P. Kathiroli and K. Selvadurai, "Energy efficient cluster head selection using improved Sparrow Search Algorithm in Wireless Sensor Networks," *J. King Saud Univ. - Comput. Inf. Sci.*, 2022, doi: 10.1016/j.jksuci.2021.08.031.

[48] A. P. Abidoye and B. Kabaso, "Energy-efficient hierarchical routing in wireless sensor networks based on fog computing," *Eurasip J. Wirel. Commun. Netw.*, 2021, doi: 10.1186/s13638-020-01835-w.

[49] H. Ahmadi and R. Bouallegue, "An accurate target tracking method in wireless sensor networks," *Indones. J. Electr. Eng. Comput. Sci.*, 2022, doi: 10.11591/ijeecs.v25.i3.pp1589-1598.

[50] M. A. Jamshed, K. Ali, Q. H. Abbasi, M. A. Imran, and M. Ur-Rehman, "Challenges, Applications, and Future of Wireless Sensors in Internet of Things: A Review," *IEEE Sensors Journal*. 2022. doi: 10.1109/JSEN.2022.3148128.

[51] N. Temene, C. Sergiou, C. Georgiou, and V. Vassiliou, "A Survey on Mobility in Wireless Sensor Networks," *Ad Hoc Networks*. 2022. doi: 10.1016/j.adhoc.2021.102726.

[52] J. Mo, Z. Hu, and W. Shen, "A Provably Secure Three-Factor Authentication Protocol Based on Chebyshev Chaotic Mapping for Wireless Sensor Network," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3146393.

[53] H. Luo, X. Wang, Z. Xu, C. Liu, and J. S. Pan, "A software-defined multi-modal wireless

sensor network for ocean monitoring," *Int. J. Distrib. Sens. Networks*, 2022, doi: 10.1177/15501477211068389.

[54] I. D. I. Saeedi and A. K. M. Al-Qurabat, "Perceptually Important Points-Based Data Aggregation Method for Wireless Sensor Networks," *Baghdad Sci. J.*, 2022, doi: 10.21123/bsj.2022.19.4.0875.

[55] M. Ali, I. A. Abd El-Moghith, M. N. El-Derini, and S. M. Darwish, "Wireless sensor networks routing attacks prevention with blockchain and deep neural network," *Comput. Mater. Contin.*, 2022, doi: 10.32604/cmc.2022.021305.

[56] T. Palanisamy, D. Alghazzawi, S. Bhatia, A. A. Malibari, P. Dadheech, and S. Sengan, "Improved Energy Based Multi-Sensor Object Detection in Wireless Sensor Networks," *Intell. Autom. Soft Comput.*, 2022, doi: 10.32604/iasc.2022.023692.

[57] S. Han, B. Zhang, and S. Chai, "A novel auxiliary hole localization algorithm based on multidimensional scaling for wireless sensor networks in complex terrain with holes," *Ad Hoc Networks*, 2021, doi: 10.1016/j.adhoc.2021.102644.

[58] T. Stephan, K. Sharma, A. Shankar, S. Punitha, V. Varadarajan, and P. Liu, "Fuzzy-Logic-Inspired Zone-Based Clustering Algorithm for Wireless Sensor Networks," *Int. J. Fuzzy Syst.*, 2021, doi: 10.1007/s40815-020-00929-3.

[59] N. Naji, M. R. Abid, N. Krami, and D. Benhaddou, "Energy-aware wireless sensor networks for smart buildings: A review," *J. Sens. Actuator Networks*, 2021, doi: 10.3390/jsan10040067.

[60] P. Rawat and S. Chauhan, "Clustering protocols in wireless sensor network: A survey, classification, issues, and future directions," *Computer Science Review*. 2021. doi: 10.1016/j.cosrev.2021.100396.

[61] F. Carrabs, C. D'Ambrosio, and A. Raiconi, "Optimization of sensor battery charging to maximize lifetime in a wireless sensors network," *Optim. Lett.*, 2021, doi: 10.1007/s11590-020-01533-y.

[62] Z. Tsiropoulos, I. Gravalos, E. Skoubris, V. Poulek, T. Petrík, and M. Libra, "A Comparative Analysis Between Battery- and Solar-Powered Wireless Sensors for Soil Water Monitoring," *Appl. Sci.*, 2022, doi: 10.3390/app12031130.

[63] A. Rajab, "Fault Tolerance Techniques for Multi-Hop Clustering in Wireless Sensor Networks," *Intell. Autom. Soft Comput.*, 2022, doi: 10.32604/IASC.2022.021922.

[64] K. Veerabadrappa and S. C. Lingareddy, "Secure Routing using Multi-Objective Trust Aware Hybrid Optimization for Wireless Sensor Networks," *Int. J. Intell. Eng. Syst.*, 2022, doi: 10.22266/IJIES2022.0228.49.

[65] M. Sajwan, A. K. Sharma, and K. Verma, "IPRA: Iterative Parent-Based Routing Algorithm for Wireless Sensor Networks," *Wirel. Pers. Commun.*, 2022, doi: 10.1007/s11277-022-09515-2.

[66] R. Kanthavel and R. Dhaya, "Wireless underground sensor networks channel using energy efficient clustered communication," *Intell. Autom. Soft Comput.*, 2022, doi:

10.32604/IASC.2022.019779.

[67] A. Ojha and P. Chanak, “Multiobjective Gray-Wolf-Optimization-Based Data Routing Scheme for Wireless Sensor Networks,” *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2021.3105425.

[68] G. Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, “An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs,” *Sensors*, 2022, doi: 10.3390/s22041407.

[69] L. Liu, G. Han, Z. Xu, J. Jiang, L. Shu, and M. Martinez-Garcia, “Boundary Tracking of Continuous Objects Based on Binary Tree Structured SVM for Industrial Wireless Sensor Networks,” *IEEE Trans. Mob. Comput.*, 2022, doi: 10.1109/TMC.2020.3019393.

[70] R. Krishnan *et al.*, “An Intrusion Detection and Prevention Protocol for Internet of Things Based Wireless Sensor Networks,” *Wirel. Pers. Commun.*, 2022, doi: 10.1007/s11277-022-09521-4.

[71] M. Dhurgadevi and P. Sakthivel, “An Analysis of Wind Energy Generation by Opting the Better Placement of Wind Turbine by Artificial Neural Network and to Improve the Energy Efficiency of Wireless Sensor Network,” *Wirel. Pers. Commun.*, 2022, doi: 10.1007/s11277-021-09255-9.

[72] X. Huang *et al.*, “Toward Efficient Data Trading in AI Enabled Reconfigurable Wireless Sensor Network Using Contract and Game Theories,” *IEEE Trans. Netw. Sci. Eng.*, 2022, doi: 10.1109/TNSE.2020.3013064.

[73] J. Wang, L. Cheng, Y. Tu, and S. Gu, “A Novel Localization Approach for Irregular Wireless Sensor Networks Based on Anchor Segmentation,” *IEEE Sens. J.*, 2022, doi: 10.1109/JSEN.2022.3143826.

[74] K. Karunanithy and B. Velusamy, “An efficient data collection using wireless sensor networks and internet of things to monitor the wild animals in the reserved area,” *Peer-to-Peer Netw. Appl.*, 2022, doi: 10.1007/s12083-021-01289-x.

[75] M. Sajitha, D. Kavitha, and P. C. Reddy, “An optimized whale based replication node prediction in wireless sensor network,” *Wirel. Networks*, 2022, doi: 10.1007/s11276-022-02928-8.

[76] M. Sheikh-Hosseini and S. R. Samareh Hashemi, “Connectivity and coverage constrained wireless sensor nodes deployment using steepest descent and genetic algorithms,” *Expert Syst. Appl.*, 2022, doi: 10.1016/j.eswa.2021.116164.

[77] B. Zhao and X. Zhao, “Deep Reinforcement Learning Resource Allocation in Wireless Sensor Networks With Energy Harvesting and Relay,” *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2021.3094465.

[78] M. K. R. Al-Juaifari, J. M. A. M. Mona, and Z. A. Abbas, “New method for route efficient energy calculations with mobile-sink for wireless sensor networks,” *Indones. J. Electr. Eng. Comput. Sci.*, 2022, doi: 10.11591/ijeecs.v25.i1.pp365-374.

[79] Y. C. Liu, T. C. Lin, and M. T. Lin, “Indirect/Direct Learning Coverage Control for Wireless Sensor and Mobile Robot Networks,” *IEEE Trans. Control Syst. Technol.*, 2022, doi:

10.1109/TCST.2021.3061513.

[80] F. Corti, A. Laudani, G. M. Lozito, A. Reatti, A. Bartolini, and L. Ciani, “Model-Based Power Management for Smart Farming Wireless Sensor Networks,” *IEEE Trans. Circuits Syst. I Regul. Pap.*, 2022, doi: 10.1109/TCSI.2022.3143698.

[81] P. Zhou, S. Wang, Z. Jin, G. Huang, J. Zhu, and X. Liu, “Data reconstruction of wireless sensor network and zonal demand control in a large-scale indoor space considering thermal coupling,” *Buildings*, 2022, doi: 10.3390/buildings12010015.

[82] N. Marriwala, “Energy Harvesting System Design and Optimization Using High Bandwidth Rectenna for Wireless Sensor Networks,” *Wirel. Pers. Commun.*, 2022, doi: 10.1007/s11277-021-08918-x.

[83] S. Sirisinahal, M. R. Murthy, S. C. Ramu, and C. R. K. Reddy, “Improvement of Data Security and Privacy in the Wireless Sensor Network Using Elliptical Curve Cryptography,” *Int. J. Mech. Eng.*, 2022.

[84] X. Xu, J. Tang, and H. Xiang, “Data Transmission Reliability Analysis of Wireless Sensor Networks for Social Network Optimization,” *J. Sensors*, 2022, doi: 10.1155/2022/3842722.

[85] A. Sedighimanesh, H. Zandhessami, M. Alborzi, and M. Khayyatian, “Training and Learning Swarm Intelligence Algorithm (TLSIA) for Selecting the Optimal Cluster Head in Wireless Sensor Networks,” *J. Inf. Syst. Telecommun.*, 2022, doi: 10.52547/jist.15638.10.37.37.

[86] F. Tossa, W. Abdou, K. Ansari, E. C. Ezin, and P. Gouton, “Area Coverage Maximization under Connectivity Constraint in Wireless Sensor Networks,” *Sensors*, 2022, doi: 10.3390/s22051712.

[87] P. Mohan, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalaf, and S. Ulaganathan, “Improved Metaheuristics-Based Clustering with Multihop Routing Protocol for Underwater Wireless Sensor Networks,” *Sensors*, 2022, doi: 10.3390/s22041618.

[88] M. A. Khan, T. M. Ghazal, S. W. Lee, and A. Rehman, “Data fusion-based machine learning architecture for intrusion detection,” *Comput. Mater. Contin.*, 2022, doi: 10.32604/cmc.2022.020173.

[89] J. Feng, F. Chen, and H. Chen, “Data Reconstruction Coverage Based on Graph Signal Processing for Wireless Sensor Networks,” *IEEE Wirel. Commun. Lett.*, 2022, doi: 10.1109/LWC.2021.3120276.

[90] S. Rani, H. Babbar, P. Kaur, M. D. Alshehri, and S. H. A. Shah, “An Optimized Approach of Dynamic Target Nodes in Wireless Sensor Network Using Bio Inspired Algorithms for Maritime Rescue,” *IEEE Trans. Intell. Transp. Syst.*, 2022, doi: 10.1109/TITS.2021.3129914.

[91] Y. Yang and J. Chen, “Comprehensive analysis of water carrying capacity based on wireless sensor network and image texture of feature extraction,” *Alexandria Eng. J.*, 2022, doi: 10.1016/j.aej.2021.08.018.

[92] C. N. H. Nwokoye, V. Madhusudanan, M. N. Srinivas, and N. N. Mbeledogu, “Modeling

time delay, external noise and multiple malware infections in wireless sensor networks," *Egypt. Informatics J.*, 2022, doi: 10.1016/j.eij.2022.02.002.

[93] R. Chéour *et al.*, "Towards hybrid energy-efficient power management in wireless sensor networks," *Sensors*, 2022, doi: 10.3390/s22010301.

[94] R. Hidalgo-Leon *et al.*, "Powering nodes of wireless sensor networks with energy harvesters for intelligent buildings: A review," *Energy Reports*. 2022. doi: 10.1016/j.egyr.2022.02.280.

[95] A. Saad, M. R. Senouci, and O. Benyattou, "Toward a Realistic Approach for the Deployment of 3D Wireless Sensor Networks," *IEEE Trans. Mob. Comput.*, 2022, doi: 10.1109/TMC.2020.3024939.

[96] U. E. Zachariah and L. Kuppusamy, "A hybrid approach to energy efficient clustering and routing in wireless sensor networks," *Evol. Intell.*, 2022, doi: 10.1007/s12065-020-00535-0.

[97] S. J. Bhat and K. V. Santhosh, "Localization of isotropic and anisotropic wireless sensor networks in 2D and 3D fields," *Telecommun. Syst.*, 2022, doi: 10.1007/s11235-021-00862-2.

[98] A. Katti, "Target coverage in random wireless sensor networks using cover sets," *J. King Saud Univ. - Comput. Inf. Sci.*, 2022, doi: 10.1016/j.jksuci.2019.05.006.

[99] R. Huang, W. Guan, G. Zhai, J. He, and X. Chu, "Deep Graph Reinforcement Learning Based Intelligent Traffic Routing Control for Software-Defined Wireless Sensor Networks," *Appl. Sci.*, 2022, doi: 10.3390/app12041951.

[100] N. dos S. Ribeiro, M. A. M. Vieira, L. F. M. Vieira, and O. Gnawali, "SplitPath: High throughput using multipath routing in dual-radio Wireless Sensor Networks," *Comput. Networks*, 2022, doi: 10.1016/j.comnet.2022.108832.

[101] S. K. Rajendran and G. Nagarajan, "Network Lifetime Enhancement of Wireless Sensor Networks Using EFRP Protocol," *Wirel. Pers. Commun.*, 2022, doi: 10.1007/s11277-021-09212-6.

[102] A. Makashov, A. Makhorin, and M. Terentiev, "Anti-jamming Wireless Sensor Network Model," *Int. J. Circuits, Syst. Signal Process.*, 2022, doi: 10.46300/9106.2022.16.43.

[103] M. ur R. Ashraf Virk, M. F. Mysorewala, L. Cheded, and A. R. Aliyu, "Review of energy harvesting techniques in wireless sensor-based pipeline monitoring networks," *Renewable and Sustainable Energy Reviews*. 2022. doi: 10.1016/j.rser.2021.112046.

[104] C. Zhang *et al.*, "Triboelectric nanogenerator-enabled fully self-powered instantaneous wireless sensor systems," *Nano Energy*, 2022, doi: 10.1016/j.nanoen.2021.106770.

[105] F. F. Jurado-Lasso, L. Marchegiani, J. F. Jurado, A. M. Abu-Mahfouz, and X. Fafoutis, "A Survey on Machine Learning Software-Defined Wireless Sensor Networks (ML-SDWSNs): Current Status and Major Challenges," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3153521.

[106] A. S. Jenkins, L. Benetti, L. Martins, L. S. Emeterio Alvarez, and R. Ferreira, “Spintronic Wireless Sensor Networks,” *IEEE Trans. Magn.*, 2022, doi: 10.1109/TMAG.2021.3082266.

[107] M. Gao, “Smart campus teaching system based on ZigBee wireless sensor network,” *Alexandria Eng. J.*, 2022, doi: 10.1016/j.aej.2021.09.001.

[108] M. Wei, C. Rong, E. Liang, and Y. Zhuang, “An intrusion detection mechanism for IPv6-based wireless sensor networks,” *Int. J. Distrib. Sens. Networks*, 2022, doi: 10.1177/15501329221077922.

[109] H. Alrahhal, R. Jamous, R. Ramadan, A. M. Alayba, and K. Yadav, “Utilising Acknowledge for the Trust in Wireless Sensor Networks,” *Appl. Sci.*, 2022, doi: 10.3390/app12042045.

[110] M. Kortas, O. Habachi, A. Bouallegue, V. Meghdadi, T. Ezzedine, and J. P. Cances, “Robust data recovery in wireless sensor network: A learning-based matrix completion framework,” *Sensors (Switzerland)*, 2021, doi: 10.3390/s21031016.

[111] S. Goudarzi *et al.*, “Real-time and intelligent flood forecasting using UAV-assisted wireless sensor network,” *Comput. Mater. Contin.*, 2021, doi: 10.32604/cmc.2022.019550.

[112] H. Al-Tous and I. Barhumi, “Reinforcement Learning Framework for Delay Sensitive Energy Harvesting Wireless Sensor Networks,” *IEEE Sens. J.*, 2021, doi: 10.1109/JSEN.2020.3044049.

[113] V. Kanwar and A. Kumar, “DV-Hop localization methods for displaced sensor nodes in wireless sensor network using PSO,” *Wirel. Networks*, 2021, doi: 10.1007/s11276-020-02446-5.

[114] S. S. Sharifi and H. Barati, “A method for routing and data aggregating in cluster-based wireless sensor networks,” *Int. J. Commun. Syst.*, 2021, doi: 10.1002/dac.4754.

[115] D. Velásquez *et al.*, “A cyber-physical data collection system integrating remote sensing and wireless sensor networks for coffee leaf rust diagnosis,” *Sensors*, 2021, doi: 10.3390/s21165474.
