Research Report

Sensor Networks

COEN 331 – Wireless & Mobile Networks

Submitted by:

BENITA REGO – W1628656

Guided by:

Dr. Keyvan Moataghed

Audience

Wireless sensor networks, their design, connectivity, and protocols are all covered in this research project document. It also covers how Wireless Sensor Networks work, how they're organized, and how they're implemented. This document goes on node localization, transport protocols, routing, network security, and future developments in detail.

This document can also be used as a reference for readers who do not have advanced academic degrees in networking but are interested in learning more about wireless networks, architecture, and protocols. For industry experts and students in this sector, this document will serve as an introduction to the field of Wireless Sensor Networks.

This research can be utilized in the classroom to discuss sensor networks and their architecture, as well as their merits and drawbacks in a few instances. Students whose academic or extracurricular interests are tied to the fast-growing interest in the field of internet of things might use this report as a reference tool.

Table of Contents

List of Figures

List of Tables

Chapter - 1

Motivation for Wireless Sensor

Sensors bridge the gap between the physical and digital worlds by gathering and displaying real-world events and transforming them into data that can be evaluated, saved, and controlled. Sensors provide a huge social advantage by being integrated into several devices, equipment, and environments.

They can help with disaster prevention, natural resource conservation, higher productivity, improved security, as well as the development of applications like systems and smart house techniques.

This research paper provides a comprehensive introduction of wireless sensor network principles, network technologies with protocols, OS, middleware and sensors, and security are all covered in this course, as well as their theoretical and practical aspects.

The first chapter of this document will introduce sensor networks which will set the tone of this research paper. It gives an overview of what sensors are, types of sensors, what they do and their purpose in integrating them into a network to achieve a variety of use cases. It also talk about the history and features of the sensors.

The second chapter will give an insight about wireless sensor networks, the components of a sensor system, the network, the classification of sensors, the features and challenges and constraints. This chapter will also describe the design factors of wireless sensor networks.

The following chapter will focus on the Radio Communications. Further it describes the properties of wireless communication.

The fourth primarily focus on the routing protocols and communication protocols respectively which are employed in wireless sensor networks.

The fifth chapter gives a brief on the issues of security in wireless sensor networks. It also mentions some of the most serious security threats in WSN.

The last chapter will conclude this document while touching on the future scope of wireless sensor networks.

1.1 Introduction to Sensor Networks

1.1.1 *Sensor Networks Definition*

A sensor network is a collection of tiny, battery-operated devices. They're frequently used to show physical and environmental factors like temperature and sound, and they send their data via the network to a central sink or base station, where it is analysed and monitored. Below is the image representing a wireless sensor network.

There are two types of sensor networks: wired and wireless. To connect sensors, wireless sensor networks (WSNs) use technologies like Bluetooth, cellular wifi, or near field communication (NFC). Ethernet cables are used to link sensors in wired sensor networks. WSNs are easier to set up and manage, and provide greater device flexibility. WSNs have emerged as a major IoT technology, thanks to the rapid growth of sensors and wireless technologies. Physical network infrastructure doesn't have to be changed for WSNs.

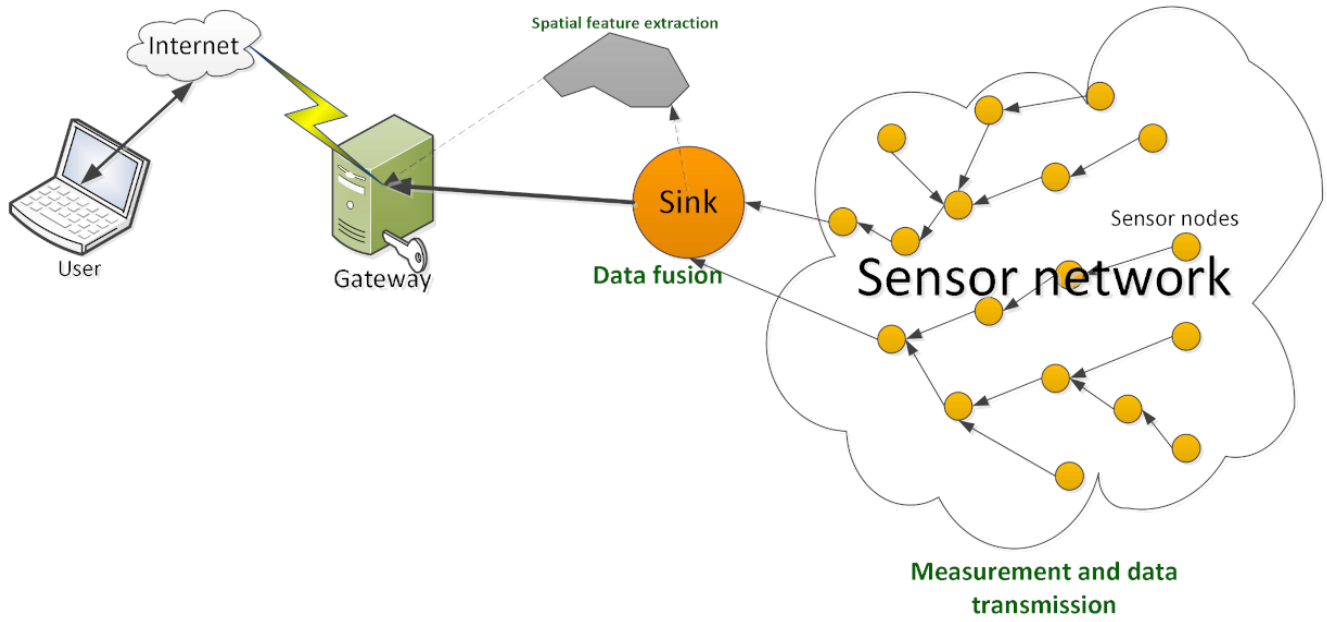

Figure 1.1 Representation of a wireless sensor network

1.2 Overview of Wireless Sensor Network

WSNs provide for new programming and necessitate non-traditional protocol layout paradigms due to many restrictions. With the need for less complex equipment and low power consumption, the correct balance of communication and signal/fact processing abilities must be discovered. A base station, also known as a sink, serves as a link between clients and the network. Using enforcing requests and receiving results from the station, information may be collected from the network.

WSN nodes have constrained sources built in: Communication bandwidth, processing speed, and storage capacity are all constrained. Researchers have increasingly focused on heterogeneous sensor networks, in which sensor nodes fight energy phase inconsistencies. New network topologies with heterogeneous devices, as well as the generation's continual development, remove present constraints and vastly expand the variety of applications for fast-converting WSNs. This necessitates a large amount of work in terms of research, standards, and time. The majority of WSN research has been on power design using computationally green techniques and protocols, with software restricted to basic fact-oriented tracking and reporting tools.

Sensor systems consist of:

- **Sensor Nodes**
  Sensor nodes are small devices that may capture information such as environmental changes and other variables in order to aid in the computation of data. There are a lot of sensor nodes in a wireless sensor network. Radio signals are used to communicate.

- **Base station**
  Acts as a hub for data transfer between multiple sensor nodes and end-user applications.

- **Radio Nodes**
  These nodes process sensor data and send it to the WLAN access point. A memory unit, power unit, transceiver, and microcontroller form up the whole system.

- **WLAN Access Points**
  It receives data that is sent wirelessly over the internet by radio nodes.

- **Evaluation Software**
  The data received by the WLAN Access Point is evaluated by Evaluation Software, which then displays the report to the users for further data processing.

1.3 Classification of Sensors

The purpose of sensor categorization is to determine which sensor is best for a particular application. The physical attribute to be measured, such as temperature, pressure, light, or humidity, determines the sensor to use. Physical properties of these are an important area of research. Aside from physical characteristics, sensors can be classified based on a range of factors, whether they need to be powered from a separate source. Sensors that require a separate power source are known as active sensors They use energy to either initiate a reaction or detect a change in the energy supplied signal (light, microwave, or sound).

The goal of sensor categorization is to determine which sensor is optimal for a specific application. The sensor to be utilized is determined by the physical property being measured, such as temperature, pressure, light, or humidity. Some of the most prevalent physical traits are summarized in Table 1.1. Sensors can be categorized using a variety of criteria in addition to physical properties, such as whether they need to be powered from a separate source. Because they use energy to provoke a reaction or detect a change in the energy provided signal (light, microwave, or sound).

Temperature	Thermistors, thermocouples
Pressure	gauges, barometers, ionization, gauges
Optical	Photodiodes, phototransistors, infrared, sensors, CCD, sensors
Acoustic	Piezoelectric, resonators, microphones
Mechanical	Strain, gauges, tactile, sensors, capacitive, diaphragms, piezoresistive, cells
Motion, Vibration	Accelerometers, gyroscopes, photo, sensors
Flow	Anemometers, mass, air, flow, sensors
Position	GPS, ultrasound-based, sensors, infrared-based, sensors, inclinometers
Electromagnetic	Hall-effect, sensors, magnetometers
Chemical	pH, sensors, electrochemical, sensors, infrared, gas, sensors
Humidity	Capacitive and resistive, sensors, hygrometers, MEMS-based, humidity, sensors
Radiation	Ionization, detectors, Geiger–Mueller, counters

Table 1.1 Classification and examples of sensors

1.4 History of Wireless Sensor Networks

In cooperation with the Rockwell Science Center, the University of California, Los Angeles presented the concept of Wireless Integrated Network Sensors, or WINS (Pottie 2001). In 1996, the Low Power Wireless Integrated Microsensor (LWIM) was delivered, was one of the WINS project's results. (Bult and colleagues, 1996). For this smart detection system, a CMOS chip was used to combine many sensors, interface circuits, computerized signal preprocessing circuits, a remote radio, and a CPU onto a single chip. The Smart Dust project (Kahn et al. 1999) at the University of California at Berkeley centered on the notion of microscopic sensor hubs known as bits. The purpose of this study was to demonstrate that a whole sensor architecture may be built into devices as tiny as a grain of sand. The Berkeley Wireless Examination Center's PicoRadio project (Rabaey et al. 2000) (BWRC) aims to produce low-power sensor devices with minimal power consumption to the point where they can manage themselves utilizing fuel sources. Solar or vibrational energy, for example, can be obtained from the workplace. Low-power equipment and programming segments for sensor hubs also are a focus of the MIT AMPS (miniature Versatile Multidomain Power-mindful Sensors) project, that also includes utilization of microcontrollers with dynamic voltage scaling capabilities and ways to rebuild information preparation to minimize product-level power needs. While scholarly organizations have largely determined previous endeavors, several business ventures have emerged in the last decade (many of them are based on some of the above-mentioned scholastic undertakings), including Sensoria, Worldsens, Dust Networks, and Ember Corporation. These companies sell sensor devices that are ready to send in a number of circumstances, as well as programming, support, and sensor data formatting administrative tools.

1.5 Features of WSN

Due to their small size, WSNs generally include sensor nodes that use less power, have a limited amount of memory, and have a low energy intake demand.
Wireless networks can be used to analyze harsh environmental physical conditions and are vulnerable to enemy attacks. They are supposed to be self-configuring and self-restorative, even if they are set up in an ad hoc manner, and to cooperate with ongoing upgrades or alterations.

- **Distributed Computing**

The algorithms used to collect the data must be monitored centrally since the processing must be centralized because the computing is done across several nodes in the network.

- **Offers an Easily Scaled Solution**

WSNs can be easily scaled for a larger environmental surveillance because they are self-configured.

- **Ad hoc implementation**

The majority of sensor nodes are used in regions where there is insufficient infrastructure, Sensor nodes are dropped from an airplane into a forest, for example. The sensor nodes are expected to establish connectivity and distribution due to their ability to self-organize.

- **Unattended procedure**

When modifications or upgrades are required, the sensor nodes are anticipated to self-organize or self-reconfigure. There is almost never any human intervention after that.

- **Unmetered**

The sensor nodes have a low energy requirement and can be powered from any source. They only have a limited amount of energy to work with, which must be used efficiently for computation and interaction. When communication takes place at a sensor node, the most energy is required. As a result, when communication/interaction is as low as feasible, for efficient use of energy.

❖ **Usage of Sensors**

The sensor node should deliver the best results while using the least amount of energy.

❖ **Low cost**

Thousands of sensor nodes are installed to collect data while monitoring an environment. This results in a thick layer, signifying a dense infrastructure. To keep total infrastructure expenses to a minimum, the specific cost of each sensor node should be as low as feasible.

❖ **Dynamic modifications**

In contrast to older traditional networks, when the primary purpose was to increase medium throughput or node development. It is critical for a sensor network to increase the system's lifetime and robustness. The sensor node must react to quickly changing environmental circumstances while also considering connection requirements such as detecting and replacing failed nodes as well as how to add more nodes to the system.

❖ **Heterogeneity**

Sensor nodes in the same network could be of many types. As a result, they must collaborate and work as a team.

❖ **Low Bandwidth**

For optimal energy efficiency, communication must be kept to a bare minimum. The data should be sent as quickly as possible.

❖ **Large Scale Coordination**

To obtain efficient findings, the sensor nodes must interact with one another.

❖ **Real Time Computation**

Because fresh data is constantly generated and the nodes have a limited source of energy, the computation of the data collection process should be as efficient and quick as possible to avoid obstruction.

❖ **Transmission back-and-fro Capabilities**

Radiofrequency signals are used by wireless sensor networks to communicate back and forth over a medium. As a result, it can communicate very efficiently across a short distance and with minimal bandwidth, as well as dynamic bandwidth changes. The medium may be unidirectional (simple) or bidirectional (complex) (half duplex or full duplex). Because there is little human intervention, WSNs must be efficient. As a result, the task becomes more challenging, and the hardware components and software programs must be carefully chosen in order to improve system longevity and resilience.

1.6 Challenges and Constraints

While sensor networks have a lot in common with other distributed systems, they also have their own set of challenges and limits. The design of a WSN is influenced by these constraints, as a result, differentiated protocols and algorithms from those used in other distributed systems have emerged.

- **Energy**

  Sensor hubs operate on limited energy constraints, which is a common restriction associated with sensor network architecture. They are frequently powered by batteries, which must be refilled or re-energized (for example, by sunshine) when they run out. For certain hubs, neither option is suitable, therefore they will be removed after their fuel supply is spent. The ability to re-energize the battery has a significant impact on the energy usage procedure. A sensor hub should be able to work with non-rechargeable batteries until the main target time has gone or it is replaced. The type of application determines the mission's duration; for instance, researchers watching frigid developments may require sensors that can work for several hours or days. In a front-line situation, however, It's possible that you'll just need it for a few hours or days. As a result, energy productivity is typically the first and most critical difficulty for a WSN.

  This essential infuses the sensor hub and organization approach in every way. The decisions taken at the actual layer of a sensor hub, for example, have an impact on the device's total energy usage and the development of higher-level standards

- **Self-Management**

  Many sensor network applications are designed to function in remote locations and extreme conditions, without any infrastructure support or maintenance and repair options. Sensor nodes must thus be self-managing in that they must setup themselves, function and communicate with other nodes, and react to failures, changes in the environment, and changes in external stimuli without the need for human intervention.

  Several sensor network applications don't require individual sensor node positions to be established and engineered. This is especially critical for networks deployed in inaccessible or rural locations. The surviving nodes, on the other hand, must execute several setup and configuration tasks on their own, including establishing contact with nearby sensor nodes, detecting their locations, and launching their sensing functions.

  Depending on this knowledge, the volume and type of data that sensor nodes create and transmit on behalf of other nodes might change. The volume and type of information that a node creates and transfers, for example, may be influenced by the number or identities of its neighbors, as well as its location.

❖ **Wireless Networking**

A sensor network designer faces various issues due to the dependency on networks and communications. For instance, as a radio frequency (RF) signal propagates over a medium, attenuation limits the range of radio broadcasts and passes through barriers, it fades (i.e., loses power).

The inverse-square law can be used to express the connection between an RF signal's received and sent power:

$$p \ \alpha \ \frac{p_t}{d^2}$$

According to this formula, the inverse of the square of the signal's distance d from the source is proportional to the received power P.

So, the required transmission power increases as the distance between a sensor node and a base station grows, so does the distance between a sensor node and a base station. As a result, splitting a long distance into multiple shorter ones saves energy, posing the difficulty of providing multi-hop communications and routing.

❖ **Decentralized Management**

Many wireless sensor networks are too large and energy-constrained to conduct network management solutions like topology management or routing (e.g., at the base station). Sensor nodes, on the other hand, must work together with their neighbors to make localized judgments, as they do not have access to global data. As a result, while these decentralized (or distributed) algorithms will not always provide optimum results, they may use less energy than centralized systems.

Routing in centralized and decentralized approaches, as an example. A base station may collect data from all sensor nodes, compute the optimum routes (for example, in terms of energy consumption), and tell each sensor node of its path. However, the overhead might be large, particularly if the topology changes. A decentralized technique, on the other hand, permits each node to make routing decisions based on limited local data (such as a list of neighbors and their distances from the base station). While this decentralized approach may result in inefficient pathways, it can considerably cut administrative expenditures.

❖ **Design Constraints**

Due to sensor nodes have the processing speeds and storage capacity of computer systems from decades ago, owing to the requirement to run specialized applications with minimal energy usage. Many desirable components, such as GPS receivers, cannot be included. These restrictions and needs have an impact on software design at multiple levels; OS, for instance, must have small memory footprints and perform resource management duties efficiently. However, the lack of complicated hardware capabilities (such as parallel execution capability) makes it easier to design small and efficient operating systems. The creation of various protocols and algorithms for usage in a wireless sensor network (WSN) is influenced by the hardware limitations of a sensor. Routing tables, for example, which include entries for each possible network destination, may be too huge for the memory of a sensor to handle.

❖ **Security**

Several distant sensor networks collect sensitive data. Sensor hub's remote and unmanaged activity increases their vulnerability to malicious disruptions and assaults. An attacker can also listen in on sensor transmissions via remote correspondences.

A refusal-of-administration attack, for example, is one of the most complicated security risks, with the goal of disrupting the normal operation of a sensor organization. Several techniques, such as a sticking attack, which employs strong remote signals to inhibit successful sensor correspondences, can be used to accomplish this. Depending on the sort of sensor network application, the implications might be severe. While there are several strategies and solutions for suitable frameworks that avoid or restrict the severity and damage of attacks, many of them demand high computational, communication, and capacity requirements that are usually intractable for asset-required sensor hubs. As a result, new solutions for key foundation and distribution, hub verification, and mystery are required for sensor networks.

Chapter-2

Architectures

2.1 Hardware components

2.1.1 Sensor Node Hardware Overview

The application's requirements are clearly a deciding factor when selecting hardware components for a wireless sensor node, especially in terms of the node's size, cost, and energy consumption – the quality of communication and computing capabilities is generally assumed to be satisfactory, The trade-offs between features and pricing, on the other hand, are critical. In even more extreme hypotheses, the nodes are said to have to be reduced to the size of dust grains. Node's size is not essential in more practical applications than its convenience and simplicity.

Despite these variances, there is a similar tendency in the literature when looking at typical hardware platforms for wireless sensor nodes.. While no one standard can cover all sorts of applications, there are some that can, this section will look at some of the most prevalent sensor node layouts. Furthermore, Because custom off-the-shelf components currently fail to fulfill some of the most stringent application requirements, a number of research programs are concentrating on reducing the size, energy consumption, and costs of any of the components. These techniques are not explored in this book because it concentrates on the networking elements of WSNs.

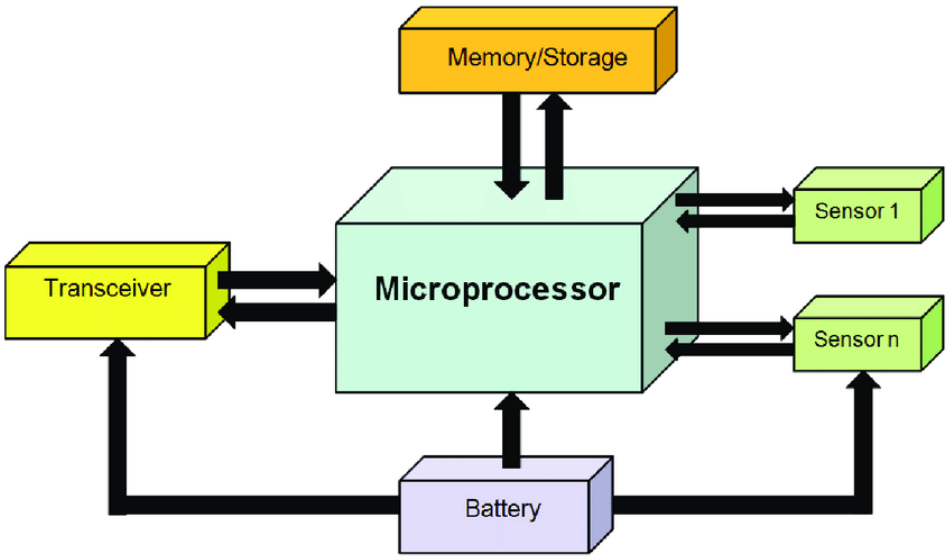

Figure 2.1 Overview of main sensor node hardware components

A typical sensor node is made up of five primary parts (see Figure 2.1):

- **Controller -** A controller that can run any code and process all relevant data.
- **Memory -** A small amount of memory for storing programs and intermediate data; programs and data are usually stored in various types of memory.
- **Sensors and actuators -** Devices that can observe or manipulate physical components of the environment serve as the actual interface to the physical world.
- **Communication -** You'll need a device that can transmit and receive data over a wireless channel to transform nodes into a network.

2.2 WSN Structures

2.2.1 Star Topology

The base station is at the heart of a star network that relays data from sensor nodes. It's also feasible to have low-latency communication between the distant node and the sink station. Below is an example depicting a star topology.

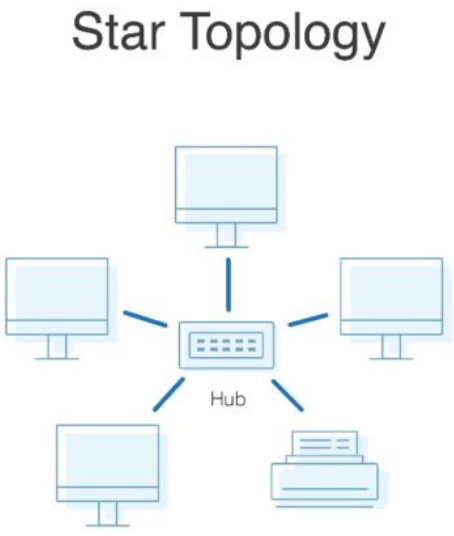

Figure 2.2 Star Topology

2.2.2 Partial Mesh Topology

Unlike a full mesh, a partial mesh does not have all nodes connected. As a result, two or more nodes are linked to one another. This results in a low degree of complexity and cost while still providing a high level of capability. Below is an example depicting a partially connected mesh topology.

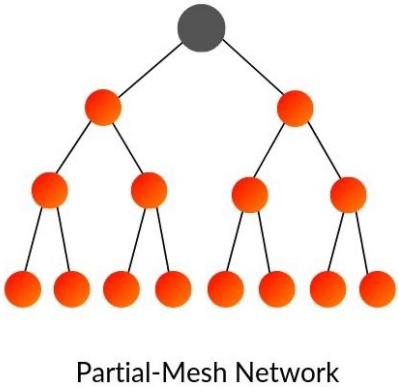

Figure 2.3 Mesh (partially connected) Topology

2.2.3 Mesh Topology

In a complete mesh network, every node is linked to every other node. A straight point-to-point link links all of the nodes together. The mesh's nodes are all equally important and have equal data transmission duty. This could raise the network's costs. Below is an example depicting a fully connected mesh topology.

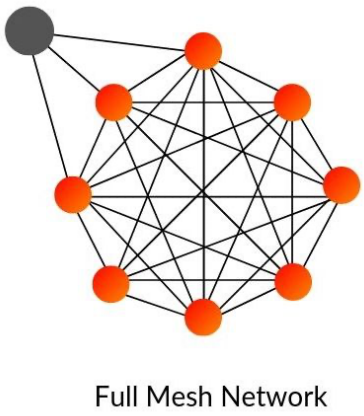

Figure 2.4 Mesh (fully connected) Topology

2.2.4 Ring Topology

Every node is connected to another node. Data is transmitted from one node to the next in a ring. A node failure not only breaks the loop and potentially shut down the entire network, but it also generates traffic congestion and double-path communication. Below is an example depicting a ring topology.

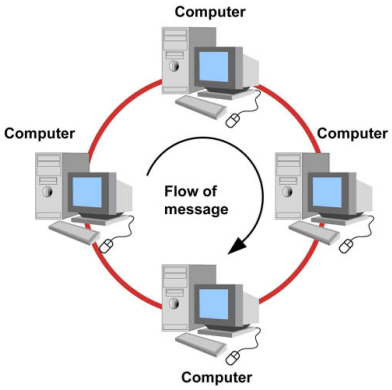

Figure 2.5 Ring Topology

2.2.5 Circular Topology

In this architecture, the sensing area is circular, and the sensing area has a sink/gateway (at center). The sensor nodes pick up on the intriguing occurrence and send the data to the sink. The nodes are arranged at random around the sink, as indicated in Figure 3.4.6, with a uniform concentration. Depending on the node's distance/length from the sink and the nodes' communication range, data must travel a single or multiple hops before being received by the sink. It's easier to set up and manage a circular web architecture, and it's also more efficient. Below is an example depicting a circular topology.

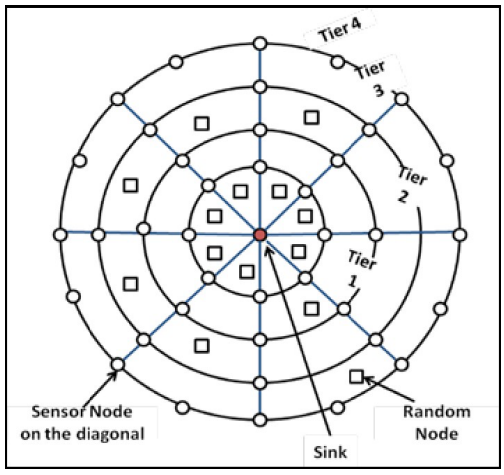

Figure 2.6 Circular Topology

2.2.6 Hybrid Topology

When one or more technologies are combined to form a network, it is called a hybrid network. The hybrid topology may be highly useful for some special goals to be implemented in a network. Hybrid networks include star-bus networks, hierarchical star networks, star-ring networks, and hybrid mesh networks. Below is an example depicting a hybrid topology.

This topology has a number of advantages, including being simple to fix and requiring minimal maintenance. The system's design can be simply changed.

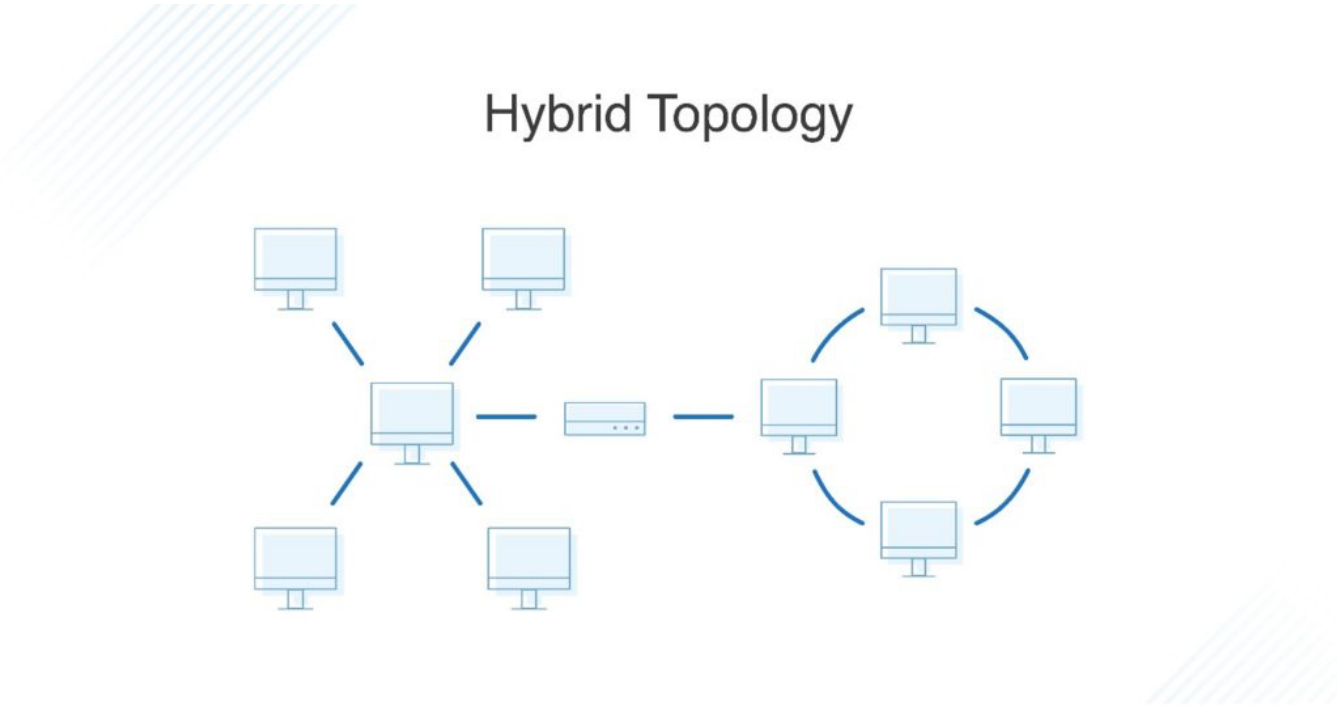

Figure 2.7 Hybrid Topology

2.3 Types of WSN

- **Cyber-physical system (CPS)** - Its goal is to better understand what these networks are capable of and what their major characteristics are when they are integrated in a physical environment. Cyber-physical systems are part of the environment and application specific, unlike other computers and gadgets that are environment agnostic. Another interesting feature is that they can change the surroundings utilizing actuators like those used in autonomous irrigation pumps, light switches, alarms, and humidity or temperature controls.

- **Body sensor networks** - It's a form of network that's meant to be worn on the body (mostly human). Just a few of the possibilities include health tracking, weight control, sports reporting, and a range of other uses. Smart footwear and T-shirts, for example, can monitor your movement and heart rate. Sensor nodes, for the most part, are tiny and can be implanted.
- **Crowdsourcing** - It's a new and rapidly evolving sort of detection where the sensors are essentially people with cell phones. Individuals can, for example, track their hiking routes and rank them in terms of street condition, safety, and commotion. This data is compiled on a single topic and organized into a single city hiking quality guide that can be tailored to each customer. The actual power of these apps is that they don't require any additional hardware; all they need is a simple client-installed app for smart phones.

- **The Internet of Things (IoT) –** It's primary idea is that everything is connected to the Internet, including a washing machine and a radio. When it comes to sensor networks, having an Internet connection offers numerous benefits and can be regarded an enabler technology. The goal, on the other hand, might be quite different, such as when you can check your emails in the microwave or while driving. The name "internet" also implies that these networks are IP-enabled and, as a result, employ a well-defined communication stack. This can be a benefit (no need to reimplement) or a disadvantage (no need to reimplement) (high energy use, little flexibility).

2.4 Power Consumption

One of the most important features to comprehend is the power consumption of sensor node hardware. Energy is required for each component of a sensor node to function. This energy is quite limited, hence on-board batteries are required. As a result, it's critical to know which components consume the most energy and only utilize them when absolutely necessary.

Component	Mode	Current Draw
Microcontroller (TI MSP430)	Active	1.8 mA
	Sleep	5.1 µA
RF Transceiver (CC2420)	Receive	19.7 mA
	Transmit (at 0 dBm)	17.4 mA
	Sleep	0.01 mA
Accelerometer (ADXL345)	Standby	0.0001 mA
	Active	0.04 – 0.145 mA
External flash (Micron M25P16)	Write	15 mA
	Read	4 mA
	Sleep	0.001 mA
Temperature sensor (TMP102)	Sense	0.015 mA
	Sleep	0.001 mA

Table 2.1 Nominal Power Consumption of Components

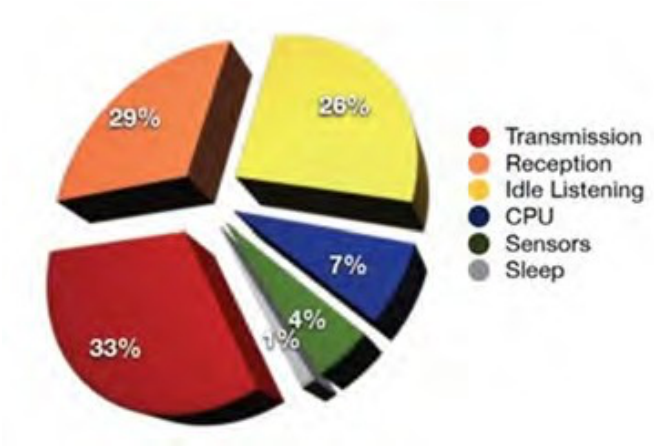

Figure 2.8 Power consumption of a WSN Node

In above Table 2.1 and in the Pi chart of Figure 2.8 all of the power usage in the above table is presented in Amperes (A). For example, even when the radio is turned off and sleeping, it consumes 0.01 mA. The sensors are supposed to deliver a continuous voltage of 3 volts from the batteries attached to the sensor node.

These are merely theoretical calculations, and actual batteries or hardware may behave differently. However, this highlights the need of minimizing individual component utilization. Even if batteries aren't perfect energy storage devices.

The view changes considerably when the radio's slumber hours are introduced (the so-called duty cycle). Saving energy, the radio is turned on and off at regular intervals in this situation.

2.5 Usage of Simulators

Instead of using real nodes, it is always preferable to utilize a simulator. A simulator is a computer program that models the behavior and interactions of another system. A sensor network simulator, for example, replicates sensor node activity and communication. There is a screenshot attached below of a COOJA stimulator for reference in Figure 2.9.

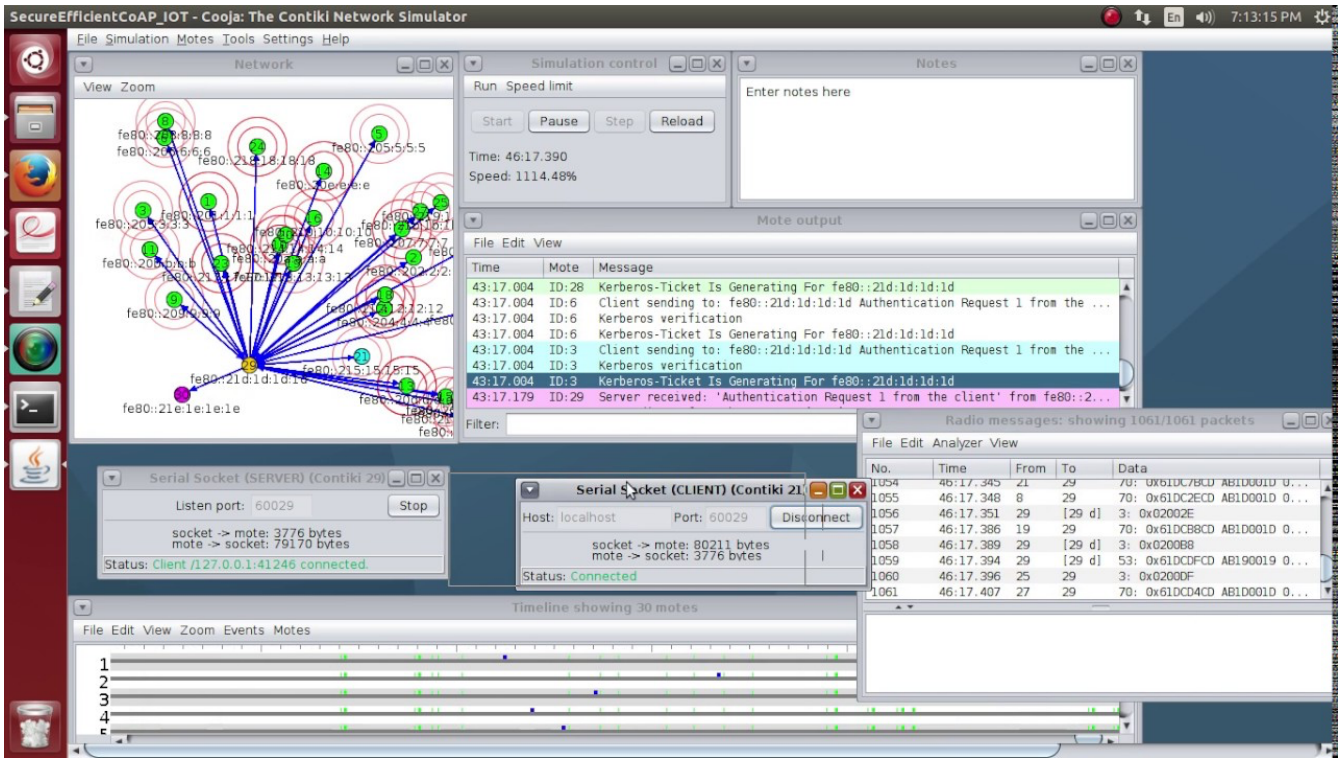

Figure 2.9 Screenshot of Cooja simulator

Wireless propagation model depicts the movement of bundles through a remote correspondence channel. It's especially important to acquire a grasp on distant medium errors like bundle misfortune and parcel defilement. The single unit plate diagram model is the simplest. If the collector is within a specified circular zone surrounding the transmitter, it means, any sensor hub can send a parcel to another sensor hub. The data collection is constantly error-free. This model is typically overly simplistic, and re-enactment runs with it give the impression that everything is running smoothly, that no bundle debasements occur, and that parcel delivery between two hubs with a consistent distance works reliably.

Mobility model defines how sensor nodes move throughout the environment. This type comes in useful when your regular sensor nodes are also moving, such as when they are placed on bikes or buses. Some models, such as the random waypoint, are relatively basic. It always selects a new random location inside the simulated region and lets the sensor to "drive" there at a constant predetermined speed, then selects another, and so on.

The number of events that have happened in the environment is determined by the **traffic model**. Sensor networks are used to detect anything, such as temperature, rain volume, and so on. Recognizing when significant events occur in a real-world setting, as well as using equivalent values for simulation, is critical.

Chapter-3

Radio Communications

3.1 Radio Communication

We all know that the capacity of WSN networks to connect wirelessly is at their core. The most often used interface is a radio transceiver that operates in one of the open bandwidths that are reserved worldwide for research and medical purposes.

Normal electromagnetic waves are what radio waves are. Their name comes from the electromagnetic spectrum's frequency range. The equation for an electromagnetic wave is as follows:

$$S(t)=A(t)sin(2\pi f(t)t+\phi(t))$$

There is no information carried by a natural wave. You must modify the properties of the radio wave in a well-defined way to encode certain information into it for data transfer, so that these changes can be noticed at the receiver side and the same information can be decoded.

Any of the three features of the radio wave, or combinations of them, can be used to modulate the signal:

- **Amplitude** A(t). The height of the wave is determined by this parameter. You may alter the amplitude to encode information from extremely little (encoding a 0) to very large (encoding a 1). (encoding a 1).

- **Frequency or period** f(t). The frequency at which the wave shape is reproduced throughout time is determined by this parameter. The frequency of the signal can be changed to represent different codes.

- **Displacement or phase** ϕ(t). This element specifies the wave's displacement in relation to the axis' start. You may move the wave to signify a code change.

The symbol you're encoding onto the modulation code wave is called a modulation code, or key. You'll have two codes or keys if you encode a 1 with a very high amplitude and a 0 with a very low amplitude, for example. Of course, more than two keys or (ones and zeros) can be encoded into the signal by using more than two levels of amplitude or more than two different frequencies. Combining several modulation codes can result in a plethora of new modulation codes. Both modulation and demodulation are simple to understand and utilize. In reality, all wireless communications employ wave modulation.

But, considering the problems that wireless communications face in everyday life, why do they periodically fail to deliver? Wave propagation characteristics over your surroundings, or what is left of the wave after it has traveled a specific distance across the environment, might cause issues (air, water, free space, etc.).

3.2 Properties of Wireless Communication

As it travels through the atmosphere, the electro propagation wave experiences numerous aberrations (we call this wave propagation). These results are mostly due to the following processes:

- **Attenuation:** This phase disperses the wave's energy over a wider area.
  It resembles a balloon that is dark red before being inflated with air but becomes virtually translucent once filled. As a result, the wave becomes less effective and harder to detect as the distance between the sender and receiver increases.

- **Reflection/Refraction:** This process causes a wave to alter direction when it impacts a surface. A piece of the wave is mirrored and takes a different route, while another is refracted into the material, changing its properties.
  Both processes produce additional secondary waves, which arrive somewhat later than the primary wave at the receiver. This is both a benefit and a drawback: when primary and secondary signals overlap, very weak signals can be caught more easily.

- **Diffraction/Scattering:** The wave will be broken into several secondary waves by sharp edges and uneven surfaces in the surroundings, each having the same consequences, Figure 3.1 shows it.

- **Doppler effect:** The frequency of a signal varies with its relative velocity to the receiver in general. The Doppler effect is well-known for its impact on police sirens, which sound different depending on whether the officer is coming or fleeing. When radio waves' frequencies are shifted in one way or the other, the same process happens, resulting in a loss of center.

All the above processes will give rise to path loss and are depicted in Figure 3.1 for reference.

Definition: ***Path Loss:*** *An electromagnetic wave's power density decreases as it travels through space, which is known as path loss.*

In wireless communications, path loss is significant because it helps you anticipate transmission quality and/or build wireless networks. The rest of this section will look at how path loss actually works and how it affects wireless communications.

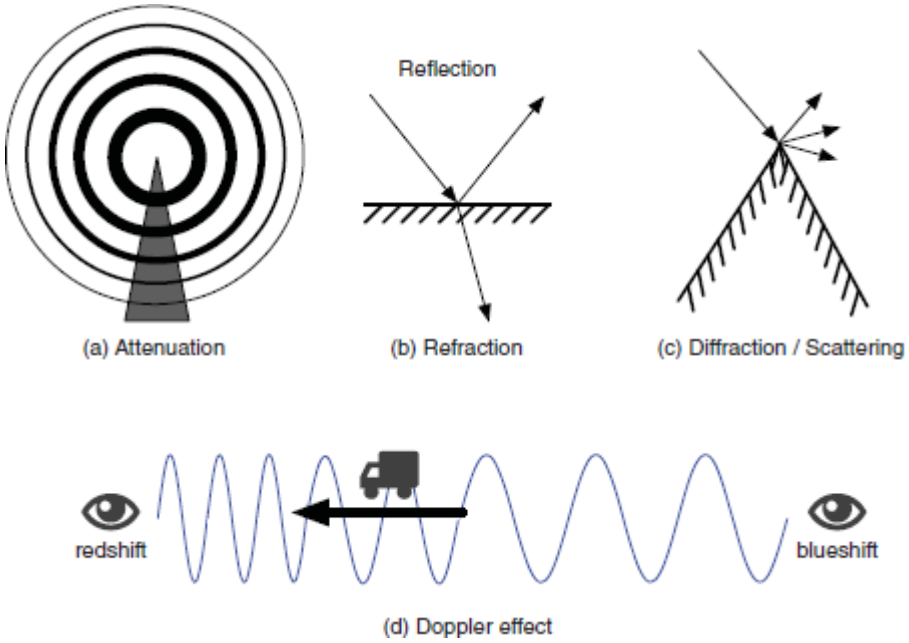

Figure 3.1 Physical Processes that lead to path loss in signal propagation

3.2.1 Hidden Terminal Problem

The Figure 3.2 is the best way to illustrate the hidden terminal problem. There are four nodes visible. From node A to node B, Packet X is sent. propagation Since node C is outside of node A's transmission range, don't know of the upcoming transmission of packet X. Described as a semi-circular area around the transmitter is the transmission range.

Node C starts transmitting a packet to node D since it is ignorant of the ongoing transmission between A and B. Interference occurs at node B, resulting in the corruption of packet X. On the other hand, communication between C and D is successful. In wireless communications, the hidden terminal problem is a significant obstacle to overcome. Let us see how to resolve the problem.

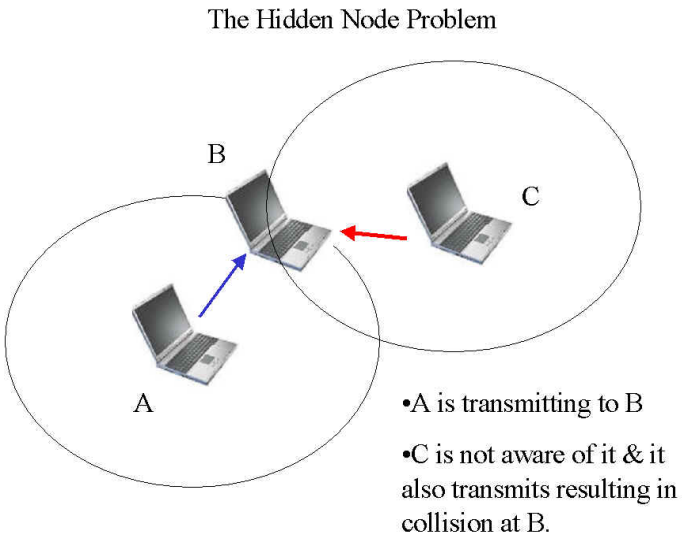

Figure 3.2 Hidden Terminal Problem in Wireless Communications

3.3 Medium Access Protocols

Sensor node access to the shared wireless medium, sometimes known as "air," is governed by Medium Access Protocols. But first, let's establish a few key metrics for determining how well a medium access protocol (MAC protocol) is doing.

The MAC protocol is intended to improve throughput at individual nodes as well as over the wireless channel. It also aspires to preserve the appearance of justice. This implies that each node should have an equal chance of sending packets out.

Definition: ***Throughput:*** *The number of bits or bytes successfully transmitted per time unit is known as throughput. Bits per second is the most common unit of measurement. The throughput of a medium (cable or wireless), a connection (between two communicating nodes), or a single node can all be described.*

Definition: ***Delay:*** *The time between sending and receiving a packet is referred to as delay. Any two communicating components – internal hardware or multi-hop end-to-end communications – may have a delay specified between them.*

3.3.1 Carrier Sense Multiple Access

CSMA (carrier sense multiple access) is a simple yet effective system that operates on the principle of "listen before chat." If the shared channel is available, the sender first listens to it before attempting to send. CSMA has two versions: collision detection (CSMA-CD) and collision avoidance (CSMA-CA) (CSMA-CA) is available. CSMA-CD attempts to identify a collision and resends the packet if a CSMA-CA fault occurs. The second aims to prevent the accident from happening at all. Because it is more extensively used and performs better, this talk will focus on CSMA-CA. The flow diagram in Figure 3.3 can be used to understand.

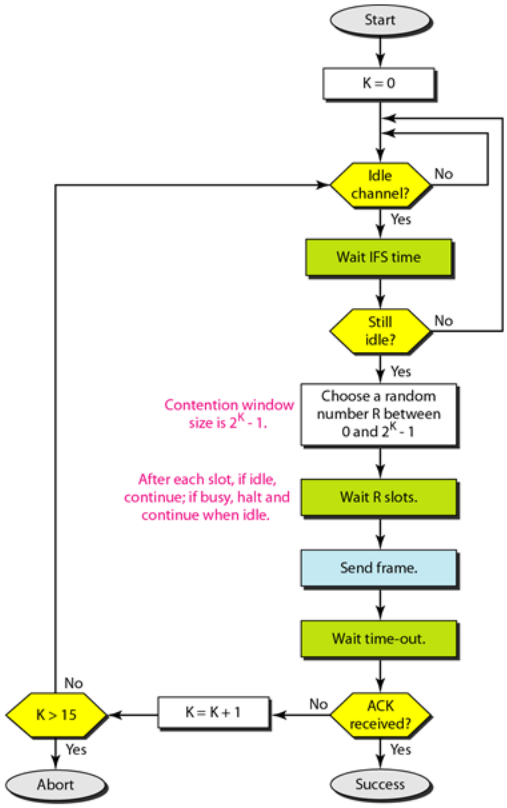

Figure 3.3 Flow diagram of general CSMA with collision avoidance

Overall, CSMA is a straightforward and easy-to-understand protocol that performs admirably in most scenarios. However, in terms of sensor networks, its biggest disadvantage is its high energy consumption. It never puts the nodes to sleep, and it rapidly (typically a couple of hours) depletes the energy of a sensor node.

3.3.2 Sensor MAC

Sensor MAC (S-MAC) was created with sleep-enabled sensor networks in mind. It allows nodes to go to sleep and only communicate when they are actively involved or awake. This is depicted in Figure 3.4, and due to its energy efficiency, it is the preferred mode of operation for sensor nodes. The service cycle is the relationship between active and sleeping time.

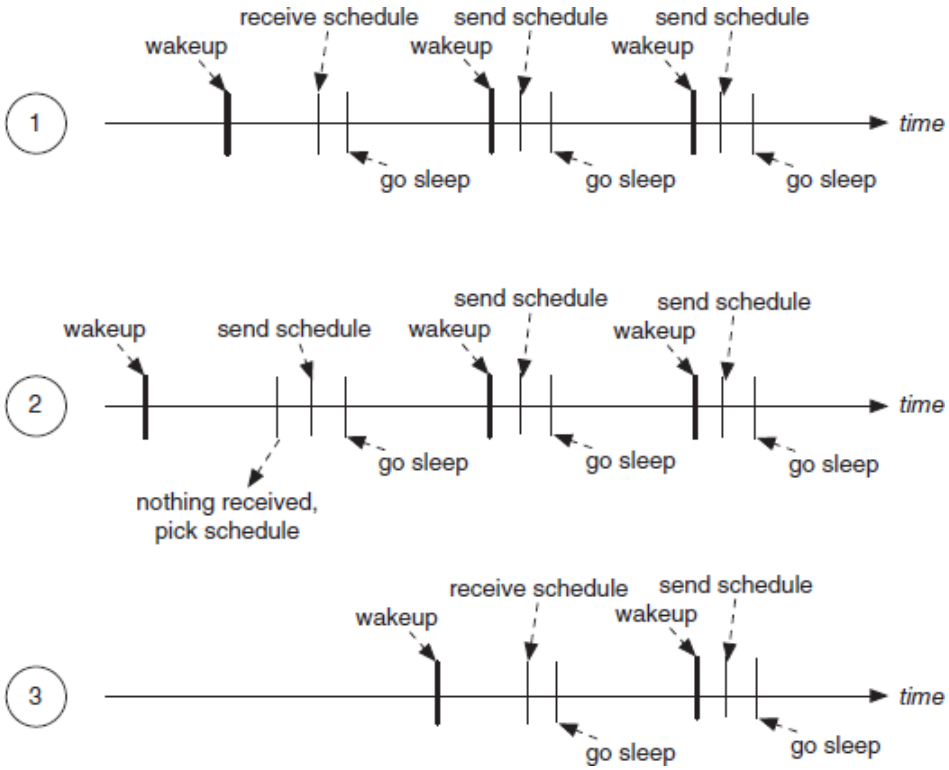

Figure 3.4 Sensor MAC general scenario

Definition: ***Duty cycle:*** *is the percentage relationship between the duration of a sensor node's active and sleeping periods. It is defined as follows:*

$$Duty\,cycle = \frac{time\,active}{period}$$

There are several general approaches you can take:

⇒***Time Division Multiple Access*** **(TDMA):** It's a communication protocol in which each node has complete control over the network for a defined amount of time (a slot). There are major delays, although there are no collisions.

⇒***Carrier Sense Multiple Access*** **(CSMA):** It says, "first listen, then talk." Although the delay is brief, it consumes a significant amount of energy (the nodes never sleep) and is not collision-free.

⇒ ***Duty cycling:*** Duty cycling is the suggested way for scheduling sensor node sleep and waking cycles. Sensor MAC, Berkeley MAC, and Box MAC all use duty cycling, which can save a lot of energy.

⇒ ***BoX*** *MAC:* It is based on B-MAC, but it simplifies communications for both unicast and broadcast broadcasts, making it the ideal MAC protocol for sensor nodes right now. It doesn't need to be synchronized, has a brief delay, and requires very little power.

Chapter-4

Routing Protocols Used in WSN

4.1 Traditional Techniques

4.1.1 Flooding Technique

If a packet is not designated for itself or the maximum number of hops a packet can traverse, flooding happens when a sensor node delivers a sent message to all other nodes, meaning that a packet is received by all of its neighbors except the node it came from. Flooding is a simple protocol to set up, and because it is reactive, it requires no maintenance. However, this requirement requires large amount of bandwidth and wastes lot of energy.

4.1.2 Gossiping Technique

A slightly modified variation of flooding occurs when a receiving node delivers a packet to a neighbor at random, who then forwards it to another neighbor, and so on. It has the advantage of preventing an implosion, but it also has the disadvantage of causing transmission delays.

4.2 Current Techniques

The many types of routing in flat-based routing, hierarchical-based routing, adaptive-based routing, multi-path routing, query-based routing, and negotiation-based routing are all terms used to describe WSNs.

4.2.1 Flat routing

Sequential Assignment Routing (SAR) - This technique creates numerous trees, each with a one-hop neighbor of the sink/gateway as its root. It is used to prevent nodes with a low throughput or a longer delay from being created. Each sensor node keeps track of two metrics for each path it travels: the total amount of energy available on the route and the delay in time units. Lower priority packets must utilize greater delay routes, whereas higher priority packets must use lower delay routes.

Directed Diffusion - The directed diffusion technique is beneficial when Sensor nodes send out requests/questions for data collected by other nodes. Data with one or more identifying parameters is received by each sensor node.

4.2.2 Hierarchical Routing

A hierarchy is established here, with higher energy sensor nodes processing and transmitting data and lower energy nodes operating sensing near the target.

LowEnergyAdaptiveClustering-It is an acronym for Low Energy Adaptive Clustering Hierarchy. TDMA is utilized in WSNs with the same type of nodes. LEACH is a self-organizing adaptive clustering mechanism. Its goal is to distribute energy consumption uniformly across sensor network nodes, collect data, promote data fusion and localized collaboration.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS) – This protocol is a step forward from the previous LEACH protocol. To extend the life of the nodes, collaborative measures are implemented. It only allows for local coordination between nodes, which reduces the amount of bandwidth consumed in communication. However, it may cause a bottleneck and a delay.

4.2.3 Multipath Routing

This is used to locate alternate routes if the main/primary path fails. Even if energy usage rises, several paths between the source sensor node and the destination sensor node can be maintained and the sink/gateway and keeping these alternate routes active by sending out frequent signals.

4.2.4 Adaptive Routing

This procedure modifies specific device characteristics, allowing them to be adapted to the network's present circumstances and available energy sources.

4.2.5 Query-based Routing

The destination node, as the query's initiator, promotes a demand for information (sensing task) from a node across the network, and a node receiving the necessary data returns data that matches the query to the query's initiator, the destination node. Natural language or high-level languages can both be used.

4.2.6 Negotiation-based Routing

WSNs use negotiation-based routing to decrease duplicate data and avoid duplication. We study bargaining as a framework for collaboration between opposing organizations in the situation of routing between two neighboring ISPs. Interdomain routing is frequently motivated by self-interest and based on a distorted perspective of the internetwork, putting routing's reliability and performance at risk. For more help in understanding the concept in Figure 4.1 in flow diagram.

Figure 4.1 Negotiation-based routing (Taken from ACM Digital Library)

Chapter-5

WSN Security Issues

Sensor networks have four security goals: confidentiality, integrity, authentication, availability, and freshness.

- **Confidentiality:** Confidentiality ensures that data can be accessed legally. By networking, confidentiality means that data concerning conversations must be kept hidden from anyone who does not have legal access.
    - Eavesdropping - Eavesdropping is the act of surreptitiously or covertly listening to another person's private discussion or communications in order to obtain information.
    - Privacy - Privacy is turning into a totally critical protection issue as the concerns at the disclosure of private data, for example, identification to unauthorized attackers, are becoming a great deal stronger.
- **Integrity:** Integrity is a guarantee that packets aren't changed in transmission. This is a crucial prerequisite for communications since the recipient has to understand exactly what the sender wants her to understand.
    - Transmission Errors - Wireless communications are prone to transmission errors due to the instability of wireless channels, channel fading, time-frequency coherence, and inter-band interference are some of the reasons that might cause this. A packet with errors is worthless and forces the sender and recipient to process more data.
    - Processing Errors - Due to the fact that no electronic equipment is perfect, errors might arise in every forwarding node. When operational conditions, such as temperature or humidity, deviate from the norm, electrical devices can malfunction, resulting in packet errors.
    - Packet Modifications – Changes can be made by the attacker on a packet before it reaches the recipient in a hostile environment. This can lead to a slew of issues. If the attacker is familiar with the packet layout and semantic meaning of the communication protocol, he or she may be able to cause more serious damage. In that situation, the attacker can alter a packet's content material so that the receiver receives the incorrect information.
    - Error Control - At the link layer, there are a few error control mechanisms that deal with transmission errors. The idea is to add a few redundancy bits to each link-layer frame, which are calculated using an error detection algorithm and are commonly referred to as a checksum. Each receiving node can examine an obtained checksum of the frame to see if it contains any errors. If a mistake occurs, the receiver can send a notification frame to the sender, requesting that the original frame be retransmitted. An automated repeat request is the name for this process (ARQ). If more redundancy bits are attached to each frame, the receiving node can add even more correct errors, eliminating ARQ.

- The checksum in each frame is produced using a mistake correction coding technique, and this mechanism is known as forward error correction (FEC). On the transport layer, both ARQ and FEC can be utilized to resolve processing errors in intermediate forwarding nodes. Every transport-layer PDU has a checksum computed by the source node, which the destination node inspects to find and repair errors.
- Message Integrity Code - The receiver can send a notification frame to the sender, requesting that the original frame be retransmitted. An automated repeat request is the name for this process (ARQ). If more redundancy bits are attached to each frame, the receiving node can add even more correct errors, eliminating ARQ. The checksum in each frame is produced using a mistake correction coding technique, and this mechanism is known as forward error correction (FEC). On the transport layer, both ARQ and FEC can be utilized to resolve processing errors in intermediate forwarding nodes. Every transport-layer PDU has a checksum computed by the source node, which the destination node inspects to find and repair errors.

- **Authenticity:** To identity communicating nodes authenticity is required. Every node wants to know that a packet it has received came from a legitimate sender. Otherwise, the receiving node may be duped into doing erroneous actions.
  - Packet Injection – Adding to augmenting existing packets, if an attacker is knowledgeable of the packet structure provided inside the network protocol stack, he can immediately inject packets. The injected packets can carry bogus information, which can happen on a regular basis via receiving nodes. Applications that are deployed in a WSN, such as environmental tracking or item tracking, may be interrupted as a result of the bogus data.
  - Message Authentication Code - Authentication is required to deal with false packets and ensure that the originating point of acquired packets is known. A device to solve the problem is a message authentication code (MAC). It is also called as MIC because it ensures packet integrity. Asymmetric key shared by the sender and receiver is necessary to construct a MAC. The payload M and MAC C of the packet are sent to the recipient. The receiver then tests whether C = C holds by recalculating a MAC C with the payload M and the shared key K. If the equation holds, the payload M is authenticated and no longer modified since the sender is most effective aware of the shared key.
  - Signature - Signature is an asymmetric key mechanism for authentication that is widely used. While releasing its public key Kp, a sender node keeps its personal key Ks hidden. To authenticate a plaintext M to the receiver, the sender uses its personal key Ks to sign M into a signature S = S(M, Ks), and then sends the signature S along with the plaintext M to the receiver. Because Ks is a secret, only the sender may produce the signature. Because Kp is widely known, any receiver may verify the signature S by entering the signature S, the plaintext M, and the general public key Kp into a verification set of rules M to calculate V(S, M, Kp). If the output is TRUE, the plaintext M is now authenticated; else, it is no longer authenticated.
  - Authenticating Public Key - The MiM attack is possible because the validity of the global public key cannot be guaranteed. As a result, validating public keys in asymmetric key systems is a critical issue. A public key infrastructure is used in the classic method to broad public key authentication (PKI). There may be a certificate authority (CA) in the PKI, which is relied on by all PKI participants. By default, all of the member nodes accept the CA's public key as an authenticated one. Every member node's general public key is signed by the CA, and the CA provides a certificate to the member node that contains the general public key and the accompanying signature. When two nodes desire to connect, one of them delivers its public key certificates to the other, which may verify

the validity of the general public key contained in the certificates using the CA's well-known public key.

The following are some of the most serious potential security threats in WSNs:

- **Selective forwarding attack:** Assuming all the active nodes in the network are dependable for forwarding it infects the network traffic. The malicious/attacked nodes simply discard such messages rather than transmitting all of them in a selective forwarding attack.

- **Sybil attacks:** In WSNs, a node generates several false identities by inventing or stealing real node identities. Attacks by Sybil will target routing techniques and topology management, limiting the usefulness of fault-tolerant systems like distributed storage and disparity. It's worth noting that regional routing is a form of scheme in which a Sybil node is used**.**

- **Sinkhole attacks:** The attacker uses traffic congestion to draw attention to an attacked node. This attack can be carried out simply by selecting a malicious node that can draw the bulk of traffic, such as one that is closest to the base station or one that is posing as a base station. Sinkhole attacks happen for a variety of reasons, including allowing selective forwarding to lure traffic to the assault.

- **Wormhole attacks:** An attacked node closer to the base station will completely annoy the traffic by tunneling messages across a short latency link. The attacker does this by tricking nodes that are further distant (multi hop) that they are closer to the base station than they actually are. A sinkhole is generated because the intruder on the opposite side of the sinkhole has a misleading route to the base station.

- **Routing loops attack:** This project focuses on the knowledge transferred between nodes. Fake error messages are formed when an attacker alters and repeats the routing information. Routing loops attract or repel network traffic, creating increased node-to-node delay.

- **Hello flood attacks:** Control is a message that was sent with a higher transmission to make it appear as though the HELLO message was being transmitted from the base station. When the nodes get the packet, they assume the HELLO message receiving node is the closest one and attempt to send all of their messages through it. In this form of attack, all nodes will expend a significant amount of energy.

WSN security is currently a prominent topic. For WSNs to be secure, three issues must be addressed: I Key management: To use cryptography, all parties must have the same cryptographic keys. Key management systems are required for each mechanism to maintain secrecy, honesty, authentication, and other security goals. It's a mechanism for establishing and keeping keys across legitimate nodes, as well as updating, revocation, and destruction of keys. Due to resource limits, providing effective key control in WSNs is difficult. (ii) Routing protection is the next issue to address. Remote attackers and infected interns' nodes are the two types of vulnerabilities to routing protocols, all of which are difficult to identify since the compromised node will produce legitimate packets.

Existing WSN routing protocols have little to no security features.

The prevention of denial-of-service attacks is the third issue. Denial-of-service (DoS) is described as any incident that reduces or destroys the network's capacity to perform the functions intended. DoS may be caused by hardware failures, programming glitches, resource depletion, environmental circumstances, or other complex relationship between these variables.

Chapter-6

WSN: CONCLUSION AND FUTURE TRENDS

In recent years, the research community has shown a great deal of interest in wireless sensor networks (WSNs). Over the last several years, a large amount of research has been conducted to answer the practical and theoretical challenges that remain unresolved, resulting in a rise in civil and military projects. Maximum sensor networks are typically used in delay-tolerant and low-bandwidth applications.

Future WSN research could concentrate on maximizing proximity throughput in clustered Wireless Sensor Networks for temporal or spatial random process estimation, accounting for a radio channel, MAC, PHY, and NET protocol layers and information aggregation techniques, simulation and experimental verification of lifetime-aware routing sensing spatial coverage, and the enhancement of lifetime-aware routing sensing spatial coverage and the enhancement of the preferred sensing spat. We agree that WSN research will have a significant impact on everyday living in the near future.

It will, for example, develop a system for continuous monitoring of physiological warnings while patients are at home. It will lower the cost of tracking patients while increasing the effective use of physiological data, and patients will have access to the most pleasant hospital treatment in the comfort of their own homes. Thus, it'll keep away from the misery and disruption due to a prolonged inpatient stay.

We expect stricter security standards to be enforced on WSN applications as wireless sensor networks (WSNs) grow more prevalent. We're crossing our fingers for the best. Because of our research and commitments, good security will most likely become a more practicable standard in the future. We also expect that ongoing and future research in the domains of privacy and trust will make WSNs a more desirable option in a variety of situations.

As a result, the analysis and development of designing technologies that optimize the outputs from the nodes in the future of wireless sensor networks. Potential domains include MAC, PHY, and NET protocol layers and knowledge aggregation methods, lifetime-aware routing sensing spatial coverage modeling and experimental verification, and augmentation of the selected sensing spatial coverage.

ACRONYMS

1. WSN – Wireless Sensor Networks
2. IoT – Internet of Things
3. 6LoWPAN – IPv6 over Low -Power Wireless Personal Area Networks
4. WLAN – Wireless Local Area Network
5. RF – Radio Frequency
6. RFID – Radio Frequency Identification
7. ID – Identification
8. HF – High Frequency
9. LF – Low Frequency
10. UHF – Ultra High Frequency
11. GPS – Global Positioning System
12. RoI – Region of Interest
13. FoV – Field of View
14. MWSN – Mobile Wireless Sensor Networks
15. 2D – Two Dimensional
16. 3D – Three Dimensional
17. OGDC – Optimal Geographical Density Control
18. CCP – Coverage Configuration Protocol
19. PCP – Probabilistic Coverage Protocols
20. OSI – Open Systems Interconnection
21. TCP – Transmission Control Protocol
22. STCP – Sensor Transmission Control Protocol
23. PORT – Price – Oriented Reliable Transport Protocol
24. PSFQ – Pump – Slowly, Fetch Quickly
25. MAC – Media Access Control
26. CSMA/CA – Carrier-sense multiple access with collision avoidance
27. TDMA – Time division multiple access
28. IEEE – Institute of Electrical and Electronics Engineers
29. QoS – Quality of Service
30. ADC – Application Delivery Control
31. SAR – Sequential Assignment Routing
32. PEGASIS – Power-Efficient Gathering in Sensor Information Systems
33. ISP – Internet Service Provider
34. SMP – Sensor Management Protocol
35. SQDDP – Sensor Query and Data Dissemination Protocol
36. RSS – Received Signal Strength
37. LEACH – Low Energy Adaptive Clustering Hierarchy
38. TOA – Time of Arrival
39. TDOA – Time difference of Arrival
40. AOA – Angle of Arrival
41. FEQ – Forward Error Correction
42. ARQ – Automatic Repeat Request
43. ISA – International Society for Automation
44. HART – Highway Addressable Remote Transducer User Interface
45. PAN – Personal Area Networks
46. PHY – Physical
47. NET – Network

APPENDIX I – REFERENCES

1. https://ieeexplore.ieee.org/document/6616688
2. https://www.intechopen.com/chapters/38793
3. https://www.intechopen.com/chapters/56541
4. https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf
5. https://www.totalphase.com/blog/2019/04/sensor-networks-the-advantages-and- disadvantages-you-need-to-know/
6. http://sensors-and-networks.blogspot.com/search?q=leach
7. https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/
8. https://www.researchgate.net/figure/Network-Models-Hierarchical-and-Distributed-Wireless-Sensor-Networks_fig1_267241899
9. https://www.researchgate.net/publication/313198672_Network_topologies_in_wireless_sensor_networks_A_review
10. https://www.elprocus.com/introduction-to-wireless-sensor-networks-types-and-applications/
11. http://sensors-and-networks.blogspot.com/2011/10/flooding.html
12. http://sensors-and-networks.blogspot.com/search?q=SPIN