Research Report

# Sensor Networks

## COEN 331 – Wireless & Mobile Networks

Submitted by:

**UDIT SHARMA – W1605819**

Guided by:

**Dr. Keyvan Moataghed**

# Audience

*Wireless sensor networks are discussed in this research study. It is a must-have resource for anyone interested in sensor network wireless communication. It begins with an overview of key ideas and protocols related to wireless sensor networks. Localization of nodes, transport protocols, network security, and future trends in WSNs are all covered.*

*The reader of this report should have a fundamental understanding of wireless networks, architecture, and protocols, along with many other basics. Students, working professionals, and anybody interested in learning more about Wireless Sensor Networks would benefit from this research.*

# 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 collecting and displaying real-world events and transforming these into data that can be analyzed, stored, and operated accordingly. Sensors, which are integrated into a variety of devices, equipment, and settings, give a significant societal benefit.

They can aid in the prevention of catastrophic infrastructure failures, conservation of natural resources, increased productivity, improved security, and the development of new applications like as context-aware systems and smart home technologies.

This research paper gives a complete overview of the fundamentals of wireless sensor networks, including network technologies and protocols, operating systems, middleware, sensor programming, and security, as well as the theoretical and practical features of each.

# 1.1 Introduction to Sensor Networks

## 1.1.1 *Sensor Networks Definition*

A sensor network is made up of a collection of small, battery-powered devices. They are commonly used to display physical or environmental conditions such as temperature and sound, and they send their data via the network to a central sink or base station, where it is analysed and monitored.

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.

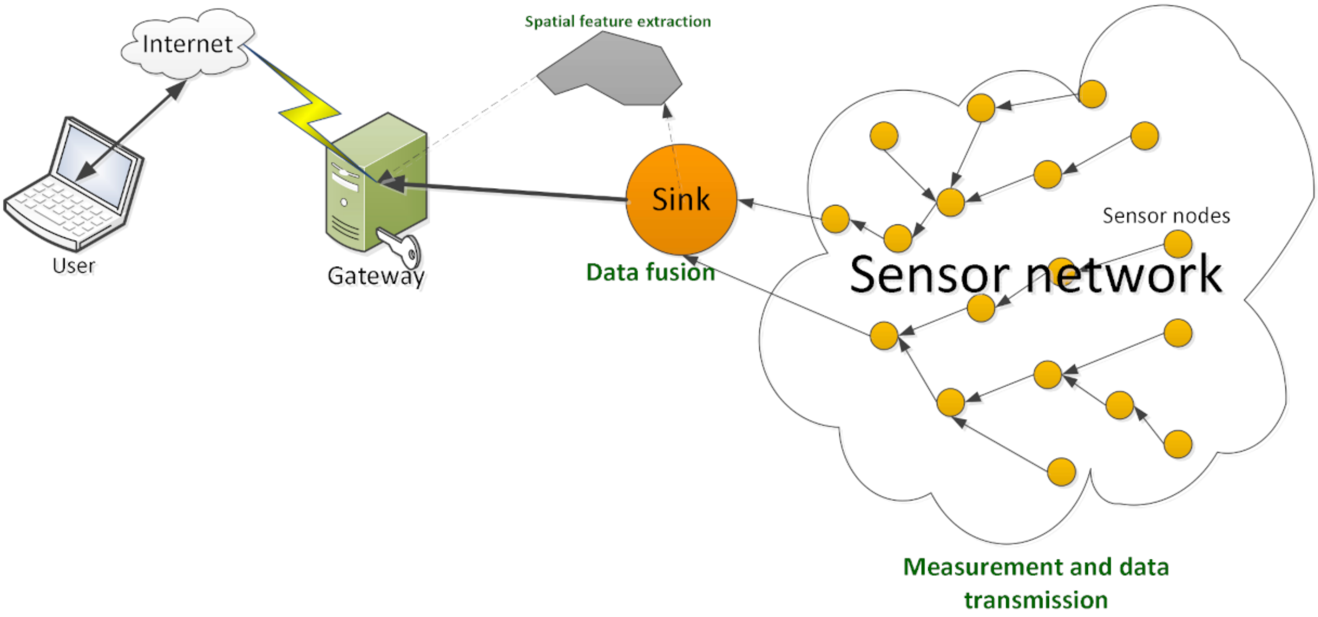


**Figure 1.1 Representation of a wireless sensor network**

## 1.2 Overview of Wireless Sensor Network

Because of the multiple constraints, wireless sensor networks (WSNs) allow for innovative programs and requires non-traditional protocol layout paradigms. 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: they have limited communication bandwidth, processing speed, and storage capacity. In recent times researchers have centered on heterogeneous sensor networks in which the sensor nodes are in contrast to every difference in phases in their energy. New network architectures with heterogeneous gadgets and the current development of this generation dispose of the contemporary obstacles and amplify the spectrum of viable programs for WSNs significantly and these kinds of are converting very rapidly. This generates a significant effort in research activities, standardization processes, and time. The most of WSN research has focused on the design of power by computationally green algorithms and protocols, with software limited to simple facts-oriented tracking and reporting programs.

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

Sensor classification is all about deciding which sensor is best for a given application. The physical attribute to be monitored, such as temperature, pressure, light, or humidity, determines the sensor to be used. Some of the most frequent physical features are summarized in Table 1.1. Aside from physical characteristics, sensors can be classified using a range of different criteria, such as whether they require an external power supply. Active sensors are those that require an external power source to operate. Because they use energy (light, microwave, or sound) to elicit a reaction or detect a change in the energy sent signal. Passive sensors sense energy in the environment and obtain their power from it; for example, infrared sensors detect infrared light emitted by things in the vicinity.

| | |
|---|---|
| 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

The University of California in Los Angeles proposed the notion of Wireless Integrated Network Sensors, or WINS, in collaboration with the Rockwell Science Center (Pottie 2001). The Low Power Wireless Integrated Microsensor (LWIM), that was delivered in 1996, was one of the WINS project's outcomes (Bult et al. 1996). This smart detection system was based on a CMOS chip that combined many sensors, interface circuits, computerized signal preprocessing circuits, a remote radio, and a microcontroller onto a single chip. The University of California at Berkeley's Smart Dust project (Kahn et al. 1999) focused on the concept of tiny sensor hubs known as bits. The goal of this project was to show that a complete sensor framework may be included into microscopic devices as small as a grain of sand or even a single molecule. The Berkeley Wireless Examination Center's (BWRC) PicoRadio project (Rabaey et al. 2000) focuses on the development of low-power sensor devices with low power consumption to the point where they can control themselves using fuel sources from the working environment, such as solar or vibrational energy. Low-power equipment and programming segments for sensor hubs are also a focus of the MIT µAMPS (miniature Versatile Multidomain Power-mindful Sensors) project, which includes the use of microcontrollers capable of dynamic voltage scaling and strategies to rebuild information preparation calculations to reduce power requirements at the product level (Calhoun et al. 2005).

While scholarly organizations have largely determined previous endeavors, a number of business ventures have emerged in the last decade (many of which are based on some of the scholarly endeavors depicted above), including Crossbow, Sensoria, Worldsens, Dust Networks, and Ember Corporation. These companies sell sensor devices that are ready to send in a variety of scenarios, as well as various administration tools for programming, support, and sensor data formatting.

# 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, such as in a forest, where sensor nodes are dropped from an airplane. 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. The individual cost of each sensor node should be as low as possible in order to keep the overall infrastructure costs to a minimum.

- **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, resulting in protocols and algorithms that differ from those used in other distributed systems.

- **Energy**

Sensor hubs operate on limited energy constraints, which is a common restriction associated with sensor network architecture. They are often powered by batteries, which must be replaced or re-energized (e.g., using sunlight-based energy) when they run out. For some hubs, neither alternative is appropriate, which means they will be discarded after their fuel source is depleted. 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 passed or the battery can be replaced. The duration of the mission is determined by the type of application; for example, researchers watching frigid developments may require sensors that can work for several hours or days, but a sensor in a front-line situation may only be required for a few hours or days.

As a result, energy productivity is often the first and most major difficulty for a WSN. This requirement pervades every aspect of the sensor hub and organization strategy. The decisions taken at the actual layer of a sensor hub, for example, have an impact on the overall energy consumption of the device and the design of higher level standards.

- **Self-Management**

Many sensor network applications are designed to function in remote locations and extreme conditions, with no infrastructure support or maintenance and repair options. Sensor nodes must therefore be self-managing, in the sense that they must configure themselves, operate and collaborate with other nodes, and adapt to failures, changes in the environment, and changes in the environmental stimuli without the need for human intervention.

Many wireless 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 a number of setup and configuration tasks on their own, including establishing communications with surrounding sensor nodes, determining their positions, and initiating their sensing responsibilities.

The amount and type of information that sensor nodes generate and convey on behalf of other nodes can vary depending on such information. For example, a node's location and the number or identities of its neighbors may impact the amount and type of information that it generates and forwards.

- **Wireless Networking**

A sensor network designer faces various issues due to the dependency on wireless networks and communications. For example, attenuation restricts the range of radio transmissions, which means that as a radio frequency (RF) signal propagates across a medium and passes through barriers, it fades (i.e., loses power).

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

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

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

As a result, as the distance between a sensor node and a base station grows, the needed transmission power grows as well. 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 vast and too energy-constrained to use centralized algorithms (e.g., at the base station) to perform network management solutions like topology management or routing. Instead, sensor nodes must work together with their neighbors to make localized judgments, i.e. without access to global information. As a result, these decentralized (or distributed) algorithms will not produce ideal outcomes, but they may be more energy-efficient than centralized alternatives.

As an example, consider routing for both centralized and decentralized methods. A base station can collect data from all sensor nodes, determine optimal routes (e.g., in terms of energy consumption), and notify each node of its route. The overhead, on the other hand, can be substantial, especially if the topology changes regularly. Instead, a decentralized method enables each node to make routing decisions based on limited local data (for example, a list of the node's neighbors and respective distances from the base station). While this decentralized strategy may result in inefficient routes, administration overheads can be greatly minimized.

- **Design Constraints**

Sensor nodes have the processing speeds and storage capacity of computer systems from decades ago, driven by the necessity to run specialised applications with minimal energy consumption. Many desirable components, such as GPS receivers, cannot be included due to the need for a tiny form factor and low energy usage. These restrictions and needs have an impact on software design at multiple levels; for example, operating systems must have compact memory footprints and be resource management tasks efficient. However, the lack of complex hardware features (such as support for parallel executions) makes tiny and efficient operating systems easier to develop. The hardware limits of a sensor have an impact on the design of various protocols and algorithms used in a WSN. Routing tables, for example, that contain entries for each potential network destination, may be too extensive to accommodate in a sensor's memory.

- **Security**

Several distant sensor networks collect sensitive data. Sensor hub's remote and unmanaged activity increases their vulnerability to malicious disruptions and assaults. Remote correspondences also make it easy for an adversary to listen in on sensor transmissions.

For example, one of the most complex security threats is a refusal-of-administration attack, which aims to disrupt a sensor organization's proper operation. This can be performed by a variety of attacks, such as a sticking attack, which uses powerful distant signals to prevent effective sensor correspondences. The consequences can be severe, depending on the type of sensor network application. While there are a variety of strategies and solutions for appropriated frameworks that prevent attacks or limit the severity and harm of such attacks, many of them impose significant computational, correspondence, and capacity requirements that are frequently insurmountable 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

When selecting hardware components for a wireless sensor node, the application's requirements are clearly a deciding factor, especially in terms of the node's size, cost, and energy consumption – communication and computation facilities are frequently considered to be of acceptable quality, but the trade-offs between features and costs are critical. An entire sensor node should, in certain extreme situations, be smaller than 1 cc, weigh (considerably) less than 100 g, cost less than $1, and dissipate less than 100 W. The nodes are often stated to have to be lowered to the size of grains of dust in even more extreme visions. In more practical applications, the size of a node is less significant than its convenience and simplicity.

Despite these differences, when looking at popular hardware platforms for wireless sensor nodes, a consistent pattern can be seen in the literature. While no single standard exists, and no single standard would be able to cover all application kinds, this section will look at some of the most common sensor node architectures. In addition, a number of research initiatives are focusing on reducing the size, energy consumption, and costs of any of the components, based on the fact that custom off-the-shelf components currently do not meet some of the more rigorous application criteria. These attempts are not explored in this book because it concentrates on the networking elements of WSNs.

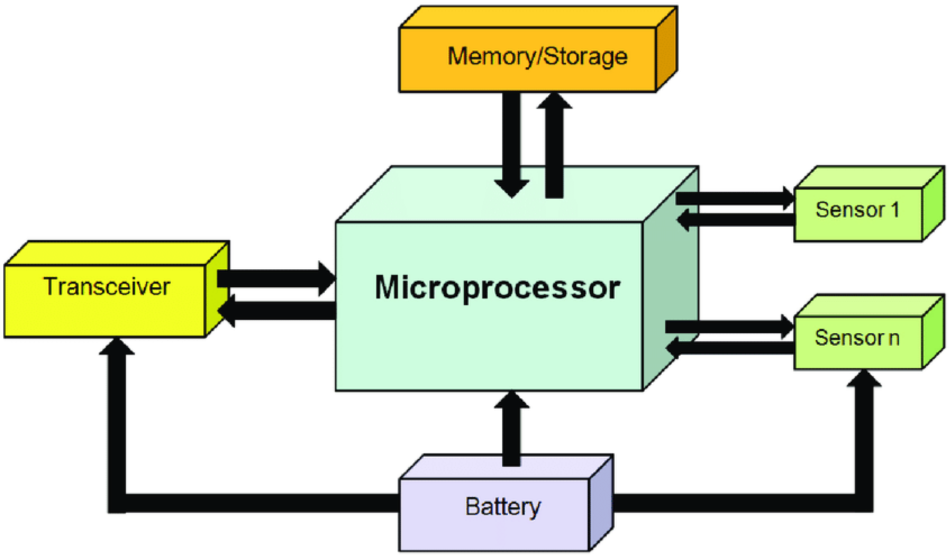


**Figure 2.1 Overview of main sensor node hardware components**

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

- **Controller -** A controller that can process all relevant data and run any code.
- **Memory -** Some memory to store programs and intermediate data; programs and data are usually stored in various types of memory.
- **Sensors and actuators -** Devices that can observe or control physical parameters of the environment are the actual interface to the physical world.
- **Communication -** To turn nodes into a network, you'll need a device that can send and receive data across a wireless channel.

# 2.2 WSN Structures

## 2.2.1 Star Topology

The base station is at the center of a star network that sends and receives data from sensor nodes. Low-latency communication between the distant node and the sink station is also possible.

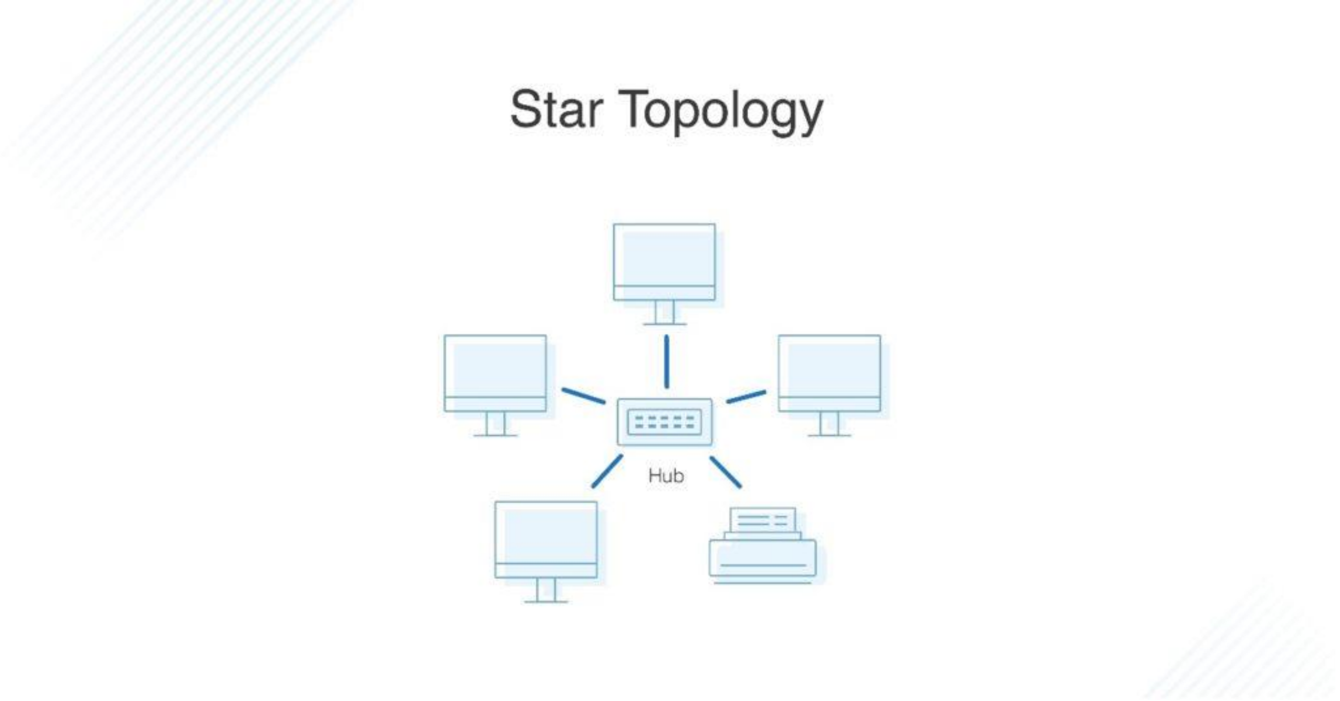


**Figure 2.2 Star Topology**

## 2.2.2 Partial Mesh Topology

A partial mesh, unlike a full mesh, does not have all nodes connected. As a result, one node is linked to two or more others. This allows for a low level of complexity and expenditure while maintaining a high level of functionality.

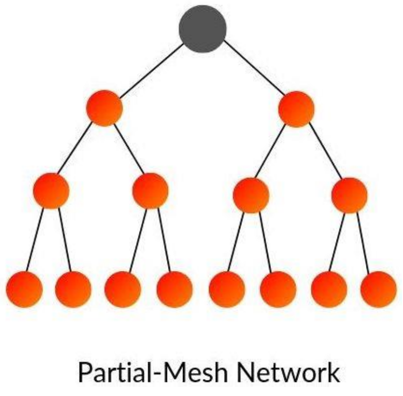


**Figure 2.3 Mesh (partially connected) Topology**

## 2.2.3 Mesh Topology

A full mesh network is one in which every node is connected to every other node. This is a direct point-to-point link between all nodes. The mesh's nodes are all equally critical, and they share equal responsibility for data transmission. This may increase the cost of the network.

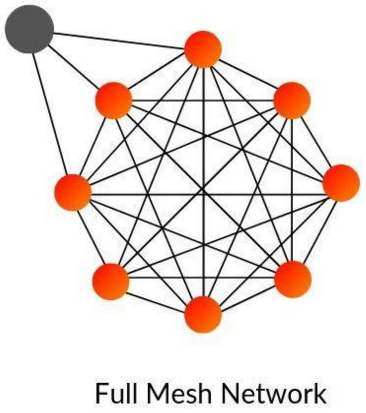


**Figure 2.4 Mesh (fully connected) Topology**

## 2.2.4 Ring Topology

Every node in a ring topology is connected to another node. Data is transmitted from one node to another node in a ring. A node failure breaks the loop and can bring the entire network down, but it also causes traffic congestion and double-path communication.

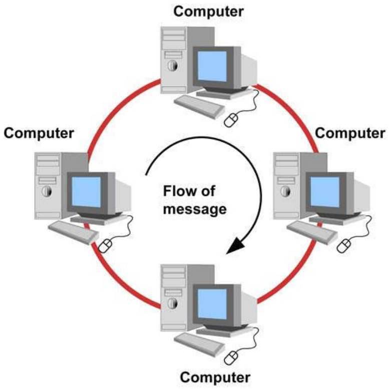


**Figure 2.5 Ring Topology**

## 2.2.5 Circular Topology

There is a circular sensing area in this topology, and the sensing area has a sink/gateway (at center). The sensor nodes detect the interesting event and communicate the information to the sink. As shown in Figure 3.4.6, the nodes are placed at random around the sink, with a uniform concentration. Data must transit single or multiple hops before being received by the sink, depending on the distance/length of a node from the sink and the communication range of the nodes. The circular web architecture is simple to set up and maintain, as well as more efficient.

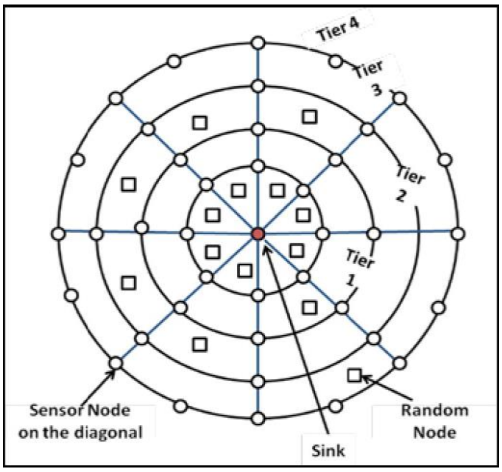


**Figure 2.6 Circular Topology**

### 2.2.6 Hybrid Topology

A hybrid network is created when one or more technologies are integrated to create a network. For some specific purposes to be implemented in a network, the hybrid topology might be quite useful. Star-bus networks, Hierarchical star networks, Star-ring networks, and Hybrid mesh networks are examples of hybrid networks.

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

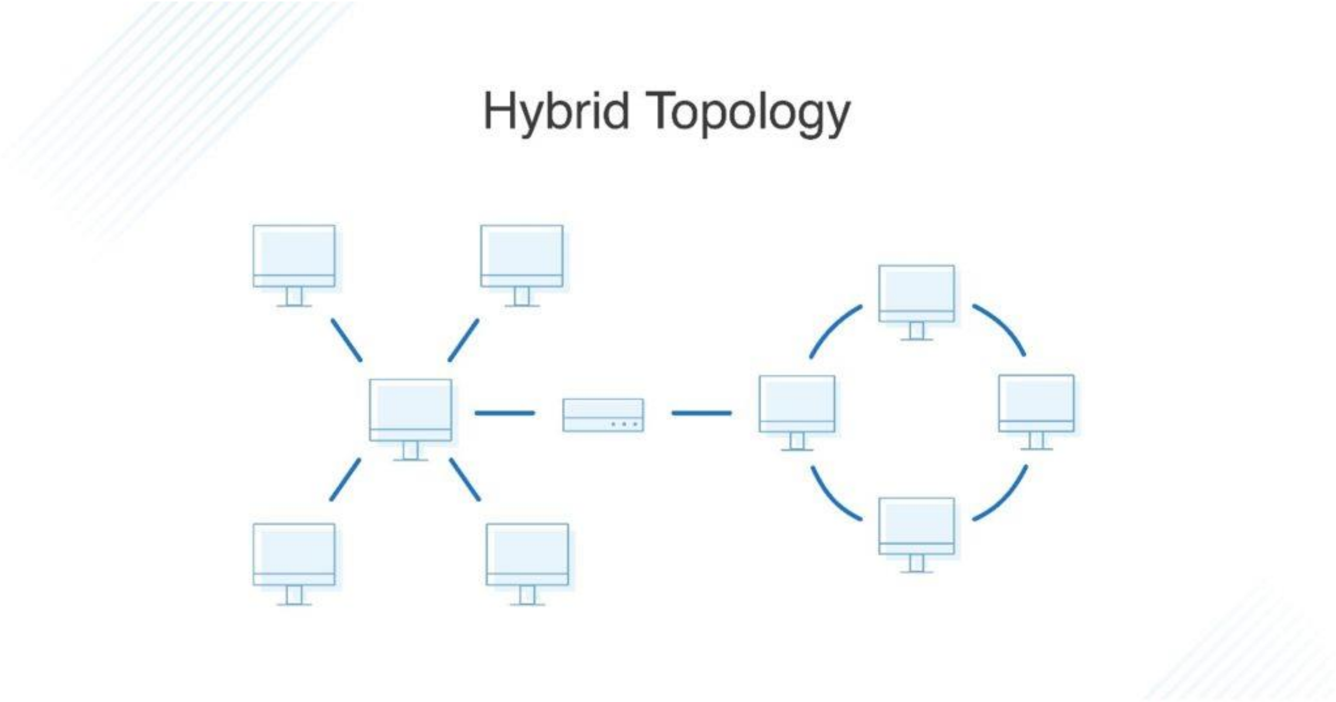


**Figure 2.7 Hybrid Topology**

## 2.3 Types of WSN

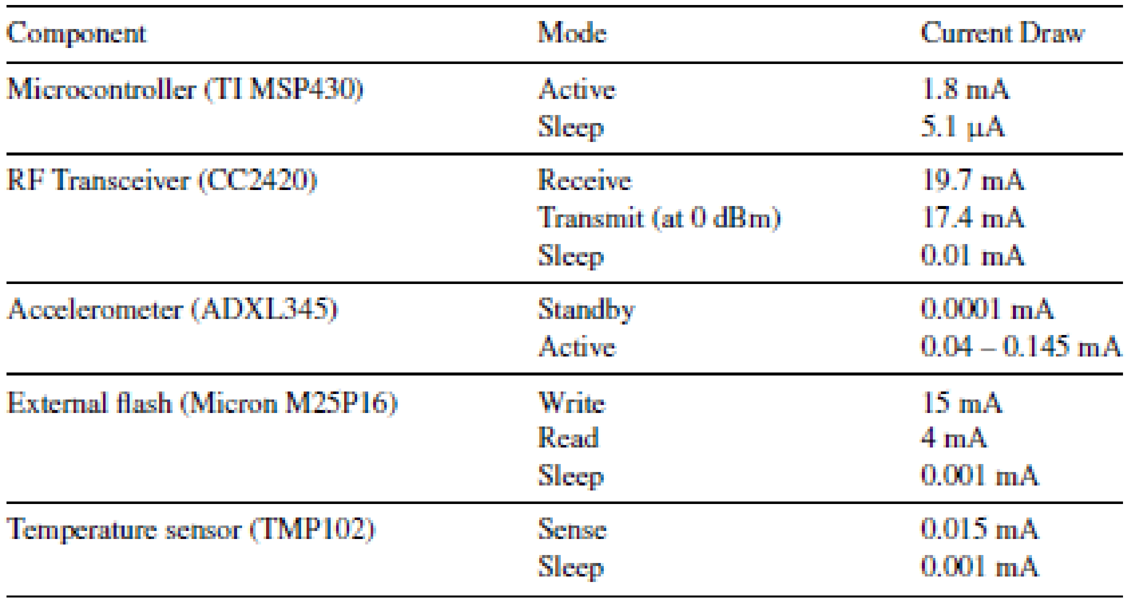
- **Cyber-physical system (CPS)** - It tries to better characterize what these networks can perform and their main qualities when they are integrated into a physical context. Cyber-physical systems, unlike other computers and gadgets that are environment agnostic, are part of the environment and application specific. Another significant feature is that they may influence the environment with so-called actuators, such as those used in automatic irrigation pumps, light switches, alarms, and humidity or temperature regulators.

- **Body sensor networks -** They are a form of network that is designed to be worn on the person's body (mostly human). Health tracking, weight control, sports reporting, and a variety of other applications are just a few of the possibilities. Smart sneakers and smart T-shirts, for example, can detect your activity or heart rate. The majority of sensor nodes are small and can be implanted.
- **Crowdsourcing** - It refers to a new and fast-developing type of detection in which the sensors are essentially people with cell phones. Individuals can, for example, follow their trekking routes and then assess them in terms of security, commotion, and street condition. This data is gathered on a crucial topic and organized into a single city hiking quality guide that can be adapted to any interested client. The real power of these applications is that they don't require any additional hardware, simply a simple client-installed program for smart phones.

- **The Internet of Things (IoT) -** The primary notion of the Internet of Things is that everything, including a washing machine and a radio, is connected to the Internet. When it comes to sensor networks, having an Internet connection provides a lot of advantages, and it can be considered an enabling technology. The goal, on the other hand, can be extremely different, such as when you can read your emails in the microwave or in your automobile. The word "internet" also implies that these networks are typically IP-enabled and hence employ a well-defined communication stack. This can be viewed as a benefit (no need to reimplement) or a disadvantage (no need to reimplement) (high energy use, little flexibility).

## 2.4 Power Consumption

The power consumption of sensor node hardware is one of the most critical properties to understand. 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<br>Sleep | 1.8 mA<br>5.1 µA |
| RF Transceiver (CC2420) | Receive<br>Transmit (at 0 dBm)<br>Sleep | 19.7 mA<br>17.4 mA<br>0.01 mA |
| Accelerometer (ADXL345) | Standby<br>Active | 0.0001 mA<br>0.04 – 0.145 mA |
| External flash (Micron M25P16) | Write<br>Read<br>Sleep | 15 mA<br>4 mA<br>0.001 mA |
| Temperature sensor (TMP102) | Sense<br>Sleep | 0.015 mA<br>0.001 mA |

**Table 2.1 Nominal Power Consumption of Components**

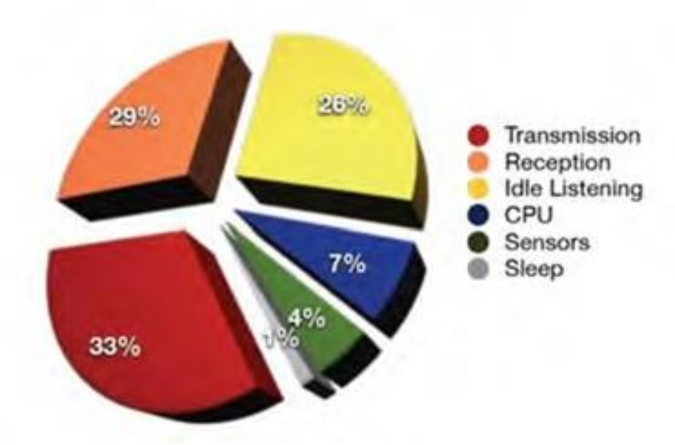


**Figure 2.8 Power consumption of a WSN Node**

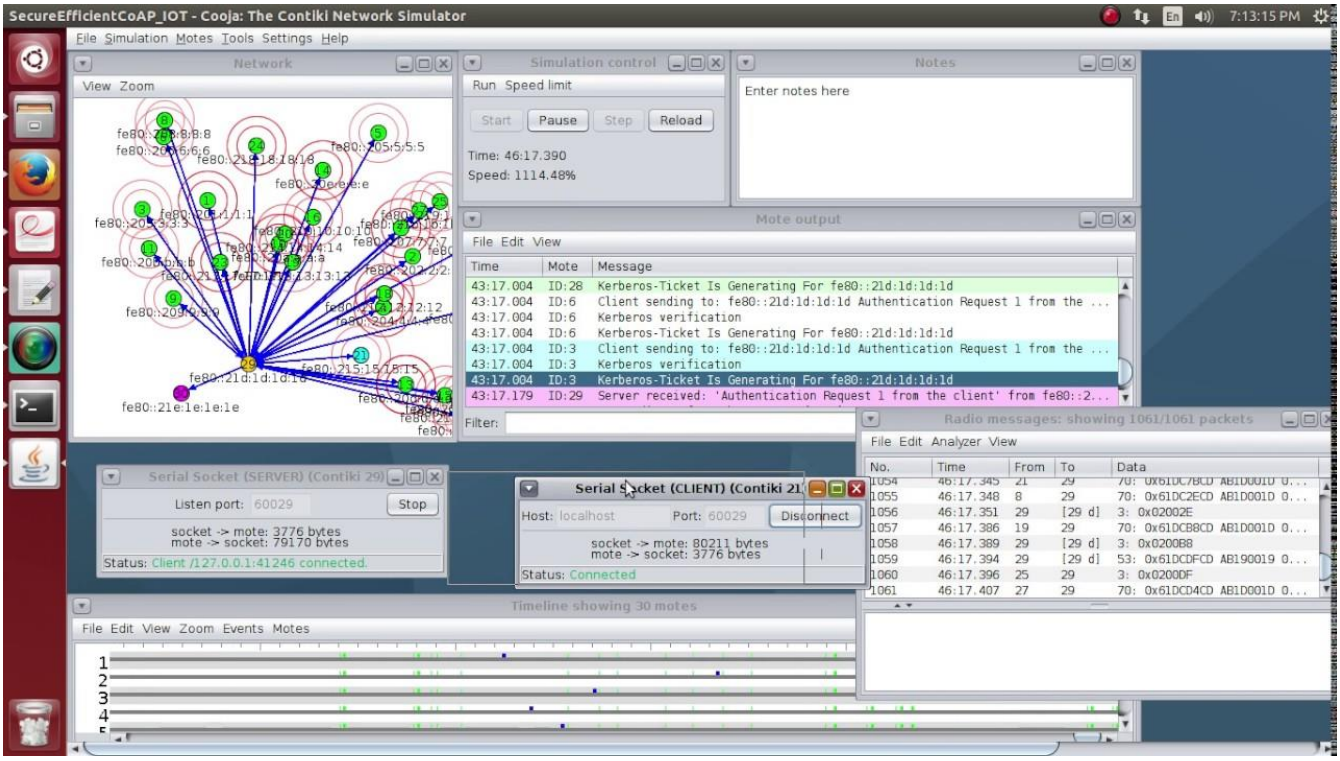
All of the power usage in the above table is presented in Amperes (A). For example, even when the radio is turned off and sleeping, it consumes 0.01 mA. The sensors are supposed to deliver a continuous voltage of 3 volts from the batteries attached to the sensor node.

These calculations are purely theoretical, and actual batteries or hardware may respond 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 sleeping hours for the radio are introduced (the so-called duty cycle). To save 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 software system that runs on a regular computer and simulates the behavior and interactions of another system. A sensor network simulator, for example, simulates the behavior of sensor nodes and their communication with one another.



Time: 46:17.390
Speed: 1114.48%

```
Time       Mote   Message
43:17.004  ID:28  Kerberos-Ticket Is Generating For fe80::21d:1d:1d:1d
43:17.004  ID:6   Client sending to: fe80::21d:1d:1d:1d Authentication Request 1 from the ...
43:17.004  ID:6   Kerberos verification
43:17.004  ID:6   Kerberos-Ticket Is Generating For fe80::21d:1d:1d:1d
43:17.004  ID:3   Client sending to: fe80::21d:1d:1d:1d Authentication Request 1 from the ...
43:17.004  ID:3   Kerberos verification
43:17.004  ID:3   Kerberos-Ticket Is Generating For fe80::21d:1d:1d:1d
43:17.179  ID:29  Server received: 'Authentication Request 1 from the client' from fe80::2...
```

Serial Socket (SERVER) (Contiki 29)

Listen port: 60029 Stop

socket -> mote: 3776 bytes
mote -> socket: 79170 bytes

Status: Client /127.0.0.1:41246 connected.

Serial Socket (CLIENT) (Contiki 21)

Host: localhost Port: 60029 Disconnect

socket -> mote: 80211 bytes
mote -> socket: 3776 bytes

Status: Connected

```
No.   Time       From  To      Data
1054  46:17.345  21    29      70: 0x61DC7BCD AB1D001D 0...
1055  46:17.348  8     29      70: 0x61DC2ECD AB1D001D 0...
1056  46:17.351  29    [29 d]  3: 0x02002E
1057  46:17.386  19    29      70: 0x61DCB8CD AB1D001D 0...
1058  46:17.389  29    [29 d]  3: 0x0200B8
1059  46:17.394  29    [29 d]  53: 0x61DCDFCD AB190019 0...
1060  46:17.396  25    29      3: 0x0200DF
1061  46:17.407  27    29      70: 0x61DCD4CD AB1D001D 0...
```

**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. It states that if the collector is inside a certain circular zone around the transmitter, 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. When your typical sensor nodes are also moving, such as when they are mounted to bikes or buses, this model is extremely handy. Some models are quite simple, such as the random waypoint. It always chooses a new random spot anywhere in the simulated area and allows the sensor to “drive” there at a steady predetermined speed, then chooses another, and so on.

**The traffic model** dictates how many events have occurred in the environment. Sensor networks are used to detect anything, such as temperature, rain volume, and so on. Understanding when events worth conveying are generated in a real environment, 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 radio transceiver operating in one of the free bandwidths, which are reserved internationally for research and medical uses, is the most widely utilized interface.

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:

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

A natural wave does not carry any information. To encode some information into it for data communication, you must change the parameters of the radio wave in a well-defined way so these changes can be detected at the receiver side and the same information can be decoded.

To modulate the signal, any of the three properties of the radio wave, or combinations of them, can be used:

_ **Amplitude** A(t). This parameter gives how high the wave is. To encode information, you can change the amplitude from very small (encoding a 0) to very high (encoding a 1).

_ **Frequency or period** f(t). This parameter dictates how often the wave form is repeated over time. The signal's frequency can be altered to signify different codes.

_ **Displacement or phase** $\phi$(t). This parameter identifies the displacement of the wave in respect to the beginning of the axes. You can displace the wave to indicate change of codes.

The symbol you're encoding onto the modulation code wave is called a modulation code, or key. For example, if you chose to encode a 1 with a very high amplitude and a 0 with a very low amplitude, you'll have two codes or keys. Of course, by using more than two levels of amplitude or more than two different frequencies, more than two keys or (ones and zeros) can be encoded into the signal. Many new modulation codes can be created by combining different modulation codes. The modulation and demodulation processes are both simple to learn and use. In reality, all wireless communications employ wave modulation.

But, given the issues associated with wireless communications in ordinary life, why do they occasionally fail to perform as expected? Wave propagation attributes across your surroundings, or what remains of the wave after it travels a certain distance through the environment, cause problems (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:** Sharp edges and uneven surfaces in the environment will split the wave into multiple secondary waves, each with the same effects as those shown in Figure 3.1.

- **Doppler effect:** In general, a signal's frequency fluctuates with its relative velocity to the receiver. The Doppler effect is well recognized for its effect on police sirens, which sound different depending on whether the officer is approaching or moving away. 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.

**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.

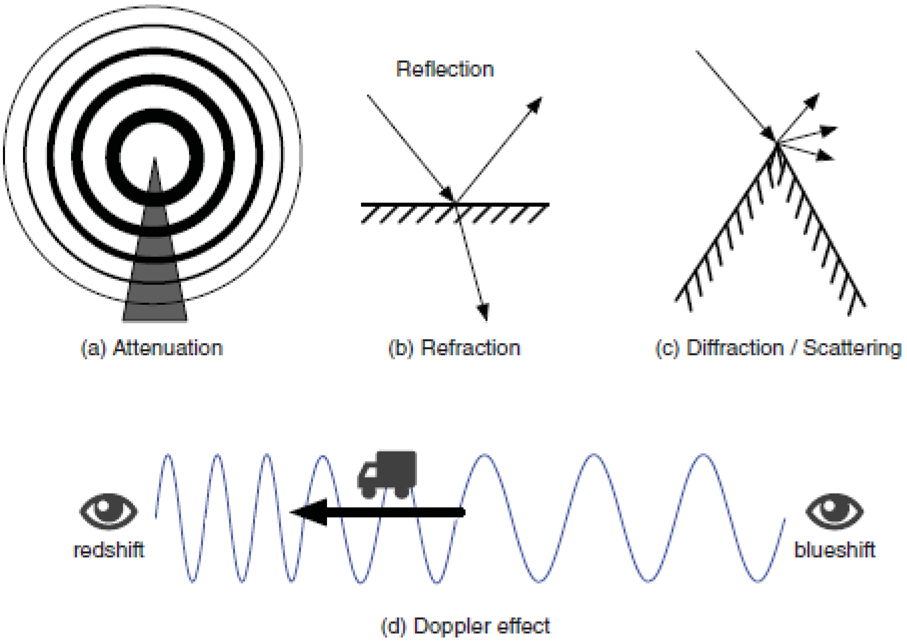


**Figure 3.1 Physical Processes that lead to path loss in signal propagation**

## 3.2.1 Hidden Terminal Problem

A diagram is the best way to illustrate the hidden terminal problem. There are four nodes visible, as you can see. Packet X is sent from node A to node B. propagation Since node C is outside of node A's transmission range, it is unaware of the ongoing transmission of packet X. The transmission range is described as a semi-circular area around the transmitter.

Since node C is unaware of the ongoing transmission between A and B, it begins sending a packet to node D. Interference occurs at node B, causing packet X to be corrupted. The transmission between C and D, on the other hand, is successful. The Hidden terminal problem is a major challenge to overcome in wireless communications. Let us see how to resolve the problem.

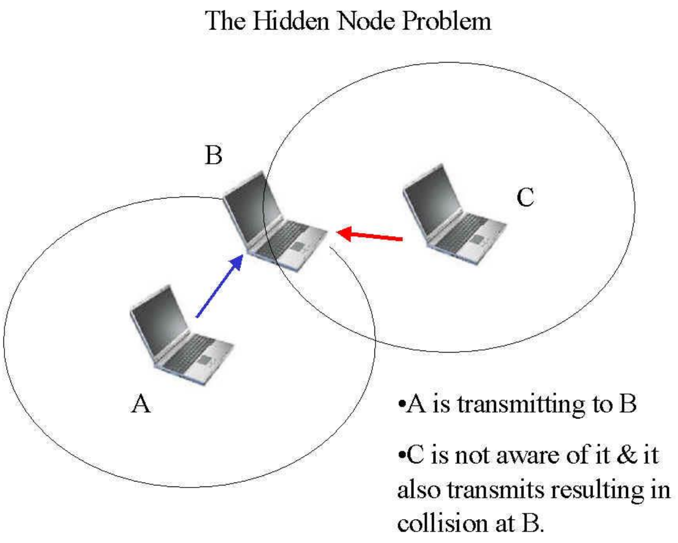

The Hidden Node Problem
B
C
A
•A is transmitting to B
•C is not aware of it & it also transmits resulting in collision at B.

**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 define some critical measures that will help you determine how well a medium access protocol (MAC protocol) is operating.

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

Carrier sense multiple access (CSMA) is a simple but effective protocol that works on the "listen before chat" premise. The sender initially listens to the shared channel before attempting to send if it is available. The two main variations of CSMA are CSMA with collision detection (CSMA-CD) and CSMA with collision avoidance (CSMA-CA) (CSMA-CA). If a CSMA-CA error occurs, CSMA-CD attempts to detect a collision and resends the packet. The second tries to avoid the accident occurring in the first place. This discussion will concentrate on CSMA-CA because it is more widely used and performs better.

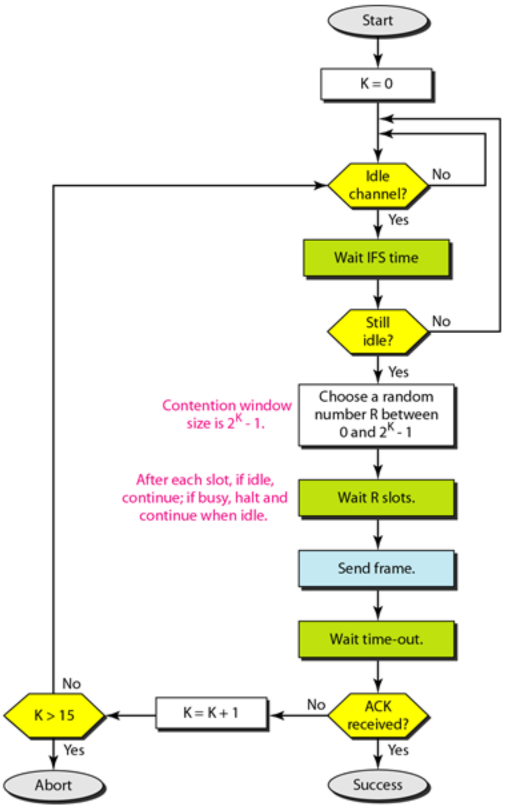

Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Contention window size is $2^K$ - 1.
Choose a random number R between 0 and $2^K$ - 1
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
No
K > 15
K = K + 1
No
ACK received?
Yes
Yes
Abort
Success

**Figure 3.3 Flow diagram of general CSMA with collision avoidance**

Overall, CSMA is a simple and easy-to-understand protocol that functions brilliantly in the majority of situations. However, its main disadvantage in terms of sensor networks is its high energy consumption. It never puts the nodes to sleep, and it quickly depletes a sensor node's energy (typically a couple of hours).

## 3.3.2 Sensor MAC

Sensor MAC (S-MAC) was designed specifically for sleep-enabled sensor networks. It allows nodes to sleep and only communicate when they are actively participating or awake. This is shown in Figure below, and it is the preferred mode of operation for sensor nodes due to its energy efficiency. The link between active and sleeping time is known as the service cycle.

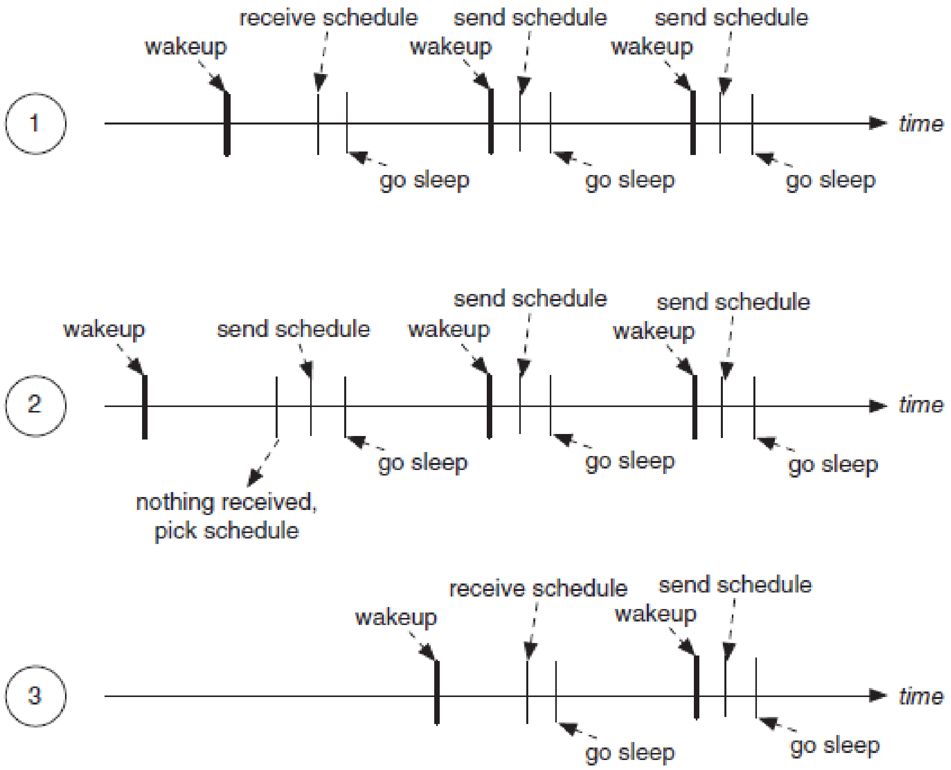


**Figure 3.4 Sensor MAC general scenario**

**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). Although there are no collisions, there are major delays.

⇒ ***Carrier Sense Multiple Access* (CSMA):** As Carrier Sense Multiple Access (CSMA) puts it, "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, implying that a packet is received by all of its neighbors save the node from whence it was received. 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 in which the receiving node sends the packet to a randomly selected neighbor, 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 WSNs are flat-based routing, hierarchical-based routing, adaptive-based routing, multi-path routing, query-based routing, and negotiation-based routing.

### 4.2.1 Flat routing

**Sequential Assignment Routing (SAR) -** The sequential assignment routing (SAR) 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. Higher priority packets take lower delay routes, and lower priority packets must use the routes of higher delay.

**Directed Diffusion** - The directed diffusion technique is beneficial when sensor nodes issue requests/queries for information sensed by other nodes. Each sensor node receives data with one or more identifying parameters.

## 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**-LEACH (Low Energy Adaptive Clustering Hierarchy) 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, and shape and manage clusters.

**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 consumption increases, it can be increased by maintaining multiple pathways between the source sensor node 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 query's initiator, the destination node, promotes a demand for information (sensing task) from a node across the network, and a node receiving the relevant data delivers data that matches the query back 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.

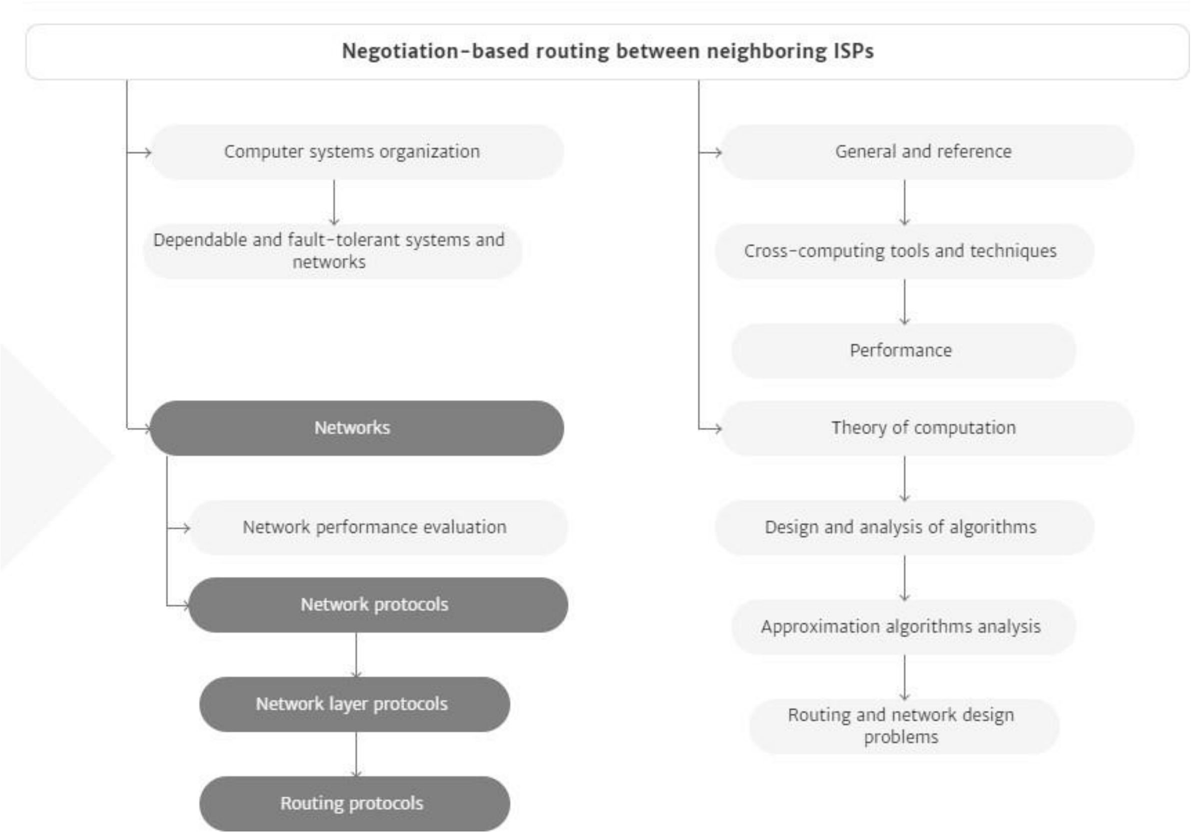

Negotiation-based routing between neighboring ISPs
Computer systems organization
Dependable and fault-tolerant systems and networks
Networks
Network performance evaluation
Network protocols
Network layer protocols
Routing protocols
General and reference
Cross-computing tools and techniques
Performance
Theory of computation
Design and analysis of algorithms
Approximation algorithms analysis
Routing and network design problems

**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. In the context of 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 primary requirement for communications due to the fact the receiver wishes to recognize precisely what the sender needs her to recognize.
    - Transmission Errors - Wireless communications are prone to transmission errors due to the instability of wireless channels, which can be caused by a variety of factors such as channel fading, time-frequency coherence, and inter-band interference. 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 operating conditions, such as temperature or humidity, are outside of the typical range, electrical devices can malfunction, resulting in packet errors.
    - Packet Modifications - An attacker can change 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 happens, the receiver can deliver a notice frame to the sender to request a retransmission of the original frame. This remarks mechanism is known as an automatic repeat request (ARQ). If extra redundancy bits are connected to every frame, the receiving node can also add even correct mistakes and accordingly avoiding ARQ.

  - This mechanism is known as forward error correction (FEC) and the checksum in every frame is computed in keeping with a mistake correction code algorithm. Both ARQ and FEC also can be used on the transport layer to address the processing mistakes incurred in intermediate forwarding nodes. The source node computes a checksum for every transport-layer PDU and the destination node inspects the checksum to discover or correct mistakes.
  - Message Integrity Code - If a mistake happens, the receiver can deliver a notice frame to the sender to request a retransmission of the original frame. This remarks mechanism is known as an automatic repeat request (ARQ). If extra redundancy bits are connected to every frame, the receiving node can also add even correct mistakes and accordingly avoiding ARQ. This mechanism is known as forward error correction (FEC) and the checksum in every frame is computed in keeping with a mistake correction code algorithm. Both ARQ and FEC also can be used on the transport layer to address the processing mistakes incurred in intermediate forwarding nodes. The source node computes a checksum for every transport-layer PDU and the destination node inspects the checksum to discover or correct mistakes.

- **Authenticity:** To identity communicating nodes authenticity is required. Every node wishes to realize that an obtained packet comes from an actual sender. Otherwise, the receiving node may be cheated into doing some incorrect actions.
  - Packet Injection - In addition to enhancing present packets, an attacker can at once inject packets if he is aware of the packet layout described inside the network protocol stack. The injected packets can convey fake information, which can be regularly occurring via way of means of receiving nodes. Applications deployed in a WSN, for instance, environmental tracking or item tracking, maybe disrupted via way of means of the fake information.
  - Message Authentication Code - In order to cope with fake packets, authentication is fundamental to make sure the starting place of obtained packets. Message authentication code (MAC) is a device to remedy the problem. It also can be known as MIC as it guarantees packet integrity as well. To compute a MAC, asymmetric key shared among the sender and the receiver is required. The packet such as payload M and the MAC C is dispatched to the receiver. The receiver recomputes a MAC C¢ with the payload M and the shared key K after which checks whether or not C¢ = C holds. If the equation holds, the payload M is authenticated and now no longer changed due to the fact most effective the sender is aware of the shared key.
  - Signature - Signature is an asymmetric key technique, that's broadly utilized in authentication. A sender node continues its personal key Ks in secret even as publishing its public key Kp. In order to authenticate a plaintext M to the receiver, the sender makes use of its personal key Ks to sign M right into a signature S = S(M, Ks) after which transmits the signature S, in addition to the plaintext M to the receiver. Only the sender can generate the signature because Ks is secret. Because Kp is publicly nicely-known, any receiver can affirm the signature S via way of means of inputting the signature S, the plaintext M, and the general public key Kp right into a verification set of rules M to compute V(S, M, Kp). If the output is TRUE, the plaintext M is authenticated, and in any other case now no longer.
  - Authenticating Public Key - The reason that the MiM assault is viable is that the authenticity of the general public key can not be assured. Therefore, authenticating public keys in asymmetric key systems is a totally vital problem. The traditional approach to the general public key authentication is to depend on a public key infrastructure (PKI). In the PKI, there may be a certificate authority (CA), that is relied on via way of means of

all of the participants the usage of the PKI. The public key of the CA is accepted via way of means of all of the member nodes as an authenticated one in default. The CA signs the general public key of every member node and issues a certificate which includes the general public key and the corresponding signature to the member node. When nodes want to communicate, one in every of them sends its public key certificates to the alternative node which could confirm the authenticity of the general public key inside the certificates with the famous public key of the CA.

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. In a selective forwarding attack, the malicious/attacked nodes simply drop those messages rather than forwarding all of them.

- **Sybil attacks:** In WSNs, a node generates several false identities by inventing or stealing real node identities. Sybil attacks will target routing algorithms and topology management, reducing the efficacy of fault-tolerant systems such as 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 occur for a variety of reasons, one of which is to allow selective forwarding to draw traffic to the attack.

- **Wormhole attacks:** By tunnelling messages over a low latency connection, an attacked node closer to the base station will totally irritate the traffic. The attacker does this by convincing nodes that are farther apart (multi hop) that they are currently closer to the base station. Since the intruder on the other side of the sinkhole has a false path to the base station, a sinkhole is created.

- **Routing loops attack:** The knowledge shared between nodes is the focus of this project. When an attacker modifies and replays the routing information, fake error messages are created. Routing loops draw or repel network traffic, causing node to node latency to increase.

- **Hello flood attacks:** a message that was broadcast with a higher transmission to make it look like the HELLO message is being sent from the base station, control is being used. As soon as the nodes get the packet, they presume that the HELLO message receiving node is the nearest one and try to transmit 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 third problem is denial-of-service prevention. 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). A significant amount of research has been done to resolve the practical and theoretical issues that remain unsolved, resulting in an increase in civil and military initiatives over the last few years.In general, maximum sensor networks are designed for delay-tolerant and low-bandwidth programs.

Future WSN research could focus 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 spatial coverage assessment techniques with realistic sensor model. We agree with that inside the near future, WSN studies will place an exquisite effect on our each day lifestyles.

For example, it'll create a system for persistent observation of physiological alerts even as the patients are at their homes. It will decrease the value concerned with tracking patients and growth the efficient exploitation of physiological information and the patients can have get right of entry to the very best pleasant hospital treatment of their very 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 has a lot of potential in the future of wireless sensor networks. MAC, PHY, and NET protocol layers and knowledge aggregation methods, simulation and experimental verification of lifetime-aware routing sensing spatial coverage, and enhancement of the chosen sensing spatial are all potential fields.

# ACRONYMS

| | |
|---|---|
| **GPS** | Global Positioning System |
| **ADC** | Analog to Digital Converter |
| **QOS** | Quality Of Service |
| **TCP** | Transport Control Protocol |
| **WLANs** | Wireless Local Area Networks |
| **RF** | Radio Frequency |
| **ISM** | Industrial, Scientific, and Medical |
| **FEC** | Forward Error Correction |
| **ARQ** | Automatic Repeat reQuest |
| **MAC** | Medium Access Control |
| **SMP** | Sensor Management Protocol |
| **SQTL** | Sensor Query and Tasking Language |
| **SQDDP** | Sensor Query and Data Dissemination Protocol |
| **TDMA** | Time Division Multiple Access |
| **FDMA** | Frequency Division Multiple Access |
| **CDMA** | Code Division Multiple Access |
| **PAN** | Personal Area Network |
| **RFD** | Reduced-Function devices |
| **FDD** | Full-Function devices |
| **SFD** | Start of Frame Delimiter |
| **PSDU** | PHY Service Data Unit |
| **LQI** | Link Quality Indication |
| **CCA** | Clear Channel Assessment |
| **GTS** | Guaranteed Time Slots |
| **CSMA/CA** | Carrier Sense Multiple Access / Collision Avoidance |
| **CFP** | Contention Free Period |
| **CAP** | Contention Access Period |
| **BER** | Bit Error Rate |
| **TOA** | Time of Arrival |
| **IBC** | Identification - Based Cryptography |
| **MIC** | Message Integrity Code |
| **PKI** | Public Key Infrastructure |
| **PDU** | Protocol Data unit |
| **MDS** | Multi-Dimensional Scaling |
| **MT** | Mobile Terminal |
| **RP** | Anchor/Reference point |
| **MNL** | Multi Hop Network Localization |
| **RPE** | Recursive Position Estimation |

# APPENDIX I – REFERENCES

[1] Bharathidasan, A., Anand, V., Ponduru, S. (2001), Sensor Networks: An Overview, Department of Computer Science.

[2] S. Waharte, R. Boutaba, Y. Iraqi, and B. Ishibashi, "Routing protocols in wireless mesh networks: challenges and design considerations," Multimedia Tools Appl., vol. 29, no. 3, pp. 285–303, 2006.

[3] Charles Bell, "Beginning Sensor Networks with XBee, Raspberry Pi and Arduino."

[4] https://doi.org/10.1007/978-1-4842-5796-8_2

[5] Anna Forster, "Introduction to Wireless Sensor Networks", IEEE Press

[6] Sherine M. Abd El-kader and Basma M. Mohammad El-Basioni. Precision Farming Solution in Egypt Using theWireless Sensor Network Technology. *Egyptian Informatics Journal*, 14(3):221–233, 2013. ISSN 1110-8665.

[7] W. Hu, N. Bulusu, C.T. Chou, S. Jha, A. Taylor, and V.N. Tran. Design and Evaluation of a Hybrid Sensor Network for Cane Toad Monitoring. *ACM Transactions on Sensor Networks*, **5**(1), 2009.

[8] K.Wehrle, M G¨unes, and J. Gross, editors. *Modeling and Simulation for Network Simulation*. Springer, 2010.

[9] http://sensors-and-networks.blogspot.com/search?q=SPIN

[10] https://waset.org/publications/9345/wireless-sensor-network-characteristics-and- architectures

[11] https://www.silabs.com/documents/public/white-papers/evolution-of-wireless- sensor-networks.pdf

[12] http://sensors-and-networks.blogspot.com/search?q=SPIN