Research Report

Sensor Networks

COEN 331 – Wireless & Mobile Networks

Submitted by:

Susmith Barigidad – W1605108

Guided by:

Dr. Keyvan Moataghed

Audience

This research report gives an overview of wireless sensor networks. It is an essential guide for anyone interested in wireless communication of sensor networks. It starts by covering important concepts and protocols associated with wireless sensor networks. It includes node localization, transport protocols, network security and future trends in WSNs.

The reader of this report is expected to have a basic knowledge of wireless networks, architecture, protocols etc. This report will be helpful to students, working professionals and anyone who is interested in knowing more about Wireless Sensor Networks

Table of Contents

List of Figures

List of Tables

Chapter - 1

Motivation for Wireless Sensor

Sensors link the physical with the digital world by capturing and revealing real-world phenomena and converting these into a form that can be processed, stored, and acted upon. Coordinated into numerous devices, machines, and environments, sensors provide a tremendous societal benefit.

They can help to avoid catastrophic infrastructure failures, conserve precious natural resources, increase productivity, enhance security, and enable new applications such as context-aware systems and smart home technologies. The phenomenal advances in technologies such as very large-scale integration (VLSI), microelectromechanical systems (MEMS), and wireless communications further contribute to the widespread use of distributed sensor systems. For example, the impressive developments in semiconductor technologies continue to produce microprocessors with increasing processing capacities, while at the same time shrinking in size. The miniaturization of computing and sensing technologies enable the development of tiny, low-power, and inexpensive sensors, actuators, and controllers. Further, embedded computing systems (i.e., systems that typically interact closely with the physical world and are designed to perform only a limited number of dedicated functions) continue to find application in an increasing number of areas. While defence and aerospace systems still dominate the market, there is an increasing focus on systems to monitor and protect civil infrastructure (such as bridges and tunnels), the national power grid, and pipeline infrastructure. Networks of hundreds of sensor nodes are already being used to monitor large geographic areas for modelling and forecasting environmental pollution and flooding, collecting structural health information on bridges using vibration sensors, and controlling usage of water, fertilizers, and pesticides to improve crop health and quantity.

This research paper provides a thorough introduction to the fundamental aspects of wireless sensor networks, covering both the theoretical concepts and practical aspects of network technologies and protocols, operating systems, middleware, sensor programming and security.

1.1 Introduction to Sensor Networks

1.1.1 *Sensor Networks Definition*

Sensing is a technique used to gather information about a physical object or process including the occurrence of events. It is a group of battery-operated small devices acting as sensor nodes. These sensors collect and transfer information to a base station where the data is used and processed. The sensor network is typically used for collecting environmental conditions like sound, wind, temperature, humidity, precipitation etc

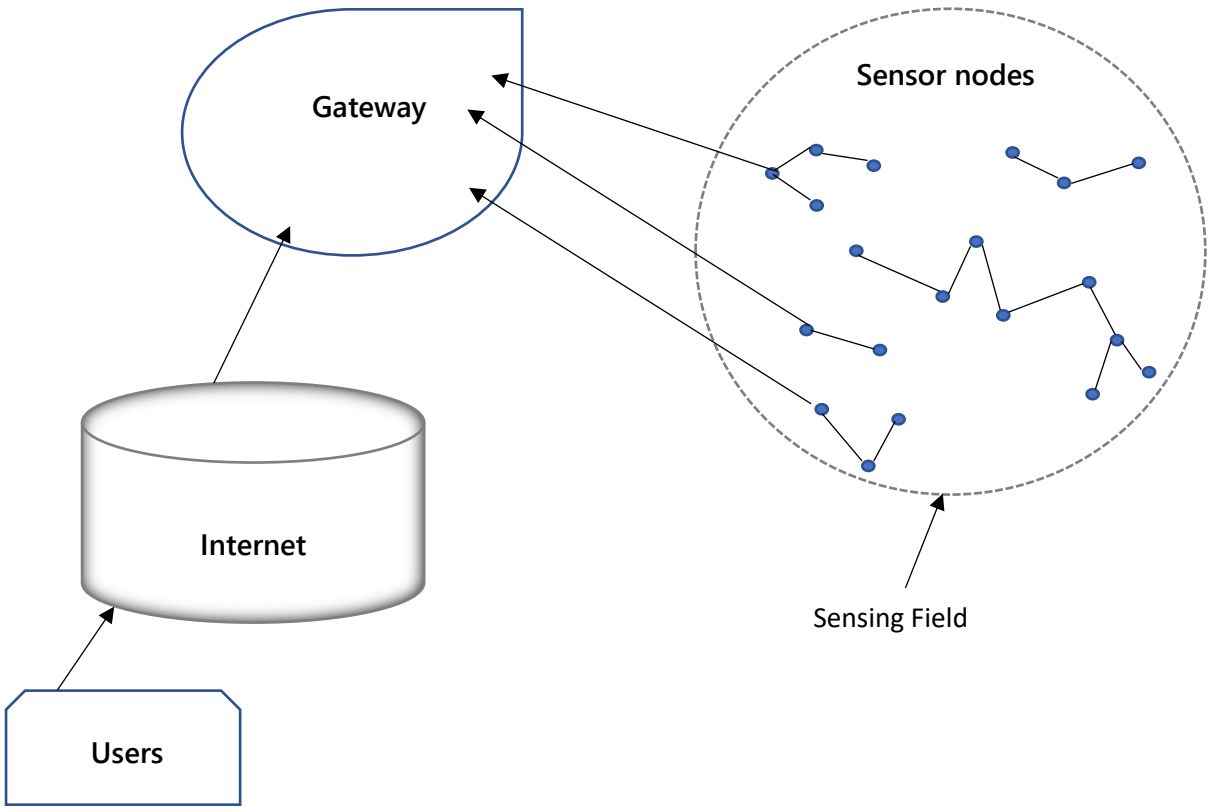

Figure 1.1 Representation of a wireless sensor network

1.2 Overview of Wireless Sensor Network

Wireless sensor networks (WSNs) allow new programs and require non-traditional paradigms for protocol layout because of numerous constraints. With the requirement for less complex equipment and low power consumption, the right stability among communication and signal/fact processing abilities should be found. A Base station or Sink behaves as a bridge among the customers and the network. Information may be retrieved from the network with the aid of using enforcing queries and gathering outcomes from the station.

The knowledge about sensor networks begins with the devices themselves, usually it is radiofrequency identification (i.e., RFID) tags and RFID reading devices (sensors). Objects are attached with an RFID tag which contains a chip which contains an ID that have an antenna. The RFID reader sends signals to the tag when the object is in the reporting area of the reader. The tag helps to discover the object. There are two types of RFID devices – The active RFID devices actually own a power source of their own and are battery or of a line powered. The passive RFID devices which are triggered by an RFID reader and there is no sort of any electricity or any source of power or any sort of battery.

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.

Sensor systems consist of:

- Sensor Nodes

  Sensor nodes are the tiny devices capable of capturing information like environmental changes and any other variables to help compute information.

A wireless sensor network contains huge amounts of sensor nodes. Communication happens via radio signals.

- **Base station**

  Acts as a gateway that transfers information between the numerous sensor nodes and end user applications.

- **Radio Nodes**

  These nodes handle the data from sensors and pass it to the WLAN access point. It consists of a memory unit, power unit, transceiver, and a microcontroller.

- **WLAN Access Points**

  It receives the data which is sent by the radio nodes wirelessly through the internet.

- **Evaluation Software**

  The data received by the WLAN Access Point is processed by a software called Evaluation Software for presenting the report to the users for further processing of the data.

1.3 Classification of Sensors

Sensor classification is all about choosing the sensor for application. Choosing a sensor largely depends on the physical property to be monitored, for example temperature, pressure, light or humidity. Studying the physical properties on these is a vital topic. Table 1.1 summarises some of the common physical properties. Besides physical properties, the classification of sensors can be based on a variety of other methods, for example, whether they require an external power supply. If the sensors require external power supply, the are said to be active sensors. Since they emit some kind of energy (light, microwave, sound) to trigger a response or to detect a change in energy transmitted signal. Passive sensors detect energy in the environment and derive their power from this energy input- for example, Infrared sensors measure infrared light radiating from the objects in the proximity.

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

Likewise with numerous different innovations, the military has been a main thrust behind the turn of events of remote sensor organizations. For instance, in 1978, the Defence Advanced Research. Activities Agency (DARPA) coordinated the Distributed Sensor Nets Workshop (DAR 1978), zeroing in on sensor network research difficulties, for example, organizing innovations, signal handling methods, and disseminated calculations. DARPA additionally worked the Distributed Sensor Networks (DSN) program in the mid-1980s, which was then trailed by the Sensor Data Technology (SensIT) program.

In a joint effort with the Rockwell Science Center, the University of California at Los Angeles proposed the idea of Wireless Integrated Network Sensors or WINS (Pottie 2001). One result of the WINS project was the Low Power Wireless Integrated Microsensor (LWIM), delivered in 1996 (Bult et al. 1996). This shrewd detecting framework depended on a CMOS chip, coordinating numerous sensors, interface circuits, computerized signal preparing circuits, remote radio, and microcontroller onto a solitary chip. The Smart Dust project (Kahn et al. 1999) at the University of California at Berkeley zeroed in on the plan of amazingly little sensor hubs called bits. The objective of this venture was to exhibit that a total sensor framework can be incorporated into minuscule gadgets, perhaps the size of a grain of sand or then again even a residue molecule. The PicoRadio project (Rabaey et al. 2000) by the Berkeley Wireless Examination Center (BWRC) centers around the advancement of low-power sensor gadgets, whose power utilization is little to the point that they can control themselves from fuel sources of the working climate, like sun based or vibrational energy. The MIT µAMPS (miniature Versatile Multidomain Power-mindful Sensors) project likewise centers around low-power equipment what's more, programming segments for sensor hubs, including the utilization of microcontrollers able

to do dynamic voltage scaling and strategies to rebuild information preparing calculations to decrease power prerequisites at the product level (Calhoun et al. 2005).

While these past endeavours are generally determined by scholarly organizations, throughout the last decade various business endeavours have likewise showed up (many dependent on a portion of the scholarly endeavours depicted above), including organizations like Crossbow (www.xbow.com), Sensoria (www.sensoria.com), Worldsens (http://worldsens.citi.insa-lyon.fr), Dust Networks (http://www.dustnetworks.com), and Ember Corporation (http://www.ember.com). These organizations give the chance to buy sensor gadgets prepared for sending in an assortment of utilization situations alongside different administration apparatuses for programming, support, and sensor information representation.

1.5 Features of WSN

WSNs primarily have sensor node which utilizes less power, applies small memory, and has minimum-enough energy intake requirement due to their tiny size.
Wireless networks can also be used for assessing extreme ecological physical conditions and can also be susceptible to enemy attacks. Even though it is set up in an ad hoc approach they are expected to be self-configured and self-restorative and expected to co-operate with continual upgrades or modifications.

- **Distributed Computing**

The algorithms utilized while collecting the data have to be monitored centrally as the processing need to be centralized as the computing is carried out on multiple nodes in the network.

- **Offers an Easily Scaled Solution**

Due to WSN being self-configured, they can be easily scaled for a larger environmental surveillance.

- **Ad hoc implementation**

Most sensor nodes are operated in areas which have no adequate infrastructure like, if it has to be installed in a forest, it would be done by discarding the sensor nodes from an airplane. Due to its characteristic of self-organizing itself, the sensor nodes are expected to establish its connectivity and distribution.

- **Unattended procedure**

The sensor nodes are expected to self-organize or self-reconfigure themselves when modifications or upgradation are required. Post which there is hardly ever any human intervention.

- **Unmetered**

The sensor nodes require very less anergy and are connected to any source of power. They only have a low source of energy, which must be optimally utilized for computing and interaction. For sensor node, the highest energy is used is when communication occurs. Thus, for efficient use of energy when the communication/interaction is very little as possible.

- **Usage of Sensors**

The sensor node should produce the maximum performance but as well as have use less amount of energy.

- **Low cost**

For surveilling an environment, thousands of sensor nodes are installed for collecting the data. This creates a very thick implying a very dense infrastructure. For the minimum cost of the entire infrastructure, the individual cost of every sensor node should be very less as possible.

- **Dynamic modifications**

Comparing to the old conventional networks where the main goal was to develop medium throughput or enhancing node development. It is very necessary for a sensor network to enhance system longevity as well as system robustness. The sensor node needs to be adapting to rapidly changing environment conditions as well as looking into connectivity requirements such as detecting failure of some nodes, replacing them and also how to add more nodes to it.

- **Heterogeneity**

The sensor nodes in the same network maybe of different types. Thus, they need to work collectively and in unison.

- **Low Bandwidth**

The communication must be very minimum for maximum energy efficiency. The exchange of the data should be efficiently transferred.

- **Large Scale Coordination**

The sensors nodes require to interact with each other to produce efficient results.

❖ **Real Time Computation**

The computation of the data collecting process should be as efficient and rapid as possible so as not to cause blockage as new data is continuously generated and the nodes have low source of energy.

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

Wireless sensor networks use radiofrequency signals to communicate back and fro amongst themselves over a medium. Thus, it can communicate very efficiently over a short range of distance as well as lower bandwidth plus dynamic modifications to the bandwidth. The medium can be either unidirectional (simplex) or bi-directional (half duplex or full duplex). WSNs need to function efficiently as there is hardly a human intervention. This makes the job a difficult one, thus the hardware parts and the software applications need to be chosen very carefully in order to enhance system longevity and system robustness.

1.6 Challenges and Constraints

While sensor networks share many similarities with other distributed systems, they are subject to a variety of unique challenges and constraints. These constraints impact the design of a WSN, leading to protocols and algorithms that differ from their counterparts in other distributed systems.

❖ **Energy**

The limitation frequently connected with sensor network configuration is that sensor hubs work with restricted energy financial plans. Commonly, they are fuelled through batteries, which must be either supplanted or re-energized (e.g., utilizing sunlight-based force) when exhausted. For certain hubs, neither one of the options is proper, that is, they will basically be disposed of once their fuel source is drained. If the battery can be re-energized essentially influences the procedure applied to energy utilization. For non-rechargeable batteries, a sensor hub ought to be capable to work until either its main goal time has passed or the battery can be supplanted. The length of the mission time relies upon the sort of use, for instance, researchers observing frigid developments may

require sensors that can work for quite a while a sensor in a front-line situation may just be required for a couple of hours or days.

As a result, the first and frequently most significant plan challenge for a WSN is energy productivity. This prerequisite penetrates each part of sensor hub and organization plan. For model, the decisions made at the actual layer of a sensor hub influence the energy utilization of the whole gadget and the plan of more significant level conventions.

- **Self-Management**

It is the nature of many sensor network applications that they must operate in remote areas and harsh environments, without infrastructure support or the possibility for maintenance and repair. Therefore, sensor nodes must be *self-managing* in that they configure themselves, operate and collaborate with other nodes, and adapt to failures, changes in the environment, and changes in the environmental stimuli without human intervention.
Many wireless sensor network applications do not require predetermined and engineered locations of individual sensor nodes. This is particularly important for networks being deployed in remote or inaccessible areas. However, the surviving nodes must autonomously perform a variety of setup and configuration steps, including the establishment of communications with neighboring sensor nodes, determining their positions, and the initiation of their sensing responsibilities.

The mode of operation of sensor nodes can differ based on such information, for example, a node's location and the number or identities of its neighbors may determine the amount and type of information it will generate and forward on behalf of other nodes.

- **Wireless Networking**

The reliance on wireless networks and communications poses several challenges to a sensor network designer. For example, *attenuation* limits the range of radio signals, that is, a radio frequency (RF) signal fades (i.e., decreases in power) while it propagates through a medium and while it passes through obstacles.
The relationship between the received power and transmitted power of an RF signal can be expressed using the *inverse-square law*:

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

which states that the received power *P* is proportional to the inverse of the square of the distance *d* from the source of the signal.
Therefore, an increasing distance between a sensor node and a base station rapidly increases the required transmission power. Therefore, it is more energy-efficient to split a large distance into several shorter distances, leading to the challenge of supporting *multi-hop* communications and routing.

❖ Decentralized Management

The large scale and the energy constraints of many wireless sensor networks make it infeasible to rely on *centralized* algorithms (e.g., executed at the base station) to implement network management solutions such as topology management or routing. Instead, sensor nodes must collaborate with their neighbors to make localized decisions, that is, without global knowledge. As a consequence, the results of these *decentralized* (or *distributed)* algorithms will not be optimal, but they may be more energy-efficient than centralized solutions.

Consider routing as an example for centralized and decentralized solutions. A base station can collect information from all sensor nodes, establish routes that are optimal (e.g., in terms of energy) and inform each node of its route. However, the overhead can be significant, particularly if the topology changes frequently. Instead, a decentralized approach allows each node to make routing decisions based on limited local information (e.g., a list of the node's neighbors, including their distances to the base station). While this decentralized approach may lead to nonoptimal routes, the management overheads can be reduced significantly.

❖ Design Constraints

Driven by the need to execute dedicated applications with little energy consumption, typical sensor nodes have the processing speeds and storage capacities of computer systems from several decades ago. The need for small form factor and low energy consumption also prohibits the integration of many desirable components, such as GPS receivers. These constraints and requirements also impact the software design at various levels, for example, operating systems must have small memory footprints and must be efficient in their resource management tasks. However, the lack of advanced hardware features (e.g., support for parallel executions) facilitates the design of small and efficient operating systems. A sensor's hardware constraints also affect the design of many protocols and algorithms executed in a WSN. For example, routing tables that contain entries for each potential destination in a network may be too large to fit into a sensor's memory.

- **Security**

Numerous remote sensor networks gather delicate data. The far off and unattended activity of sensor hubs builds their openness to malevolent interruptions and assaults. Further, remote correspondences make it simple for a foe to listen in on sensor transmissions.

For instance, quite possibly the most difficult security dangers are a refusal of-administration assault, whose objective is to upset the right activity of a sensor organization. This can be accomplished utilizing an assortment of assaults, including a sticking assault, where powerful remote signals are utilized to forestall effective sensor correspondences. The results can be serious and rely upon the kind of sensor network application. While there are various strategies and answers for appropriated frameworks that forestall assaults or contain the degree furthermore, harm of such assaults, large numbers of these cause huge computational, correspondence,

furthermore, capacity prerequisites, which regularly cannot be fulfilled by asset obliged sensor hubs. As an outcome, sensor networks require new answers for key foundation and dispersion, hub verification, and mystery.

Chapter-2

Architectures

2.1 Hardware components

2.1.1 Sensor Node Hardware Overview

When choosing the hardware components for a wireless sensor node, evidently the application's requirements play a decisive factor with regard mostly to size, costs, and energy consumption of the nodes – communication and computation facilities as such are often considered to be of acceptable quality, but the trade-offs between features and costs is crucial. In some extreme cases, an entire sensor node should be smaller than 1 cc, weigh (considerably) less than 100 g, be substantially cheaper than US$1, and dissipate less than 100 μW. In even more extreme visions, the nodes are sometimes claimed to have to be reduced to the size of grains of dust. In more realistic applications, the mere size of a node is not so important; rather, convenience, simple power supply, and cost are more important.

These diversities notwithstanding, a certain common trend is observable in the literature when looking at typical hardware platforms for wireless sensor nodes. While there is certainly not a single standard available, nor would such a standard necessarily be able to support all application types, this section will survey these typical sensor node architectures. In addition, there are a number of research projects that focus on shrinking any of the components in size, energy consumption, or costs, based on the fact that custom off-the-shelf components do currently not live up to some of the more stringent application requirements. But as this book focuses on the networking aspects of WSNs, these efforts are not discussed here.

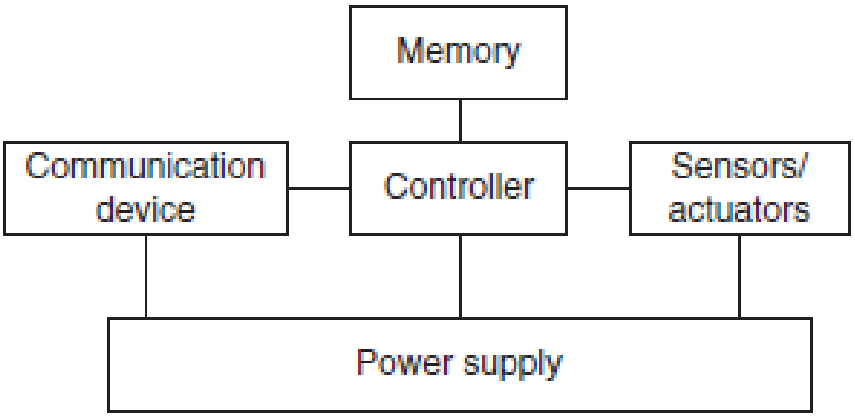

Figure 2.1 Overview of main sensor node hardware components

A basic sensor node comprises five main components (Figure 2.1):

- **Controller** A controller to process all the relevant data, capable of executing arbitrary code.
- **Memory** Some memory to store programs and intermediate data; usually, different types of memory are used for programs and data.
- **Sensors and actuators** The actual interface to the physical world: devices that can observe or control physical parameters of the environment.
- **Communication** Turning nodes into a network requires a device for sending and receiving information over a wireless channel.

2.2 WSN Structures

2.2.1 Star Topology

A star network is a topology in which the base station is at center and transfers data to and from the sensor nodes. It additionally lets in low latency communications among the faraway node and sink station.

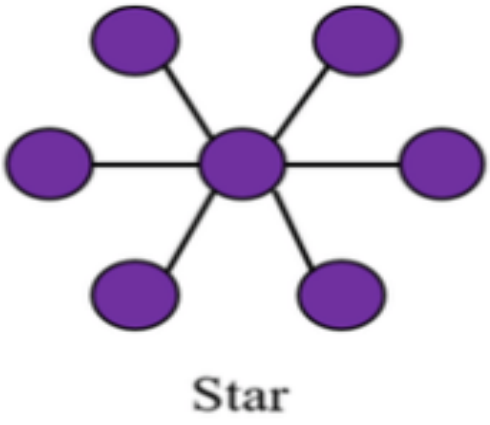

Figure 2.2 Star Topology

2.2.2 Partial Mesh Topology

Unlike full mesh, in a partial mesh, not all nodes are connected to each other. One node is connected to two or more nodes and so. This helps in keeping the complexity and expenses low but functioning high.

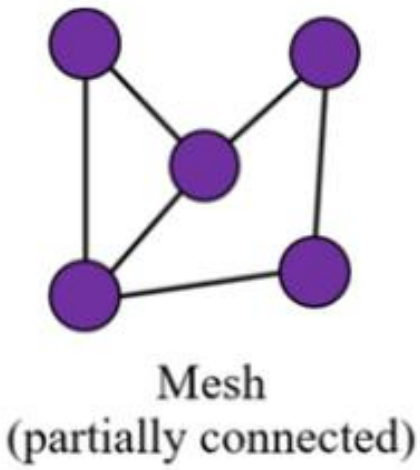

Figure 2.3 Mesh (partially connected) Topology

2.2.3 Mesh Topology

A network in which every node is connected to every other node is a full mesh network. This is a point-to point direct connection among all nodes. All the nodes in the mesh are equally important and take equal responsibility for full data transmission. This can cause the network to be expensive.

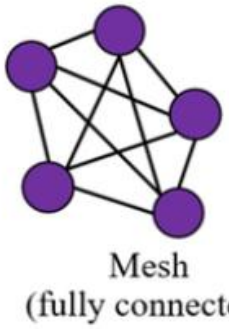

Figure 2.4 Mesh (fully connected) Topology

2.2.4 Ring Topology

Ring topology means every node is connected to one other node. Data transmission takes place from one node and travels to another node in a ring. A failure in node breaks the loop and can shut down the entire network but congestion of traffic and double path communication.

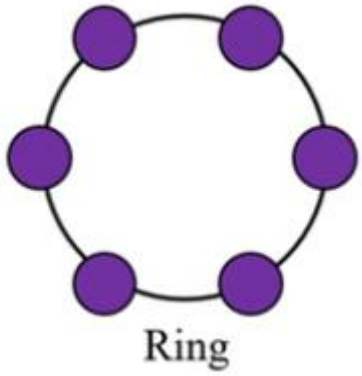

Figure 2.5 Ring Topology

2.2.5 Circular Topology

In this topology, there is a circular sensing area and that the sensing area has a sink/gateway (at center). The sensor nodes sense the event of interest and send these data to the sink. The nodes are randomly installed with uniform concentration all around the sink as shown in Figure 3.4.6. Depending on the distance/length of a node from the sink and the communication range of the nodes, data must traverse single or multiple hops before being received by the sink. The circular web topology is easy to establish and install, easy to maintain, and more efficient.

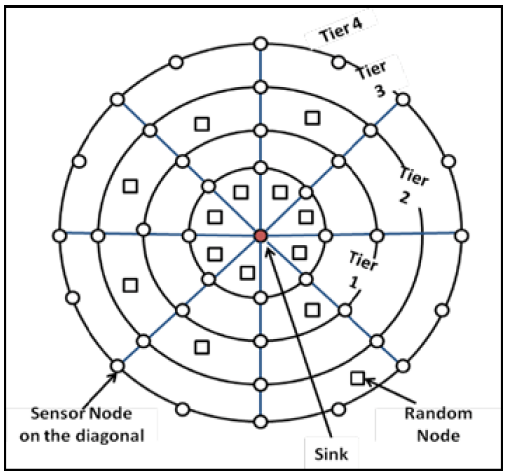

Figure 2.6 Circular Topology

2.2.6 Hybrid Topology

When one or more technologies are combined to design a network it is a hybrid network. The hybrid topology can be very useful for certain specific purpose to be implemented in a network. The different types of hybrid networks are: Star-bus network, Hierarchical star network, star-ring network, Hybrid mesh network.

Some of the advantages of this topology are its easy to repair and has less maintenance cost. The design of the system can easily be modified.

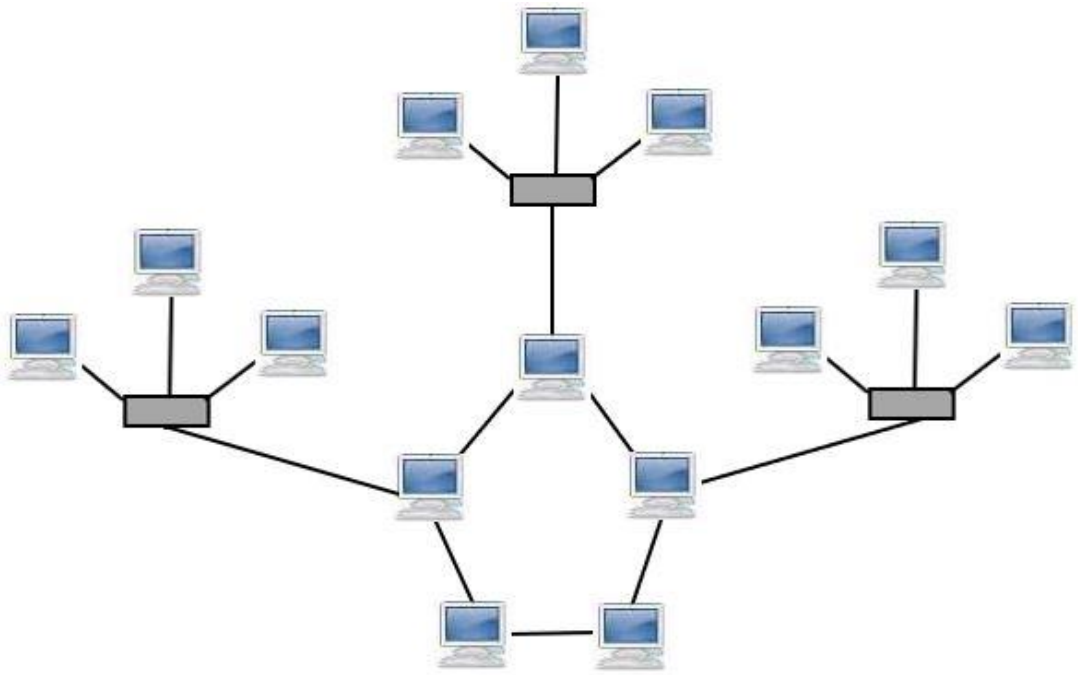

Figure 2.7 Hybrid Topology

2.3 Types of WSN

- Cyber-physical system (CPS) is a newer term for a wireless sensor network. It attempts to better describe what you can do with these networks and their main properties when being integrated into a physical environment. Different from other computers and devices, which are environment agnostic, cyber-physical systems are part of the environment and application restricted. Another important property is the fact that they also can affect the environment via so-

called actuators such actuators as in automatic irrigation pumps, light switches, alarms, and humidity or temperature regulators.

- Body sensor networks refer to a specific type of network, designed to be carried on the body (mostly human). Applications include health monitoring, weight management, sports logging, and many others. There are some peculiar examples, such as smart shoes or smart T-shirts, which can sense your activity or heart rate. Most of the sensor nodes are tiny, sometimes even implantable. The current trend is clearly moving towards one integrated device that can sense all functions, instead of several different sensors on various parts of the body.

- Crowdsourcing alludes to another and quick creating kind of detecting in which sensors are basically people with their cell phones. For instance, individuals can follow their trekking ways and afterward assess them regarding security, commotion, or street quality. This information is accumulated on an essential issue and handled into a solitary trekking quality guide of a city, which can be appropriated to any intrigued client. The genuine force of these applications is that no extra equipment is required, just a somewhat straightforward client arranged application for brilliant telephones.

- The Internet of Things (IoT) is often mistaken to be a sensor network. However, IoT's main concept is that all things, such as a washing machine or radio, are connected to the Internet. The Internet connection has significant advantages when implementing sensor networks and can thus be seen as an enabling technology. However, the target can also be very different, e.g., when you can read your emails from the microwave or from your car. The term Internet is also a hint that usually these networks are IP enabled and thus use a well-defined communication stack. This can be seen as an advantage (no need to reimplement) or as a disadvantage (high energy use, little flexibility).

2.4 Power Consumption

One of the most important properties to understand about sensor node hardware is its power consumption. Each of the components of a sensor node requires energy to operate. This energy is highly restricted and needs to be provided by on-board batteries. Thus, it is crucial to understand which components are most energy hungry and to use them only when absolutely needed.

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

The above table could be read as, all the power consumption is given in Ampere (A). For example, when radio is sleeping and off, it still consumes 0.01 mA. The batteries attached to sensor node to the sensor node are expected to provide a constant voltage of 3 V.

These preceding calculations are strictly theoretical and real batteries or hardware may behave differently/ However; this also illustrates how important it is to minimize the usage of individual components. Even if batteries do not behave like perfect containers of energy.

When introducing sleeping times for the radio (the so-called duty cycle), the picture changes dramatically. In this scenario, the radio is switched on and off periodically to enable power saving.

2.5 Usage of Simulators

It is always better to use a simulator instead of real nodes. A simulator is a software system, running on a normal computer which mimics the behaviour of some other system and its interactions. For example, a sensor network simulator mimics the behaviour of sensor nodes and their communication with each other.

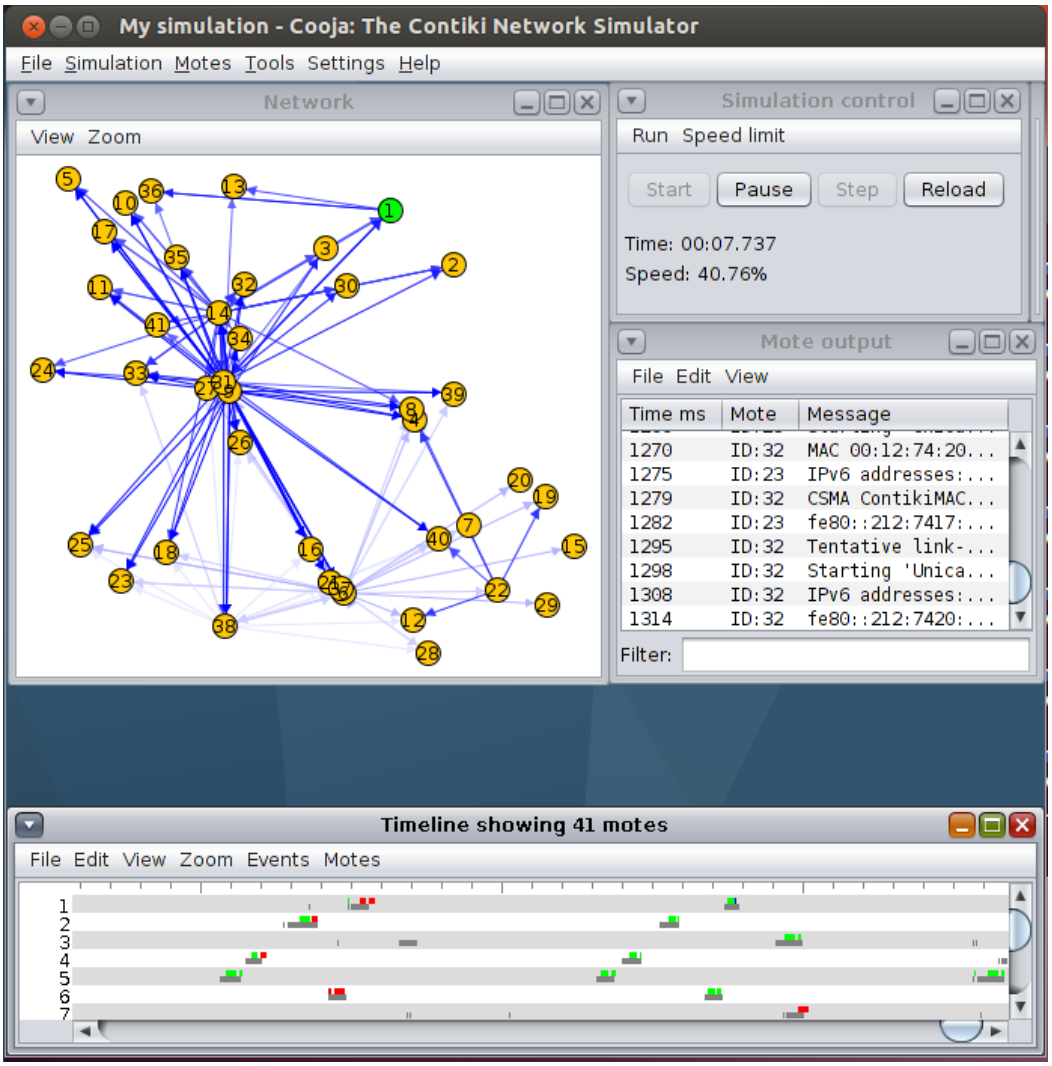

Figure 2.8 Screenshot of Cooja simulator

Wireless propagation model is demonstrating how bundles are moved through the remote correspondence medium. It is particularly critical to get a handle on the mistakes of the remote medium, like bundle misfortune and parcel defilement. The least complex model is the supposed unit plate diagram model. It says that every sensor hub can send a parcel to unit plate chart model another sensor hub if the collector is inside a specific circular region around the sender. The gathering is consistently errorless. This model is normally excessively basic, and re-enactment runs with this model lead to the feeling that everything is functioning admirably, and no bundle debasements happen or that between two hubs with a consistent distance the sending of parcels consistently work.

Mobility model is needed to define how sensor nodes are moving around the environment.

This model is very useful when also your normal sensor nodes are moving, for example when they are attached to bikes or buses. There are some very simple models, such as the random waypoint. It always selects a new random point some- random waypoint where in the virtual

environment and lets the sensor "drive" there with some constant predefined speed, then selects a new one, etc.

The traffic model dictates how many events have occurred in the environment. Sensor networks are typically sensing something, e.g., temperature, rain volume, etc. It is important to understand when events worth sending are generated in a real environment and to also use similar values for simulation. For example, if the application is trimmed to report only temperature data below 15 and over 25 degree Celsius, the traffic model needs to realistically mimic how often and in which sequence such events realistically occur.

Chapter-3

Radio Communications

3.1 Radio Communication

We all know that heart of WSN networks is their ability to communicate wirelessly with each other. The most broadly used interface is the radio transceiver operating in one of the free bandwidths, which are reserved worldwide for research and medical applications.

Radio waves are normal electromagnetic waves. Their name refers to their frequency range in the electromagnetic spectrum. Electromagnetic wave follows the equation:

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

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.

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

_ **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 frequency of the signal can be changed to indicate different codes.

_ **Displacement or phase** ϕ(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.

A modulation code, or key, is the symbol that you are encoding onto the modulation code wave. For example, if you decide to use a very high amplitude to encode a 1 and a very low amplitude to encode a 0, you have two codes or keys. 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. Combinations of different modulation codes also lead to many additional modulation codes. The process of modulation and demodulation is rather simple to understand and use. In fact, wave modulation is used for all wireless communications.

But knowing from everyday life the problems connected to wireless transmissions, why do they sometimes not work as expected? Problems arise from the wave propagation properties through your environment, or in other words, what remains from the wave after it travels some distance through the environment (air, water, free space, etc.).

3.2 Properties of Wireless Communication

The electro propagation wave encounters many distortions as it travels through the atmosphere (we call this wave propagation). These are primarily attributable to the processes mentioned below:

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

- Reflection/Refraction: When a wave hits a surface, this mechanism causes it to change direction. A portion of the wave is mirrored and follows a new path, while another portion is refracted into the material, changing its properties.
  Both processes generate new secondary waves, which arrive at the receiver slightly later than the primary wave. This is both a blessing and a curse—very weak signals could be detected better when primary and secondary signals overlap.

- Diffraction/Scattering: Sharp edges and uneven surfaces in the atmosphere will split the wave into many secondary waves, all of which have the same effects as shown below in the Figure 3.1.

- 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 effect on police sirens, which sound different depending on whether the police car is approaching or moving away from the observer. The same thing happens with radio waves when their frequencies are moved in one direction or the other, resulting in a loss of centre.

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.*

Path loss is important in wireless communications because it helps you to predict transmission quality and/or design wireless links. The rest of this section will look at how path loss works in practice and how it affects wireless communications.

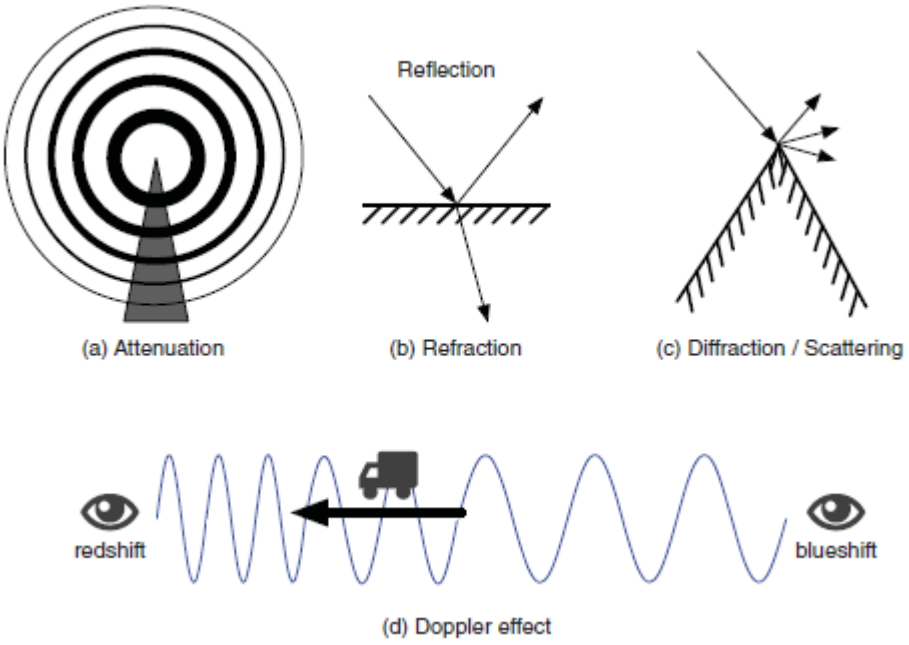

Figure 3.1 Physical Processes that lead to path loss in signal propagation

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.

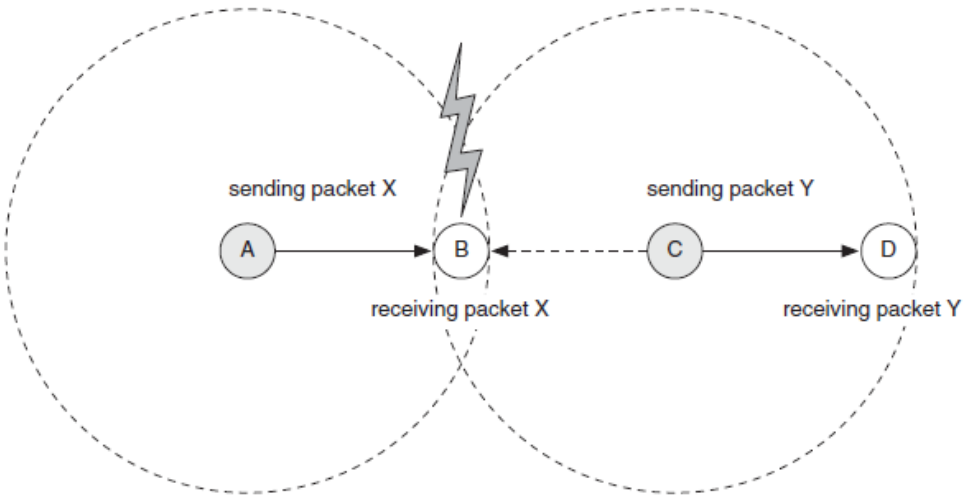

Figure 3.2 Hidden Terminal Problem in Wireless Communications

The Hidden terminal problem is a major challenge to overcome in wireless communications. Let us see how to resolve the problem.

3.3 Medium Access Protocols

Medium Access Protocols are responsible for regulating sensor node access to the shared wireless medium, also known as "air." However, we will start by defining some key metrics that will assist you in determining how well a medium access protocol (MAC protocol) is performing.

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.*

A MAC protocol is designed to optimize throughput at both individual nodes and the wireless medium. It also seeks to maintain a semblance of justice. This means that each node should have an equal opportunity to send packets out.

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 straightforward but effective protocol that operates on the principle of "listen before chat." This means that the sender first listens to the shared channel and then attempts to send if it is available. CSMA has two primary variants: CSMA with collision detection (CSMA-CD) and CSMA with collision avoidance (CSMA-CA) (CSMA-CA). CSMA-CD attempts to detect a collision and, if a CSMA-CA error occurs, resend the packet. The second attempts to prevent the accident from happening in the first place. Since it is more commonly used and works better, this discussion focuses on CSMA-CA.

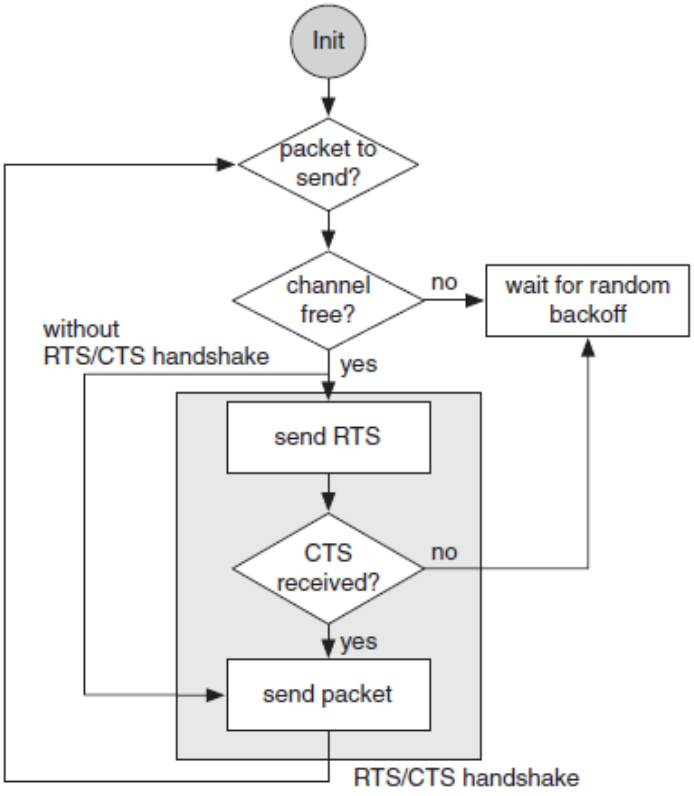

Figure 3.3 Flow diagram of general CSMA with collision avoidance

Overall, CSMA is a very straightforward and easy-to-understand protocol that performs admirably in most cases. However, in the sense of sensor networks, its key drawback is its high energy consumption. It never puts the nodes to sleep, and it easily depletes the energy on a sensor node (typically a couple of hours).

3.3.2 Sensor MAC

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

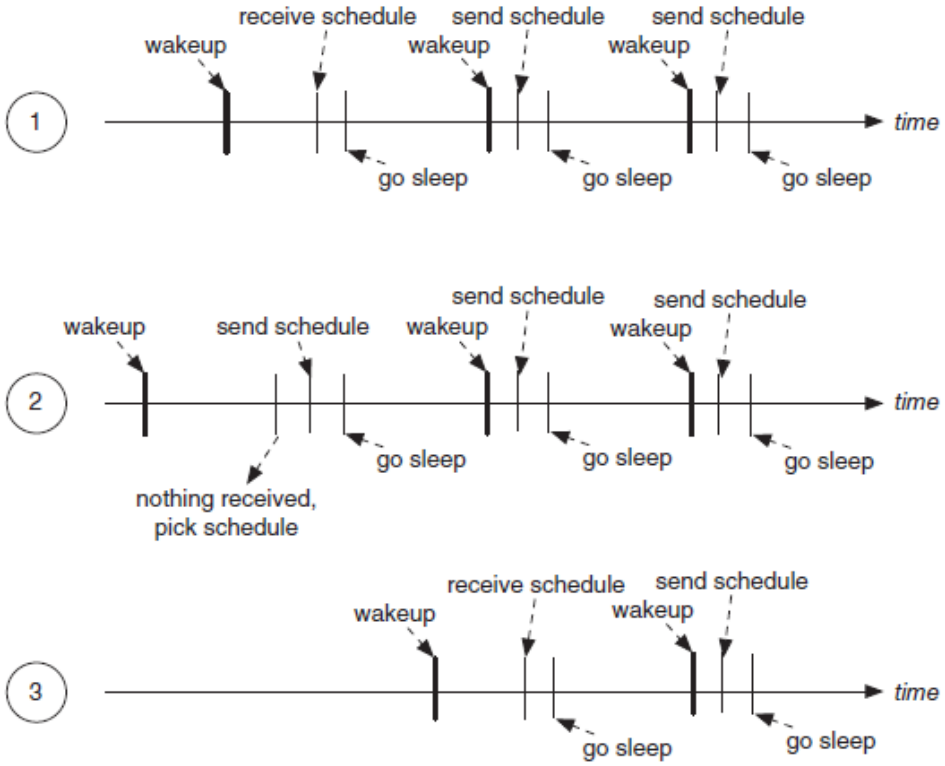

Figure 3.4 Sensor MAC general scenario

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):** is a communication protocol in which each node has complete control for a set period (a slot). This is collision-free, but there are significant delays.

⇒ ***Carrier Sense Multiple Access*** **(CSMA):** "First listen, then talk," as Carrier Sense Multiple Access (CSMA) puts it. Although the delay is short, it requires a lot of energy (the nodes never sleep) and is not collision-free.

⇒ ***Duty cycling:*** The recommended method of organizing sensor node sleep and awake cycles is duty cycling. Duty cycling is used by Sensor MAC, Berkeley MAC, and Box MAC, all of which can save a lot of energy.

⇒ ***BoX*** *MAC is based on B-MAC, but it provides streamlined communications for both unicast and broadcast transmissions, making it the preferred MAC protocol for sensor nodes now. It does not require synchronization, has a short delay, and uses little energy.*

Chapter-4

Routing Protocols Used in WSN

4.1 Traditional Techniques

4.1.1 Flooding Technique

Flooding occurs when a sensor node sends a transmitted message to all other nodes, meaning that a packet is received by all its neighbours except the node from which it was received, if the packet is not destined for itself or the maximum number of hops a packet can pass is not exceeded. Flooding is an easy protocol to set up, and it is a reactive protocol, so it does not require any maintenance. However, this requirement requires large amount of bandwidth and wastes lot of energy.

4.1.2 Gossiping Technique

A slightly improved version of flooding in which the receiving node transfers the packet to a randomly chosen neighbour, who then advances the packet to another neighbour, and so on. It has the benefit of preventing the implosion, but it also has the downside of transmission delay.

4.2 Current Techniques

Flat-based routing, hierarchical-based routing, adaptive-based routing, multi-path routing, query-based routing, and negotiation-based routing are the different types of routing in WSNs.

4.2.1 Flat routing

Sequential Assignment Routing (SAR) - The sequential assignment routing (SAR) algorithm works by creating multiple trees, where the root of each tree is a one-hop neighbor of the sink/gateway. It is used to prevent nodes with low throughput or higher delay. Each sensor node records two parameters about each route that it takes: all available energy resources on the route and delay in time units. Higher priority packets take lower delay routes, and lower priority packets must use the routes of higher delay.

Directed Diffusion - When sensor nodes produce requests/queries for information sensed by other nodes, the directed diffusion protocol is useful. Each sensor node connects to data that includes 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.

Low Energy Adaptive Clustering Hierarchy (LEACH) is an acronym for Low Energy Adaptive Clustering Hierarchy. For WSNs with the same type of nodes, TDMA is used. LEACH is an adaptive clustering protocol that self-organizes. Its aim is to evenly spread energy consumption across the sensor network's nodes, to accumulate data, to support data fusion and localized collaboration, and to shape and operate clusters.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS) – This is an improvement over the previous LEACH protocol. Collaborative approaches are used to extend the existence of the nodes. It only allows for local coordination between nodes, reducing the amount of bandwidth used in interaction. It can, however, result in a bottleneck and a delay.

4.2.3 Multipath Routing

If the main/primary path fails, this is used to find alternative routes. Even if the energy consumption rises, this can be increased by maintaining several pathways between the source sensor node and the sink/gateway and keeping these alternate routes active by sending out periodic messages.

4.2.4 Adaptive Routing

Specific device parameters are modified in this process, meaning that they are tailored to fit the network's current circumstances and available energy sources.

4.2.5 Query-based Routing

The destination nodes promote a demand for information (sensing task) from a node across the network, and a node receiving the appropriate data sends data that matches the query back to the query's initiator, the destination node. It is possible to use natural language or high-level languages.

4.2.6 Negotiation-based Routing

Negotiation-based routing in WSNs is designed to reduce redundant data and avoid duplication. For the case of routing between two neighboring ISPs, we investigate negotiation as a framework for cooperation between conflicting entities. Interdomain routing is often motivated by self-interest and focused on a skewed view of the internetwork, compromising routing's reliability and performance. We present a mechanism for sharing information between adjacent ISPs based on coarse preferences.

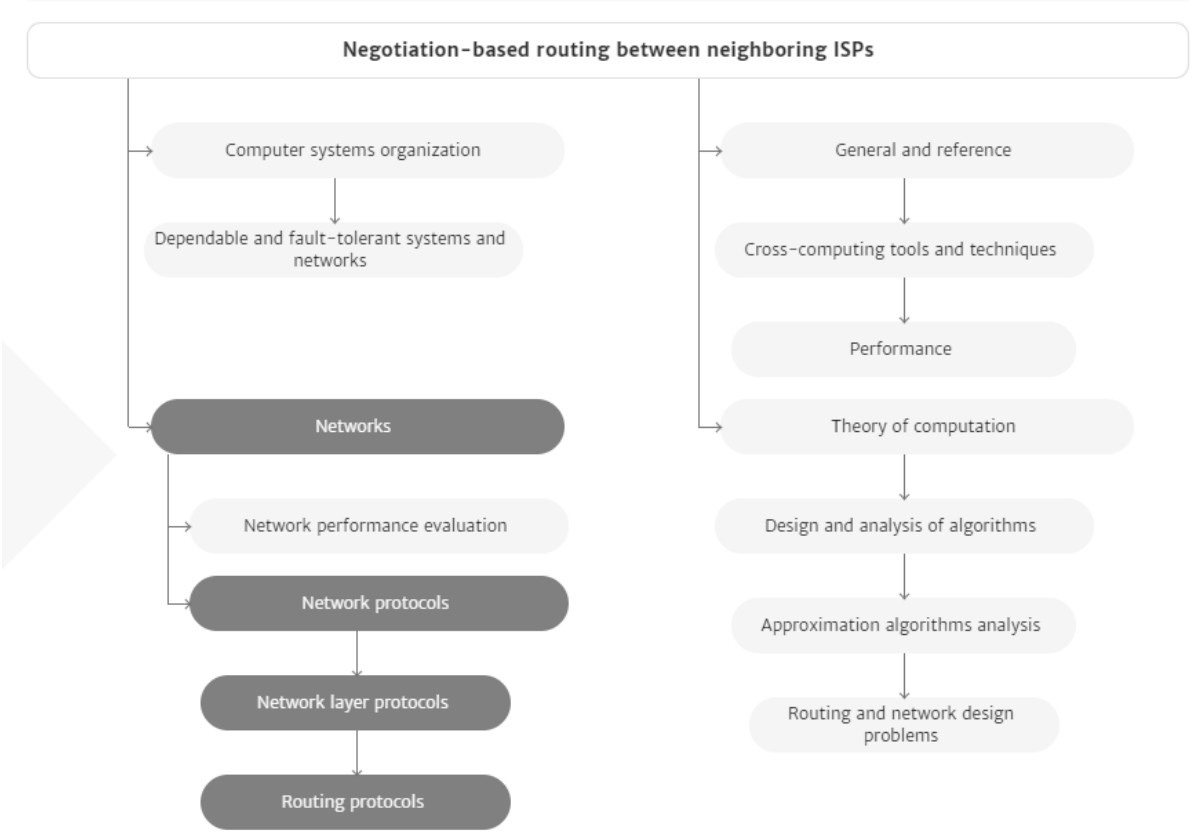

Figure 4.1 Negotiation-based routing

Chapter-5

WSN Security Issues

Sensor networks have four security goals: confidentiality, integrity, authentication, availability, and freshness. Freshness is a new security target in WSN, implying that the receiver receives the most recent and fresh data, preventing an attacker from replaying the old data. When the WSN nodes use shared keys for message communication, this requirement is particularly important since a potential attacker can initiate a replay attack using the old key before the new key is refreshed and has reached all the WSN nodes. To keep contact new, a mechanism like a nonce or a time stamp should be included in each data packet.

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 a hot topic right now. There are three problems that must be addressed for WSNs to be secure: I Key management: To use cryptography, all parties must have the same cryptographic keys. Per mechanism requires key management systems to ensure secrecy, honesty, authentication, and other security objectives. It is a method for establishing and maintaining keys between valid nodes that also allows for key updating, revocation, and destruction. Providing effective key control in WSNs is difficult due to resource constraints. (ii) The next problem to fix is routing protection. 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

The group has been paying growing attention to the research and deployment of wireless sensor networks. Sensor network-based technologies are being used in an increasing number of civil and military programs. Sensor networks that are highly efficient in terms of energy consumption and correctness have been around for a long time. As a result, the construction of such networks, as we see it, is more difficult.

WSNs are vulnerable to a variety of security risks that may jeopardize application performance. Due to the restricted energy, connectivity space, and computing ability of WSNs, security assistance is difficult. Furthermore, sensors are often used in an open environment with little physical protection. Given the variety of WSN applications and the possibility of varying security conditions.

If wireless sensor networks (WSNs) become more popular, we expect higher security standards to be imposed on WSN applications. We are hoping for the best. Good security will more likely become a more practical standard in the future because of our studies and commitments. We also hope that current and future work in the areas of privacy and trust will make WSNs a more appealing choice in several new areas.

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.

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