

WIRELESS SENSOR NETWORKING

A THESIS SUBMITTED TO
THE FACULTY OF ARCHITECTURE AND ENGINEERING
OF
EPOKA UNIVERSITY

BY

STEFANOS PASHA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
COMPUTER ENGINEERING

JUNE, 2022

Approval sheet of the Thesis

This is to certify that we have read this thesis entitled “WIRELESS SENSOR NETWORKING” and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Dr. Arban Uka
Head of Department
Date: June, 30, 2022

Examining Committee Members:

Assoc. Prof. Dr. Carlo Ciulla (Computer Engineering) _____

Dr. Shkelqim Hajrulla (Computer Engineering) _____

Dr. M. Maaruf Ali (Computer Engineering) _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name Surname: Stefanos Pasha

Signature: _____

ABSTRACT

WIRELESS SENSOR NETWORKING

Pasha, Stefanos

M.Sc., Department of Computer Engineering

Supervisor: Dr. M. Maaruf Ali

Since the beginning of time we have seen the first examples of wireless sensors. These wireless sensors have been our brain. Receiving and giving information through our ears, eyes, mouth, nose and even our skin. Nowadays the technology lets us use wireless communication to make our daily life easier. In this paper I talk about WSN architecture and sensor nodes which are easily distributed in case of disruption. I have used cnMaestro, a software platform which provides us secure end-to-end network control. There I have explained how does a tower(node) connects and communicates with the access points wirelessly and the configurations needed to remote control and configure any of these slaves (access points) through the software receiving any data and host they get.

Keywords: *wireless sensors, WSN architecture, nodes, wireless communication, end-to-end network control, access points.*

ABSTRAKT

RRJETAT ME SENSORË PA TELA

Pasha, Stefanos

Master Shkencor, Departamenti i Inxhinierisë Kompjuterike

Udhëheqësi: Dr. M. Maaruf Ali

Që nga fillimi i kohës ne kemi parë shembujt e parë të sensorëve me valë. Këta sensorë me valë kanë qenë truri ynë. Marrja dhe dhënia e informacionit përmes veshëve, syve, gojës, hundës dhe madje edhe lëkurës sonë. Në ditët e sotme teknologjia na lejon të përdorim komunikimin me valë për të bërë më të lehtë jetën tonë të përditshme. Në këtë punim flas për arkitekturën WSN dhe nyjet sensore të cilat shpërndahen lehtësisht në rast të ndërprerjes. Unë kam përdorur cnMaestro, një platformë softuerike e cila na ofron kontroll të sigurt të rrjetit nga fundi në fund. Aty kam shpjeguar se si një kullë (nyje) lidhet dhe komunikon me pikat e hyrjes me valë dhe konfigurimet e nevojshme për të kontrolluar nga larg dhe për të konfiguruar ndonjë prej këtyre skllëvërve (pikat e hyrjes) përmes softuerit duke marrë çdo të dhënë dhe host që ata marrin.

Fjalët kyçe: sensorëve me valë, arkitekturën WSN, nyjet sensore, komunikimin me valë, kontroll të rrjetit nga fundi në fund, pikat e hyrjes.

TABLE OF CONTENTS

ABSTRACT	iii
ABSTRAKT	iv
LIST OF FIGURES	vi
CHAPTER 1	vi
INTRODUCTION	1
1.1 Problem Statement	1
1.2 Thesis Objective	2
1.3 Scope of works	3
1.4 Organization of the thesis	3
CHAPTER 2	3
LITERATURE REVIEW	3
2.1 Sensor nodes	3
2.2 A brief description of the architecture	5
2.3 Evaluation metrics for a WSN	8
<u>2.3.1 System evaluation metrics</u>	<u>8</u>
2.3.2 Individual node evaluation metrics	11
2.4 Wireless sensor network applications	14
2.5 Classification	17
<u>2.5.1 Classification based on mode of operation</u>	<u>17</u>
2.5.2 Classification according to the way the node communicates with BS.....	18
2.5.3 Classification according to network structure	18
2.6 Existing protocols	19

2.7 Hierarchical routing protocols.....	22
2.8 Location-based routing protocols.....	24
2.9 Addressing the data management problem	26
2.10 Data transmission	28
2.11 Treat WSN as distributed databases.....	30
2.12 Naming and indexing of data	31
2.13 Data storage.....	32
2.14 Data processing	35
CHAPTER 3	38
METHODOLOGY.....	38
CHAPTER 4	45
RESULTS AND DISCUSSIONS	45
Results.....	48
Troubleshooting Tools	49
CHAPTER 5	53
CONCLUSIONS.....	53
5.1 Conclusions.....	53

LIST OF FIGURES

Figure 1. Shows the components of the sensor node.	5
Figure 2. Shows the layers of the WSN architecture.	8
Figure 3. Reflects a concise overview of all WSN uses.	17
Figure 4. Node communication between each other.	20
Figure 5. Shows the data processing in WSN.	27
Figure 6. Shows the distribution of data in the WSN.	31

Figure 7. Shows data processing model.	37
Figure 8. Sign in page.	38
Figure 9. cnMaestro main page.	39
Figure 10. access point menu.	40
Figure 11. Enabling remote management	40
Figure 12. Approval of new device.	40
Figure 13. Monitor and manager.	41
Figure 14. Device Configuration menu.	42
Figure 15. Dashboard of the device	43
Figure 16. Performance graphs of Access point.	43
Figure 17. Ping test to another access point.	44
Figure 18. Dashboard of tower.	45
Figure 19. Menu of configuration and location.	47
Figure 20. Alarms.	48
Figure 21. Software Upgrade menu.	49
Figure 22. status of the device.	50
Figure 23. logs checker.	50
Figure 24. Link test tool.	50
Figure 25. Node statistics.	51
Figure 26. Performance Graphs	52

CHAPTER 1

INTRODUCTION

1.1 Problem Statement

Since then, further progress has been made and new technologies have been developed. The main function of these new techniques is to rely on the concept of distributed indexes. One of the main ideas was to use a distributed hash table (DHT) that associates nodes with data. Therefore, finding a node with specific data is an easy task. Due to the specific characteristics of WSNs, resources related to battery life, computing power, and communication capabilities are very limited, requiring a highly efficient and scalable data management and routing scheme. There are some similarities between WSNs and typical P2P schemes, and our work motivates the use of peer-to-peer techniques for efficient data management in WSNs. Nodes refer to peers in P2P systems and sensor nodes in sensor networks, so these often look like this [18]:

1. Resource sharing. Within a group of nodes, each node can use the resources of other nodes in addition to its own resources, especially for storage and computing functions.
2. Distributed architecture. In such an architecture, the system is unaware of the concept of global coordination. That is, the nodes work together locally.
3. Temporary connection. Nodes in P2P systems are often disconnected due to poor connectivity or the user leaving the system. WSN causes nodes to fail for a variety of reasons, including:
 - B. Physical destruction of the node, power failure, or communication link failure.
4. Equal rights and functions. Nodes are equivalent partners with symmetrical features. Each node is completely autonomous with respect to its own resources.

5. ID management. Normally, the node ID changes, so it is not always possible for a node to reach the same address. Because the connection is temporary, the node is dynamically assigned a new ID each time it connects to the network.

6. Message routing and forwarding. Communication is completely controlled by the nodes operating locally. Network communication usually involves the presence of a tracking mechanism. For example, a node sends a message on behalf of another node [19].

1.2 Thesis Objective

Sensor nodes can not only measure physical phenomena, but also process, store, and distribute these measurements. The community of sensor nodes that work together to build ad hoc networks using wireless communication is called a wireless sensor network (WSN) [18]. Sensor nodes are usually randomly placed in or near the survey area. These sensor nodes process important parts of signal processing, data processing, and self-configuration to build a high-performance, scalable, and durable network. Therefore, WSNs are cheap and practical and offer the opportunity to support many real-world applications [3].

The main purpose of various environmental monitoring applications is to collect as much data as possible that characterizes the environment under investigation. Therefore, managing this data remains an important task for these monitoring systems, especially as the network size continues to grow. WSNs are very often used in such applications because they meet the following requirements: Low cost, simple infrastructure, scalability, and efficient use of routing techniques. WSN data acquisition and sensor node power limits distinguish sensor data management from management of other communication networks [4].

Sensor nodes are typically very limited in computational, storage, and power resources. In contrast, peers in P2P systems are computers with processing power, ample storage resources, and uninterruptible power supplies. Another important difference is the separation of physical and logical networks. This complicates the use of P2P concepts in WSNs. In the world of search, clustering of nodes in a cluster is

gaining momentum as networks grow larger and scalability needs to be significantly improved these days. Therefore, our goal was to use peer-to-peer technology in a clustered WSN network [5].

1.3 Scope of works

- I. What are sensor nodes?
- II. What is the WSN architecture?
- III. How are sensor nodes classified and where are they used?
- IV. How are they classified and which protocols apply to WSN?
- V. How is WSN data managed?
- VI. What are the steps in the WSN data management process?

1.4 Organization of the thesis

This thesis is divided into 5 chapters. The organization is done as follows:

In Chapter 1, the problem statement, thesis objective and scope of works is presented. Chapter 2, includes the literature review about sensor nodes, WSN and WSN architecture, protocols, data management and WSN database. Chapter 3, consists of the methodology followed in this study. In Chapter 4, the experimental results. In Chapter 5, conclusions.

CHAPTER 2

LITERATURE REVIEW

2.1 Sensor nodes

Technological development has made it technically easy and very economical to manufacture very small and inexpensive sensors. Sensor technology has made great

strides and more development is underway. A sensor is a device that converts a physical phenomenon into an electrical signal. The type of phenomenon you are monitoring also determines the type of sensor you need. The type of sensor, on the other hand, determines the type of data that is collected or measured. In addition, for the same phenomenon, changing the required accuracy can affect the size of the generated data [18]. Sensors therefore represent part of the interface between the physical world and the world of electrical equipment such as computers. The rest of this interface is presented by performers who transform electrical signals into physical phenomena. Sensor nodes usually consist of multiple sensor types for sampling physical phenomena. These nodes have communication and sensor capabilities in addition to traditional computing capabilities, which are superior to traditional sensors. Sensor nodes can not only measure physical phenomena, but also process, store, and distribute measurement information. Models for these devices include real-time tracking, environmental condition monitoring, comprehensive environmental computing, and local health monitoring [6].

Unlike traditional wireless devices, wireless sensor nodes do not need to communicate directly with the nearest base station, they only communicate with the local node. Instead of relying on a predefined infrastructure, each sensor independently participates in infrastructure-wide decisions. Again, sensor nodes have attractive features such as price and compactness, but their capabilities are very limited. In some cases, the sensor node does not even have a unique identifier. However, to truly benefit from these node networks, these nodes must operate in a collaborative, decentralized, self-organized way. The following is an overview of the sensor node properties. Computing WSN nodes typically use small, low power, slow microcontrollers that can provide basic computing operations. Memory normally, microcontrollers operate with less kilobytes of RAM. Programs are stored in hundreds of kilobytes or megabytes of flash memory instead of the hard drives used by regular computers. A small K-byte EEPROM used for configuration may be used [7].

Communication functionality is limited for short distances and weak connections. Low power radios are typically used (for example, the CC1000 chip operating in the ISM-433915 MHz band). Nodes may only provide broadcasts as a communication model. The power sensor node has a battery as the only power source. This is a data routing issue within the network, as energy is primarily used for

communication between nodes. Interfaces Sensor nodes typically contain various interfaces for connecting sensors to them. The interface can be serial (UART, I2C) or parallel (GPIO). Most microcontrollers used in sensor nodes also include an analog input connected to an internal ADC. Analog sensors can be connected through these interfaces. Sensors Various low power sensors are placed on the sensor node or connected through an interface. Various types of sensors can be sensitive to temperature, light, humidity, and pressure [8].

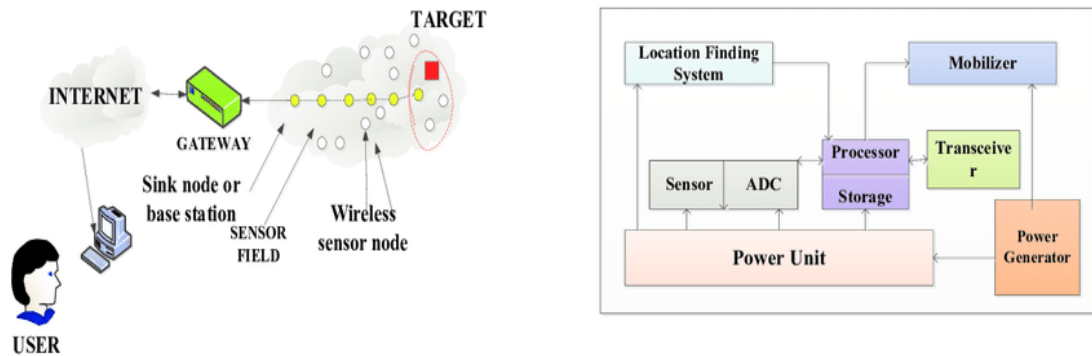


Figure 1. Shows the components of the sensor node.

2.2 A brief description of the architecture

In a typical WSN architecture, the sensor nodes are tightly distributed and when useful information is displayed, the data is sent to the central station. Hundreds of nodes grouped across the field form a network and send data to the collection point. Sensors record temperature, light conditions, and soil moisture at hundreds of points in the field and send the data to the base station over a multi-hop network for further analysis. A sink node is an independent node that acts as a gateway between the WSN and a standard communication network such as the Internet. Data is collected and combined within the node, consuming power and storage resources and requiring additional calculations. The WSN protocol stack used by sink and sensor nodes is similar to that used by MANET networks (the same stack used by TCP / IP networks), but with a management plan shared by all. The difference is that it has been added. Works between layers. Stack addresses the challenges of WSN constraints by combining routing and power consumption, integrating data into network protocols,

efficiently using the power of wireless communication, and facilitating sensor node collaboration [9].

Depending on the capabilities of the sensor, you can create different types of software applications for use in the application layer. This section describes the sensor management protocol SMP (sensor management protocol). It is used to make lower layer hardware and software transparent to sensor network management applications. System administrators and programmers interact with sensor networks via SMP. In fact, it takes into account the lack of global identification and the non-infrastructure nature of sensor networks. SMP provides rules for the following issues that enable interaction between applications and sensor networks [10].

- Naming based on data collection, attributes and grouping.
- Data exchange related to location algorithms.
- Time synchronization.
- The movement of the sensor node.
- Turn the joint on and off.
- WSN configuration status request, WSN reconfiguration.
- Authentication, key distribution, and security [11].

The transport layer is needed to keep data flowing when needed by a particular application. Traditional transport protocols cannot be applied directly to a sensor network without modification. The network layer routes the collected data from the source sensor node to the sink node. Due to the tightly distributed sensor nodes, the adjacent nodes are in close proximity, allowing multi-chip short-range communication. In this case, the source node operates with a routing protocol that selects the most energy efficient multi-chip switch. The data link layer guarantees data framing, frame monitoring, channel access, and error control. The most important feature is channel access control, which stands for MAC. The MAC is responsible for the proper channel access between competing transmitters. To save power, the radio should be turned off to avoid collisions when the sensor is not sending or receiving packets [12].

The physical layer supports low-level air interface operations for consistent transmission and packet reception in harsh wireless environments. These operations include frequency selection, transmit power, modulation, signal acquisition, and coding. Energy, function, and mobility management plans monitor energy, mobility, and task distribution across sensor nodes. The power management plan manages how the sensor node uses that power. For example, a sensor node can turn off the receiver after receiving a message from a neighbor. This is done to avoid duplicate messages. If the sensor node has a low power level, the node notifies the neighboring node that the message cannot be forwarded due to the low power level. The remaining energy is reserved for the senses [13].

Mobility management plans recognize and record joint movements, maintain return routes, and track adjacent joints. Sensor nodes can balance power consumption and functionality by detecting adjacent nodes. Most sensor applications are static, but we cannot rule out the possibility that some applications will have wearable sensors. This is true when the sensor is mounted on mobile platforms such as robots, humans, animals and cars. The path used to send information over the network has a finite lifetime and must be repaired regularly by node mobility. A path that is valid at some point may not be valid for a little longer, even if it is not mobile, because the path may be lacking in energy or may deviate from the joint following the awakening / sleep cycle. In both cases, the road surface is primarily responsible for road maintenance [14].

The mission control plan balances and schedules the unique sensing capabilities for a selected region. Some sensors in a given area, for example, can grow to become off briefly if there's sufficient data left over from different sensors in that area. Also a few senses extra than others relying on the power degree they have. These control layers are important for the sensor nodes so that it will paint collectively to have a green power consumption, to course statistics over a community of cell nodes, and to proportion sources among sensor nodes. Without those layers, the nodes might cooperate personally inefficiently for the community as a whole [15].

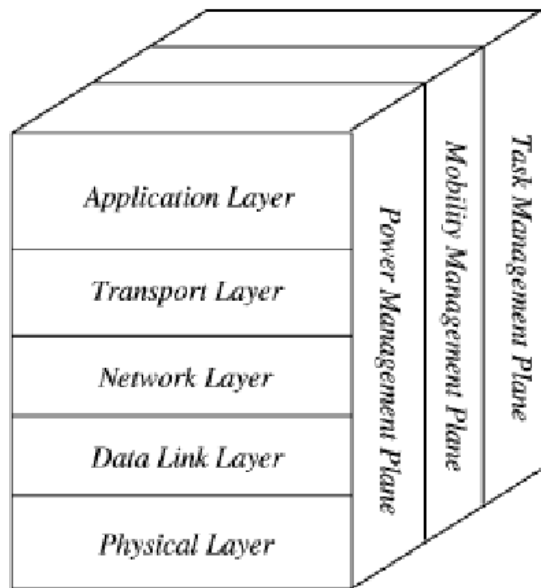


Figure 2. Shows the layers of the WSN architecture.

2.3 Evaluation metrics for a WSN

2.3.1 System evaluation metrics

The key metrics for wireless sensor systems are lifespan, range, cost and ease of installation, response time, timing accuracy, security, and effective sampling speed. Many of these metrics are interrelated. Performance often needs to be derated to metrics such as sampling rate to extend life. In summary, this set of metrics forms a multidimensional space that can be used to describe networking capabilities with wireless sensors [16].

Lifespan: The purpose of both environmental monitoring and security applications is to ensure that nodes in the area do not require human intervention for months or years. Therefore, the expected life expectancy is important when installing these networks. A high-energy diet is a major factor limiting the lifespan of WSNs. Each node should be designed to manage local power to maximize the life of the entire network. For many designs, it is not the average joint life that matters, but the minimum joint life. In a wireless security system, nodes need to last for years. Single node failures create vulnerabilities in these systems. The most important factor in

determining the life of a node is the power consumption of the radio. On wireless sensor nodes, the radio consumes a lot of system power. This power consumption can be reduced by reducing the output power of the transmitter or by reducing the duty cycle of the radio. Using any of these options will have to sacrifice coverage for other system metrics [17].

Coverage: After a long life, coverage is the next key indicator for assessing wireless networks. The ability to distribute the network to as many physical areas as possible greatly increases the value of the system to the end user. Keep in mind that network coverage is not the same as the wireless communication link distance used. Multi-chip communication technology can extend network coverage beyond the distance of wireless technology. In theory, you can increase your network distance indefinitely. However, for certain transmission distances, multi-hop network protocols can increase node power consumption and shorten network life. It also requires a minimum connection density threshold, which can increase distribution costs. Scalability is an important element of WSN value proposition that affects coverage parameters. Increasing the number of nodes in the system will affect the lifetime or effective sample rate. The more sensor points your system has, the more data you need to send and the more power your network consumes. This can be offset by reducing sampling [18].

Cost and simplicity of installation: A key gain of WSNs is their ease of installation. For distribution structures to be successful, the community needs to be self-configured. It has to be feasible for the joints to be positioned everywhere in the surroundings via the means of an untrained individual and the machine placed into operation. The community has to be capable of investigating the niche of records dissemination at the community and document any potential problems. This interprets into the requirement that every tool be capable of carrying out connection detection and decide the relationship nicely. In addition to the preliminary configuration phase, the machine needs to additionally adapt to converting environmental conditions. Throughout the installation, the joints may be repositioned or huge bodily gadgets may be moved via means of interfering with the communicate among the 2 joints. The community has to be capable of reconfiguring itself mechanically while requested to tolerate those occurrences. Initial distribution and configuration are most effective a part of the existence of the community. For longer terms, the overall price of the

machine relates extra to the price of renovation than to the price of preliminary delivery. In actual installations, a fragment of the overall power finances has to be committed to machine renovation and verification. Generating diagnostic and reconfiguration visitors reduces community lifetime and decreases the powerful sampling rate [19].

Response time: Particularly in safety detection packages with inside the area of safety, machine` reaction time is a crucial overall performance metric. An alarm has to be alerted right now while an intrusion is detected. In addition to low-energy operation, nodes need to be successful in getting high-priority, on the spontaneous messaging to speak over the community as quickly as feasible. Response time is likewise essential while environmental tracking is used to manipulate manufacturing unit equipment and equipment. Many customers envision WSNs as crucial equipment for controlling the economic process. These structures could be realistic if the reaction time ensures they have been met. The capacity to have quick reaction time conflicts with a number of the strategies used to boom community lifespan. Network lifespan may be extended via means of having nodes to function the radios for quick durations of time. Reaction time may be progressed via way of means which include joints which are fed all of the time. These nodes can pay attention for alarm messages and direct them to a fundamental routing while necessary. This, however, reduces the convenience of machine delivery [20].

Timely Accuracy: In tracing and environmental applications, samples from multiple nodes can be correlated to determine the nature of the phenomenon being measured. The required accuracy of this correlation mechanism will depend on the propagation of the measured phenomenon. In the case of determining the average temperature of a building, just millisecond accuracy is sufficient to determine how a building responds to a seismic event. To achieve time accuracy, a global clock must be maintained, which can be used to catalog patterns and events in chronological order. In a distributed system, energy is used to maintain a distributed clock. Synchronization time information must be communicated continuously between nodes. The frequency of synchronization messages depends on the desired timing accuracy [4].

Security: In some cases, it can be important to protect the security of information collected by an environmental monitoring application. Networks with wireless sensors must be able to keep the information they gather from eavesdropping

secret. When considering security-driven applications, data security becomes even more important. Not only must the system maintain privacy but it must also be able to authenticate data communication. A combination of privacy and authenticity is required to address the needs of different scenarios. Using cryptographic encryption and authentication has the cost of both network power and bandwidth. Additional calculations must be performed to encrypt and decrypt additional data and bits must be transmitted with each packet. This affects application performance by reducing both the number of samples that can be taken from a given network and the expected lifespan of the network [21].

Effective sample rate: In a data collection network, the effective sample rate is a key performance metric. Effective sampling rate is defined as the sampling rate at which sensory data is received at each individual sensor and communicated to a collection point in the data collection network. Environmental data collection applications require a sampling rate of 12 samples per minute. However, beyond the sampling rate of a single sensor, one must consider the impact of a multi-step architecture on a node's ability to efficiently transmit data to surrounding nodes. In a data collection tree, a node must manage the data of all its children. If a node has n descendants, it has to transmit n times more data and can make measurements in one sampling cycle many times. This exponential increase has a significant effect on the system requirements. One mechanism to increase the effective sampling rate is to use network processing, such as different forms of compression, to reduce the required communication bandwidth by maintaining the same sample rate or local storage for as long as possible [22].

2.3.2 Individual node evaluation metrics

The set of metrics used to assess the overall performance of the sensor community as an entire is associated with the traits of the person nodes that guide them. Evaluation metrics of person nodes also are correlated. A development in a single node stage metric estimate (e.g., distance) regularly reasons any other to expend (e.g. electricity). The following describes every of those metrics [23].

Power: To meet the necessities of packages for lots of years, the person sensor nodes ought to be of extraordinarily low electricity. Unlike mobile ular phones, with a

mean electricity intake of loads of mill amperes and a lifespan of numerous days, the common electricity intake for WSN sensor nodes is measured in microamperes. This extraordinarily low electricity operation may be accomplished with the aid of combining each low electricity hardware additives and coffee obligation cycle operation techniques. During energetic operation, radio communicate will represent an enormous fraction of the full electricity finances of the node. Algorithms and protocols ought to be advanced to lessen radio hobby each time viable. This may be accomplished with the aid of using the usage of localized calculations to lessen the information streams generated with the aid of using the sensors and by using precise utility protocols. For instance, activities from a couple of sensor nodes may be mixed collectively with the aid of using a neighborhood set of nodes earlier than an unmarried end result is transmitted throughout the sensor community [23].

Flexibility: The huge variety of regions of use taken into consideration calls for that the node structure be bendy and adaptive. Each utility situation would require exceptional mixes of: toughness, sampling speed, reaction time, and in-community processing. A WI-FI community sensor structure wishes to be bendy sufficient to deal with a huge variety of utility behaviors. Furthermore, for value motives every tool may have most effective the hardware and software program that it presently wishes for a given utility. The structure ought to make it smooth to bring together the proper set of software program and hardware additives [1-3].

Strength: In order to guide toughness necessities, every joint ought to be designed to be as strong as viable. In a normal distribution, loads of nodes should be painted in concord for years. To gain this, the gadget ought to be constructed in this sort of manner to tolerate and adapt to the failure of person nodes. System modularity is an effective device that may be used to expand a robust gadget. By dividing the capability of the gadget into remote subparts, every characteristic may be completely examined in isolation earlier than being mixed right into an entire utility. To facilitate this, gadget additives ought to be as unbiased as viable and feature designated interfaces, to save you unexpected interactions. In addition to growing the gadget's resilience to node failure, a WSN ought to additionally be strong to outside interference. Since those networks will co-exist with different WI-FI systems, then they ought to own the capacity to evolve their behavior. The electricity of WI-FI

connections to outside interference may be substantially stronger with the aid of the usage of multi-channel and broad-spectrum radios [24].

Safety: In order to satisfy utility-stage safety requirements, man or woman nodes have to be able to appear complicated encryption and authentication algorithms. Wireless information communicate is without problems touchy to eavesdropping. The handiest manner to preserve the information of those non-public and real networks is to encrypt all information transmissions. The CPU has to be capable of both carrying out the specified cryptographic operations itself or with the assistance of the cryptographic accelerators involved [25].

Communication: In phrases of communicate the primary assessment metrics for every WSN are: communicate velocity, strength intake and radius. The transmission distance has a good-sized effect at the minimal applicable density of joints. If the nodes are positioned too some distance apart, an interconnected community or a community with sufficient redundancy to hold an excessive stage of reliability might not be created. Communication velocity additionally has a good-sized effect at the overall performance of the nodes. Higher communicate speeds translate into the capacity to acquire better powerful sampling speeds and decrease grid strength intake. As the bit fee will increase the transmissions require much less time and for that reason probably require much less strength. However, a boom with inside the radio bit fee is frequently followed through a boom in strength intake [13].

Calculation: The maximum in depth computing operations for a sensor node are information processing with inside the community and the control of low-stage WI-FI communicate protocols. Upon admission to the information at the community, the CPU has to concurrently manipulate the radio and record / decode the incoming information. Higher communicate speeds require quicker calculations. In addition to being capable of domestically processing, improving, and discarding sensor readings, sensor nodes have to additionally integrate information with neighboring sensors earlier than transmitting over the community. Results from more than one node may be summarized together. This in-community processing calls for extra computing resources. 2-four processing MIPS (million commands in line with second) are required to put into effect the radio communicate protocols utilized in WSN. Beyond that, processing utility information can eat an arbitrary quantity of calculations relying on what number of calculations it performs [3].

Time Synchronization: To support time-correlated sensor readings and low-cycle activity in data collection application scenarios, nodes must be able to maintain primary time synchronization with other members of the network. Nodes must sleep and wake up together to communicate cyclically. Faults in the timing mechanism create inefficiencies that lead to increased duty cycles [26].

Size and cost: The physical size and cost of individual sensor nodes have a direct and significant impact on the ease and cost of distribution. In data collection networks, researchers often operate with a fixed budget. Their main goal is to collect data from as many locations as possible without going over their fixed budget. Reducing the cost per node will lead to the ability to purchase more nodes, distribute a higher density sensor network, and collect more data. The physical size also affects the ease of distribution across the network. Smaller buttons can be placed in more locations and used in more situations. In the audience tracking scenario, the smaller size and lower cost nodes will track more audience [27].

2.4 Wireless sensor network applications

The small size of node devices, their independent wireless operation, and the large-scale development of high-density networks make WSN very attractive for many applications. Compared to traditional communication networks, WSN nodes do not necessarily require an ID (e.g., address). Rather, it focuses on the data collected by the sensor. Attributes are typically assigned to data, allowing an application to request data related to a particular attribute. This separates the data from the sensor that generated it. This allows for robust application design. If a node fails, you can copy the data generated by the node to another sensor (e.g., neighbor) for later retrieval. Therefore, if one of the nodes fails, a new topology will be configured and data will continue to be distributed throughout the network [28].

The more nodes that are placed in the field, the more routing opportunities will be created. Various criteria are used to classify multiple WSN applications. The following topics show two types of classifications that serve as criteria. Data processing methods and areas of life where these uses are implemented. Classification criteria are important because their choices give different perspectives on building a

network architecture. Sensor nodes can be used for continuous acquisition, event acquisition, or position acquisition. To get an accurate picture of how this data is reported in a timely manner, we classify applications into three main classes: environmental data acquisition, security monitoring, and sensor node tracking [29].

Sensor networks consist of different types of sensors such as seismic, thermal, visual, acoustic, infrared, and radar, and monitor different environmental conditions, including: B.: Object properties such as temperature, humidity, vehicle movement, lighting, pressure, noise level, presence / absence of object, speed, direction, size. The level of detail of these nodes and the concept of wireless connectivity has led to the widespread use of WSNs-used for most of human activity. Although the classification into different categories may not be absolute, WSN applications can be categorized into the following groups according to the context of activities in different areas of life: military, environmental, commercial, Health, robotics [30].

Fast installation, self-employer and fault tolerance are desired capabilities for navy packages. In those networks we've got a dense and low-value placement of sensor nodes, so the destruction of a few nodes with the aid of using enemy assaults has no impact on the navy operation as a whole. In navy packages, WSNs are used for intelligence gathering, enemy monitoring, and surveillance on a battlefield. Enemy type and monitoring are fundamental battlefield tactical packages. Other examples encompass detecting chemical assaults (nuclear, organic), anti-sniper tactics, etc. [31].

If we have been to organization in a single class all of the packages associated with environmental tracking we will say that they're several in exceptional regions which includes: monitoring actions of birds, small animals and insects; tracking of environmental situations affecting vegetation and livestock; irrigation; macro-contraptions for large-scale Earth tracking and planetary exploration; chemical and organic detections; tracking of the oceanic and atmospheric environment; woodland hearthplace detection; meteorological or geophysical research; flood detection and pollutants study. This extensive variety of packages is split into groups: indoor tracking and outside tracking [32].

In indoor tracking we will point out the automated lighting fixtures and heating structures of buildings, in which networks with sensors screen mild and temperature situations with the intention to have a green and within your means use of the gadget of those structures. Other indoor packages are emergency services, structures that cope

with decreasing the unfolding of hearth place and examining earthquake harm thru buildings. In outside tracking we will point out ecological, agricultural packages and early caution structures in case of disasters. Forest hearth place detection, flood detection, volcanic eruption tracking, unsafe substance detection are the primary examples of those packages [33].

When WSNs are designed for scientific functions, they're regularly known as WI-FI scientific sensor networks (WMSNs). These nets are established with inside the patient`s frame and used to carefully screen the physiological situations of the sufferers. Their sensors screen important symptoms and symptoms of the patient`s frame (which includes temperature, coronary heart rate, blood pressure, oxygen saturation, etc.) and transmit records to a far-off middle without human intervention. A medical doctor can then interpret the sensor readings to help in step with the patient's situations. From this sufferer can gain long-time period tracking even after discharge from the hospital. In general, the packages of WI-FI sensor networks in healthcare structures may be divided into 3 categories: Clinical tracking of sufferers, home tracking with the aid of using care facilities for persistent and aged sufferers, Long-time period series of medical databases [34].

Several applications have paired sensor nodes with robots supporting large-scale sensor network research involving robots. Intel is conducting research in this area, where mobile robots are seen as gateways into the WSN to support the network. Some of the tasks are: indefinitely storing power supplies, maintaining and configuring the hardware, detecting sensor failures, and deploying accordingly to enable interconnection between nodes. Another important application involves the localization of nodes in the sensor network using mobile robots. This approach aims to solve the problem of unifying a network that has been isolated due to disconnected sensors. In all of these studies, the robots were integrated as part of the sensor network [36].

Industrial/Structural Monitoring: Equipment/physical condition monitoring is a typical industrial application that can utilize WSNs. Sensors connected to critical equipment can detect and prevent future equipment failures. In addition, WSN is used for structural condition monitoring to detect damage to bridges, buildings, vehicle tracking and detection, and more [35].

Transportation and logistics: Inventory control and warehouse monitoring are difficult tasks in transportation and logistics applications. Using WSNs assets can be monitored from production to distribution to the end user [37].

Automated Homes: Sensor nodes can be placed on various home appliances and form an internal network that connects to an external network via the Internet allowing people to control and manage their home even remotely. Nowadays, such applications have been developed and are known as smart environments [38].



Figure 3. Reflects a concise overview of all WSN uses.

2.5 Classification

Routing technique is used to send data during communication between sensor nodes and base stations. Various routing protocols have been proposed for wireless sensor networks, which are classified according to different parameters. In this issue we will deal with classification based on: mode of operation and application type, communication method of the node with BS (Base Station) and classification according to the structure of the network [39].

2.5.1 Classification based on mode of operation

Protocols can be classified as proactive, reactive, and hybrid, depending on how they work and the type of target application. In an active protocol, nodes activate their sensors and transmitters, sense the environment, and transmit data to the base station via a predefined path. The LEACH protocol falls into this category. In the case of a reactive protocol, if there are unexpected changes in the perceived properties beyond

some predefined limit value, the nodes will respond immediately. This type of protocol is used in time-critical applications. TEEN is an example of a reactive protocol. Hybrid protocols like APTEEN (Adaptive Periodic TEEN) include concepts of both types: proactive and reactive. They first compute all routes and then improve these routes at routing time [40].

2.5.2 Classification according to the way the node communicates with BS

Depending on how the node communicates with the BS, routing protocols can be classified into direct communication protocols, planar protocols, and clustering protocols. The BS node is a separate network node that represents the main network node for data collection. This button can often also act as a sink button. In direct communication protocols, each node can send information directly to the BS. When this is applied to a very large network, the energy of the sensor nodes can be exhausted very quickly. Scalability in this case is very low [41]. SPIN (Sensor Protocol for Negotiating Information) is an example of this type of protocol. In the case of a flat protocol, such as Rumor Routing [43], if a node needs to transmit data, it first searches for a valid path to the BS and then transmits the data. In this case, the nodes around the base station can quickly run out of power, indicating average scalability. According to the clustering protocol, all the nodes in the network are divided into multiple clusters. Each cluster has a head node, hereinafter referred to as CH (Cluster Head), which communicates directly with the BS. All nodes in the pool send their data to the respective CH node (we refer to TEEN again, for example) [42].

2.5.3 Classification according to network structure

According to the structure of the network, protocols can be classified into hierarchical, data-centric, and location-based protocols. Hierarchical routing (e.g., LEACH, TEEN, APTEEN) is used to achieve energy efficient routing, nodes with higher energy level can be used to process and send information; nodes with less energy are used to direct the sensation into the area of interest. Meanwhile, in data-

centric protocols, in the absence of a global node identifier, attribute-based labels are needed to identify the required data quality through questionnaires. These questionnaires are sent to certain areas by the base station of the network, which will wait for data from sensors located in the selected area. Hence, we are treating data-driven routing differently than traditional routing based on node addresses, where we create paths between addressable nodes managed by the network layer in the transport stack. Depending on the question, the sensors collect specific data from the area of interest and only that specific information needs to be transmitted to the BS, thus reducing the number of transmissions [44] [46]. SPIN is the first data-centric protocol. Location-based protocols use the node's location information to transmit data to desired areas [42]. Location information can be obtained from GPS signals (Global Positioning System), received radio signal strength, etc. The use of location information allows an optimal route to be formed without the use of inundation techniques. GEAR (Geographic and Energy Aware Routing) is an example of a location-based routing protocol [48].

2.6 Existing protocols

Data-centric routing protocol: In some sensor network applications, it is not possible to enter a common ID for each node due to their very large number. Data is usually transmitted from sensor nodes in areas with multiple redundancies. In terms of energy use, this surplus is a source of inefficiency. Therefore, routing protocols must be able to select a set of sensor nodes and must account for data aggregation when transmitting. These circumstances have led to the advent of data-centric routing. In this route, the receiver nodes send queries to some specific regions and wait for data from sensors located in the selected regions [47].

Flooding and turbulence: Two classical mechanisms for transmitting data across sensor networks are flooding and turbulence, which do not require routing algorithms or topology maintenance. In the event of a flood, each sensor broadcasts the received data packet to all its neighbors, and this process continues until the packet reaches its destination or when the packet has reached its maximum expected number. multi. Chatter, on the other hand, is a version in which the receiving node sends a

packet to a randomly chosen neighbor, which forwards the packet to another random neighbor and so on until the destination. Flooding is done very simply but has some problems like: duplicate messages on the same node, overlapping packets in case two nodes feel in the same area and sending similar packets to the same neighbors and does not store limited resources, consuming large amounts of energy [40] [41] [42] [43]. The duplicate problem (presented in below pictures) is explained in the figure where node A overflows its data to all neighboring nodes. Node D receives two identical copies of this data. Two sensor nodes cover a geographical overlap r and node D receives identical copies of the data from them. Chatter avoids the problem of message duplication simply by forwarding the packet to a randomly selected node instead of transmitting it. But in this method, another problem appears which is the delay in sending data across the nodes [13].



Figure 4. Node communication between each other.

SPIN is part of a family of adaptive protocols that use algorithms that work with data negotiation and resource customization. It is a data-centric routing protocol. It makes two assumptions: 1) all nodes in the network are base stations, 2) adjacent nodes have similar data. The main idea of SPIN is to name data using a high-level descriptor or metadata. Since all nodes are assumed to be base stations, all information is broadcast to each node in the network. Thus, the user can query any node and can get the information instantly. Nodes in this network use higher-level labels to describe their collected data called metadata [42] [54].

SPIN has three types of messages: ADV, REQ, and DATA. An ADV message is generated when a node has data to send. This message contains metadata. The REQ message that a node sends when it wants to receive data. The DATA message contains single-ended data containing the metadata for that data. Before a DATA message is sent, the sensor node transmits an ADV message containing the descriptor (i.e., metadata) of the data. If a neighbor is interested in this data, it sends a REQ to the DATA message, which is then sent to this neighbor. Correspondingly, the adjacent

node repeats the same process until the data is sent to the sink node (or BS). [18] One of the advantages of SPIN is that topology changes are localized because each node only needs to recognize its neighbors after only one hop. SPIN is also more power efficient than flooding, and meta data negotiation cuts data redundancy by almost half. However, SPIN has obvious disadvantages. First of all, it's not scalable. Second, the nodes around the sink node can drain all of their energy if the sink is interested in multiple events. Finally, the ADV data notification mechanism cannot guarantee data dissemination. For example, if the nodes interested in data are too far away from the source node and the nodes between the source and destination are not interested in that data, the data will not reach the destination [19].

Directed Diffusion is an information-centric, application-particular protocol wherein information generated through sensor nodes are named through attribute-cost pairs. This pair is used to request information on the time of request, through questionnaires. Using this naming scheme avoids useless routing operations at the grid layer whilst saving strength. The DOJ includes four elements: hobby kind messages, information messages, gradients and amplifiers. A hobby message (a listing of attribute, cost pairs) describes a target. Data messages are named using attribute, cost pairs. A gradient specifies the date price and course of the event. Amplifiers pick out a selected route from a fixed path. A BS diffuses a questionnaire closer to the nodes with inside the location of hobby. The questionnaire or message of a hobby is subtle hop through hop. Each sensor that gets the message of hobby locations a gradient of nodes from which it gets the message. This technique maintains till all gradients from the supply node to BS are set [19].

Sensitive information is dispatched to BS through opposite routes. Intermediate nodes can mix their information relying on the information message, hence lowering the fee of communication. As the transmission right here isn't always dependable BS periodically resends the message of hobby till it begins off evolving receiving the information asked through the supply. The gain of DD is strength saving through deciding on the top-of-the-line route, storage (caching) and information processing in the network. However, he has a few problems. Initially, information aggregation calls for time-synchronization strategies that aren't without difficulty applied in WSN. Furthermore, it cannot be implemented to packages that require non-stop information transmission, as it might convey inefficiency, because it makes use of an on-call for

information transmission model. DOJ is consequently now no longer a very good preference as routing protocol in packages along with environmental monitoring. Also, the technique of linking the information to the questionnaires creates extra load at the sensors [57].

Rumor Routing, is a version of DD and is in particular utilized in packages in which geo-routing cannot be applied. DD makes use of flooding to inject a utility throughout the community. But every so often the quantity of statistics required is so small that flooding turns into unnecessary. An opportunity manner is to flood occasions whilst their wide variety is small and the wide variety of requests is high. The fundamental concept is to path requests to nodes which have located a specific occasion in preference to asking the whole community with the aid of using flooding to get records at the incidence of the occasion. RR generates numerous long-lived programs known as dealers. When a node detects an occasion, it provides it to its nearby occasion desk and generates an agent. Agents tour the net to unfold the phrase approximately nearby occasions to faraway nodes, following random paths. The nodes visited with the aid of using them create a gradient for the occasions. When a node generates a request for an occasion, nodes which have created a gradient over the occasion can reply with the aid of using relating to their occasion tables. Thus, its miles are not vital for flooding throughout the community, consequently lowering the price of communication [18] [19].

2.7 Hierarchical routing protocols

Even in sensor networks as in many other communication networks, scalability remains one of the most important design attributes. In a single node-level network, there can be an increase in the load at the gateway node level with increasing sensor density. This payload can lead to communication delays and incomplete tracking of events. Furthermore, the single-port architecture is not scalable when a very large number of sensors cover a large study area. In order for the system to support the additional load and cover a large study area without sacrificing service, the concept of a clustered network has been introduced in several routing methods. The formation of special clusters is based on the stored energy of the sensors and their proximity to the

leader node. Using cluster method increases the scalability and efficiency of communication, so it has been used to implement efficient routing in WSN [3].

In the hierarchical architecture, high energy nodes are used to process and send information, and low energy nodes are used to sense the vicinity of the target. As such, creating clusters and assigning specific tasks to master nodes contributes to the longevity and scalability of the entire system as well as energy efficiency. The main purpose of hierarchical routing is to maintain efficient power consumption at sensor nodes by including them in multi-hop communication in a separate cluster and performing data aggregation and scrambling to reduce the number of messages transmitted to the BS. In a flat catalog all nodes play the same role, while hierarchical protocols aim to group nodes together so that the main node of the group does a bit of aggregation and data reduction to save power at the network level. Similar to a cellular network, here sensor nodes send their data to a central master node, which then sends the data to the intended receiver [4].

LEACH: The idea is to form clusters based on received signal strength and use local master nodes as routers to the receiving node. This will save energy as the transmission will only be done by CH nodes instead of all sensor nodes. The CH node collects data from its cluster nodes and sends it directly to the receiving node after their aggregation. In order for all nodes in the network to consume an equal amount of energy and thus increase the lifetime of the network, this algorithm randomly changes the CH nodes every cycle. The only node that joins the group has the leader node closest to the node in question. Simple nodes never communicate directly with the base station. They only communicate with the leader node of their group. Communication with the base station takes place through the main CH nodes. It is assumed that the CH nodes manage to communicate directly by one hop with the base station [5].

PEGASIS (Sufficient Energy Collection in Sensor Information System) is an improvement of LEACH. Instead of forming multiple clusters, it forms a chain with sensor nodes where each node transmits and receives from an adjacent node and only one node in the chain is selected to transmit to the base station. Collected data is transmitted from one node to another, aggregated and sent to the base station. String construction is done in a greedy way. Node c2 passes the queue to node c4, the queue sends its data to node c3. Node c3 aggregates these data with its own and transmits them to node c2. This node expects to receive data from two neighboring nodes, then

aggregates its data with that of its neighbors, and finally transmits a message to the base station. PEGASIS assumes that all sensor nodes have the same power level and die more or less at the same time. According to this protocol, all nodes have information about all other nodes and each node is capable of transmitting directly to the BS. Therefore, since the nodes are static and have global knowledge of the network, the chain is easily built using a greedy algorithm. PEGASIS outperforms LEACH in terms of longevity and this has been demonstrated in different mesh sizes and topologies. This result is due to the removal of the dynamic clustering load, the small transmission distance between non-conductive nodes, and the limitation on the number of transmissions. But on the other hand, PEGASIS brings unnecessary delay to nodes far in the chain, and configuration with only one master node can lead to deadlock [5].

2.8 Location-based routing protocols

The GEAR (Geographic and Energy Aware Routing) protocol makes use of the power and heuristic know-how of selecting pals to course a package deal to the favored vicinity. It considers best a positive vicinity rather than sending hobby throughout the community as happens in Direct Diffusion for that reason lowering the range of interests. In GEAR every node calculates a fee of evaluation and a fee of getting to know to attain the vacation spot via its pals. Estimation fee is a mixture of residual power and distance to vacation spot. The fee of getting to know is an evaluation of the fee of evaluation that takes under consideration the routing round potholes with inside the community. A pit happens while a node has no neighbor towards the vacation spot vicinity than itself. When there aren't any potholes the fee of evaluation is same to the fee of getting to know. The fee of getting to know is tracked at the manner lower back whenever a package deal arrives on the vacation spot so that it will regulate the course diagram for the following package deal. There are ranges with inside the algorithm [47].

Phase 1 - Tracking programs across the goal vicinity. Upon receiving a packet, a node assesses its pals to peer if it has any towards the goal than itself. If there's greater than one, the closest one is chosen for the following jump. If all of the pals are in addition far from the goal than the node in question, then a pit is formed. In this case,

one of the paths is chosen on the idea of the getting to know fee function. The choice is up to date in line with the convergence of this fee at some point of the transport of the package deal. Phase 2 - Forwarding the package deal with inside the goal vicinity. Once the packet reaches the goal vicinity, it is able to be subtle in that vicinity with the aid of using both recursive geographical monitoring or flooding. District flooding is ideal while the sensors aren't densely distributed. In better density networks recursive geographical flooding is greater efficient. In his case, the vicinity is split into 4 sub-areas and 4 copies of the message are created, one for every. Then every of those sub-areas is split into 4 components once more and so forth the separation and forwarding of packet copies maintains whilst regions continue to be best one node [47].

The GAF (Geographic Adaptive Fidelity) protocol became firstly designed for ad-hoc networks, however can also be implemented to sensor networks. Although it's far from region-primarily based totally type, it is able to additionally be carried out as a hierarchical protocol wherein clusters are primarily based totally on geographical region. Initially the place of hobby is split into numerous constant regions forming a digital community. The nodes in every place have one-of-a-kind functionalities and every of them makes use of its GPS region to attach itself to a community factor. Nodes placed on the equal community factor are taken into consideration equally in phrases of packet routing fee. This equivalence is cut up to preserve numerous nodes of a specific community placed in sleep mode to shop power. Moreover, GAF will increase community lifestyles while the range of nodes with inside the community will increase. GAF conserves energy, preserving off pointless grid nodes however without affecting the extent of routing reliability. The GAF consists of 3 states: detection country, lively country, and sleep country. Detection country is used to outline acquaintances with inside the digital community. The lively country is used for the routing manner and on the time of sleep country the node radio is switched off. To deal with mobility, every node with inside the community estimates its departure time from the community and sends it to its acquaintances. Sleeping acquaintances alter their sleep time in keeping with retaining ordinary reliability. Before the time for the node to leave the lively country expires, the nodes with inside the dozing country awaken and certainly considered one among them turns into lively [6].

VCP (Virtual Cord Protocol), is a special protocol that belongs to the group of protocols that are based on the virtual location of the node, but also has a data centric

nature. It consists of setting up a virtual cord that connects the nodes to an ordered series of unique coordinates. An intermediate node has the ancestor and descendant with coordinates directly below and above it. The VCP uses the virtual cord to connect the data to the relative position of the nodes. Each node keeps in a table its ancestor, descendant, and physical neighbors if any. By means of a hash function the generated data is connected to a key and stored in that node which is responsible for the key in question, i.e., in that node which has the coordinate closest to the value of the key. The same hash function is used to query the data. Thus, VCP performs data lookup using the relative positions of the nodes. There is no need to know the real addresses, for packet routing a simple mechanism is used that of the neighbor with the relative address closest to the destination. The proposed method integrates the virtual addressing technique that VCP uses to enable easy routing to leading WSN nodes with clusters [7].

2.9 Addressing the data management problem

The usefulness of the records can't be decided a priori, as it relies upon the form of utility, the bodily phenomenon to be determined and the predicted lifespan of the sensor community. As intense cases, we will take for example a utility that reviews the temperature in a far-flung vicinity and a utility of hearth place alarm structures that come across hearth place in a public office. In each utility, temperature is the phenomenon to be measured. However, with inside the first case the quiet person is extra interested by gathering a huge range of sensor readings over an extended length of time. This case is characterized by means of huge volumes of facts amassed over an extended length of time, however without the want for intense accuracy with inside the records amassed. On the other hand, the utility of hearth place alarm structures is in a dormant country maximum of the time, however they have to be very dependable and correct whilst hearth place is detected. All of those issues are meditated in how a WSN is programmed and the way the facts circulating with inside the sensor community is processed and managed [8].

Data processing in WSN

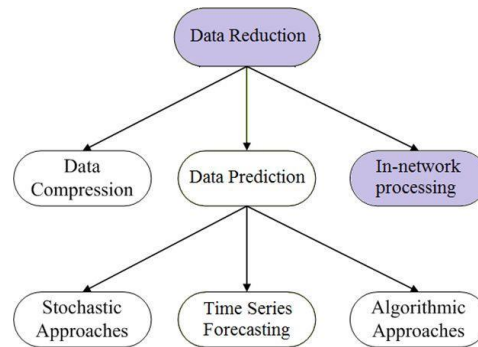


Figure 5. Shows the data processing in WSN.

The conventional methods which have been used for many years adapt to the opportunities of the WSN. For instance, the usage of a P2P gadget that's self-organizing, which includes entities known as friends which are the equal and autonomous. These entities together use the assets allotted in a community surroundings even as averting the usage of centralized assets. New methods had been proposed to set up a hyperlink among the facts, content material and the node identifier (as an example IP address). These networks are called based P2P networks. The courting among the content material identifier and the node identifier is generally primarily based totally on Distributed Hash Tables [DHT]. DHT tables control facts via means of splitting it throughout community nodes and put into effect a routing scheme that lets in a node to efficiently look for the node wherein a selected fact is located. The fundamental concept of DHT is simple: the facts are related to numbers, and every node with inside the community is chargeable for a string of those numbers [29 [7] [8].

Although DHT-primarily based totally P2P structures can use distinctive routing schemes to look for every other connection, the best rule they have to observe is for messages to enhance to the ones friends which have numbers in the direction of the vacation spot identifier. Therefore, the answer of consecutive jumps is decided by means of algorithms and routing metrics. A not unusual place metric is the numerical proximity metric. This scheme, preferably routes dependable messages to the vacation spot with a small jump. But realistically, it's far harder to layout algorithms with routing metrics wherein node disasters and routing of wrong records have very little

effect on routing accuracy and gadget stability. In current sensor networks for tracking purposes, the sensors are assumed to be pre-programmed and have to ship the facts to a significant terminal wherein it's far amassed and saved for evaluation at a later time. This manner gives essential drawbacks: 1) the person can't dynamically extrade the conduct of the system and 2) communication networks are so much more costly than nearby calculations, so nearby processing and garage inside the community can lessen aid use and boom the lifespan of the sensor community.

2.10 Data transmission

The main source of power consumption in WSN is data transmission. Much work and research has been done to optimize data transmission at the physical, data link and network layers. The basic tasks of the physical layer are frequency selection and modulation. One option for the communication channel is to use the industrial, scientific, and medical (ISM) bands, which allow license-free communications in most countries. The data link layer is primarily responsible for controlling access to the environment and controlling errors. Based on tests carried out to study packet delivery performance in three different environments (in an indoor office building, in a tree-lined habitat, and in an open parking lot), Significant asymmetries were observed in real world environments, and performance in those environments was rather pessimistic [18] 11].

As mentioned earlier, since one of the activities that consumes the most energy is data transmission, WSN's research focuses more on the research and design of energy-saving algorithms for data transmission. from the sensor nodes to the base station. Usually data transmission is multi-hop (from node to node to base station) and this leads to a polynomial increase in the energy cost of radio transmission depending on the transmission distance. Today, research is mainly focused on the network layer, which is primarily responsible for routing strategies. The classification of routing algorithms and protocols has been discussed extensively in the third chapter. We return specifically to two large groups of routing algorithms used in WSNs, where one is based on how the network reacts to changes in topology and the other based on the location of the node's knot [9].

Many ad-hoc algorithms primarily based totally on topology modifications had been tailored to paintings at the WSN. We have stated this institution earlier than as a class primarily based totally at the mode of operation, however when you consider that this class additionally influences the mode of transmission, the subsequent describes the maximum regular characteristics. As we stated this institution changed into proactive, reactive and hybrid. This class comes from the conventional class used for routing protocols on ad-hoc cellular networks (MANET). Proactive protocols also are known as international country protocols. They keep routing data for legitimate routes at the community even though those routes aren't presently in use. Routing tables are saved modern-day through the community message flooding approach to tune topological modifications. The principal downside of those algorithms is that the upkeep of unused roads occupies a sizable part of the bandwidth while the topology modifications frequently. This results in a sluggish reaction in instances of restructuring and failures [10].

Reactive routing protocols however preserve the handiest of the routes which are presently in use. Routing infrastructure is created handiest while a node seeks to transmit a packet. This manner saves assets at some stage in inactive periods, however has the overhead of route detection for every originating node. These protocols are typically greater scalable, as they generate much less community visitors, and are as a result appropriate for tremendously dynamic ad-hoc networks. However, avenue upkeep handiest while its miles used calls for a disclosure manner earlier than packet alternate among the 2 verbal exchange entities. This brings postponement for the primary bundle to be transmitted. The lengthy postpone time and of route additionally the era of detection packets will increase the visitors while we've topology extrude and may cause community blockage. Hybrid protocols, integrate functions of the 2 classes stated above. They preserve an international view handiest for a positive wide variety of jumps for every node. Routing is first of all created with numerous proactive pathways after which serves the call for from the nodes activated with the aid of using reactive coverage. The answer for one technique or any other calls for predetermination for regular instances. The hassle with those algorithms is they depend upon the wide variety of nodes activated and that the reaction to traffic requests relies upon at the traffic extent gradient.

Geo-based or location-based routing algorithms remove some topology-based routing constraints by using the locations of the nodes. Geolocation algorithms can mainly be divided into two categories: based on physical location and based on virtual location. In the first type, each node needs to know its own physical location. It is generally assumed that each node determines its location using the Global Positioning System & # 40; GPS & # 41; or some other location service. Location services are used by the packet sender to determine the destination location and then enter it into the packet's destination address. The routing decision in each packet is then based on the destination location contained in the packet and the locations of the neighboring nodes that will forward the packet. In the second type, a virtual location is assigned to each node. The goal of the method proposed in this article is to use this node which depends on the virtual coordinates of the node [11].

2.11 Treat WSN as distributed databases

Usually, a WSN is surrounded by the phenomenon it monitors. The most common way is for the user to query the sensors via a query-like statement (such as SQL). It is an efficient way to summarize system data and relies on a user-friendly interface to program the sensors. This, as we said at the beginning, is why we can look at the WSN network as a distributed database. But there are certainly differences between a WSN and a traditional database system, which must be taken into account in carefully designing the query sublayer to benefit from efficient data management. Some of these differences are:

- Data flow tracking - Unlike a database, WSN responds by sending data at predetermined time intervals when receiving a query.
- Communication errors - While the data obtained from the database response is completely reliable, the data generated by the sensor nodes is distributed to the sink node via multi-hop communication, where the communication lines may be unreliable and that are influenced by errors. This means that the data reaches the sink node with a quite variable delay and reliability.
- Real-time processing - Since the energy expended in processing operations is several orders of magnitude smaller than that spent on communication, it is usually preferable to process information in real-time, in order to avoid unnecessary transmissions. The energy problem is not essential in databases [12].

There are several processor implementations for translating query with SQL-like syntax into system operations. TinyDB is a query processor implementation that runs on top of the TinyOS operating system. The advantage of using a user-friendly interface, allows the remote user to easily search for data in WSN using the appropriate SQL syntax. The COUGAR data-centric protocol is another implementation that uses a questionnaire plan to determine the role of nodes in in-network processing of queries. COUGAR also deals with the study of the interaction of the query sublayer with the bottom of the routing layer [12].

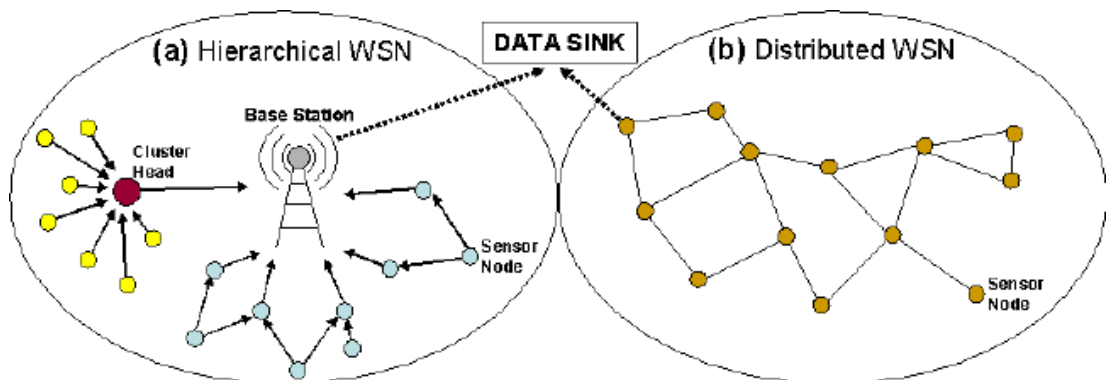


Figure 6. Shows the distribution of data in the WSN.

2.12 Naming and indexing of data

There are two ways to use the data generated by the sensors: transmitting real-time information to the base station or retrieving the required data via the queries mentioned above. For the second way, it is necessary to link the names to the data produced. There are well known and efficient naming methods for web data that can be adapted to WSN. However, the nature of the data in WSN is different from that of web data. Internet users are more interested in the data itself than when and where the data was created. In contrast, in a WSN, these attributes can be of the same importance as the data itself. The second difference is that inline data (net) is usually named manually. On the other hand, the sensor nodes will automatically name the generated data. This results in a large domain namespace on the Internet as opposed to a very limited WSN namespace. The document addresses the challenges of naming and indexing sensory data. The origin of the data (origin) is considered the basis for naming

and resolving them. Before something is indexed, the granularity at which it will be indexed is chosen [13].

Theoretically, any sensor reading could be indexed. However, this seems impractical, from the absolute number of readings and also not necessarily usable, as the individual readings from the separate sensors make no sense. A better solution is to index groups of sensor metrics, grouped by some characteristic, usually time. For example, a set of readings might contain all readings of a particular nature over a period of one hour or one minute. For data collection to be practical, each sensor reader must have a unique name. The underlying problem is that the name is trying to encode a set of properties. In many areas, this identifying information is referred to as provenance. Provenance of data collection is not just a useful description. This is the unique identifier for this data set. This, in effect, makes Provenance the name of the dataset. Therefore, origin must be an important factor [13].

Instead of encoding the name as a string, a more complete representation is made as a set of name-value pairs. Of course, the traditional designation can also be used. In addition, the provenance can be application specific. The use of an indexing structure in systems that store sensory data provides efficient search in many respects. The document proposes an efficient data distribution method by distributed indexing over very large WSNs. This method minimizes the use of computer resources and at the same time ensures quick response to the questionnaire. In addition, by storing indexed data distributed across the network, scalability and load balancing are ensured [13].

2.13 Data storage

The effective local storage of data at the communication level is done to store them. However, to retrieve data from the network, the only option is to ask as many nodes as possible if they currently have the required data. Although the storage complexity is only $O(1)$, the network data retrieval complexity is $O(N)$. Local storage mode has the advantage that no active effort is required to maintain the routing table. But on the other hand, the limited storage space at the nodes suggests that the storage capacity of the nodes can be depleted quickly, as seen in a single node. Therefore,

storage capacity is a concern to be taken into account when data is stored locally on the nodes. There are many ways that can be used to get data from the network. One way is to flood a network of questionnaires to find answers. This technique, which we will call flooding, returns a very fast response, which is very pleasant to dynamic changes in the network, but requires too many messages, leads to depletion of the node farm, and can overdo it. network load, especially in dense networks [15] [16] [20].

One of the most common flooding techniques used as a query algorithm in WSNs is directional broadcasting. This algorithm includes several factors: preferences, data messages, gradients, and gain. An interest message is a query that specifies what the user is looking for. Each preference contains a description of the sensor task supported by the sensor network to receive data. Events can be data collected or processed by a physical phenomenon. Data is named using attribute-value pairs. A discovery task (or a subtask of it) propagates through the network as an interest in labeled data. This distribution produces gradients in the grid that are set to "complete" the event (data meets interest). The direction of the gradient is towards the adjacent node from which the interest is taken. Events started coming to people who became interested along many gradient paths. Then, the receiving node, upon receiving the response, consolidates the paths with better quality. To support this large message load, several algorithms have been developed based on random or predetermined event motion, including ACQUIRE and Rumor Routing [14].

External hosting mode is similar to client-server mode. Each sensor reading must be transmitted to the base station in real time. Unlike local storage, offline storage does not impose communication costs to retrieve data. Currently, this conservation strategy is usable when all sensorial indicators are involved, for example in habitat monitoring. Typical systems that use external storage require efficient routing algorithms to ensure low communication costs for data storage. In these algorithms, the complexity to store data is $O(N)$. Since all collected data is stored on an external server, there is no cost to retrieve the data, since its storage location is known in advance. However, the communication channel at the Sink node may experience heavy traffic loads, thereby causing system-wide limitations. In general, the external storage method is better for simple and small networks because the cost of retrieving data is optimal. However, scalability is an essential trait that is penalized because this

approach requires the availability of a path at all times from each node of the network to the Sink node [14].

Both of the above methods have limitations that may affect the scalability and efficiency of WSNs. In this case, we gradually understand that if the system grows by several orders of magnitude, the complexity of storing and finding nodes will not increase too much. Indeed, external storage is penalized by nonlinear complexity due to communication with the Sink node. Local storage mode avoids managing references to other nodes, so data retrieval becomes more expensive and causes scalability issues due to communication load and power consumption. A better solution to data recovery would be to avoid these problems by finding a satisfying medium between these two methods. Instead of storing data in a single node outside of the network, it is stored by distributing it to different nodes in the network. The collected data is stored in each node of the network and not necessarily in the node that collected the data. This means that the data sent will be sent to one or a group of nodes in the network, and all requests for this data will go to that node or group of nodes that host it. A convenient method of determining how data storage will be distributed is distributed indexing, used in P2P systems, usually implemented as DHT [15].

Therefore, in scientific work that is data-driven in nature, certain methods associate the name of the sense data with the specific nodes that will contain this data, often using a binding function. Therefore, requests are sent directly to the respective node. A typical network storage for WSN is the Geographic Hash Table (GHT) method. GHT combines the idea of DHT with geographical naming and routing. In GHT there is space for button id and key. Unlike other DHTs, this space is not virtual but physical. GHT hashes the keys to geographic coordinates, so the data stored in the sensor node is geographically closer to its primary hash. There are many other examples of network attached storage schemes in WSN such as DIFS and DIMENSIONS. DIFS is another case that builds on top of GHT and considers high-level events with many properties. This considers a distributed index based on key values by hash keys. DIFS builds a hierarchical index with multiple roots that balances communication overhead to efficiently support zone requests. DIMENSIONS is a data storage system in which new data is stored in its entirety, while long-term data is stored incompletely. It uses temporal and spatial aggregation in a hierarchical structure, to find the right subset of sensor nodes that respond to a given set of questionnaires. Its

performance is highly dependent on data correlation due to aggregated data schema. In the literature, the replacement of storage nodes is used to minimize the total energy costs for data collection at the storage nodes [15].

There are two options for storing data in DHT. In the first method known as direct storage, the data is copied after entering the node responsible for it. The good thing is that the data is located directly in the P2P system and the node that received the data can then leave the DHT without losing the ability to have the data. The downside is that it is expensive in terms of storage space and network bandwidth. Since nodes can fail, data must be replicated to multiple nodes to increase its availability. Also, for many nodes, a large amount of storage space is required for each node. The other option, called indirect storage, stores references to data. The data sensor node provides only a data pointer to the node responsible for that data, resulting in reduced load on the DHT. The data itself remains in the node that feels it. However, data is only available when the node responsible for it is available. Thus, the first method results in more traffic in memory, but the request message finds the final destination faster than the second method. The most appropriate method for WSN depends on the size of the data. Direct storage is better for small data, while indirect storage is more suitable for larger data [16].

2.14 Data processing

Data processing commonly results in information discount and therefore reduces the usage of energy sources, bandwidth and garage with inside the community. Events in a WSN are detected through units of space-scattered sensors that paint collectively to make decisions. One manner is to catch up on pre-transmission information to lessen energy, as a few losses may be normal without affecting utility results. Data gathered from sensors which might be too near show spatial correlation. If the samples gathered over the years are from the equal source / sources, the information additionally display a time correlation. As with information garage schemes, there are 3 schemes for processing information. Simple and correlated information may be processed in nodes (nearby processing). Some statistical values (as an instance: mean, maximum) or occasion detection may be acquired from interoperability (in-community processing). Complicated information ought to be

processed on state-of-the-art machines (outside processing). The first schemes (nearby and in-community processing) are normally used for information discount. External processing is especially used for visible presentation of information and for functions of information meaning [19] [20] [21] [22].

Local: The most important cause of processing information in a node is to lessen the quantity of information that desires to be saved with inside the node and as a way to be transmitted over the community to the sink node. The electricity saving is proportional to the quantity of jumps that the information passes thru the community. Data processing takes numerous forms: as an instance it could be used to do away with noise from measured values, extract statistics from information or compress information. One information compression set of rules on the sensor node is S-LZW, which makes use of the sphere of sensor information traits to lessen energy intake through greater than 1. five instances in addition to different information alterations that take gain of the information shape to lessen grid energy intake through a median of 2. five instances. Thus, financial savings are supplied each with inside the sensor node and with inside the entire community. There are compression strategies for lowering historic statistics in sensor networks. Here, correlation and redundancies among a couple of measurements at the equal sensor are applied and an excessive diploma of information discount is performed through coping with even the smallest information of recorded measurements. This approach is predicated on the concept that the values of the aggregated measurements showcase similarities over the years [17].

In network: This processing is often referred to as data collection and is one of the most common ways to reduce communication costs. This technique tries to make the most of the correlations of the data in order to minimize their size and hence the communication cost. Besides the fact that sensor nodes are resource-constrained devices, multiple nodes working together can generate significant computing power. Because the nature of WSNs encourages nodes to collaborate, distributed algorithms are more widely used, providing ways of eliminating data redundancy in a dense, fully distributed WSN. Collaboration enables highly efficient compression across sensor networks without establishing communication between nodes, using fast and well-researched cryptographic algorithms for error correction. In some application situations, the information of interest is presented not in an individual sensor node, but in statistics that aggregate information between a sensor. In Geographic Gossip, they

present sums such as average, max/min or count while reducing power consumption. Instead of the ability to reduce the number of bits transmitted, in a wide range of application scenarios the end user is not interested in the full historical data of the sensor network, but in the detection of specific events. certain. (E.g., trigger an alarm) or in a precise view of the observed phenomenon (e.g., maximum temperature in the monitored area). Network processing is concerned with the storage and forwarding of message processing, where a message is a meaningful unit of data that a node can process. At each node in the sensor network, an internal network processing layer is responsible for managing incoming messages, processing them, and deciding what other messages to send [17].

External: For intensive data processing, it is more efficient to process the data in a sophisticated machine where it is collected, analyzed and presented. Also, data processing on nodes often takes longer than on high-volume machines, so for real-time applications external data processing is preferred. Clearly, data analysis and visual presentation make data more accessible to users [15] [16].

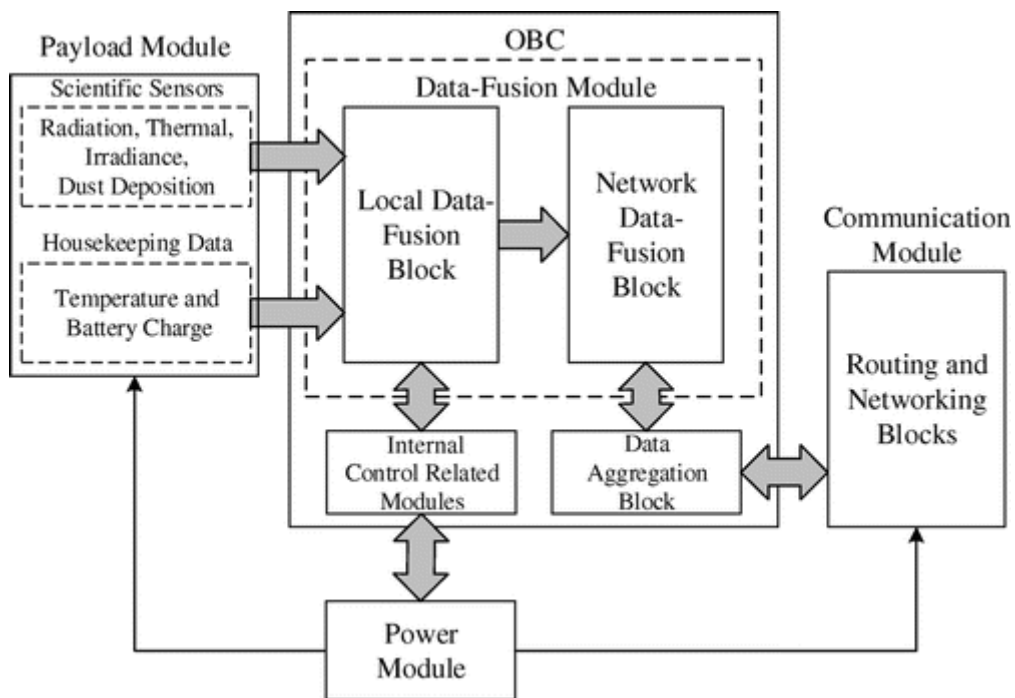


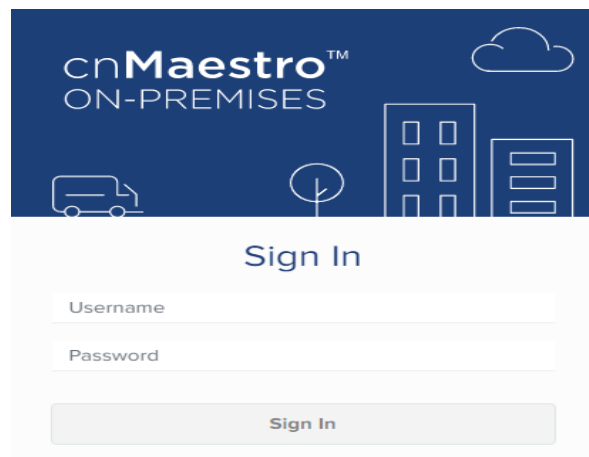
Figure 7. Shows data processing model.

CHAPTER 3

METHODOLOGY

In this chapter we will discuss how to have end-to-end network control using cnMaestro. cnMaestro is a software platform which provides us secure end-to-end network control. cnMaestro is a wireless network manager that simplifies real device management by offering full network visibility and zero touch provisioning. The possibilities to manage and collect the data of so many nodes at the same time without being physically on site, makes this software a very good one to be used in big ISP companies.

In order to use cnMaestro we need to configure it on a Linux server. Which can be accessible from our network. After the configuration is made we open our software Ip on a web inside our network and log in with the user and password that was created for us.



The image shows a web interface for 'cnMaestro ON-PREMISES'. The top section is a dark blue header with the logo and several white icons: a truck, a tree, and two buildings. Below the header is a white sign-in form. The form has a title 'Sign In' in blue. It contains two input fields: 'Username' and 'Password'. Below the fields is a grey button with the text 'Sign In'.

Figure 8. Sign in page.

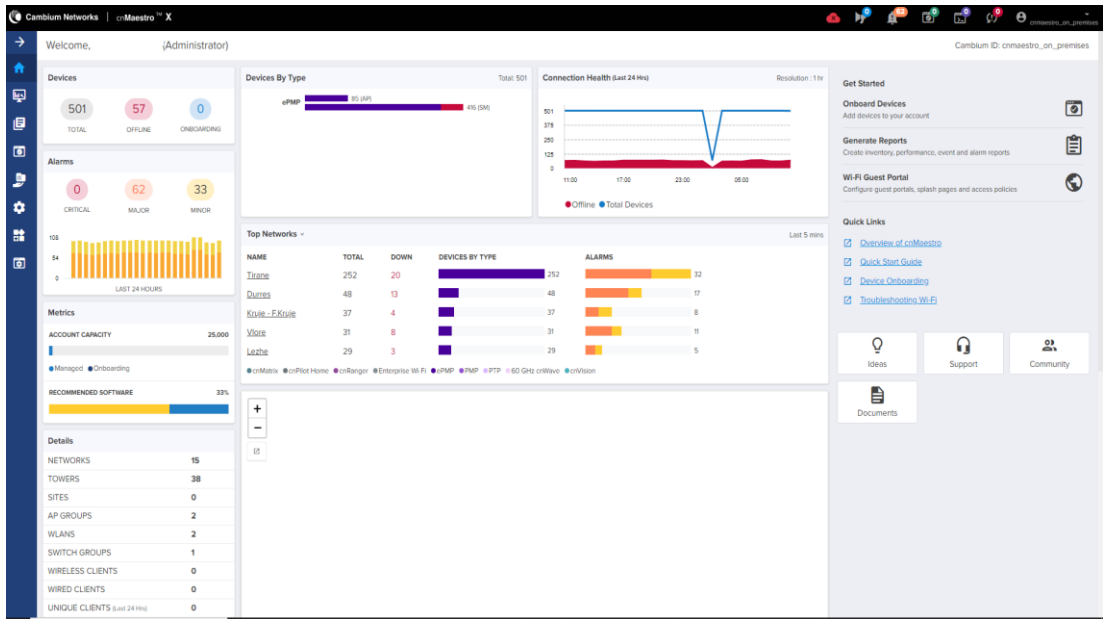


Figure 9. cnMaestro main page.

After we have signed in we can add or remove any device that we desire.

Let's suppose our field engineer just did the installation of an antenna (access point) with a specific IP and a strong signal towards our node and we want to control it through our software.

First, we search the Ip of our access point on web. and after we log in on our device, we go to configuration then system and scroll down to remote management where we will put our server's IP. Here we will enable the remote management and at cnMaestro URL we put the Ip of our software. Now we can log out our access point because it has sent a notification asking for approval to be managed from cnMaestro.

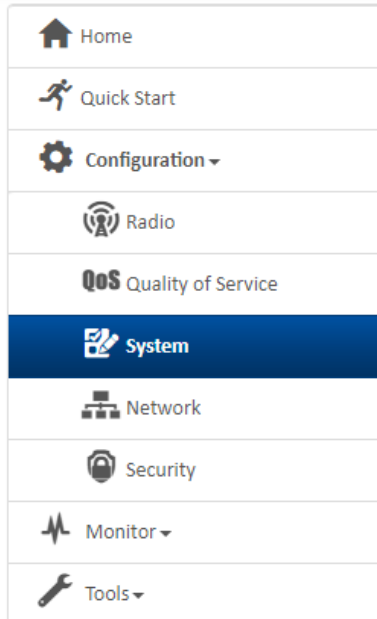


Figure 10. Access point menu.

Remote Management Disabled Enabled

192.168.101.151

.....

Figure 11. Enabling remote management.

IP Address	Added By	Status	Duration	Configure	
192.168.127.7	- Unsolicited	Waiting for Approval	< 1m	<input type="button" value="Configure"/> <input type="button" value="Refresh"/> <input type="button" value="Download"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Approve"/> <input type="button" value="Delete"/>

Figure 12. Approval of new device.

After we give the approval of our new device it will show itself at the monitor and manager of networks. Our access point will be part of the default network ready for us to send it to the it's respective place.

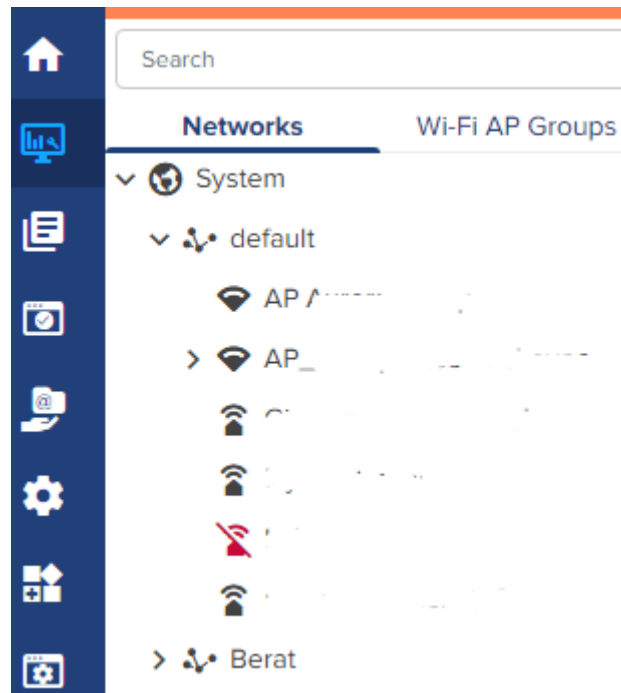


Figure 13. Monitor and manager.

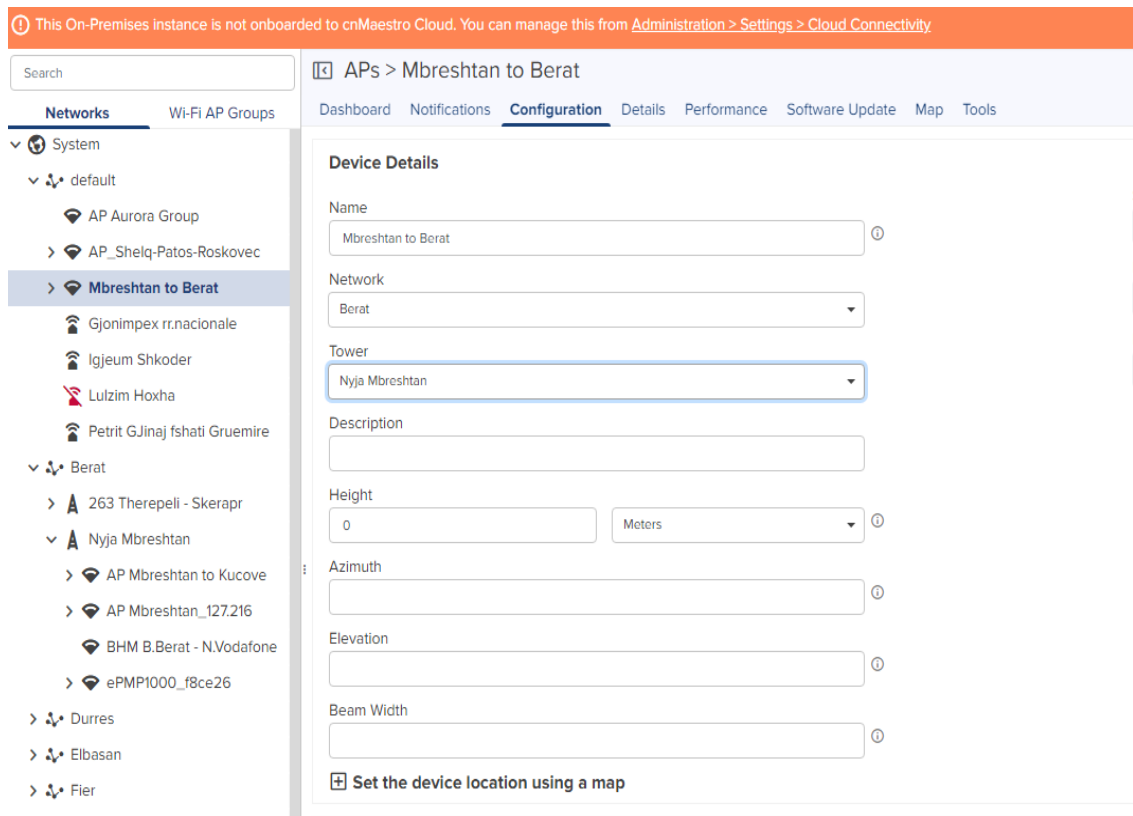


Figure 14. Device Configuration menu.

After we click on our device it will pop up the menu of the device, we need to go to configuration. Where we can change the original name of our device, put it on another network and what tower it is connected to. We can make a description of it and even put the height of its installation. Putting the coordinates can help us identify how far away is the access point from the node.

Dashboard is used to see how many children(devices) are connected to the Access Point, as well as the product name, mac address, IP, software, serial number, description. We can check the throughput of the last hour as well.

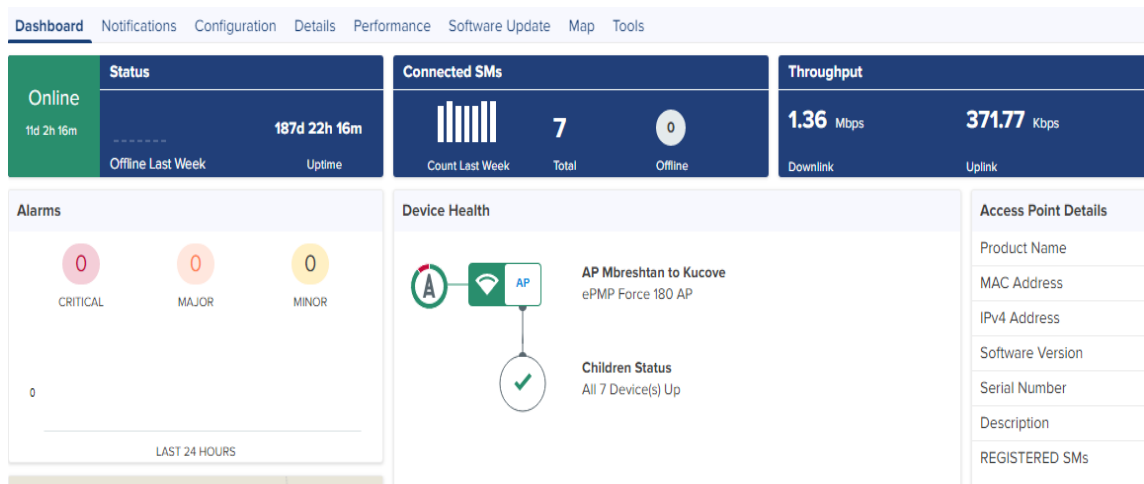


Figure 15. Dashboard of the device

Performance page senses and puts us on a graph of all the output, input, linked devices and lost signal. So, we can have a better understanding of what exactly is happening with our antenna.

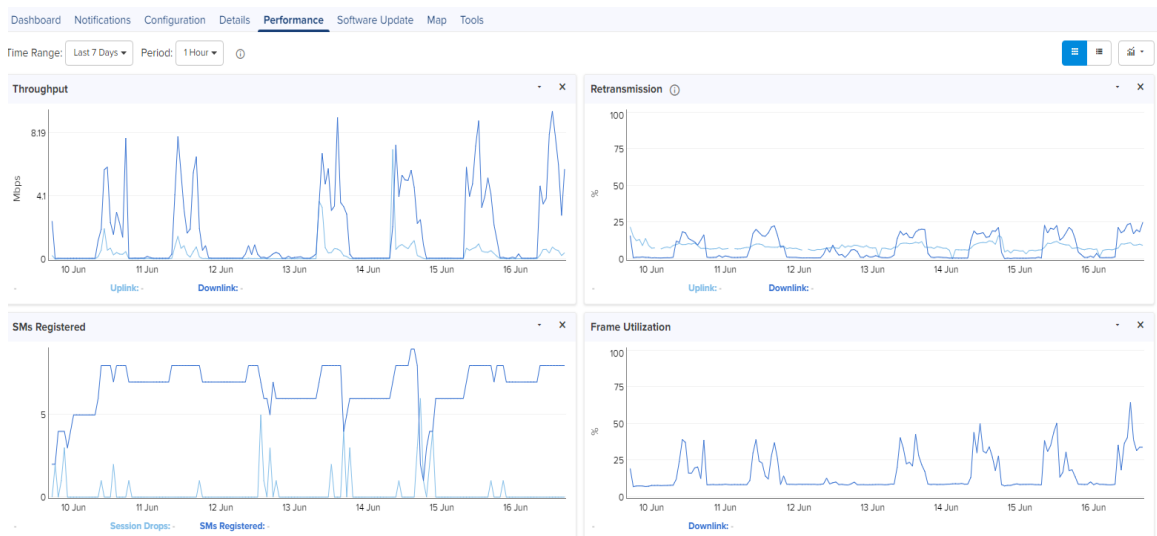


Figure 16. Performance graphs of Access point.

Another very interesting feature of cnMaestro is the tools section. Here you can make different tests to check the status of your device or communicate with other devices to see if the link is stable. Here as you can see we ping our device to a neighbor device to see if we have any losses(fig.17).

Dashboard Notifications Configuration Details Performance Software Update Map **Tools**

Status Debug **Network Connectivity** Subscriber Modules Link Test eDetect

Test Type
Ping Network ping to a hostname or IP address.

IP Address or Hostname
192.168.1.100

Number of Packets (-c)
3 Min = 1, Max = 10

Buffer Size (-s)
56 Min = 1, Max = 65507

Start Ping

Ping Result
Complete
Hostname 192.168.1.100

```

PING 192.168.145.211 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=63 time=33.5 ms
64 bytes from 192.168.145.211: icmp_seq=2 ttl=63 time=15.9 ms
64 bytes from 192.168.145.211: icmp_seq=3 ttl=63 time=33.5 ms

--- 192.168.145.211 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 15.951/27.660/33.528/8.279 ms

```

Figure 17. Ping test to another access point.

Other tests that can be executed are:

- Log tests to check on the reason for any failure.
- The Link Capacity Test measures the throughput of the RF link between two ePMP/cnVision modules. The device’s link test only utilizes the spare sector capacity for this test, therefore, sector traffic will not be disrupted. For the most accurate wireless link test results, it is best to run this test when there is no or very little customer data traffic being sent for the duration of the test.
- eDetect will scan and detect 802.11 ePMP AP and its ePMP SM on the current channel. It will process frames received from 802.11 interferers including other ePMPs not in its own sector and display the MAC Address, RSSI and MCS of the interfering.

Nodes(towers)

Here we can see the tower and all the devices with their information. Any information that is needed from any access point shows in the dashboard on our tower. Any error, connection made and even location of the access point in the real world. For every device we add that connects to an access point it will automatically show at the dashboard of our tower on the access point that it is connected.

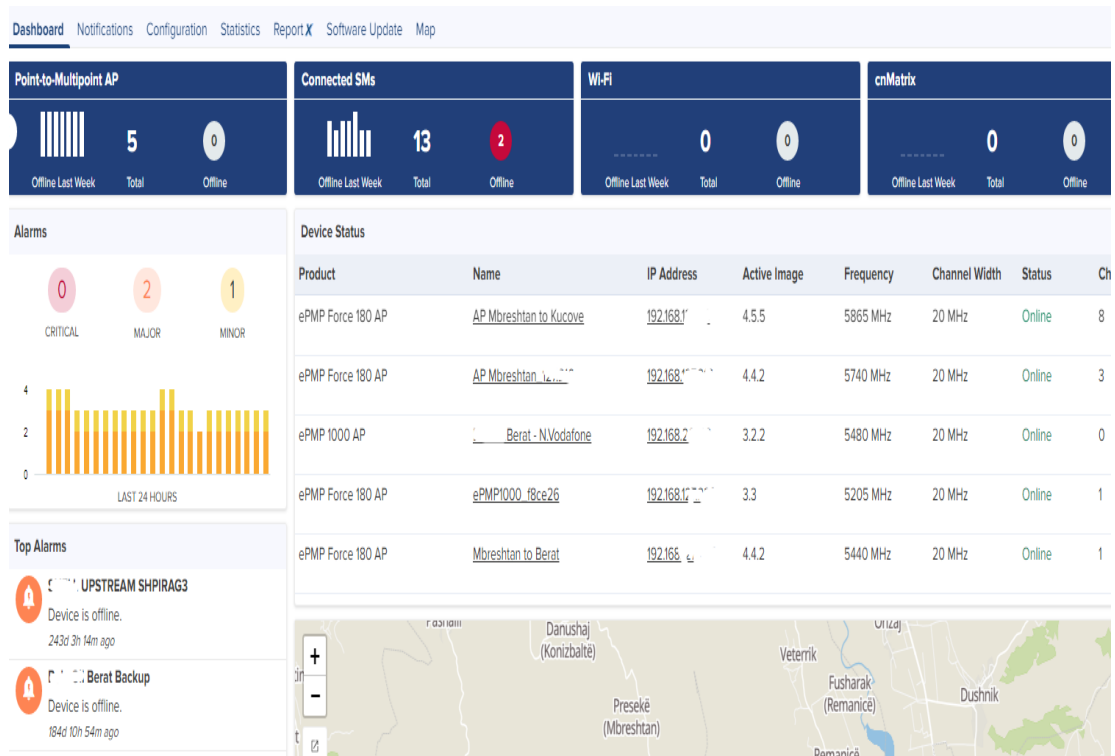


Figure 18. Dashboard of tower.

CHAPTER 4

RESULTS AND DISCUSSIONS

Here we can say that sensor nodes are generally made up of a variety of sensor types that are used to sample physical events. In addition to standard processing capabilities, these nodes include communication and sensing capabilities that are superior to traditional sensors. Sensor nodes are capable of not only measuring physical occurrences, but also of processing, storing, and disseminating measurement data.

There are distinct distinctions between a WSN and a standard database system that must be considered when developing the query sublayer in order to achieve effective data management. Some of these distinctions include: Data flow tracking - When a

query is received, WSN reacts by providing data at specified time intervals, unlike a database.

Communication faults - While data collected from database responses is totally trustworthy, data created by sensor nodes is sent to the sink node via multi-hop communication, which might be faulty and impacted by mistakes. This implies the data arrives at the sink node with a wide range of latency and dependability.

Real-time processing - Because processing processes consume several orders of magnitude more energy than other operations, real-time processing is essential.

Here we use a cloud-based or on-premises software platform called cnMaestro that allows safe end-to-end network control. Which provides complete network visibility and zero touch provisioning, the program's wireless network manager makes it easier to manage devices. A complete set of wireless network management operations may be viewed and executed in real time. Increase throughput, improve system uptime, and address new demands from commercial and residential users.

We are able to put a map of all our nodes with their access points. And divide them in different cities and networks, creating a spider web which can help us identify and fix faster if there can be any need for troubleshooting in case any of our clients will need support on finding a solution for any kind of problem that might occur.

cnMaestro helps us to fully control and configure any device that is remotely accessible from the software and keep them virtually in the same order that they are linked physically.

Each access point will have under itself automatically all the devices that are connected to it. From where we can do all the configuration we need.

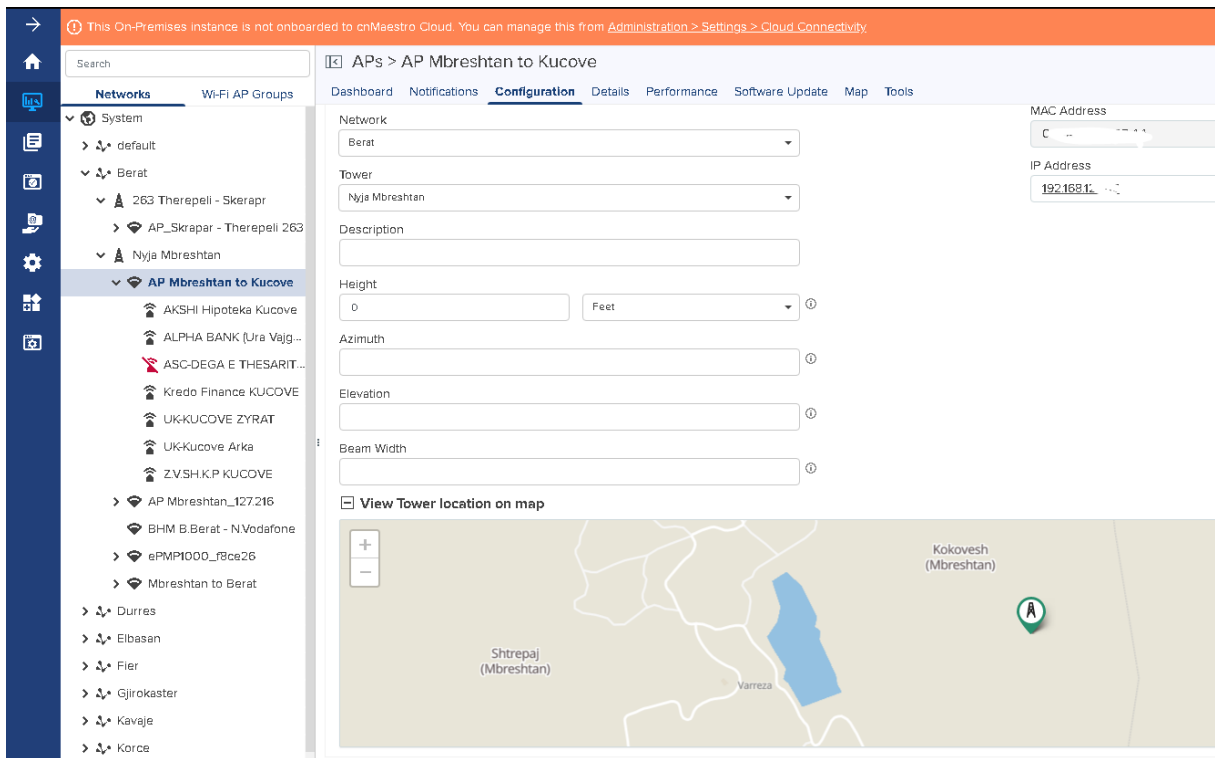


Figure 19. Menu of configuration and location.

In the figure above we can configure our device's name, network, tower it is connected to without being connected directly to it. We can also put the height in meters that it is installed in meters (0 to 500) or feet (0 to 1640). Its azimuth are the degrees from north (0 to 360), elevation which is the degrees from horizon (-90 to 90) and beam width which degrees go from 1 to 360. Here we can see the real location of the device on map and have a better understanding where it is physically.

All this information helps us put together the spider-net we create with all our Antennas. In any casualty that might happen knowing the exact position of each of our towers helps us to define what other towers will be affected or if some engineers happen to be working close to another tower our system will help us to determine the time needed to go from one tower to the other and fix the problem as soon as possible. Even in case of any injury of our staff we can give the exact coordinates and send the medical team as soon as possible knowing every detail like the height of the place, location and the terrain. In other words, everything that can be done physically connected to the access point we can do it from our software. Which reduced the cost and effort that would be needed if this system wouldn't exist.

1. Main Result

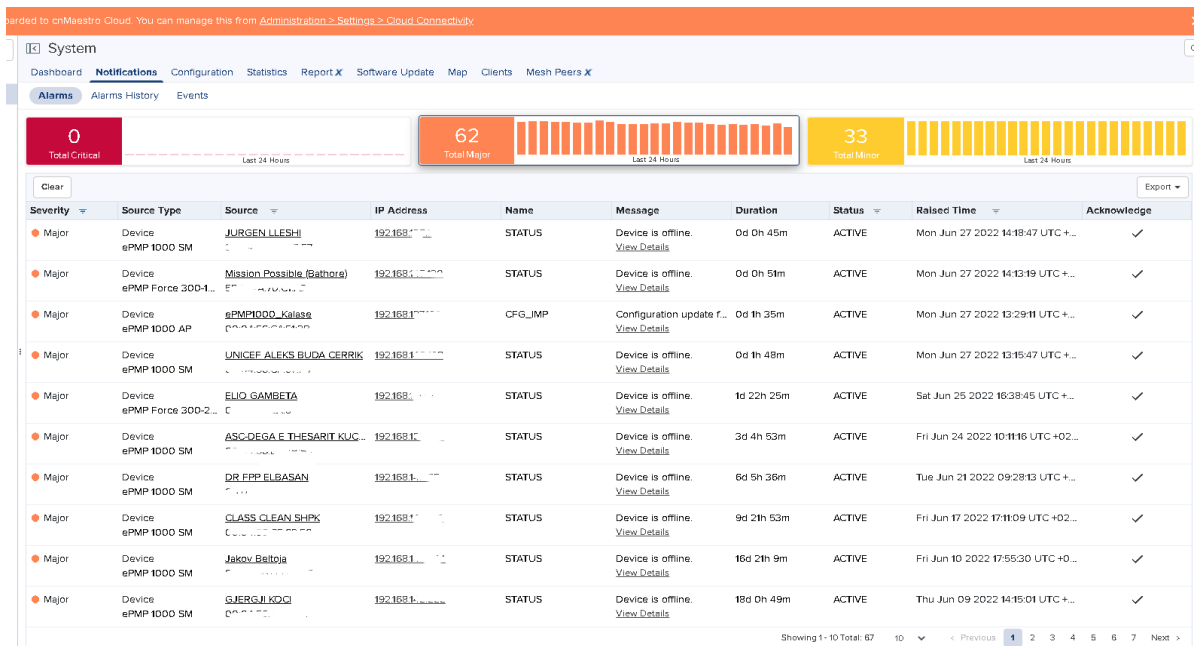


Figure 20. Alarms.

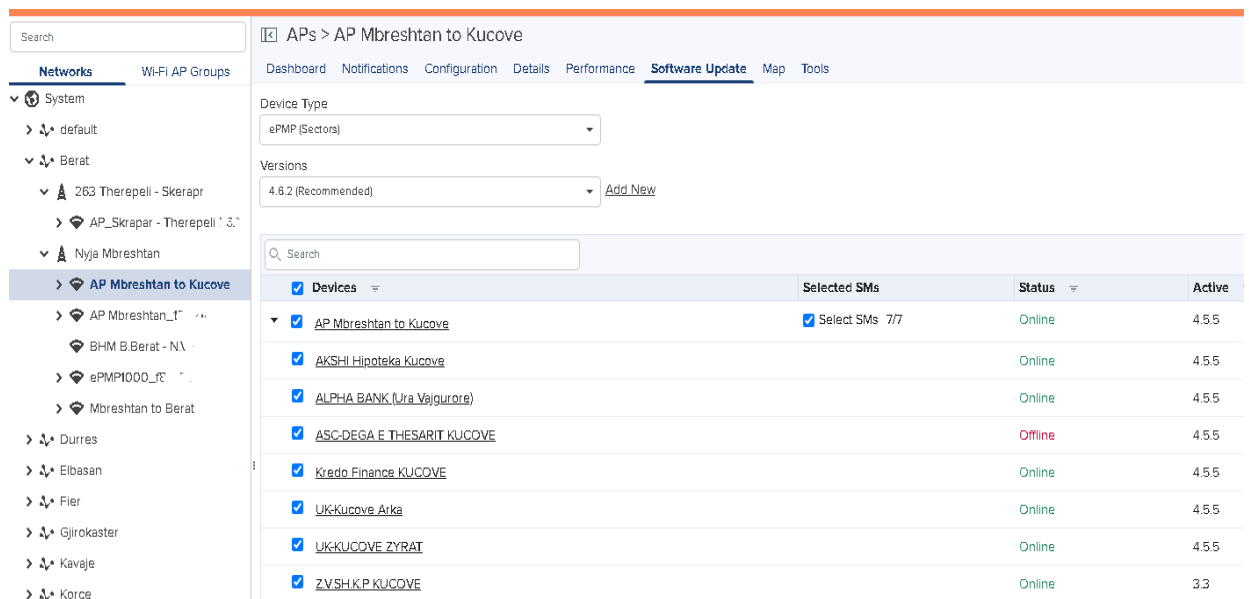
On our tests we saw how our system behaves when a device is disconnected for different reasons like: bad signal, device freeze, software upgrade problems or power failure. On the menu of alarms, we can see every alarm caused which divides into three groups.

Most common group is the minor alarms which include the devices with less connected users, those alarms are triggered when the device's GPS firmware is out of date. Our system tells us the exact time and date this has happened and the status it is currently. When the device is up it will show the status it currently has.

Major alarms are the ones that will tell us about disconnected devices most of these alarms come from power failure of our devices. This may happen for different reasons, such as: client shuts down the electric power, power supply unit will fail due to overheating or tension or device reboot.

Our system tells us the exact time and date it is disconnected and the status it is currently, even giving us information about the reason for disconnection. When the device is up it will show the status it currently has. Major alarms usually are caused when a tower has any issue but these alarms most likely never happen.

2. Software Update.



The screenshot shows a web-based network management interface. On the left is a navigation menu with categories like 'System', 'Berat', and 'Nyja Mbreshtan'. The main area is titled 'APs > AP Mbreshtan to Kucove' and has tabs for 'Dashboard', 'Notifications', 'Configuration', 'Details', 'Performance', 'Software Update', 'Map', and 'Tools'. The 'Software Update' tab is active, showing a 'Device Type' dropdown set to 'ePMP (Sectors)' and a 'Versions' dropdown set to '4.6.2 (Recommended)'. Below this is a search bar and a table of devices. The table has columns for 'Devices', 'Selected SMS', 'Status', and 'Active'. The 'Devices' column has checkboxes for each device, and the 'Selected SMS' column shows 'Select SMS: 7/7' for the first device. The 'Status' column shows 'Online' for most devices and 'Offline' for 'ASC-DEGA E THESARIT KUCOVE'. The 'Active' column shows version numbers like 4.5.5 and 3.3.

Devices	Selected SMS	Status	Active
<input checked="" type="checkbox"/> AP Mbreshtan to Kucove	<input checked="" type="checkbox"/> Select SMS: 7/7	Online	4.5.5
<input checked="" type="checkbox"/> AKSHI Hipoteka Kucove		Online	4.5.5
<input checked="" type="checkbox"/> ALPHA BANK (Ura Vajguore)		Online	4.5.5
<input checked="" type="checkbox"/> ASC-DEGA E THESARIT KUCOVE		Offline	4.5.5
<input checked="" type="checkbox"/> Kreda Finance KUCOVE		Online	4.5.5
<input checked="" type="checkbox"/> UK-Kucove Arka		Online	4.5.5
<input checked="" type="checkbox"/> UK-KUCOVE ZYRAT		Online	4.5.5
<input checked="" type="checkbox"/> ZVSH.K.P KUCOVE		Online	3.3

Figure 21. Software Upgrade menu.

Every device needs an upgrade from time to time. When we need to upgrade any of our access points, we will go under the software upgrade menu as shown in fig.21 and click on add new version. After that we will need to select the access point with all the clients that are connected to it. If we let any of the devices connected to our access point with an older software it might disconnect from our main antenna and will be needed to go and connected directly to our clients' devices to perform the software upgrade so we can have the device connected to the access point and accessible from cnMaestro. Therefore, in simple words every time we perform a software upgrade, we need to upgrade not only our access point but also every device that is connected to it.

1. Troubleshooting Tools

On the tools menu we are able to perform different types of tests and troubleshooting. First is the status of the device. It will show us if the device is online

or offline. In case it is not connected to the access point it will cause a major alarm telling us the reason it is not connected.

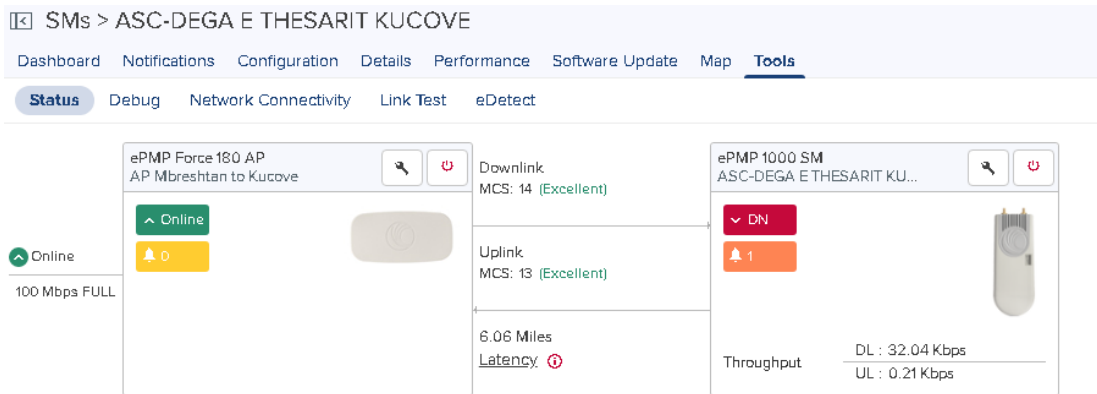


Figure 22. Status of the device.

The second one is the debug. Here we can see all the logs that are done to this device.

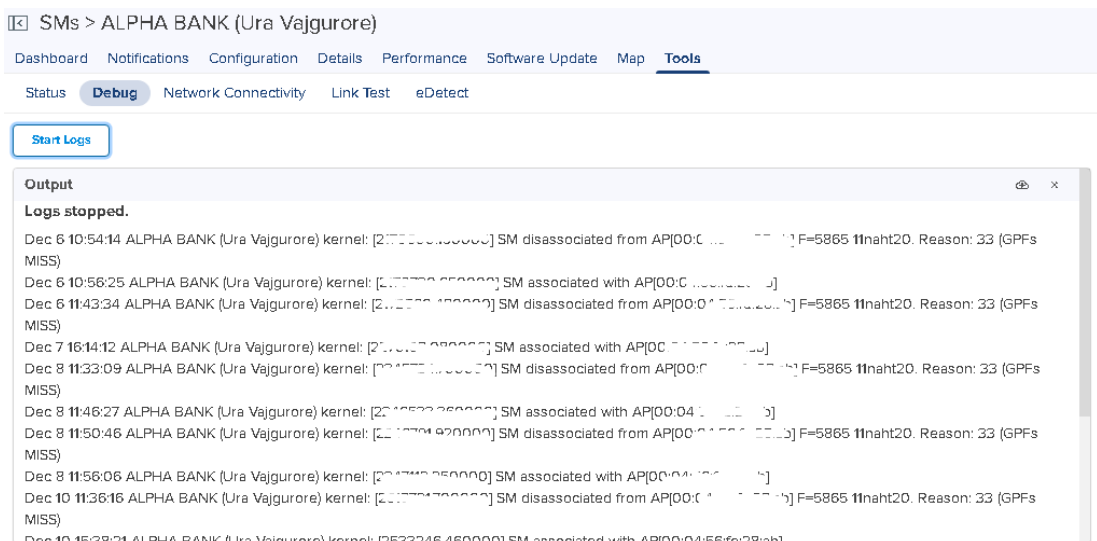


Figure 23. Logs checker.

Third is Network connectivity. Here as you can see on fig.17, we transfer packages from our device to a neighbor device to see if we have any losses.

Link test is another interesting feature we can use. It helps us detect if the link between our access point and the device installed at the client is unstable and needs improvement(fig.24). Feature sends a 128, 800 or 1500 bytes packet during the interval we choose and after the interval it will give us the results which show us the downlink

capacity and uplink capacity. The links that are better usually are the ones with less traffic which makes them perform better.

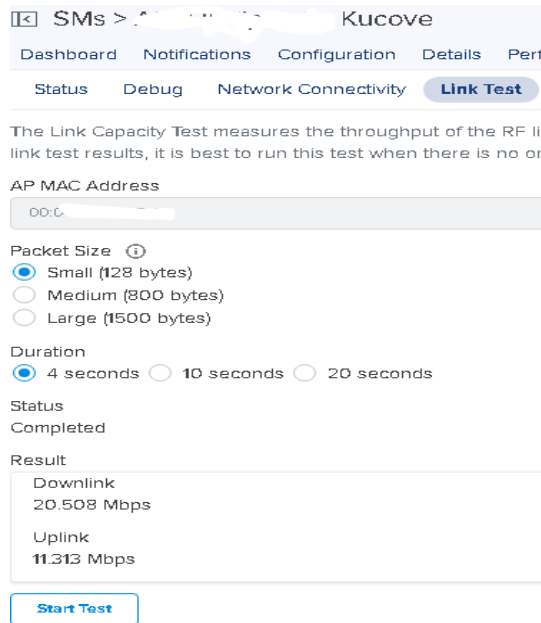


Figure 24. Link test tool.

Device	IP Address	Status	Frequency	Bandwidth	DL/UL Ratio	Max Range	DFS Status	Throughput (UL)	Throughput (DL)	Registered SMs
AP Mbreshtan to Kucove	192.168.1.1	Online	5885 MHz	20 MHz	Flexible	20 Miles	N/A	23.83 Kbps	56.37 Kbps	6
AP Mbreshtan to Kucove	192.168.1.2	Online	5740 MHz	20 MHz	Flexible	20 Miles	N/A	87.4 Kbps	2.31 Mbps	3
BHM B.Berat - N.Vodafone	192.168.1.3	Online	5480 MHz	20 MHz	Flexible	15 Miles	N/A			0
ePMP1000_f...	192.168.1.4	Online	5205 MHz	20 MHz	Flexible	20 Miles	N/A			0
Mbreshtan to Berat	192.168.1.5	Online	5440 MHz	20 MHz	Flexible	20 Miles	N/A	0.34 Kbps	35.6 Kbps	1

Figure 25. Node statistics showing us all the access points connected to it.

From the information that ncMaestro gives us we can clearly see that our access points operate on similar frequencies with a bandwidth of 20Mhz.

This type of frequencies are used in Europe to maximize the range of the antennas without losing the performance and not harming the environment.

On **figure 26** are shown to us four different graphs any device we select goes through the week. On the first graph we have the traffic that goes throughout the week, download and upload at any time we need to measure (all in mbps).

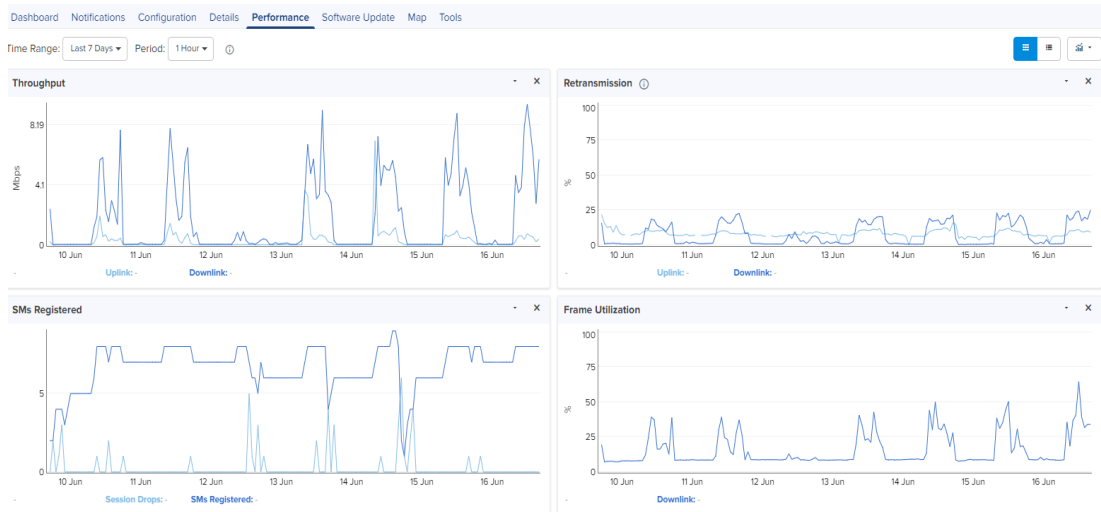


Figure 26. Performance Graphs

The second graph shows us the retransmission in percentage, this graph will give us the uplink retransmission after 24 hours or more. The SMs registered graph gives us the number of devices connected to our access point. Making it easier for us to detect when a client is turning off their device. And last, we have the frame utilization graph also in percentage. From our graphs we can see that devices and traffic behave the same on the same days of each week. And most of our traffic is done from 7.00am to 4.00pm. From this we can say that people behave on this Monday the same as they behaved on last Monday and so on the other days. And having the need to use their devices (Antennas) during their work hours because most of the clients that cannot have a fiber connection live in rural zones where the infrastructure is not yet developed for fiber technologies.

CHAPTER 5

CONCLUSIONS

5.1 Conclusions

In conclusion we can say that wireless sensors are different from traditional wireless connection because not only they let us fully control them without being directly connected to them but help us gather information on the health, downlink and uplink, different attacks that might occur and minimize the need to use men power visiting the site.

Sensor nodes are generally made up of a variety of sensor types that are used to sample physical events. wireless sensor nodes do not need to communicate directly with the nearest base station, they only communicate with the local node. Instead of relying on a predefined infrastructure, each sensor independently participates in infrastructure-wide decisions.

On our software we are able to see how we can create a spider net and have our business running on the requirements that our clients have. Support in real time for any disruption of their network. Verification of the problem through troubleshooting using cnMaestro. Logging on clients' devices and testing the link capacity, going through logs and even helping on improving the signal of client's device to the access point.

We put a map of all our nodes with their access points to work. And divide them in different cities and networks, which helps us identify and fix the problem faster if there is any need to interfere. We saw how on each week on Monday's people behave similarly. Same goes on Tuesdays, each Tuesday has almost the same traffic as the previous one and so on with the other days of the week. The fact that most of the clients are businesses gives us another result on which we saw that most of their traffic would be from 7.00 am to 4.00 pm. After 4.00 pm their traffic would go down or the devices

would be switched off. We can add the fact that most wireless connected links are in rural areas, where there is no fiber infrastructure.

cnMaestro helps us to fully control and configure any device that is remotely accessible from the software and keep them virtually in the same order that they are linked physically. Just like our software there are other cloud-based applications who evolve each day, making our lives easier. And the possibilities with 5G and the future technologies will make everything even easier and wireless sensors are and will be the key to putting physically together and running every bit of our technologies.

In the end we can say that our technologies are evolving constantly giving us new opportunities every day to achieve the impossible. This pushes us all forward to learning and breaking the barriers we put ourselves.

REFERENCES

- [1] Z. Rehena, S. Roy and N. Mukherjee, "A modified SPIN for wireless sensor networks," in *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, Bangalore, 2011.
- [2] S. Pandey and P. Pal, "Spin-MI: Energy Saving Routing Algorithm Based on SPIN Protocol in WSN," *National Academy Science Letters*, vol. 37, no. 4, pp. 335-339, 2014.
- [3] A. Althoubi, R. Alshahrani and H. Peyravi, "Delay Analysis in IoT Sensor Networks," *Sensors*, vol. 21, no. 11, p. 3876, 2021.
- [4] N. Amini, A. Vahdatpour, W. Xu, M. Gerla and M. Sarrafzadeh, "Cluster size optimization in sensor networks with decentralized cluster-based protocols," *Computer Communications*, vol. 35, no. 2, pp. 207-220, 2012.
- [5] A. R. Sankaliya, "PEGASIS : Power-Efficient Gathering in Sensor Information Systems," *IJSRST*, vol. 1, no. 5, pp. 2395-6011, 2015.
- [6] J. Grover, S. Shikha and M. Sharma, "A Study of Geographic Adaptive Fidelity Routing Protocol in Wireless Sensor Network," *IOSR Journal of Computer Engineering*, vol. 16, no. 5, pp. 88-96, 2014.
- [7] A. Awad, A. Mitschele-Thiel and F. Dressler, "Reactive Virtual Position-Based Routing in Wireless Sensor Networks," in *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, Lahaina, Hawaii, 2011.
- [8] G. Jesus, A. Casimiro and A. Oliveira, "A Survey on Data Quality for Dependable Monitoring in Wireless Sensor Networks," *Sensors*, vol. 17, no. 9, p. 2010, 2017.
- [9] J. Wang, Z. Zhang, F. Xia, W. Yuan and S. Lee, "An Energy Efficient Stable Election-Based Routing Algorithm for Wireless Sensor Networks," *Sensors*, vol. 13, no. 11, pp. 14301-14320, 2013.

- [10] F. Khan and S. K. Nguang, "Distributed localization algorithm for wireless sensor networks using range lookup and subregion stitching," *IET Wireless Sensor Systems*, vol. 11, no. 5, pp. 179-205, 2021.
- [11] A. Rao, C. Papadimitriou, S. Shenker and I. Stoica, "Geographic routing without location information," in *ACM Press*, New York, 2003.
- [12] J. Capella, J. Campelo, A. Bonastre and R. Ors, "A Reference Model for Monitoring IoT WSN-Based Applications," *Sensors*, vol. 16, no. 11, p. 1816, 2016.
- [13] D. J. Lee and B. Stvilia, "Practices of research data curation in institutional repositories: A qualitative view from repository staff," *PLOS ONE*, vol. 12, no. 3, p. e0173987, 2017.
- [14] N. A. Pantazis, S. A. Nikolidakis and D. D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 551-591, 2013.
- [15] A. Dâmaso, N. Rosa and P. Maciel, "Reliability of Wireless Sensor Networks," *Sensors*, vol. 14, no. 9, pp. 15760-15785, 2014.
- [16] S. Sarmady, "A Survey on Peer-to-Peer and DHT," *Sensor*, 2010.
- [17] M. H. Anisi, A. H. Abdullah, S. A. Razak and M. A. Ngadi, "Overview of Data Routing Approaches for Wireless Sensor Networks," *Sensors*, vol. 12, no. 4, pp. 3964-3996, 2012.
- [18] G. S. Manku, "Routing networks for distributed hash tables," in *Proceedings of the twenty-second annual symposium on Principles of distributed computing - PODC '03*, New York, New York, USA, 2003.
- [19] A. I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.
- [20] S. Bader and B. Oelmann, "Adaptive synchronization for duty-cycling in environmental wireless sensor networks," in *2009 International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, Sundsvall: Mittuniversitetet, 2009.
- [21] V. Naresh and N. Lee, "A Review on Biosensors and Recent Development of Nanostructured Materials-Enabled Biosensors," *Sensors*, vol. 21, no. 4, p. 35, 2021.

- [22] A.-B. Garcia-Hernando, J.-F. Martinez-Ortega, M. Lopez-Navarro, A. Prayati and L. Redondo-Lopez, *Problem Solving for Wireless Sensor Networks*, Berlin: Springer, 2008.
- [23] N. Srivastava, "Challenges of Next-Generation Wireless Sensor Networks and its impact on Society," *Journal of Telecommunications*, vol. 1, no. 1, pp. 128-133, 2010.
- [24] J. C. Cuevas-Martinez, M. A. Gadeo-Martos, J. A. Fernandez-Prieto, J. Canada-Bago and A. J. Yuste-Delgado, "Wireless Intelligent Sensors Management Application Protocol-WISMAP," *Sensors*, vol. 10, no. 10, pp. 8827-8849, 2010.
- [25] O. Gurewitz, M. Shifrin and E. Dvir, "Data Gathering Techniques in WSN: A Cross-Layer View," *Sensors*, vol. 22, no. 7, p. 2650, 2022.
- [26] J. Jones and M. Atiquzzaman, "Transport Protocols for Wireless Sensor Networks: State-of-the-Art and Future Directions," *International Journal of Distributed Sensor Networks*, vol. 3, no. 1, pp. 119-133, 2007.
- [27] L. K. Ketshabetswe, A. M. Zungeru, M. Mangwala, J. M. Chuma and B. Sigweni, "Communication protocols for wireless sensor networks: A survey and comparison," *Heliyon*, vol. 5, no. 5, p. 1591, 2019.
- [28] Y.-C. Wang, F.-J. Wu and Y.-C. Tseng, "Mobility management algorithms and applications for mobile sensor networks," *Wireless Communications and Mobile Computing*, vol. 12, no. 1, pp. 7-21, 2012.
- [29] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1-25, 2017.
- [30] A. Cortés-Leal, C. Del-Valle-Soto, C. Cardenas, L. J. Valdivia and J. A. Del Puerto-Flores, "Performance Metric Analysis for a Jamming Detection Mechanism under Collaborative and Cooperative Schemes in Industrial Wireless Sensor Networks," *Sensors*, vol. 22, no. 1, p. 178, 2021.
- [31] L. N., S. M. S. and S. R. K., "Trade-off between Accuracy and Longevity in Wireless Sensor Networks," *International Journal of Computer Theory and Engineering*, vol. 7, no. 3, pp. 223-230, 2015.

- [32] Y. Liu, J. Pu, S. Zhang, Y. Liu and Z. Xiong, "A Localized Coverage Preserving Protocol for Wireless Sensor Networks," *Sensors*, vol. 9, no. 1, pp. 281-302, 2009.
- [33] D. Ye, D. Gong and W. Wang, "Application of wireless sensor networks in environmental monitoring," in *2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS)*, Shenzhen, 2009.
- [34] M. Lazarescu, "Design and Field Test of a WSN Platform Prototype for Long-Term Environmental Monitoring," *Sensors*, vol. 15, no. 4, pp. 9481-9518, 2015.
- [35] S. Ahmad Salehi, M. Razzaque, P. Naraei and A. Farrokhtala, "Security in Wireless Sensor Networks: Issues and challenges," in *2013 IEEE International Conference on Space Science and Communication (IconSpace)*, Melaka, 2013.
- [36] M. S. Kordafshari, A. Pourkabirian, K. Faez and A. M. Rahimabadi, "Energy-Efficient SPEED Routing Protocol for Wireless Sensor Networks," in *2009, Venice/Mestre, 2009 Fifth Advanced International Conference on Telecommunications*.
- [37] Q. Mamun, "A Qualitative Comparison of Different Logical Topologies for Wireless Sensor Networks," *Sensors*, vol. 12, no. 11, pp. 14887-14913, 2012.
- [38] P. S. Rathore, J. M. Chatterjee, A. Kumar and R. Sujatha, "Energy-efficient cluster head selection through relay approach for WSN," *The Journal of Supercomputing*, vol. 77, no. 7, pp. 7649-7675, 2021.
- [39] J. Sen, "Security and Privacy Challenges in Cognitive Wireless Sensor Networks," in *Cognitive Radio Technology Applications for Wireless and Mobile Ad Hoc Networks*, Mumbai, igi global, 2013, pp. 194-232.
- [40] S. Karthik and D. A. A. Kumar, "Challenges of Wireless Sensor Networks and Issues associated with Time Synchronization," in *UGC sponsored national conference on advanced networking and applications*, Udumalpet, 2015.
- [41] F. Losilla, A.-J. Garcia-Sanchez, F. Garcia-Sanchez, J. Garcia-Haro and Z. J. Haas, "A Comprehensive Approach to WSN-Based ITS Applications: A Survey," *Sensors*, vol. 11, no. 11, pp. 10220-10265, 2011.
- [42] G. Terrasson, R. Briand, S. Basrou, V. Dupé and O. Arrijuria, "Energy Model for the Design of Ultra-Low Power Nodes for Wireless Sensor Networks," *Procedia Chemistry*, vol. 1, no. 1, pp. 1195-1198, 2009.

- [43] C. Buratti, A. Conti, D. Dardari and R. Verdone, "An Overview on Wireless Sensor Networks Technology and Evolution," *Sensors*, vol. 9, no. 9, pp. 6869-6896, 2009.
- [44] E. Karapistoli, I. Mampentzidou and A. A. Economides, "Environmental Monitoring Based on the Wireless Sensor Networking Technology," *International Journal of Agricultural and Environmental Information Systems*, vol. 5, no. 4, pp. 1-39, 2014.
- [45] M. Ndiaye, G. Hancke and A. Abu-Mahfouz, "Software Defined Networking for Improved Wireless Sensor Network Management: A Survey," *Sensors*, vol. 17, no. 5, p. 1031, 2017.
- [46] J. Hwang, C. Shin and H. Yoe, "Study on an Agricultural Environment Monitoring Server System using Wireless Sensor Networks," *Sensors*, vol. 10, no. 12, pp. 11189-11211, 2010.
- [47] L. Ruiz-Garcia, L. Lunadei, P. Barreiro and I. Robla, "A Review of Wireless Sensor Technologies and Applications in Agriculture and Food Industry: State of the Art and Current Trends," *Sensors*, vol. 9, no. 6, pp. 4728-4750, 2009.
- [48] P. Kumar and H.-J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," *Sensors*, vol. 12, no. 1, pp. 55-91, 2011.
- [49] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications - WSNA '02*, Berkeley, 2002.
- [50] D. Puccinelli and M. Haenggi, "Wireless sensor networks: applications and challenges of ubiquitous sensing," *IEEE Circuits and Systems Magazine*, vol. 5, no. 3, pp. 19-31, 2005.
- [51] F. P. Lim, "Wireless Sensor Network for Intelligent Supply Chain Management," in *Future Generation Information Technology*, London, 2016.
- [52] O. Çetinkaya and O. B. Akan, "Thermal-Aware Communication Protocols for Body Sensor Networks," in *Emerging Communication Technologies Based on Wireless Sensor Networks*, London, CRC Press, 2016, pp. 144-167.

- [53] M. Ullah and W. Ahmad, "Evaluation of Routing Protocols in Wireless," *Computer Sciences Telecommunications*, vol. 1, no. 1, p. 52, 2009.
- [54] P. Kumar, M.P.Singh and U.S.Triar, "A Review of Routing Protocols in Wireless Sensor Network," *Sensors*, vol. 1, no. 4, p. 14, 2012.
- [55] X. Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks," *Sensors*, vol. 12, no. 8, pp. 11113-11153, 2012.
- [56] M. Omari, N. Tiouririne and D. Dahmani, "Simulation of the TEEN and the SPIN Protocols," *JSAT*, vol. 16, no. 6, p. 7, 2012.
- [57] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications - WSNA '02*, New York, 2002.
- [58] M. H. Anisi, A. H. Abdullah, S. A. Razak and M. A. Ngadi, "Overview of Data Routing Approaches for Wireless Sensor Networks," *Sensors*, vol. 12, no. 4, pp. 3964-3996, 2012.
- [59] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6-28, 2004.
- [60] N. Shabbir and S. R. Hassan, "Routing Protocols for Wireless Sensor Networks (WSNs)," in *Wireless Sensor Networks - Insights and Innovations*, London, InTech, 2017, pp. 1-11.
- [61] C. Nakas, D. Kandris and G. Visvardis, "Energy Efficient Routing in Wireless Sensor Networks: A Comprehensive Survey," *Algorithms*, vol. 13, no. 3, p. 72, 2020.
- [62] S. M. Hedetniemi, S. T. Hedetniemi and A. L. Liestman, "A survey of gossiping and broadcasting in communication networks," *Networks*, vol. 18, no. 4, pp. 319-349, 1988.