REPUBLIC OF TURKEY

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Information Technologies

OPTIMAL ROUTING IN INTERNET OF THINGS NETWORKS USING ARTIFICIAL INTELLIGENCE

Taha Hussein Merie ALHASAN

Master's Thesis

Supervisor

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Istanbul, 2022

OPTIMAL ROUTING IN INTERNET OF THINGS NETWORKS USING ARTIFICIAL INTELLIGENCE

Taha Hussein Merie ALHASAN

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled OPTIMAL ROUTING IN INTERNET OF THINGS NETWORKS USING ARTIFICIAL INTELLIGENCE prepared by Taha Hussein Merie ALHASAN and submitted on 16/12 /2022 has been **accepted unanimously** for the degree of Master of Science in Information Technology.

Asst. Prof. Dr. Abdullahi abdu IBRAHIM

Supervisor

Thesis Defence Committee Members:

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Engineering and Architecture Altinbas University	________________
Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN	Department of Engineering and Architecture Altinbas University	________________
Asst. Prof. Dr. Serdar KARGIN	Department of Biomedical Engineering Beykent University	________________

I hereby declare that this thesis meets all format and submission requirements of a master's thesis.

Submission date of the thesis to Institute of Graduate Studies: __ /__ /__

I hereby declare that all information and data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Taha ALHASAN

Signature

DEDICATION

I devote and pledge this research work to my supervisor who is salient for guiding me through the whole research work as well as my family for always assisting me in my hard time.

PREFACE

First and foremost, I'd like to thank my supervisor, Asst. Prof. Dr. Abdullahi abdu IBRAHIM, thank you for mentoring and assisting me with this dissertation. Discussing my progress, difficulties, and ideas with my supervisor Asst. Prof. Dr. Abdullahi abdu IBRAHIM helped me significantly in comprehending the reasoning behind the research a couple of times a week. It helped me understand the technological requirements for this study project.

ABSTRACT

OPTIMAL ROUTING IN INTERNET OF THINGS NETWORKS USING ARTIFICIAL INTELLIGENCE

ALHASAN, Taha

M.Sc. Information Technologies, Altınbaş University,

Supervisor: Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Date: 12/2022

Pages: 98

IoT will touch society more than past digital revolutions. It impacts global business, environment, and safety. IoT won't replace humans. Billion-connected Things require expertise. IoT enhances living, resource usage, and industry efficiency. If security precautions are not followed, the quantity of networked devices makes them vulnerable to intrusion, which can entail financial loss and death. Guard devices. Cybersecurity-certified devices are released. IoT creates commercial prospects. Benefits require infrastructure-to-endpoint security. Secure people and processes. Human less security wastes millions. Users voted this. Trusting devices and weak passwords. Most corporate users support weak-pass worded third-party devices on the internal network. “Every company will be invaded, we simply don't know when,” said a consultant and strategic adviser. Home and corporate users should understand device vulnerabilities and risks before using them. AI, 5G, and edge computing improve IoT. We proposed sensor-coupled module chains and simulated annealing module placement for edge computing. Our simulation reduced energy and latency. Cloud and IoT are new ideas. Communication, distributed cognition, and on-demand massively parallel processing enable it. Cloud computing helps IoT. Complex IoT demands more computing. Understanding computer activity scheduling optimization approaches is vital. In a multi-cloud system with poor parallelism, enormous arrival rates, and variable runtimes, we investigated simulated annealing. Discrete event simulators evaluated system performance and cost. Simulations show this scheduling method increases performance and cost**.**

Keywords: IOT, ROUTING, ACO, PSO, CLUSTERING.

TABLE OF CONTENTS

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

AI	:	Artificial Intelligence
FSK	:	Frequency Shift Keying
IoT	:	Internet of Things
PAN	:	Personal Area Network
OFDM	:	Orthogonal Frequency Division Multiplexing
TDMA	:	Time Division Multiple Access

1. INTRODUCTION

1.1 BACKGROUND

In this section, we define the basic concepts, namely what constitutes a smart devices and Internet of things. We also define the collection and deployment methods. Finally, we present the different topologies, the connectivity models and the various challenges that we have to face when working with this type of network. show in Figure 1.1

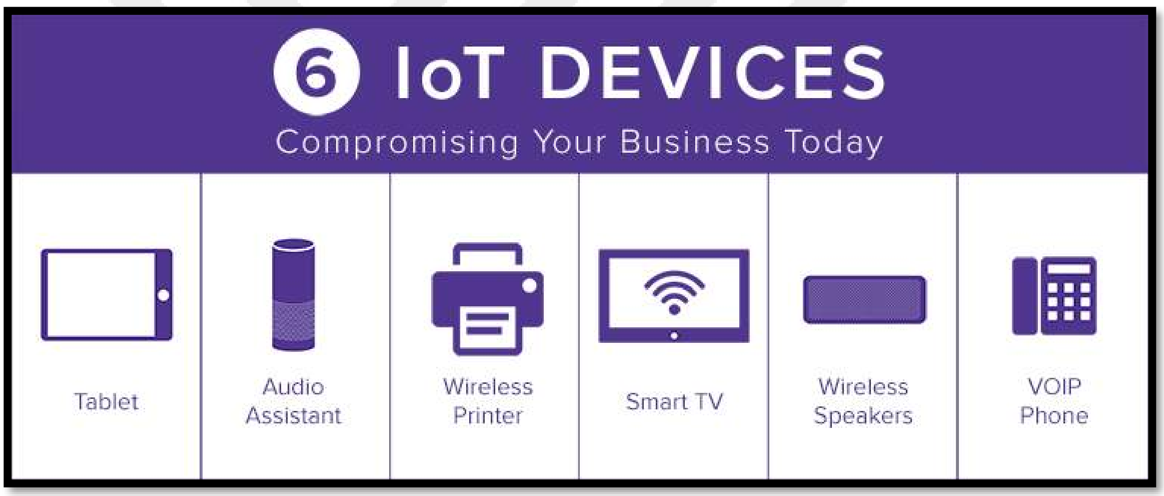

Figure 1.1: Types of IOT devices [31]

1.1.1 Smart Devices Node

A smart devices node is an electronic device capable of acquiring environmental data, processing it and communicating it to an end user.

In the rest of the manuscript, we use the terms smart devices or node to designate an IOT device node in an abbreviated way. A smart devices node consists of the following components:

i. A processor with limited computing power. It is used to process the data captured and the data transmitted by the other smart devices.

ii. A memory used both to store collected data and to run a program.
iii. A radio transceiver allowing communications between smart devices via a wireless medium.

The signal strength used determines the communication range. However, the higher the power, the greater the energy consumption.

i. A sensing unit for measuring physical quantities such as temperature, luminosity or even humidity. The captured data is then transformed into digital data that can be used by the processor.
ii. A power source providing the energy necessary for the operation of the other components. The energy resource most often used is the battery. However, depending on the applications, the smart devices can be connected to a continuous energy source.
iii. A GPS (Global Positioning System) to geolocate the smart devices. This is an optional device because economic and energy constraints limit its use.

The various components that we have just mentioned are represented in figure 1.2.

We can see that the main constraints of smart devices are these limited resources.

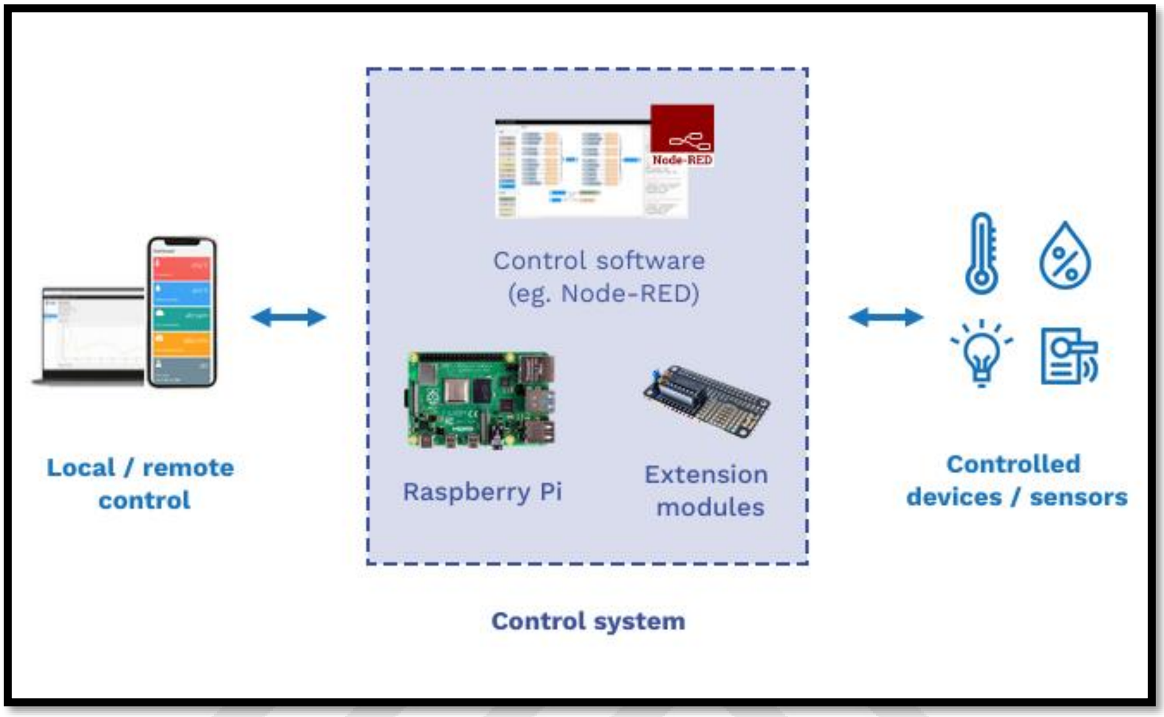

Figure 1.2: Components of a smart devices [43]

The operations performed by a smart device using energy are the acquisition of environmental data, data processing and communication. The costliest operations in terms of energy are communication and acquisition of surrounding data [43]. As part of this thesis, we will focus on energy saving and, more particularly, energy saving during communication.

Using smart devices in groups forms a IOT network as we will see in the next section.

1.1.2 Internet of Things

In this section, we present IOT network in general. Then, we detail the various models allowing to model them according to the characteristics to be taken into account. Finally, we will explain the different challenges specific to this type of network.

A. General Information on Internet of Things

We define, in this section, what constitutes a network of wireless smart devices, their fields of use, the different modes of collection and deployment and, finally, the topologies.

According to the definition, A smart device node and a sink node are the two types of nodes in an IOT network. The former aim to collect information on the catchment area and then transfer it to the collection point represented by the base station or the well. The base station, for its part, recovers the information transmitted to it and sends it to the processing center. It can also send a message to all the smart devices nodes in order to disseminate information such as, for example, the periodicity of the acquisition of environmental data.

An IOT network can consist of one or more base stations:

We are talking about mono-base station network (mono-sink) or multi-base station network (multi-sink).

IOT network belong to the family of ad hoc networks. Within this type of network, communication takes place through radio waves. They are characterized by their ability to organize themselves without a previously defined infrastructure.

Areas of use:

The fields of use of IOT network are diverse and varied [21, 42]. In the following, we give some examples:

i. Health: an example is the Body Area Network. It is a wireless network allowing the interconnection on, around or in the human body, of tiny devices that can perform measurements (smart devices) or act actively (actuators). These smart devices are able to communicate with a remote service center in order, for example, to communicate the state of the patient under observation. Examples of body smart devices are blood glucose or blood pressure smart devices [49]. Notably, implanting a biosmart devices in a patient provides a more accurate and less invasive method of measuring glucose levels and, depending on the result, an add-on device can perform automatic insulin injection.

ii. Urbanization and infrastructure: smart devices are used, for example, in the context of smart cities. Federspiel et al. [9] study the improvement of energy production, distribution and consumption through the use of smart devices. Idwan et al. [80] propose the use of IOT network to optimize waste management through the use of smart dumpsters equipped with waste level smart devices. Knowledge of the level can be used by municipalities to deploy the sufficient number of trucks and people for waste collection. Additionally, route planning and routes to follow can be done to minimize the time and fuel required.

iii. The environment: smart devices are used to monitor nature. For example, they allow the detection of floods or the presence of fire in forests. Another example of application can be the prediction of meteorological weather. One of the most representative examples is the deployment of a IOT network consisting of 32 nodes on Great Duck Island [11]. The smart devices used detected temperature, barometric pressure and humidity. The aim was to monitor the natural environment of a bird (sea petrel) and its behavior in relation to climate change.

iv. The military field: smart devices are used to detect explosives or in a battlefield to detect the movements of enemy troops. For example, the University of Virginia proposes replacing mines with thousands of scattered smart devices that will detect an intrusion by hostile units [17].

The information measured by the smart devices can be collected in different ways. This point will be dealt with in the next subsection.

Methods of collection:

The collection of environmental information can be done in three different ways:

i. Supervision (Monitoring): This mode allows continuous acquisition of the quantity to be measured. The smart devices periodically send the acquired data.

ii. Collection on demand: When we want to have the information, the base station performs a broadcast to propagate the request. The smart devices carry out the measurement and send the measured information back to the base station.

iii. Collection following an event: When an event occurs (sudden change in temperature, detection of a movement, expired timer, etc.), the smart devices having detected the information send it back to the base station.

Deployment modes:

IOT network can be deployed in a pre-configured topology or randomly dispersed [23].

There are networks of mobile wireless smart devices whose deployment is not fixed. We are not interested in the mobile aspect in our work.

Once the smart devices have been deployed, a logical topology can be set up to compensate for the lack of physical infrastructure of Internet of things.

Topologies:

A IOT network can be organized according to different topologies: star, mesh, grid or tree.

In the star topology drawn in Figure 1.3, the nodes are all connected to a central node. All the nodes are therefore at a distance of one hop from the central node.

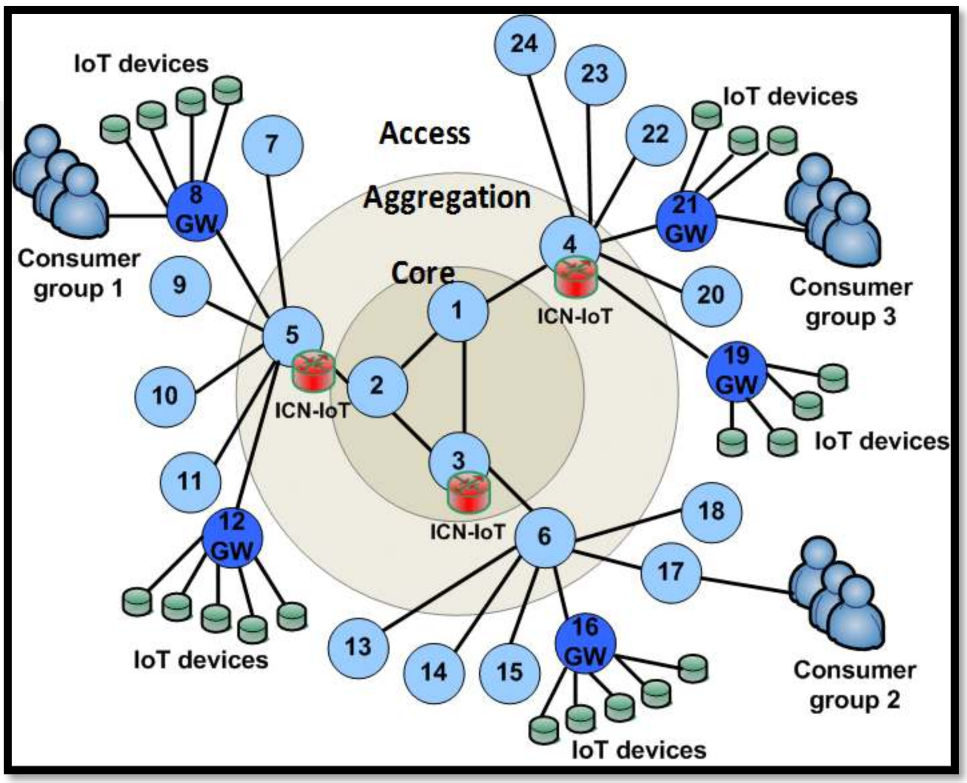

Figure 1.3: Topologies of a IOT network mesh tree [52]

In a mesh topology, all nodes are peer-to-peer connected without the presence of a central hierarchy. This topology is shown in Figure 1.3.

In the tree topology, a hierarchy is established between the different nodes. The network is divided into levels. The top level contains the base station which is connected to several nodes at a lower level. These nodes can themselves be connected to other lower level nodes. This constitutes a tree as shown in Figure 1.3.

To abstract IOT network, researchers have proposed different models, as we will see in the following sections.

B. Connection Models

A network of things can be modelled via a graph. In this case, the smart devices are the vertices and the connections between the smart devices are represented by edges. This representation is detailed. The advantage of using this type of modelling is to facilitate the mathematical study of the proposed algorithms, their correction as well as their performance. The simplest connectivity model is called the General Graph. It is represented by an undirected graph devoid of particular properties. This type of model is considered too pessimistic because the connectivity in a network of things is subject to geometric rules that we do not find in general graphs. This is why in the literature, different models have been proposed according to the level of abstraction at which we want to position ourselves or according to the property/constraint studied. Schmid and Wattenhofer [32] and Yu et al. [70] present the most commonly used connectivity models. We will see in the following the description of some of them.

i. Unit Disk Graph (UDG):

A Unit Disk Graph is an undirected graph in which the nodes are deployed in a two-dimensional plane. It represents a collection of discs all having the same unit diameter. In other words, two nodes are neighbors if, and only if, their Euclidean distance is less than or equal to 1. In this case, all nodes have the same transmission range. In this model the nodes are assumed to have an omnidirectional radio antenna and to be dispersed in a planar environment devoid of obstacles.

ii. Quasi Unit Disk Graph (QUDG):

The quasi unit disk graph is a model generalizing the unit disk graph. Indeed, this one makes it possible to take into account the directional antennas or the presence of small obstacles. As in previous models, the nodes are dispersed in a two-dimensional plane. Two nodes can be neighbors if their Euclidean distance is at most ρ where ρ belongs to the interval (0,1]. Two cases can arise. The Euclidean distance is between 0 and ρ or it belongs to the interval $(\rho,1]$. In the first case, the nodes are neighbors. In the second case, the nodes may or may not be neighbors.

iii. Disk Graph (DG):

In the case of disk graphs (Disk Graph) [13], the network is modeled by a directed graph. The nodes of the graph are located in a Euclidean plane and each node has its own transmission range. A node i neighbors a node j if, and only if, the Euclidean distance between them is less than or equal to the transmission range of node i. We notice that in this case, it is possible that node i has node j as a neighbor but that node j does not have node i as a neighbor. Indeed, it depends on their transmission range.

iv. Disks graph with bidirectional links (BDG):

This model is a special case of the disk graph model in which only a subset of the edges is considered: the bidirectional edges. That is, an edge exists between two nodes u and v if the Euclidean distance between them is less than or equal to the smallest span among ru and rv. In this case, the disk graph with bidirectional links is modeled by an undirected graph.

The unit disk graph model makes it possible to model a homogeneous IOT network: all the smart devices have the same communication range. On the other hand, the models of disk graph, disk graph with bidirectional links and quasi graph of unit disks make possible the representation of a network of heterogeneous smart devices. The heterogeneity is implemented here at the level of the communication range assigned to the various smart devices of the network. However, disk graphs with bidirectional links do not take into account the case where the neighborhood relation is unidirectional, which represents the most generic case.

The models that we have just seen allow the abstraction of the IOT network by highlighting its connectivity. In addition, there is another category of models making it possible to represent the network from the point of view of the interference present between the various nodes constituting it.

C. Interference Patterns

In general, in wireless networks and, in particular, in Internet of things, the communication medium is shared and, therefore, the transmissions are subject to interference. Concretely, a node may not be able to correctly receive a message from an adjacent node if a simultaneous transmission is being performed nearby. The role of an interference model is to highlight the transmissions which, carried out simultaneously, create a disturbance of the wave thus resulting in poor or even non-reception of the message sent. When the transmissions are not made during the same time slot, no interference occurs. A certain number of models making it possible to represent these interferences have been proposed. Schmid et al. [32] list a number of them. In the following, we present the most commonly used as well as the simplified model that we used in the context of the thesis.

i. Signal-to-Interference Plus Noise (SINR):

The best known model is the physical model named SINR. It is commonly used to define interference at the lower layers. This model considers that the reception is successful depending on the received signal strength, the ambient noise level as well as the interference caused by the simultaneous transmission of the nodes.

ii. Simplified Interference Model:

In our simplified interference model, we consider that a node u can create interference for a node v if v is within the transmission range of u. We consider two types of collisions: the primary or explicit collision and the secondary or implicit collision. The primary collision occurs when a node transmits and receives during the same time slot. This is shown in Figures 1.4 and 1.5. Figure 1.4 represents the case where node 2 receives a message from node 1 and sends a message to node 3 during the same slot. Figure 1.5 illustrates the case where node 2 receives a message from node 1 and 3 during the same slot. The secondary collision occurs when a node, which receives a transmission intended for it, is disturbed by another transmission which is not intended for it. This is shown in figure 1.6, in which node 3 sends a message to node 4 at the same time as node 1 transmits a message to node 2. Now, nodes 1 and 3 are in the transmission range of one of the other, so it causes a collision. Therefore, to avoid collisions, the transmission slots of the two nodes that may cause a collision must be scheduled at different time intervals.

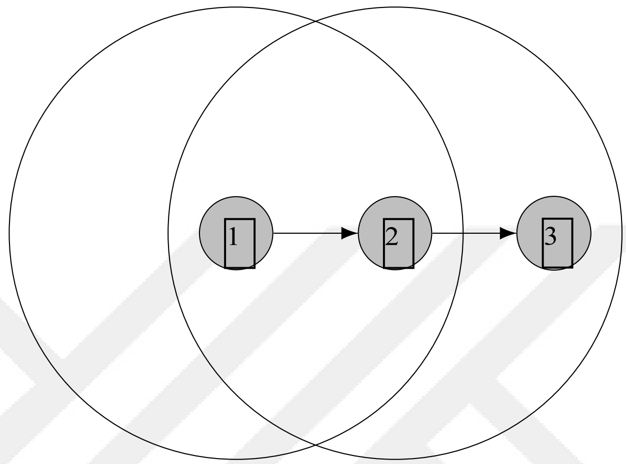

Figure 1.4: Example 1 of primary conflict [21]

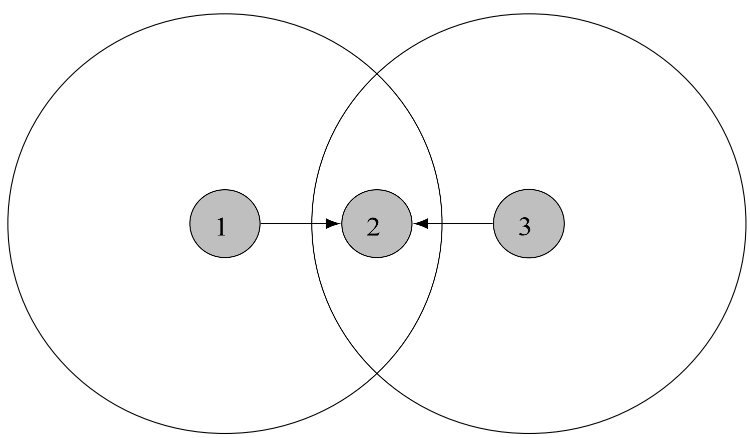

Figure 1.5: Example 2 of primary conflict (hidden node) [21]

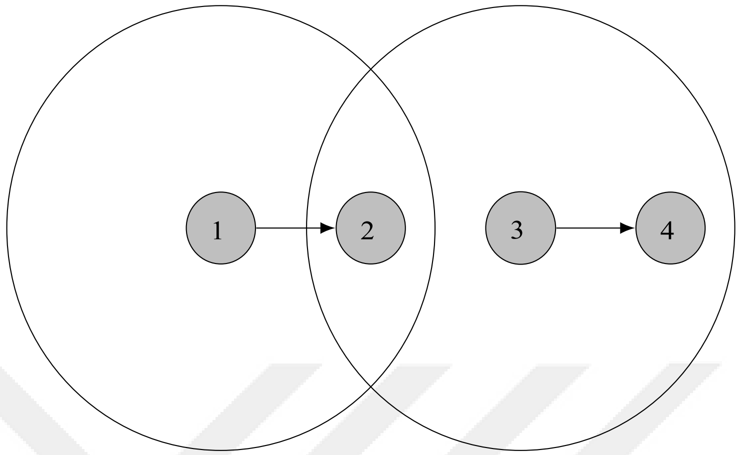

Figure 1.6: Example of secondary conflict (exposed node) [21]

D. CHALLENGES

Although IOT network share many similarities with other distributed systems, they are subject to a variety of unique challenges and constraints. This section describes the most important constraints in a IOT network.

i. Limited resources:

The constraint most often associated with the IOT network is energy. This is because nodes are mostly powered by batteries, which need to be replaced or recharged (for example, using solar power) when they run out. In some cases, the smart devices are deployed in a hostile environment or difficult to access, which means that when their energy source is exhausted they will be unusable. An unusable node can cause a variety of problems ranging from lack of metering in the catchment area to network partitioning.

ii. Self-organization:

The nature of many IOT network applications requires smart devices to be dispersed in remote areas or in hostile environments. Therefore, smart devices must be able to self-organize and adapt to failures without human intervention. Another aspect that may generate the need for a reorganization of the network may be the presence of mobile smart devices.

1.2 PROBLEM STATEMENT

In this section we present the problems studied in this thesis: broadcasting and multi-layer routing in Internet of things. As seen previously, we model the IOT network by a weighted disk graph. In the following, we give the definition of broadcasting and routing using graph theory.

1.2.1 Diffusion

Broadcasting is an operation commonly used in wired and unwired networks. It allows information to be disseminated throughout the network. The formal definition is as follows.

A naive way to perform broadcasting is to instruct each smart devices to re-transmit the received message. The problem with this method is that all the smart devices are transmitting. Therefore, the cost of broadcasting is given by the sum of the costs of all the nodes constituting the network. This means that all the nodes of the network are solicited and therefore that we consume the energy of each of them. In the literature, different approaches have been proposed to perform diffusion more efficiently. The idea is to define a subset of the smart devices which is in charge of the re-transmission. There are different approaches: probabilistic, by area and backbone.

In graph theory, a backbone is defined by a connected dominating set. First, let's define a dominating set:

For the message to propagate from the base station, we need the retransmitting nodes to be neighbors to each other, hence the need to add the notion of connectivity presented in the next definition.

Sometimes it is interesting to build a backbone made up of as few nodes as possible. For example, if we consider that all the nodes have the same transmission range C, fewer nodes retransmit, less energy is spent. To do this, we construct a connected dominating set of minimal size defined as follows.

Constructing a connected dominating set of minimal size is an NP-problem

Difficult [4].

To take into account nodes of different weights while minimizing the energy, we construct a connected dominating set of minimal weight. The formal definition is as follows:

1.2.2 Multi-Layer Routing

During the thesis, we were interested in routing in IOT network. In particular, multi-layer routing between the Network and Data Link layers. To clarify the problem addressed, we first present the basic concepts, namely the layered model and the cross-layering method.

1.2.3 The Layered Model

Generally, the communicating processes of a network are divided into seven layers following the OSI (Open Systems Interconnection) model. This model was proposed by the ISO organization (International Organization for Standardization). Given the specific characteristics of IOT network, only five layers are used [51, 57]: the physical layer, the data link layer, the network layer, the transport layer and the application layer, as shown in Fig. 1.7. The physical layer is responsible for transmitting and receiving signals over a physical communication medium, including frequency generation, signal modulation, transmission and reception, data encryption, etc.

The data link layer is mainly responsible for the multiplexing of the data stream, the transmission and reception of data frames, the access to the medium as well as the error control. It is composed of two sublayers: the channel access control sublayer (Media Access Control or MAC) and the logical link control sublayer (Logical Link Control or LLC). The first sublayer determines, for a smart devices, the possibility and the moment to access the communication channel. The protocols allowing the management of this sub-layer are called MAC protocols. The second checks the data flow as well as the errors.

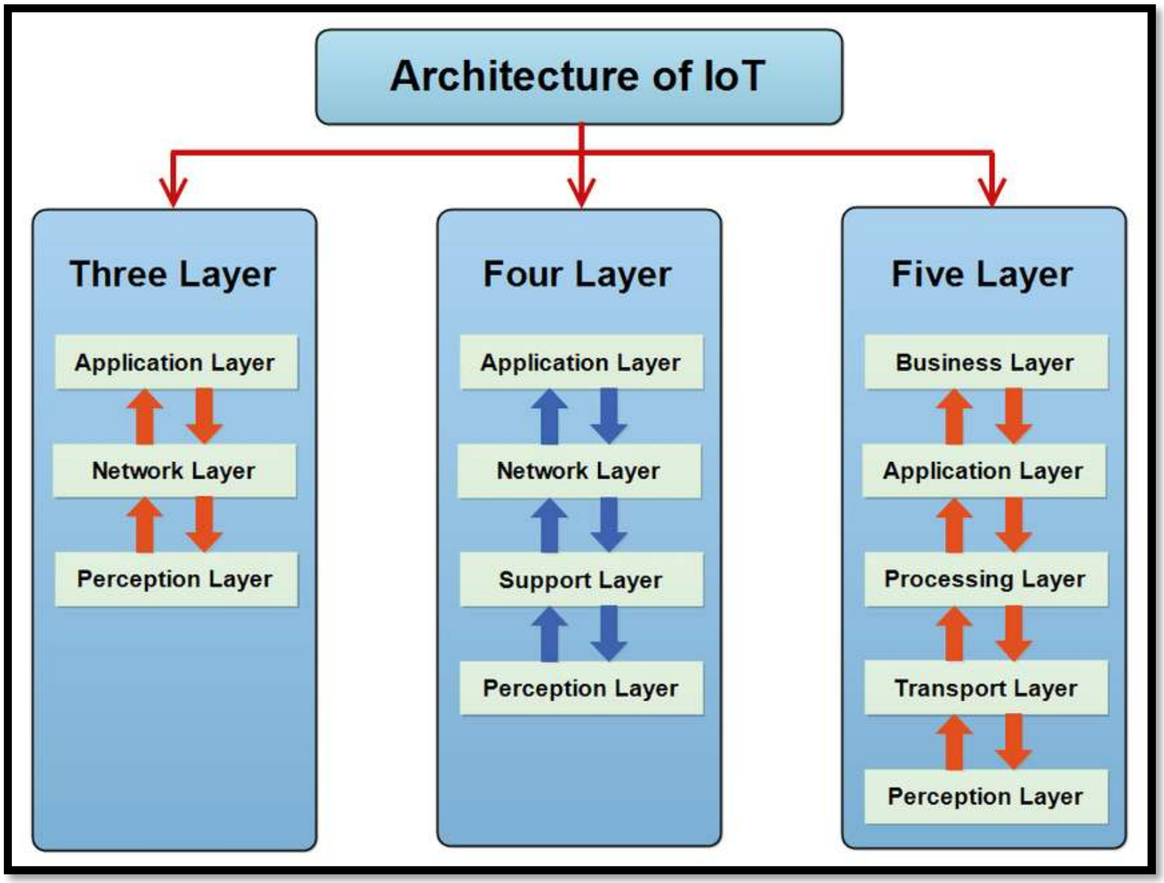

Figure 1.7: Layered model for IOT network [19]

Thus allowing the reliability of MAC protocols. The third layer is called the Network layer. The Network layer is primarily responsible for forwarding and routing packets in the network. The fourth is the transport layer. It guarantees the transfer of packets or raw bytes without corruption, loss, reordering or duplication. She is responsible for managing end-to-end communications.

The Application layer contains a variety of protocols specific to the various applications of the IOT network. It constitutes an interface between the end user and the network of things allowing a transparent interaction with this one.

The majority of proposed protocols for IOT network follow the traditional layered protocol architecture shown in Figure 1.7. Melodia et al. [25] point out that these types of protocols achieve very high performance for the metrics relating to each of these individual layers, but they are not jointly optimized to maximize the overall performance of the network while minimizing the energy expenditure. This is why research has turned to joint inter-layer optimization presented in the next section.

1.2.4 Cross-Layering

The cross-layer design indicates that the parameters of two or more layers can be retrieved and/or modified to achieve an optimization goal. The concept of cross-layer was first proposed for TCP/IP networks, when wireless links were deployed [27]. Since the TCP/IP stack was proposed for wired connections, using this new approach resulted in a decrease in performance. Lately, cross-layering research is an area that is receiving more attention in Internet of things research.

Different solutions have already been proposed in the literature, and at least in the context of simulations, they have proven to perform better than their layered counterparts [56].

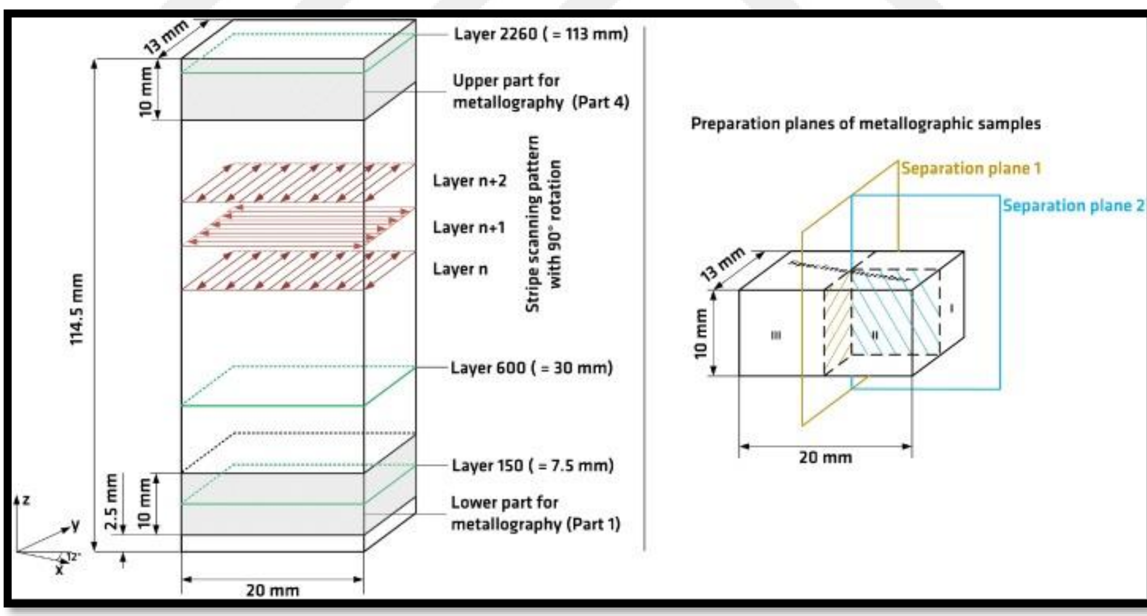

Figure 1.8: Inter-layer cross-layering (left) and layer fusion (right) [27]

1 and Layer 2. In this first type of cross-layering, the Layer 2 protocol uses the Layer 1 information or vice versa, as shown in Figure 1.8a. For example, consider the Network layer

and the Data Link sublayer. A form of cross-layering can be the following: the MAC sub-layer uses the information of the Network layer, that is to say that the temporal decisions are made according to the spatial decisions.

The second type is a layer fusion approach. It is a question of defining a super-layer able to ensure the functionalities of the layers constituting it. Let's go back to the example of the Network layer and the Data Link sublayer. In this case, the temporal and spatial decisions of the respective layers are made simultaneously.

These two types of cross-layering can be performed between two or more layers and they can be based on any combination of layers [39].

1.2.5 Mac Under layer Protocols

In Internet of things, MAC protocols can be divided into two categories: protocols with or without contention. In the first category, we find, for example, ALOHA (Additive Link On-Line Hawaii System) and CSMA (Carrier Sense Multiple Access).

In MAC protocols without contention, the access of nodes to the medium is divided with respect to time (Time Division Multiple Access or TDMA), or frequency (Frequency Division Multiple Access or FDMA) or code (Code Division Multiple Access or CDMA). These methods allow different nodes to access the medium without interfering with each other and thus effectively avoid collisions. The most popular medium access control mechanism for ad-hoc networks uses CSMA (Carrier Sense Multiple Access). However, in the case of wireless networks, it has many drawbacks, such as a high energy cost or even an increased access time. For these reasons, TDMA (Time Division Multiple Access) seems more appropriate for this type of network [79].

The number of time slots in each TDMA frame is called the frame length. A timeslot has a unit length of time required for a packet to be transmitted between adjacent nodes. When the nodes are close, collisions can occur in case of simultaneous transmissions. Therefore, the use of TDMA as a MAC protocol in wireless multihop networks requires node scheduling to avoid collisions.

A TDMA protocol aims to define a schedule. This consists of determining a number of time intervals or slots. Each node is associated with a slot to transmit its data and a certain number of slots to receive data from its neighbours.

Throughout the thesis, we focus on the optimization of energy as well as latency. This is why in chapter 5, we propose a multi-layer approach between the Network layer and the MAC sub-layer using the TDMA protocol.

In the next section, we present the different optimization methods applicable for solving the problems addressed.

1.3 CONTRIBUTIONS AND OBJECTIVES

Before we start solving a problem, we need to look at the difficulty to get solutions. In computer science, efforts are made to propose algorithms capable of calculating them in a reasonable time. For this, it is necessary to propose efficient algorithms.

An algorithm is said to be efficient if it has a time complexity of the form O(nk) where n is an integer representing the size of the input of the problem treated and k is a constant. We say that the algorithm has polynomial time complexity.

The class of problems that can be solved in polynomial time is Class P. More precisely, problems of class P can be solved in polynomial time on a deterministic Turing machine.

The problems we deal with in this thesis are NP-hard, that is, they are harder than any problem belonging to the class NP. The problems of the class NP are the problems which can be solved in polynomial time on a non-deterministic Turing machine.

Whether P = NP is still an open question to this day. This means that we do not know any efficient algorithm allowing to solve a problem of class NP, a fortiori for NP-hard problems.

Therefore, to solve the problems addressed, we use different methods depending on the size of the problem. For small instances, an exact method is used: integer linear program. In this method, the problem is modeled by an objective to be minimized or maximized (we speak of an objective function) and by variables subject to constraints defined by linear relations. For large instances, we seek an approximate solution, computable in polynomial time. For this, there are three methods that can be used:

i. Heuristics

ii. Metaheuristics

iii. Approximation algorithms

A heuristic makes it possible to calculate a solution but does not give any guarantee on the quality of the result. On the other hand, an approximation algorithm gives a solution whose quality relative to the optimum is bounded mathematically. As for metaheuristics, they can be considered as general methodologies that can be used to solve optimization problems. Metaheuristics, like heuristics, give an approximate solution but do not guarantee the optimality of the solutions obtained.

Among the approximation algorithms, there is a family called Polynomial-Time Approximation Scheme (PTAS). These are approximation algorithms taking as argument an instance of an optimization problem and a parameter ≥ 0. They produce in polynomial time, in the size n of the processed instance, a solution having an approximation factor of 1 + of the optimal solution.

Metaheuristics can be classified into two families: the family of metaheuristics with a single solution and that with populations of solutions. As part of our work, we will only use the first family represented by the local search. This type of metaheuristic starts with a given solution and iteratively improves it by choosing a neighbouring solution allowing the improvement of the objective function. The search is stopped when all the neighbouring solutions do not allow improvement. The main problem with this method is that it can lead to a local optimum. To avoid convergence to a local optimum, two local search methods, Tabu Search and Simulated Annealing,

Simulated annealing is a method inspired by physical annealing. The latter is a process used in metallurgy to improve the quality of a solid. For this, it alternates cycles of heating (annealing) and cooling. The objective is to reach a minimum energy state corresponding to a stable metal structure. The process begins at a very high temperature where the material is liquid. Then follows a phase of gradual decrease in temperature allowing the material to return to its solid state. Simulated annealing was developed by three IBM researchers, S. Kirkpatrick et al. in 1983 [2] and independently by V.

Simulated annealing begins with an arbitrarily chosen configuration. Then, a neighbouring configuration is chosen at random. This configuration is kept according to the value of the objective function associated with it. If this value improves the objective function, the new configuration is kept.

2. RELATED WORKS

2.1 INTRODUCTION

It may seem like fiction, but we are living in a futuristic reality. Products and technologies that years ago we didn't even imagine, are now part of our daily lives. According to the IT4CIO article, Futurist Reality: pointing out tomorrow's innovations today (2020, p.1), changes, whether technological or behavioral, do not take more years to materialize, and the way we see the world around us changes as quickly as we can adapt. In his article, The Transformation of Everyday Life with the Technological Revolution of IoT (2020), Katia Simooes states that with the arrival of the Internet of Things, life will no longer be the same. And it's not about future change, on the contrary, the revolutionary technology that allows all objects to transmit information, is already starting to change the way business is done, communicates and interacts. Nowadays, there are already watches that measure the physical performance of a sports practitioner, transmitting their data to his computer or to the doctor who accompanies him, vehicles that park themselves, monitor the traffic indicating the best route to reach the destination. Houses that turn on lights, turn on bathtubs, turn on air conditioners, play the owner's favourite music at the specified time, cities are becoming smart. These are just some examples. the IDC, On the other hand, an invisible enemy will emerge that will require the manufacturers of these devices to invest heavily in security to ensure that data transmitted from vehicles, homes, smartphones and other connected devices are protected from unauthorized access. In the book Future Crimes by Marc Goodman (2022, p244), it was possible to identify that the concern with the security of all this technology is not following at the same speed. In this book, the author reports how the cybercrime underworld works, that is, "if everything is connected, everything is vulnerable" (GOODMAN 2022, p244). For this reason, the Internet of Things may also increase risks, involving threats to the security of people and companies around the world. The good news is that tech giants have become aware of the danger and are investing millions of dollars to improve the security of smart devices. As with mainframe and personal computers, the fight against cybercrime will be eternal, just know who will be ahead. This article is divided into six sections, this being the first. The second section describes the emergence of the Internet of Things and its growth. In the third section it is shown where the Internet of Things is already found on a large scale. The fourth section presents the Internet of Things trends for the coming years. The fifth section seeks to alert and make users aware of device security. Finally, the sixth section presents the final considerations, highlighting that the growth of the Internet of Things is irreversible, and the benefits provided in all areas will be increasing, as long as its use is conscious.

2.2 EMERGENCE OF THE INTERNET OF THINGS

In the last 10 years we have seen the birth of a sea of global data, objects, people and nature have always emitted a large amount of information and until then human beings were not aware of these messages. This is precisely what the Internet of Things has brought to our reality differently, according to the article Why We Love the Internet of Things published by InQuesti (2020). The Internet of Things is radically changing the way society lives, and the way personal and corporate transactions are being made, providing a link between objects and the internet, transforming the way we interact with the world and how the world interacts with us. , changing not only the way we live, but also the way we work. The Internet of Things is a term coined in 1999 by Kevin Ashton, a British technology pioneer who conceived a ubiquitous sensor system connecting the physical world to the internet while working on radio frequency identification (RFID). According to the article Internet of Things: from Theory to Practice, published by Santos, BP et al. (2021) the Internet of Things, in a nutshell, is nothing more than an extension of the current internet, which provides everyday objects (anyone), with computational and communication capacity, to connect to the internet. The connection to the World Wide Web will make it possible, first, to remotely control the objects and, second, to allow the objects themselves to be accessed as service providers. The Internet of Things can be divided into two camps, commercial and consumer devices. The Consumer Internet of Things, or Consumer IoT, includes things like TVs, DVRs , home security systems, appliances, lights, printers, and clocks, while the Commercial Internet of Things includes devices such as monitors, sensors, inventory tags, radio frequency-enabled IDs, valves, switches, and shop floor devices. There are hybrid segments being developed like IoMT (Internet of Medical

Things), which includes things like patient monitors, infusion pumps and assessment tools. As published by Mônica Mancini (2020), the first device connected to the internet was a toaster in 1990 by John Romkey. This device could be turned on and off over the internet. This feat allowed Romkey to present the device at the Interop '89 Conference. In 2019, the Nabaztag was launched, a rabbit-shaped object connected to the internet that could be programmed to receive the weather forecast and read e-mails, among others. This was the first smart object to be commercialized on a large scale. Also according to Mônica (2020), as of 2022 the Internet of Things is already a reality and about 4.9 billion things are connected and in use, an increase of 30% compared to 2019 and which will reach about 30 billion by 2020. The Internet of Things has become a powerful force for business transformation and its disruptive impact on all industries and society.

2.3 INTERNET OF THINGS APPLICATIONS

Smart devices are everywhere and can be found in the most diverse fields of activity. The possibilities that come with the Internet of Things are endless, not only for large companies, but also for small, medium and consumer goods. In order to reduce costs, increase production and provide comfort, the Internet of Things can be found at (EMBRATEL, 2020):

i. Urban Mobility: Vehicles are becoming autonomous, they indicate the best route, parking and toll payments are automatic, as well as onboard entertainment and information. Public transport is gaining intelligence, calculating vehicle availability according to capacity. Traffic lights are also gaining intelligence by calculating the changeover time according to the flow of vehicles

ii. Financial Market: Credit cards are everywhere in addition to commercial establishments, also in taxis, in street vendors, at fairs. Digital banks are fully autonomous, with no need for personal contact.

iii. Retail Commerce: When a customer enters an establishment, through their smartphone the person is identified and their shopping profile will be presented to an attendant who will provide personalized service, as he will know the products of interest to the customer.

iv. Industry: Industrial automation that gives the concept of Industrial Revolution 4.0, which is the integration of physical and digital technologies, from the development stages, from production engineering and from the entire chain to the use of the final product and the operations linked to it.

v. Agriculture: In this segment, mechanized planting with autonomous machines, control and tracking of herds, irrigation control, soil and pest control are some of the applications.

vi. Health: The expectation is that this segment will be one of the pillars of the Internet of Things. It will make clothing and accessories health gauges and controllers.

Pressure, fever, pain will be diagnosed early and the action will be indicated to the user. Doctors will receive exam diagnoses from their patients in real time and can give immediate referrals.

i. Smart Cities: Sensors control lighting, warn when it will be necessary to collect garbage, when drains are clogged, warn when there is a water leak, surveillance systems assist in security with monitoring connected to control centers in real time. This intelligence is also available in buildings for water, energy, gas, sewage controls with digitized markers. The city of Barcelona in Spain is one of the pioneers in the implementation of the services described above.

ii. Consumer Goods: In this segment there will be a greater variety of smart devices available such as smart homes, smartphones, smart TVs, wearables and many others.

The examples of applications above are already reality, but it is safe to say that there is still much to come. Applications that are still far from being imagined will still emerge, so the expression “the sky is the limit” applies very well.

2.4 INTERNET OF THINGS TRENDS

In addition to everything that already exists, it is difficult to imagine what is yet to come, but there are already some clues. What was previously unimaginable in a few years will become reality, for example (ABRITTA, 2021):

I. The first body-implantable smartphone will be available in 2025: These devices will be able to identify diseases, track people, send data to monitoring centers and automatically release medicines;

II. Our eyes will interface technologies in 2023: Technology will be able to connect our own vision to electronic devices;

III. People will wear clothes connected to the internet: Chip could be placed in clothes, allowing to track children and detect habits, in 2022;

IV. A trillion sensors connected to the internet: Experts suggest that in the future, all physical products could be connected to communication infrastructure and sensors everywhere allowing people to have complete perception of their environment, by 2022;

V. Smart cities: we will see the city with more than 50 thousand inhabitants and no traffic lights. Progressive cities such as Singapore and Barcelona are already implementing services that work through data. Even the roads will be connected to the internet. The sensors will facilitate from moving to removing garbage from the streets, in 2026;

VI. Many jobs are already influenced by robots: In 2021, according to forecasts, the first pharmaceutical robot will appear and the population will be able to trust the technology for drug prescriptions;

VII. Production of the first 3D-printed car in 2022: Currently, 3D printers work mainly in the manufacture of plastic products, which are made layer by layer. However, many companies are already working on the idea of using other types of materials. It is now possible to print chocolate. Liver transplantation can also be done using titanium powder.

VIII. By 2025, 5% of the products consumed will be produced by 3D printers: In this scenario of 3D printing possibilities, products could be software that people download and print at home, customized and on demand. This could reduce costs and increase accessibility to these products.

The trends above may seem futuristic, but in a few years they will definitely be a reality. Who doesn't remember the emergence of the cell phone in the early 90's? Who could imagine someone talking to someone else through a wireless device? Examples like this awaken the imagination and creativity of technology geniuses.

2.5 SECURITY OF THE INTERNET OF THINGS

Security against unauthorized access is perhaps the biggest concern when it comes to the Internet of Things. Although many people ignore it, the danger is real, it exists and can bring a lot of damage, not only financial but also against the physical integrity of the user.

2.5.1 SCRATCHS

ISO/IEC 27002(2019) defines risk as the possibility of an asset, such as an Internet of Things device, to be subject to vulnerability and incidents that may compromise the continuity of its activities.

The more we connect devices into the global network, the more vulnerable we become to cybercriminals who know how the underlying technologies work and how to exploit them to their advantage. Therefore, in terms of risks, it is natural that the Internet of Things presents a variety of potential security issues that can be exploited, including:

i. Unavailability of services: it can cause huge losses and make environments inaccessible;

ii. Vulnerabilities: device failures can enable hacker attacks to control these equipment and data hijacking (ransomware attacks);

iii. May allow unauthorized access, facilitate access to other systems;

iv. Privacy: security flaws in these devices can totally compromise your privacy, allowing access and use of personal information causing financial losses and damage to the image, whether in people or companies;

v. Infrastructure: More and more data and information are stored in the cloud.

However, security in this mode can be easily compromised.

Another great risk, which may seem innocent, is the one practiced through social engineering. (POPPER, 2019), using the power of persuasion, that is, through a good conversation. It is very common to have access passwords passed on when visiting an acquaintance's house, at a company to someone who is providing some support service, and sometimes even written down on tickets and glued to the monitor. Naivety is a behaviour to change in the culture of people and companies so that they actually increase their security. This finding came about in a survey carried out in January 2018, with home and corporate users who have some type of Internet of Things device such as monitoring systems, alarms, home automation, production controllers and even robots. The result of the research in general is worrying, when it comes to security against unauthorized access. Following is the mapping of the responses:

I. Every device connected to the internet can be hacked. Do you worry that you might be hacked? Do you trust the device's security system?

i. D: 75% of respondents are unaware of the fact that they can be hacked and trust the security of the device. 25% believe in this possibility, but do not know how to proceed to improve security.O Ç: 66% of respondents use the internal network to access the device for support and maintenance and only 33% have a separate network with user and limited access.

II. Do you have any idea what can happen if the internal network or device is hacked?

i. D: 100% believe in the security of the device and do not believe in this possibility, but if it happened, the biggest concern would be about the disclosure of internal images.

ii. C: 100% is aware of the damage that could be caused in the event of an invasion, such as theft or loss of information and ransomware.

III. Do you take care to avoid incidents of this nature, such as creating strong passwords, updating device software when available?

i. D: 75% use default passwords that have never been changed and also have never updated the device software. 25% changed the default passwords, but they use passwords considered weak and also never updated the device software.

ii. C: 66% use internal network access and user and update device software when prompted by the manufacturer. 33% have specific user access to support services and only update device software when prompted by the manufacturer.

IV. If an incident happens, do you know what to do or who to turn to?

i. D: 100% would turn to the companies responsible for the installation.

ii. C: 100% would isolate the device from the network and trigger internal or manufacturer support.

V. Even aware of the risks, would you recommend the devices to other people/companies and continue using them?

i. D: 100% will continue using it and would recommend it to others.

ii. C: 100% will continue to use and invest more in automation when possible, but would not recommend it to other companies because these automations can be a competitive differentiator in the market.

As a result of the research, it became evident, in the case of home users, that the security issue is as new as the devices installed and that the concern against intrusion is almost nil. In companies, this concern exists, but many sin in simple details such as allowing access to external technicians from the internal network. In summary, the security issue is not at the top of the priorities and there is a lot to be done to achieve the minimum recommended security.

2.5.2 SAFETY

The emergence of the Internet of Things has not gone unnoticed by cybercriminals, who seek to exploit its weaknesses. Therefore, in terms of risks, it is natural that the Internet of Things presents a variety of potential security problems that can be exploited, in companies and, mainly, in domestic consumers, where security concerns are minimal. In his article Understanding the IoT Explosion and Its Impact, Phill Keeley (2020) comments that most IoT devices were not designed with security in mind. Many do not have an operating system or even enough memory or processing power to implement security solutions, while an alarming number of devices have passwords hardcoded into their firmware. Security is not an isolated activity, but a dynamic part of the Internet of Things ecosystem. Inserting new devices, decommissioning devices at end-of-life, integrating a device with a new cloud ecosystem or vice versa, controlling downloads, firmware and software, all these activities need comprehensive identity management. , keys and tokens (GEMALTO, 2018). The Internet of Things brings unique security challenges because it places potentially insecure data, computing power, communications, sensors and other devices in complex or fluid environments such as factories, smart cities and enterprises where traditional security notions do not always apply. Unfortunately, edge protection such as firewalls and anti-malware software do not provide the visibility or security needed in this new world of computing (HPE, 2020). The Internet of Things jeopardizes the security of thousands of devices that were previously beyond the reach of hackers. It turns simple objects such as coffee pots or watches into real data access ports, espionage, theft of sensitive business information and, in the case of vehicles and medical prostheses, threats to the lives of its users. With the Internet of Things, a new category of crimes arises, a kind of ransomware, such as the blocking of houses and vehicles, where the criminal demands payment of ransom to release access. In the video entitled “The Wolf”, The Wolf,points out that only 2% of installed printers have some type of security and that through a smartphone it is possible to access their operating system. Through social engineering, with an email containing malware, for example, it is possible to infiltrate the printing system, circumvent the company's security, gain access to unencrypted data not only of the documents that are in the printers, but of the data of all network computers and send them to the attacker.

2.5.3 Guarantee the Security of Iot

To ensure the security of your network or device, it is very important to identify which devices are connected. If any of them are connected and not identified, they can compromise all security rules. In the article Internet of Things and its Security Challenges (PROOF, 2018), there are some rules to increase the security level:

i. Choose quality devices and verify security criteria: it is important to check the manufacturer and the product's security criteria, making sure of the quality and the manufacturers' ability to perform security updates on the devices.

ii. Updating systems, software, and devices: Keeping up to date helps protect against intrusions, ransomware attacks, and other malware. The updates fix any vulnerabilities that may be found.

iii. Create complex passwords: it is important to use different passwords in different internet services, in addition, Long passwords with upper and lower case letters, numbers, and special characters improve security. Default device passwords should be avoided, as in addition to being easy to discover, many of them are known to hackers. It is recommended that passwords be changed every 3 months. Using password managers helps to maintain the standard of secure passwords, and makes it easier to change them, avoiding their reuse.

iv. Back up regularly: Don't underestimate the power of backups. Have an external hard drive with important data and back it up regularly. Cloud storage is also another option, but the copy needs to be on a server with high-level encryption and multiple authentication factors. If possible, keep both forms of backup.

v. Enable a second factor of authentication: an extra layer of security that can be enabled across multiple systems, whether by specific apps, mobile SMS or biometrics. Not all systems use double authentication, but the vast majority have adhered to this practice.

vi. Carefully scan all incoming emails to detect undercover threats and prevent intrusions. In general phishing emails features, fake email addresses, misspellings, suspicious links, urgent or threatening tone, irrefutable offers, unsolicited attachments, request for personal information, and lack of signature detail.

vii. Install Adblock, which is an extension that exists in all browsers and blocks any type of inappropriate content, such as malvertising13 which is a type of online advertisement that is generally used to spread malware on the internet.

viii. Segmenting the network is another recommendation to increase security by isolating critical points from shared access points.

No device is completely immune to a cyber-attack, but following the above recommendations is extremely important in prevention and mitigation.

2.6 WHAT IS BEING DONE

At matter published at magazine electronics gives computer world (COMPUTERWORLD 2021), IBM is leveraging Watson's analytics and machine learning capabilities to develop what she calls cognitive security, in which artificial intelligence systems learn to understand information terms and concepts to reduce threat detection and response time.. In the lecture by Guilherme Araújo, security leader at IBM Brazil (SECURITY LEADERS 2021), he explains that Watson for Cyber Security has been trained in partnership with 10 universities, including MIT, to effectively analyze this gigantic mass of structured data and unstructured, understand the nuances, ambiguities, and complexity of human writing, in order to better understand and interpret these threats in order to help security analysts respond more assertively and quickly to threats. When Watson is ready, it will be able to identify and correlate suspicious actions that happened on an endpoint, such as running an application from a spreadsheet. Which is not normal, but they are the main forms of attacks used by hackers to invade devices. In this way, it will be possible to shorten the total time required to address a potential threat To ensure the security of the Internet of Things in homes or businesses, it is recommended to segment the network by creating Vlans for each area, such as financial, commercial, ballroom, bedrooms, etc. This process, in addition to being laborious, requires specialized technicians both in implementation and maintenance. To make it easier, Cisco developed micro segmentation, a kind of badge not only for people but also for devices. The previously defined access policies are registered for all devices in the DNA18 Center (CISCO, 2018), a single platform that covers switches, routers and wireless networks. Thus, the badge of a device can circulate throughout the network accessing the equipment to which it is allowed access. According to its vice president of products and solutions, John Maddison (FORTINET, 2020), Fortinet, a global leader in high-performance cybersecurity solutions, also has products focused on the Internet of Things' security. It has a solution called the Fortinet Security Fabric that offers companies a comprehensive solution that spans the entire Internet of Things attack surface, providing the performance and threat intelligence needed to learn, segment and ultimately protect the various surfaces of attacks created for the Internet of Things. Above were Watson solutions that learn to interpret structured and unstructured data identifying potential threats, Cisco with its network segmentation solution based on the user profile and not the device, and Fortinet with firewall solutions that also identify and blocks threats. The implementation of this set of solutions, if well configured, will make the environment safe.

2.6.1 What to Do in Case of Invasion

In the suspicion that an invasion or contamination by a virus may have occurred in one or even in all the devices of the Internet of Things, the first step is to isolate that or those devices from the others, removing it from the network. Then contact a qualified technician who can identify the vulnerability and, if possible, the source of the attack or contamination. In more extreme cases it will be necessary to format the devices and configure them again. After the devices are "clean", regardless of whether or not they have been breached, change all passwords on all devices and try to enter new secure passwords. Despite all the investments that big tech companies are making in security, the weakest link remains the human being. So, don't believe everything you see on the device's screen, don't open emails and especially attachments from strangers, don't believe in miraculous promotions, change device passwords frequently, always with secure passwords and create a separate network for visitors limiting access. By following these steps, the security will still not be insurmountable, but it will help a lot.

3. ARTIFICIAL INTELLIGINCE AND IOT

3.1 OPTIMIZATION OF AI

Artificial intelligence AI occupies a very important place in operational research and computer science. Many applications are modelled as a problem of AI such as the traveling salesman, the multi-backpack and the task scheduling [50].

A combinatorial optimization problem (COP) is defined by a discrete and finite set of solutions, and an objective function (also called a cost function) to evaluate each solution. The best solutions (or the optimal solutions) are those which minimize (or maximize) the value of the objective function. Mathematically, a COP can be formulated as follows: Let S be the set of feasible solutions and $f : S \rightarrow \Re$ the objective function. A combinatorial optimization problem consists in finding a solution $s^* \in S$ minimizing (resp. maximizing) f, that is, $f(s^*) = \min_{s \in S}\{f(s)\}$ (resp. $f(s)^*) = \max_{s \in S}\{f(s)\}$).

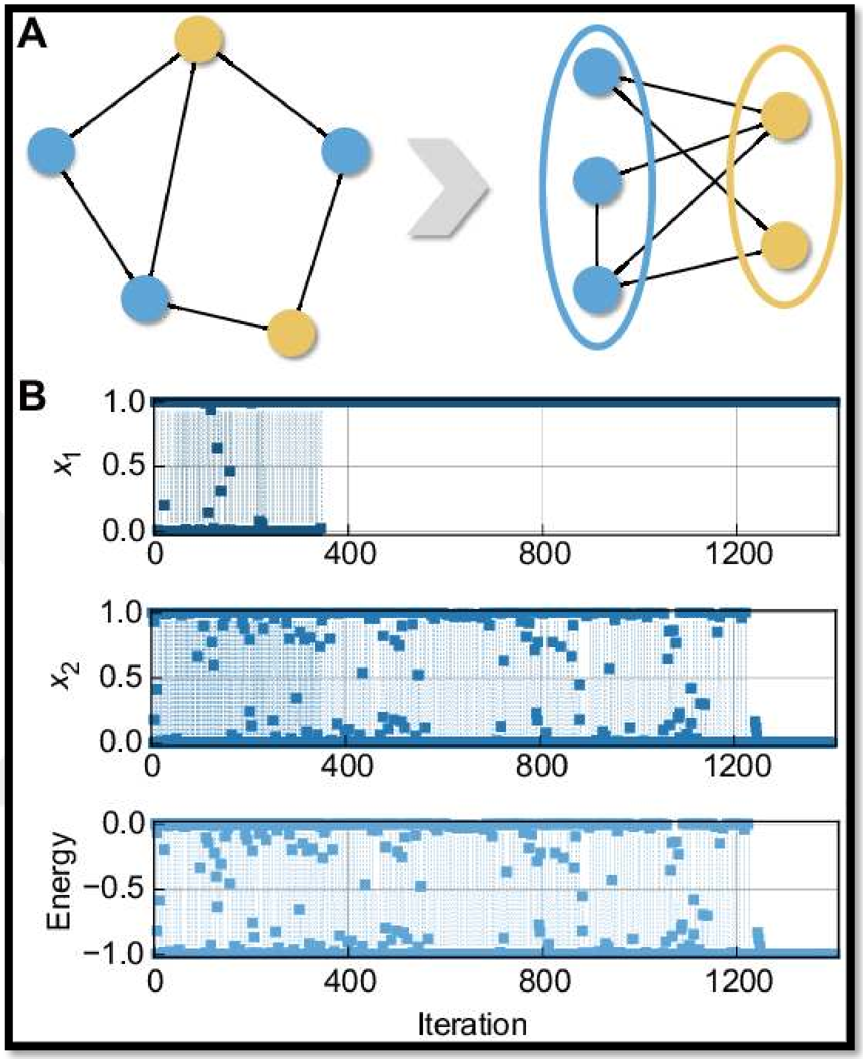

Figure 3.1: A combinatorial optimization problem (COP) [44]

Many methods have been proposed to solve the COP. These methods are classified into two categories: exact methods which guarantee the optimality of the solution found, and approximate methods which relax the criterion of optimality of the solution to gain in resolution time. In this thesis work, we are particularly interested, among the exact methods, in linear programming and, among the approximate methods, in heuristics and metaheuristics. Hereafter, we give some notions on the complexity of optimization problems. Next, we describe each of the methods cited.

3.1.1 Complexity of a COP

The complexity of a problem is the amount of resources (in number of instructions and in memory space) that an exact algorithm needs to find an optimal solution calculated on a Turing machine [20]. A problem is of polynomial (resp. exponential) complexity if there exists an algorithm allowing to find an optimal solution for all its instances in a polynomial (resp. exponential) time compared to the size of the instance. An example of a polynomial problem is to find all the shortest paths between pairs of vertices in a graph. The exact algorithm found by Floyd-Warshall [53] solves it in O (n3) polynomial time, where n is the number of nodes in the graph.

Below we list the different complexity classes for the COP.

i. The class P: one COP reduced to a decision problem is of class P if it can be solved, in an exact way, by an algorithm of polynomial complexity. We can cite for example the problem of calculating the shortest path in a graph.

ii. The class NP: one COP reduced to a decision problem is said to be of class NP if and only if, we can verify that any proposition is indeed a solution of the problem, in polynomial time.

iii. The class NP: complete: one COP reduced to a decision problem is said to be of class NP − complete if it verifies the following two properties: (i) it is possible to verify a solution in polynomial time, and (ii) all problems of class NP reduce to this via a polynomial reduction [50].

iv. The class NP: difficult: an NP − difficult problem is a problem which simply satisfies the second condition (quoted in the previous paragraph), and therefore can be in a larger and more difficult class of problem than the class NP.

We recall here that the problem addressed in this thesis (ie the optimization of the data placement in the Fog) is a class NP − difficult problem [76].

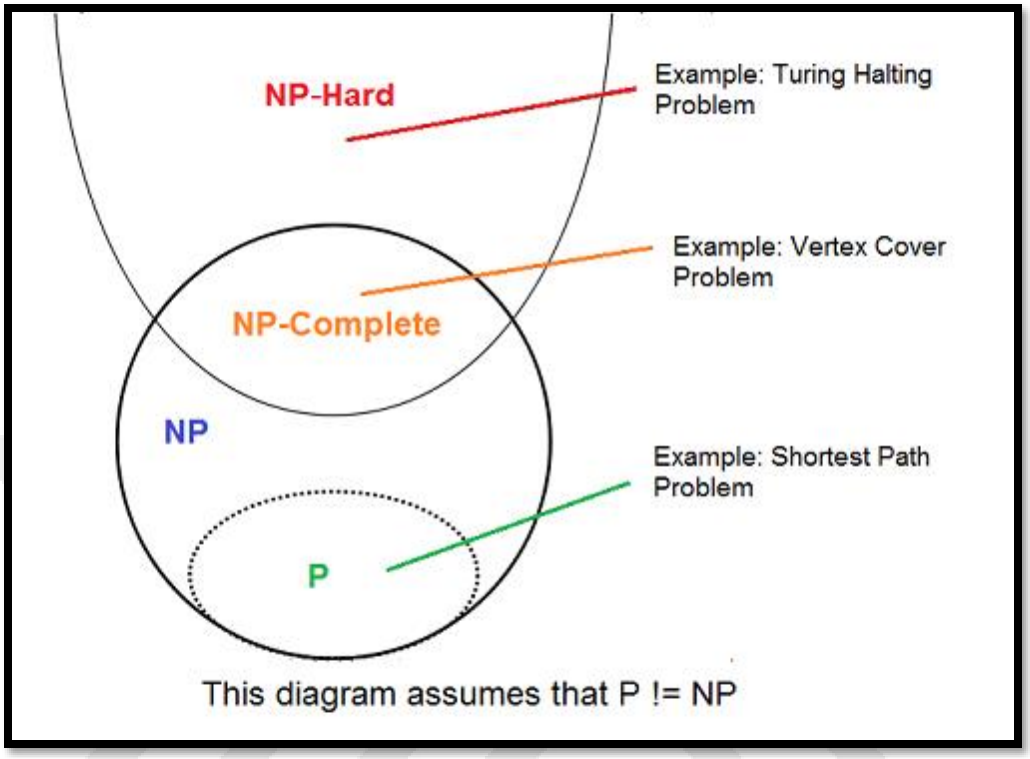

Figure 3.2: Levels of difficulty in AI based problems [53]

3.1.2 Heuristics

A heuristic is an approximation algorithm that often finds in polynomial time, at least one feasible solution, taking into account the objective function, but without assurance on the optimality of the solution found. In general, a heuristic is designed for a particular problem, by studying its structure (ad hoc heuristic). Heuristics can be classified into two categories [67]:

i. Construction methods: who build the solution by a series of partial and definitive choices. These methods are also known as greedy methods.

ii. Local excavation methods: which start from an initially complete solution and, in a repetitive way, try to improve this solution by exploring its neighbourhood in the search space. For example, descent methods substitute a neighbouring solution for the current solution if and only if the second is better.

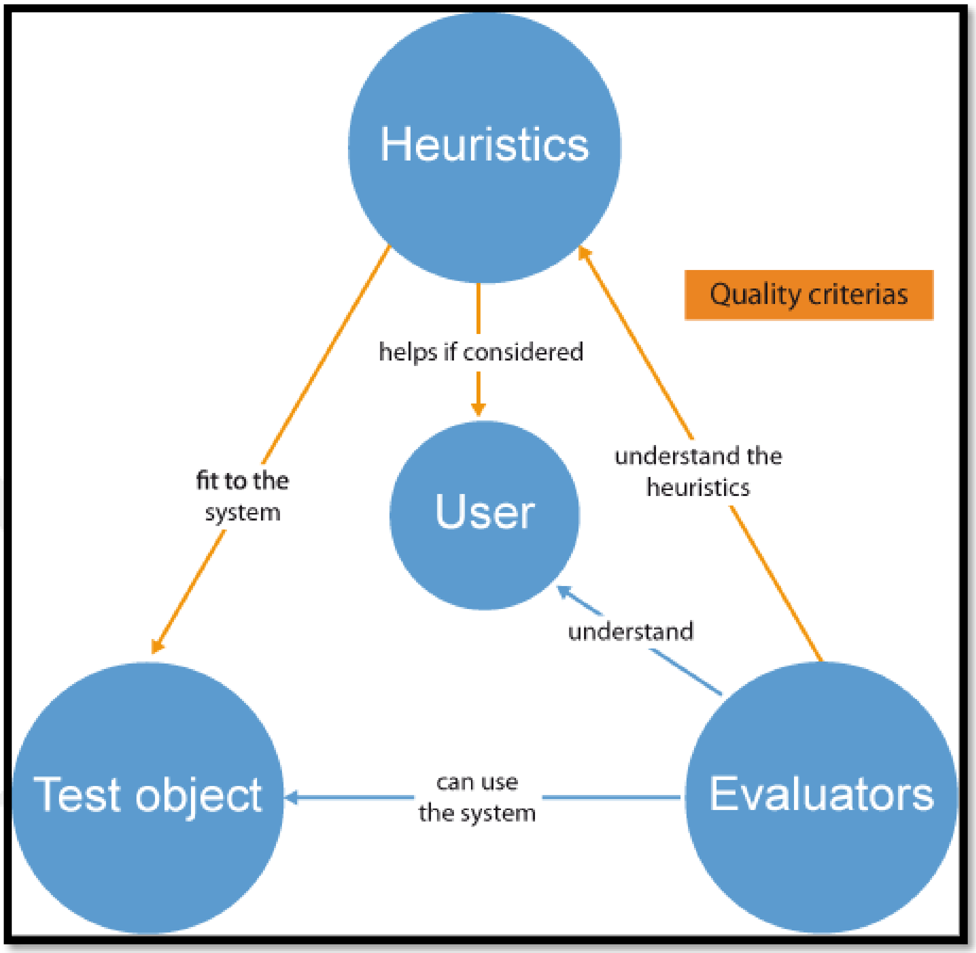

Figure 3.3: Heuristic approach to solving AI problems [67]

3.1.3 Meta-Heuristics

The previous heuristic methods can be trapped in a local minimum. In Figure3, a heuristic starts with an initial solution S, by exploring its neighbourhood, this heuristic returns the final solution which is a local minimum, i.e., an optimal solution in this part of the search space and not on a global scale of possible solutions. Meta-heuristics try to escape these local minima by temporarily accepting solutions that do not improve the objective function [79]. Metaheuristics provide a general method for exploiting the space of solutions and seek a compromise between the exploitation of this space and the exploration by local improvement of the solutions found. A meta-heuristic can be adapted for different types of problems, while a heuristic is dedicated to a given problem. Several meta-heuristics are inspired by natural systems in many fields such as: biology (genetic algorithms) physics (simulated annealing), and also ethology (ant colony algorithms).

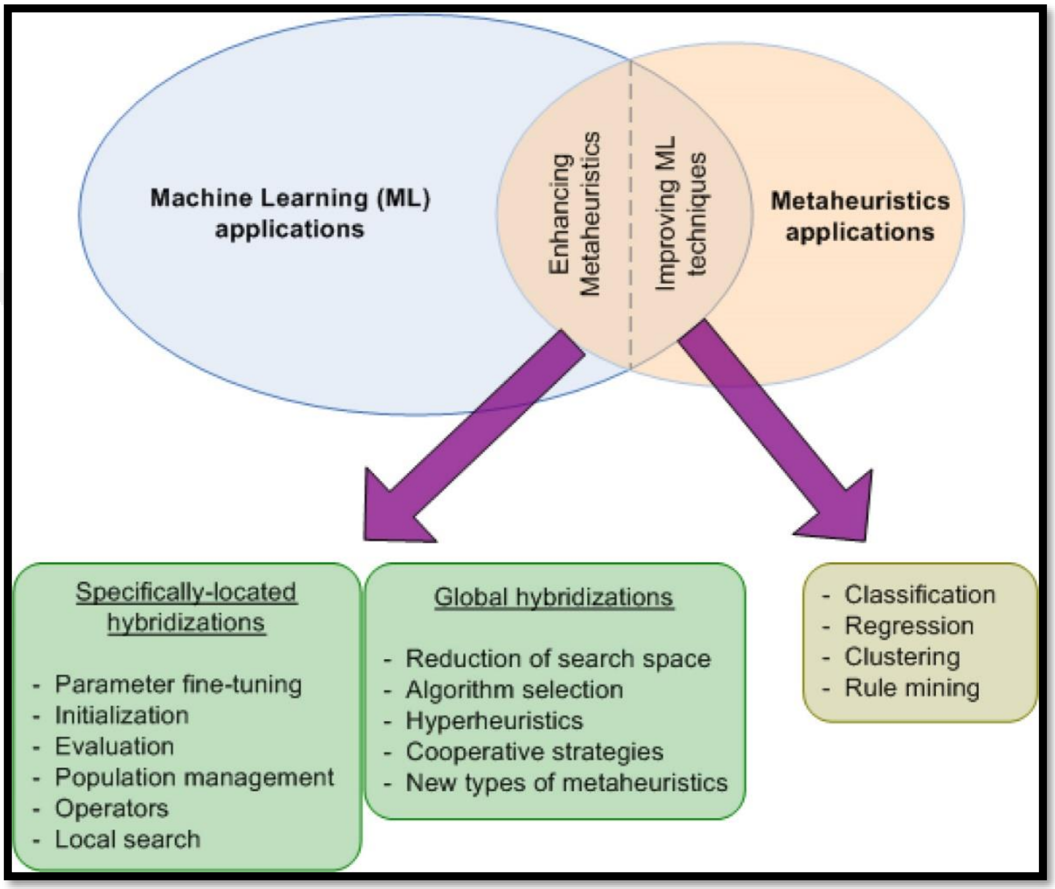

Figure 3.4: Metaheuristic approach to solving a problem [50].

i. Genetic algorithms (AG): are algorithms inspired by the theory of evolution. A typical evolutionary algorithm is composed of three essential elements: (1) a population consisting of several individuals representing potential solutions to the problem in question, (2) a mechanism for evaluating the adaptation of each individual in the population to the respect to its external environment, and (3) an evolution mechanism composed of operators allowing the elimination of certain individuals and the production of new individuals from the selected individuals.

ii. Simulated annealing: it is a method based on local search. That is, exploring the neighbourhood space of the current solution to find a better solution. But, in these methods, an unfavourable solution can be accepted (according to a probability which decreases during the algorithm) as a current solution in order to escape the local minima.

iii. Ant colonies: these are algorithms inspired by the behaviour of ants when they seek the shortest path between their nest and a source of food [48]. Their principle consists in allowing an ant to choose the shortest path between the nest and the source of food by taking the path most used by the other ants (using a pheromone). In this category of metaheuristics, each solution is considered as an ant moving on the search space. The ants mark the best solutions, and take previous markings into account to optimize their search

In this section, we have seen that there are several complexity classes for COP. Also, there are several ways to solve them: exact, heuristic and metaheuristic. Depending on the resolution method used, the optimality and the search time of the solution are different.

3.2 ARCHITECTURE MODEL OF THE CONSIDERED SYSTEM

In this section, the contributions to this thesis are outlined, together with the underlying architectural model, notations, definitions, and assumptions that supported the development of those contributions.

3.2.1 System Architecture

A notable use of the Internet of Things is the "smart city" [93]. By empowering urban residents with smart solutions for their transportation, home automation, health, energy, and water needs, etc., the plan aims to enhance the quality of life in urban areas for all. Many of the aforementioned functions can be coordinated by a single "smart city" app. Information between these platforms is possible. The home automation service, for instance, may make use of information gleaned from the energy management service.

In this paper, we consider a generic "smart city" [39] system deployed in a fog-like architecture, complete with sensors, fog nodes, data centers, and Internet of Things (IoT) service instances.

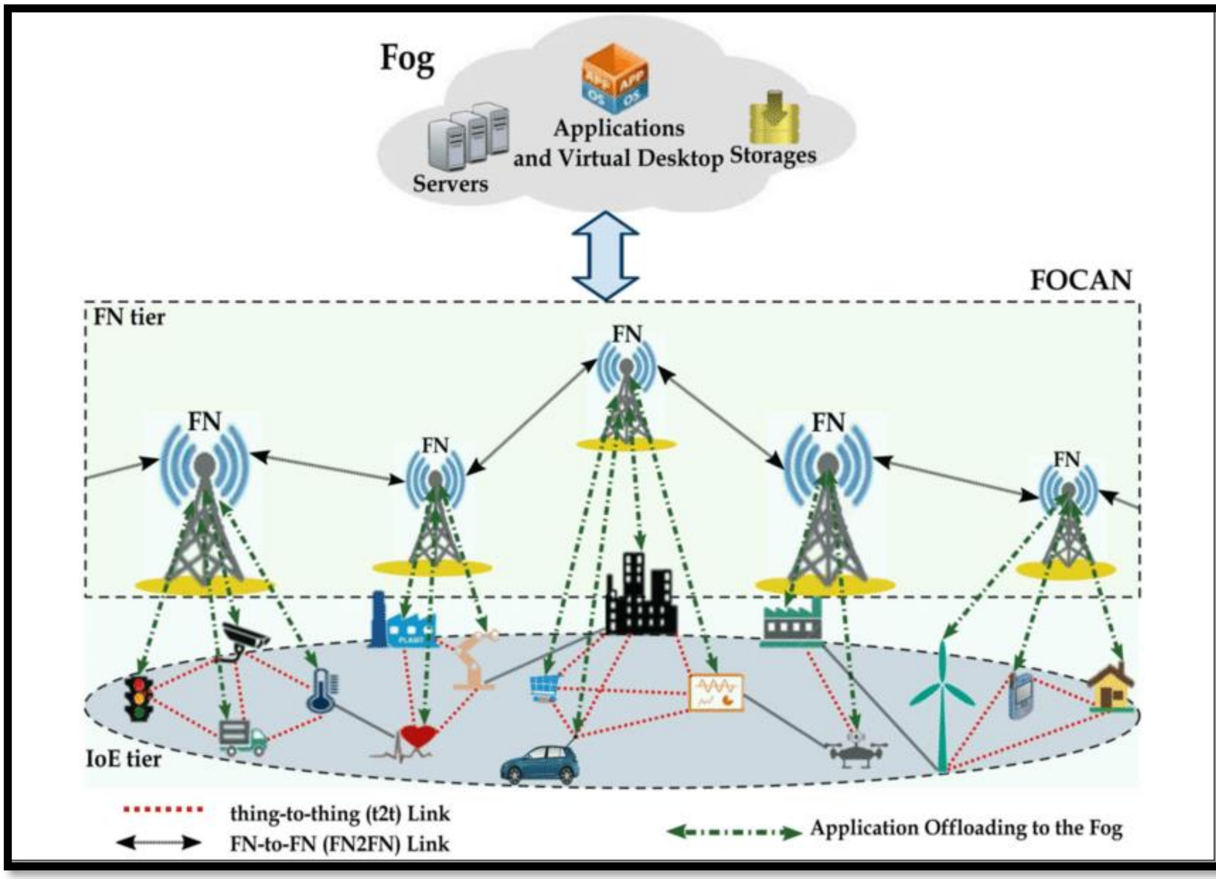

Figure 3.5: System infrastructure of a smart city scenario deployed in Fog [49]

In this system, each service instance is deployed in a single fog (or cloud) node chosen by a service instance orchestrator. The orchestrator is an entity that has a partial or global view of the infrastructure (latencies, performance, etc.) and manages the placement of service instances [94]. The choice of the node is based on several criteria, in particular that of the available resources, the desired level of security or the availability offered by the chosen node [94].

In this scenario, the sensors considered as data producers collecting information related to the physical environment (eg temperature values). This information is sent to associated service instances through gateways. Then, the recipient service instances considered as data consumers process the information sent to make decisions or act on the environment (eg turn off the heating or trigger an alarm). However, these service instances may in turn produce other data. In this case, these service instances are considered both producers and consumers of data. The data produced in our system can be stored in different nodes of Fog and data centers of the infrastructure.

In the following sections we give the different definitions, assumptions and notations used in this thesis work.

3.3 SERVICE INSTANCE PLACEMENT SOLUTIONS OF IOT IN THE FOG

The concept of the "smart city" is an innovative Internet of Things application [39]. The strategy aims to improve the overall quality of life in urban areas by giving inhabitants with access to innovative technologies that can assist them in meeting a range of needs, including those connected to transportation, home automation, health, energy, and water, among others. A single app intended for "smart cities" can serve as the coordinating hub for a number of the tasks listed above. Information transfer between these two platforms is possible. It is possible, for instance, that the home automation service will utilize the data gathered by the energy management service.

In this study, we investigate a general system for "smart cities" [39] that is constructed using a fog-like architecture. This system consists of sensors, fog nodes, data centers, and instances of Internet of Things (IoT) service).

3.3.1 Linear Programs

In a fog computing environment, [87] proposed an infrastructure that would deliver a range of resources. They created a model based on integer linear programming to determine the optimal approach for spreading work (or service instances) across clusters of Fog nodes (called Fog colonies). Each cluster is governed by a strong fog node that serves as its brain. As a broker and task orchestrator, the latter collects and distributes work orders that have been sent from specific nodes in the cluster. Cloud computing is utilized for tasks that cannot be performed elsewhere, often owing to a lack of resources. Their task placement methodology aims to I maximize the number of completed jobs inside each cluster (and, consequently, CPU, RAM, storage, and bandwidth) and (ii) locate the node that is physically nearest to the controller in terms of latency. I. Optimizing the Number of Completed Tasks Within Each Cluster

However, the purpose of the suggested model does not take into account the amount of time necessary to complete the work. Undoubtedly, the authors operated under the assumption that all Fog nodes behave identically inside each cluster. When choosing where a job will be assigned, the sole consideration examined is the amount of time it takes for data to flow between the controller and the node. In reality, the processing performance (CPU and RAM) of Fog nodes is highly variable, resulting in a spectrum of execution times. Because of this, the authors proposed in [88] that their task allocation model may be improved by imposing time limits on each activity. These constraints would define the maximum time that could be allocated to each task.

Motivated by availability constraints, Nader et al. [46] formulated the task placement problem in a fog environment as an integer linear program. This strategy was utilized to fix the issue. Their solution facilitates the replication of a user's task over many Fog nodes to achieve the necessary level of availability. In reality, they assigned: I an availability value to each Fog node; II a realization cost to each job; III a maximum budget for each user to complete its duties; and IV a maximum duplication value of a task to each user. The cost of realization was the same for all Fog nodes. Using the objective function of their model, they were able to determine how to allocate the available resources so that each user had access to the level of service that best fulfilled their demands at the most cost-effective price.

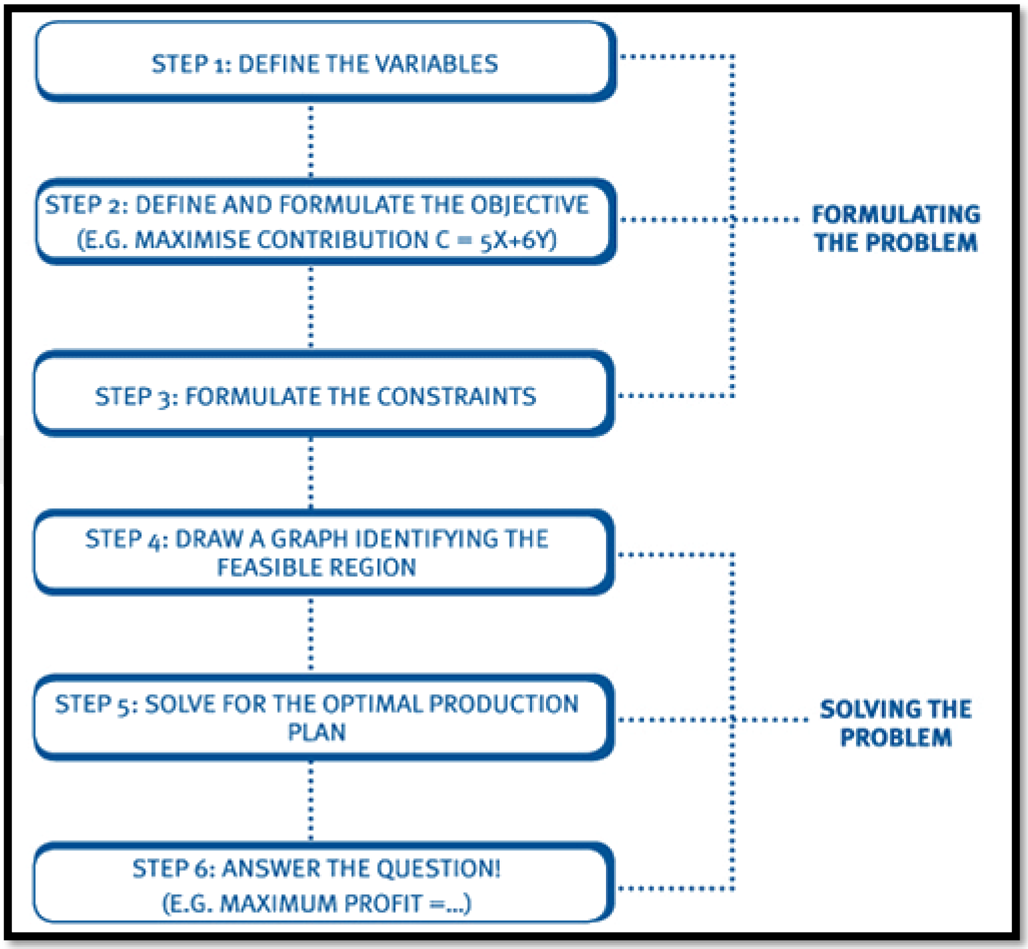

Figure 3.6: Linear programming for solving a problem [91]

The identical price shows a possible flaw in their model. Cost can be assessed in a variety of ways, such as the length of time required to complete a task, the amount of energy it uses, the amount of bandwidth it consumes, or any other applicable factor. In addition, the throughput and access latency of individual Fog nodes vary significantly. This shows that the cost of completing a task will vary based on the specific Fog node used to do it. One option to improve the effectiveness of their strategy is to assign a different price to each conceivable combination (task, Fog node). These expenses may be affected by a variety of factors, including those addressed thus far.

To optimize the placement of Internet of Things devices, services in the Fog, Velazquez et al. [94] devised a methodology based on the ILP program. I lowering the number of existing hops between the sites of the cooperative services; II reducing the number of hops between the locations of the cooperative services; and III reducing the total number of service migration by relocating many services (for example).

3.3.2 Heuristics

In [25], the authors proposed: (i) a formulation MILP the service instance placement problem in a Fog infrastructure and (ii) several heuristic-based policies for service instance placement. Their overall idea is to place the service instances in the Fog infrastructure without the use of an orchestrator (global or partial) which requires knowledge of the system infrastructure (ex. latencies, available performance, etc.) . Indeed, in their policy, each Fog node deploys a placement algorithm and behaves independently of the others. In order to choose the Fog node that executes a task, the authors associated each task with a maximum response time. Upon receipt of the tasks, if this time is satisfied by the receiving Fog node and if this node hosts an instance of the requested service, then the task is executed in this node. Otherwise, it is redirected to the next node in the hierarchy. If none of the nodes is chosen, the task is thus redirected to the Cloud. Furthermore, for the placement of service instances, each node counts the number of accepted and rejected tasks, as well as the average response time required by all the tasks. Then, according to these two metrics, the Fog node chooses the service instance that will be kept running.

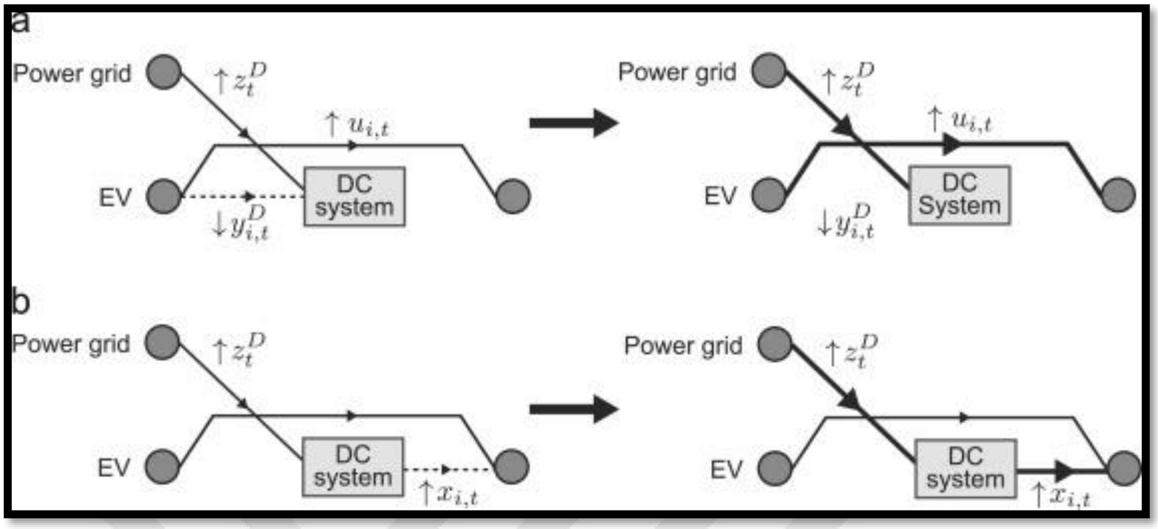

Figure 3.7: Linear program heuristic [12]

Gu et al. [60] developed a linear programming-based model and heuristic for work placement in a Mobile Edge Computing environment using the same decentralized task management concept. This task allocation model and heuristic were developed. Their approach accomplishes this by ensuring that the required response times for tasks are satisfied, thereby optimizing the amount of global energy spent as a result of the execution and transmission of tasks. The server nodes, which are actually performing the task, interact inside their heuristic to share the performance metrics they acquire (the frequency of theCPU). Each job is sent to a possible server node by the individual who originally developed it. The node that will be utilized is determined by an energy-based function. When a node receives a task, one of two possible outcomes could occur: I the node could meet the required response time, in which case it could process the task locally; or (ii) the node could fail to meet the response time, in which case it could send the task to a neighboring server node based on the nodes' aggregated performance data. Depending on whether or not the node reaches the response time, each of these scenarios is possible. It is possible to decentralize the algorithm for task placement because tasks are assigned based on information already known by multiple nodes. We do not utilize task orchestrators since doing so would necessitate the employment of one or more, which would prevent the placement method from being scalable.

A approach comparable to that described by Gu et al. [60] is proposed in [100] as a means of placing tasks within a Fog framework with the aim of decreasing the system's overall latency. In order to determine where to locate fog nodes, the suggested method utilizes data collected from other fog nodes regarding their own performance. In addition, probabilistic models have been developed to estimate the time required to accomplish a task within a Fog node.

Taneja et al. [90] offer a heuristic for the deployment of service IoT instances within a Fog architecture. They propose a system in which I I Fog nodes are ranked according on their processing performance and (ii) service instances are ranked based on the quantity of resources they demand. Next, they will do heuristic searches for each unique service instance to identify which Fog node will offer the highest processing performance. A service instance is uploaded to the cloud when it cannot be located.

Although simple to comprehend and straightforward to implement, the offered heuristic has a number of limitations. It does not seek to spread the burden uniformly across the many Fog nodes, nor does it consider any constraints on the execution duration of the instances. If only one node can meet the needs of all service instances, their heuristic allocates all service instances to the Fog node with the lowest performance, even if additional accessible Fog nodes are available. Alternatively, the response time of these service instances may have been reduced through the use of parallelization, which required the installation of service instances on separate nodes. To minimize delay and optimize performance, it would be ideal if each service instance could be assigned to a single Fog node. The ability to avoid deploying service instances on nodes situated in different regions of the world is a major advantage of this method. In addition, in order to resolve the workload balance issue, you will need to replace the co-located service instances many times with instances located in available or faster-responding Fog nodes.

3.3.3 Meta-Heuristics

In their study [72], Mebrek and colleagues presented a genetic algorithm as a meta-heuristic with the intention of optimizing the placement of jobs within a Fog infrastructure. This was done in order to maximize efficiency. Their strategy cuts down on the amount of wasted energy during the transfer and execution of jobs, all while maintaining the required response time for each operation. According to their model of optimization, the time it takes to send a task, the time it takes to complete the work, and possibly the time it takes to redirect the request to the cloud are all factored into the response time of a project (in the case of insufficient resources). On the other hand, the rate of energy consumption is calculated by adding up all of the energy that is used throughout the processes of transmitting the request across the network, processing the request, and storing the response. This is done in order to determine the total amount of energy that is consumed during the process.

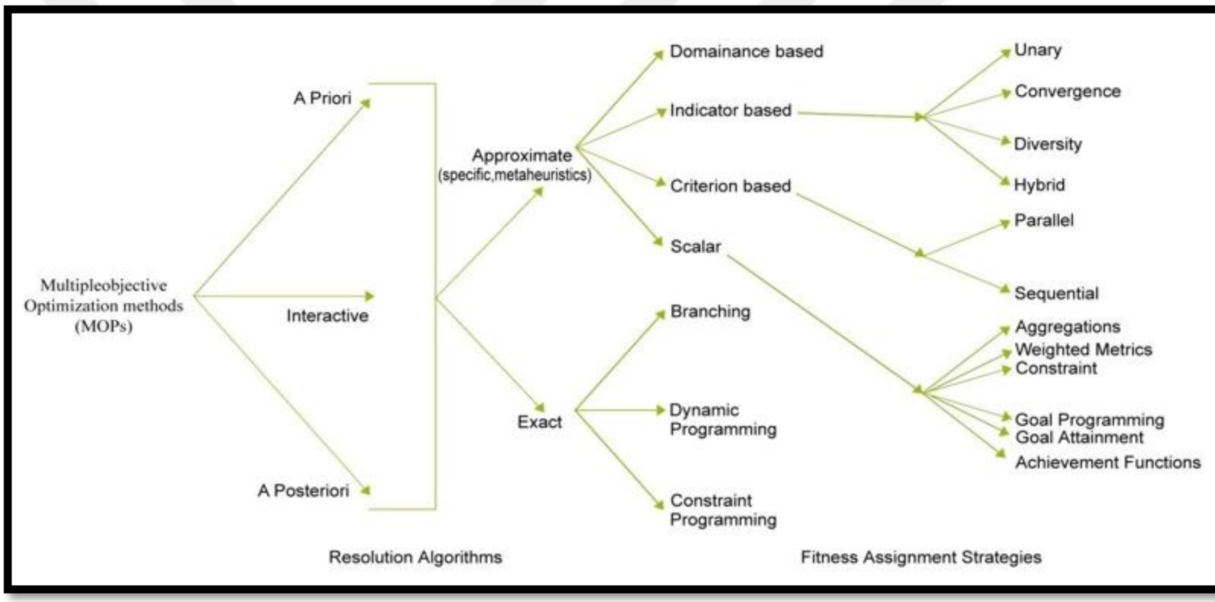

Figure 3.8: Linear program metaheuristic [60]

3.3.4 Others

The challenge of the placement of IoT in the fog is stated as a nonlinear program that respects limitations on QoS in terms of response time in [101]. This topic was posed by the authors of [101]. When formulating the objective function for their approach, they took into account the amount of time required for processing, communication, storage, and service deployment. The model that has been suggested incorporates constraints to do the following: I restrict the average response time of all the services; (ii) respect the resources that are available in the Fog nodes; and (iii) limit the number of violations of the ALS in terms of response time. Two different heuristics were presented by the authors as potential solutions to the placement issue. The first one optimizes location in order to limit infractions of the ALS, while the second one optimizes placement in order to decrease the amount of money the system spends on operations.

Ye et al. [95] came up with a more complicated model to optimize the positioning of service instances in the fog. The objective purpose of their model is to reduce, as much as possible, the amount of time that is typically required to respond to the various service requests that are made. In addition to imposing limitations on latency, available resources, and bandwidth, they restricted the places to which a given instance could be moved. Instances, for instance, can only be installed in specific fog nodes so as not to violate anyone's privacy. An precise algorithm as well as two heuristics have been proposed for putting service instances by the authors, and they have been based on Backtrack Search Algorithms. On the other hand, the authors made the assumption that the amount of time it takes to run an instance does not differ depending on where it is run. As was discussed earlier, the performance of different fog nodes might vary widely, which can affect the total execution time.

3.3.5 Synthesis

In this section, we have seen that the problem of placing service instances IoT in the Fog has been studied using several methods. Researchers have proposed linear programs to solve this problem and others have proposed heuristics to reduce placement time in large infrastructures. These heuristics are based on two approaches: (i) those that use one or more service orchestrators and (ii) those that do not. The advantage of the first approach is that these methods can achieve efficient placement, but they rely on knowledge of the state of the system that is difficult to collect. Conversely, the methods of the second approach in which each node behaves independently of the others achieve rapid placement and no single point of failure, but lack of knowledge about system state can lead to misplacement (eg load balancing issue). Also, other authors have proposed exact algorithms for placing services. But, given the great complexity of the system, these algorithms are inapplicable in reality. Moreover, investment methods based on metaheuristics are very rarely offered in this context. This comes down, in our view, to the novelty of the Fog computing paradigm which is still in the initiation phase. Investment methods based on metaheuristics are very rarely offered in this context. This comes down, in our view, to the novelty of the Fog computing paradigm which is still in the initiation phase. Investment methods based on metaheuristics are very rarely offered in this context. This comes down, in our view, to the novelty of the Fog computing paradigm which is still in the initiation phase.

In this thesis, we propose three strategies for data placement of the IoT in Fog frameworks, in the form of an exact approach and two heuristics. In these strategies, we implement orchestrators that place data in one or more partitions of the infrastructure in an independent way in order to reduce the time to resolution. The problem of load balancing between Fog's nodes (see the paragraph discussing the work [90]) is processed at the partition level by the data orchestrators because they have a view of the managed partitions. Also, the dependence of the placement cost on the chosen nodes (see the paragraph discussing the work [46]) is also supported in our solutions. On the other hand, we did not consider a limit on the data transmissions, this can nevertheless be added to our linear program model.

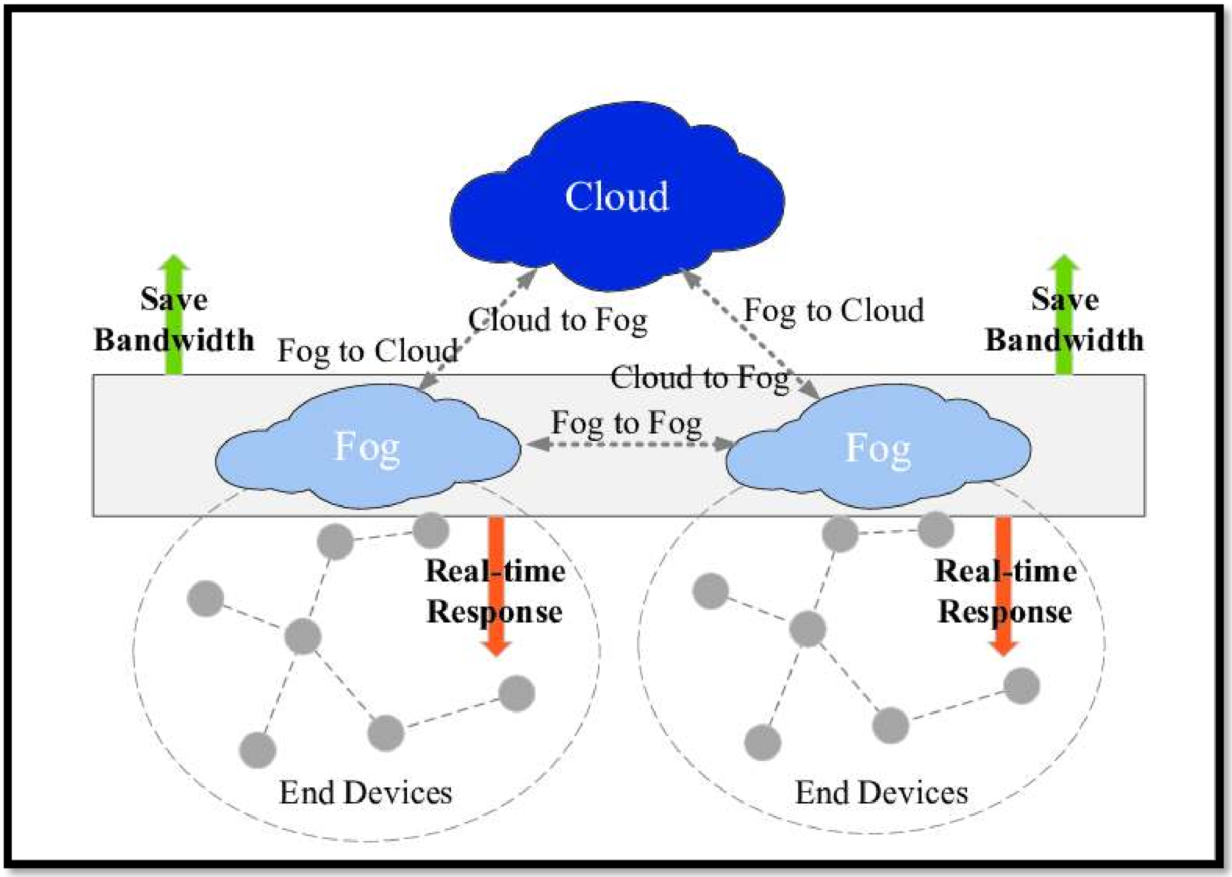

Figure 3.9: IOT and Fog system [46]

3.4 TOOLS FOR EVALUATING DATA PLACEMENT SOLUTIONS IN THE FOG

This section summarizes cutting-edge research on data placement management in the context of fog and IoT. Table 2 depicts a classification of existing work on the deployment of fog and IoT based on four criteria:

i. data placement management

ii. Taking into account the environment of Fog.

iii. The modelling of connected objects.

iv. The type of tool proposed among S (simulation), E (emulation) and R (real platform).

We recall here that each method has advantages and disadvantages. For example, simulations are less costly in terms of evaluation time and implementation budget but their results are not precise. Emulation is more expensive but more accurate than simulation whereas real rigs are very expensive but more accurate in terms of results.

3.4.1 Real Platform

In [23], Adjih et al. proposed FIT-IoT-LAB, a large-scale federated experimental platform for the design and comparison of IoT protocols, applications and services.IoT. It includes 2,700 wireless physical sensors including 117 mobile robot nodes deployed at six sites in France. This platform does not integrate Fog nodes or data placement strategies.

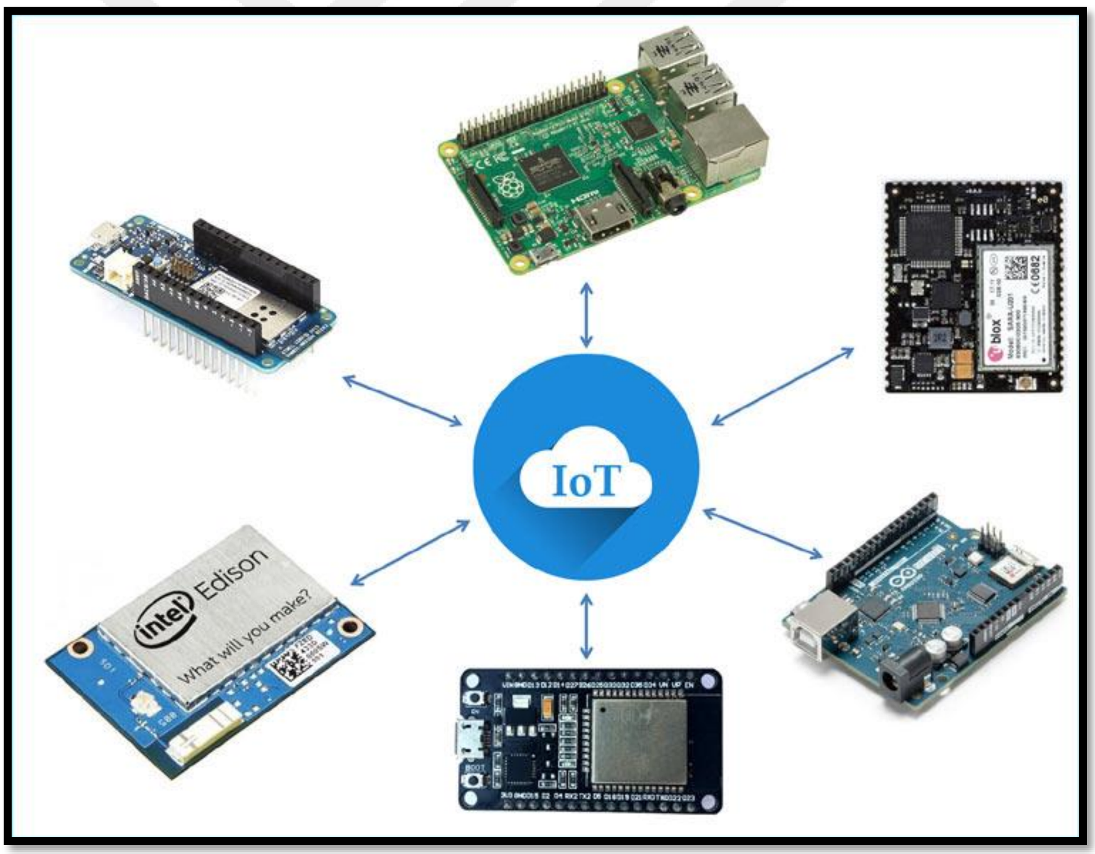

Figure 3.10: IOT hardware devices [71]

3.4.2 Emulator

Regarding emulation-based tools, Mayer et al. proposed EmuFog [71], and Coutinho et al. have introduced Fogbed [43], two Fog environment emulators. Both consider Fog infrastructures including switches and routers but they do not emulate connected objects. However, Fogbed uses simulation to manipulate connected objects. Moreover, these two emulators do not integrate the management of data placement. Due to the high density of Fog infrastructures, emulation-based solutions can be very expensive in terms of resources and emulation time (several weeks or even months).

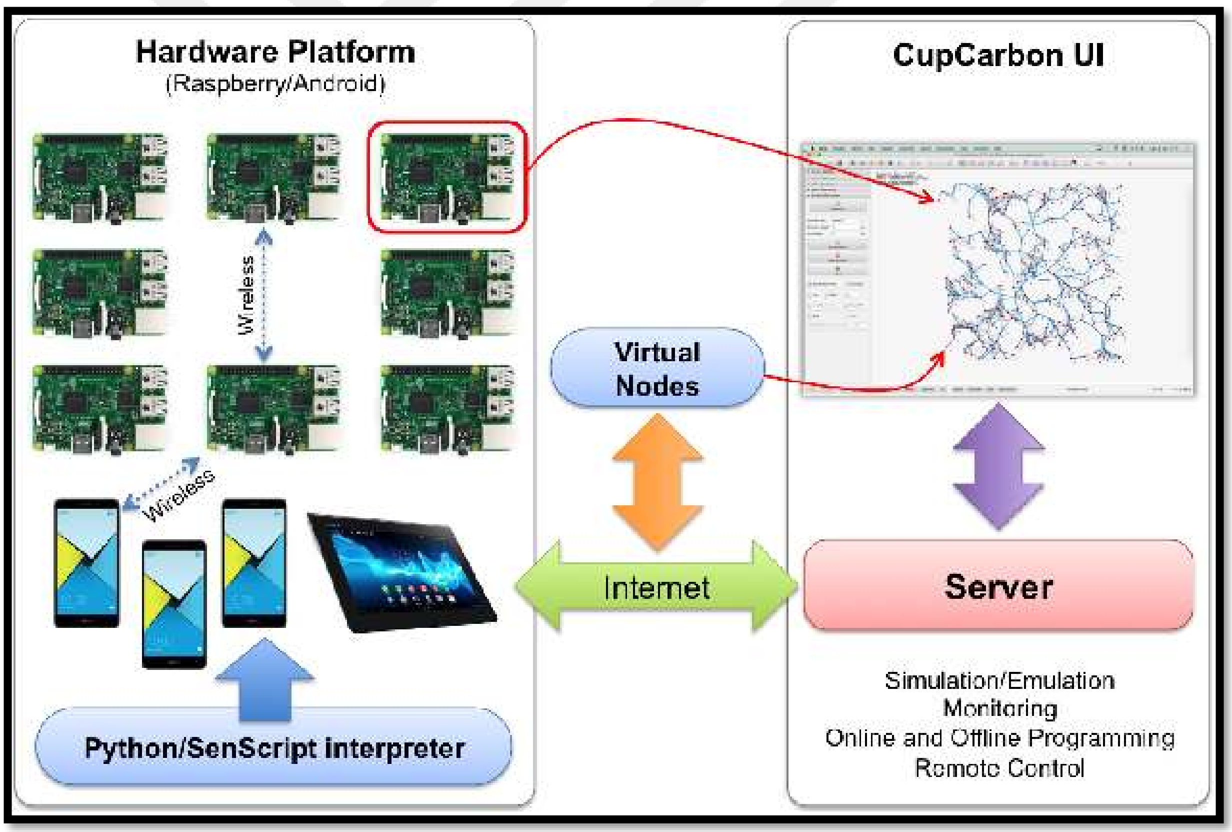

Figure 3.11: IOT emulation software [71]

3.4.3 Simulator

a simulator of peer-to-peer environments and Computing Grids. It makes it possible to model and simulate grid resources and networks, and to evaluate solutions for allocating and scheduling tasks, and finally to manage the placement of data in the simulated infrastructure. However, there is no dedicated support for fog environments andIoTin GridSim. Thus, users need to define Fog node models and Fog objects.IoTin order to implement their data placement strategies in this context.

a Fog environment simulator in order to be able to assess the impact of the use of Fog in terms of service latency. Their simulator simulates data centers and fog nodes, but it does not simulate the connected objects or the management of data placement in the simulated infrastructure. In [32], the authors introduced FogTorch. This is a prototype environment simulator of Fog andIoT. It was used mainly in [32] for the implementation of an algorithm to find the deployment of an application ofIoTin a Fog infrastructure. This deployment is constrained by various Latency and bandwidth requirements for quality of service. Fog Torch takes as input the specifications (a static model) of the Fog infrastructure, the application to be deployed and the Sequester in terms of latency and bandwidth, and outputs the deployment solution that meets these requirements. On the other hand, the simulation of the behaviour of the environments of Fog and of IoT is not yet deployed in Fog Torch (at the time of writing this manuscript): simulation of sending, processing and storing data has not been implemented in this simulator. These features are needed to evaluate the dynamic behaviour of user policies (eg for data placement) following different state changes.

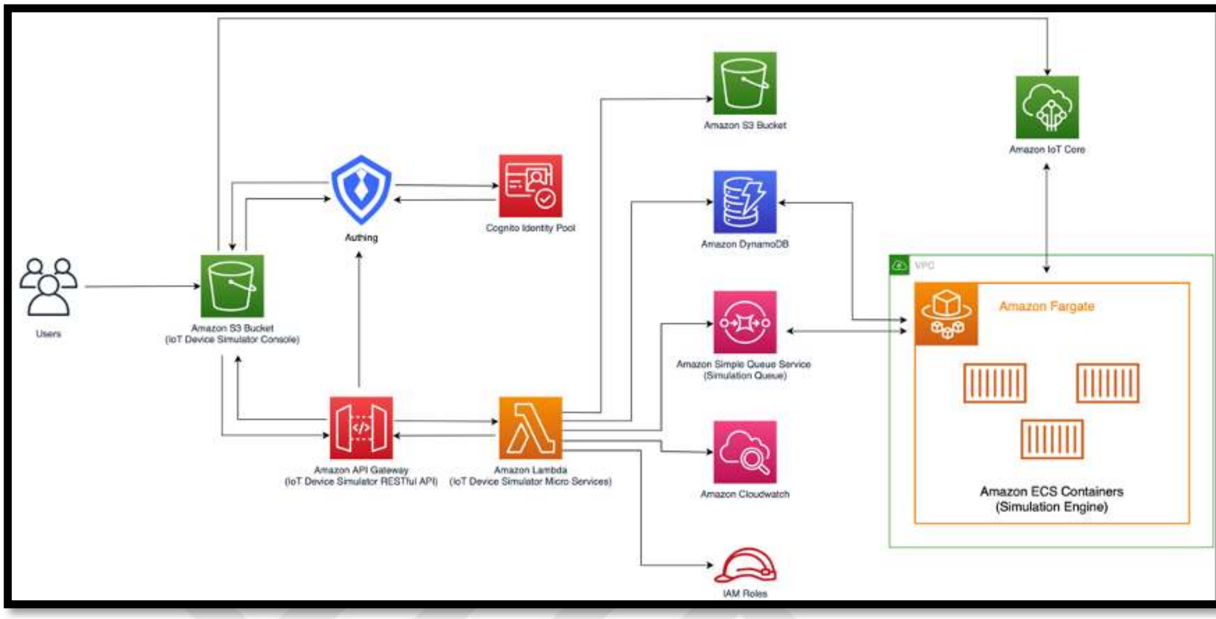

Figure 3.12: IOT simulation software [82]

In proposed I Fog Sim, a simulator of Fog environments and IoT. This software simulates infrastructures with millions of connected objects and thousands of fog nodes (and cloud data centres). It allows users to define and implement their resource management solutions for service placement and scheduling. IoT in the simulated infrastructure, and measure the impact in terms of service latency, network congestion, energy consumption and operational cost. However, data placement management is not implemented in this simulator.

3.4.4 Synthesis

Given the characteristics of I Fog Sim (scaling up, modelling of Fog and IoT), we chose to adapt this simulator to implement and evaluate our data placement management strategies. In addition, this simulator has been used in the context of numerous works in the context of Fog and IoT [30]. we propose an extension of this simulator allowing to deploy and evaluate data placement management strategies in the context of Fog and IoT.

4. PROPOSED METHODOLOGY

4.1 SYSTEM OUTLINE

The internet of things (iot) is a network that connects computer devices sensors, and other nodes. this network then sends the data received from these sensors to a central data repository, also known in some situations as a "sink." the term "internet of things" (iot) can also be used to refer to a system that consists of a variety of devices located in different parts of the world and that work together to capture and store data regarding the physical status of the environment. The internet of things is being utilized not only by the military, but also by the medical industry, the government, and even ordinary households. Failure tolerance, scalability in production, cost, operational environment, transmission medium, and power consumption are but a few of the numerous factors that may influence the architecture of a device network. There are plenty other factors to consider. Therefore, conducting research into energy-efficient transmission techniques for live events is a significant challenge that must be overcome. a static technique, such as that used in forest monitoring, and a dynamic strategy, such as that used in target tracking, are two examples of the numerous types of monitoring techniques necessary for diverse objectives. These procedures are examples of the various monitoring tactics that must be implemented.

4.1.1 IOT Activation

When an Internet of Things is activated, a sequence of steps are taken to establish the network's essential architecture. These actions are required for the network's establishment. These operations include the distribution of device nodes and the routing of data transmission. The normal operation of the apps running on the device node is dependent on the effective completion of both of these tasks. Each individual node is responsible for determining which other nodes it is theoretically capable of establishing direct connections with, and the radio power of that node must be sufficient to ensure connectivity.

Typically, Internet of Things-connected devices are configured to monitor either continuous activities or isolated events. Taking readings of constant variables such as temperature and humidity is a method that can be characterized as being relatively straightforward. In contrast, cases of uncooperative occurrences are examples of dynamic occurrences. These may include the movement of whales in the water or an unwanted vehicle on a battlefield. Due to their erratic up-and-down movement, it may be challenging to monitor them. There is a protocol that must be adhered to in order for device networks to perform to their fullest potential. To exemplify this notion, a protocol could be developed in the form of an application that follows a specified sequence in order to achieve the goals of data collection and power consumption. This kind of network construction is referred to as hierarchical routing. Hierarchical routing is the very definition of the term. In addition, we have a data centric routing protocol that describes a network configuration in which a device node employs a data centric approach to application delivery in order to choose the best route from multiple sources to a single destination. This protocol also incorporates a data-centric approach to application delivery. In addition, this protocol handles the distribution of applications using a data-centric manner. Due to this, the data held on each node can be described by a collection of attribute-value pairs known as attribute-based addresses, and the availability of each node can be broadcast to the remainder of the device network. Attribute-based addresses are a sort of address that is determined by the attributes of the addressed object. Due to the often tiny amount of power made accessible to individual nodes in IoT networks, it is of the utmost significance that the consumption of this power be reduced as much as is practically possible. There is a correlation between a growth in society's reliance on IOT network technology and a subsequent increase in the complexity of individual networks and an increase in the future number of networks. This is because a growth in society's reliance on IOT network technology is connected with a rise in the future number of networks.

Internet of Things devices are often powered by batteries, meaning that the nodes that comprise these devices have restricted access to power and a limited energy budget [1]. If we want the devices to continue running for as long as feasible, every component of the network must be precisely designed to consume the least amount of energy physically possible. The Internet of Things (IoT) could benefit from the organization of devices into clusters, with each component talking only with the "cluster head" (CH) of the cluster and the CH transmitting the aggregated data to the base stations. This configuration would permit more efficient data collecting. This is one of the several techniques that may be taken to reduce the Internet of Things' energy consumption. To reduce the amount of energy required to carry data from nodes to the base station, devices must be arranged in clusters. This is achieved by device clustering.

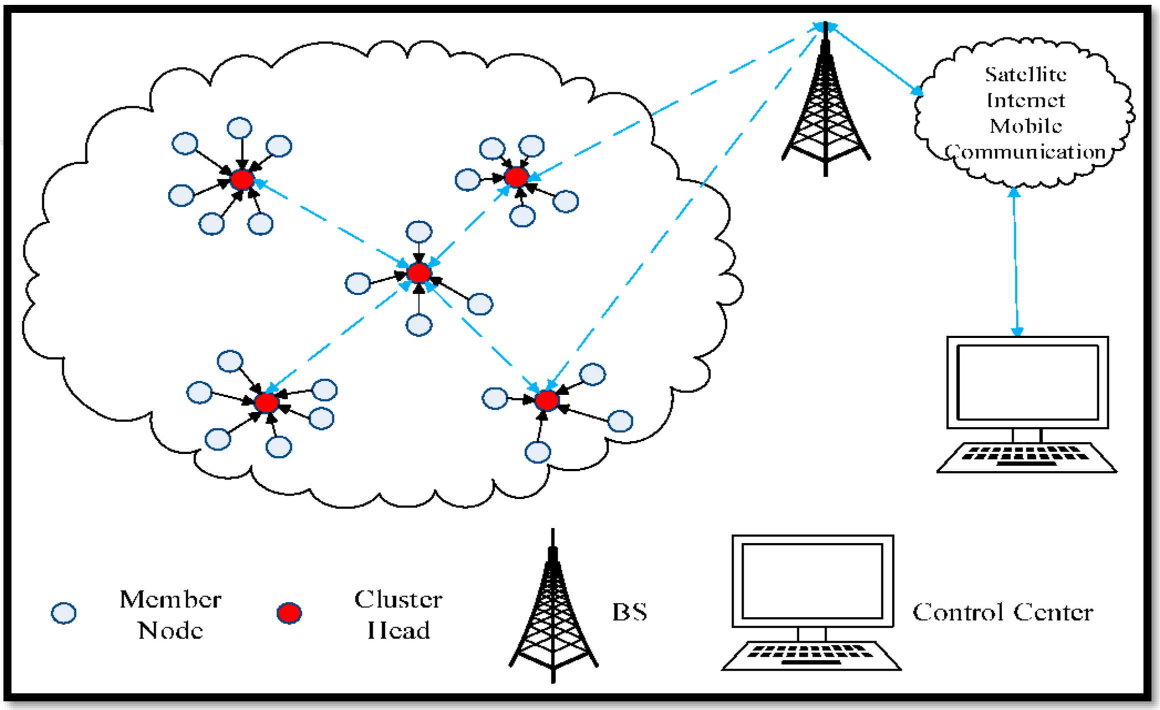

Figure 4.1: Structure of IOT and WSN system [12]

4.1.2 Routing Protocol Analysis for IOT

In recent years, the "Internet of Things" (IoT) has developed as a relatively new phenomenon in the field of information technology. Intelligent interfaces allow things with identities and virtual personalities to interact with one another, as well as with the social environments in which they are embedded and the human users of those environments. Moreover, intelligent interfaces allow these objects to engage with the social environments in which they are embedded. A protocol known as "routing" specifies how routers exchange data that enables them to determine the most efficient paths between any two network nodes. This enables routers to determine the shortest and most direct route between any two network nodes.

Due to the limits imposed by IoT systems, a routing protocol that satisfies a predetermined set of criteria and implements a variety of techniques is required. This is because a routing protocol that satisfies a predetermined set of criteria is vital. Two of the most significant factors to consider when it comes to a system of this type are its energy efficiency and its capacity to support the regular traffic flow in the area. Memory and processing power must be able to properly adjust to irregular changes in location and size. It is of the utmost importance that a routing system for the Internet of Things can identify and avoid inefficient one-way networks while minimizing the amount of energy wasted during transmission. Mobility and the ability to use IPv6 are two highly sought-after qualities. Both of these features are in high demand. In contrast to reactive routing, which only looks for available paths when absolutely necessary, proactive routing takes advantage of an always-accessible and full view of the network topology.

Due to the fact that each node in an Internet of Things network serves not only as a host but also as a router and sends data to the network's gateways, the routing must be performed appropriately. The manner in which data is carried from source to sink influences the amount of energy utilized by forwarding nodes.

Any comprehensive wireless transmission and Internet of Things (IOT) system is comprised of several interconnected subsystems, one of which is the transfer of data from its source to its destination, also known as the "sink."

The development of a routing protocol is advantageous for any complex network with dynamic properties, such as a continually shifting topology or traffic flow. The development of routing protocols for device-to-device communication between Internet of Things devices is required for the Internet of Things to reach its full potential (IoT).

To achieve this objective and enable IoT devices to connect to one another autonomously, it is necessary to implement routing protocols that can be exploited by the network.

There is a stage of the Internet of Things that has advanced even further than IOT itself. Another way to express this is to say that Internet of Things-related systems make substantial use of Internet of Things-related technology. A large number of devices can connect to one another and form a mesh network in an Internet of Things (IoT) system. Each of these devices is capable of independently collecting data, which is then transmitted to the internet via a router. In addition, it is vital to remember that "the internet of things" is a broader concept than "the internet of things network," which refers primarily to a wireless device network. "The network for items connected to the internet" Because a wired device tied to a network is not a wireless system, "Internet of Things network" cannot be used to describe a network to which a wired item has been added. In practice, it does not matter what type of device you employ as long as it is network-connected.

A gadget that is connected to the internet is known as an Internet of Things device. The term "Internet of Things system" is used to refer to a network of interconnected technological gadgets. In an Internet of Things-enabled environment, each device would have its own dedicated Internet connection and would routinely and continuously transmit data to the larger network. Using a thermometer is necessary for monitoring the temperature of any body of water, such as a lake. At this point, the data are either immediately sent to a remote server or are sent there at regular intervals. After the data has been transmitted to the remote server, it is processed and then given to the user via an interface. In contrast, an IOT is in no manner directly connected to the internet. Instead, each device must first establish a connection with either a router or a hub in order to access the network. Beginning at the router or hub, the sender is able to transmit the data via any route they want. Therefore, an Internet of Things (IoT) system can benefit from an Internet of Things (IoT) network by exchanging data with the network's router to utilize the network. The Internet enables a wide variety of geographically distinct entities to interact and share information in order to influence change. IoT technology, which enables the monitoring and distribution of environmental data, also serves as the backbone of IoT systems. This is due to the fact that the technology is responsible for supporting IoT systems.

The Internet of Things (IOT) and its associated networks are useful tools for monitoring and sharing about a wide range of environmental activities. This can be performed by utilizing these gadgets. This phrase contains all of these many types of instruments. The characteristics of the devices that will be used in an Internet of Things network are essential for its successful development and deployment. As the number of devices that can connect to the internet continues to increase, IoTs are likely to emerge as the sector's underlying infrastructure technology. The Internet of Things is made possible by the broad availability of wireless devices, which opens the door to an endless number of options and possibilities.

4.1.3 Leach Protocol

The Internet of Things architecture includes a hierarchical routing method based on clustering. Using this method, as depicted in Figure 4.2, the function of cluster leader is passed to each node in succession. This is a random occurrence. To achieve scalability and dependability, LEACH collects data at the level of cluster heads and applies localized coordination for the dynamic network. Both of these objectives are realizable. As a result, the amount of data delivered to the sink is decreased, leading to an increase in available bandwidth.

Figure 4.3, which may be viewed by clicking the provided link, is a depiction of the LEACH method's essential flowchart. Each node must apply a CH selection indicator function at the beginning of the clustering phase in order to choose which neighbours to include in the cluster. Figure 4.3 depicts the steps that must be taken. The selected cluster heads then utilize the non-persistent protocol to send an Advertisement (ADV) message. Each cluster head is assigned a unique identification in this message, and the cluster heads are stated in the order in which they were chosen (CHID).

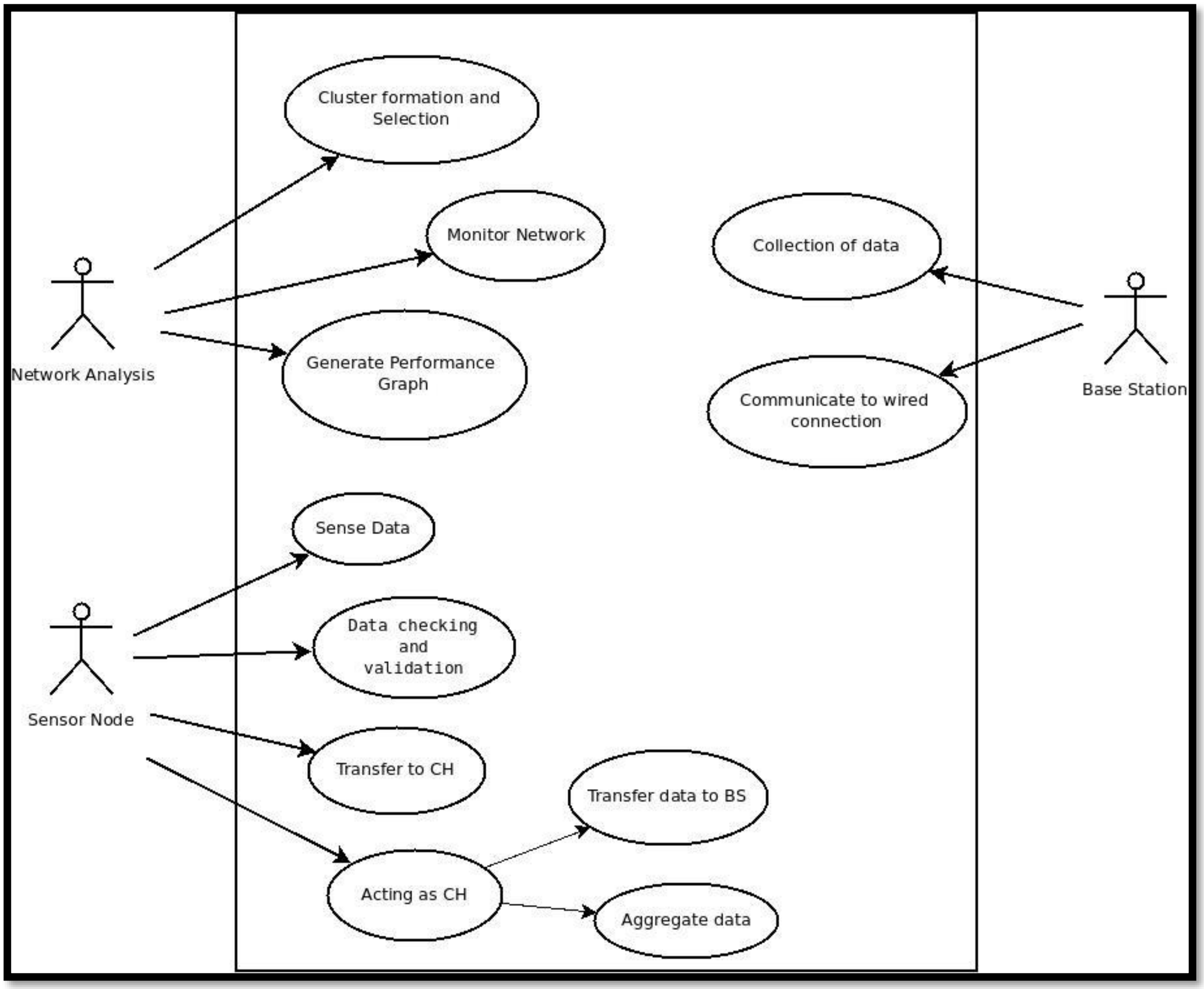

Figure 4.2: the proposed IOT system Project Analysis Diagram [52]

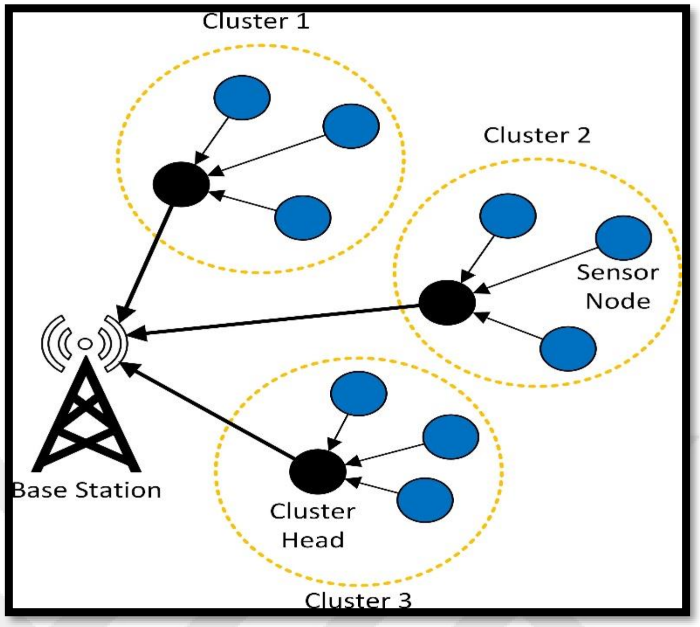

Figure 4.3: clustering and distribution in the devices [53]

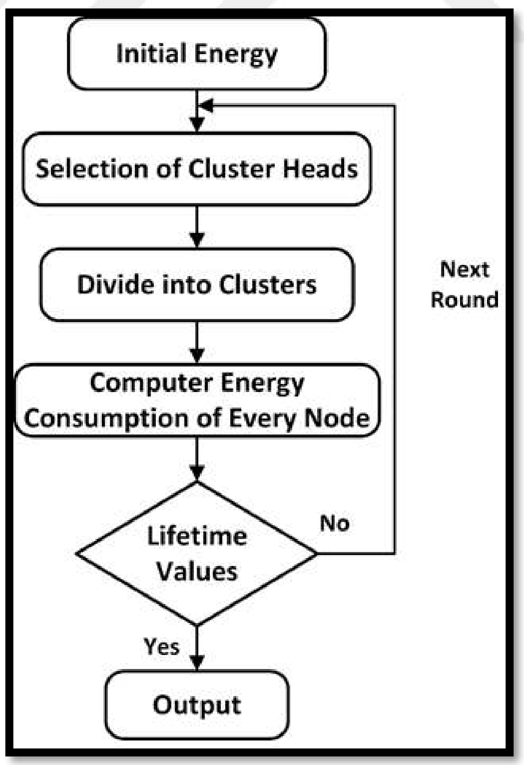

Figure 4.4: LEACH protocol diagram [44]

Device networks consist of a massive number of unconnected, low-powered, and diverse devices. These separate devices constitute the device networks. A device node is an autonomous piece of electronic hardware that is powered by batteries, is capable of data processing and short-range radio communication, and may incorporate integrated devices. Because it is fueled by batteries and is capable of functioning independently, it can operate on its own. In order to develop Internet of Things networks that are not only secure but also scalable, a tremendous deal of research has been devoted to identifying techniques for connecting large numbers of these devices (IOTs). Internet of Things (IoT) systems seek to be energy efficient, self-organizing, scalable, and robust, despite the restricted capabilities of individual device nodes. In an effort to identify the answers to these issues, a substantial quantity of study has been performed.

In order to fulfil both the goals of load balancing and extending the network's useful life, it is essential that the network's topology be organized in an efficient manner. This is owing to the rapid adoption of the Internet of Things (IoT), which has necessitated the implementation of an energy-efficient strategy. It is common knowledge that network clustering enhances its lifespan and provides the required scalability for its operation. When a bottleneck phenomenon occurs inside a network of Internet of Things (IoT)-connected devices, the network loses communication with its home base and the energy resources of the still-connected nodes are wasted.

4.2 LEACH PROTOCOL WOKFLOW

Because LEACH is a hierarchical protocol, the transmissions that originate from individual nodes are sent to the cluster heads. These cluster heads receive the vast bulk of these broadcasts. These communications are brought to the attention of the cluster chiefs. After that, the cluster heads collect all of the data, package it into a more manageable format, and then transmit it to the base station (sink). • A leader of a cluster is the person who is in charge of developing a plan for the transmission of data among the nodes that make up the cluster. This plan will be carried out by the nodes. All of the nodes in the cluster will operate in accordance with this timetable. The selection of the CH is handled through the LEACH protocol, which includes an implementation of a method known as distributed CH election. In this strategy, a predetermined number of nodes in the network are selected at random to take on the role of CHs, while the remaining nodes in the network are added to the cluster as member nodes. The CHs are the ones who are accountable for ensuring that the network continues to function properly. After that, the CH will make an announcement proclaiming its new status as a CH, and after that, the other nodes will choose to join the CH that has the strongest received signal in order to complete the CH. After that, the CH will make an announcement announcing its new status as a CH.

After the data has been obtained at one of the cluster member nodes, it is transferred to the CH through a single communication hop before being transferred to the BS from that location. The CHs are in charge of controlling the nodes that are a part of the cluster, collecting the data that is transmitted by the nodes, fusing the data that has been collected, and sending it to be processed by other clusters. Because of this, the CHs rotate, and the cluster topology is changed on a constant basis; both of these things are done in an effort to make the power consumption of the nodes more equal to one another.

The LEACH Protocol is made up of two distinct parts, which can be broken down into the following categories:

The Beginning Steps of the Procedure Stability in All of Its Different Expressions

During the part of the procedure known as Initial Configuration, you will be responsible for selecting the cluster nodes that will be used.

During the time period known as the steady-state, nodes continue to share information with one another while simultaneously preserving their status as the leader of the cluster.

Notation:

N: number of nodes CH: cluster head BS: a base station

Setup Stage:

In this stage, clusters are made and CHs are chosen

For Each (N)

N selects a random number T (n) between 0 and 1 If (T (n) < threshold value)

N becomes a Cluster-Head

N transmits a message announcing its CH status Else

N becomes a typical node

N receives the announcing messag of CHs End if

End for

For Each (CH)

Calculate a distance from N to CH and from CH to BS

N chooses the CH with minimum distance from it to CH to BS N appraises the selected Cluster-Head and becomes a cluster part

End for

For Each (CH)

TDMA schedule is made by Cluster-Head for each node to transfer data TDMA schedule is advertised to each node in the cluster by Cluster-Head

End for

Notation:

N: number of nodes.

CH: cluster head

Steady-state Stage:

For Each (N)

N gathers data that has been sensed

N transfers the data that has been sensed into the Cluster-Head in the corresponding TDMA time point

End for

For Each (Cluster-Head)

Cluster-Head gets data from the cluster nodes Cluster-Head aggregates the data

Cluster-Head transfers the data to the base station

End for

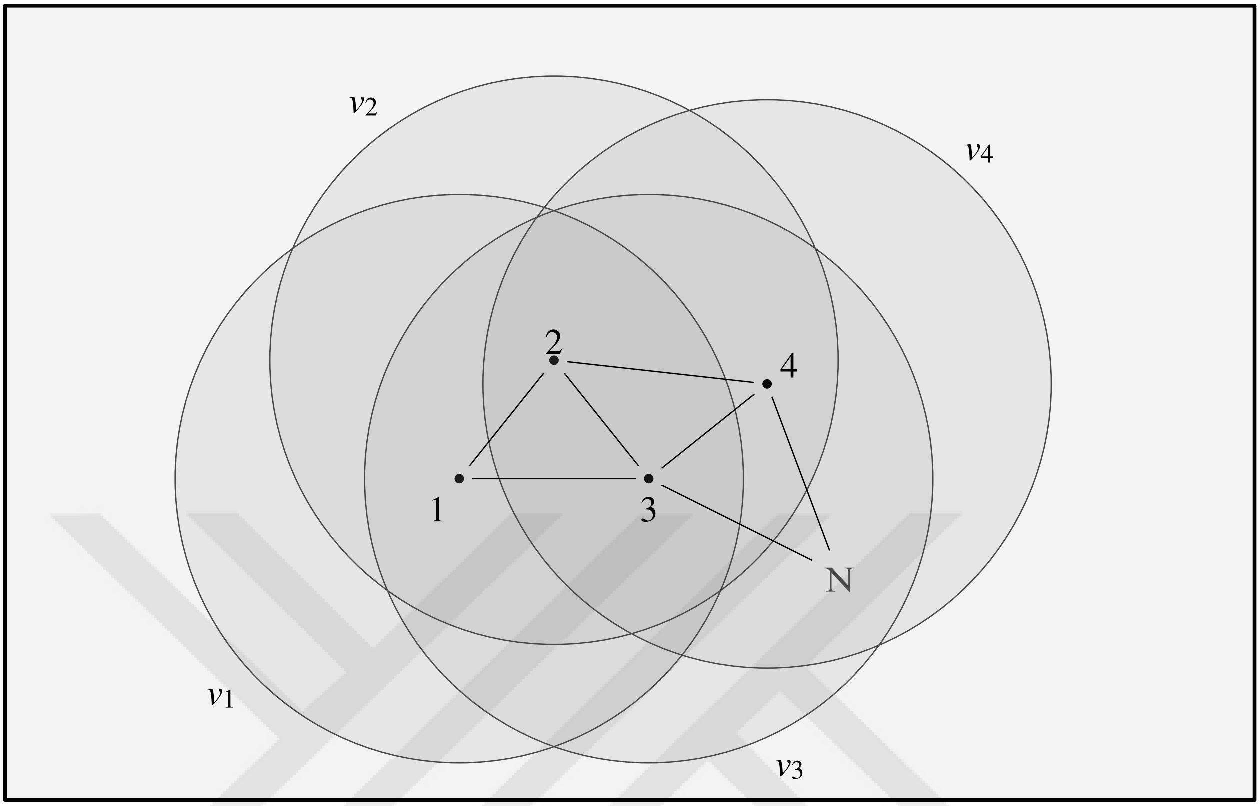

Figure 4.5: Node deployment using LEACH

4.3 CLUSTERING IN IOT NETWORK

It is possible to organize the nodes of a device into a hierarchical structure if they are first grouped together according to how closely they are situated to one another. This step is necessary before moving on to the next step. The use of a hierarchical approach (device node clustering), which is applied in the transmission of data from the physical environment to the BS, produces an improvement in energy efficiency. This improvement is brought about as a result of the utilization of a hierarchical method. It is vital to organize many devices into clusters since doing so will assist to reduce the size of the routing table, which will, in turn, make it simpler to utilize discovery mode across different devices. Clustering can help conserve communication capacity because it limits the scope of inter-cluster connections to CHs and avoids the requirement that device nodes continuously broadcast the same information. This, in turn, reduces the amount of data that needs to be transmitted. Each node in the network of devices, after performing a route table lookup, shares the information that it has collected with the CH after it has located the CH in its region. After the node has located the CH, this step is carried out. The CH works out how to get to the BS or to another receiving CH by selecting the path that will take it the least distance possible between the two locations. In order to be at the location in the shortest amount of time possible, this action might be taken. In order for the routing table to be able to adapt to the varying amounts of energy that are required for data transmission at each node, the connections that are established between the devices need to be changed on a regular basis. This is required in order for the table to be able to adjust to the varying quantities of energy.

4.4 CLUSTER FORMATION AND ROTATION

The life expectancy of device nodes can be significantly increased through the utilization of clustering, which is an effective way for controlling device nodes. As the expansion of the trend toward the use and administration of IoT continues, this method is gaining more and more significance, making it an increasingly important strategy. In the past, numerous strategies for the formation of clusters have been developed. One example of these strategies is called random competition based clustering (RCC), and it can be discovered in [18]. The RCC technique makes use of a random timer and takes the First Declaration Wins Rule as its guiding concept when determining how to label nodes during the clustering process. This ensures that the best possible decision is made. According to this criterion, the governorship of a radio network will be granted to the node that proclaims itself as the CH first to the other nodes that are a part of the network. This will determine the order in which the nodes in the network receive radio transmissions. The job of administering the network will be delegated to this particular node.

The broadcasting method is an additional strategy that can be adopted in order to promote the construction of clusters. This can be done by broadcasting information to multiple receivers at once. The process of one node in an Internet of Things (IoT) network delivering a packet to each and every other node in the network is referred to as broadcasting. It is vital to keep in mind that not all broadcast messages contain information of value, and that some of the messages delivered by the device node are ignored since the status of the device node has already been given. This is something that must be kept in mind at all times.

Direct broadcasting involves sending a cluster advertisement message to all of the devices in a certain area at the same time. This is done in order to reach all of the devices in the area simultaneously. To provide an example, in order to construct two clusters, it is necessary to select two nodes at random for the purpose of broadcasting. This is done so that the clusters may be constructed properly. An initiator is a node in a chain of events that is chosen at random to be the starting point. This node is considered to represent the beginning of the chain. An announcement for a new cluster is sent across the network to each and every node in the system. This advertisement is sent to the nodes individually. In the event that a node in the network that is not an initiator is the recipient of an advertisement message within the cluster, then the node in question will respond by sending a message to the initiator that delivered the advertisement message. Along with issuing a response, it will also, for the duration of that simulation cycle, ignore any further cluster advertisement signals that are sent its way. Despite this, the device node that is being driven to become a member of the cluster that this initiator is driving will have its membership added.

Direct broadcasting is a straightforward method; yet, it results in a substantial amount of wasted electricity consumption while providing an unsatisfactory rate of return on investment. This is because the CH sends broadcasts to each and every device node that is part of the network. Although this does not guarantee a response from the device, it is vital for the device nodes that are located at a large distance from the CH to be able to receive broadcast. This, however, does not guarantee that the device will respond. However, if a device node receives a broadcast from an initiator, the device node will refrain from transmitting the subsequent broadcast message. This will lead to the loss of transmission energy.

All of the cluster's nodes are able to simultaneously receive the same advertisement thanks to multi-hop broadcasting; however, this is only achievable within a specific geographical region. The duty of relaying the cluster advertised message to all of the device nodes that are within range of the node that is currently receiving it falls on the node receiving the message at the time. This approach is similar to the direct broadcasting method in that an initial initiator node is chosen to broadcast cluster formation requests to the other nodes in the cluster. However, unlike the direct broadcasting method, this method does not include any intermediate nodes. The procedure of determining which device nodes should be included in the cluster of "initiators" is referred to as "minimal communication energy," and it is explained in greater detail in [4]. When clusters are established in a dynamic manner, restructuring also takes place at regular intervals at regular intervals at regular intervals at regular intervals at regular intervals at regular intervals. In order to structure the cluster, at the beginning of each period, one of the strategies that have been mentioned previously is chosen. After then, a decision is made regarding which initiator would be in charge of disseminating messages via broadcast. As a direct result of using several hops in the transmission of signals, the amount of power used is reduced to an absolute minimum. Given the fact that the maximum amount of energy that may be lost is equivalent to the minimum amount of transmission energy that can be gained from device nodes in the surrounding area, it is obvious that there is a limit to the quantity of data that can be transmitted. This is because the maximum amount of energy that may be lost is equivalent to the minimum amount of transmission energy that may be gained. Because of this, it won't be essential for extremely distant device nodes to engage in direct communication with one another. This will make the network more efficient. One of the most notable downsides of this method, especially when compared to the earlier technique of broadcasting, is that it results in a delay in the transmission of the signal. This is one of the most significant drawbacks of this method. This is due to the fact that data in multi-hop broadcasting must be processed by each device node along the multi-hop path. This is one of the reasons why this is the case. As a direct consequence of this necessity, the process of grouping together into clusters is slowed down. If, on the other hand, the issue of latency can be managed, then multi-hop transmission is preferable to direct transmission. Direct transmission is not recommended.

4.5 CLUSTER HEAD SELECTION

After the clusters have been established, the CHs are chosen to assume leadership roles within the clusters. The cluster head is the one who is in charge of aggregating the data and conducting the routing; the cluster head is also the one who transmits the information that is sent to the base station from each cluster node. Additionally, CHs that service larger cluster sizes have a greater burden than CHs that serve smaller cluster sizes since the former need to receive, collect, and send a greater quantity of data than the latter do. This is because the former must collect more data than the latter.

The individual who created the network gets to decide whether a CH will be chosen at random or will be pre-assigned to each node in advance. This decision can be made either way. When choosing a CH, it is also possible to take into account any remaining energies that are contained within the cluster nodes. These energies can be found in the cluster nodes. It is common knowledge that CHs carry a disproportionately heavy burden in comparison to the other nodes in the cluster. As a result, the role of CH is rotated in order to disperse the load equitably, which in turn helps to increase the operational lifespan of the cluster. In addition, this helps to ensure that the cluster continues to function effectively for a longer period of time.

A node is chosen at random during the process of random selection under the presumption that there is a high possibility that it has never been selected as CH before in the entirety of the network's existence. This is the premise that underpins the random selection process. As a result of the function of the CH being divided over all of the device nodes, the CH itself is subjected to a reduced traffic burden than would otherwise be the case. The turning occurs at intervals that have been established in advance. When employing the method for selecting residual energy, in contrast, the device node that has the most energy left over is the one that is chosen to be the leader of the cluster. This ensures the most efficient use of the available resources. It will continue to act as CH until the amount of energy it holds decreases to a level that is lower than the average for the cluster. When the energy of CH drops to a level that is lower than the average of the cluster, a rotation will take place. It is possible that the CHs can be reorganized in such a way as to provide a more dependable distribution of the overall energy that the network produces. The lifetime of the network is going to continue to increase over time as a direct result of utilizing this technique. A second technique for picking a cluster head is one that is based on reducing the distance that separates the nodes of the cluster. This helps to reduce the amount of power that is required in order to transmit data to the base station (BS). It is possible to improve the cluster formation in order to make more effective use of energy during the transmission process by adopting this strategy, which involves reducing the total sum of the distances to CH as much as possible. This tactic can assist save money on electricity because it shortens the distance that data has to travel from the device node to any CH in order to get to where it's going.

It is essential to take into account the amount of energy required for communication when working with wireless transmission, and it is common knowledge that the amount of energy required for communication changes significantly depending on the distance between the sender and receiver of the message. As a consequence of this, it is strongly recommended to shorten the distance that the CH has to travel in order to send data from device nodes to the base station. This will allow for a more efficient transmission of data. Because of this, there is a decrease in the amount of power that is used by the IoT network.

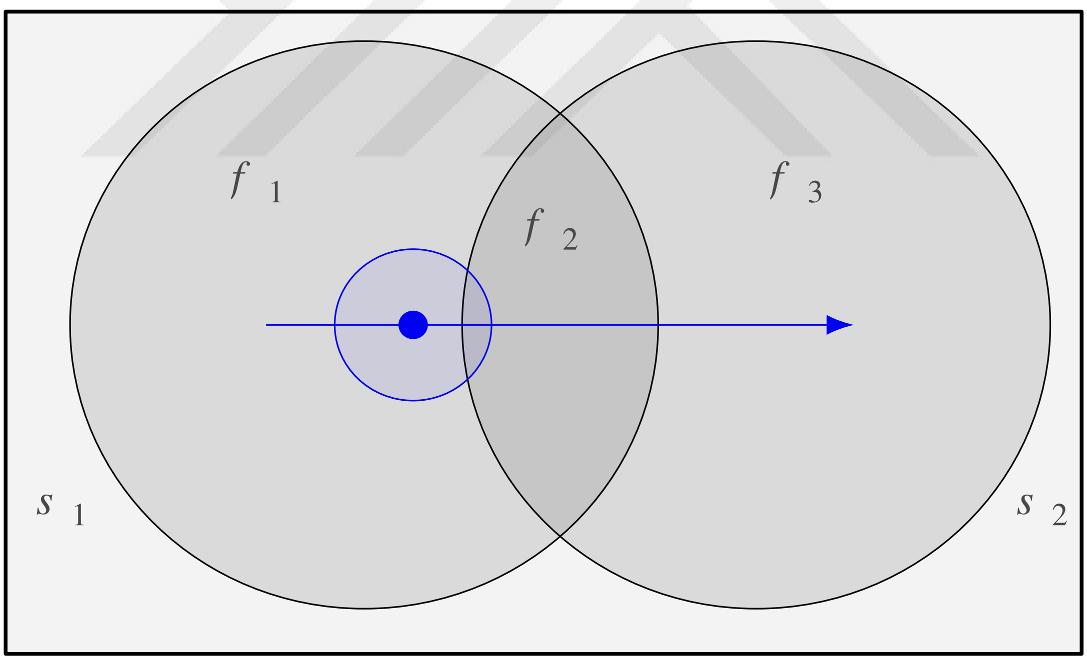

Figure 4.6: Transmission between the source node and the cluster head

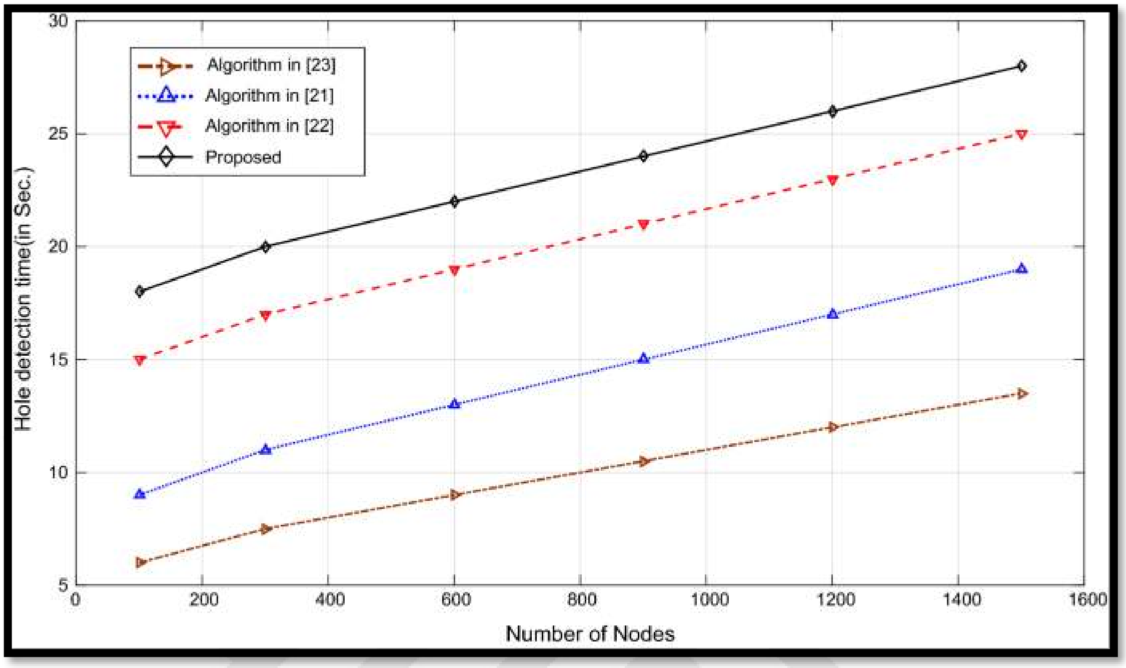

Figure 4.7: comparing the proposed success rate in transmission between the source node and the cluster head using multichip.

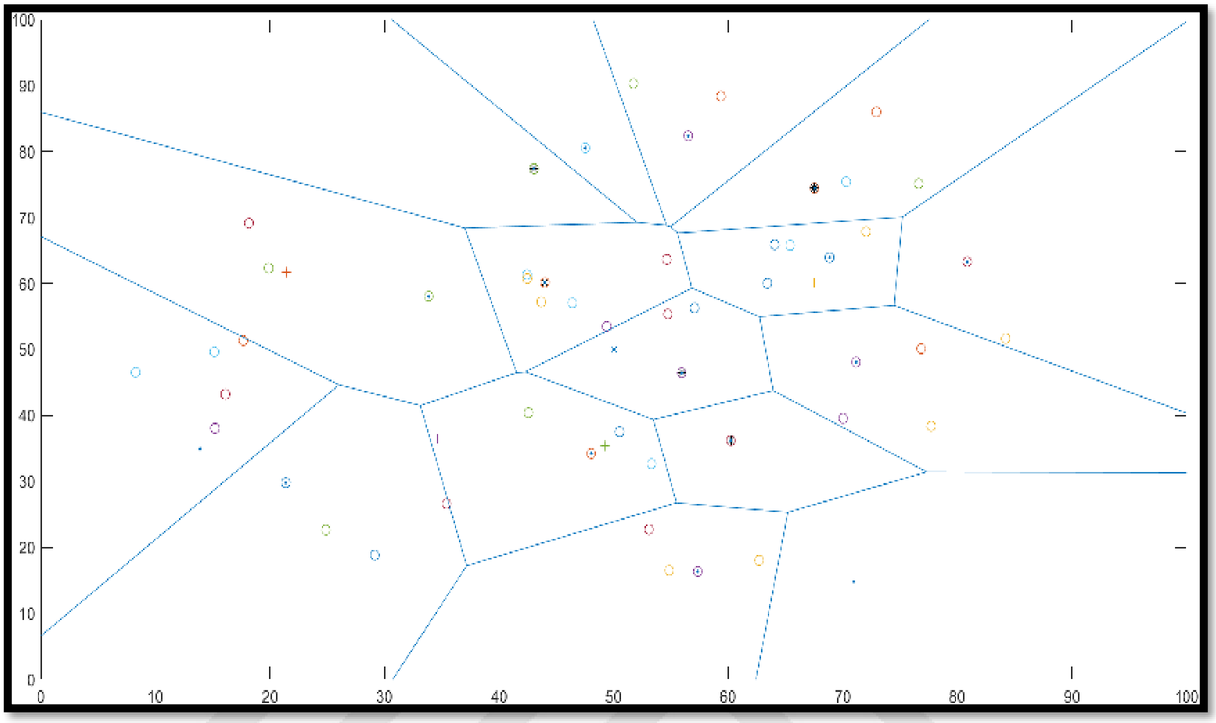

Figure 4.8: Clustering the network simulated in MATLAB

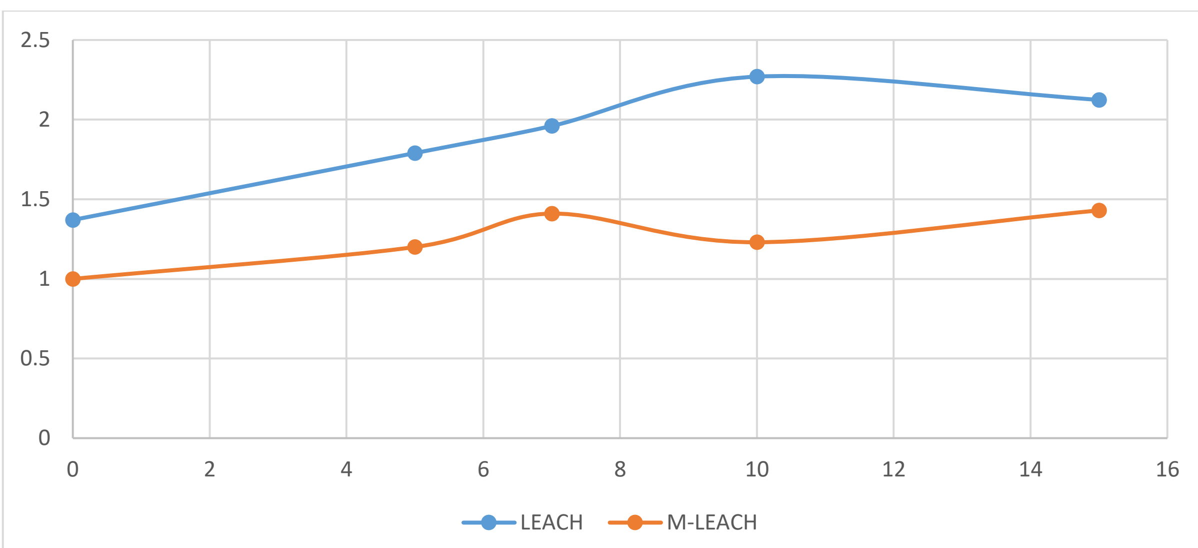

Figure 4.9: Energy consumption using the proposed Metaheuristic and the regular LEACH protocol

4.6 DATA TRANSMISSION

The procedure of data transmission can start once the clusters have been formed and the TDMA schedule has been created and implemented. It is assumed that nodes will always have data that needs to be transferred, and these nodes are the ones responsible for sending that data to the cluster head within the allotted amount of time for their transmissions. This transmission is only going to work properly if it is supplied with a negligibly little amount of electricity (chosen based on the received strength of the cluster-head advertisement). The radios on all of the other nodes in the cluster can be switched off to save power until it is that node's turn to send data. This can be done when it is not that node's turn to send data. If the node that serves as the cluster's head does not keep its receiver enabled at all times, then it will not be possible to retrieve the data from the other nodes that make up the cluster. Following the completion of the data collection procedure, the control node of the cluster will apply signal processing in order to combine all of the data into a single signal. If the data in issue are, for example, seismic or audio signals, the cluster-head node is able to beam form the separate signals in order to make a composite signal. This is possible because of the node's ability to produce a composite signal from individual signals. The combined signal is then transmitted to the base station, which is the recipient of the transmission. The strength of this broadcast can be attributed to the fact that the base station is situated at such a significant physical distance. The LEACH networks have arrived at their steady state of operation and are functioning normally within this configuration. After an interval of time that has been decided in advance, at the beginning of the following round, each node will decide for itself whether or not it ought to serve as a cluster-head for this particular round.

The following is the formula for computing the total quantity of data broadcast and received by the base station from the IOT nodes: Data = dataCHtoBS + dataNtoBS.

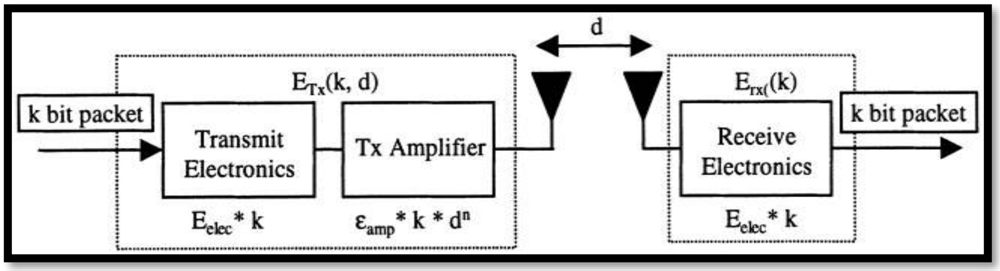

Figure 4.10: Dissipation Diagram for Data

Energy dissipated in data transmission is being estimated by: -

$$ETX = \{k * E\text{elect} + k * \varepsilon\text{fs} * d\hat{}2 \text{ if } d \leq do,$$

$$k * E\text{elect} + k * \varepsilon\text{mp} * d\hat{}4 \text{ if } d \geq do,$$

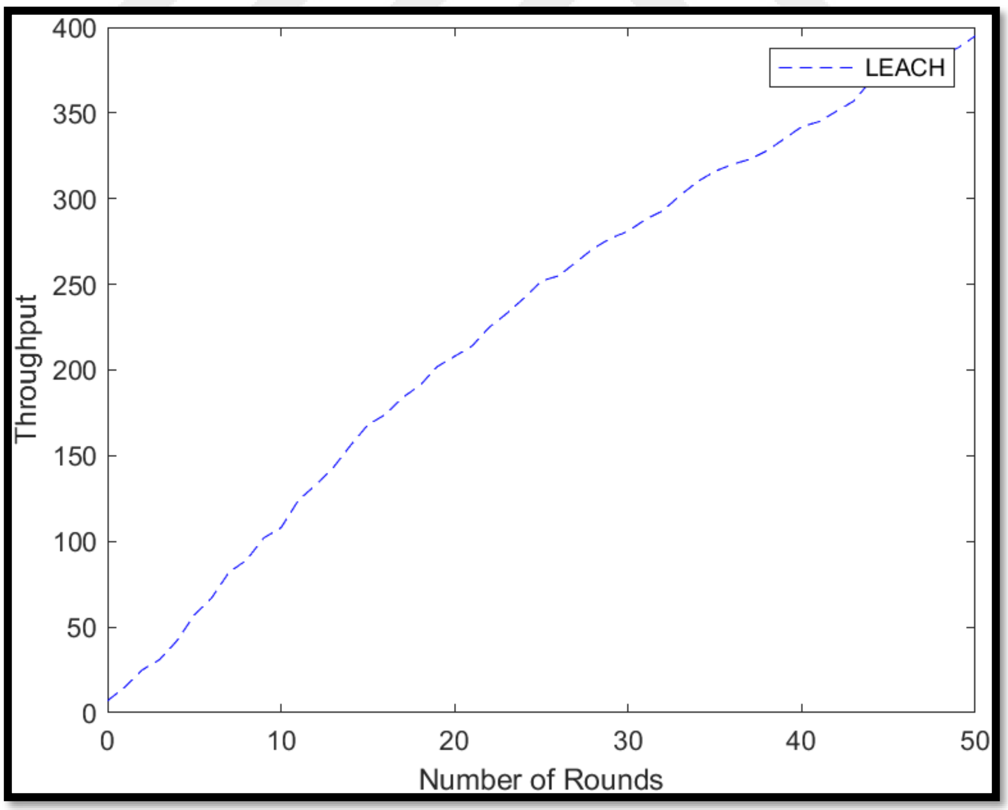

Figure 4.11: Sends a Packet to the Home Base

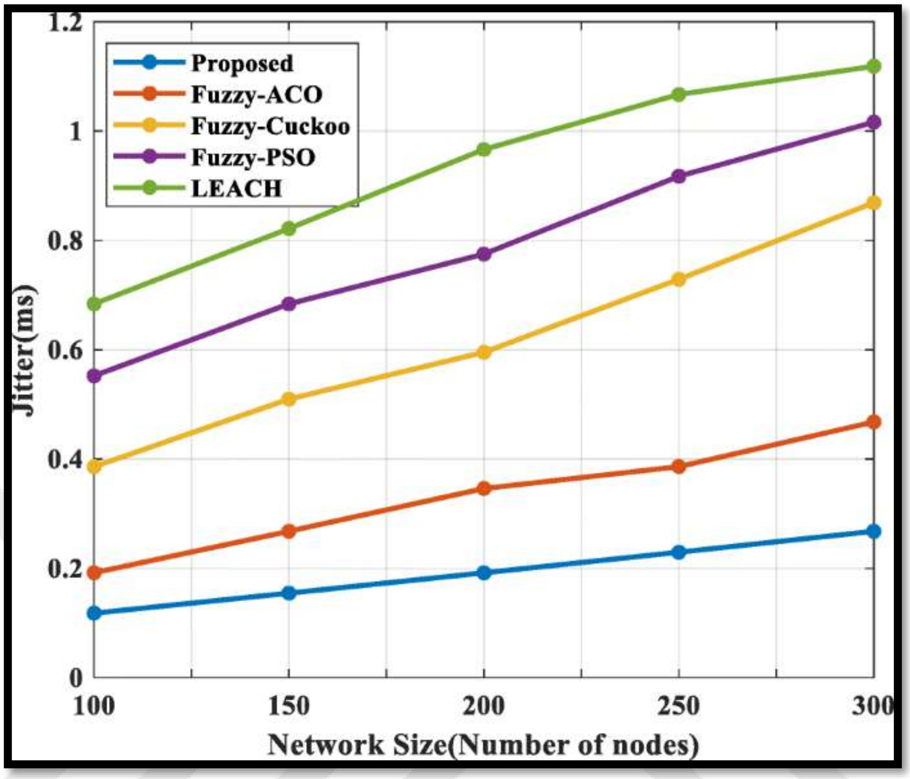

Figure 4.12: Comparing the proposed Metaheuristic-LEACH to other algorithms in terms Jitter in the network

4.7 DISCUSSION AND LIMITATIONS OF THE WORK

As a result of signal-hop routing from the individual nodes to the "center" of the cluster, network traffic is minimized, and energy is conserved. This is due to the fact that the "head" of the cluster integrates all of the data. As a result, the amount of time that the underlying network of devices may be used efficiently grows as a direct result of this.

The formation of a cluster using this method does not require any prior knowledge of the precise locations of the nodes in order to be successful.

i. It is not necessary for LEACH to have any prior knowledge of the network or any control information that originates from the base station in order for it to function properly because LEACH is entirely decentralized.

On the other hand, LEACH is not without its drawbacks, some of which are presented in the following paragraphs for your perusal.

ii. The overall number of cluster leaders that are now present in the system is in no way reflected by LEACH in any manner, shape, or form.

The fact that the data gathered by the cluster nodes would never be transferred to the Base Station in the event that the Cluster head were to perish due to any reason is one of the many problems that plague the LEACH system. LEACH also has a number of other shortcomings. For instance, compared to other clusters, some have a higher total number of nodes in their composition. This phenomena can lead to an increase in the total quantity of energy that is consumed and can have a significant bearing on the overall performance of the network. While some cluster heads are located in the inside of the cluster, others are located on the outside of the cluster's perimeter.

Hierarchical routing is a method that cuts down on the amount of power that is used. In this method, the leaders of clusters are chosen based on the amount of energy that is anticipated to be transmitted along the shortest path to the base station. Hierarchical routing helps reduce the amount of power that is consumed. Our strategy makes use of the geographical clustering of device nodes, with the CH role being cycled between nodes, the selection of CHs being optimized by the prediction of transmission energy in each simulation iteration, and the data being aggregated prior to being transferred to the BS. We investigated and placed an emphasis on the most important components of the hierarchical routing technique that we suggested for the purpose of transferring data to the base station. These components include cluster building and rotation, cluster head election and rotation, and cluster optimization. According to the findings of our investigation, the implementation of hierarchical routing has the potential to considerably enhance the energy efficiency of systems that are connected to the Internet of Things. It is conceivable to construct protocols for the Internet of Things (IoT) that make better use of energy by using the ideas behind hierarchical routing. This is something that is currently possible. In our methodology, the nodes are organized into clusters of varying sizes, each of which is spread over multiple locations. This is done with the intention of analyzing the potential impact that these clusters could have on the dependability of IoT networks over the course of time. In this thesis, we focused on developing an energy-aware protocol with the intention of reducing the total amount of energy that was spent by Internet of Things (IoT) devices while simultaneously improving the length of time that those devices were able to function reliably. In order to accomplish this objective, we came up with a hierarchical system that would transport the data to the BS via the route that required the least amount of transmission energy and also took the shortest amount of time. This was our plan. According to the findings of our simulations, the proposed protocol that we have developed provides a more efficient solution to the problem of energy efficiency in an IOT in contrast to both LEACH and a non-hierarchical technique.

We were able to show that our strategy was successful by analyzing the second-level hierarchy, in which three clusters were built inside the network; and by observing an increase in network lifetime, which is a sign of higher energy efficiency within the IOT. Both of these observations were based on our observations of the IOT. In the subsequent research, we will be able to determine whether or not there is an ideal level of hierarchy. This would require expanding the number of clusters to four, five, six, and so on. As a consequence of this, we are in a position to investigate the ways in which the lifespan of the network will be impacted, and in the event that the lifetime is reduced at a specific level of the hierarchy, we are also in a position to determine the size of the cluster that will be most effective in that circumstance. This work may be developed to optimize the number of device nodes in each cluster so that they can be equitably distributed into clusters utilizing approaches such as base-station controlled clustering protocol. This work can also be expanded to optimize the number of device nodes in each cluster. This will solve the issue of uneven data flow in device networks in a wider and more comprehensive manner. Expanding on this work to improve the number of device nodes contained inside each cluster is possible. Matlab is yet another tool that might be utilized in the process of evaluating our suggested procedure. This is accomplished by presenting a more in-depth perspective of the validation process and the data that is generated by it. When packets are routed in IoT networks, the energy of some device nodes is squandered because it is used to relay the data of other nodes rather than processing the device's own data. This occurs because some device nodes are used to relay the data of other nodes. Because of this, the device node will not be able to use its own energy in order to process its own data. As a consequence of this fact, future research should emphasize on establishing techniques for restricting the amount of power that can be consumed by nodes that have little or no energy reserves. This is because nodes that have little or no energy reserves can consume an excessive amount of power. Another aspect that may play a role in determining how long a network continues to operate successfully is the price of communication.

5. CONCLUSIONS AND FUTURE WORK

The Internet of Things is destined to have a greater impact on society than previous digital revolutions. It will cause major worldwide changes, affecting our interaction with the world and having a direct influence on our lives, the environment, our companies, and our safety. It will bring about many changes on a global scale, transforming our relationship with the world and having a direct impact on our lives, the environment, our businesses, and our safety. While the Internet of Things is designed to increase efficiency and reduce costs, it will not replace human dependency. It will require increasingly specialized professionals, as the billions of connected Things will demand support on behalf of human customers. The Internet of Things, if used consciously and responsibly, certainly brings a better quality of life, provides a more efficient use of resources and increases efficiency in industries as well. However, the number of connected devices increases exposure and makes these devices susceptible to intrusion if security measures are not followed, which can cause financial damage and even threaten life. As such, device manufacturers will have to introduce higher security standards. Devices must go through cybersecurity verification and certification processes before being released to the market. It is correct to say that the Internet of Things makes possible a multitude of opportunities that must be observed by markets and industries. However, for them to bring the expected benefits, it is essential that security issues are present at all stages of the implementation, from the infrastructure up to the endpoint. Big tech companies are doing their part, but security is also about people and processes. The millions invested in technology to increase security will be worthless if the human factor is left in the background. This situation was evident in the survey carried out with home and corporate users. The former do not believe in the possibility of being hacked and blindly trust the security of the devices to the point of using weak passwords in addition to sharing them with those who ask for them. Among corporate users, there is a certain concern with security, and some even know the risks, but most use weak passwords and when they need third-party support service on the devices, they usually use the internal network access. a consultant and strategic adviser, commented in a generic way: “Every company will be invaded, we just don't know when”. Therefore, it is recommended that home and corporate users know their vulnerabilities and risks and know how to circumvent them before deploying the devices, thus achieving a safer environment and being able to safely enjoy all the benefits that the Internet of Things provides. Edge computing, as an extension of cloud computing, expands IoT potential with AI and 5G. We proposed a new edge computing architecture in this paper, with the module chain bound to each sensor and a new module placement algorithm integrated with the simulated annealing algorithm. The simulation results were presented to demonstrate the benefits of our proposed method in terms of latency reduction and energy consumption. The Internet of Things (IoT) and cloud computing are two unique concepts that are both fast expanding in their respective fields of application. The former is made possible by a variety of technologies ranging from communication networks to distributed intelligence, whilst the latter allows for massively parallel processing on demand. As a result, we may include Cloud Computing as an enabler in the larger picture of IoT. Given the complexity of IoT computing principles, it is reasonable to predict that this complexity will someday generate computing workloads that are distinct from those now available. As a result, it is critical to investigate how existing scheduling optimization strategies might be applied to such computing jobs. We investigated the use of simulated annealing in a multi-cloud system supporting a workload of processes with low parallelism but high arrival rates and highly variable run-times. A discrete event simulator was utilized to evaluate the system's performance as well as its cost. The simulation findings show that the suggested scheduling strategy may yield considerable benefits in both performance and cost in this setting.

REFERENCES

[1] Parpinelli, Rafael S., and Heitor S. Lopes. "New inspirations in swarm intelligence: a survey." *International Journal of Bio-Inspired Computation* 3.1 (2011): 1-16.

[2] Pandey, Avinash Chandra, et al. "Spiral salp swarm optimization algorithm." *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*. IEEE, 2019.

[3] Garnier, Simon, Jacques Gautrais, and Guy Theraulaz. "The biological principles of swarm intelligence." *Swarm intelligence* 1.1 (2007): 3-31.

[4] Fortino, Giancarlo, and Paolo Trunfio, eds. *Internet of things based on smart objects: Technology, middleware and applications*. Springer Science & Business Media, 2014.

[5] Zedadra, Ouarda, et al. "Towards a reference architecture for swarm intelligence-based internet of things." *International Conference on Internet and Distributed Computing Systems*. Springer, Cham, 2017.

[6] Johri, Anubhav, and Ashish Tripathi. "Parkinson disease detection using deep neural networks." *2019 Twelfth international conference on contemporary computing (IC3)*. IEEE, 2019.

[7] Holland, John H. "Genetic algorithms." *Scientific american* 267.1 (1992): 66-73.

[8] Kar, Arpan Kumar. "Bio inspired computing–a review of algorithms and scope of applications." *Expert Systems with Applications* 59 (2016): 20-32.

[9] Ma, Haiping, et al. "Biogeography-based optimization: a 10-year review." *IEEE Transactions on Emerging Topics in Computational Intelligence* 1.5 (2017): 391-407.

[10] Goldberg, David E. *Genetic algorithms*. Pearson Education India, 2006.

[11] Beyer, Hans-Georg, and Hans-Paul Schwefel. "Evolution strategies–a comprehensive introduction." *Natural computing* 1.1 (2002): 3-52.

[12] Pan, Xiaoying, and Licheng Jiao. "A granular agent evolutionary algorithm for classification." *Applied Soft Computing* 11.3 (2011): 3093-3105.

[13] Jaderyan, Morteza, and Hassan Khotanlou. "Virulence optimization algorithm." *Applied Soft Computing* 43 (2016): 596-618.

[14] Kirkpatrick, Scott, C. Daniel Gelatt Jr, and Mario P. Vecchi. "Optimization by simulated annealing." *science* 220.4598 (1983): 671-680.

[15] Mittal, Himanshu, et al. "A new intrusion detection method for cyber–physical system in emerging industrial IoT." *Computer Communications* 190 (2022): 24-35.

[16] Hatamlou, Abdolreza. "Black hole: A new heuristic optimization approach for data clustering." *Information sciences* 222 (2013): 175-184.

[17] Rashedi, Esmat, Hossein Nezamabadi-Pour, and Saeid Saryazdi. "GSA: a gravitational search algorithm." *Information sciences* 179.13 (2009): 2232-2248.

[18] Kashan, Ali Husseinzadeh, Reza Tavakkoli-Moghaddam, and Mitsuo Gen. "Find-Fix-Finish-Exploit-Analyze (F3EA) meta-heuristic algorithm: An effective algorithm with new evolutionary operators for global optimization." *Computers & Industrial Engineering* 128 (2019): 192-218.

[19] Tabari, Amir, and Arshad Ahmad. "A new optimization method: Electro-Search algorithm." *Computers & Chemical Engineering* 103 (2017): 1-11.

[20] Geem, Zong Woo, Joong Hoon Kim, and Gobichettipalayam Vasudevan Loganathan. "A new heuristic optimization algorithm: harmony search." *simulation* 76.2 (2001): 60-68.

[21] Eusuff, Muzaffar, Kevin Lansey, and Fayzul Pasha. "Shuffled frog-leaping algorithm: a memetic meta-heuristic for discrete optimization." *Engineering optimization* 38.2 (2006): 129-154.

[22] Blum, Christian, and Daniel Merkle, eds. *Swarm intelligence: introduction and applications*. Springer Science & Business Media, 2008.

[23] Dorigo, Marco, and Christian Blum. "Ant colony optimization theory: A survey." *Theoretical computer science* 344.2-3 (2005): 243-278.

[24] Hu, Xiaohui, Yuhui Shi, and Russ Eberhart. "Recent advances in particle swarm." *Proceedings of the 2004 congress on evolutionary computation (IEEE Cat. No. 04TH8753)*. Vol. 1. IEEE, 2004.

[25] Karaboga, Dervis, and Bahriye Akay. "A comparative study of artificial bee colony algorithm." *Applied mathematics and computation* 214.1 (2009): 108-132.

[26] Li, Xiao-lei. "An optimizing method based on autonomous animats: fish-swarm algorithm." *Systems Engineering-Theory & Practice* 22.11 (2002): 32-38.

[27] Sharma, Avinash, et al. "Ageist spider monkey optimization algorithm." *Swarm and Evolutionary Computation* 28 (2016): 58-77.

[28] Rajakumar, B. R. "The Lion's Algorithm: a new nature-inspired search algorithm." *Procedia Technology* 6 (2012): 126-135.

[29] Tripathi, Ashish Kumar, et al. "A new recommendation system using map-reduce-based tournament empowered Whale optimization algorithm." *Complex & Intelligent Systems* 7.1 (2021): 297-309.

[30] Sharma, Nirmala, et al. "Chaotic spider monkey optimization algorithm with enhanced learning." *Soft computing for problem solving*. Springer, Singapore, 2019. 149-161.

[31] Bhardwaj, Sanjay, and Dong-Seong Kim. "Dragonfly-based swarm system model for node identification in ultra-reliable low-latency communication." *Neural Computing and Applications* 33.6 (2021): 1837-1880.

[32] Bitam, Salim, Sherali Zeadally, and Abdelhamid Mellouk. "Fog computing job scheduling optimization based on bees swarm." *Enterprise Information Systems* 12.4 (2018): 373-397.

[33] Chu, Xianghua, et al. "Learning–interaction–diversification framework for swarm intelligence optimizers: a unified perspective." *Neural Computing and Applications* 32.6 (2020): 1789-1809.

[34] Couceiro, Micael, and Pedram Ghamisi. "Particle swarm optimization." *Fractional order darwinian particle swarm optimization*. Springer, Cham, 2016. 1-10.

[35] Martínez-Álvarez, Francisco, et al. "Coronavirus optimization algorithm: a bioinspired metaheuristic based on the COVID-19 propagation model." *Big Data* 8.4 (2020): 308-322.

[36] Liu, Yuhu, et al. "Bearing fault diagnosis based on energy spectrum statistics and modified mayfly optimization algorithm." *Sensors* 21.6 (2021): 2245.

[37] Zhao, Weiguo, Liying Wang, and Seyedali Mirjalili. "Artificial hummingbird algorithm: A new bio-inspired optimizer with its engineering applications." *Computer Methods in Applied Mechanics and Engineering* 388 (2022): 114194.

[38] Dasgupta, Dipankar, ed. *Artificial immune systems and their applications*. Springer Science & Business Media, 2012.

[39] Del Ser, Javier, et al. "Bio-inspired computation: Where we stand and what's next." *Swarm and Evolutionary Computation* 48 (2019): 220-250.

[40] Castelli, Mauro, et al. "Salp Swarm Optimization: A critical review." *Expert Systems with Applications* 189 (2022): 116029.

[41] Del Ser, Javier, et al. "Bioinspired computational intelligence and transportation systems: a long road ahead." *IEEE Transactions on Intelligent Transportation Systems* 21.2 (2019): 466-495.

[42] Kallioras, Nikos Ath, Nikos D. Lagaros, and Dimitrios N. Avtzis. "Pity beetle algorithm–a new metaheuristic inspired by the behavior of bark beetles." *Advances in Engineering Software* 121 (2018): 147-166.

[43] Passino, Kevin M. "Biomimicry of bacterial foraging for distributed optimization and control." *IEEE control systems magazine* 22.3 (2002): 52-67.

[44] Greensmith, Julie. *The dendritic cell algorithm*. Diss. University of Nottingham, 2007.

[45] Gandomi, Amir Hossein, and Amir Hossein Alavi. "Krill herd: a new bio-inspired optimization algorithm." *Communications in nonlinear science and numerical simulation* 17.12 (2012): 4831-4845.

[46] Rabanal, Pablo, Ismael Rodríguez, and Fernando Rubio. "Using river formation dynamics to design heuristic algorithms." *International conference on unconventional computation*. Springer, Berlin, Heidelberg, 2007.

[47] Lam, Albert YS, and Victor OK Li. "Chemical reaction optimization for cognitive radio spectrum allocation." *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. IEEE, 2010.

[48] Cheng, Shi, et al. "Brain storm optimization algorithm for solving knowledge spillover problems." *Neural Computing and Applications* (2021): 1-14.

[49] Bogar, Esref, and Selami Beyhan. "Adolescent Identity Search Algorithm (AISA): A novel metaheuristic approach for solving optimization problems." *Applied Soft Computing* 95 (2020): 106503.

[50] Yang, Xin-She, and Suash Deb. "Cuckoo search via Lévy flights." *2009 World congress on nature & biologically inspired computing (NaBIC)*. Ieee, 2009.

[51] Nanda, Satyasai Jagannath, and Ganapati Panda. "Swarm and Evolutionary Computation." (2013).

[52] Jain, Mohit, Vijander Singh, and Asha Rani. "A novel nature-inspired algorithm for optimization: Squirrel search algorithm." *Swarm and evolutionary computation* 44 (2019): 148-175.

[53] Mafarja, Majdi, et al. "Efficient hybrid nature-inspired binary optimizers for feature selection." *Cognitive Computation* 12.1 (2020): 150-175.

[54] Mehrabian, Ali Reza, and Caro Lucas. "A novel numerical optimization algorithm inspired from weed colonization." *Ecological informatics* 1.4 (2006): 355-366.

[55] Zhang, Jinhao, et al. "Queuing search algorithm: A novel metaheuristic algorithm for solving engineering optimization problems." *Applied Mathematical Modelling* 63 (2018): 464-490.

[56] Yang, Xin-She. "Firefly algorithms for multimodal optimization." *International symposium on stochastic algorithms*. Springer, Berlin, Heidelberg, 2009.

[57] Yang, Xin-She. "A new metaheuristic bat-inspired algorithm." *Nature inspired cooperative strategies for optimization (NICSO 2010)*. Springer, Berlin, Heidelberg, 2010. 65-74.

[58] Moscato, Pablo. "On evolution, search, optimization, genetic algorithms and martial arts: Towards memetic algorithms." *Caltech concurrent computation program, C3P Report* 826 (1989): 1989.

[59] Rahnamayan, Shahryar, Hamid R. Tizhoosh, and Magdy MA Salama. "Opposition-based differential evolution." *IEEE Transactions on Evolutionary computation* 12.1 (2008): 64-79.

[60] Liu, Changan, et al. "The wolf colony algorithm and its application." *Chinese Journal of Electronics* 20.2 (2011): 212-216.

[61] Sharma, Harish, Jagdish Chand Bansal, and K. V. Arya. "Fitness based differential evolution." *Memetic Computing* 4.4 (2012): 303-316.

[62] Sharma, Nirmala, Harish Sharma, and Ajay Sharma. "Beer froth artificial bee colony algorithm for job-shop scheduling problem." *Applied Soft Computing* 68 (2018): 507-524.

[63] Tsai, Chun-Wei, et al. "Metaheuristic algorithms for healthcare: Open issues and challenges." *Computers & Electrical Engineering* 53 (2016): 421-434.

[64] Eichelberg, Marco, et al. "A survey and analysis of electronic healthcare record standards." *Acm Computing Surveys (Csur)* 37.4 (2005): 277-315.

[65] Zhou, Hangjun, et al. "A big data mining approach of PSO-based BP neural network for financial risk management with IoT." *IEEE Access* 7 (2019): 154035-154043.

[66] Wang, Rong, Chuangang Yu, and Jia Wang. "Construction of supply chain financial risk management mode based on Internet of Things." *IEEE access* 7 (2019): 110323-110332.

[67] Shepherd, Carlton, et al. "An exploratory analysis of the security risks of the Internet of Things in finance." *International Conference on Trust and Privacy in Digital Business*. Springer, Cham, 2017.

[68] Pavlidis, Michalis, et al. "Selecting security mechanisms in secure tropos." *International Conference on Trust and Privacy in Digital Business*. Springer, Cham, 2017.

[69] Botteghi, Nicolò, et al. "Multi-agent path planning of robotic swarms in agricultural fields." *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences* 1 (2020): 361-368.

[70] Albani, Dario, et al. "Monitoring and mapping with robot swarms for agricultural applications." *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE, 2017.

[71] Sinai, Lior. *Efficient path planning for multiple agents in agriculture fields*. MS thesis. University of Twente, 2020.

[72] Zedadra, Ouarda, et al. "Swarm intelligence and IoT-based smart cities: a review." *The internet of things for smart urban ecosystems* (2019): 177-200.

[73] Tripathi, Ashish Kumar, et al. "A parallel military-dog-based algorithm for clustering big data in cognitive industrial internet of things." *IEEE Transactions on Industrial Informatics* 17.3 (2020): 2134-2142.

[74] Tripathi, Ashish Kumar, Kapil Sharma, and Manju Bala. "A novel clustering method using enhanced grey wolf optimizer and mapreduce." *Big data research* 14 (2018): 93-100.