T.C.

ALTINBAŞ UNIVERSITY

Electrical and Computer Engineering

MONITORING SYSTEM BASED ON BLUETOOTH MESH SENSOR NETWORK

BILAL HASHIM HAMEED

Master Thesis

Supervisor

Asst.Prof. Dr. Sefer Kurnaz

Istanbul, 2019

MONITORING SYSTEM BASED ON BLUETOOTH MESH SENSOR NETWORK

by

Bilal Hashim Hameed

Electrical and Computer Engineering

Submitted to the Graduate School of Science and Engineering

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2019

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of ....

Academic Title Name SURNAME	Academic Title Name SURNAME
Co-Supervisor	Supervisor

Examining Committee Members (first name belongs to the chairperson of the jury and the second name belongs to supervisor)

Academic Title Name SURNAME	Faculty, University	____________________
Academic Title Name SURNAME	Faculty, University	____________________
Academic Title Name SURNAME	Faculty, University	____________________
Academic Title Name SURNAME	Faculty, University	____________________
Academic Title Name SURNAME	Faculty, University	____________________

I certify that this thesis satisfies all the requirements as a thesis for the degree of ....

Academic Title Name SURNAME

Head of Department

Academic Title Name SURNAME

Director

Approval Date of Graduate School of Science and Engineering: ____/____/____

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

Bilal Hashim Hameed

ABSTRACT

MONITORING SYSTEM BASED ON BLUETOOTH MESH SENSOR NETWORK

Aldarraji, Bilal Hashim Hameed,

M.Sc. Electrical and Computer Engineering, Altinbaş University,

Supervisor: Asst.Prof. Dr. Sefer Kurnaz

Co-Supervisor: Asst.Prof. Dr. Adnan Hussein Ali

Date: July/2019

Pages: 82

The security in wireless sensors networks is one of the most important things to focus on, especially in Internet of think instrument (IOT) applications. In the last five years the sensors networks applications have increased because, these sensors networks are involved in all aspects of life such as (smart residential houses and commercial building, medicine, agriculture, …. etc.). In this work, we designed a new Security Monitoring System for smart home and bulling application. This system designed base on Bluetooth Mesh Sensor Network (BMSN), because the Bluetooth (HC-06) used due to with low energy consumption and 100 m communication distance between point to point. In addition it has been used GSM mobile to send the warning message from the master control system. The Bluetooth sensors network is one of the most important Internet of thinks (IOT) application. The Arduino Nano was used as microcontroller unit for each parts of the networks. The Arduino Nano receives signals from the motion sensors until the cameras are controlled and also send and received the signals between two parts in the mesh sensor network by Bluetooth and depending on these signals, the cameras are turned ON and OFF and moved Right or Left. The system was described and simulated in our research and all the results were discussed . The main advantage of this work is to design of a cheap Bluetooth sensors security network with low storage capacity in terms of recording control videos.

Keywords: Mesh Network,Bluetooth, Wi-Fi, ZigBee, GSM, 3G, Motion Sensors HC-06

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF ABBREVIATIONS

WSN	Wireless Sensor Networks
WAP	Wireless Application Protocol
ISPs	Internet Service Providers
SIG	Special Interest Group
WLANs	Wireless Local Area Networks
GPRS	General Packet Radio Service
GSM	Group Special Mobile
UMTS	Universal Mobile Telecommunications System
ITU	International Telecommunication Union
LTE	Long Term Evolution
DSS	DSS
SIG	Special Interest Group
IEEE	Electrical and Electronics Engineers
BMSN	Bluetooth Mesh Sensor Network
PIS	Passive Infrared Sensor
IOT	Internet of thinks

1. INTRODUCTION

1.1 INTRODUCTION

The sensors are devices capable of detecting certain physical phenomena through the use of transducers.

With the evolution of technology, the sensor market offers not only increasingly precise and reliable products, but also increasingly sophisticated functions, and new types of communication methods, including the possibility of communicating through wireless technologies.

This technological evolution, wireless communication, allows the sensors to be able to abandon the cables, which makes it possible to build wireless sensor networks, wireless sensor networks (WSN), which can have applications in many sectors. But on the one hand the fact of not having cables leads to the possibility of applications that were previously unworkable or impractical, on the other hand it opens up other problems that can limit the use of such devices. One of these problems is food.

The absence of the power cable means that the device must be able to operate with an autonomous power supply. Despite the development of new energy sources (eg solar energy) and a progressive reduction in the consumption of electronic devices, it is still unthinkable to have a device that maintains an active permanent functioning with an autonomous power supply. This means that the device has a consumption limit (the capacity of the batteries, the maximum solar energy that can be used in a day, etc.), so to make the device as efficient as possible it is necessary to limit the consumption of energy only in the necessary moments. From the experimental data, the greater power consumption, for wireless sensors, occurs when the information is transmitted. So to make energy consumption efficient it is necessary to transmit the least amount of data possible, but this must in no way compromise the quality of the data detected by the WSN.

1.2 MOTIVATION

Wireless Application Protocol (WAP) is a technical standard for accessing information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones that uses the protocol. Wireless performances like remote meter reading and RFID tags for refuse bins have previous to now found their way out of the building and into the community. These systems have been promoted by the service providers with their interest in mind, meaning cost savings and ease of service. It is fair to say that communities can exploit these initiatives also, as service providers can choose to pass this usefulness onto the consumer in terms of cost savings and quality of service.

This dissertation examines how better to develop a wireless network to provide these and other services to a building community which primarily usefulness the community. This dissertation is a report on the research, design and development of a wireless mesh sensor network to be deployed in a building estate environment and establish the identity some of the benefits this kind, of network could present. Networks already exist between many buildings in a building estate. At present this is mainly through the internet protocol TCP/IP, which mostly is an indirect link provided by Internet Service Providers (ISPs). Wireless links are too becoming further common, with Wireless Local Area Networks (WLANs) based on the IEEE 802.11 (Wi-Fi) standards. Numerous of these WLANs have a gateway to the internet provided by wireless broadband service providers. The direction for this dissertation is to develop a new building estate network based on license exempt, low power wireless technology, not in race with IEEE 802.11. This system must be both inexpensive and useful to a building community. These advantage, may also expand to service providers to the building community.

1.3 DISSERTATION OBJECTIVES

The objectives of this dissertation are:

1) To design a new wireless mesh network based security monitoring system.

2) To simulate and investigate the designed wireless security monitoring system.

3) To detect the intrusion and response accordingly via Bluetooth and GSM technology.

1.4 DISSERTATION CONTRIBUTIONS

This dissertation is a report on the design and improvement, of a new application based on wireless mesh sensor networks the main contributions which were made by this thesis are:

1) System design of a new building community monitoring network based on Wireless mesh sensor networks by using Bluetooth technology.

2) The design of a MAC protocol to support wireless sensor nodes.

3) Software design of a wireless mesh node and a wireless sensor node, specifically designed to meet the requirements of the system outlined in this dissertation.

1.5 OUTLINE OF THE DISSERTATION

The remainder of this Dissertation is structured as follows:

Chapter 2:

The field of wireless sensor networks is very broad, so we will discuss in this chapter the most important in an accurate and concise. The topics that will be discussed are the characteristics and elements of wireless sensor networks as well as the applications and topologies of these networks.

Chapter 3:

The short-range wireless communications are used in applications where fast transmissions of a volume of data are not very high and efficiently. For example, in the sensor networks several devices are used to collect information about the temperature or smoke detection and communicate with other devices in order to act on that information. The short-range wireless communication technologies that will be analyzed and disruption in this chapter: classic Bluetooth, Bluetooth Smart, ZigBee and ANT / +.

Chapter 4:

In this chapter examines the system design overview, of the proposed WMSN. It presents a high level design overview which encompasses all aspects of the system. It also discusses the reasoning behind the approach of the design. The system design concept focuses on a hybrid solution for a wireless mesh sensor network, in which wireless mesh nodes are deployed in a fixed infrastructure and transmit-only sensors are deployed wirelessly also presents a detailed design of software pertaining to the wireless sensor node and wireless mesh node respectfully. The chapter concludes with a discussion on how the system is expected to perform.

Chapter 5:

In this chapter the conclusions of the work done are made and presents concluding discussions and outlines a few ideas for future work on this research.

2. WIRELESS SENSOR NETWORKS

2.1 INTRODUCTION

The field of wireless sensor networks is very broad, so we will discuss in this chapter the most important in an accurate and concise. The topics that will be discussed are the characteristics and elements of wireless sensor networks as well as the applications and topologies of these networks.

2.2 WIRELESS SENSOR NETWORKS

Sensor networks is a deployment of several devices that have sensors that are installed in an area in which they perform the measurement together, which have the ability to obtain information from their environment, store information, monitor events and communicate dat .An administrator is responsible for collecting all the information provided by these devices.

Wireless sensor networks are composed of several devices [1], among which are the sensors that control one or several conditions, which can be location (GPS), temperature, pollutants, light, sounds, solar radiation, humidity and a long variety of parameters. One quality that these networks have is that they use nodes that only activate when they are indicated, thus they have a low consumption and lower energy requirement, which lengthens the useful life of the battery. Another is that wireless networks have the advantage that when a node fails it can establish communication by another node.

2.2.1 Characteristics Of Wireless Sensor Networks

Wireless sensor networks have many features such as topology, fault tolerance, maintenance, energy, among others. Below its main characteristics:

- Your topology is dynamic, the network depends on the environmental conditions in which they are deployed.
- It is a fault-tolerant network, it has the ability to continue functioning even if there is an error in the system.

- Its maintenance is in a period of months or years.
- It is easy to be able to integrate with other technologies.
- Facility of deployment, the same network can be moved in different environments.
- It has a low energy consumption, it feeds the sensors with batteries or small solar panels.
- The messages are usually small, so it is not necessary to fragment them.
- Data from the sensors are stored on the device and real-time and historical data can be consulted on the Internet from anywhere.

2.2.2 Wireless Sensor Networks Elements

The networks of wireless sensors are mainly three elements that are the node, the information collector and the external system, which are detailed below, and the element was presented in the Figure 2.1.

1) Node, device in charge of gathering data, autonomous that is composed of: microcontrollers, battery, communication and storage modules.
2) Data collector, as it says it collects the information from the nodes and transmits the information to the external system, it can be a central node.
3) External system, is the data collection and management center, which sends the information to a server where they process the information.

Figure 2.1 : Elements of sensor networks

The nodes of the wireless networks have different parts [2]:

- **Sensor,** can be one or several sensors, responsible for collecting data.
- **Data processor and control**, is a processor that has a small memory to save the data collected by each sensor.
- **Wireless communication**, is the means to transmit the information of the sensors to other nodes of the network.
- **Power source**, battery or small solar panels that serve to feed the node.

2.2.3 Types of Nodes

In the network we have three types of nodes that are the central node, the cluster-head node and the sensor node. Figure 2.2 shown the different nodes in a network. The types of nodes are [3]:

- **Central node:**

  For each network there can only be one central node that is responsible for managing the communications between all the devices in the network.

- **Cluster-head:**

  Its function is to route the messages of the nodes to the central node. It allows that the different sensors connect to the network and that they can connect to other routers.

➢ **Sensor node:**

It is the device that collects the data, its functionality because it is not in process of sending information.

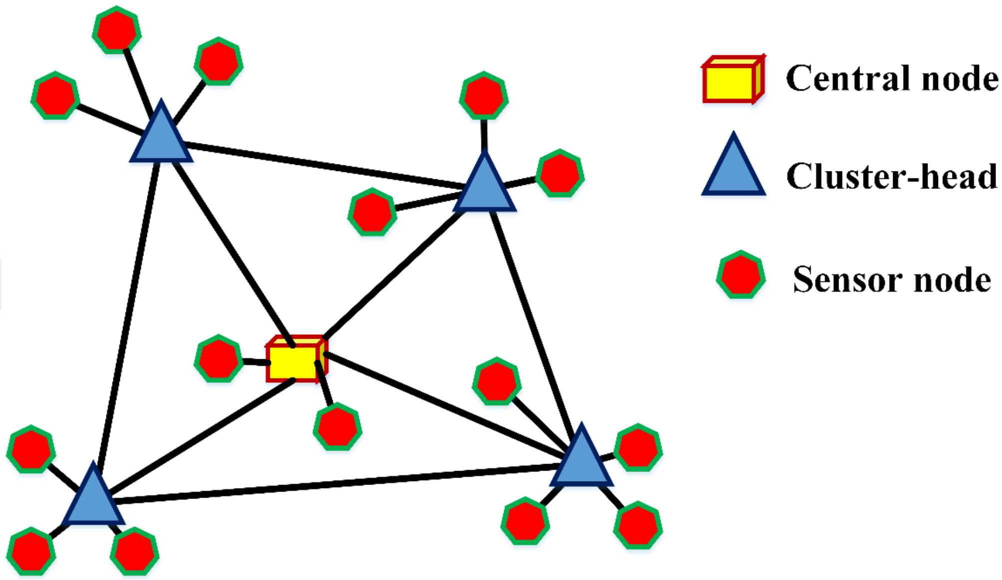


Figure 2.2 : Types of nodes

2.2.4 Principles Design Of Wireless Networks

When designing a network we must take into account the principles for its construction, then we will explain some principles of network design [4]:

➢ **Energy Efficiency**

The nodes are located in places that are not easily accessible, for which the battery must be durable because the possibilities of change are minimal. It is very important that the option chosen for energy aims to prolong the life of the sensor network.

➢ **Scalability**

Sensor networks can have up to thousands of nodes working together, so the network must be prepared to interact with a large number of nodes.

- **Autonomy**

In the wireless sensor network there is no device in charge of making the routing decisions, for which reason this action can be carried out by any node in the network.

- **Heterogeneity**

The network consists of several sensors which may have different characteristics but must work together, so the network must be provided for the heterogeneous operation of the devices.

- **Fault tolerance**

Nodes must be able to have alternative routes to transfer information when a node fails. The nodes can run out of energy or have damage caused by the environment where it is located.

- **Mobility**

The sensor network has several sensors that are randomly distributed in the geographical area of application and may require that the sensors change their position in the network, so they must be able to move without difficulty.

2.2.5 Types Of Wireless Communication

When we talk about wireless networks we refer to those that have an established infrastructure and those that do not, then those wireless communications will be explained.

- **Wireless Networks With Infrastructure**

Figure 2.3 present the wireless networks with infrastructures, they have a fixed number of wired links, communication is direct (terminal-base station), there is only communication within the coverage area. Examples: Wi-Fi networks, mobile telephony

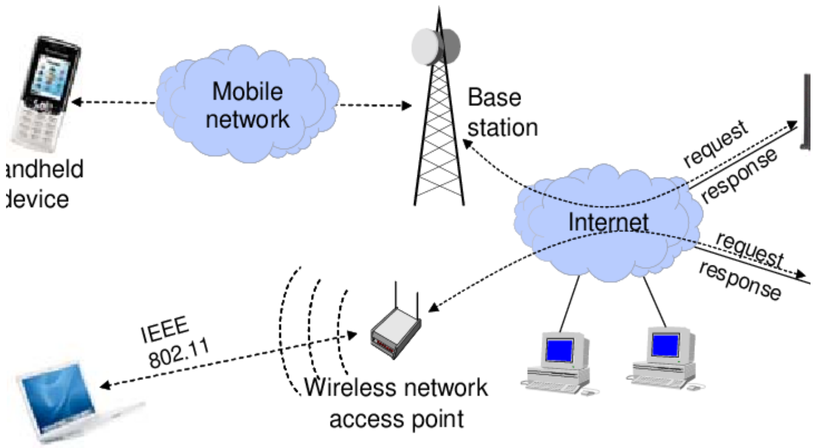


Figure 2.3 : Wireless networks with infrastructures

➢ **Wireless Networks Without Infrastructure (Ad-hoc)**

All hosts are mobile, connected to each other arbitrarily and dynamically. Figure 2.4 present the wireless networks without infrastructures, the nodes work as routers, which seek and maintain the routes [5]. The information is collected from the environment, the data is processed and transmitted to the base station or node. Also the number of sensors is greater, the nodes can be fixed or not, the sensor nodes have no identification and are networks with energy restriction and bandwidth.

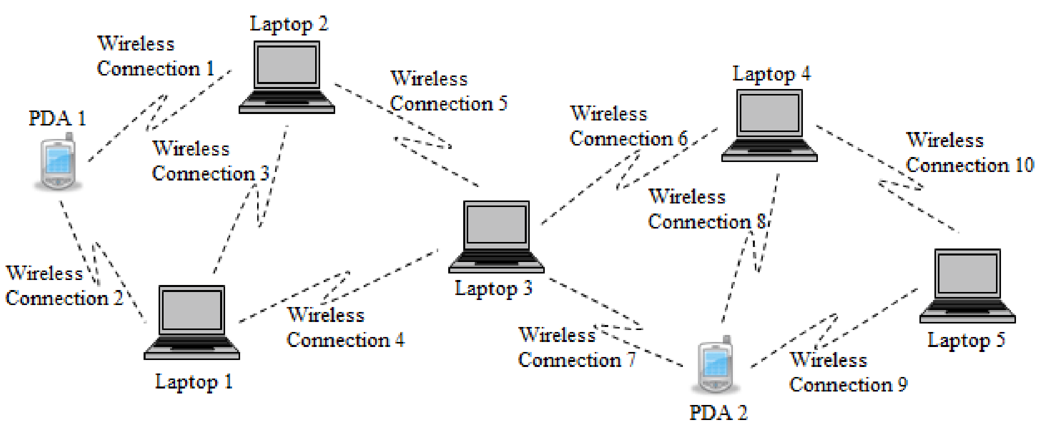


Figure 2.4 : Wireless networks without infrastructure

2.3 WIRELESS SENSOR NETWORKS APPLICATION

Wireless sensor networks can be used in different environments offering support to various applications. The sensors can measure several conditions, these are some of these types of sensors in Table 2.1.

Table 2.1: Comparison of consumptions between modules

Illumination	Noise levels
Humidity	Temperature
Pressure	Address
Movement	Speed
Acceleration	Vibration
Angle	Displacement

The variety of applications is quite of which these are the most used [6]:

2.3.1 Home Applications

Security control in all the installations of the house in the Figure 2.5, energy management and home automation. Detection of infrastructure damage and leakage alarms. Inventory of the warehouse and notice when products are missing.

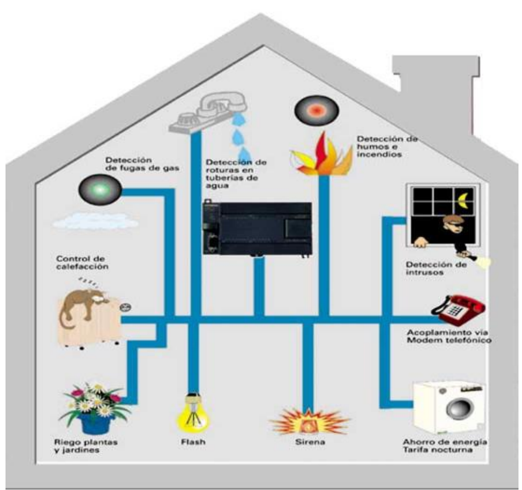


Figure 2.5: Application for home automation

2.3.2 Military Applications

Mine detection, detection of intruders in the field and detection of attacks. Follow-up of confrontations and exploration of the lands. Monitoring of vehicles and equipment in enemy terrain. Damage evaluation in the combat field and surveillance of location systems in the Figure 2.6.

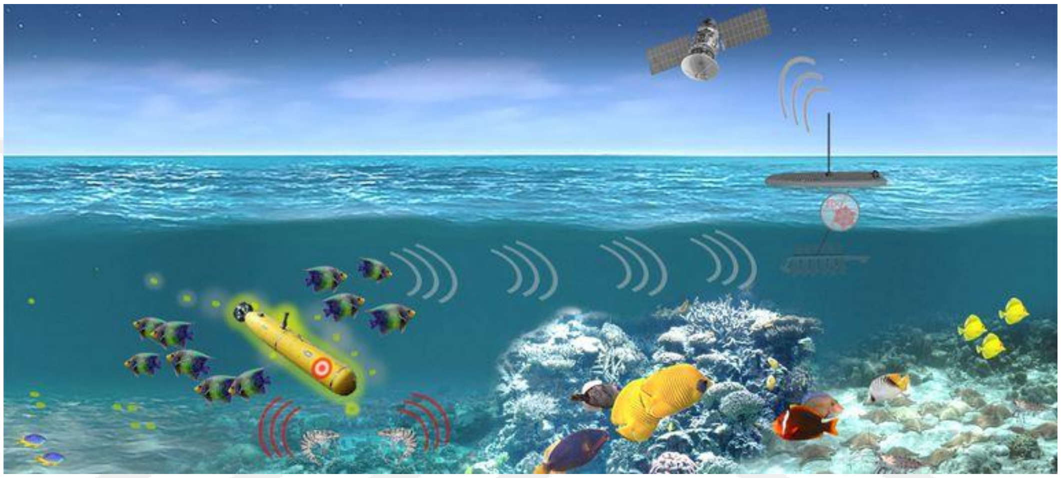


Figure 2.6 : Application for the detection of submarine intruders

2.3.3 Environmental Applications

Monitoring of animals in open territories and monitoring of the environment. Location of contamination and detection of natural disasters. Recognition of the environment and meteorological research. Sensors of soil moisture levels, temperature, etc. Figure 2.7 present the Animal tracking application.

Figure 2.7 : Animal tracking application

2.3.4 Medical Applications

Emergency alarms from where the patient is to hospitals and ambulances. Tele monitoring of physiological information and deployment of biosensors in patients. Control of the medication regimen and help for patients with disabilities. Figure 2.8 present the patient monitoring applications.

Figure 2.8 : Patient monitoring applications

2.4 TOPOLOGIES OF WIRELESS NETWORKS

At the moment of building a wireless network we realize that there are three types of wireless network topologies that are star, mesh and cluster tree [7], which we will explain below:

2.4.1 Star Topology

In the star topology in the Figure 2.9, each sensor is connected directly to the central node. All sensor data passes the information first through the central node before reaching its destination.

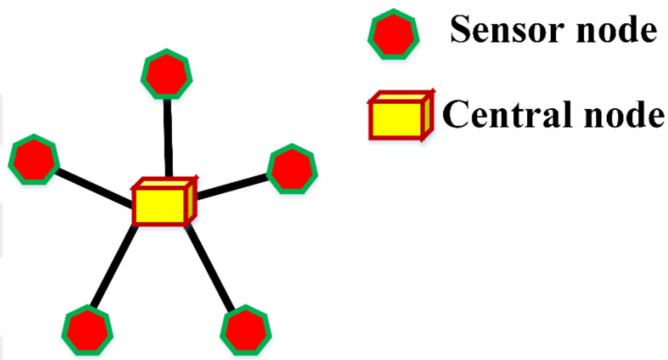


Figure 2.9 : Star Topology

2.4.2 Mesh Topology

There are two types of topology in the Figure 2.10: partial mesh and full mesh. In the full mesh topology there are direct links between all the sensors in the network. In contrast, only partial sensors are connected in the partial mesh topology.

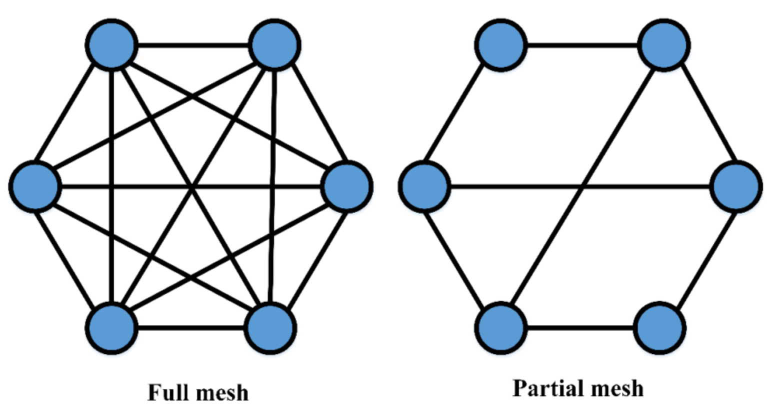


Figure 2.10 : Mesh network**.**

2.4.3 Cluster Tree Topology

Topology Cluster Tree or Set Tree in the Figure 2.11, all the sensors of each coverage area have a cluster-head. The central node serves to communicate the different sensors through the heads of sets.

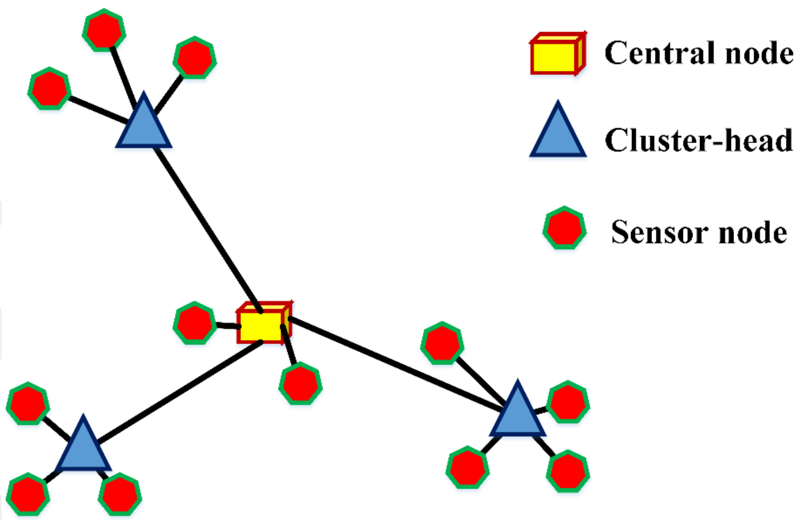


Figure 2.11 : Cluster Tree Topology

2.5 STANDARDS OF COMMUNICATION SYSTEMS

To be able to communicate the wireless network of sensors we have to know the communication standards that we have such as: Bluetooth, wireless communication systems, WiFi, ZigBee, which are explained below.

2.5.1 Bluetooth Network

It was created to replace the infrared and to suppress the connections by cables, is based on a radio link of low cost and short range. It is an easy network to establish, the best option for point-to-point links and has a high rate of data transfer. Bluetooth [8] was developed in 1998 by Bluetooth SIG (Special Interest Group), it uses the IEEE 802.15.1 standard and its data rate is from 1 MB / s to 100 MB / s. It has a range of 10 meters, operating frequency is 2.4 Ghz and has an average power consumption. Up to 10 seconds are required for the connection of the device and 2 to 8 devices can be connected. The Bluetooth network is presented in the Figure 2.12.

Figure 2.12 : Bluetooth Technology

2.5.2 Cellular Communication Systems

Among the communication standards are cellular communications systems that have evolved over time. Below we will explain some of the cellular communication systems such as GPRS, 3 G and LTE.

- **GPRS Network**

General Packet Radio Service (GPRS) or 2.5 G technology [9] in the Figure 2.13, is a technology for data transmission through packets. It emerges as evolution of GSM networks (Group Special Mobile) to provide greater speed and improvements in mobile access to data and internet services. GPRS has a data transmission speed of 40 Kbps to 150 Kbps per communication, it also allows each channel to be shared by several users and improves the efficiency of network resources. GPRS has a permanent connection, the connection establishment time is less than one second. The cost is for the amount of information transmitted and not for connection. GPRS efficiently uses the radio spectrum, shares the frequency bands with GSM and allows connection with different external data networks.

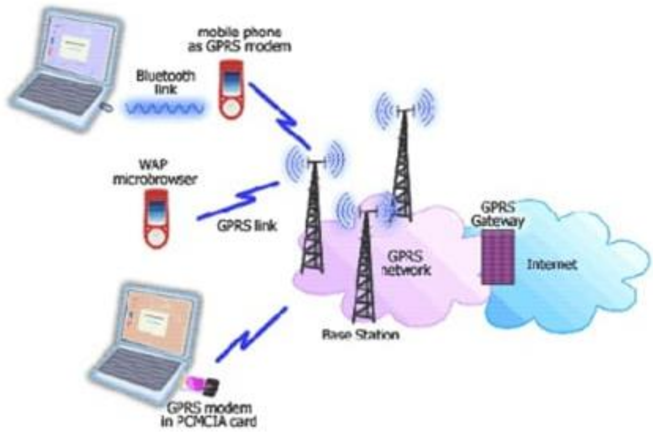


Figure 2.13 : GPRS Technology

➢ 3G Network

3G or UMTS (Universal Mobile Telecommunications System) [10] is a member of the IMT-2000 global family of the International Telecommunication Union (ITU) standards system. UMTS allows connection speeds of up to 2 Mbps, allows voice and data support in packets and average speeds is 220 to 320 Kbps. UMTS uses a combination of CDMA and TDMA technologies for efficient spectrum use. It has a higher spectral efficiency for data speeds higher than 100 Kbps. The bandwidth is on demand and multiplexed with different QoS services. The frequency bands for UMTS are the following:

- 1920-1980 and 2110-2170 MHz, for Frequency Division Duplexing (WCDMA).
- 1900-1920 and 2010-2025 MHz, for Time Division Duplexing (TDCDMA)
- 1980-2010 and 2200 MHz for satellite links.

The evolution of 3G wireless standards is presented in the Figure 2.14.

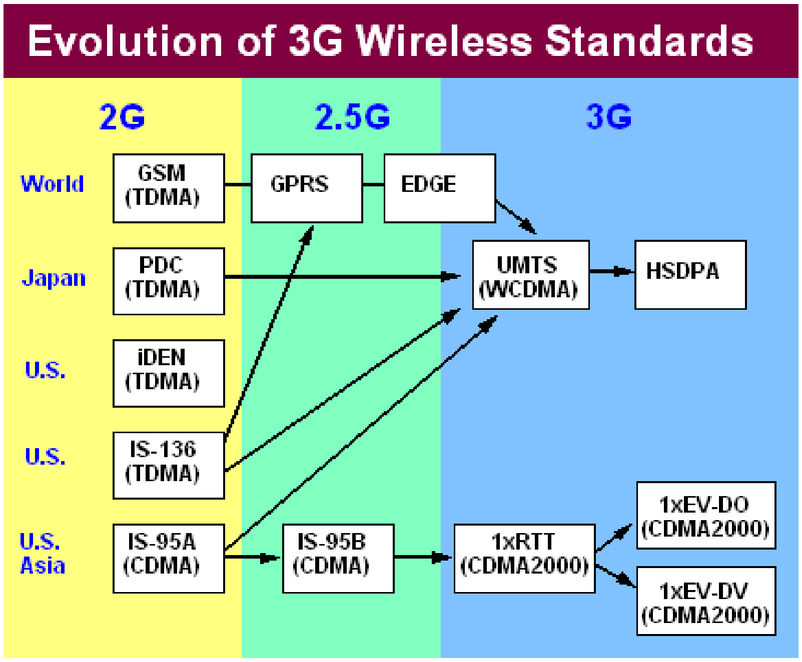


Figure 2.14 : Evolution of 3G wireless standards

➢ LTE Network

Long Term Evolution (LTE) is a radio platform technology that will allow operators to achieve maximum performance even greater than HSPA + in the upper spectrum bandwidth [11]. Work began on LTE since 2004 and its deployment began at the end of 2009, the standard developed by 3GPP. LTE is based on GSM and EDGE networks and uses UMTS and HSPA technologies of the network.

LTE is a mobile network technology that is being deployed by mobile operators in both GSM and CDMA technology paths [12]. LTE offers very fast data rates in downlink up to 100 Mbps and up to 50 Mbps. It also provides high level of spectral efficiency and low latency. LTE is compatible between 1.4 MHz at 20 MHz channel bandwidth of spectrum. It also provides a high level of performance and network capacity.

The fundamental objective of LTE is to provide high performance radio access technology and congeniality with HSPA and previous networks. Operators can easily migrate their networks due to the scalable bandwidth. The evolution of 3GPP Technology is presented in the Figure 2.15.

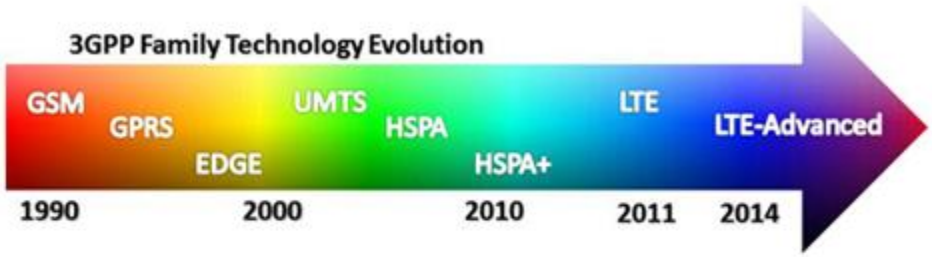


Figure 2.15 : Evolution of 3GPP Technology

2.5.3 Wi-Fi Network

It is the best known standard of all, it is a replacement for the Ethernet cable and its certification process is taken by the Wi-Fi Alliance, an independent group consisting of several electronic companies and communications. Wi-Fi [13] came out as an alternative to facilitate the work of ATM machines in 1985, the community for standardization was established in 1990 and the series was launched in 1997. The Wi-Fi Technology is presented in the Figure 2.16

Figure 2.16 : Wi-Fi Technology**.**

It has been standardized under the IEEE 802.11 standard present in Table 2.2, it has variants of the "a", "b", "g", "n" and etc. The maximum data transfer speed for the 802.11b standard is 11 Mbps and for 802.11c it has 54 Mbps. It operates on the common frequency of 2.4 GHz and the least used 5 GHz, although recently it is working on the 60 GHz frequency Wi-Fi has a range between 30 to 100 meters and a bandwidth of 0.3, 0.6 or 2 MHz. Regarding the power consumption has a high consumption and they need good backup battery if you want to use it for more than 10 hours. The size of the network can be up to 2007 nodes and for security and network override WEP, WPA and WPA2 protocols are used.

Table 2.1 : The standards of Wi-Fi network.

Standard	Speed (Maximum)	Bandwidth Frequency
802.11	1-2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mpbs	2.4 GHz
802.11g	54 Mpbs	2.4 GHz
802.11n	mas 100 Mbps	2.4 - 5 GHz

2.5.4 ZigBee Network

The wireless communication protocol is under the IEEE 802.15.4 standard, was created in 1999 and was launched in 2004, it was launched by the ZigBee Alliance [13]. ZigBee operates in the free frequency bands of the 800-900 MHz and 2.4 GHz ranges, has a specific frequency of 868 MHz for European countries. ZigBee in Figure 2.17 has a channel bandwidth of 1 MHz and has a range between 10 and 100 meters. ZigBee has a data transfer speed of only 250 Kbps and uses DSS (Direct Sequence Spread Spectrum) modulation. The power consumption is minimal, and devices powered by two AA batteries can hold up to 2 years without changing batteries. ZigBee for security uses AES 128-bit encryption, which allows authentication and encryption in communications. ZigBee is aimed at application of low levels of data transfer and low energy consumption, was designed for exchange and is more frequent in wireless sensor networks. ZigBee allows the sending of data, normally sensor information, through multi-hopped meshed networks, which allows covering large areas so they use packet forwarding by repeating nodes and with redundant links, if a route does not work , information is sent automatically through another path, which makes ZigBee a robust network suitable for application in critical environments.

Figure 2.17 : ZigBee Technology

ZigBee can have up to nodes, you can group up to 255 clusters that can have 64770 nodes. It has several uses of network topologies such as star, mesh or group of trees. There are three types of devices [14]:

- Coordinator, there can only be one per network and starts the formation of the network.
- Router, is associated with the network coordinator or another router, can act as coordinator and is responsible for the routing of multiple messages jumps.
- Final device, is the basic component of the network and does not handle routing.

3. SHORT-RANGE WIRELESS TECHNOLOGY

3.1 INTRODUCTION

Short-range wireless communications are used in applications where fast transmissions of a volume of data are not very high and efficiently. For example, in the sensor networks several devices are used to collect information about the temperature or smoke detection and communicate with other devices in order to act on that information. The members of a network like that, must have a moderate consumption so that its useful life is as long as possible and being networks that communicate in a short radius, its transmission power does not need to be very high, that is why technologies such as Wi-Fi, WiMAX or RF are not used in low power applications, because their high power and transmission speed result in excessive consumption peaks to be implemented in the sensor networks that are to be implemented.

Within the market of wireless technologies you can find various solutions that allow the connection between devices.

The specifications to which we must pay more attention when selecting one are:

1) Consumption: The selected module must have a reduced consumption so that the device allows the monitoring of the patient for as many hours as possible.

2) The interconnection capabilities: The device should allow the exchange of information with several devices in a network, therefore a module with a topology that allows flexibility when creating a network will be chosen.

3) Interoperability between different manufacturers: Although the main objective is communication with mobile phones, in the future, the device must communicate with other devices.

3.2 STATE OF THE ART

The study of short-range communication technologies offers an overview of the most remarkable aspects of each technology, paying special attention to the requirements that are set in this final degree project, as well as the interoperability between devices, the efficiency in the consumption and the ability to connect with various devices forming networks. The short-range wireless communication technologies that will be analyzed in this chapter are: classic Bluetooth, Bluetooth Smart, ZigBee and ANT / +.

3.3 CLASSIC BLUETOOTH (V2.1)

Bluetooth is a standardized wireless technology for sending and receiving data over short distances and was developed by Ericsson in 1944 [16,17]. The standard was presented to replace serial communication and its RS-232 interface, allowing communication between two nodes wirelessly. The Bluetooth brand is developed and managed by the Bluetooth Special Interest Group (SIG) and standardized by the Electrical and Electronics Engineers (IEEE) in the WPAN 802.15 working group.

Version 2.1 of the standard is available on most mobile devices, such as laptops or telephones, which use this communication technology as a substitute for wired peripherals, as well as headphones, keyboards or sensors, among others. Bluetooth has been extended, largely by its ease of pairing and omnidirectional data transfer, and can also be backward compatible with previous versions, except for the latest update of the standard, version 4.0, which has lost this retro compatibility capability to make way for a new procedure in order to reduce consumption.

The Bluetooth hierarchy is based on a point-to-point, or point-to-multipoint communication, governed by a master, which communicates with one or more slaves forming a network, called a piconet. In a piconet, the same master, can be, according to standard [18], communicated with a maximum of 7 slaves synchronized with the same clock as the master. A device with the role of master in a piconet can be attached to another piconet as a slave, forming a set of piconets, called scatter net. The exchange of information between Bluetooth is established through profiles, which are defined by the standard for its specific use in an application, such as the heart rate monitor or audio transmission. The standard also offers the possibility of creating specific profiles for any application that a manufacturer or developer wants to give.

To take an example of consumption in a device with Bluetooth v2.1 technology, the reference values of the manufacturer Bluegiga have been taken in its model WT12 [18]. Table 3.1 shows the consumption of WT12 in its most common modes. The consumption of 3 mA at rest is somewhat high, as well as the consumption peaks in the shipment or reception of data.

Table 3.1 : Consumption of the WT12 module

	Maximum Consumption Tx	**Maximum Consumption Rx**	**Minimum Consumption at rest**	**Maximum Consumption at rest**
WT12	70 mA	70 mA	56 µA	3 mA

3.4 SMART BLUETOOTH

The latest version of the Bluetooth standard was initially developed by Nokia Research Center under the name of Wibree [19,20] in 2006. The project was acquired by SIG and renamed to Bluetooth Ultra-Low Power to finally be recognized as Bluetooth Smart as in the Specification of the Bluetooth System [18] in force since 2010. The use of this technology allows devices permanently connected to the Internet, mainly sensors, to work for years without the need to renew the battery, for example, simply using a CR2032 battery throughout its useful life.

Bluetooth Smart connects with other devices in the form of star networks or point-to-point, where a central node, called master, establishes connections with slaves or peripherals. These networks are called Pico nets, as in the previous standard, but with the difference that Bluetooth Smart cannot create scatter nets, because the standard defines that a slave can only establish connection with one master at a time.

This latest version of the standard also works through profiles as in previous versions, with the difference that they are not retro compatible, because the transmission procedure is different, as well as the amount of data supported when transmitting. By leaving a gap between the versions of the standard in retro compatibility, you can use both versions in a single device which is called

Bluetooth Smart Ready. This device incorporates a driver that allows you to connect with other devices depending on the version of Bluetooth you use.

Bluetooth Smart Ready devices are devices that act as a node between both technologies in order to cover all the possibilities of connection with peripherals, such as laptops or mobile phones. This technology allows to maintain both technologies, with the advantages that each one brings, such as heart rate monitoring, with a Bluetooth Smart sensor and the transmission of audio to headphones through classic Bluetooth.

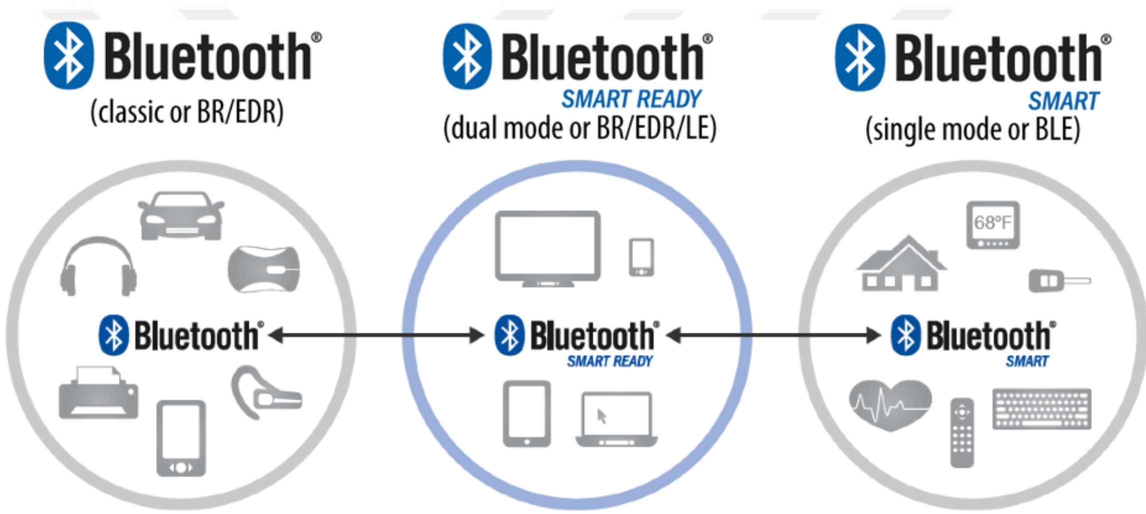


Figure 3.1 : Bluetooth Smart Ready as a link between Bluetooth Smart and classic

The Table 3.2 compares the specifications between both versions. The Bluetooth Smart device, chosen for comparison, is the model BLE112 [20] from the manufacturer Bluegiga.

The maximum consumption, as shown in Table 3.3, is lower compared to the previous version of the standard, likewise it has also improved in the ways in which the device is at rest. With this data it is possible to estimate an improvement in the aspect of consumption between the two generations of Bluetooth. The Bluetooth Smart device, chosen for comparison, is model BLE112 [20] from the manufacturer Bluegiga.

Table 3.2 : Comparison between classic Bluetooth and Bluetooth Smart

Technical Specification	Classic Bluetooth	Smart Bluetooth
Frequency	2.4GHz	2.4GHz
Operating range	~ 10-100 meters	~ 10-100 meters
Transfer speed	1-3 Mbps	1 Mbps
Slaves	7	Theoretically unlimited
Security	56 a 128 bit	128 bit AES
Sturdiness	FHSS	FHSS
Connection Time	100 ms	< 6 ms
Use of technology	Worldwide	Worldwide
Certifier	Bluetooth SIG	Bluetooth SIG
Transmit voice	Yes	No
Communication network	Point to point, scatter net	Point to point, star
Reference consumption	1	$^1/_2 - ^1/_{1000}$ [121]
Use of services	Yes	Yes
Use of profiles	Yes	Yes
Main use	Audio, video, files of data	Sports, health, safety, home automation.
Outline	Serial port, hands-free, OBEX *, A2DP **, among others.	Proximity sensor, battery level, thermometer, among others

** OBEX: Binary object exchange communication protocol*

*** A2DP: Advanced Audio Distribution Profile*

Table 3.3 : Consumption of the BLE112 module

	Maximum Consumption Tx	Maximum Consumption Rx	Minimum Consumption at rest	Maximum Consumption at rest
BLE112	36 mA	25 mA	0.4 µA	235 mA

3.5 ANT/ANT+ TECHNOLOGY

The ANT technology [21] was developed in 2004 by Dynast ream Innovations Inc., A subsidiary of Garmin. ANT is a protocol of wireless communication of low consumption, used in sanitary, sports applications or of any type of monitoring that needs sensors.

ANT + is an update of the technology that adds more modes of interoperability between devices, being compatible with the previous ANT technology. The network topology in ANT / +, allows connections in star, mesh or point to point and the devices are characterized by the roles of master and slave. The exchange of information is done like Bluetooth, through profiles, where each profile is linked to the use of a specific application.

ANT / + is a proprietary technology, and its development is private and not standardized for the creation of a free application. In order to implement this technology in a device, it is necessary to comply with the requirements of the owner company and thus obtain a certification that approves the use of the application. The consumption of an ANT / + device, model ANTAP281M4IB [21], as specified by the manufacturer is summarized in Table 3.4.

The module ANTAP281M4IB stands out for its low consumption when transmitting or receiving data, that means an energy saving in communications using this module.

Table 3.4 : Consumption of the ANTAP281M4IB module

	Maximum Consumption Tx	Maximum Consumption Rx	Minimum Consumption at rest	Maximum Consumption at rest
ANTAP281M4IB	15 mA	17 mA	0.5 µA	2 µA

3.6 ZIGBEE MODULE

Zigbee technology [22] is a specification for wireless data transmission, based on the IEEE 802.15 standard. It was created in 2002 by an alliance between different multinationals, universities, government regulatory groups and other institutions, both public and private, with the aim of creating a new standard for low-power wireless communication.

The standardization of the ZigBee technology, like Bluetooth, allows the applications developed by the manufacturers to be completely interoperable with each other, thus guaranteeing the end customer reliability, control, security and comfort. ZigBee communication is used in embedded applications with very low data transmission and energy consumption requirements, where, for example, it can be used to perform industrial control, collect data from sensors, and systems such as smoke detection or intruders to home automation.

The communication topology in ZigBee can be done by star, tree, point a point or mesh:

1) In the star configuration, one of the devices assumes the role of network coordinator and is responsible for initializing and maintaining the devices in the network. All other ZigBee devices, speak directly with the coordinator and are called end devices.

2) In the mesh configuration, a device acts as the coordinator and is responsible for initializing the network and choosing the parameters of the network, but the network can be extended through the use of ZigBee routers. The routing algorithm uses a question-answer protocol to eliminate routes that are not optimal. The final network can have up to 254 nodes. Using local addressing, you can configure a network of more of 65,000 nodes divided into 255 subnets.

Table 3.5 shows the consumption of a device, as indicated by the technical specifications of an XBee RF module [23].

The consumption of the module is at acceptable values for low consumption applications. The resting modes allow the device to compensate the energy expenditure of the peaks in the data transfer.

Table 3.5 : Consumption of XBee RF module

	Maximum Consumption Tx	Maximum Consumption Rx	Minimum Consumption at rest	Maximum Consumption at rest
XBee RF	45 mA	50 mA	10 µA	10 µA

Comparison and choice of technology

The study compiles the possibilities provided by each standard and an example of each technology is analyzed in the implementation of a manufacturer of said technology in order to obtain real data on consumption, scope and speed among others.

Among the short-range wireless communication technologies that exist in the market, one must choose one that meets the specific requirements established by the project's objectives. The project requires a technology capable of establishing communications with several devices in a network, that has interoperability between devices of other brands that implement the same technology and also that consumption is moderate in order to optimize the battery life of the devices.

Table 3.6 and Table 3.7 summarizes the characteristics of the modules offered by the manufacturers of each technology.

Bluetooth has better specifications in terms of real effective speed and security with respect to ANT / +, in addition to the ease of implementation offered by the technology to create an application with Bluetooth standard only with the module of the manufacturer, certified by Bluetooth SIG. It is interesting from the point of view of the development of the project due to the low cost and the rapidity in which an application can be made ready for its real use. The ANT / + module, on the other hand, has a lower consumption and the creation of networks, like ZigBee, seems to be an interesting point because it can be adapted to the most convenient topology for each application.

Table 3.6 : Comparison between modules of wireless communication technologies

	Bluegiga WT12 (Classic Bluetooth)	**Bluegiga BLE112 (Bluetooth Smart)**	**ANTAP281M4IB (ANT / ANT +)**	**Digi Xbee (ZigBee)**
Indoor reach	10 m	10 m	10 m	10 m
Frequency	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz
Theoretical speed	2-3 Mbps	1 Mbps	1 Mbps	250 Kbps
Effective speed	2.1 Mbps	250 Kbps	20 Kbps	64 Kbps
Topology	Point to point, mesh and scatter net	Point to point and star	Point to point, mesh, star and tree	Point to point, mesh, star and tree
Number of nodes	7 nodes	5917 nodes	300 nodes	65535 nodes
Security	56-bit key	128-bit AES	64-bit key	128-bit AES
Wake-up time	100 ms	6 ms	0 ms	30 ms
Certification	Bluetooth SIG	Bluetooth SIG	Garmin	ZigBee Alliance
Network standard	IEEE 802.15.1	IEEE 802.15.1	Owner	IEEE 802.15.4

The communication topologies of ZigBee and ANT / +, offer the possibility of increasing the number of devices by the different network structures, being able to create networks of multiple nodes and manage effectively, due to the roles acquired by the members of the network. the net. But in the requirements of the project, they specify that the members of the network must be able to communicate with other types of devices, such as headphones or mobile phones, so interoperability between elements, would require a separate implementation for these cases, since In the market there is little variety of devices, such as mobile phones or audio devices that use these technologies.

Bluetooth, on the other hand, brings the advantage of the number of devices in the market that use this technology to communicate and the interoperability it offers among them. Between the two versions of the standard, this advantage is present in both, but to a lesser extent for Bluetooth Smart, since it has just been released to the market, but with the arrival of Smart Ready devices, Bluetooth can reach two main modes of communication with the advantages that each one brings.

Table 3.7 : Comparison of consumptions between modules

	Maximum Consumption Tx	**Maximum Consumption Rx**	**Minimum Consumption at rest**	**Maximum Consumption at rest**
WT12	70 mA	70 mA	56 µA	3 mA
BLE112	36 mA	25 mA	0.4 µA	235 mA
ANTAP281M4IB	15 mA	17 mA	0.5 µA	2 µA
XBee RF	45 mA	50 mA	10 µA	10 µA

Another requirement of the project is the consumption of the module to transmit and send the information. In this aspect, the modules that have a lower consumption are those designed to transmit small data frames, such as the modules that implement the Bluetooth Smart, ANT / + and ZigBee technologies. In the case of the classic Bluetooth WT12, when offering profiles, such as audio transmission or data files, which requires movements of large amounts of data at a higher speed, it has as a consequence a higher consumption, as in the case of a video call, that the voice data have to arrive in real time in both directions of the channel.

3.7 SUMMARY

The current 9x2 device with Bluetooth 2.1 and ZigBee technology used in projects like REMPARK, offers a wider range of possibilities, being able to establish connections with more devices than if only using a single technology. The device has drawbacks for communication with a mobile phone by ZigBee, since the technology is not present in mobile phones (with the exception of the implementation through the USD-ZigBee card, whose associated problems do not allow its extended use). Likewise, both technologies in the same device also increase their size and consumption to achieve the same purpose, therefore, it is necessary to implement a technology that includes compatibility with the majority of peripherals that will be used.

The best option in the aspect of compatibility is Bluetooth, since its extensive range of profiles has made proliferate in the market a large number of peripherals compatible with each other, besides being able to be used in mobile phones and computers. But the consumption of these modules is high for applications that require little data traffic and long duration, such as sensors, thus, Bluetooth Smart is presented as an option to these peripherals.

The star network typology allows a device to manage, with a single technology, the network of sensors and actuators that they require in projects such as REMPARK. For example, the devices used in this project would be configured in the following way in a star Bluetooth network:

- The 9x2 device, would communicate by Bluetooth Smart with another sensor, such as the wrist, to detect the condition of the patient from the waist and the tremor from the wrist. In addition, it would communicate, also with Bluetooth Smart, with the mobile phone to send the data to a server. As it is a low-consumption technology, it would optimize the battery of the sensors, in addition to being able to communicate with the mobile phone in a native way.

- The mobile phone would have a Bluetooth Smart Ready module to establish connection with the sensors, through Bluetooth Smart, and with other peripherals, such as headphones, with classic Bluetooth. The phone has a battery with more capacity than the sensors, so this device is ideal for managing the network

4. SYSTEM SIMULATIONS AND RESULTS

4.1 STATE OF THE ART

The WSNs are an innovative technology that has allowed the creation of sensor networks that were previously unrealizable with wired sensors, learning new perspectives and application fields. But this technology is still under development, there are still problems that limit its use.

In the previous chapter, a description of the several wireless mesh sensor networks for a building community used in this dissertation were presented. In the present chapter the simulation settings used and the results obtained will be addressed.

4.2 SYSTEM DESCRIPTION OF BMSN

In this section, we look at the full system simulation model and software of the security monitoring system based on Bluetooth Mesh Sensor Network (BMSN) and the main building blocks. As indicated by Figure 4.1, the BMSN comprises of a simulation component and software programs. The full simulation component in the designed system is divided into four circuits and all circuits dependent to five parts . The main part of the simulation parts is the Arduino Nano, motion sensor and Bluetooth HC-06. The open source Arduino IDE program was used to program the full system.

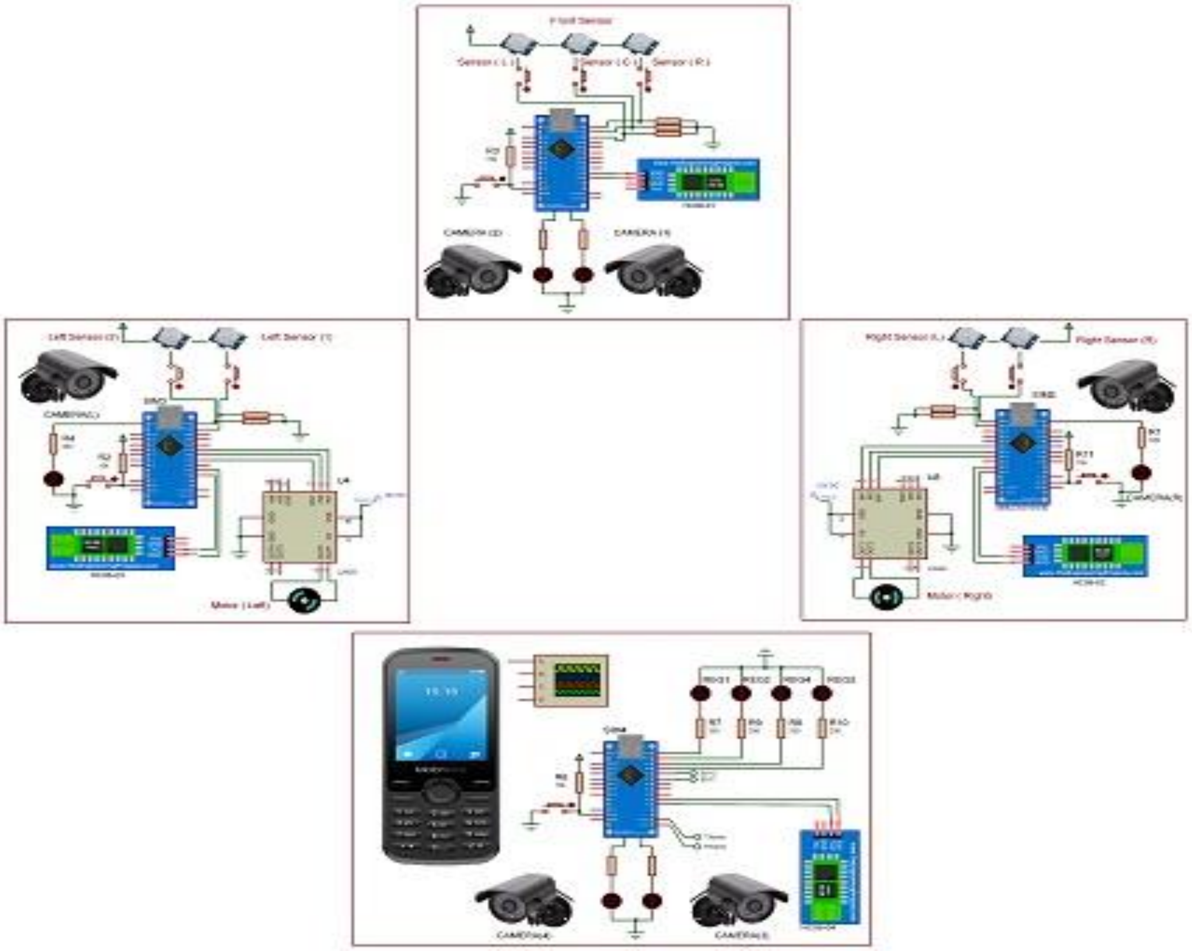


Figure 4.1 : The full system simulation of the BMSN

4.2.1 Simulation Circuit Of The BMSN.

The main circuits and components of the BMSN simulation circuits in the Figure 4.1 are divided into Five parts:

1. Arduino microcontroller : The Arduino Nano microcontroller in the Figure 4.2 (a) is the main part of the BMSN circuits, the main bin diagram of the Arduino Nano is present in the Figure 4.3 and the main properties of this microcontroller is presented in the Table 4.1[25].

Table 4.1 : Main properties of Arduino Nano [25]

Parameter	Value
Microcontroller	ATmega328P – 8 bit AVR family microcontroller
Operating Voltage	5V
Recommended Input Voltage for Vin pin	7-12V
Analog Input Pins	6 (A0 – A5)
Digital I/O Pins	14 (Out of which 6 provide PWM output)
DC Current on I/O Pins	40 mA
DC Current on 3.3V Pin	50 mA
Flash Memory	32 KB (2 KB is used for Bootloader)
SRAM	2 KB
EEPROM	1 KB
Frequency (Clock Speed) Communication	16 MHz IIC, SPI, USART

2. Motion sensors : The motion sensors in Figure 4.2(b) or PIR (Passive Infrared Sensor) is a sensor that is usually used to detect a human movement or to enter a human being somewhere. And unlike the infrared sensor Infrared Sensor (IR sensor) It does not contain a transmitter of the red light, but receives this radiation from the surrounding bodies. Hence Passive. The motion sensor applications are used to detect the human body to protect against theft, lighting a lamp or opening a door or for the economy of electric power. But to know how to work a sensitive movement must first know that anybody has a temperature of more than zero degree of sending infrared energy. The higher the temperature of the body increased the proportion of energy emitted from it. This energy or radiation cannot be seen with the naked eye (the camera can be used to see it), but the pyrolytic materials within the PIR sensor can detect this radiation. For the information only, the pyroelectric materials used in the PIR sensor include Glymantride, Cassim Nitrate, and Lithium[27].

3. Bluetooth HC-06: This type of Bluetooth module in Figure 4.2(c) can easily achieve wireless data transmission serial. Its operating frequency is 2.4GHz ISM frequency band for medical, Industrial, scientific applications. It adopts Bluetooth 2.0 + EDR standard. In

Bluetooth 2.0, the signal transmission time of the various devices stands at a time interval of 0.5 seconds, so the workload of the Bluetooth chip can be greatly reduced and more sleep time can be provided for Bluetooth. This module is set with a serial interface, is easy to use and simplifies the design and development cycle in general. The main properties of the Bluetooth HC-06 are presented in Table 4.2[24].

Table 4.2 : Main properties of Bluetooth Transceiver Module HC-06[24]

Parameter	Value
Bluetooth protocol	Bluetooth 2.0+ EDR standard
USB protocol	USB v1.1/2.0
Operating frequency	2.4GHz ISM frequency band
Transmit power	≤ 4dBm, second stage
Sensitivity	≤-84dBm at 0.1% Bit Error Rate
Transmission speed	2.1Mbps(Max)/160 kbps(Asynchronous) ; 1Mbps/1Mbps(Synchronous)
Supply Voltage	+3.3 VDC 50mA
Operating temperature	-20 to 55℃
Size and Weight	36.5*16mm Weight: 4g

4. Motor driver circuit : This circuit is a used to drive the camera's motor and move the camera to left or right. Figure 4.2(d) presents this circuit.

5. Mobil phone : In the full system of BMSN used any older phone instrument just to send the SMS to any phone number selected.

4.2.2 Software’s Of The BMSN.

In general, the Arduino language is a set of C/C++ functions and then is passed directly to a C/C++ compiler that can be used with my software. This program is open-source Arduino Software (IDE) It runs on Windows, Mac OS X, and Linux. The Arduino IDE is a free software electronics prototyping platform based on flexible, easy to use all types of Arduino hardware’s and software. The IDE makes it easy to write code and upload it to the board. Figure 4.4 shows the main widows of the IDE software[19].

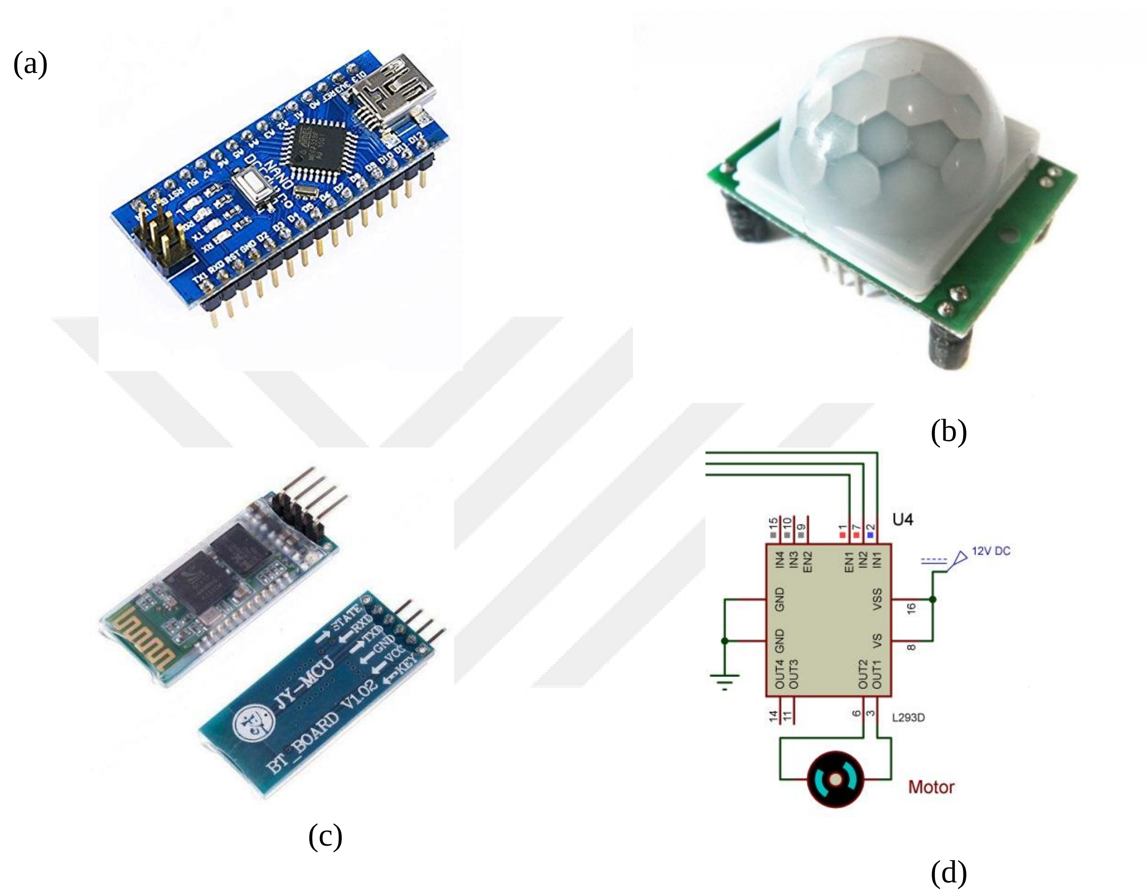


Figure 4.2 : Main Component of the BMSN:(a) Arduino Nano kit,(b) motion sensor, (c) Bluetooth HC-06 and (d) motor driver circuit

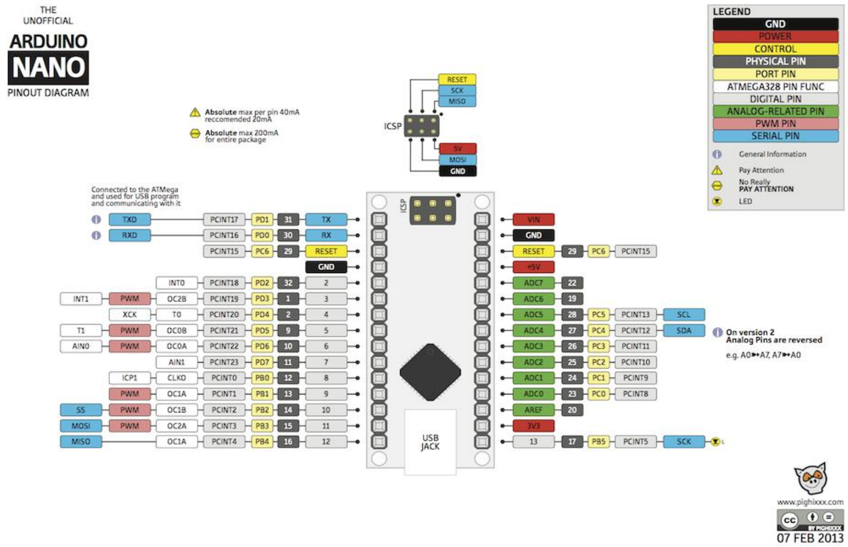


Figure 4.3 : The main bin diagram of the Arduino Nano[25]

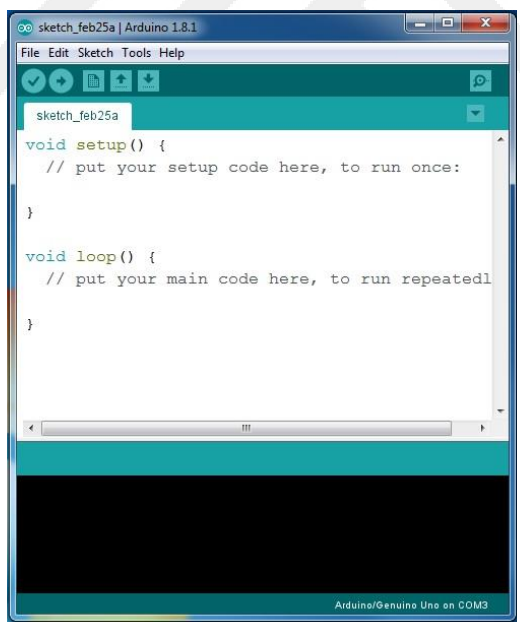


Figure 4.4 : The main widows of the IDE software[26].

4.3 SYSTEM SIMULATION RESULTS

The flowcharts of security monitoring system based on Bluetooth mesh sensor network are shown in Figure 4.5 to Figure 4.8. The flowcharts of the system are divided into four programs. Figure 4.5 shows a flowchart of the front monitoring circuit, this flowchart presents how to check the status of the three motions sensors output , turn ON/OFF the cameras and then send the status of sensors to the main, left and right circuits. Figure 4.6 shows a flowchart of the right monitoring circuit. This flowchart presents how this circuit receives the signals from the front circuit, turn ON/OFF the cameras and sending the states of the sensors to the main circuit. Figure 4.7 shows a flowchart of the left monitoring circuit. This flowchart presents how this circuit receives the signals from the front circuit, turn ON/OFF the cameras and sending the states of the sensors to the main circuit. The last flowchart in Figure 4.8 shows the main circuit flowchart. This flowchart presents the full status of the system according the Bluetooth signals from the front, right and left circuits and how to send the warning SMS.

In this part will be present and discuss the simulation results of the full system. The system is simulate (1) by using Proteus 8.4 Professional software[28]. The results in this work can be divested more than seven situations, but will be discuss only seven according to the movement of the human:

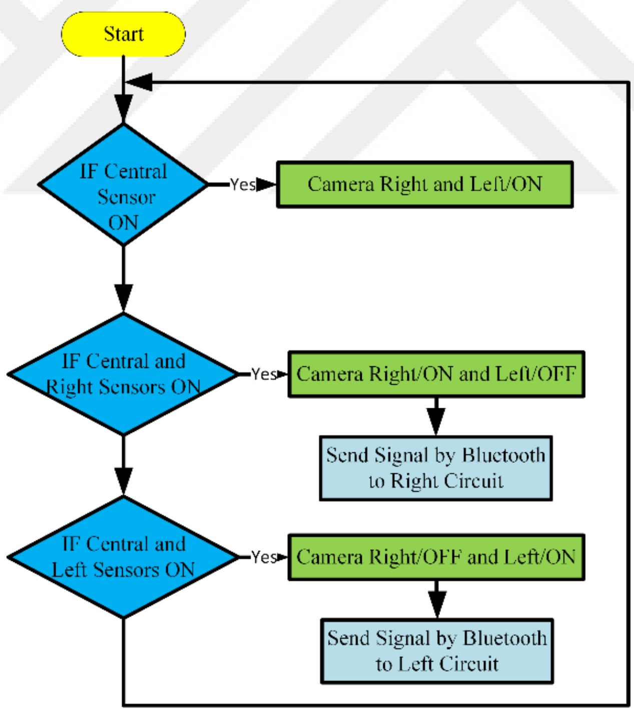


Figure 4.5 : Flowcharts of the front circuit

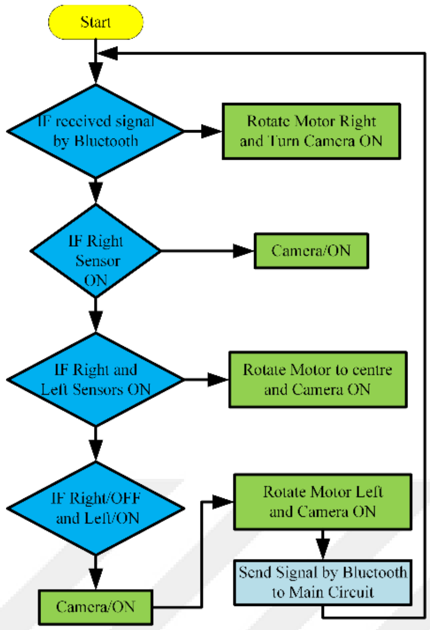


Figure 4.6 : Flowcharts of the right circuit

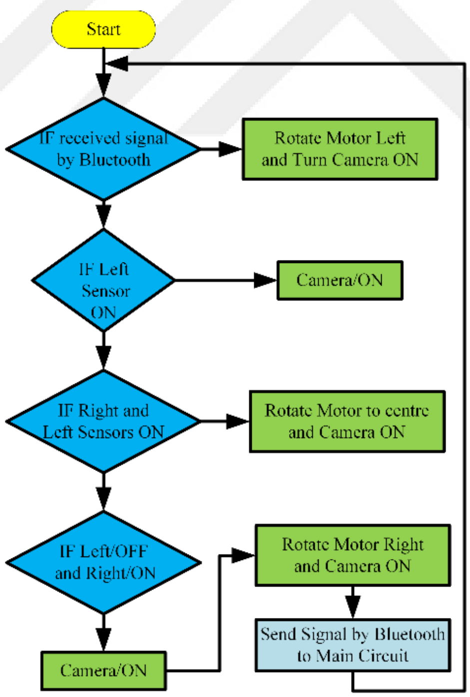


Figure 4.7 : Flowcharts of the left circuit.

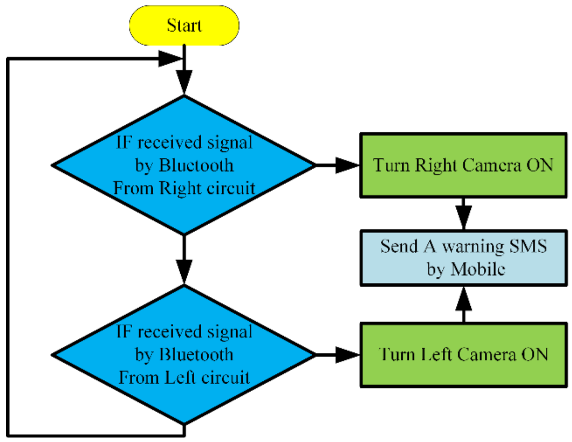


Figure 4.8 : Flowcharts of the main circuit

4.3.1 Situation 1.

In this situation, the person stands in Front of the building entrance. Figure 4.9(a) explain locate the person in this situation, in this case the central sensor in the front circuit is ON and the Left and right sensors are OFF, Figure 4.9 present the front circuit with situation of the cameras (the camera right and left are ON) and the output results of the sensors are presented in the Figure 4.9 (c).

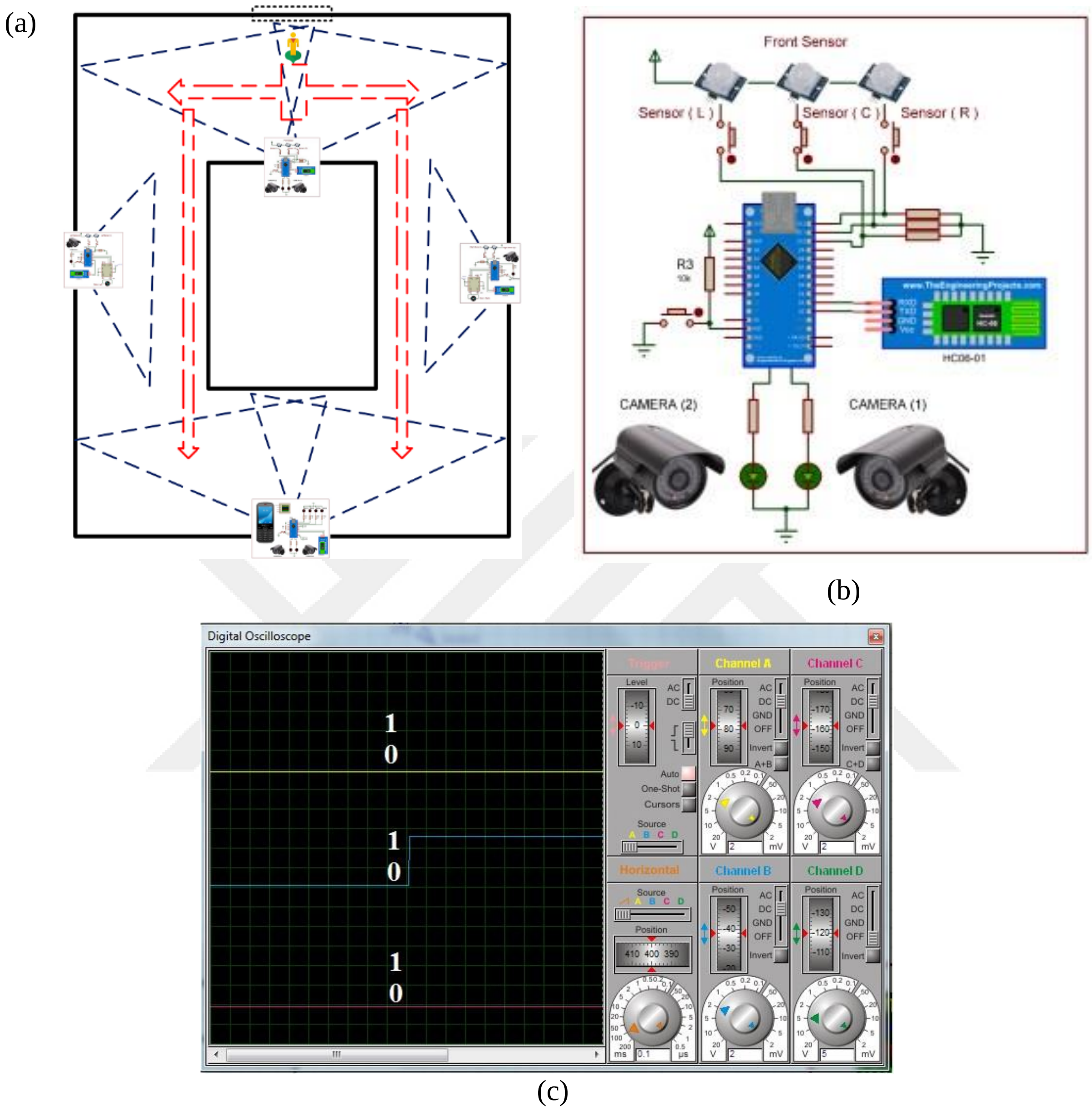
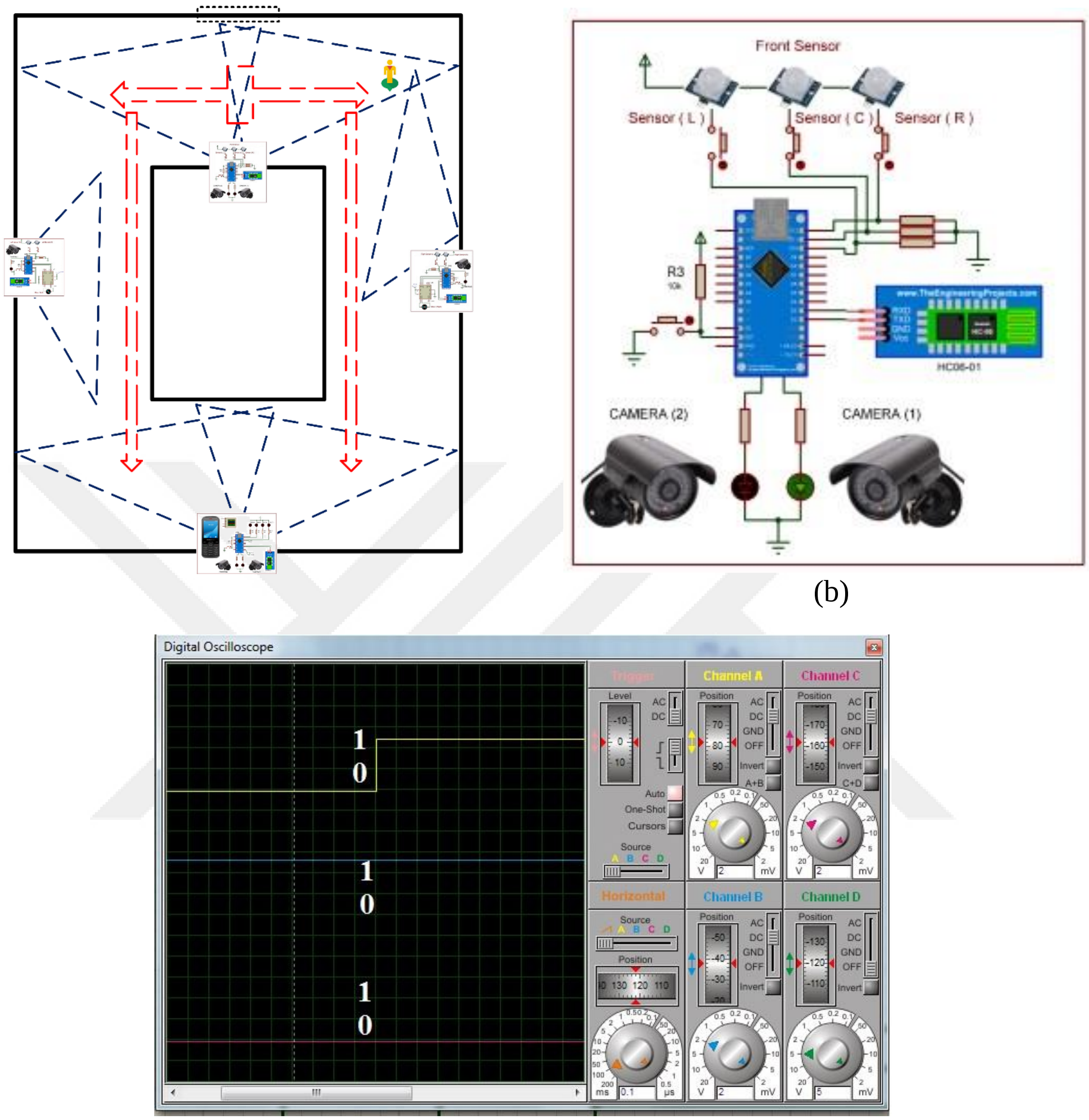


Figure 4.9 : Situation 1 states and results:(a) The person location,(b) circuit diagram and the situation of the cameras and (c) sensors output results

4.3.2 Situation 2.

In this situation, the person stands in Front-Right of the building entrance. Figure 4.10 (a) explain locate the person in this situation, in this case the central and right sensors in the front circuit is ON and the left sensor is OFF, Figure 4.10 (b) present the front circuit with situation of the cameras (the camera right is ON and left is OFF) and the output results of the sensors are presented in the Figure 4.10 (c).

(a)



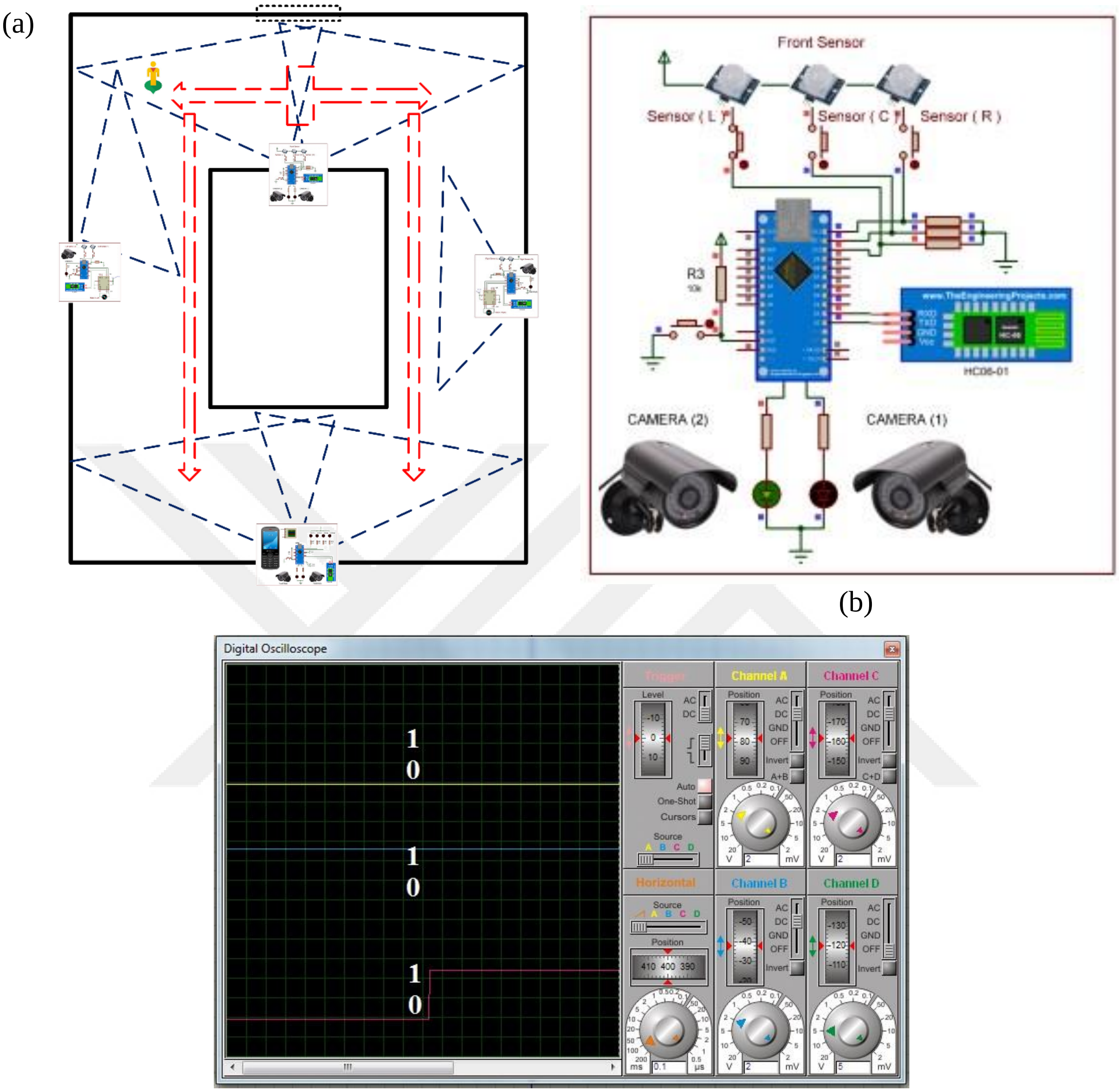
(b)

(c)

Figure 4.10 : Situation 2 states and results:(a) The person location,(b) circuit diagram and the situation of the cameras and (c) sensors output results

4.3.3 Situation 3.

In this situation, the person stands in Front-Left of the building entrance. Figure 4.11 (a) explain locate the person in this situation, in this case the central and left sensors in the front circuit is ON and the right sensor is OFF, Figure 4.11 (b) present the front circuit with situation of the camera and output results of the sensors are presented in the Figure 4.11 (c) (the camera right is OFF and left is ON).

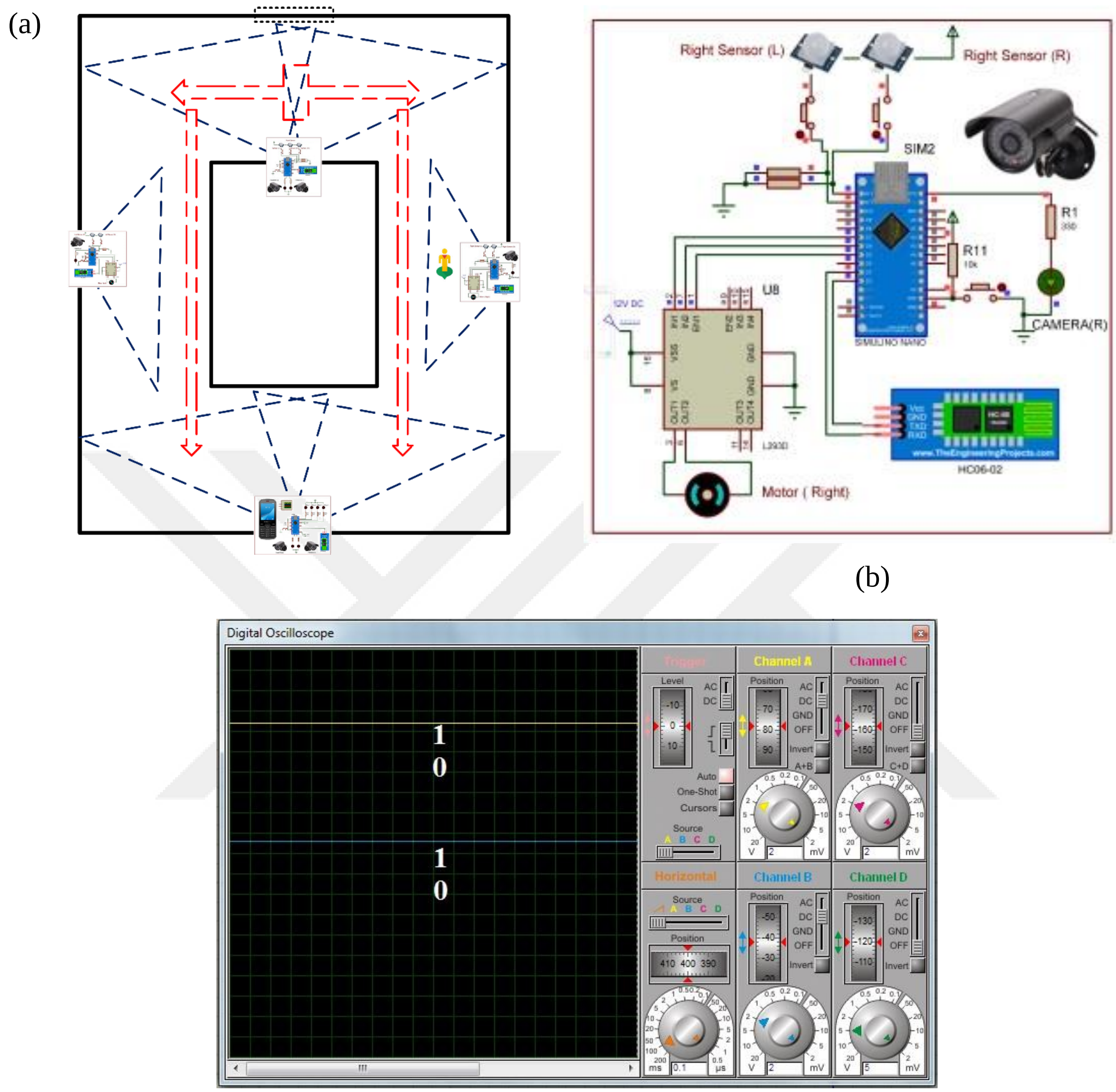


(c)

Figure 4.11 : Situation 3 states and results:(a) The person location,(b) circuit diagram and the situation of the cameras and (c) sensors output results

4.3.4 Situation 4.

In this situation, the person stands in canter of Right side of the building. Figure 4.12 (a) explain locate the person in this situation, in this case the central and left sensors in the front circuit is ON and the right sensor is OFF, Figure 4.12 (b) present the front circuit with situation of the cameras (the camera is ON) and output results of the sensors are presented in the Figure 4.12 (c).

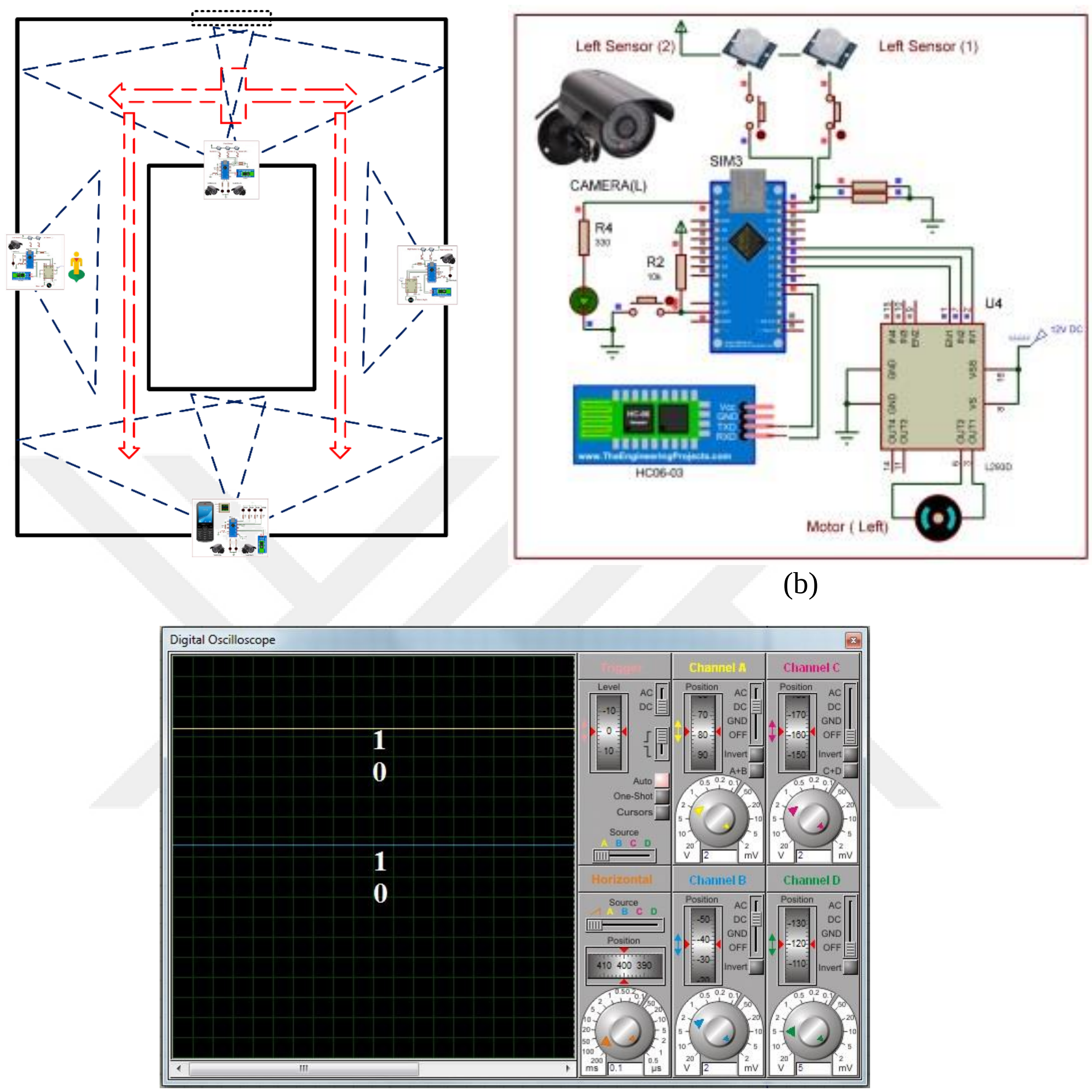


(c)

Figure 4.12 : Situation 4 states and results:(a) The person location,(b) circuit diagram and the situation of the cameras and (c) sensors output results

In this situation, the person stands in canter of Light side of the building. Figure 4.13 (a) explain locate the person in this situation, in this case the central and left sensors in the front circuit is ON and the right sensor is OFF, Figure 4.13 (b) present the front circuit with situation of the camera(the camera right is ON). and output results of the sensors are presented in the Figure 4.13 (c).

(a)



(b)

(c)

Figure 4.13 : Situation 5 states and results:(a) The person location,(b) circuit diagram and the situation of the cameras and (c) sensors output results

4.3.5 Situation 6.

In this situation, the person stands in left of the building entrance. Figure 4.14 (a) explain locate the person in this situation, in this case the central and left sensors in the front circuit is ON and the right sensor is OFF, Figure 4.14 (b) present the front circuit with situation of the camera and output results of the sensors are presented in the Figure 4.14 (c) (the camera right is OFF and left is ON).

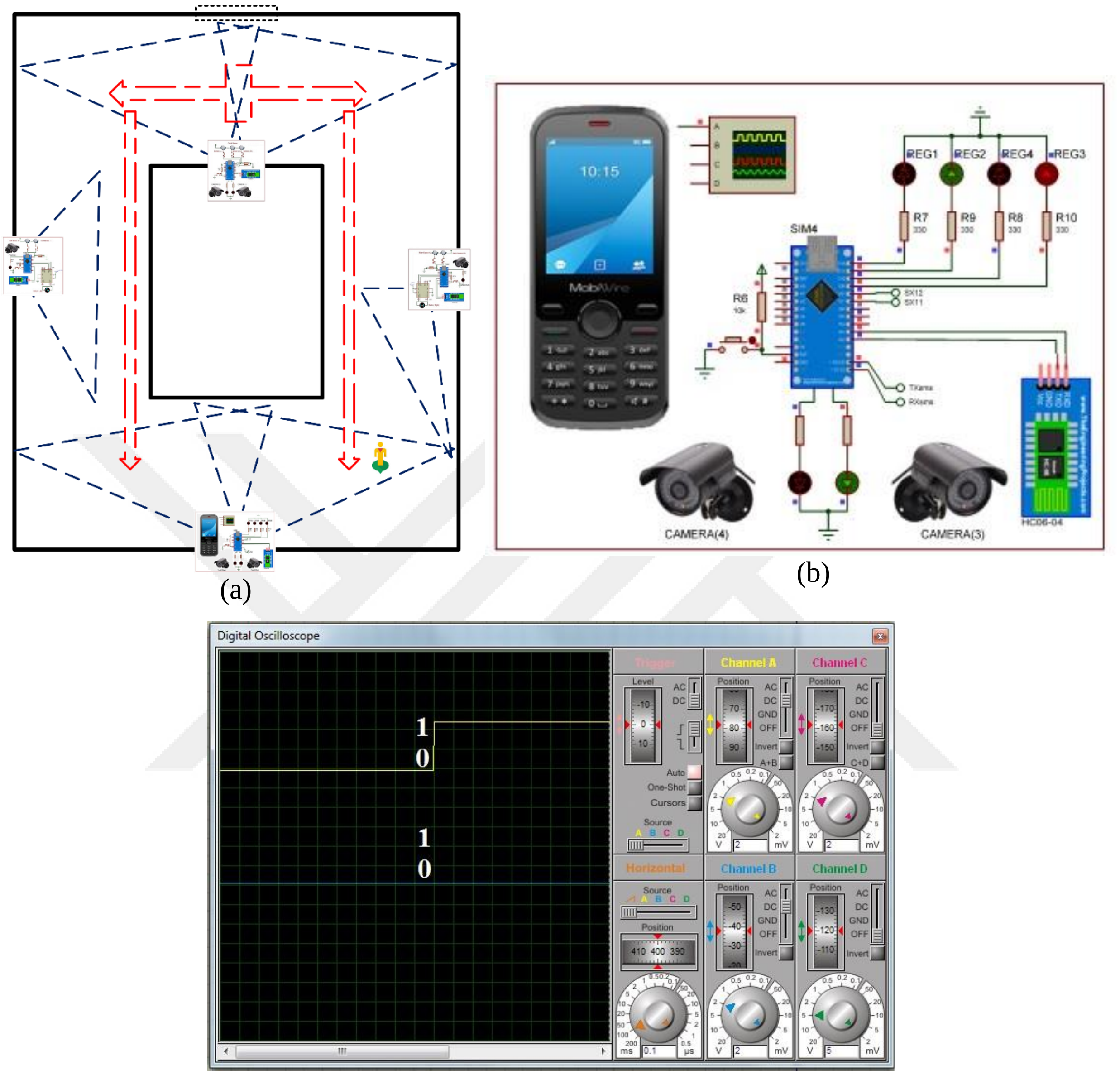


Figure 4.14 : Situation 6 states and results:(a) The person location,(b) circuit diagram and the situation of the cameras and (c) sensors output results

4.3.6 Situation 7.

In this situation, the person stands in left of the building entrance. Figure 4.15 (a) explain locate the person in this situation, in this case the central and left sensors in the front circuit is ON and the right sensor is OFF, Figure 4.15(b) present the front circuit with situation of the camera and output results of the sensors are presented in the Figure 4.15(c) (the camera right is OFF and left is ON).

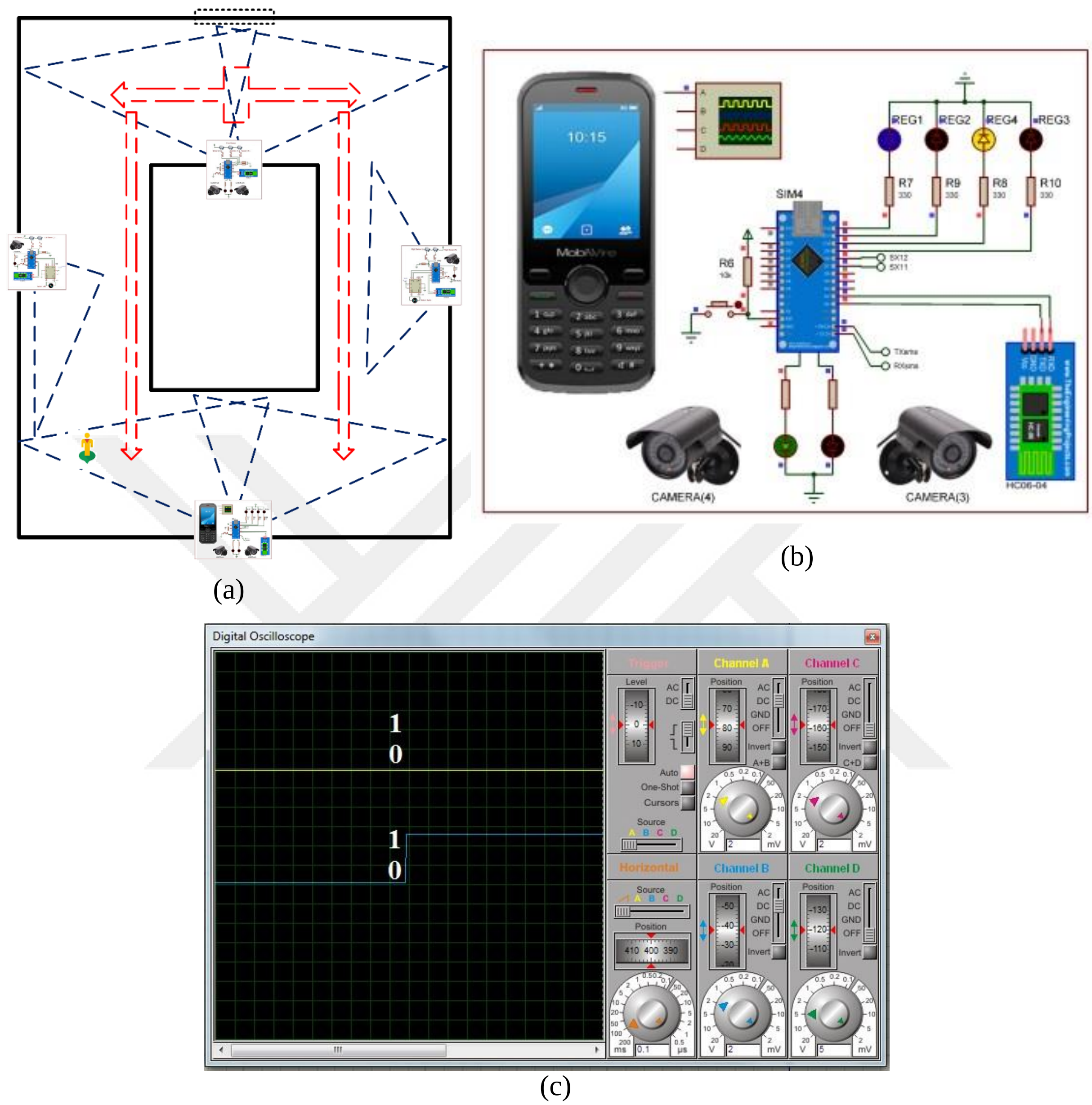


Figure 4.15 : Situation 7 states and results:(a) The person location,(b) circuit diagram and the situation of the cameras and (c) sensors output results

For (situation 6 and Situation 7), the person stands in Left or Right side of the end of the building present the same results. Figure 4.14(a) and Figure 4.15(a) explain locate the person in this situations, the right sensor is ON and left sensor is OFF in the end(master) circuit, the camera right ON ,and the master circuit in the end of the building send the warring SMS. Figure 4.16 present the output signal result of the SMS from mobile.

For (situation 6 and Situation 7), the person stands in Left or Right side of the end of the building present the same results. Figure 4.14(a) and Figure 4.15(a) explain locate the person in this situations, the right sensor is ON and left sensor is OFF in the end(master) circuit, the camera right ON ,and the master circuit in the end of the building send the warring SMS. Figure 4.16 present the output signal result of the SMS from mobile.

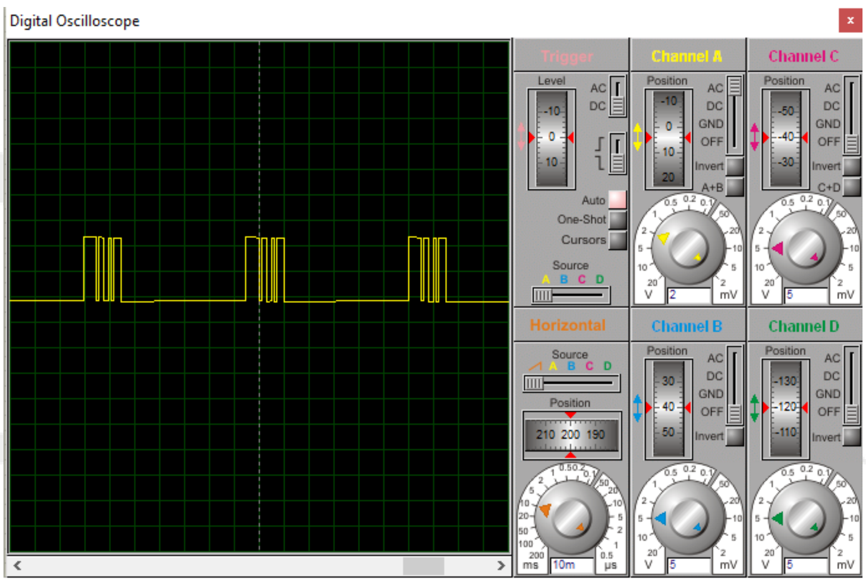


Figure 4.16 : The output signal result of the SMS from mobile

5. CONCLUSIONS AND FUTURE WORK

5.1 CONCLUSIONS

The ability of self-healing and self-organization is key factor in WMNs which reduces the network complexity and maintenance. Provides the backbone ability through which a user can connect to internet anywhere any time. WMNs are a promising technology for next generation wireless networking. WMNs have enhanced the capability and reliability of ad hoc networks. There are still many problems in WMNs which needs to be improved. The existing approaches are effective at specific layers but there is still need to have a comprehensive mechanism which can prevent from the attacks at protocol layers. For self-healing and self-organization WMNs still requires an inclusive protocol. The main focus of this thesis survey is to provide right recommendation and direction towards security enhancement. The security solutions used in Wireless LANs are not getting ready for WMNs. Cryptography, key management; WEP and TKIP are considerable solutions which are available right now for WMNs devices. IEEE task group defines 802.11s which is a pre-draft for wireless mesh networks. In near future it can be deployed with its full functionality. Right now 802.11s is using the techniques of 802.11i. There are still many research problems in WMNs but it is most promising technologies for next-generation wireless networking. As a promising scheme for next generation networks, the wireless mesh network is superior in flexibility and for introducing new revenue. However, the security issues on each layer of the backbone and access networks are still problematic for massive deployment. Simultaneous research on network performance and device behavior monitoring in this rapidly developing network will realize both security and network design.

In chapter 3 an overview of existing related Bluetooth technology has been presented. It has centered on the key areas of wireless mesh networks and sensor networks. A number of advantages that such a network could provide a building community have been discussed.

In this work, we designed a new Security Monitoring System for smart home and bulling application. This system designed base on Bluetooth Mesh Sensor Network (BMSN), because the Bluetooth (HC-06) used due to with low energy consumption and 100 m communication distance between point to point. In addition it has been used GSM mobile to send the warning message from the master control system. The Bluetooth sensors network is one of the most important Internet of thinks (IOT) application. The Arduino Nano was used as microcontroller unit for each parts of the networks. The Arduino Nano receives signals from the motion sensors until the cameras are controlled and also send and received the signals between two parts in the mesh sensor network by Bluetooth and depending on these signals, the cameras are turned ON and OFF and moved Right or Left. The system was described and simulated in our research and all the results were discussed . The main advantage of this work is to design of a cheap Bluetooth sensors security network with low storage capacity in terms of recording control videos.

One of the key appearances of the system is the capability to track individual sensor nodes. This provides the ability of monitoring the location of person, pets or assets within the targeted area. The network uses sensor nodes that are wirelessly connected to a fixed infrastructure of mesh nodes strategically place to cover the target area. This allows for more flexibility in sensor deployment. It has been apparent that the use of transmit-only sensor nodes can be advantageous in term of cost, power and complexity. The sensor node software designs have been presented. The sensor node has been prototyped to a developed stage with tests and results presented. The battery powered sensor nodes uses a mechanical motion sensor which powers the device when activated.

5.2 FUTURE WORK

As Wireless mesh network security is still in its infancy so it is quite difficult to overcome on these threats and attacks. Security is a tough challenge which influences the deployments of wireless mesh networks however there should be strong efficient solution for WMNs. The security requirement varies in different scenarios. There trusted

relationship should be developed between the users. As authentication, authorization, and accounting are important parameters so there will be trusted handshakes between the users. By following these recommendations one can overcome on many problems, issues, threats and attacks. Numerous ideas exist for extending the work in this dissertation. These ideas are now outlined:

1) Proper implementation and management of security controls is needed

2) Network management tools need to be developed for mesh design, maintenance, monitoring and management

3) Still need better and secure routing protocols to handle multi-hop networks and other issues unique to WMNs.

4) Performance management is very important from administrative prospective because through proper management an administrator can overcome on many threats.

5) Neighbor monitoring to avoid from malicious attacks

6) Protect the privacy of users as the position of user can easily be determined

7) Presently, this proposed WMSN application is a monitor-only system. It would be worth investigating, as part of future work, the possibility of incorporating and implementing control aspects. Possible applications include being able to remotely switch on/off lights, control temperature and even water garden plants. In part, this could be achieved without any hardware modifications and only minor software changes. The building node offers a solution, as it is equipped with a transceiver and is not part of the fixed infrastructure of mesh nodes. Therefore it can be deployed at any location in the system. To minimize the software changes required, control commands from the base station could be broadcast and relayed to all nodes. This would avoid the need to establish ‘reverse’ routes from the base node to a destination building node. Another feature of control is that pertaining to the sensor node. Being able to send data to the sensor node would allow for the possibility of “paging” person wearing these nodes.

8) Encouraging future research will look to increase the number of sensing and monitoring performances and too to expand the capabilities of the system by addressing some/all of the future work possibilities outlined here.

REFERENCES

[1] Doherty, L., Algorithms for Position and Data Recovery in Wireless Sensor Networks. 2000, UC Berkeley EECS Masters Report.

[2] N. Dey, A. S. Ashour, S. Fuqian, and S. Fong, “Developing Residential Wireless Sensor Networks for ECG Healthcare Monitoring,” no. November, 2017.

[3] Berkeley, U.o.C. 800 node self-organized wireless sensor network. 2001, Available: http://today.cs.berkeley.edu/800demo/].

[4] P. Ferrari, D. Marioli, and E. Sisinni, “Wired and wireless sensor networks for industrial applications,” no. October 2017, 2009.

[5] J. Jones and M. Atiquzzaman, “Transport Protocols for Wireless Sensor Networks : State-of-the-Art and Future Directions,” pp. 119–133, 2007.

[6] U. On and F. For, “A S URVEY ON E NERGY E FFICIENCY FOR W IRELESS.”

[7] C. Sinoquet, N. L. Zhang, and P. Leray, “A Survey on Latent Tree Models and Applications,” vol. 47, pp. 157–203, 2013.

[8] M. L. J. Vora, “EVOLUTION OF MOBILE GENERATION TECHNOLOGY : 1G TO 5G AND REVIEW OF UPCOMING WIRELESS TECHNOLOGY 5G,” pp. 281–291, 2015.

[9] I. Monitoring, H. Distributed, and G. Penetration, “Development of a Transmission and Distribution High Distributed Generation Penetration,” 2017.

[10] ((Acceso a red UMTS)). Available: http://isa.uniovi.es/domotica/Temas/T3/T3-UMTS.htm

[11] W. Paper, “Long Term Evolution (LTE): an introduction,” no. October, 2007.

[12] ((LTE: Long Term Evolution)). Available: https://en.wikipedia.org/wiki/LTE_(telecommunication)

[13] ((Difference of ZigBee vs WiFi)) [En línea]. Available: https://www.link-labs.com/blog/zigbee-vs-wifi-802-11ah

[14] A. Tomar, G. Technology, and C. Volume, “Introduction to Zibgbee Technology,” vol. 1, no. July, pp. 1–24, 2011.

[15] Bluegiga Technologies. (2013, Mayo) WT12 Datasheet. Documento PDF.

[16] Bluetooth SIG. (2013) Bluetooth. Available: http://www.bluetooth.com/Pages/Basics.aspx

[17] Wikimedia Fundation. (2013, Junio) Wikipedia. Available: http://en.wikipedia.org/wiki/Bluetooth

[18] Bluetooth SIG. (2010, Junio) Specification of the Bluetooth System. Documento PDF.

[19] Ed Grabianowski. (2006, Diciembre) How Stuff Works. Available: http://www.howstuffworks.com/wibree.htm

[20] Bluegiga Technologies. (2013, Mayo) BLE112 Datasheet. Documento PDF.

[21] Dynastream Innovations Inc. (2013, Noviembre) This is ANT. Available: http://www.thisisant.com/company

[22] Dynastream Innovations Inc. (2012) AP281MxIB Datasheet. Documento PDF.

[23] ZigBee Alliance. (2013) Zigbee. Available: www.zigbee.org/About/AboutAlliance

[24] HC-Bluetooth. Bluetooth Module—User Instructional Manual; HC Ser. Bluetooth Prod.: Guangzhou, China, 2011; pp. 1–16

[25] Available online : https://store.arduino.cc/arduino-nano.

[26] Available online : https://www.arduino.cc/en/Main/Software.

[27] P. M. Utc, “PIR Motion Sensor,” 2018.

[28] Available online : https://www.labcenter.com/whatsnew/

APPENDIX A

FRONT CIRCUIT PROGRAM CODES

```
///////////////////////Start program 1 ////////////////////////

void setup() {

  pinMode(2, OUTPUT);

  pinMode(3, OUTPUT);

  pinMode(4, OUTPUT);

  pinMode(5, OUTPUT);

  pinMode(10, INPUT);

  pinMode(11, INPUT);

  pinMode(12, INPUT);

}

void loop() {

  if (digitalRead(10)==LOW  && digitalRead(11)==LOW && digitalRead(12)==LOW )

{

  digitalWrite(4,LOW);
```

```
  digitalWrite(5,LOW);
  digitalWrite(2,LOW);
  digitalWrite(3,LOW);
    }
else if (digitalRead(10)==LOW  && digitalRead(11)==HIGH && digitalRead(12)==LOW)
{
  digitalWrite(4,HIGH);
  digitalWrite(5,HIGH);
  digitalWrite(2,LOW);
  digitalWrite(3,LOW);
  }
else if (digitalRead(10)==HIGH  && digitalRead(11)==HIGH && digitalRead(12)==LOW )
{
  digitalWrite(4,LOW);
  digitalWrite(5,HIGH);
  digitalWrite(2,LOW);
  digitalWrite(3,LOW);
```

```
  }

else if (digitalRead(10)==LOW && digitalRead(11)==HIGH && digitalRead(12)==HIGH )
{
 digitalWrite(4,HIGH);
 digitalWrite(5,LOW);
 digitalWrite(2,LOW);
 digitalWrite(3,LOW);

 }
else if (digitalRead(10)==LOW && digitalRead(11)==LOW && digitalRead(12)==HIGH )

{
 digitalWrite(4,HIGH);
 digitalWrite(5,LOW);
 digitalWrite(2,HIGH);
 digitalWrite(3,LOW);
```

```
  }
  else if (digitalRead(10)==HIGH  && digitalRead(11)==LOW && digitalRead(12)==LOW )
{
  digitalWrite(4,LOW);
  digitalWrite(5,HIGH);
  digitalWrite(2,LOW);
  digitalWrite(3,HIGH);
    }
else if (digitalRead(10)==HIGH  && digitalRead(11)==HIGH && digitalRead(12)==LOW )
{
  digitalWrite(4,LOW);
  digitalWrite(5,HIGH);
  digitalWrite(2,LOW);
  digitalWrite(3,LOW);
    }
}
```

////////////////////////////////**End Program 1** //

APPENDIX B

RIGHT CIRCUIT PROGRAM CODES

```
////////////////////////////Start Program  //////////////////////

int Camera = 0;

void setup() {

  pinMode(2,INPUT);

  pinMode(3,OUTPUT);

  pinMode(4, OUTPUT);

   pinMode(5, OUTPUT);

  pinMode(6, OUTPUT);

  pinMode(7, OUTPUT);

  pinMode(11, INPUT);

  pinMode(12, INPUT);

  pinMode(13, OUTPUT);

}

void loop() {

  if (digitalRead(2)==HIGH  && digitalRead(11)==LOW && digitalRead(12)==LOW )
```

```
{
 digitalWrite(13,HIGH);
 if (Camera== 0)
  {
   digitalWrite(5,HIGH);
 digitalWrite(6,HIGH);
 digitalWrite(7,LOW);
delay(1000);
 digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
   Camera= 1;
      }

 // RuN Motor


  }
```

```
else if (digitalRead(2)==LOW  && digitalRead(11)==LOW && digitalRead(12)==LOW)
{
  digitalWrite(13,LOW);
  digitalWrite(3,LOW);
   if (Camera== 1)
  {
    digitalWrite(5,HIGH);
 digitalWrite(6,LOW);
 digitalWrite(7,HIGH);
delay(1000);
  digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
    Camera= 0;
        }
```

```
      }
    else if (digitalRead(2)==LOW  && digitalRead(11)==HIGH && digitalRead(12)==HIGH)
{
  digitalWrite(13,HIGH);
  digitalWrite(3,LOW);
     if (Camera== 1)
  {
    digitalWrite(5,HIGH);
 digitalWrite(6,LOW);
 digitalWrite(7,HIGH);
delay(1000);
  digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
    Camera= 0;
        }
  }
```

```
else if (digitalRead(2)==LOW  && digitalRead(11)==HIGH && digitalRead(12)==LOW)
{
  digitalWrite(13,HIGH);
  digitalWrite(3,HIGH);
   if (Camera== 1)
  {
    digitalWrite(5,HIGH);
 digitalWrite(6,LOW);
 digitalWrite(7,HIGH);
delay(1000);
  digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
    Camera= 0;
        }       }
  else if (digitalRead(2)==LOW  && digitalRead(11)==LOW && digitalRead(12)==HIGH)
```

```
{
  digitalWrite(13,HIGH);
  digitalWrite(3,LOW);
     if (Camera== 1)
  {
    digitalWrite(5,HIGH);
 digitalWrite(6,LOW);
 digitalWrite(7,HIGH);
delay(1000);
  digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
    Camera= 0;
        }    }   }
```

//////////////////////////////////**End Program 2**//////////////////////////

APPENDIX C

LEFT CIRCUIT PROGRAM CODES

```
////////////////////////////////////////////Start program 3 ////////////////////////////////////////////////////
int Camera = 0;
void setup() {
  pinMode(2,OUTPUT);
  pinMode(3,INPUT);
  pinMode(5, OUTPUT);
  pinMode(6, OUTPUT);
  pinMode(7, OUTPUT);
   pinMode(11, INPUT);
  pinMode(12, INPUT);
  pinMode(13, OUTPUT);
}
void loop() {
  if (digitalRead(3)==HIGH  && digitalRead(11)==LOW && digitalRead(12)==LOW )
{
  digitalWrite(13,HIGH);
 if (Camera== 0)
  {
    digitalWrite(5,HIGH);
 digitalWrite(6,HIGH);
 digitalWrite(7,LOW);
delay(1000);
  digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
```

```
   Camera= 1;
       }
  }
else if (digitalRead(3)==LOW  && digitalRead(11)==LOW && digitalRead(12)==LOW)
{
  digitalWrite(13,LOW);
  digitalWrite(2,LOW);
   if (Camera== 1)
  {
    digitalWrite(5,HIGH);
 digitalWrite(6,LOW);
 digitalWrite(7,HIGH);
delay(1000);
  digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
    Camera=0;
       }
      }
    else if (digitalRead(2)==LOW  && digitalRead(11)==HIGH && digitalRead(12)==HIGH)
{
  digitalWrite(13,HIGH);
  digitalWrite(2,LOW);
     if (Camera== 1)
  {
    digitalWrite(5,HIGH);
 digitalWrite(6,HIGH);
```

```
 digitalWrite(7,LOW);
delay(1000);
  digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
    Camera=1;
        }
  }
else if (digitalRead(3)==LOW  && digitalRead(11)==HIGH && digitalRead(12)==LOW)
{
  digitalWrite(13,HIGH);
  digitalWrite(2,HIGH);
    if (Camera== 1)
  {
    digitalWrite(5,HIGH);
 digitalWrite(6,HIGH);
 digitalWrite(7,LOW);
delay(1000);
  digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
    Camera=0;
        }
  }
  else if (digitalRead(3)==LOW  && digitalRead(11)==LOW && digitalRead(12)==HIGH)
{
  digitalWrite(13,HIGH);
```

```
 digitalWrite(2,LOW);
   if (Camera== 1)
 {
   digitalWrite(5,HIGH);
 digitalWrite(6,HIGH);
 digitalWrite(7,LOW);
delay(1000);
 digitalWrite(5,LOW);
 digitalWrite(6,LOW);
 digitalWrite(7,LOW);
   Camera=0;
       }
 }
}
```

//**End Program 3** //

APPENDIX D

MASTER CIRCUIT PROGRAM CODES

///////////////////////////////Start program 4 ////////////////////////

```
void setup() {
  pinMode(0, OUTPUT);
  pinMode(1, OUTPUT);
  pinMode(2, INPUT);
  pinMode(3, INPUT);
  pinMode(7, INPUT);
  pinMode(8, INPUT);
  pinMode(4, OUTPUT);
  pinMode(5, OUTPUT);
  pinMode(9, OUTPUT);
  pinMode(10, OUTPUT);
  pinMode(11, OUTPUT);
  pinMode(12, OUTPUT);
}
void loop() {
if (digitalRead(2)==HIGH)
{
  digitalWrite(10,HIGH);
  }
    else if (digitalRead(2)==LOW )
{
  digitalWrite(10,LOW);
  }
```

```
if (digitalRead(3)==HIGH)
{
  digitalWrite(11,HIGH);
  }
    else if (digitalRead(3)==LOW )
{
  digitalWrite(11,LOW);


  }
if (digitalRead(7)==HIGH)
{
  digitalWrite(9,HIGH);
 digitalWrite(4,HIGH);
digitalWrite(0,HIGH);
delay(500);
digitalWrite(0,LOW);
delay(10);
digitalWrite(0,HIGH);
delay(200);
digitalWrite(0,LOW);
delay(20);
digitalWrite(0,HIGH);
delay(100);
digitalWrite(0,LOW);
delay(10);
digitalWrite(0,HIGH);
delay(300);
```

```
digitalWrite(0,LOW);


  }
    else if (digitalRead(7)==LOW )
{
  digitalWrite(9,LOW);
  digitalWrite(4,LOW);
 }
  if (digitalRead(8)==HIGH)
{
  digitalWrite(12,HIGH);
  digitalWrite(5,HIGH);
digitalWrite(0,HIGH);
delay(5);
digitalWrite(0,LOW);
delay(1);
digitalWrite(0,HIGH);
delay(2);
digitalWrite(0,LOW);
delay(2);
digitalWrite(0,HIGH);
delay(1);
digitalWrite(0,LOW);
delay(1);
digitalWrite(0,HIGH);
delay(3);
digitalWrite(0,LOW);
```

```
delay(50);
  }
    else if (digitalRead(8)==LOW )
{
  digitalWrite(12,LOW);
  digitalWrite(5,LOW);
      }
}
```

////////////////////////////////End Program 4 //////////////////////////////////