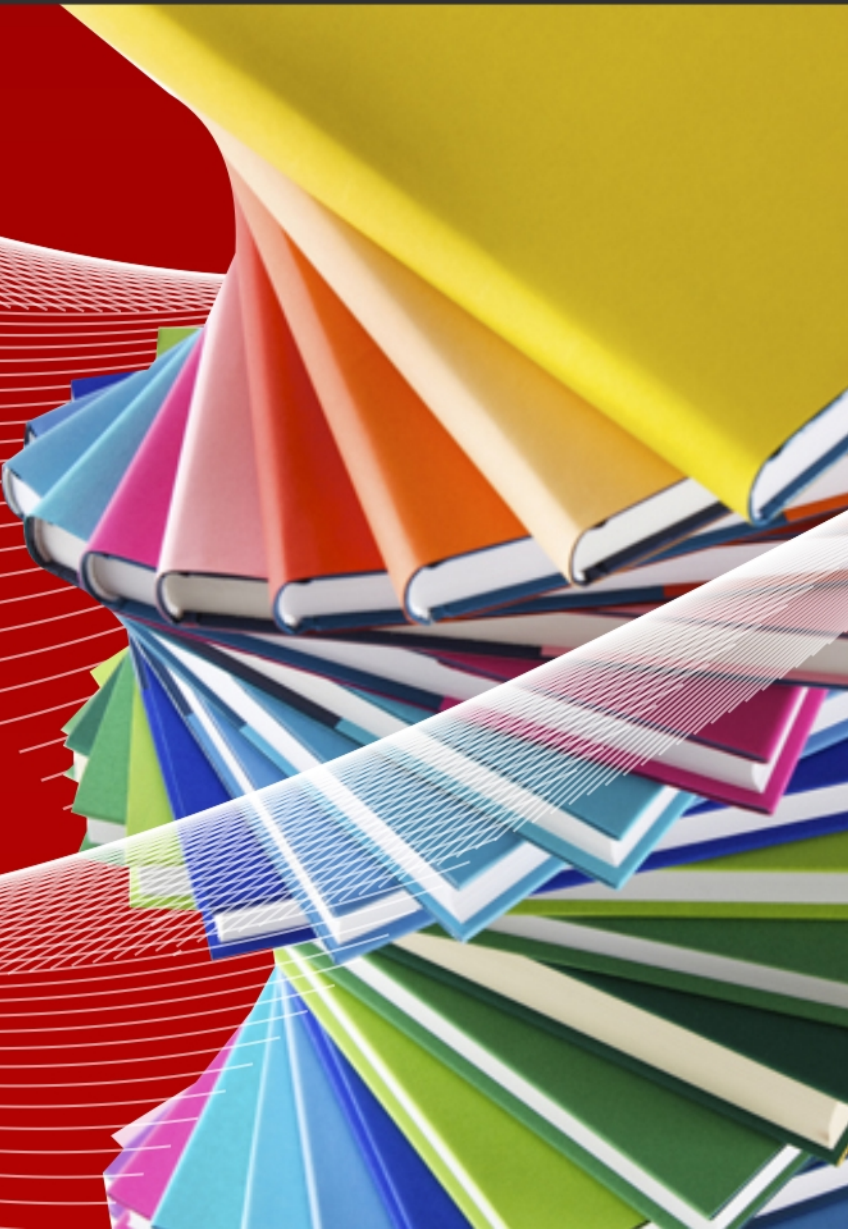
澳 門 大 學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

Outstanding Academic Papers by Students
學 生 優 秀 作 品



UHF RFID FOR INTELLIGENT ACCESS CONTROL SYSTEM AND INDOOR TRACKING

by

Loi Kin Chong (DB325147) Pun Chi Hin (DB325907)

Final Year Project Report submitted in partial fulfillment of the requirements for the Degree of

Bachelor of Science in Electrical and Computer Engineering

2017

Faculty of Science and Technology
University of Macau

********* Bachelor's Thesis Quote (OPTIONAL) **********

Bachelor's Thesis (or Final Report of ECEB420 Design Project II)

In presenting this Final Report of Design Project II (ECEB420) in partial fulfillment of the requirements for a Bachelor's Degree at the University of Macau, I agree that the **UM Library** and **Faculty of Science and Technology (FST)** shall make its copies available strictly for internal circulation or inspection. No part of this thesis can be reproduced by any means (electronic, mechanical, visual, and etc.) before the valid date (usually less than 3 years) limit listed below. Copying of this thesis before the valid date from other parties is allowable **only** under the prior written permission of the author(s).

Printed name: _________________

Signature:_____________________

Student number: _______________

Date: ________________________

Reliable Contact information (address, tel. no., email, etc.) of author:

____

____

____

____

Valid date until ________________

********* End of Bachelor's Thesis Quote **********

DECLARATION

I declare that the project report here submitted is original except for the source materials explicitly acknowledged and that this report as a whole, or any part of this report has not been previously and concurrently submitted for any other degree or award at the University of Macau or other institutions.

I also acknowledge that I am aware of the Rules on Handling Student Academic Dishonesty and the Regulations of the Student Discipline of the University of Macau.

Signature : ________________ __________________(e-signature OK)

Name : __Loi Kin Chong_ & __Pun Chi Hin___

Student ID :____DB325147___ & ___DB325907____

Date : _________12 May, 2017___________

APPROVAL FOR SUBMISSION

This project report entitled "**UHF RFID FOR INTELLIGENT ACCESS CONTROL SYSTEM AND INDOOR TRACKING**" was prepared by Loi Kin Chong (DB325147) and Pun Chi Hin (DB325907) in partial fulfillment of the requirements for the degree of Bachelor of Science in Electrical and Computer Engineering at the University of Macau.

Endorsed by,

Signature : ______________________________

Supervisor : Prof. Wai Wa CHOI

ACKNOWLEDGEMENTS

The authors would like to express their sincere thanks to those professionals below, first is our project instructor Prof. Wai Wa Choi, he gave us many of comments and ideas to improve the qualities for this project. Second is the lab technicians Huizheng Bu, Pedro and Tim, they gave us fully technical support for the instruments operating and measuring. Lastly, we would like to special thanks the Adjunct Associate Professor Dr. Sio Weng Ting of his suggestion for our project idea.

ABSTRACT

Radio Frequency Identification (RFID) is identification of objects or people by incorporating the use of radio frequency waves to transmit data, without any line-of-sight alignment or physical contact between the tag and the reader.

In this project, a UHF RFID-based intelligent access control system at a frequency range of 902MHz to 928MHz is developed by integrating the UHF RFID reader, Arduino, electromagnetic lock and PIR sensor. To trigger the electromagnetic lock, the PIR sensor monitors the immediate environs of the door solidly. It also has a contribution to energy conservation since the electromagnetic lock does not need to be energized the whole time if there is nobody walking by. Only people with authenticated tag can access. Our proposed system can converse up to 50% of the energy in contrast to the traditional access control system. Also, the recovery time of the PIR sensor is greatly decreased from 5.5s to 0.2s after the hacking, which means the door can be locked promptly whenever a visitor comes up. This ensures the security of the system.

Another feature of the system is contactless communication between the reader and the tag that is realized by backscatter coupling mechanism. It facilitates the process of entering a locked room without even taking out the tag and placing it on the reader. Although the read range of the system is 1m, it can be expanded with a higher power antenna rather than the one used in our prototype.

Apart from the access control system, the characteristic of RFID is called into play to implement testing of indoor tracking. RSSI is the core of the indoor tracking. After the comparison with the most popular formula, a model describing the relationship between the RSSI and the distance is constructed. Results show an average error of 0.20%.

TABLE OF CONTENTS

LIST OF TABLES/FIGURES

CHAPTER 1

INTRODUCTION

1.1 Motivation

Nowadays, Radio Frequency Identification (RFID) technology is extensively used in daily life. Enormous number of RFID application can be found in various fields such as Cargo Management, Medical Applications, Anti-theft Applications, Highway Toll System and Access Control System. For the Access Control System, we found out two general issues could be improved. First is the energy used of access lock. We found that most of the Access Control System are using electromagnetic lock as the access lock. But in reality, they consume a part of energy in every day, to greater or lesser degree, we think it is possible to be reduced by using some simple but smart method to implement. Second, a part of users have ever felt that, more or less, the security system is a hindrance to their daily work. Because in every time when user want to be verified by access control system, it is necessary to type the password or use access card. Surely, access card is more convenient than typing password for access and itself has a robust security mechanisms, so that access card is the most commonly tools for access system in near decade. Now a day’s access card also is one of the RFID technology of HF (High Frequency). But the disadvantage of HF card is that, the card is required to put very close to the reader for scanning. It is a hindrance for user, especially you must take out the access card when one’s hands are full or for some action invariable person such as disabled people or wheelchair. According to an article said: “The next step is for us to realize that access control is not just about security but also about convenience and ease of use.” [7] After soon we found another

RFID technology may have great potential to improve the access control system, it is UHF.

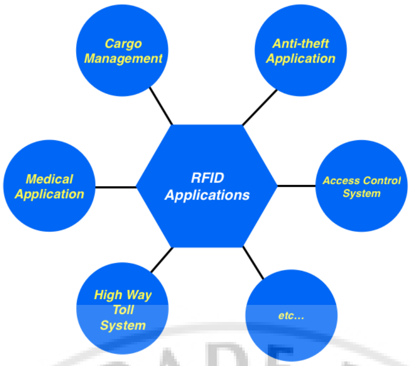


Fig 1. 1The Different Area Application of RFID

UHF stand for Ultra High Frequency, the main difference between HF is it can provide higher operating range, which mean it can achieve assess verify in certain range without put the access card close to reader. Moreover, if UHF applied in access control system, it can provide multiple function not just only for security access. For example, indoor tracking or say indoor positioning, it is a very popular topic in the world who want to achieve. Due to GPS signal obstructed by the wall, it cannot offer the signal into buildings, so that's why GPS positioning only available for outdoor application.

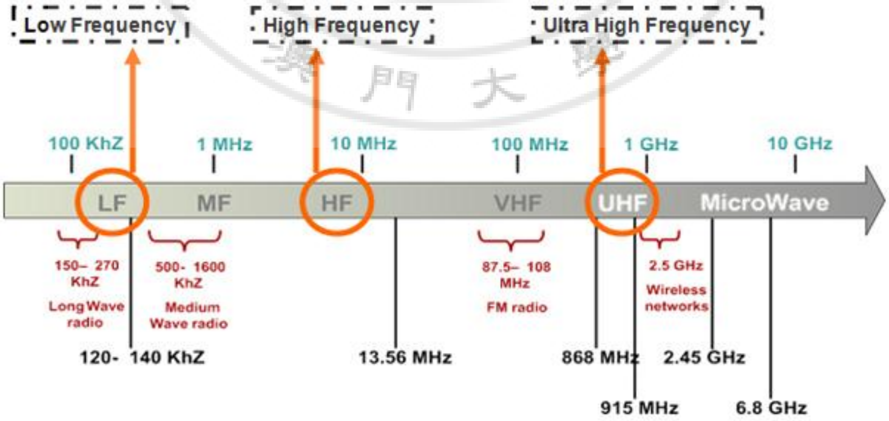


Fig 1. 2The Different Area Application of RFID [1]

UHF could be one of the method to achieve for indoor positioning, refer to the long-range communication properties, reading the RSSI from the tag to analysis data and infer the position, then display the position on the user personal device that to achieve. So the function of the access control system it apart from security access, it integrates smart energy saving and indoor positioning. We called it Intelligent Access Control System.

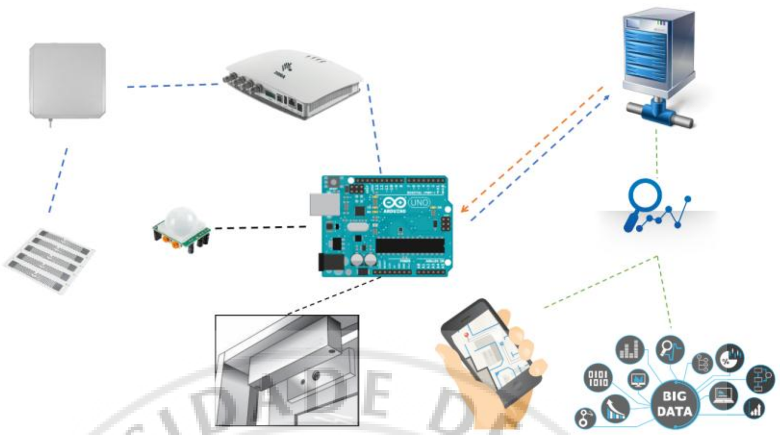


Fig 1. 3 The Intelligent Access Control System want to design in this project

1.2 Organization

This project proceeds as follow. Chapter 2 contains four sessions contributed by Chong, it gives the background of RFID, describes the component of RFID system. Chapter 3 contains 3 sessions done by Hin which presents the working principle and performance of various sensors such as Doppler Radar and PIR Sensor, it has written the work to do the noise reduction for Doppler Radar and the blocked time limitation solution scheme for the PIR sensor. Chapter 4 contains five sessions, gives the design and architecture of the system, more details about the system components by Chong and discuss the energy used by Hin. Chapter 5 explore the RFID indoor positioning, to investigate its reliability and feasibility, Chong and Hin did the experiment and measurement together, and Hin mainly focus on the experiment set up and data arrangement, Chong focus on the analysis from the result and conclude the reliability and feasibility of using UHF RFID indoor positioning. Last Chapter 6 concludes the thesis and states the future research directions.

CHAPTER 2

INTRODUCTION TO RFID

Chapter 2 will provide a comprehensive overview and introduction to RFID technology which is necessary for better understanding of the following chapters.

2.1 RFID

RFID stands for Radio Frequency Identification. It is one of several technologies known as auto-identification (Auto-ID) technology which uses radio frequency signal to identify the tagged objects and collect the relevant data in a non-contact manner. A complete RFID system generally consists of a reader, RFID tag which is also known as transponder and data processing subsystem. Similar to other identification systems such as barcodes, the reader reads from some source of identification data. Then, the identification data is normally processed by a data processing subsystem or server.

Compared to the traditional barcode technology, RFID has brought many advantages. The notable difference in relation to barcode is that RFID does not require mechanical or optical contact between the identification system and a particular target since RFID is able to read the data through external materials. One of the advantages of RFID is that it can read the data automatically at a rate of hundreds of times per second from some distance away. In addition, barcode can only recognize a single item at a time whereas RFID can simultaneously read data from multiple tags and work under harsh environment. Furthermore, RFID can hold additional functionality which means more bits of information than barcode.

With significant advantages mentioned previously, RFID is used extensively in various fields and become the main building blocks of the Internet of Things (IoT) paradigm. Current RFID technology is manly focusing on the following aspects, ranging from supply chain (inventory management, asset tracking), manufacturing (automotive system) to pharmaceutical (product authentication), health care (patent and equipment tracking) and so on [14]. Thereby it enables manufacturers to know the location of each product during its operation life, and also help to control and manage all types of tangible assets.

2.2 Components and Function of RFID

2.2.1 Reader

The reader, also referred to as the interrogator, is mainly composed of a radio frequency module, a control unit, the central processing unit (single-chip microcontroller) and a coupling element. It can utilize the related search technology or protocol to have the capability of identifying hundreds of different RFID tags per second. The operating principle is described as the following. The reader broadcasts radio frequency electromagnetic wave through its antenna. If an RFID tag is present within the interrogation zone of the reader, it will transmit the internal data to the reader via its built-in radio frequency mechanism. After receiving the data of the RFID tag, the reader forwards the received data to the data processing subsystem by wired (interface such as RS232, RS485, RS422) or wireless (interface such as Bluetooth, GPS) means for object identification or other application processing.

In the case of passive and semi-active tags, the reader is in charge of providing tags enough energy to power up by emitting a predefined low-power radio wave field. The range of this field is usually determined by two factors: the size of the antenna on both sides and the power of the reader. Depending on the application, the size of the antenna has different requirements. However, the power of the reader, which defines the strength and extent of the generated electromagnetic field, is generally limited by regulations. Each country has its own set of standards and regulations on the amount of power generated at various frequencies.

2.2.2 Tag

In an RFID system, every object to be identified is physically labelled with a tag. Tag, also known as transponder, carries the data that is transmitted to the reader when being interrogated by the reader. Normally, it consists of an electronic microchip with some computation and storage capabilities, and a coupling element such as antenna coil for communication. The memory element serves as writable and non-writable data storage, which can range from few bytes up to several kilobytes. Tags can be programmed to read-only, write-once read-many or fully rewritable. Depending on the kind of tag, tag programming can occur at the manufacturing level or application level.

As long as the required power is obtained, the tag will return the Electronic Product Code (EPC) stored in its microchip with built-in radio frequency radio waves, such as product number, code number, expiry date etc. The transmitted digital signal must use different frequencies in order to prevent interfering with other weak signals.

A tag can obtain power from the reader, or it can have its own internal source of power. Therefore, the source of power becomes a key classification of tags. They may be one of the three types – passive, active and semi-passive as shown in Figure 2.1. The most popular tags today are passive tags.

- **Passive tags**: Passive tags do not contain any sort of on-board power source. They rely on external electrical power to drive the circuit. In the absence of a reader, they do not have the ability to communicate or compute without drawing the power by harnessing the electromagnetic energy emitted from the reader. The internal antenna module induces the coupled current and charges the capacitor, in order to answer with its own information stored in the memory of the microchip. Because of the lack of an on-board power supply, they are small sized and can be produced at very low cost. Moreover, they could reach a nearly unlimited operational lifetime as long as the circuit is intact. However, the range of a passive tag is very limited that it can be read only at very short distances.
- **Active tags**: Active tags contain an on-board power source, such as a battery, which is used to run the circuitry on microchip and power the outgoing signal. They do not require energy provided by reader to energize them. Thus, active tags can automatically initiate their own communications with the reader. Compared with passive tags, active tags have a far longer working distance and larger memory capacity available for reading and writing data. Unfortunately, the main disadvantages of these tags may be relatively big size and high production price. Also, the operational life might be limited to a maximum of 10 years depending on operating temperatures and the battery type.

- **Semi-passive tags**: Semi-passive tags are a combination of active tags and passive tags. They contain an on-board battery which is exclusively designed to help them run the circuitry on the microchip and support the data storage. They are not the initiator of the communication between readers and them either. They still harvest the power for preparation of response from electromagnetic field generated by reader. Therefore, semi-passive tags do not require the presence of a reader to wake them up until they have to transmit or receive data. One of the advantages of these tags is all received power can be used for transmitting back a signal, which allows increasing communication distance with a quite cheap solution.

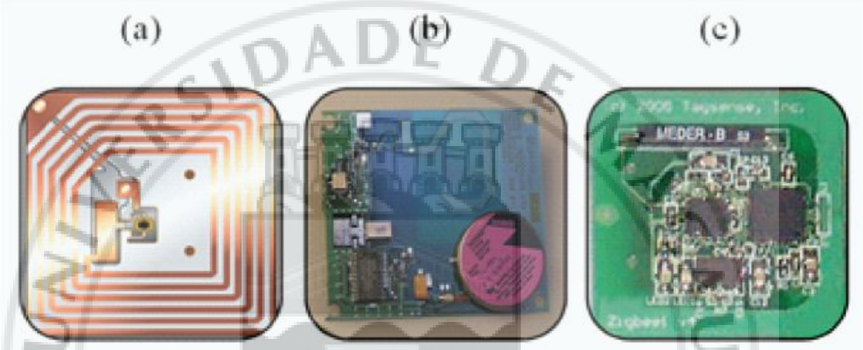


Fig 2.1 Passive, semi-passive and active tags respectively [2]

2.2.3 Antenna

Antennas are the key device that enable data communication between the tag and the reader as they receive and transmit the electromagnetic waves effectively. They convert electrical signal into a radiating field and vice versa. Therefore, the design and placement of the antenna plays a significant role in determining the interrogation zone, range and accuracy of communication. [5][8]

In an RFID system, antennas are mainly divided into two different types which is reader antenna and tag antenna. The former is integrated with the reader or physically attached at its port by the means of a cable while the latter is usually manufactured with the tag chip and packaged as a whole. Figure 2.2 shows several typical passive tags and antenna designs. Since the size of a tag chip can be very tiny that less than a unit square millimeter, the dimension of the entire tag package generally depends on the size and shape of the antenna.

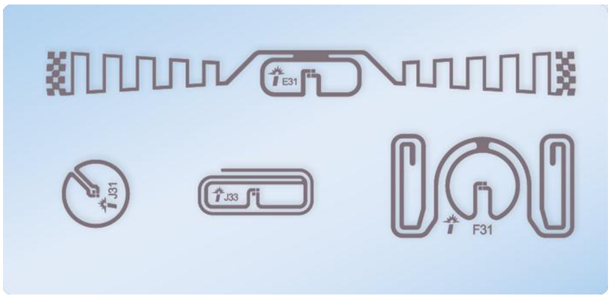


Fig 2.2 Typical passive RFID tags with antenna [3]

With UHF and microwave, reader antenna polarization is a factor in the circumstances of use. It refers to the orientation of the propagating electric field. Figure 2.3 shows two common polarizations, linear and circular. When the tag and reader antenna is aligned in the same direction, maximum power transfer is achieved.

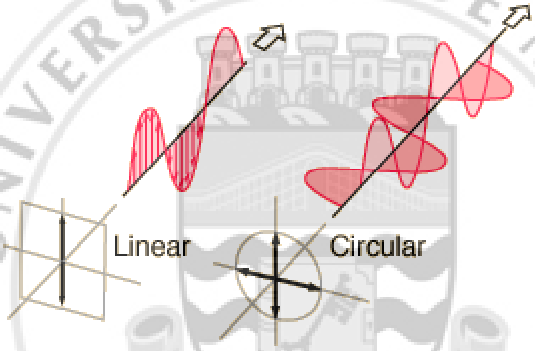


Fig 2.3 Linear polarization and circular polarization [4]

- **Linearly polarized antenna**: Linear polarization takes the surface of the earth as a reference where horizontally polarized waves travel parallel to the ground and vertically polarized waves travel perpendicular to the ground[10]. A linearly polarized antenna emits a narrower radiation beam which helps it to read tags within a longer as well as well-defined region, rather than randomly from its surroundings. As a result, a linearly polarized antenna is sensitive to tag orientation compared to a circularly polarized antenna. These types of antenna are therefore best for applications where the tag orientation is known and fixed.
- **Circularly polarized antenna**: A circularly polarized wave basically rotates in a circular manner as it travels. It is composed of horizontal and vertical components so that a circularly polarized antenna is largely unaffected by the tag orientation. A circularly polarized antenna reads tag in a wider area by

emitting a wider radiation beam. Due to its insensitivity to tag orientation, it is an excellent detector for tags in a mixed environment where orientation is unknown and unpredictable. This antenna is preferred for an UHF or microwave frequencies RFID system considering there is a high degree of radio frequency reflectance which is caused by the presence of metals or waters.[10]

Selection of an appropriate antenna is based on the application of the RFID system. A circularly polarized antenna would be a suitable candidate for doorway or portal tracking in the light of limited or no control at all on the tag orientation, while the reader is generally stationary. In terms of the antenna polarization, circularly polarized reader antenna is extensively adopted in RFID system as the reader antenna. The purpose of circular polarization is to ensure the reliability of communications between readers and tags and provide better detecting range. For tag antenna, single dipole of which the polarization is linear is mainly used in backscattering tags to increase the reflection directivity, as opposed to circular is typically employed on inductive coupling to maximize the magnetic field.

2.2.4 Data processing subsystem

The data processing subsystem or server is used to overcome the computational limitations of tags and readers. It retrieves the internal information of the tag via the reader by wired or wireless way, then uses this information to meet the requirements of different application for further processing. It can also be applied in the production, logistics, warehousing and preservation etc. combined with network functions. In order to reduce the cost of RFID readers, cryptographic functions or data processing algorithm should be left to a data processing subsystem or server. In this project, we use Arduino as the data processing subsystem of RFID.

2.2.5 Operating Frequency for RFID

The operating frequency, which usually refers to the frequency of radio waves selected by the reader to transmit its predefined data, is a very important element in RFID system. In addition to determining the operating range that the reader can read the tag, this operating frequency is also a factor of data transfer rate. Namely, the higher the data transfer rate desired, the higher the operating frequency required. Hence, the characteristic of various operating frequencies needs careful consideration in designing an RFID solution.

To avoid the standards on radio frequency in different countries causing confusion, most of the international community comply with the International Telecommunications Union (ITU) radio regulations. Low frequency (LF) between 120 and 140 kHz is the most common RFID frequency. It is a near-field propagation which offers an operating range between 0 to 1 m. Increasing the system frequency to high frequency (HF) at 13.56 MHz, ultra-high frequency (UHF) at 860-960 MHz or microwave frequency at 2.45 GHz, a higher operating range can be achieved.

These 4 types of frequencies have their own advantages and disadvantages. In general, a lower frequency means a shorter operating range and slower data transfer rate. But it has a better reading performance in metal or liquid environment since metal or moisture will shorten the operating range by interfering with or absorbing radio waves. Therefore, environmental conditions should be also taken into account as well as the characteristic of various operating frequencies.

2.3 Passive Coupling Mechanisms

Active tag has its built-in power supply and can communicate by transmitting radio frequency signal on which data is carried. In contrast, passive tag does not come with its own power supply. It typically obtains sufficient power from the field generated by the reader. Therefore, energy transfer and data transfer comprises the communication between a passive tag and a reader. Coupling via electromagnetic fields is established to transfer the energy from one medium to another similar medium, such as metallic wire or optical fiber.[12] As the name implies, an electromagnetic field consists of electrical component and magnetic component. Passive tag utilizes either the either one of the field or both for energy.

There are various means of coupling and can be categorized into three areas where passive tags mainly rely on: backscattering, inductive coupling and capacitive coupling. Fundamentally, different coupling mechanisms are important when it comes to several operating characteristics of the RFID system including the read range along with frequencies.

2.3.1 Inductive coupling

Magnetic field is generated around the current-carrying conductor. Instead, when a conductor is placed in a magnetic field, the current flow in the conductor by the influence of the magnetic field. This phenomenon is known as inductive coupling shown in Figure 2.4.

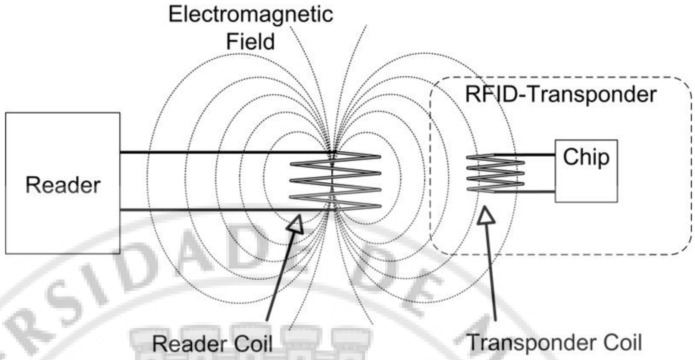


Fig 2.4 Inductive coupling [5]

Inductive coupling is the coupling of the tag and the reader through a shared magnetic field due to the mutual inductance. For this type of coupling, both the tag and the reader will have antenna coils which are referred to as a ‘transformer’[2]. All the energy obtained in the tag is drawn from the magnetic field generated by current in the reader coil. Once the tag is placed close enough to the reader, a part of the emitted magnetic field penetrates the antenna coil of the tag. Then a voltage will be induced in the tag that serves as the power supply for the microchip, which resembles the primary winding of the transformer generating a voltage in the secondary winding.

To pass the data from the tag to the reader, microchip on the tag modulates the magnetic field by switching the impedance load on its coil according to the data stream. As a result of the mutual coupling, the reader can detect the variations and demodulate the transmitted information. [15]

Inductive coupling is used by low-frequency (LF) or high-frequency (HF) communication as their wavelengths are much larger than the distance between the tags and the readers. The typical reading distance ranges from a few millimeters up to one meter, which is considered as a near field effect.

2.3.2 Capacitive coupling

Capacitive coupling transfer energy by means of mutual capacitance instead of mutual inductance. Basically, it uses capacitive effects that acted as dielectric material to provide the coupling between the tag and the reader. The efficiency is optimal when items like smart cards are inserted into a reader [15]. Then the capacitance created above and below the tag is measured by the electrical storage capacity and voltage across them. The electromagnetic wave generated by the reader is picked up within the tag and used to power up the tag in the same as inductive coupling. By modulating the load, the data is returned to the reader.

The conductive patches which must be held parallel in a very close proximity on the reader and the tag results in the formation of a capacitor. In order to provide the required coupling, capacitive coupling uses electrode plates of the capacitor rather than having coils or antennas. Different from inductive coupling whose read range can be extended by a larger antenna area, the antennas of capacitive coupling cannot as they are replaced by electrodes. Hence, the read range is generally less than 2 centimeters.

2.3.3 Backscatter coupling

Apart from inductive and capacitive coupling, there is another type of coupling which is known as backscatter coupling. The principle of backscatter coupling is quite similar to radars basing on the reflection of electromagnetic wave by most objects if the dimesons of them are larger than half the wavelength. The efficiency of this kind of reflection is called the reflection cross-section.

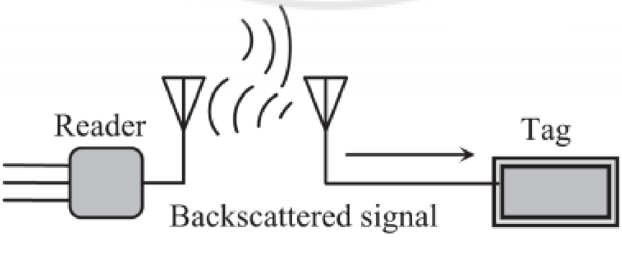


Fig 2.5 Backscatter coupling

As Figure 2.5 illustrated, a reader transmits a continuous electromagnetic wave in a radial manner at a specific frequency. When a tag appears in the area, it interacts with the incoming electromagnetic wave. Varying the load connected to the antenna can dampened the reflection cross-section. Therefore, data transmission from the tag to the reader is accomplished by switching on and off the load resistor connected in parallel with the antenna synchronously with the data stream from the microchip. The amplitude of the power can be modulated due to the switching of resistor and reflected towards the reader eventually[2]. Several factors such as tag cross sectional area, antenna properties would significantly affect how the incoming signal is reflected. With the help of directional coupler, the transmission and reception of a signal is allowed to occur at the same time.

Unlike inductive and capacitive coupling, backscatter coupling works beyond the near field. In other words, the read range is longer than those two coupling methods. Backscatter coupling is commonly used by ultra-high-frequency (UHF) or microwave frequency communication.

2.4 The Security of UHF

Compare with MIFARE, UHF somewhat cannot offer the same level of security as MIFARE, since the characteristic of UHF can make long distance transfer, during the traveling may let hackers that are tapping data with an unauthorized reader. MIFARE can offer the robust security mechanisms but UHF cannot yet. However, in recent year, UHF systems are able to provide almost same level of security for sensitive data as an MIFARE system. Such as EPC Gen 2 provides built in security measures, including 32-bit access and cover-coding of transmitted, kill password etc.

People usually focus on the encryption for communication between the access card can card reader, but we often forget two important aspects, through multiple authentication methods can also achieved a higher security level, and the technical side of achieving a higher security level somewhat depends on a complete chain of measures. If some zones are really confidential must ensure on body can access without authorized, it is suitable for use combi card (See Fig 2.1) which combines UHF with a second technology such as MIFARE. This allows user just use one card for both convenient access and for high security access. We can partition the building, decide for each zone entrance whether convenience or security is more importance. [17]

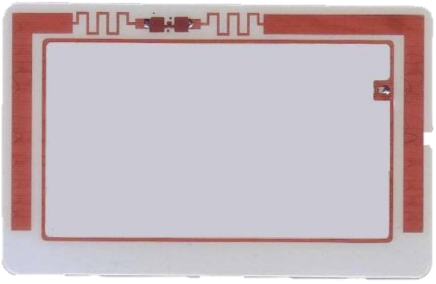


Fig 2. 6The Combi Card which combines UHF and MIFARE [6]

CHAPTER 3

SENSOR AND TECHNOLOGY FOT MOTION SENSING

3.1 Motion Sensor

Motion sensor is an important part in this project, previously we have mentioned that energy saving especially the electromagnetic door lock power consumption is one of the goal want to achieve in this project, to give or not to give power to the electromagnetic door lock is determined by the motional sensor. Hence motion sensor as a key role to make sure the whole systems are security and energy saving. In this project, Doppler radar and infrared sensor were considered be motion sensor.

3.2 Doppler Radar

Doppler radar is one of the motion sensor that can detect the motion, it can provide velocity and distance data according the Doppler Effect, the main function of it was done by reflecting the microwave signal at the desired target and analyzing how the motion of the object changes the frequency of the return signal. Nowadays, Doppler radar is very common use in police, use it to determine the speed of a moving vehicle.

3.2.1 Doppler Effect

Doppler Effect proposed by Christian Doppler who is the Austrian physicist in 1842. His theory can simply say, when a listener moves toward a stationary source or when a source of sound waves is approaching the listener, the frequency of the sound hear is higher than what you hear when stationary. On the other hand, when the listener moves away from the stationary sound source or a wave source that emits a sound wave is moving away from listener, the frequency of the sound of listener hear will be lower than what he hear when stationary. [1] One more example get easier to know, there have two people A and B, one as the pitcher (people A) another one as the catcher (people B). In the first situation, A and B stay in fix positions, the distance between each other is 10m, people A pitches the ball in every second (namely frequency f_p= 1Hz), the velocity of the ball is 10m/s. According the formula $t = \frac{d}{v}$ (do not concern with gravity), we got time t will equal to 1s, that mains people B catches the ball in every second (namely frequency f_c=1Hz). Second situation, people B is fix position, people A sill pitches the ball (velocity v is 10m/s) in every second (f_p= 1Hz) but for now will walk toward B. So the distance d between A and B will become shorter, in simple physic can show the ball will use less time through from A to B. It means people B can catch the ball in less than one second, therefore the frequency of people B to catch ball will become higher. In third situation, people B also in fix position, people A sill pitches the ball (velocity v is 10m/s) in every second (f_p= 1Hz) but for now will walk gradually away from B, the distance between A and B will become far. So the frequency of people B to catch ball will become lower. That is Doppler Effect. Doppler Radar is according to this principle to produce electromagnetic wave when it touches with a moving object and reflect back to origin, through the frequency different to calculate the object velocity respect to radar.

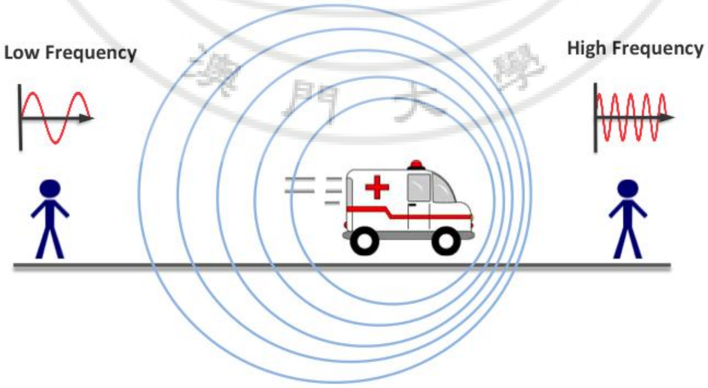


Fig 3. 1 Doppler Effect perform for sound wave [7]

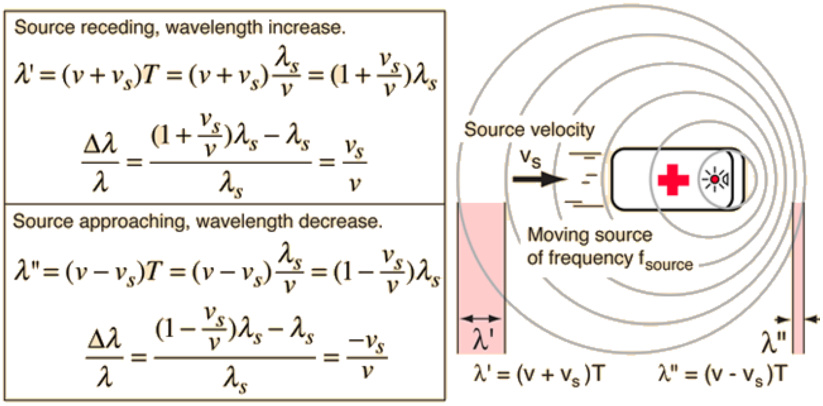

Source receding, wavelength increase.
$\lambda' = (v + v_s)T = (v + v_s)\frac{\lambda_s}{v} = (1 + \frac{v_s}{v})\lambda_s$
$\frac{\Delta\lambda}{\lambda} = \frac{(1 + \frac{v_s}{v})\lambda_s - \lambda_s}{\lambda_s} = \frac{v_s}{v}$
Source approaching, wavelength decrease.
$\lambda'' = (v - v_s)T = (v - v_s)\frac{\lambda_s}{v} = (1 - \frac{v_s}{v})\lambda_s$
$\frac{\Delta\lambda}{\lambda} = \frac{(1 - \frac{v_s}{v})\lambda_s - \lambda_s}{\lambda_s} = \frac{-v_s}{v}$
Source velocity
v_s
Moving source
of frequency f_{source}
λ'
λ''
$\lambda' = (v + v_s)T$
$\lambda'' = (v - v_s)T$

Fig 3. 2 Basic calculation to find the sound wavelength while source is receding or approaching [8]

3.2.2 HB100 Doppler Radar

In the project, HB100 Doppler Radar motion detector (Fig. 3.3) was chosen as one of the sensor, for the size, length 3.8cm, width 4.5cm. For the power, it need 5V DC voltage can be provided by Arduino, the HB100 have two pair of antennas for radiate or receive electromagnetic wave, in Fig. 3.5 shown, the pair of left antenna is Tx antenna to radiate an electromagnetic wave to certain area, pair of right is Rx antenna to receive the reflected signal. [4] The transmit frequency and power of the module is set by factory. User cannot take adjustment in this device. The radiation patterns of the antenna and their half power beam width (HPBW) are shown in Fig. 3.6.

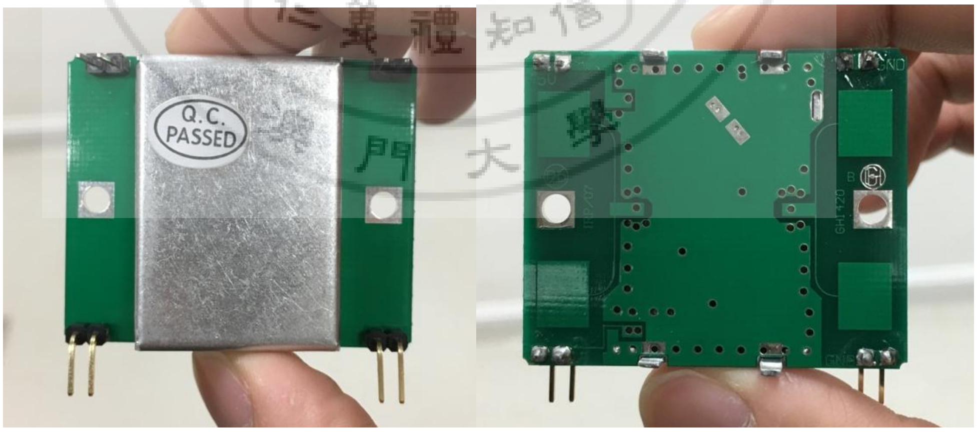


Fig 3. 3 HB100 Doppler Radar motion detector (Left is back, right is fount)

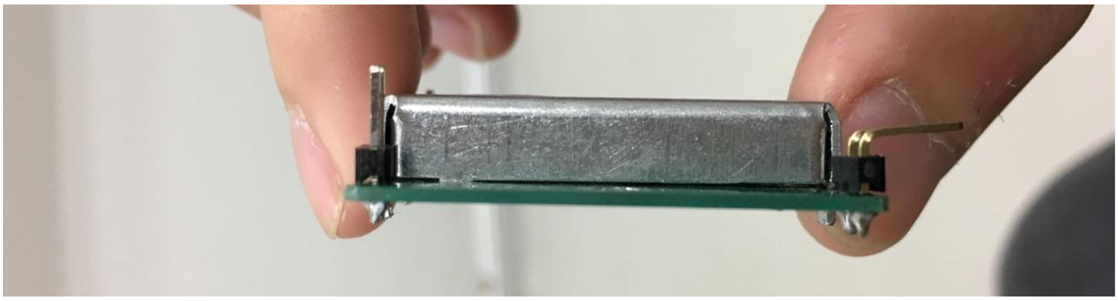


Fig 3. 4 The side face of HB100, we can see the back has a metal cover which can reduce external distortion.

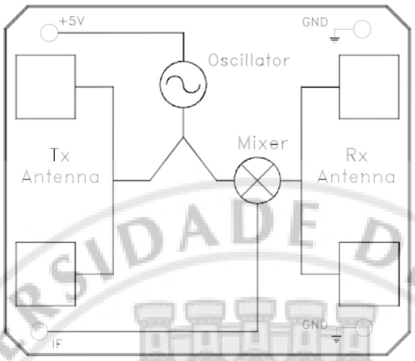


Fig 3. 5 The Block Diagram of HB100 [9]

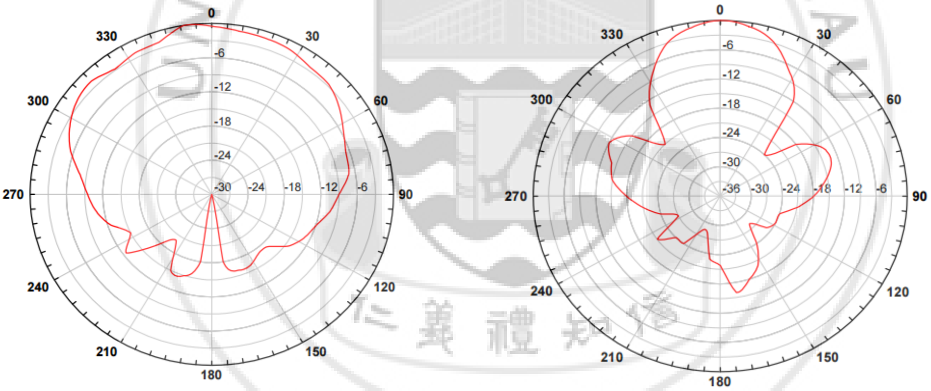


Fig 3. 6 The radiation patterns of HB100 [9]

3.2.3 Basic Performance of Doppler Radar

At the beginning, 5V DC voltage source was given to supply the HB100 Doppler Radar motion detector and connect the IF to oscilloscope (Fig. 3.7), after connected, we can use the hand for testing, when the hand moves closer to the detector, the oscilloscope will generate an oscillate waveform like Fig. 3.8, it is a dynamic waveform that depends on the object size, velocity and movement direction, different condition will show different level. For example, a high velocity object can generate high frequency wave; if the moving direction is perpendicular toward detector that the waveform would more distinctness, moreover, if the moving direction is across the detector, the waveform would not very conspicuous (Fig. 3.9).

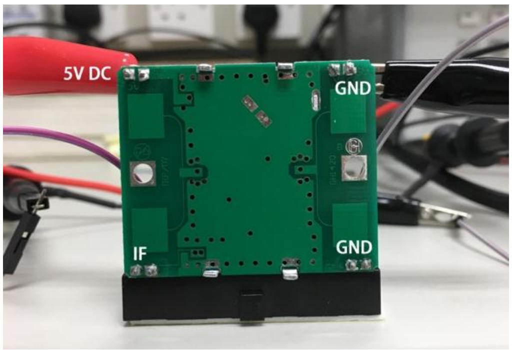


Fig 3. 7 Circuit connection for HB100

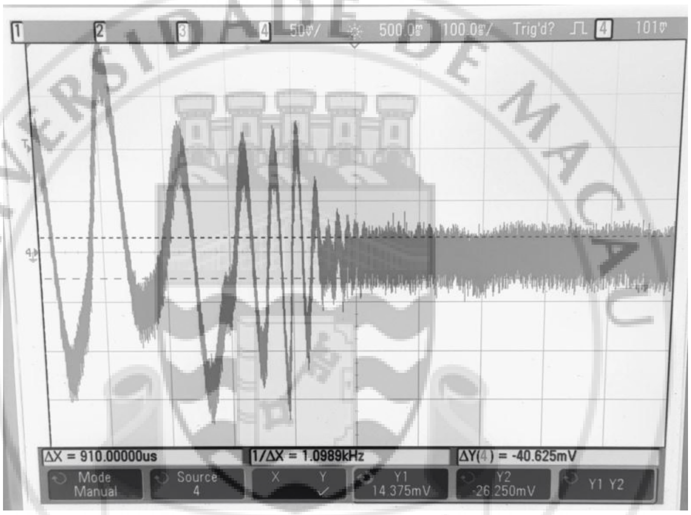


Fig 3. 8 The waveform generated by HB100 when an object approach.

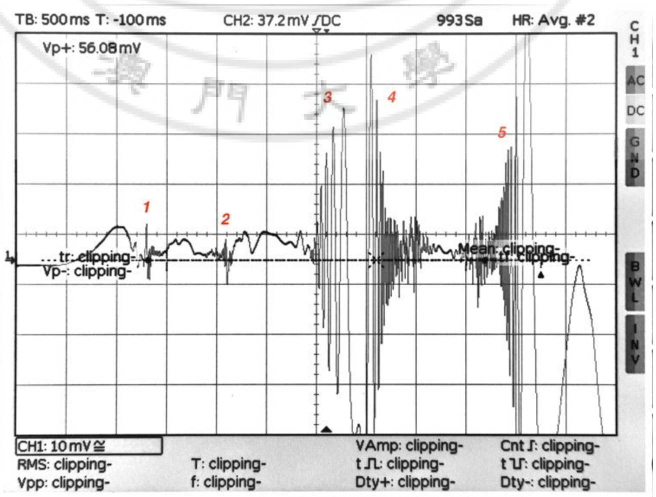


Fig 3. 9 The waveform performance in different movement,1&2: An object across the detector; 3&5: Object approach perpendicular toward detector; 4: Object keep away from detector.

3.2.4 Performance Improvement for Doppler Radar

However, as the result we found that there have two problems: the noise and weak signal intensity. We did Fast Fourier transform (FFT) can see as Fig. 3.10 have many high frequency noise in the result, therefore we design a passive 1st order low pass filter try to fill out the noise in high frequency by the formula:

$$f_c = \frac{1}{2\pi RC} \text{---------------------------------------} (3.1)$$

Set the cut off frequency f_c is around 106.103Hz, resistor R choose 150Ω, capacitor C should equal to 10μF. The circuit of the passive 1st order low pass filter like Fig 3.11 and filter performance was shown in Fig 3.12. As the compare result in Fig 3.13, there only have little improve for the signal result (see Fig 3.13), it is not satisfying. Thereafter we found the signal intensity is very weak, the scale has been zoomed in very small actually. The oscillate signal $V_{p\text{-}p}$ only between 2~300mV which in weak level, so here we have a hypothesis that when gain the output signal to get rid of the weak level same as the noise, the performance should be better. Therefore, the low pass amplifier was chosen to design. Logically in the project we need to process the Doppler radar detector signal from analogue to digital, which called digitalize, the Arduino can through the digitalized signal to analyze the motion situation, the basic logic, some moving objects was detected when digital signal higher than a critical point. To make the detector be more sensitive, it should set lower critical point, but for original case if set low critical point, that will easy be breached by noise. Hence low pass amplifier is necessary to build.

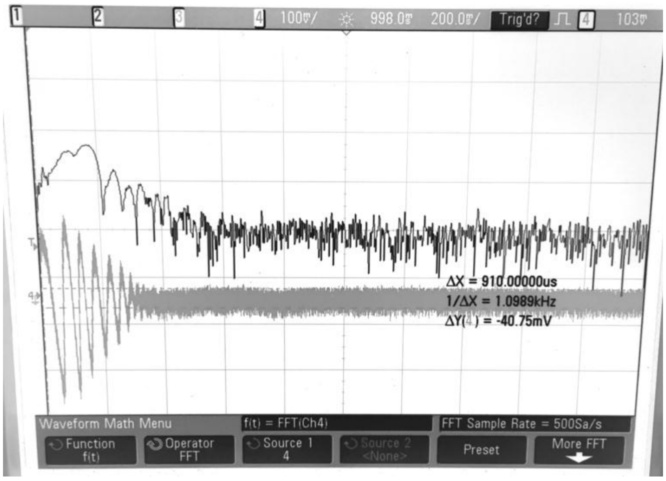


Fig 3. 10 In the FFT (purple path) can see many noise in high frequency domain

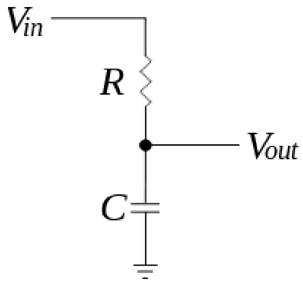


Fig 3. 11 Circuit for passive 1st order low pass filter

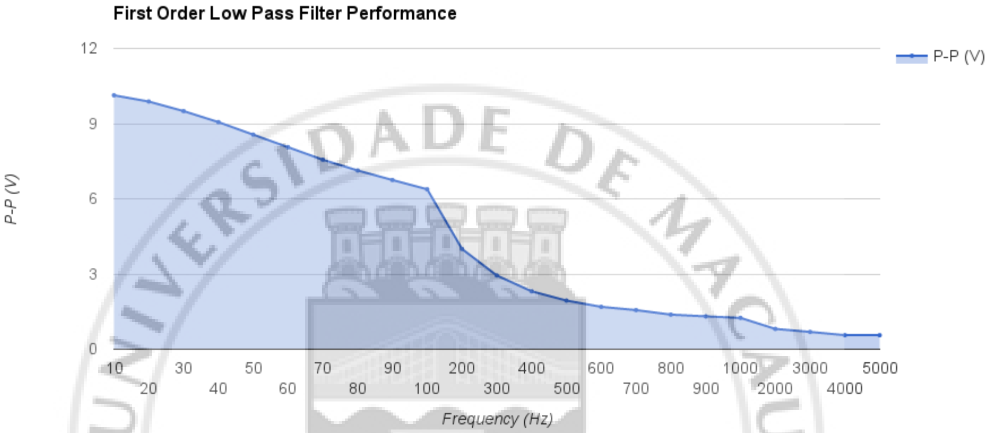


Fig 3. 12 The measurement result of 1st order low pass filter

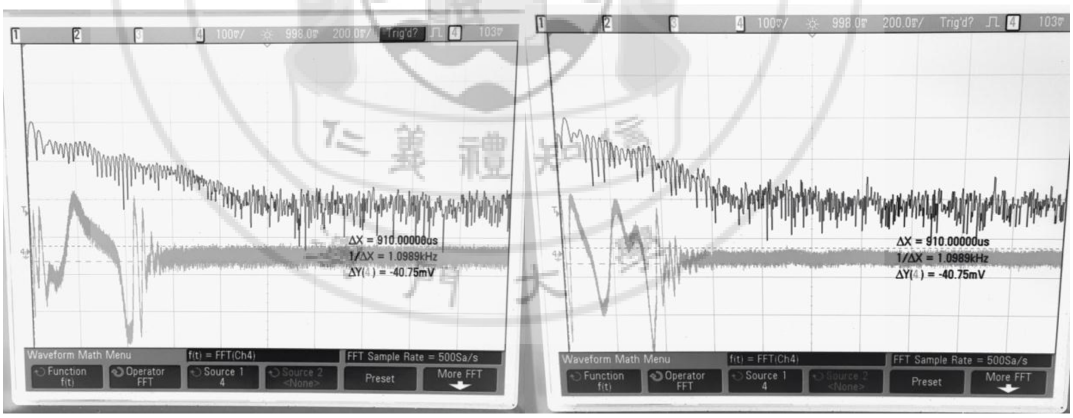


Fig 3. 13 Left one is without low pass filter, right one is with filter

According to this formula as follow to design the amplifier gain:

$$\text{DC gain} = 1 + \frac{R_2}{R_1} \qquad (3.2)$$

Set R_1=200 Ω, R_2=20KΩ,

$$\text{DC gain} = 1 + \frac{20K\Omega}{0.2K\Omega}$$

$$\text{DC gain} = 101$$

Hence, we got DC gain equals to 101.

For the low pass filter amplifier, the circuit like Fig 3.14, V_{in} will connect with the IF of HB100, amplifier component initially chooses 741 (Fig 3.15). The practical connection may refer to Fig 3.16. After build up the HB100 with low pass amplifier, the performance has been changed obviously (See Fig 3.17), due to the signal has been gain to very large, the noise relatively less even didn't see. The voltage level was gain from original micro voltage mV level to voltage level, the noise still in micro level, hence we can infer that the noise is depends on the Doppler radar detect quality or come from another electromagnetic wave exist in the atmosphere.

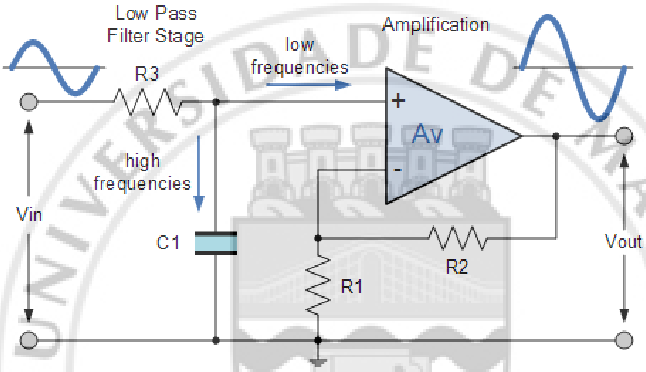


Fig 3. 14 Low pass amplifier circuit connection [10]

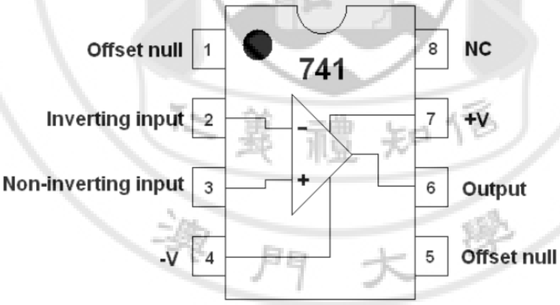


Fig 3. 15 741 8 pin IC configurations [11]

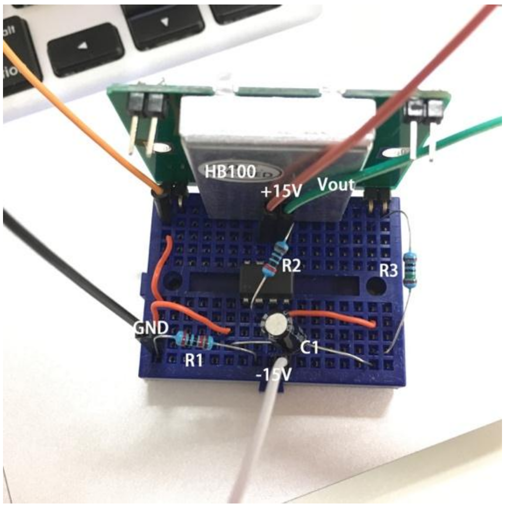


Fig 3. 16 Connection in laboratory

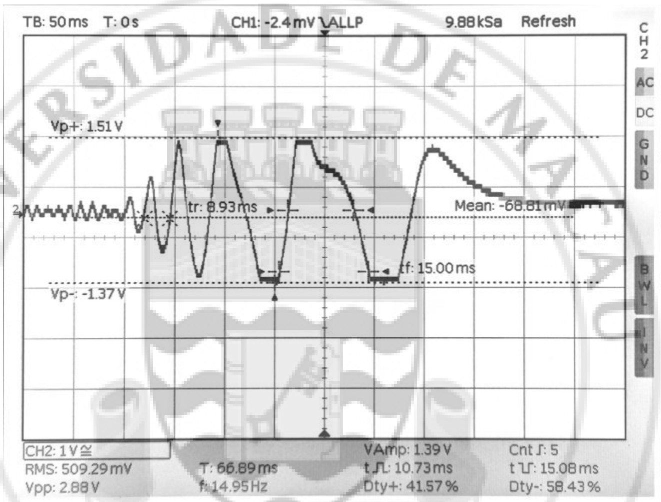


Fig 3. 17 The waveform generated by HB100 with low pass amplifier, the signal has been gained to voltage level

3.2.5 Challenge of Doppler Radar

The analog signal has been got, we may need to consider how to digitalize the signal to Arduino for processing. We found the peak to peak voltage V_{p-p} change in different situation, if no object is moving in the detect area, the V_{p-p} normally is around 100mV (Fig 3.18), namely 0.1V; if the detector has detected dynamic objects, the V_{p-p} is between 0.6V~1.4V (Fig 3.19 & Fig 3.20), the voltage intensity depends on the distance between the detector and object. As a case, if we can be sampling the V_{p-p} data to Arduino and determine when V_{p-p} higher than a critical point, the digitalize is achievable. Moreover, the detector sensitivity will depend on the critical point.

LM741 op-amp is a comment use component in university even industry, however there have some issue when use LM741 be amplifier in our project.

According to the LM741 datasheet (Table 3.1), the normal supply voltage should +/-15V, minimum is +/-10V. For the Arduino only can maximum supply 5V output to other device, it is not possible to be the power supply for LM741. It is necessary to find other op amp to replace it, LT1006 (Fig 3.21) should one of the suitable op amp component for the detector amplifier, it can operate in single supply voltage, its design has been optimized for single supply operation with a full set of specifications at 5V. [19]

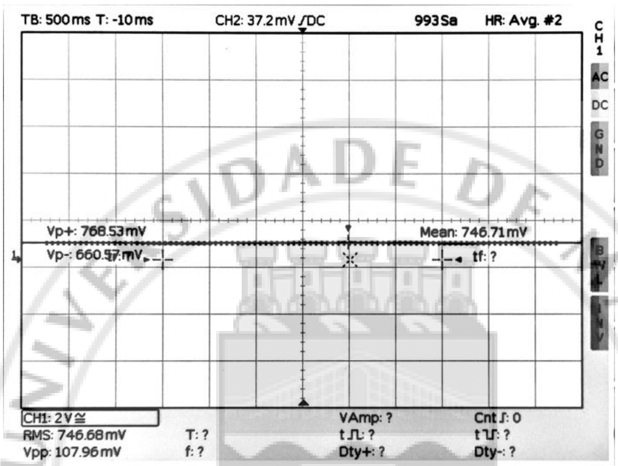


Fig 3. 18 Nothing be detected, V_{p-p} is around 100mV

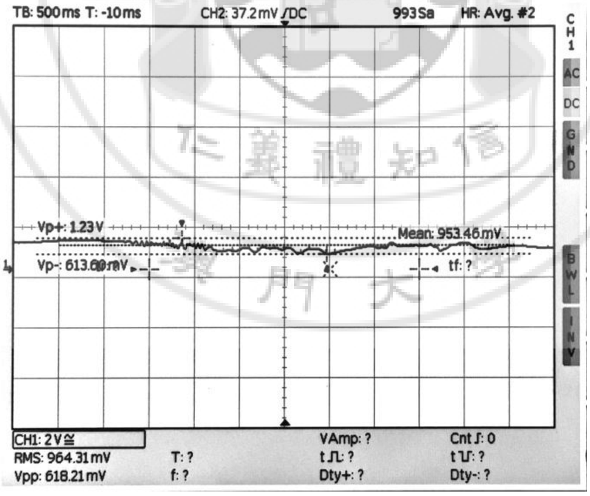


Fig 3. 19 A dynamic object was detected, distance between 1m, V_{p-p}=618mV

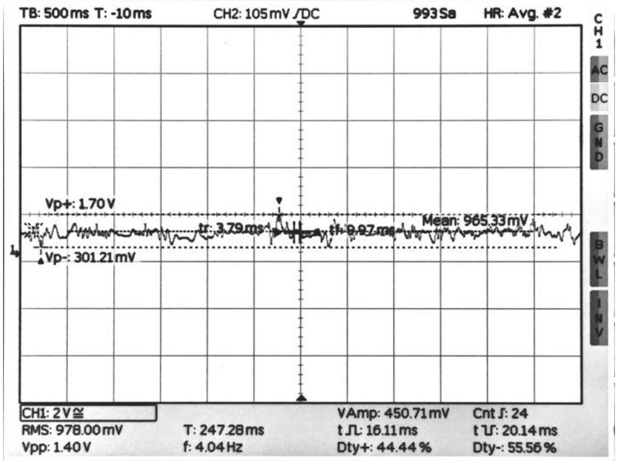
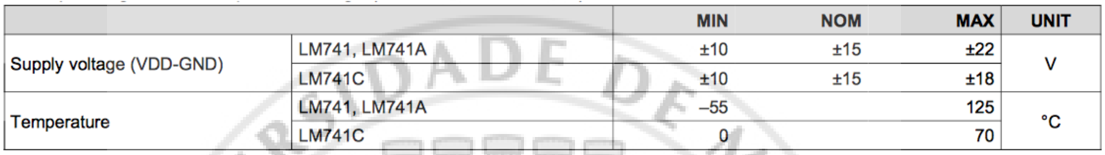


Fig 3. 20 Detected object distance between 30cm from HB100, $V_{p\text{-}p}$=1.4V



		MIN	NOM	MAX	UNIT
Supply voltage (VDD-GND)	LM741, LM741A	±10	±15	±22	V
	LM741C	±10	±15	±18	
Temperature	LM741, LM741A	–55		125	°C
	LM741C	0		70	

Table 3. 1 Recommended Operating Conditions of LM741 [12]

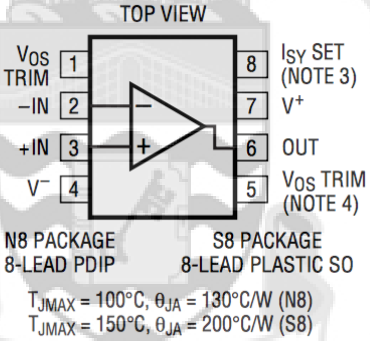

TOP VIEW
V_{OS} TRIM
1
–IN
2
+IN
3
V^-
4
8
I_{SY} SET (NOTE 3)
7
V^+
6
OUT
5
V_{OS} TRIM (NOTE 4)
–
+
N8 PACKAGE 8-LEAD PDIP
S8 PACKAGE 8-LEAD PLASTIC SO
T_{JMAX} = 100°C, θ_{JA} = 130°C/W (N8)
T_{JMAX} = 150°C, θ_{JA} = 200°C/W (S8)

Fig 3. 21 LT1006 Signal supply op amp [12]

3.3 Infrared Sensor

Infrared radiation is a part of electromagnetic spectrum having wavelengths longer than visible light wavelengths, the infrared region roughly from 0.75μm to 1000 μm, for human eyes is not able to see. Infrared include near infrared (wavelength region of 0.75μm to 3 μm), mid infrared (3 μm to 6 μm) and far infrared (higher than 6 μm). [11] For many distinct types of infrared sensor, basically their physics is governed by three laws, Planck’s radiation law, Stephan Boltzmann Law and Wien’s Displacement Law.

Planck’s radiation law said every object emits radiation if the temperature T higher than 0K (-273C^{O}), the temperature and surface condition of an object determine the infrared radiant energy.

Stephan Boltzmann Law said the total energy emitted is relate to the temperature of the object, he stated a formula:

$$W_b = \sigma T^4 \text{---------------------------------------}(3.3)$$

Where,

$W_b: Total\ energy\ emitted, \sigma: Constant = 5.67\times10^{-8} m^{-2} K^{-4},$
$T: Temperature\ of\ the\ object$

Wien’s Displacement Law shows a hotter the object, the shorter the wavelength of the radiation spectrum or the higher the frequency of the radiation spectrum. The formula as follow:

$$\lambda_{max} = \frac{b}{T} \text{---------------------------------------}(3.4)$$

Where λ_{max} is the peak of the wavelength, b is a constant $2.8978\times10^{-3} m \cdot K$, T is the temperature of the black body.

3.3.1 Types of infrared sensor

Basically, infrared sensor can separate in two types, active infrared sensors and passive infrared sensors. Active infrared sensors are the types of infrared sensor that emit infrared radiation and received by the receiver. [3] To emit the IR generally use IR Light Emitting Diode (LED), receive IR will use phototransistor, photodiode or photoelectric cells. Break beam sensors and reflectance sensors are the common active infrared sensors.

Break beam sensors like Fig 3.22, the IR emitter emit towards the receiver continuously, if an object in between the emitter and receiver, the receiver will not receive any IR signal, hence in this situation was considered the sensors has detected something. It is very easy to digitalize the signal, since the receiver only to consider receive or not receive signal, it just like 1 or 0 in digital. However, break beam sensor cannot provide wider range detection, due to its properties only able to emit a line path IR. Therefore, it may not appropriate use in security situation.

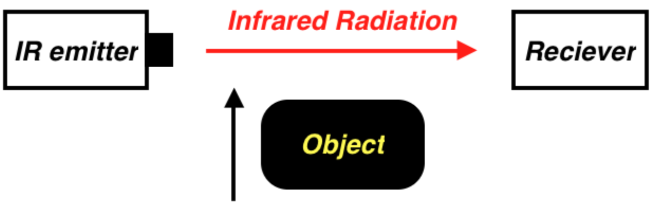


Fig 3. 22 Break beam sensors

Reflective is one of the property of infrared, reflectance sensors productize according to this property, the working principle is that (see Fig 3.23), the emitter emits an IR beam and reflected by the object, the receiver receive IR reflected signal if the receive value has been changed, it is means some object is moving into the detection area, the receive value can refer the IR intensity.

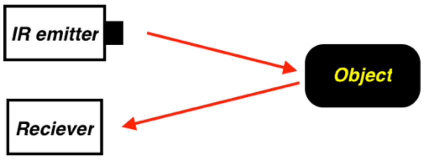


Fig 3. 23 Reflectance sensors

Passive infrared sensor doesn't emit any infrared itself, hence it doesn't have emitter but detect the infrared radiations from external source, Pyroelectric infrared sensor (PIR) is one of the passive infrared sensor, nowadays are very famous to use in many systems especially in smart or energy saving system. Moreover, PIR sensor can provide wide range detection, since we found PIR have more advantages than active infrared sensor, finally we decide to choose PIR to motion detector in IR sensor field.

3.3.2 Pyroelectric infrared sensor (PIR)

3.3.2.1 Theory

In part 3.3.1 has mentioned that PIR sensor is absorb infrared which emitted by the object itself. When the infrared radiates to the material and produce charge, called Pyroelectric infrared sensor, the optical sensor for that kind of human infrared sensor made by Glycine sulfate (TGG) or Piezo acid piezoelectric materials (PZT) [13]. The circuit like Fig 3.24.

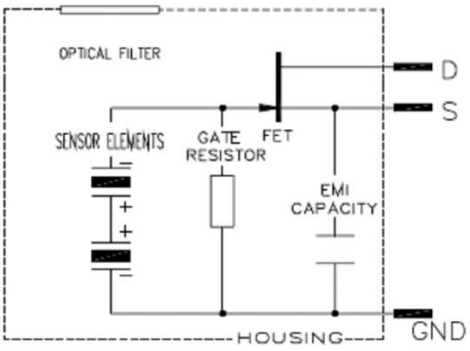


Fig 3. 24 Part of circuit of PIR

In Fig 3.24 can see there have two sensor elements, they can receive all wavelengths of infrared, in other words they don't have selectivity for themselves, to solve this issue by adding an optical filter on the sensor elements, it designs for wavelength of infrared between 7 to 14 μm can pass through, it is because the infrared wavelength is 10 μm when the human temperature in 36.5 ^{O}C.

The sensor elements were designed in pair opposite polarity, if don't have any thermal sources move in the detection range, fundamentally generated faint charge will be low because of the polarity of each other; when the thermal source move in the PIR detection range, one of the sensor element will accumulate charges than potential difference will be produced, hence sensor element make voltage difference like Fig 3.25; one more situation when the static thermal source in the detection area, two sensor elements induce the infrared is equal, both of them accumulate a certain amount of chargers, therefore the sensor will keep the status like don't have any thermal sources move in the detection range. In our project, HC-SR501 was chosen as the PIR motion detector.

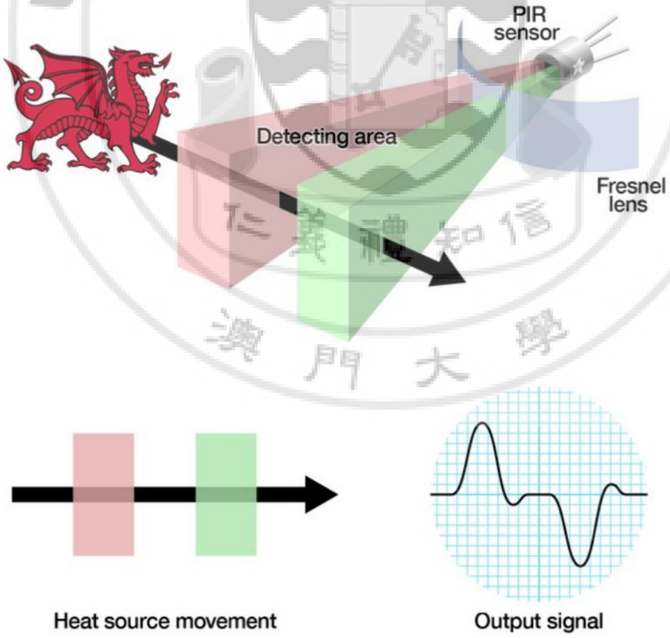


Fig 3. 25 The reaction of the PIR sensor element when it sense the object [13]

3.3.2.2 PIR HC-SR501

HC-SR501 (see Fig 3.26-3.28) is commonly used with Arduino, its size very small, length 2.5cm and width 3.2cm,low power with 5V DC can supplied by Arduino, the output has been digitalized, it output high when motion is detected (high is 3.3V) or low when no motion is detected . On top side can see a lens cover the Pyroelectric infrared-detector, it is very important component that make the wider detection range, later will talk about how do the lens works. In under side have some components can be adjusted by the user, which are time delay adjust, sensitivity adjust and trigger selection jumper, for position of the components please refer to Fig 3.27.

The time delay adjustment restricts how long the output of the PIR sensor will remain high if the motion was detected. The adjustment range from minimum 3 seconds to maximum 5 minutes. The sensitivity adjust means the adjustable range, the minimum range from 3m to maximum 7m. The trigger selection jumper allows user to select single or repeatable triggers, single trigger mean if the sensor has detected some objects, the time delay will begin immediately; for repeatable triggers, each detected motion resets the time delay. [22]

The HC-SR501 has 110^{o} cone view area, to achieved the wide range due to the lens, the lens actually has a special appellation called Fresnel lens. The Fresnel lens can condense light, and providing a larger range of IR to the sensor (See Fig 3.29). [18]

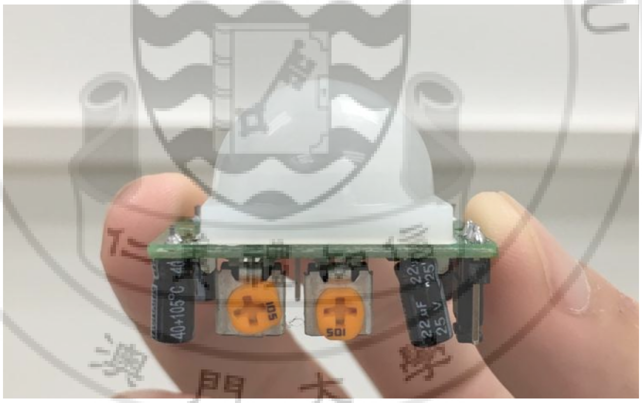


Fig 3. 26 HC-SR501 PIR motion detector

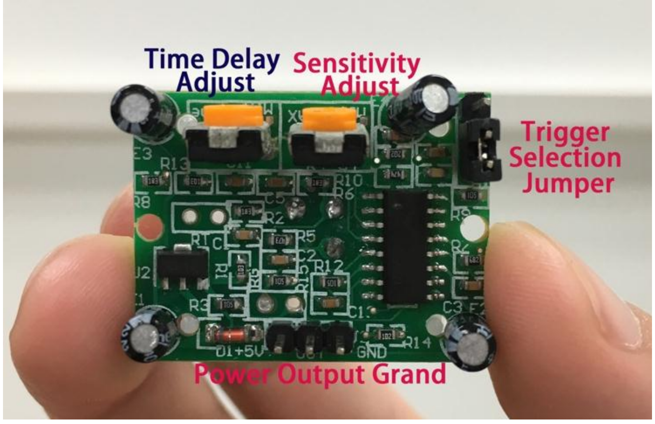


Fig 3. 27 The Circuit board of HC-SR501

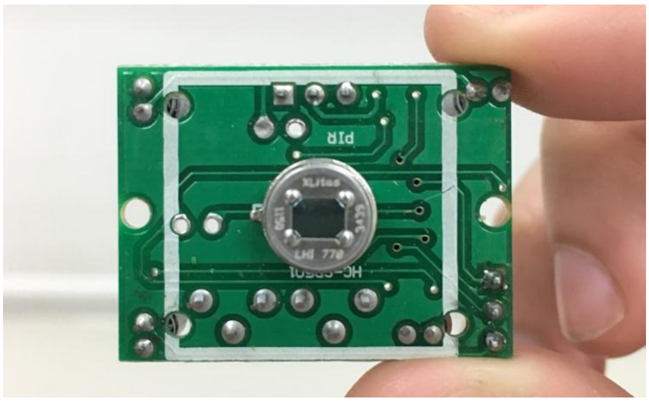


Fig 3. 28 Remove the lens can see the LHI778 Pyroelectric infrared-detector

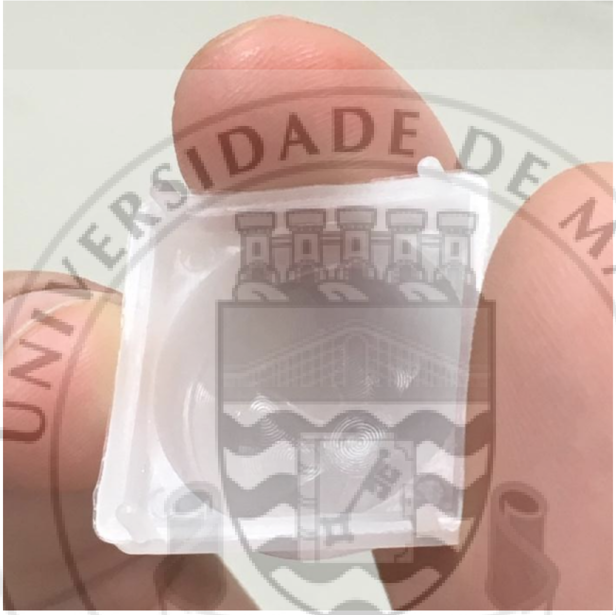


Fig 3. 29 Fresnel lens

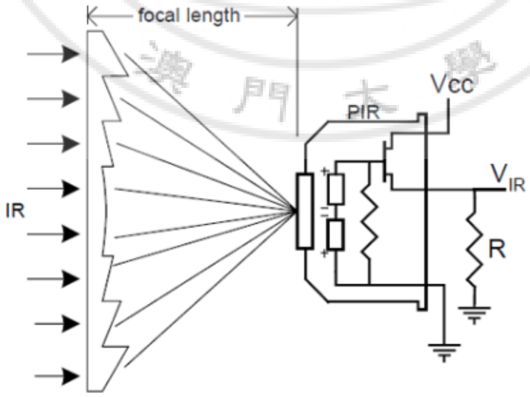


Fig 3. 30 The performance of Fresnel lens [13]

3.3.2.2 Blocked Time Limitation

The HC-SR501 itself has 3 second block time [22], which mean the detector stops detection for 3 seconds after the delay time, it is quite not safe for security view especially for our project. However, according to some datasheet said the block time can be made a range to 0.2 seconds [22], therefore, in the next part we will discuss how to deal with the blocked time problem.

3.3.2.4 The Solution Scheme of Blocked Time Limitation

HC-SR501 PIR Sensor was selected be the motion sensor which due to its digitalize output and its sensitivity is better than Doppler radar. However, refer to the specification of the PIR Sensor, itself have 2.5 second blocked time in default setting or say factory settings. Blocked time happen when PIR sensor detect some heat radiation explored by the object, the sensor will be trigged in high level mode, which means the output is high voltage (around 3V) or say 1. The time duration in high mode is depends on a factor Tx, actually for HC-SR501 Tx is adjustable through screw the variable resistance (Fig 3.31), therefore Tx value depends on one of the resistor value, to identify which resistor on the circuit will mention later. After Tx, the sensor output mode from high drop back to low, then blocked time will happen. Refer to Fig 3.32 could see even some objects are moving in the detected range during blocked time period, the PIR sensor does not have any response. Obviously, this is security loophole if apply in the system, imagine somebody could use this 3 second sensor blocked time loophole to access the door without any permission, definitely this system we are not expect. After that through some research found that some methods could modify the blocked time shorten to 0.2 second only, which called "Hacking". At the following, will talk about the procedure of PIR hacking.

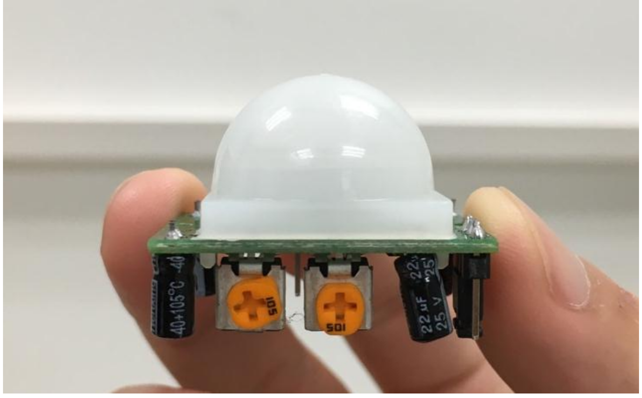


Fig 3. 31 Screw the left variable resistance can adjust the Tx

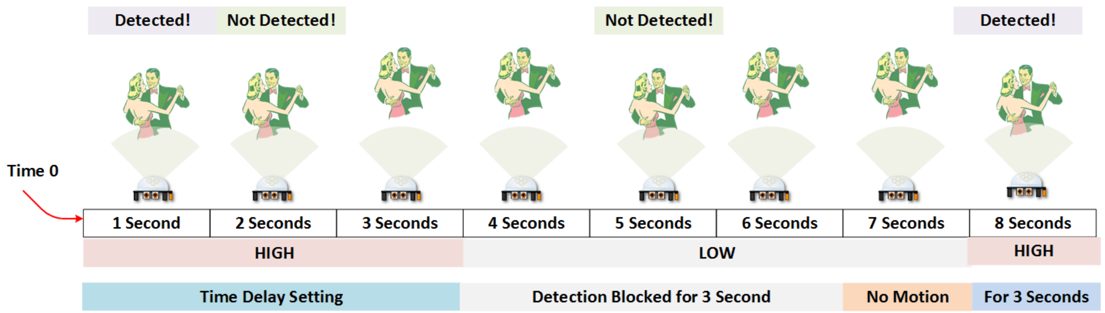


Fig 3. 32 Blocked time (Gray bar) happen after High mode of PIR sensor [14]

HC-SR501 PIR sensor designed according to the circuit like Fig 3.33, the design includes a chip called BISS0001, which is a Micro Power PIR Motion Detector IC, it takes the output of the sensor and does some minor processing on it to emit a digital output pulse from the analog sensor, also it built-in Power up disable & output pulse control logic. BISS0001 has 16 pins (Fig 3.34), for each pin description and working principle can refer to Table 3.2 and Table 3.3.

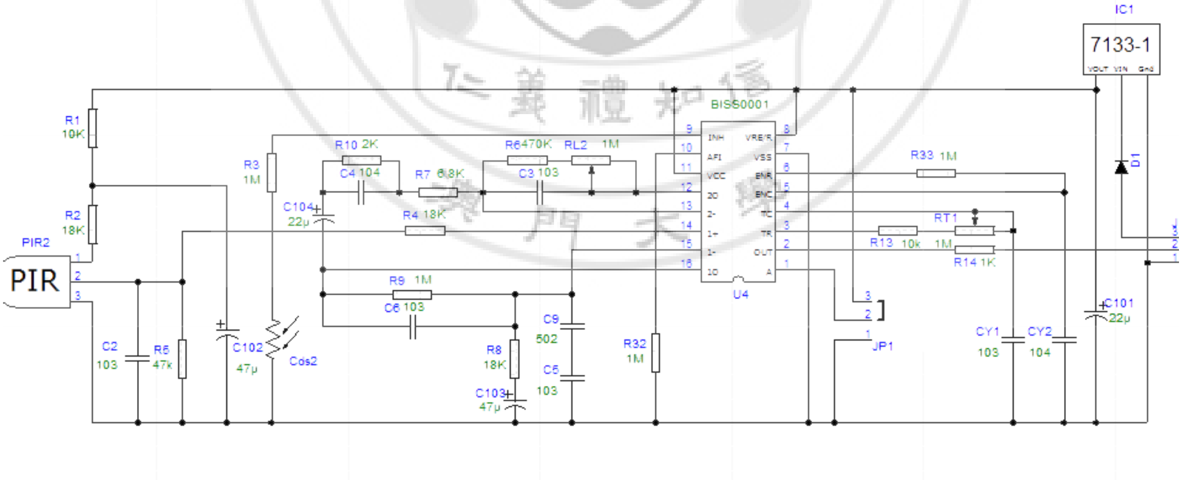


Fig 3. 33 HC-SR501 Circuit Design [13]

Pin Number	Symbol	Description
1	A	Retriggerable & non-retriggerable mode select (A=1 :re-triggerable)
2	VO	Detector output pin (active high)
3	RR1	Output pulse width control (Tx)
4	RC1	Output pulse width control (Tx)
5	RC2	Trigger inhibit control (Ti)
6	RR2	Trigger inhibit control (Ti)
7	V_{SS}	Ground
8	V_{RF}	RESET & voltage reference input (Normally high. Low=reset)
9	V_C	Trigger disable input (V_C >0.2V_{dd}=enable; V_C<0.2V_{dd}=disabled)
10	I_B	Op-amp input bias current setting
11	V_{dd}	Supply voltage
12	2OUT	2nd stage Op-amp output
13	2IN-	2nd stage Op-amp inverting input
14	1IN+	1st stage Op-amp non-inverting input
15	1IN-	1st stage Op-amp inverting input
16	1OUT	1st stage Op-amp output

Table 3. 2 Pin Description of BISS0001

DESCRIPTION	CONDITION	RANGE	UNIT
SUPPLY VOLTAGE	n/a	3 to 5	V
INPUT VOLTAGE	n/a	V_{ss} -0.3 to V_{dd} +0.3	V
OUTPUT CURRENT	V_{dd}=5V	10	mA
OPERATING TEMPERATURE	n/a	-20 to +70	°C
STORAGE TEMPERATURE	n/a	-40 to +125	°C

Table 3. 3 Working Principle of BISS0001

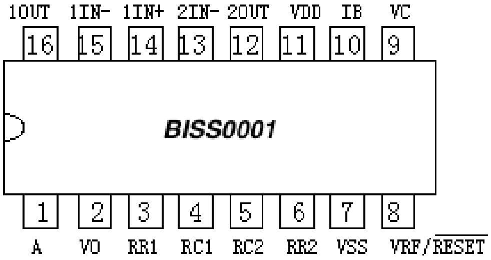


Fig 3. 34 BISS0001 Pins [15]

From Table 3.2 We see there have two values T_x and T_i, for definition, T_x = The time duration during which the output pin (V_o) remains high after triggering; T_i = During this time period, triggering is inhibited. Simply speaking T_i is a factor which relate to the blocked time. And there are two formulas in below show how to control the T_x, T_i values.

$$Tx \approx 24576\ \text{x}R13\ \text{x}\ CY1\text{--------------------------------}(3.5)$$

$$Ti \approx 24\ \text{x}\ R33\ \text{x}\ CY2\text{-----------------------------------}(3.6)$$

According to Fig 3.33 can see, resistors R13, R33 and capacitors CY1, CY2 have their own design values by factory setting (See Table 3.4 & Table 3.5), just simple calculation can precisely to calculate the shortest high state output time delay (Tx) is 2.4576 second, refer to datasheet roughly say is 3 second. For the shortest blocked time delay (Ti) in precisely calculation is 2.4 second, similarity in datasheet roughly say is 2.5 second. Moreover, in the HC-SR501 circuit design diagram could see there has an addition resistor RT1 series with resistor R13, it is a 1M ohms variable resistance can be adjusted by user, it means user can through this variable resistance to control the high state output time delay, and also by simple calculation we can calculate that the longest time delay is 248.2176 second around 4~5 minutes.

Tx Component	Value from factory Setting
R13	10kΩ
CY1	10nF

Table 3. 4 The value from factory setting of T_x

Ti Component	Value from factory Setting
R33	1MΩ
CY2	100nF

Table 3. 5 The value from factory setting of T_i

The shortest high state output time delay:

$$Tx \approx 24576\ \mathrm{x}R13\ \mathrm{x}\ CY1$$

$$Tx \approx 24576\ \mathrm{x}10k\Omega\ \mathrm{x}\ 10nF$$

$$Tx \approx 2.4576s$$

The longest high state output time delay:

$$Tx \approx 24576\ \mathrm{x}(R13+RT1)\ \mathrm{x}\ CY1$$

$$Tx \approx 24576\ \mathrm{x}(10k\Omega+1M\Omega)\ \mathrm{x}\ 10nF$$

$$Tx \approx 248.2176s$$

The shortest blocked time delay:

$$Ti \approx 24\ \mathrm{x}\ R33\ \mathrm{x}\ CY2$$

$$Ti \approx 24\ \mathrm{x}\ 1M\Omega\ \mathrm{x}\ 100nF$$

$$Ti \approx 2.4s$$

Clear thinking, to shorten the blocked time delay, just to reduce the value of R33, or remove it directly. Theoretically, if R33 was removed, it means equals to zero, the modified blocked time should almost be equal to zero.

We decided remove resistor R33 and make it short circuit (Fig 3.35), since the resistor is very small, the circuit is very close with others. The welding work must need be careful, otherwise it will get permanent damage for the PIR sensor. Finally, we success to remove R33 and weld Tin wire connect it again. From Fig 3.36 can see the blocked time was around 5.5s before hacking, but after hacking (like Fig 3.37), the blocked time is much more shorten to less than 200ms for each time. Therefore, the solution scheme is satisfactory and successful.

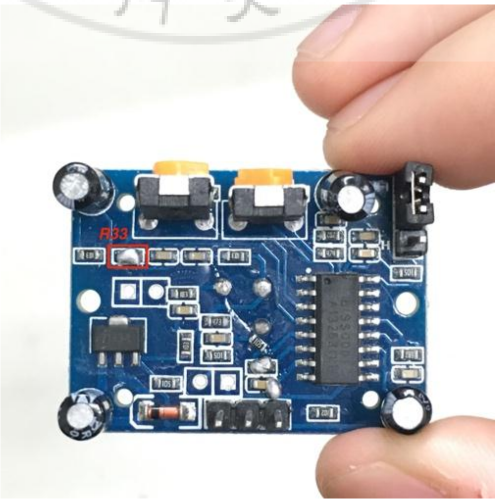


Fig 3. 35 To remove the R33 and short it.

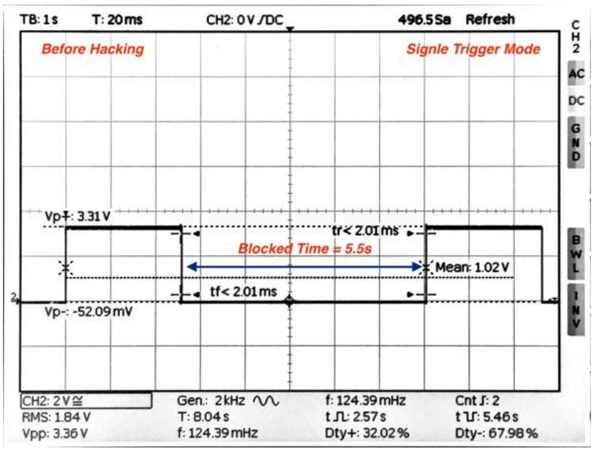


Fig 3. 36 Before hacking the HC-SR501 blocked time is 5.5s

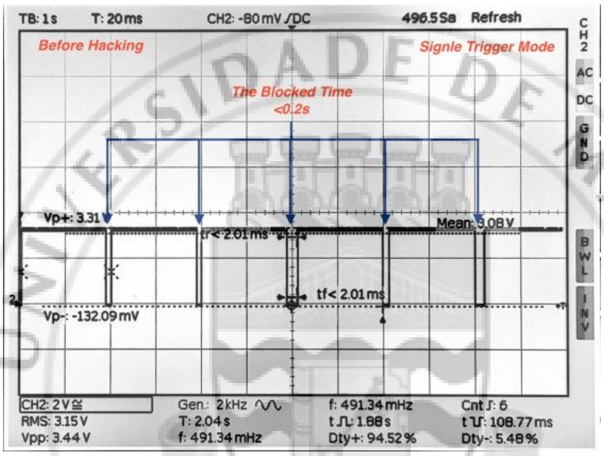


Fig 3. 37 After hacking the HC-SR501 blocked time less than 200ms

CHAPTER 4

SYSTEM DESIGN AND ARCHITECTURE

4.1 Component Arrangement

4.1.1 RS232

RS232 (Recommended Standard 232) is an asynchronous serial communication standard interface that was introduced by the Electronic Industries Association (EIA) in 1969. It is so called “asynchronous transmission” as the transmission of data by RS232 do not require an additional transmission line to send synchronization signals, then the data can be successfully transmitted to the other side.

In the electrical characteristic of RS232, +3V to +15V represent high potential while +3V to -15V represent low potential with respect to the common ground, which is unlike the usual use of Transistor-transistor Logic (TTL) level. Valid signal is either in the range of +3V to +15V or the range of -3V to -15V. Consequently, the transmission potential is not a valid RS232 level when it is greater than +15V, less than -15V or between -3V and +3V. This is where attention should be paid when using RS232. For data transmission lines (TxD, RxD), a positive voltage between +3V and +15V represents a logic 0 and the signal condition is called “space”. On the other hand, logic 1 is negative voltage between -3V to -15V and the signal condition is termed "mark". RS232 connector has 9 pins. Pin 2,3 serve as transmission and reception of the data respectively. The pin assignment of a female RS232 connector is tabularized below.

Pin Number	Signal
1	Data Carrier Detect (DCD)
2	Transmitted Data (TxD)
3	Received Data (RxD)
4	Data Terminal Ready (DTR)
5	Signal Ground
6	Data Set Ready (DSR)
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	Ring Indicator (RI)

Table 4.1 DB9 Female Pin Assignments

4.1.2 SP3232E

SP3232E is an integrated circuit (IC) connected to RS232 serial port as a mechanism for electrical level conversion. Most microcontrollers currently have built-in UARTs (Universally Asynchronous Receiver/Transmitter) that can be used to serially receive and transmit data. The method of transmitting one bit at a time at a specific baud rate (i.e. 9600bps, 115200bps, etc.) by UARTs is sometimes referred to as TTL serial. TTL serial signals exist between the limits of 0 and a microcontroller's maximum voltage supply V_{cc}, which is typically 3.3V or 5V. A signal at V_{cc} level indicates a logic 1, while 0V signal represents a logic 0.

RS232 signals are analogous to serial signals from the microcontroller in a manner that they transmit one bit at a time at a specific baud rate. However, RS232 is like TTL serial turning upside down. By the RS232 negative voltage – anywhere from -3V to -15V – corresponds to a logic 1 whereas a logic 0 transmits a positive voltage that can be anywhere from +3V to +15V.

Although TTL is much easier to implement in embedded circuits between the two serial signal standards, it is more likely to suffer losses along the transmission line in the long-range serial transmission. Thus, the more extreme voltages of an RS232 signal help to make it less susceptible to noise, interference and degradation.

A TTL serial device can't interface with an RS-232 bus directly. To interconnect any two different logic levels, their respective logic 1s and logic 0s must match up. When two serial devices connect to each other that one of which works over TTL and the other over RS232, the logic 1 of TTL (around 3.3V—5V) is required to convert into the logic 1 of RS232 (around -3V — -15V), and similarly the logic 0 of TTL (around 0V—0.8V) into the logic 0 of RS232 (around +3v — +25v). Without the electrical level conversion, logic 0 of TTL would be interpreted as a logic 1 in RS232, making all the data transfer go wrong.

Not only do the signals have to be inverted, but the potentially harmful RS232 voltages also have to be regulated to something that won't damage the serial pins of microcontroller. Actually, there are a lot of solutions to this problem of voltage converting and inverting. The solution proposed here is connecting an SP3232E which is employed to convert signals from RS232 serial port TTL to signals suitable for use in TTL-compatible digital logic circuit, or vice versa between the two devices.

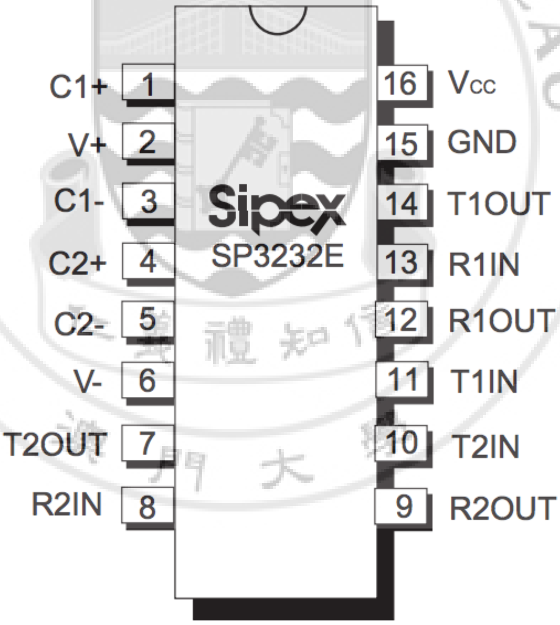


Fig 4.1Pinout Configuration for the SP3232E [16]

4.1.3 S-8600 UHF RFID reader

RFID reader works as a central role in the RFID system. S-8600 used here is a fixed UHF RFID reader with extremely reliable reading and writing capabilities. It is important to note that the reader conforms to the ISO 18000-6C protocol (an international standard describing a series of diverse RFID technologies), which guarantees interoperability with EPC Class 1 Gen 2 compatible tags. The specification of the reader is shown in Table 4.2.

Tag inventory means finding out which tags are nearby, then picking out the tags that are currently responding. The performance of it greatly determines the merits of the reader. Data acquired by tag inventory will be either uploaded immediately or cached firstly then uploaded all at once when called, which forms the real-time mode and buffer mode respectively. Real-time mode is recommended if the instant response is desired since the aggregated data in buffer mode will take certain time to filter out the duplicate when the reader identifies a large number of tags.

S-8600 UHF RFID Reader	
Host Communication	RS232 or TCP/IP
Dimension	230mm(L) x 160mm(W) x 28mm(H)
Weight	1.8 kg
Air Interface Protocol	EPC global UHF Class 1 Gen 2 / ISO 18000-6C ISO 18000-6B
Input Voltage	DC 12V – 18V
Spectrum Range	860MHz – 960MHz
Output Power	0 – 33dBm
Receive Sensitivity	< -85dBm
Peak Inventory Speed	> 700 tags/sec
Tag Buffer Size	1000 tags @ 96-bit EPC
Tag RSSI	Supported
Max Baud Rate	115200 bps

Table 4.2 Specification of S-8600 UHF RFID reader

4.1.4 Microcontroller

The microcontroller is the central processing unit in the system. It is responsible for storing and executing the system software, and interfacing with all of the peripheral devices. The Arduino Mega 2560 is an open source microcontroller board based on the ATmega2560, mostly running by a 16MHz crystal oscillator with 256Kb of flash memory. It features 54 digital input/output pins, 16 analog inputs, 4

UARTs. The RFID reader needs only 4 pins: TX, RX, Vcc, GND. It also provides a Universal Serial Bus (USB) connection to PC for programming and debugging.

4.2 Access Control System Lock - Electromagnetic Lock

Many types of the door locks can be chosen as the Access Control System Lock, some types are very common to use such as Electric Dropbolt, Electric Strike and Electromagnetic Lock. For those three locks, physically their function are same, we finally decided choose electromagnetic lock as the Access Control System Lock, because it is easier to install for prototype.

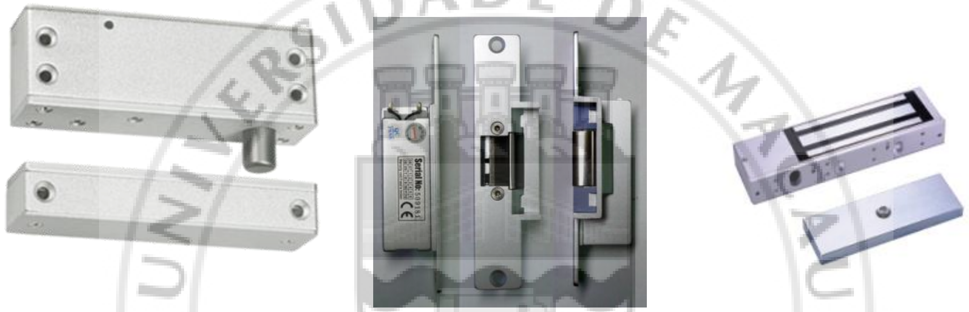


Fig 4.2 Three common types of door lock Electric Dropbolt, Electric Strike and Electromagnetic Lock (From left to right) [17]

An electromagnetic lock, also called magnetic lock or maglock, is one of the locking device that consists of an electromagnet and an armature plate. Its principle is according to the electromagnetism to lock the door when energized, magnetic field produced when current flow through the coil. The magnetic force make the electromagnet and armature plate stick together, creating a locking action, also the force is very large, typical single door electromagnetic locks are offered in both 600 Ibs.(272kg) and 1200 Ibs.(544kg) dynamic holding force capacities. The maglock able to offer large magnetic force is because the mating area of the electromagnet and armature is relatively large, the magnetic force is strong enough to keep the door locked even under stress.

The electric locking can mainly separate in two types, “fail safe” and “fail secure”. A fail-secure locking device can remain locked when power is lost, like electric strikes. Fail-safe locking devices are unlocked when no power supply. A "fail safe" magnetic lock requires power to remain locked and typically is not suitable for high security applications because it is possible to disable the lock by disrupting the power supply. To solve this kind of issues, by adding a magnetic bond sensor to the lock and by using a power supply which includes a backup capability, so that some specialized higher security applications can be implemented.

Here have some equations to calculate the magnetic flux density and magnetic force:

$$B = \frac{\mu_0 \mu_r IN}{l} \text{---------------------------------------}(4.1)$$

B is magnetic flux density induced by a solenoid of effective length l with a current I through N loops.

$$F = \frac{B^2 S}{2\mu_0} \text{--}(4.2)$$

F obviously is magnetic force, S is surface area about the electromagnet and the armature plate exposed to the electromagnet.

From the above formulas, we can see if want to control the force of the magnetic lock, it is possible to change the magnetic flux or surface area about the electromagnet and the armature plate that make the magnetic force become larger, usually surface area will not be made very large, so industry prefer to change magnetic flux rather than surface area. As the formula above can find when the current becomes larger the magnetic flux will become so, there have proportional relative of these two factors. Of course, the number of coils also can affect the magnetic flux, factory will use the number of coils determines the holding force which characterizes the lock, for micro size, the holding force is 275lbf (1,220N); 650 lbf (2,990N) holding force for mini size; 800 lbf (3,600N) for midi size; 1,200 lbf (5,300N) for standard size; and 2,000 lbf (8,900N) for shear lock. Most of the gate locks are belong to standard size. To define the holding force, a pulling force was added to the armature plate, the pulling force from small increase to large until the pulling force reach a point of force to make the electromagnet and the armature plate separate, that force can be defined as holding force of the magnetic lock.

The electromagnetic lock is working at DC current, the power around 5~6W, when the voltage supply is 12VDC, the current is around 0.5~0.6A, 0.25A when the voltage supply is 24VDC.

4.3 Hardware Architecture

In our prototype, the whole logical process is that, the motion sensor determined whether the area have people or not, if people was detected, the signal will send to the Arduino, the Arduino immediately turn on the electromagnetic lock and sent read tag command to the RFID reader, the reader will send back to Arduino to be verified, if the tag was read and is verified, the Arduino will send command to unlock the electromagnetic lock.

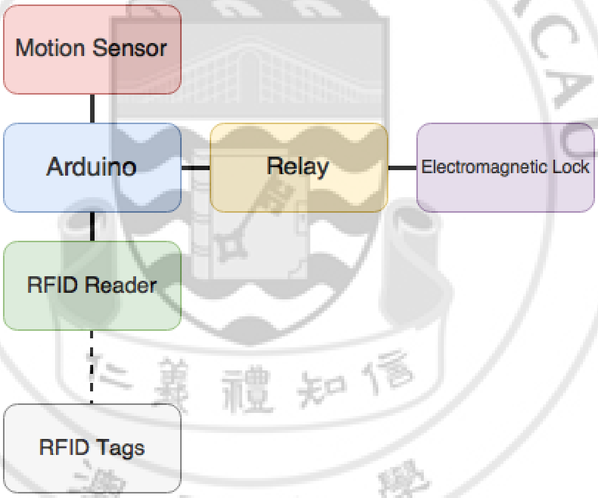


Fig 4.3 System structure diagram

4.4 Software Architecture

The figure below show how the program operates. The code which can realize the entire system by using interrupt on digital pin can be found in the Appendix.

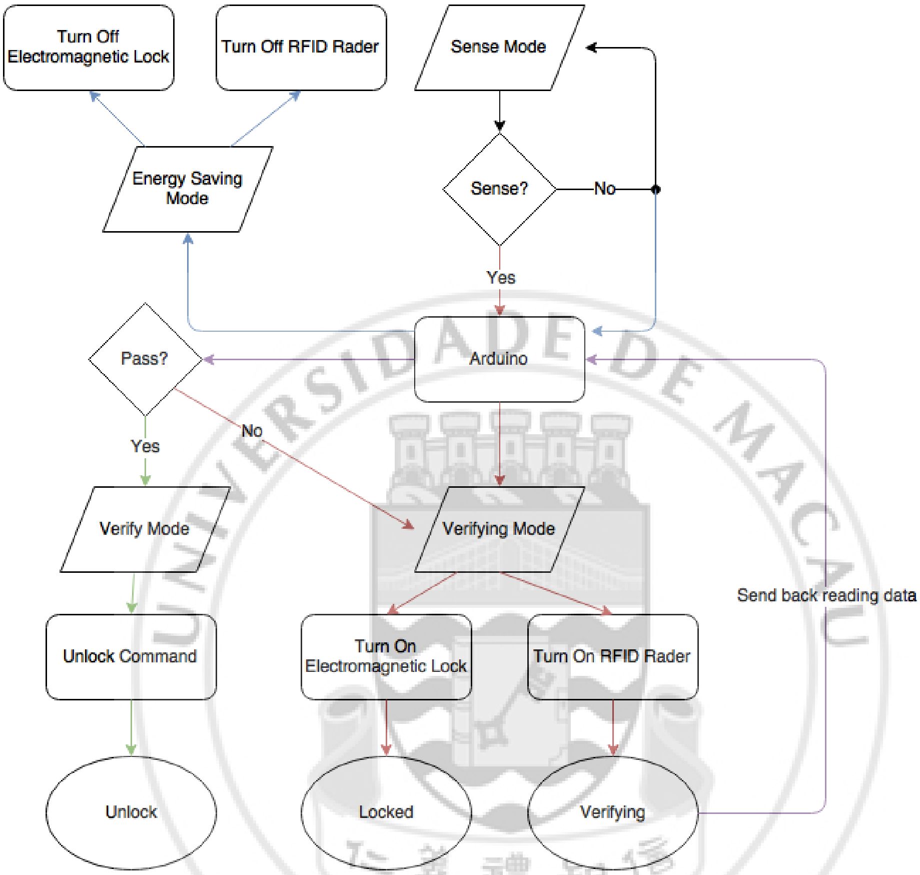


Fig 4.4 The flow of the system

4.5 Evaluation of Energy Used for the System

Energy saving is one of the goal we want to reach in this project, since now a day, humans are facing with different environmental issues such as global warming, climate change or sea-level rise. Those problems are due to humans over use or abuse the sources in the earth. Many places are moving forward to urbanization, urbanization will make larger electricity usage, moreover, most of the city still mainly use nonrenewable resources to produce electricity. In 2014, there have 69% power generated by fossil fuels [6] (see Fig 4.4), greenhouse gases produced during burn the fossil fuels for power generate, Carbon Dioxide CO_2 is one of the common greenhouse gas, and it is the murderer cause global warming, since it can absorb infrared. As the solar radiation to the majority of visible light, these visible light can penetrate the atmosphere directly to reach and heat the ground. And the heated ground will emit infrared light to release heat, but these infrared cannot penetrate the atmosphere, so the heat will remain in the atmosphere near the ground, resulting in greenhouse effect. [16]

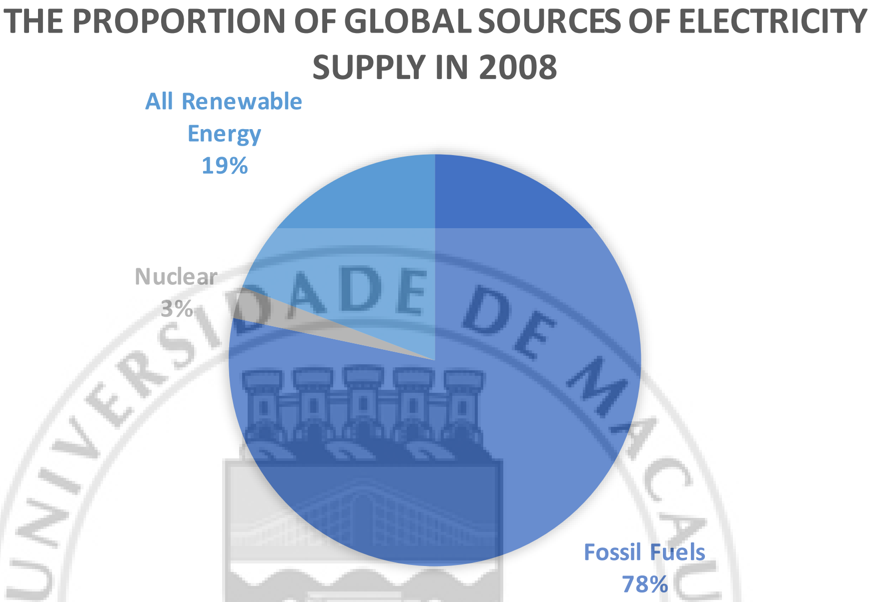


Fig 4.5 Data from REN21 Renewables 2010 Global Status Report

Our system design can reduce the energy usage since we can significantly reduce the working time of electromagnetic lock. In general access control system, the electromagnetic is power all the time, and each lock need 12V DC supply and 0.5A current, the power should be 6W, for more details of the electromagnetic lock please refer to another chapter about. We could calculate that if general access control system their electromagnetic locks power all 24 hours each day, the energy consumption will equal to 51.84kWh per year for one electromagnetic lock. If assume the building's access control system has hundred locks, the energy consumption will be 518.4kWh. Following shown the energy consumption calculation:

$$E_{(kWh)} = \frac{P_{(W)} \times t_{(hr)}}{1000} \text{ --(4.3)}$$

For one Electromagnetic Lock:

$$P_{lock} = 6W \quad t_{(year)} = 24\times365 = 8{,}760hr$$

$$E_{(kWh)} = \frac{6W\times8760hrs}{1000}$$

$$E_{(kWh)} = 52.56\text{kWh/Year}$$

For hundred Electromagnetic Locks:

$$P_{lock} = 6W \quad t_{(year)} = 24\times365 = 8{,}760hr$$

$$E_{(kWh)} = \frac{6W\times8760hrs}{1000}\times100$$

$$E_{(kWh)} = 525.6\text{kWh/Year}$$

The result above just a hypothesis, the energy consumption may much larger if consider in other situation such as in our whole UM campus. In view this, we initiate an idea to implement the access control system to be more energy saving. The idea is adding a motion sensor to the electromagnetic lock detect whether have people passing in front of the door, and the door will power off directly if nobody was detected. Actually, it is not much innovation idea, since this kind of scheme has been applied in light system for energy saving. However, we think it has condition to apply in access control system for electromagnetic lock energy saving. We have done some measurements and calculation that our scheme actual can save the energy up to 54.2%.

Let's go through the power of each hardware in our intelligent access control system, refer to data sheet could found the Arduino power is 0.425W [9], HC-SR501 PIR sensor 0.325W [20], Electromagnetic lock 6W, the RFID reader generates two different power depends on the mode, 2W in standby mode, and 8.6W in scanning mode. After got the power data information, we can mathematically calculate the power consumption. First, to presume an environmental condition is better for comparison, UM's computer room was chosen as the case study. UM's computer room locate in E5 on 2&3 floor. There total have 7 electromagnetic locks for access control system. In general system, the total energy used of those 7 locks for a year should be 51.84kWh × 7 = 362.88kWh, calculation which according to previous done. 362.88kWh must be used no matter have student or not. However, in our system we need to consider how many times the students use computer room that the electromagnetic lock will be powered on. We set the system for each detect will power the locks for 3 seconds, if student stay in the detection zone continuously, the power on time will longer than 3 seconds. Another case is, when the student trigger the system but verified his tag rapidly, the locks power time can be less than 3 seconds. For these unpredictable probability, we probably set each student use times will power on the electromagnetic lock for 3 seconds. According the data from UM registry office, it has 9,987 resisted students in 2016, we could use this data percentage to assume the times of student for access or using the computer room, to calculate the locks energy use accordingly, that's it.

For assuming, every day have 20% of all use the computer room, mainly 1,997 times access the system. For annual energy used of computer access system, the calculation shown following:

20% of all students:

$$9{,}987 \times 20\% = 1{,}997.4$$

According to our setting, each detect will power on the lock for 3 seconds:

$$t_{(Hours\ for\ lock\ and\ reader\ in\ scanning\ mode)} = 1{,}997.4 \times \frac{3}{3600} = 1.6645 hrs/day$$

$$t_{(Hours\ for\ reader\ in\ standby\ mode)} = 24 - t_{(Hours\ for\ lock\ and\ reader\ in\ scanning\ mode)}$$

$$= 24 - 1.6645 = 22.3355 hrs/day$$

Energy used for electromagnetic lock per year:

$$E_{(Lock)} = \frac{P_{(Lock)} \times t_{(Hours\ for\ lock\ and\ reader\ in\ scanning\ mode)} \times 365}{1000}$$

$$E_{(Lock)} = 3.65 kWh/year$$

Energy used for RFID reader in scanning mode per year:

$$E_{(Reader\ scanning)} = \frac{P_{(Reader\ scanning)} \times t_{(Hours\ for\ lock\ and\ reader\ in\ scanning\ mode)} \times 365}{1000}$$

$$E_{(Reader\ scanning)} = 5.22kWh/year$$

Energy used for RFID reader in standby mode per year:

$$E_{(Reader\ standby)} = \frac{P_{(Reader\ standby)} \times t_{(Hours\ for\ reader\ in\ standby\ mode)} \times 365}{1000}$$

$$E_{(Reader\ standby)} = 16.30kWh/year$$

Also, here have some devices working all the time like Arduino and PIR Sensor, there energy used are:

$$E_{(Arduino\ MEGA)} = \frac{P_{(Arduino)} \times 24 \times 365}{1000}$$

$$E_{(Arduino\ MEGA)} = 3.72kWh/year$$

$$E_{(PIR\ Sensor\ HC-SR501)} = \frac{P_{(PIR\ Sensor\ HC-SR501)} \times 24 \times 365}{1000}$$

$$E_{(PIR\ Sensor\ HC-SR501)} = 2.85kWh/year$$

Now, here got the total energy used for 7 locks annually:

$$E_{(Total)} = (E_{(Lock)} + E_{(Reader\ scanning)} + E_{(Reader\ standby)} + E_{(Arduino\ MEGA)} + E_{(PIR\ Sensor\ HC-SR501)}) \times 7$$

$$E_{(Total)} = 222.18kWh/year$$

The total locks energy used for general access control system annually:

Since $E_{(Lock\ for\ general\ system)} = 52.56kWh/year$

$$E_{(Total\ for\ general\ system)} = E_{(Lock\ for\ general\ system)} \times 7$$

$$E_{(Total\ for\ general\ system)} = 367.92kWh/year$$

Compare with the general access control system, our scheme is able to save 39.6% energy used, 140.7kWh/year.

$$Percentage\ of\ energy\ saving = 1 - \frac{E_{(Total)}}{E_{(Total\ for\ general\ system)}} \times 100\% \qquad \text{------(4.4)}$$

$$Percentage\ of\ energy\ saving = 39.6\%$$

According to the data from Taiwan Bureau of Energy, Ministry of Economic Affairs, for each kWh can emit 0.636kg CO_2, it's mean it can reduce 92.82kg CO_2 per year if use our system. To a greater or lesser degree, it is an ecofriendly access control system.

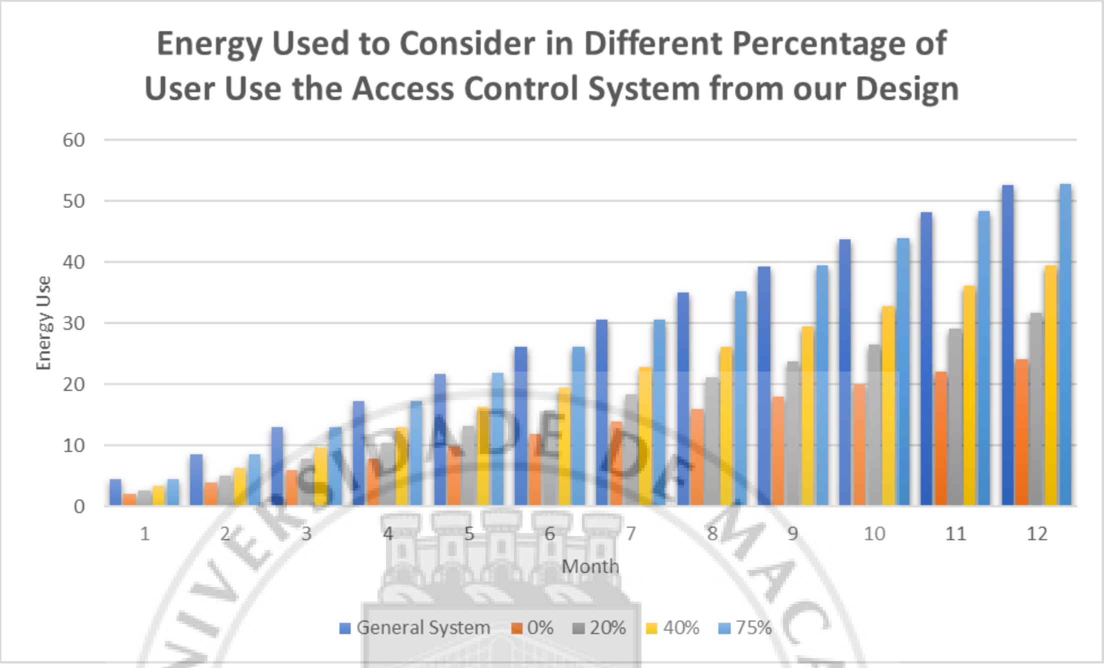


Fig 4.6 Energy Used to Consider in Different Percentage of User Use the Access Control System from our Design

From the figure above can see if no body use the area but still need access control system, it can save 54.2% energy which is the maximum value. One more need to be attention, when the percentage of use reach 75%, there will have same energy used between general system and our design system. Therefore, our access control system for energy saving is suitable for small to intermediate level use times environment.

CHAPTER 5

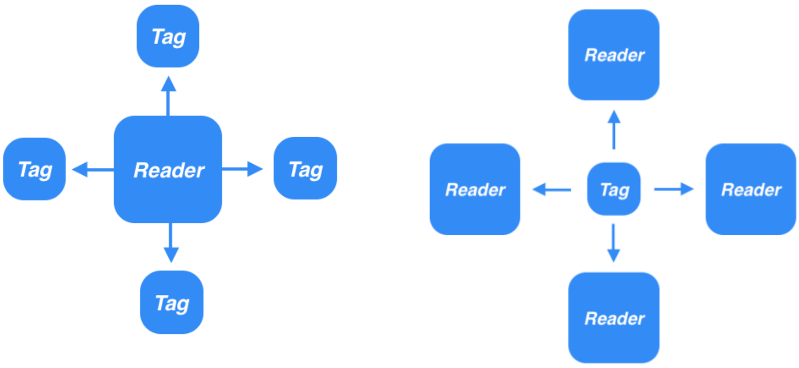
BRIEF RESEARCH AND EXPERIMENT FOR RFID INDOOR POSITIONING

5.1 Extensional Function of UHF RFID Access Control System

UHF technology used in access control systems, in addition to convenience, it has potential to extend another feature, such as indoor resources intelligent response. Imagine that when user walk approach to the public printer, the printer can identify that who are using now and show your documents the user want to print out. Another situation can imagine, when the user walk in certain area, the UHF RFID signal will communicate with the user tag, in addition to verify the security, it also is able to send some information to user's personal device to describe the location about. To deal with the above problems, it has a key problem which the system need to know the user position that to response right information to the user. Hence, we need to discuss about how to implement the indoor positioning feature base on UHF RFID.

5.2 Literature Review of RFID indoor positioning

RFID-based indoor positioning can be divided into two categories: fixed-tag positioning and fixed- reader/antenna positioning, according different roles of tags and readers/antennas (See Fig 5.1). In a fixed-tag scheme, the tags are dispose on the ceiling or floor with some rules, and the reader / antenna is usually connected to the moving object. This is cost effective when the object to be tracked is large, the number is small, and it is usually moved on a 2D plane or on a path. In the fixed-reader/antenna scheme, the readers/antennas and tags are placed in an opposite way to the fixed-tag scheme. The readers/antennas are installed at fixed positions while the tags are attached to the items to be tracked. It is useful for most applications where a lot of items need to be located and tracked at the same time since the tags are much cheaper and smaller than the readers/antennas. [23] We will base on this scheme for our indoor positioning.



(a) Fixed-tag scheme (b) Fixed-reader scheme

Fig 5.1 Two common RFID Indoor positioning schemes

The algorithms of RFID indoor positioning, here have serval ways to obtained such as Received Signal Strength Indication (RSSI), Angle of Arrival (AOA), Time of Arrival (TOA), Time Difference of Arrival (TDOA), or Adaptive Power Multilateration (APM). [24] Received Signal Strength Indication (RSSI) is the most common using for RFID positioning, RSSI is a measurement of the power from a received radio signal to identify the position of objects with passive tags. The position of an object can be determined accurately if through the relationship between the distance and the signal strengths. [25] Some of the researcher will combine Time of Arrival (TOA) another algorithm to increase accuracy of the positioning. [26]. In addition, some system uses a Particle Filter to combine RSSI data and image data to improve RFID and camera localization accuracy. [27] To combine other algorithm is because RSSI is complex in an indoor environment because furniture, equipment windows and doors can affect the signal performance, which may cause multipath propagation, such as reflection, refraction and diffraction. [26]

In our research scheme, we would like to discuss and verify about the relationship between the distance and RSSI, to investigate whether RSSI is reliable and feasible to be used for indoor positioning.

5.3 Experiment Setup

We decided to use single antenna to measure about the relationship between the RSSI and distance, S9028PC was chosen as the UHF antenna, the detail of model can refer to Table 5.1. The experiment choses corridor outside the laboratory for the measurement site (See Fig 5.2). The maximum distance set to 4.5m, and take measure in every half meter (See Fig 5.3), the RFID tag stick to the mobile stand face to the antenna center horizontally.

Specifications

Frequency MHz:	902 ~ 928
Gain dBic:	9.0 Nominal
VSWR:	1.5:1 Nominal
Beam width:	60^{O}
Polarization:	Circular (L) left (R) right
Antenna Weight lb. (kg):	2.3(1.04)
Power watts:	10
Mounting:	2 threaded studs (rack mount)
Dimensions, in(cm):	10×10×1.5(25.4×25.4×3.8)

Table 5.1 The Specification of UHF Antenna S9028PC

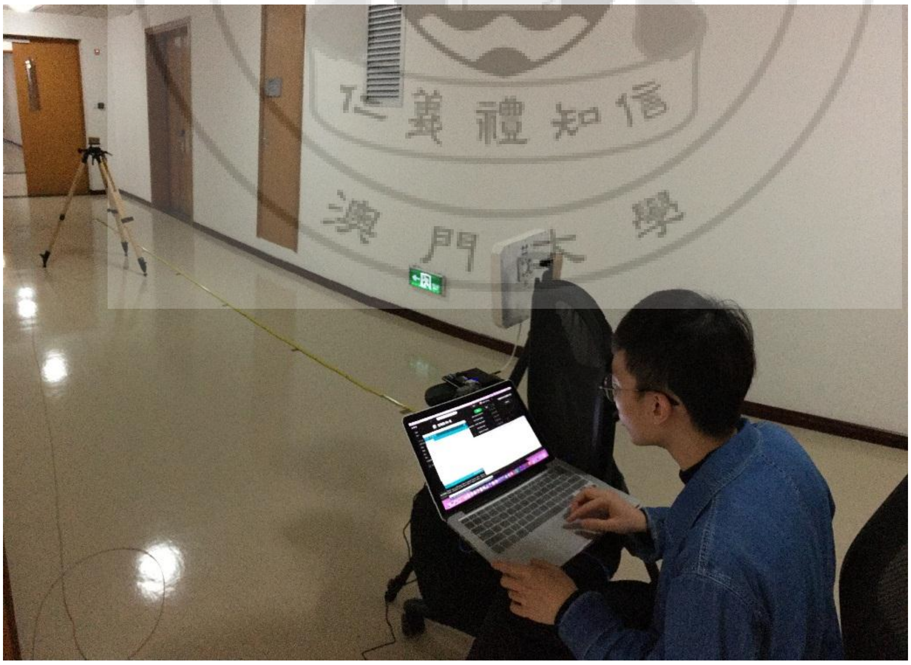


Fig 5.2 The Actual Scene for Indoor Positioning Measurement

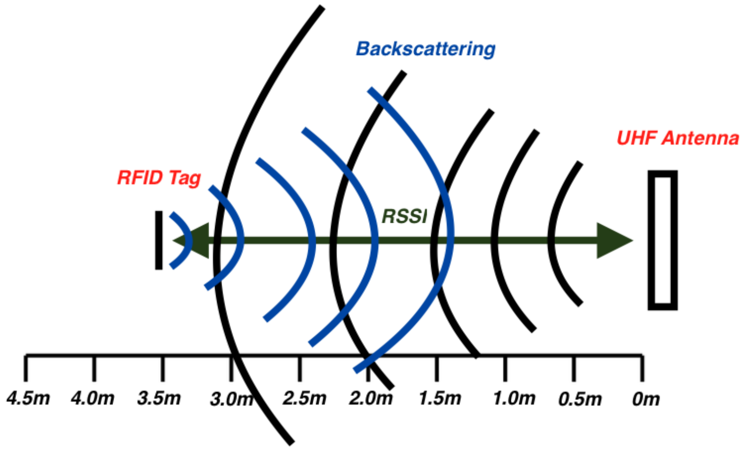


Fig 5. 3 The Measurement Method in the Experiment

Each distance will take three set of measurements, each set contain a hundred RSSI data. Take average for each set RSSI data then plot to the chart. Taking average can make the result more accuracy.

5.4 Measurement Result

A part of the distance in 3.5 cannot get the result during the measurement, it may due to the multipath propagation in indoor, hence we have no data when distance is 3.5m (See Fig 5.4), and Fig 5.5 shown the curve which using the average values from the measurement result, the dotted line is the trendline line plotted according to the result.

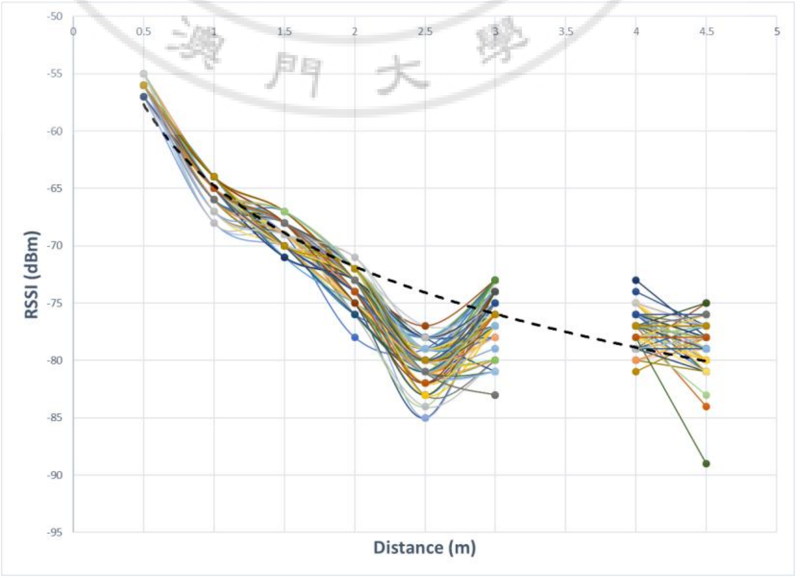


Fig 5.4 The RSSI result which have taken a hundred of measurement

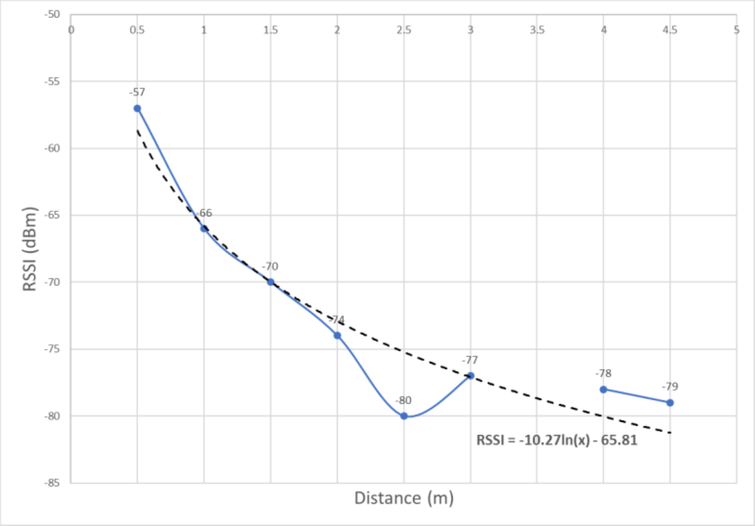


Fig 5.5 The Relationship between RSSI and Distance from measurement

5.5 Discussion and Analysis for Propagation Model

The relationship between RSSI and the distance is specified as the following equation. [28]

$$\mathrm{RSSI} = -(10\times\mathrm{n})\log_{10} d - A \text{-----------------------------(5.1)}$$

RSSI denotes the radio signal strength indicator in unit of dBm, n is the signal propagation constant or exponent, d is the relative distance between the reader and the tag, and A is a reference received signal strength in dBm at 1m distance. Assume n is equal to 2.35.

In Fig 5.6, the measured RSSI is shown along with the calculated RSSI. Note that there is a non-monotonicity in the curve around 2.5m. To approximate the RSSI using the distance to the reader, the following logarithmic equation was derived by curve fitting.

$$\mathrm{RSSI} = -10.27\ln d - 65.81 \text{--------------------------(5.2)}$$

As can be observed in Fig 5.6, the asymptotic line of the measurement is very analogous to the reference curve. Substituting a series of distance into equation 5.1 and 5.2 for quantitative analysis, the average error is 0.20% as shown in Table 5.2. Therefore, RSSI ranging with a single antenna is somewhat reliable in a simplified environment despite the occurrence of multi-path fading.

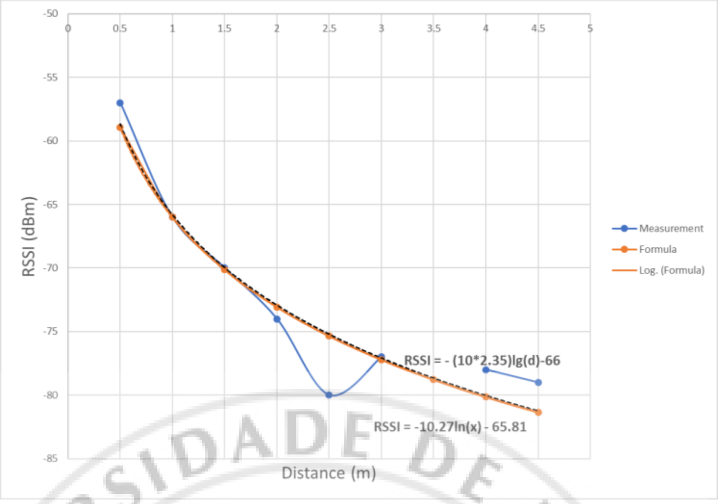


Fig 5.6 The trend line of the measurement along with the reference

Distance (m)	Reference (dBm)	Trend Line (dBm)	% Error
0.5	-58.9257951	-58.69137846	-0.40%
1	-66	-65.81	-0.29%
1.5	-70.13814459	-69.97412666	-0.23%
2	-73.0742049	-72.92862154	-0.20%
2.5	-75.3515902	-75.22030582	-0.17%
3	-77.21234949	-77.0927482	-0.15%
3.5	-78.78559904	-78.67587569	-0.14%
4	-80.1484098	-80.04724309	-0.13%
4.5	-81.35049407	-81.25687486	-0.12%

Table 5.2 Comparison of the result from reference and the equation of the trend line

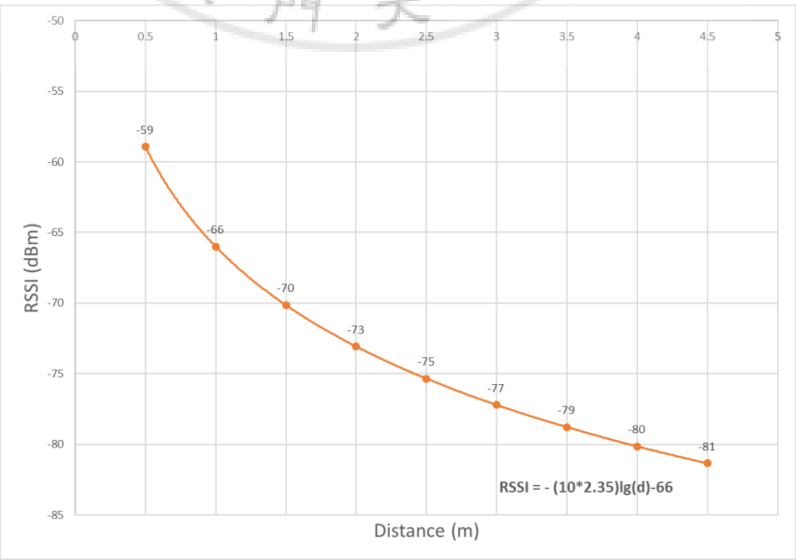


Fig 5.7 The reference curve

By aligning two antennas facing each other, the accuracy of the RSSI ranging can be improved. The following figure is the result of rough simulation in this configuration from substituting value into the equation. When the tag is close to antenna A, the RSSI reported by antenna A is higher than by antenna B and vice versa.

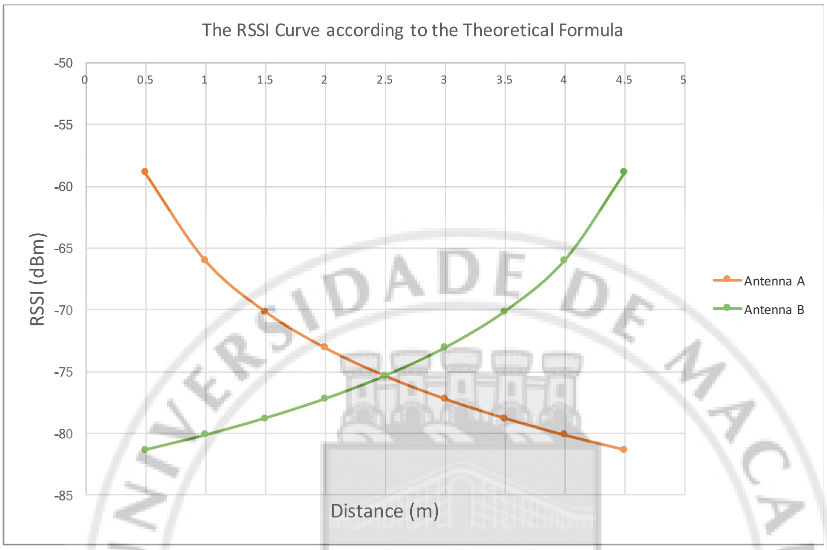


Fig 5.8 The reference curve of the simulation

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

In last semester, a verification system of our proposed idea is basically built. To select the suitable candidate for the hardware mainly the sensor, a series of testing had been conducted. In this semester, a complete system integrating with the RFID reader, Arduino, the electromagnetic lock and the PIR sensor is achieved. The operating frequency of the system is around 902MHz to 928MHz. By hacking of the PIR sensor, the recovery time of the system is decreased from 5.5s to less than 0.2s, which effectively addresses the issue of security.

In contrast to the traditional electromagnetic door lock, the power consumption falls sharply without the sacrifice of the security since the system can consciously decide when to lock the door. This means a huge amount of energy as far as 50%, according to our evaluation in 4.5, can be conserved during light stream of visitors.

Moreover, the system can be furthered to execute some simple indoor tracking with the aid of the RSSI. A mathematical model with respect to the relationship between RSSI and distance at the scene of corridor is constructed. Referring to the most popular equation 5.1, the average error is 0.20%.

6.2 Future Work

In the future, the system is expected to connect with the online database so that the Arduino can look up for authorization productively. Also, the activation or deactivation of the tag can be easily carried out if the system is in real time. Regarding the indoor tracking, the accuracy with a single antenna is not enough. It has a room for improvement in it. The placement or the number of the antenna may affect the outcome of the indoor positioning.

REFERENCE

[1] L. K. Sun, "Understanding Dublin Weather Radar - Basic Principles and Performance," 2016. [Online]. Available: http://www.aeromet.org.tw/chinese/aeromet/aw002/02_03.pdf.

[2] H. Stockman, "Communication by Means of Reflected Power," *Proc. of the IRE,* no. 36, pp. 1196-1204, 10 1948.

[3] Sharmar, "Infrared sensors," 16 5 2014. [Online]. Available: https://metropolia.fi/display/sensor/Infrared+sensors.

[4] A. Sense, "MSAN-001 X-Band Microwave Motion Sensor Module Application Note," 2016. [Online]. Available: http://www.limpkin.fr/public/HB100/HB100_Microwave_Sensor_Application_Note.pdf.

[5] D. P. Sanghera, RFID+ Study Guide and Practice Exam, Syngress Publishing, Inc., 2007.

[6] REN21, "Renewables 2016 Global Status Report," 2016. [Online]. Available: http://www.ren21.net/wp-content/uploads/2016/10/REN21_GSR2016_FullReport_en_11.pdf.

[7] Nedap, "UHF IS AN ENHANCEMENT FOR ACCESS CONTROL," [Online]. Available: http://www.nedapidentification.com/news/insights/uhf-is-an-enhancement-for-access-control.html.

[8] B. Manish and M. Shahram, RFID Field Guide: Deploying Radio Frequency Identification Systems, Prentice Hall PTR, 2005.

[9] T. LEXTRAIT, "Arduino: Power Consumption Compared," 22 5 2016. [Online]. Available: https://tlextrait.svbtle.com/arduino-power-consumption-compared.

[10] S. Lahiri, RFID Sourcebook, New Jersey: Prentice Hall PTR, 2005.

[11] P. Jain, "Infrared Sensors or IR Sensors," 2012. [Online]. Available: https://www.engineersgarage.com/articles/infrared-sensors.

[12] B. Glover and H. Bhatt, RFID Essentials, O'Reilly, 2006.

[13] Frank, "Control Principle and Application of Infrared Human Body Sensor," 2016. [Online]. Available: http://www.seraphim.com.tw/upfiles/c_supports01326073876.pdf.

[14] K. Finkenzeller, RFID Handbook: Fundamentals and Application in Contactless Smart Cards and Identification, John Wiley and Sons Inc., 2003.

[15] P. H. Cole, B. Jamali and D. Ranasinghe, "Coupling relations in RFID systems," *Auto-ID Center white paper,* 2003.

[16] J. Bird, "How carbon causes global warming," 19 7 2005. [Online]. Available: https://www.theguardian.com/science/2005/jun/19/observerfocus.climatechange.

[17] A. I. I. S. a. X. ADT/Tyco Fire & Security, "RFID and UHF: A Prescription for RFID Success in the Pharmaceutical Industry," [Online]. Available: http://www.alientechnology.com/wp-content/uploads/Whitepaper-RFID-and-UHF-A-Prescription-for-RFID-Success-In-Pharmaceutical-Industry.pdf.

[18] L. Ada, "How PIRs Work," 28 1 2014. [Online]. Available: https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor/how-pirs-work.

[19] "LT1006 Precision, Single Supply Op Amp," 2016. [Online]. Available: http://cds.linear.com/docs/en/datasheet/1006fa.pdf.

[20] "HC-SR501 PIR MOTION DETECTOR," 2017. [Online]. Available: https://www.mpja.com/download/31227sc.pdf.

[21] "HC-SR501 PIR MOTION DETECTOR," 2016. [Online]. Available: https://www.mpja.com/download/31227sc.pdf.

[22] "Arduino HC-SR501 Motion Sensor Tutorial," 2016. [Online]. Available: http://henrysbench.capnfatz.com/henrys-bench/arduino-sensors-and-input/arduino-hc-sr501-

motion-sensor-tutorial/.

[23] J. Wu, " Tree-Dimensional Indoor RFID Localization System," 2012.

[24] Y. T. M. A.-R. A. A.-D. a. Y. J. Wenhuan Chi, "A Revised Received Signal Strength Based Localization for Healthcare," 2015.

[25] S. K. A. H. T. a. G. T. H. S.L. Ting, "The Study on Using Passive RFID Tags for Indoor Positioning," 2011.

[26] R. F. G. A. R. S. J. J. P. Z. S. T. R. H. Murofushi, "Indoor Positioning System Based on the RSSI using Passive Tags," 2016.

[27] P. ,. Ms.Aarti Vaidya, "POSITION LOCATION METHODOLOGY BASED ON RSSI USING RFID," 2014.

[28] D. Qian and W. Dargie, "Evaluation of the Reliability of RSSI for Indoor Localization," 2012.

[29] A. Zavvari, "Critical Evaluation of RFID Security Protocols," Malaysia, 2012.

FIGURES REFERENCE

[1] http://www.cxjrfidfactory.com/wp-content/uploads/2016/08/6.jpg

[2] A. Zavvari, "Critical Evaluation of RFID Security Protocols," Malaysia, 2012.

[3] https://www.cisper.nl/resources/faqs/

[4] http://hyperphysics.phy-astr.gsu.edu/hbase/phyopt/polclas.html

[5] https://www.omicron-lab.com/bode-100/application-notes-know-how/application-notes/rfid-resonance-frequency-measurement.html

[6] http://www.nedapidentification.com/news/insights/uhf-is-an-enhancement-for-access-control.html

[7] https://surrealsciencestuff.wordpress.com/tag/doppler-effect/

[8] http://hyperphysics.phy-astr.gsu.edu/hbase/Sound/dopp.html

[9] http://thiwell.en.seekic.com/product/integrated_circuits_ics/HB100.html

[10] http://www.electronics-tutorials.ws/filter/filter_5.html

[11] https://electrosome.com/opamp/

[12] http://www.datasheetcafe.com/lt1006-datasheet-pdf/

[13] https://www.mpja.com/download/31227sc.pdf

[14] http://henrysbench.capnfatz.com/henrys-bench/arduino-sensors-and-input/arduino-hc-sr501-motion-sensor-tutorial/

[15] https://www.insidegadgets.com/2012/11/10/alarm-system-modification-part-5-modifying-the-pir-sensor/

[16] http://www.waveshare.net/shop/sp3232e-price.htm

[17] https://dir.indiamart.com/delhi/bolt-lock.html

APPENDIX A

Arduino code

```
bool execute = true;
volatile bool cardPresent;
byte receivedMessage[70];
volatile int lengthOfMessage;
volatile int interruptState;
const int sensorPin = 2;
const int ledPin = 11;

void setup() {
  Serial.begin(9600);
  Serial2.begin(115200);
  pinMode(ledPin, OUTPUT);

  attachInterrupt(digitalPinToInterrupt(sensorPin), sensorStateChange,
CHANGE);
}

// interrupt service routine that wraps a user defined function
void sensorStateChange() {
  if (digitalRead(sensorPin) == 1) {
    digitalWrite(ledPin, HIGH);
  }

  cardPresent = true;

  if (digitalRead(sensorPin) == 0) {
    cardPresent = false;
    digitalWrite(ledPin, LOW);
  }
}

void getTag() {
  byte invetoryRealTime[] = {0xA0, 0x04, 0xFE, 0x89, 0x01, 0xD4};
  Serial2.write(invetoryRealTime, sizeof(invetoryRealTime));
}

void saveTag() {
  lengthOfMessage = 0;

  while (Serial2.available()) {
    receivedMessage[lengthOfMessage] = Serial2.read();
    lengthOfMessage++;
  }

  for (int i = 0; i < lengthOfMessage; i++) {
    if (receivedMessage[i] == 0xA0) {
      Serial.println();
    }
    Serial.print(receivedMessage[i], HEX);
    Serial.print(" ");
  }
}


void loop() {
  while (cardPresent == true) {
    if (digitalRead(sensorPin) == 1) { //if somebody comes up
      getTag(); //send command to the RFID reader
      saveTag(); //obtain the data packet
      if (receivedMessage[18] == 0x48 || receivedMessage[36] == 0x48
|| receivedMessage[54] == 0x48) {
        digitalWrite(ledPin, LOW);

      }
      memset(receivedMessage, 0, sizeof(receivedMessage));
      delay(100);// added by Hinnes
    }
  }

  Serial.println();
  Serial.print("Sensor off");
  Serial.println();
  delay(1000);
}
```