A Control Method to Reduce Interferences and Collisions between Multiple RFID Tags and RFID Readers

By

TAY ZAR ZAW WIN

FINAL PROJECT REPORT

Submitted to the Electrical & Electronics Engineering Programme
in Partial Fulfillment of the Requirements
for the Degree
Bachelor of Engineering (Hons)
(Electrical & Electronics Engineering)

Universiti Teknologi Petronas

Bandar Seri Iskandar

31750 Tronoh

Perak Darul Ridzuan

© Copyright 2011

by

Tay Zar Zaw Win, 2011

CERTIFICATION OF APPROVAL

A Control Method to Reduce Interferences and Collisions between Multiple RFID Tags and RFID Readers

by

Tay Zar Zaw Win

A project dissertation submitted to the
Electrical & Electronics Engineering Programme
Universiti Teknologi PETRONAS
in partial fulfilment of the requirement for the
Bachelor of Engineering (Hons)
(Electrical & Electronics Engineering)

Approved:

____

Dr Mohamad Naufal Bin Mohamad Saad

Project Supervisor

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

May 2011

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

Tay Zar Zaw Win

ABSTRACT

Radio frequency identification technology (RFID) is one of the fastest developing technologies today. Although it has significant performance in use of Auto-ID applications, the presence of multiple tags in a RFID system can lead to interferences between each tags which is called Collision. There are many method to overcome this issue and this project introduces the use of DS-CDMA technique to overcome this issue. The Simulink simulation environment is used to simulate the use of DS-CDMA in RFID system. The results obtained clearly show the concept of this method is leading to a solution for RFID collision issues. However, the further improvement in simulations and concept of the method is most recommended in future project work.

ACKNOWLEDGEMENT

I would like to express my special gratitude to my project supervisor A.P Dr Mohamad Naufal Bin Mohamad Saad for giving the opportunity to learn and carrying out this project works. The guidance and motivation given are most appreciated. I would also like to express my gratitude to UTP FYP Coordinators and management team for all the support and helps provided throughout this project.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1. BACKGROUND OF STUDY

Radio Frequency Identification (RFID) is defined as any method of identifying unique items using radio waves. Typically, a reader (also called an interrogator) communicates with a transponder, which holds digital information in a microchip. But there are chipless forms of RFID tags that use material to reflect back a portion of the radio waves beamed at them [1]. An RFID system usually has an Interrogator (Reader), Tag and the Controller (Middleware). The tag stores and carries a unique data to be identified by the reader. RFID technology doesn't need a Line of Sight communication between the Reader and the Tag.

The technology is currently applied in many countries in the world in many applications such as, libraries, transportation, supply chain management, animal tracking, electronic passports and many other identification applications. Because of its contactless and none line-of-sight ability, the RFID systems are very convenient for the users thus the technology is being developed for better and more advanced features.

1.1 Radio Frequency Identification Technology

A typical RFID system consists of three main components which are Reader, Tag and Controller. The Reader's function is to send out the radio waves and to receive the signals transmitted by the Tag. A typical RFID Reader has both receiver and transmitter. The size and functions of a RFID reader is varied according to the RFID system, there are handheld RFID readers as well as standing RFID readers that can be found in most of the convenient stores and supermarkets. The controller or middleware is to store the data received by the RFID reader and to process the received data as necessary. The Tag's function is to carry the stored data and to send out to the reader. The types of tags can be grouped into three main groups, Active, Semi Passive and Passive Tags. Semi Passive tags are somewhere in between Active and Passive Tags therefore in this paper, only the Active and Passive tags are going to be considered regarding the RFID tag types.

1.1.1 Passive Tags

This type of tag doesn't have any power source onboard and it needs power from the reader and thus the cost of this type of tags is usually very low. The power from the reader is transmitted to the tag by means of electromagnetic radiation such as inductive coupling for near-field radiation and back scattering for far-field radiation [2]. In passive tags, when a passive tag is in an area of a reader's electromagnetic waves, the electromagnetic waves from the reader induces current in the tag and the tag draws power from that current and transmit the stored data to the reader via radio waves through the antenna. Passive tags need to be in the nearest distance from the reader to be able to communicate with the reader.

1.1.2 Active Tags

An onboard power source is present on the tag thus it costs more than the passive tags. The active tags can transmit much longer transmit range than passive tags. Active tags have limited life time because the tag uses the onboard battery for the power source. An active tag transmits stored data on a regularly scheduled rate which is called beacon rate [1]. The tag can be configured to have any beacon rate from seconds to several minutes, the shorter the rate is the more power it will consume thus it may have the shorter life time. Active tags are used in systems such as inventory tracking of a factory or organizations, museums, mostly on systems which need RTLS (Real Time Locating System) for the status of the tags all the time while passive tags are only read at times when it is needed.

1.2 Problem Statement

In a RFID system, if there are many tags being present in a reader zone, the reader is confused by the signals transmitted at a same time by the tags. Similarly, when more than one reader read the signal from a single tag, the tag gets confused and undesired results come out in the system. When the reader initiates communication without any knowledge of the tag identification numbers (IDs), all the tags in the operating area begin the transmission at the same time. The radio signals emitted from different sources will mutually interfere, causing disturbances in the receiver which result in information losses. This interference between tags and readers themselves is called "Collision" [3]. The collisions in the RFID systems limits its usages to a certain level, such as a reader cannot read certain amount tags at an instance, taking longer time for the users. A successful anti-collision method can eliminate these limits from the RFID technology and in other words RFID systems which need to read the multiple tags at an instance need an efficient RFID anti-collision protocol. An anti-collision protocol is a general term used to cover methods of preventing radio waves from one device from interfering with radio waves from another. Anti-collision algorithms are also used to read more than one tag in the same reader's field [1].

1.3 Objective and Scope of Study

1.3.1 Objective of the Project

The objective of this project is to study the one of the latest and efficient technology, RFID, and to study its fundamental theories and working principles. The project also studies in detail of RFID Anti-Collision Protocols of those which are already approved and using and of those which are proposed theoretically. After those objectives are carried out, this project approached to develop a new Anti-Collision Protocol using the gained knowledge from earlier objectives. Therefore, the objectives of this project are

- To study the RFID technology fundamentals and its working principles.
- To study the RFID anti-collision protocols in detail
- To approach in developing of a RFID Anti-Collision Protocol.

1.3.2 Scope of Study

The development of the anti-collision protocol requires research based activities and simulation of the proposed protocols. This may include

- Detail study on the existing RFID technologies and systems
- Thorough study on the existing anti-collision protocols
- Simulation of the proposed protocol using software
- Analysis of the results from the simulation

The simulations for the studies of this project are done in MATLab and Simulink simulation environment. This project is relevant to the Communication Systems studies especially on the radio frequency technologies, electromagnetic theories and microwave communication theories. The latest technology of the RFID and its usages will be studied from various information sources especially from IEEE research papers and journals. The new anti-collision protocol is approached to be developed based on the existing protocols. Mathematical proofs and simulation results will be obtained to show the effectiveness and efficiency of the new protocol.

CHAPTER 2

LITERATURE REVIEW

2. ANTI-COLLISION PROTOCOLS FOR RFID

In this chapter, the related studies done on the anti-collision protocols and methods in developing the new protocol are mentioned and discussed.

2.1 Electromagnetic Waves

RFID technology is a latest technology which uses the properties of electromagnetic properties effectively. Electromagnetic waves are actually a radiation that has a form of self-propagating waves that can travel in vacuum or matter. The electromagnetic waves are such as, light, microwave, x-rays are all kinds of electromagnetic waves. Since they are called wave, they have the frequency and wavelength. The large amount of the variation of frequencies of the electromagnetic waves creates many types of electromagnetic waves. The wavelengths of the electromagnetic waves are varied from the size of a very tall building to the size of a smallest atom. The waves with longer wavelengths are rather safe while the short wavelength waves such as x-rays and shorter waves are extremely dangerous for living creatures.

The electromagnetic wave carries energy and momentum. Every object on the earth which has the electric charges can create electrostatic potential, inversely proportional to the distance (inverse square law). Since electrical charges have positive and negative which are opposite and attracted to each other, most of the time, the electric charges are cancelled each other. However, there are cases of the cancellation failures, which is the reason of radiations being present. The electromagnetic waves are utilized efficiently in communication purposes, such as radio, satellite, mobile phones, wireless and many more applications such as RFID.

The figure below shows the electromagnetic spectrum, classification of the waves, frequency of the waves and wavelength of the waves.

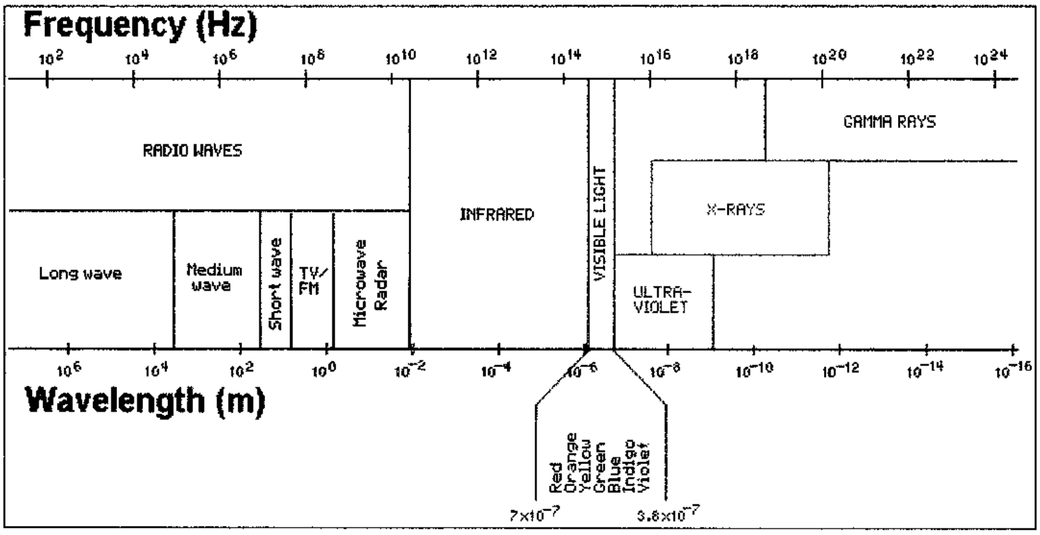


Figure.1 Electromagnetic Wave Spectrum

These electromagnetic waves can be created (such as radio waves) and efficiently utilize to carry data and information on these waves. RFID technology makes the auto identification to objects by use of electromagnetic waves to send the signals and energy. Time dependent signal voltage is usually written as the product of amplitude and periodic functions like sine or cosine [4].

$$V(t) = v_0 \cos(\omega t) \qquad (1)$$

A continuous signal has components such as frequency, phase and amplitude. In order to carry information, a continuous signal needs to be changed its frequency, phase or amplitude time to time. Thus, a signal without varying these values doesn't carry any information. Thus, information is carried by these waves by means of the change in "Frequency", "Amplitude" and "Phase" as in Frequency Modulation (FM), Amplitude Modulation (AM) and Phase Shift Keying (PSK) modulation schemes. Modulation can be written mathematically as

$$V(t) = m(t) \, . \cos(\omega_c t) \qquad (2)$$

The above equation (2) shows that, m(t) is the information data and the cosine function is the carrier frequency. Sometimes the information data is another sine or cosine function with much more lower frequency than carrier frequencies, we use trigonometric identities to rewrite the equation. For example

$$V(t) = \cos(\omega_m t) \cdot \cos(\omega_c t) \quad \{\omega_m \ll \omega_c\} \tag{3}$$

$$V(t) = \tfrac{1}{2}\{\cos([\omega_c + \omega_m]t) + \cos([\omega_c - \omega_m]t)\} \tag{4}$$

Thus, as we can see, the two sidebands are created by the modulation which carries the information data. When a signal is modulated, the resulting frequency spectrum becomes wider [4].

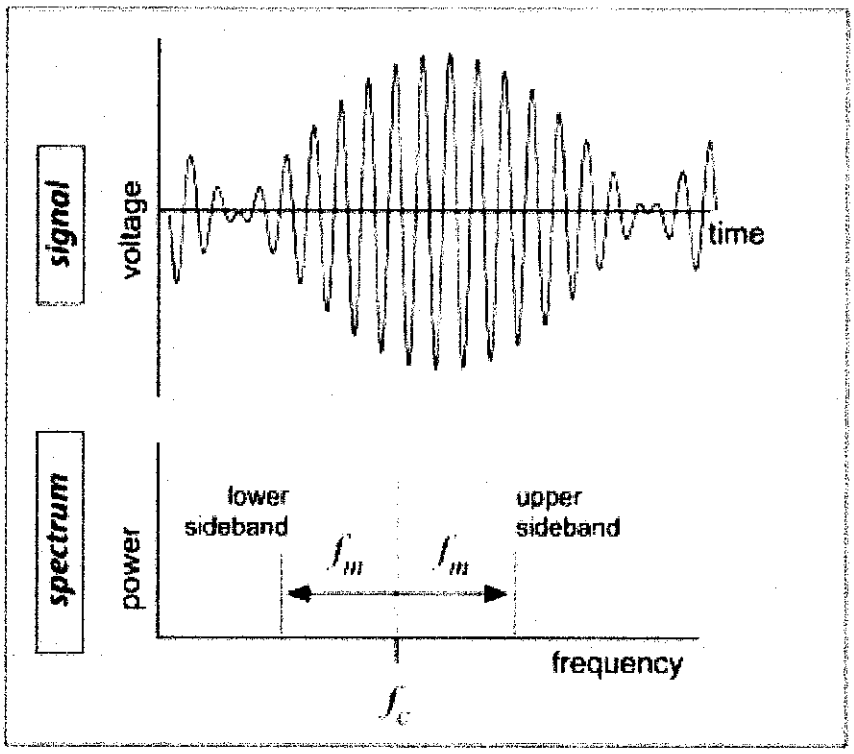


Figure.2 Signal in Time Domain and Frequency Domain

2.2 Collisions in RFID Systems

RFID is considered as one of the most reliable and advanced Auto Identification technologies however there are collisions issues in RFID systems. Since the usage of RFID tags and readers are increasing and the number of tags and readers in a RFID system are increasing. Thus, when a reader sends out a wake up signal, there are many tags replying to the reader simultaneously. This makes the reader confused between the signals or the signals from tags are interfere against each other which make the reader impossible to detect all of the signals to receive at that time. This is called collision. Figure.3, shows the multi tags sending out the signal to a single reader, that may result in the reader misses signals from certain tags.

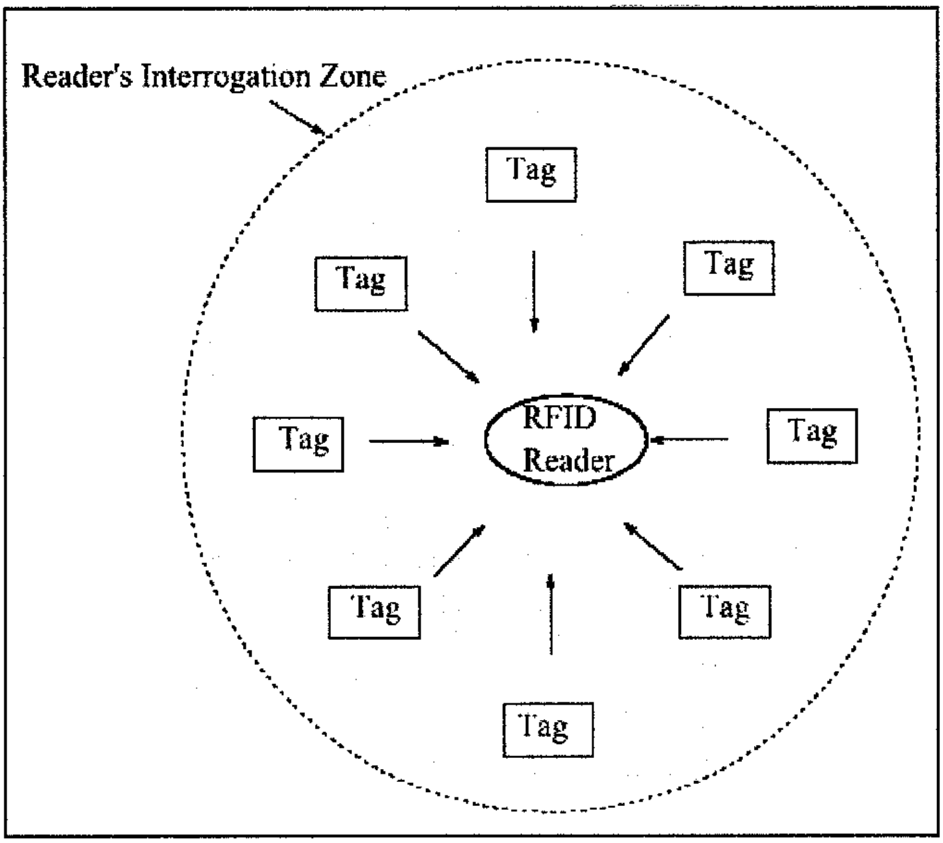


Figure.3. Multi-tags transmitting signals to a single Reader

2.3 Anti-Collision Protocols and Methods

There are many different ways of solving the multi-tags collisions or multi-reader collisions problem in RFID systems. Most of the methods and protocol, the Time Division Multiple Access (TDMA) method is the most common one. This TDMA method includes ALOHA [1] and its variances and Tree Based Protocols such as Binary Tree. ALOHA protocols are based on listening the collision after transmission. A tag sends out a signal and it'll wait for acknowledgement from the reader, if the tag doesn't get the acknowledgement from the reader, there's a collision with other signals transmitted from other tags. Then the tag will transmit the signal again. Binary Tree based protocols can be considered as RTF (Reader Talks First) protocols. The reader will acknowledge certain tags in order of which will be sending signals first. The reader will repeat this process again and again until there's no tag which hasn't sent out the signal. Thus Binary Tree based protocols need more energy and time. The overall methods for anti-collision in RFID systems are shown on Figure.4.

There are several RFID standards including International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Ubiquitous ID (UID) from Japan and Electronic Product Code (EPC) or EPCglobal mainly used in Europe. Among all these standards, ISO/IEC 18000 and EPC are the most widely used standard in RFID applications. In year 2006, the ultrahigh frequency standard which is proposed by EPCglobal is accepted as ISO/IEC 18000-6C regulation. RFID technology can be used in various frequency channels. These protocols have different multi-tag anti-collision algorithms as listed in Table.1 [5].

Table.1. Anti-collision Algorithms in ISO Protocol

Protocol	Frequency	Anti-Collision
ISO/IEC 18000-2	<135kHz	Query Tree
ISO/IEC 18000-3	13.56MHz	Query Tree, Pure ALOHA, Flame slotted ALOHA
ISO/IEC 18000-4	2.45GHz	Adaptive Binary Tree
ISO/IEC 18000-6	860-960MHz	Flame slotted ALOHA (type A/C), Adaptive Binary Tree (type B)
ISO/IEC 18000-7	433MHz	Flame slotted ALOHA

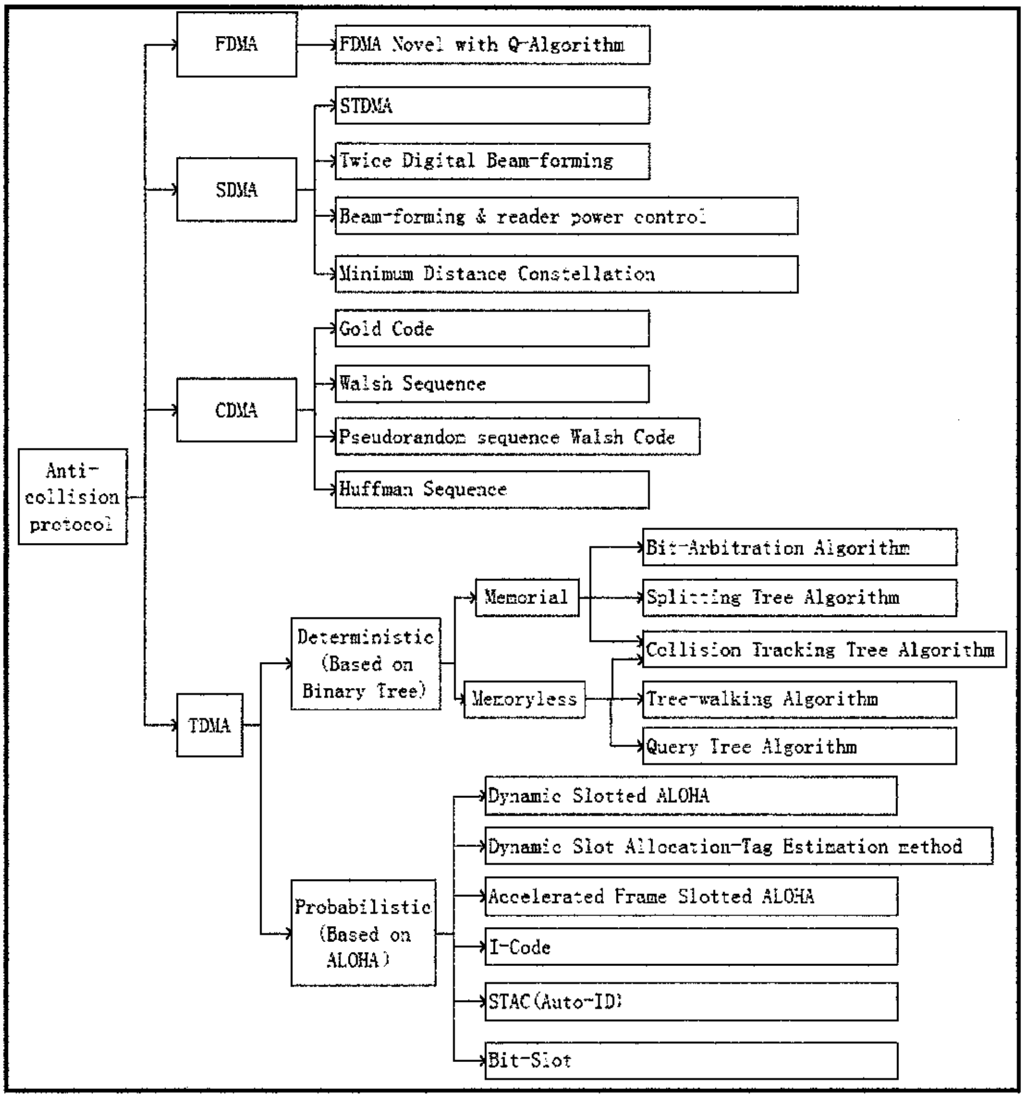


Figure.4. Anti-Collision Methods in RFID System

2.3.1 ALOHA Protocol

If there are several tags in a reader zone, the reader transmits the wake up signal to the tags, and the tags will respond after a time delay to avoid communicating with the reader at the same time. The time to respond is generated randomly by each tag or it is assigned by the reader. Once the reader has received the transmitted data from the tag, the reader commands the tag to "sleep" and receives data from another tag. In this way the reader avoid getting confused by the tags.

In this protocol, the tags can choose the time slot to respond the reader's request. When collision occurs, the tags involved in the collision are read on further iterations. The iterations are made until the collision is eliminated. Compare to other protocols, the ALOHA type of protocols take less time, however there are possibilities of tags not being read at a given number of iterations by using ALOHA protocol.

The ALOHA was developed in 1970s, for a packet radio network. The basic principle is, the sender station sends out the signals when it has signals to send, then the station listen to the broadcast to find out whether a collision is present. If there is a collision detected, the station sends the signal again after a random period. This type of protocol is regarded as a simplest type of protocol because the sender just needs to listen to the collision.

Slotted ALOHA and framed slotted ALOHA protocols are the variants of the pure ALOHA protocol. In slotted ALOHA protocol, time is divided into discrete time intervals (slots) and a packet can only be sent at the beginning of a slot and because of the slots, the collision duration is reduced. Although the pure ALOHA has partial collisions, in slotted ALOHA, frames can collide or not collide at all. Theoretically, the slotted ALOHA doubles the channel utilization of pure ALOHA [6].

Framed slotted ALOHA is even more efficient than the slotted ALOHA. Certain numbers of slot are formed together as a frame, and signals are transmitted in the slots. Tags transmitted at most once in a period of a frame. Thus, only one collision per frame is possible using the framed slotted ALOHA protocol. In Figure.5, graphical illustration of a Frame-slotted ALOHA is shown.

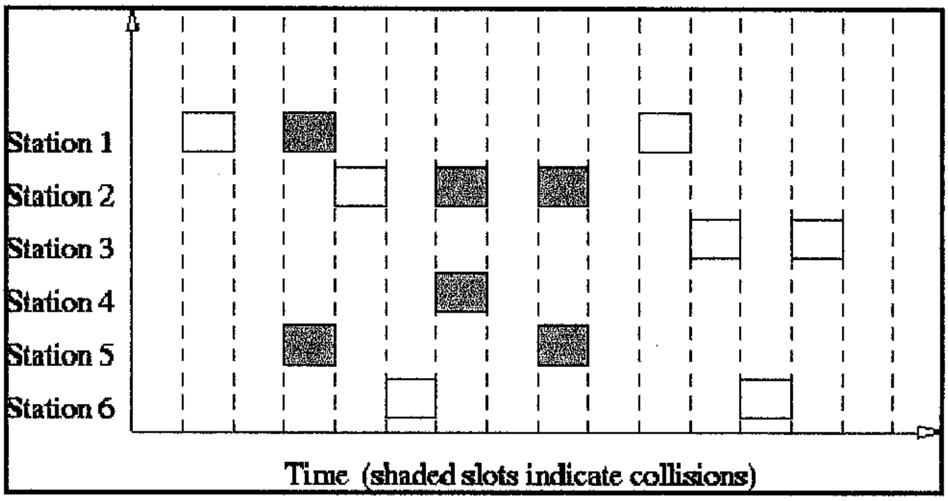


Figure.5. Graphical Illustration of slotted ALOHA

2.3.2 Binary Tree Protocol

The protocol uses EPC (electronic product code) in its method. The reader using this protocol will look for the EPC binary codes of the tag. First, the reader wakes up all the tags in the zone and asks to respond all the tags with a "1" MSB. If there is more than 1 tag that responds, the reader asks all tag with both 1 at MSB and LSB. The reader keeps asking for the tags with the binary values and finally all the tags in the zone are read without any collision.

The tree-based algorithms operate by going through the tree from top to bottom. The root of the tree is common to all the tags, and each leaf node of the tree represents a specific tag. These algorithms narrow down the tag of interest by successively muting tags that are involved in collisions. This type of protocol needs numbers of iteration to identify a given tag and the circuits required in the tag to be able to communicate with the reader is complicated. In Figure.6, the graphical illustration of a binary tree is shown.

There is a protocol which is somewhat like ALOHA called Q Protocol, when the reader sends out its wake up signal, the tags respond with a unique number. The reader then read the data from the tags according to their responded unique number one at a time. After a tag is read, the reader commands the tag to be in an alternate state where the tag will not be respond until receiving another wake up signal by the reader.

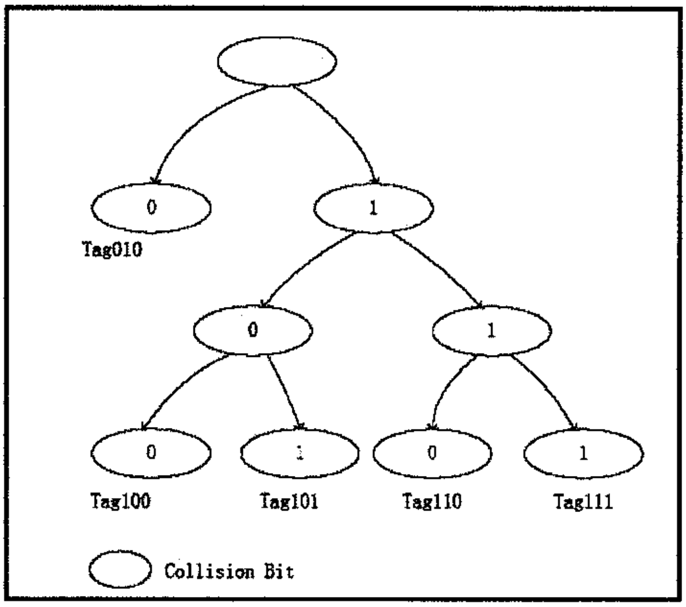


Figure.6. Binary Tree, Illustrating the collision bits

CHAPTER 3
METHODOLOGY

3. PROCEDURE IDENTIFICATION

The approach of the anti-collision method for this project is based on the studies that are done and mentioned in this report. There are several critical points that are taken into consideration while approaching for the anti-collision method. That includes the type of tag, power usage of the tag, the complexity of the tag and reader structure and the available environment of the simulation. The passive tags are usually less intelligent than active tags. The active tags have onboard battery source for the power to transmit, thus it can be implemented with more devices in the tag which provides wider field of anti-collision method. Since the limited capability of active tags is majorly depended on the battery life time of the tag, reducing the power usage of the tag is an advantage. The complexity of the anti-collision method is designed to be very low comparing to other typical anti-collisions, such as the tag will only be equipped with transmission devices and there is no need to listen any data from the reader. The simulation environment for the anti-collision method is in Matlab and Simulink environment since Matlab has the wide programming features.

The approach of the anti-collision method is based on the usage of Direct Sequence Spread Spectrum Code Division Multiple Access (DC-CDMA) [7] transmission scheme. The tag transmits the signal with spread spectrum thus reducing the interference from other noise sources in the channel and the most significant advantage is because of the DC-CDMA transmission scheme, the multi-tag collision in the RFID system is reduced because the reader is capable of receiving the signals sent from the tags and able to parallel process the signals. Due to the limited time frame, this project has only designed the detail Tag Structure of the anti-collision method.

3.1 DS-CDMA Anti-Collision Method

Code Division Multiple Access transmission scheme is widely applied in many radio networks such as Cellular Mobile Networks [8]. One of the basic concepts in data communication is the idea of allowing several transmitters to send information simultaneously over a single communication channel. This allows several users to share a band of frequencies [9].

3.1.2 Transmit Signal Structure

The Transmit Signal S_{TX} has the data stream of System Identification Data, Unique Identification Data and Cyclic Redundancy Check Bits. Each of these data are 16 bits long thus the transmit data is 48-bit long signal. The system identification data is to identify the RFID system so that the data won't be confused with other tags from other RFID systems, the CRC bits are for error detection of the transmit signals and the Unique ID of the transmit signal is to identify the tag. The transmit signal S_{TX} is to be sent out according to beacon rate T_R. The Figure.7 below shows the simplified transmit signal structure of the method.

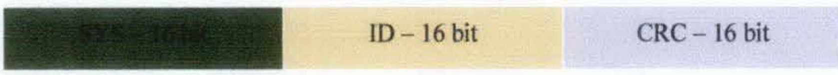


Figure.7. Transmit Signal Structure, S_{TX}

Having the ID Field as 16-bit, 2^{16} numbers of tags can be used in this system. This is more than necessary for typical Active RFID systems because Active RFID systems usually use small amount of tags. This bit sequence of the tag is spread prior to the transmission from the tag by multiplying the bipolar representation of each bit with a spreading code, such as Pseudo Noise Sequences. Spreading sequences such as Gold-sequence or maximal length sequences can also be used for spreading purpose.

3.1.3 Tag Structure

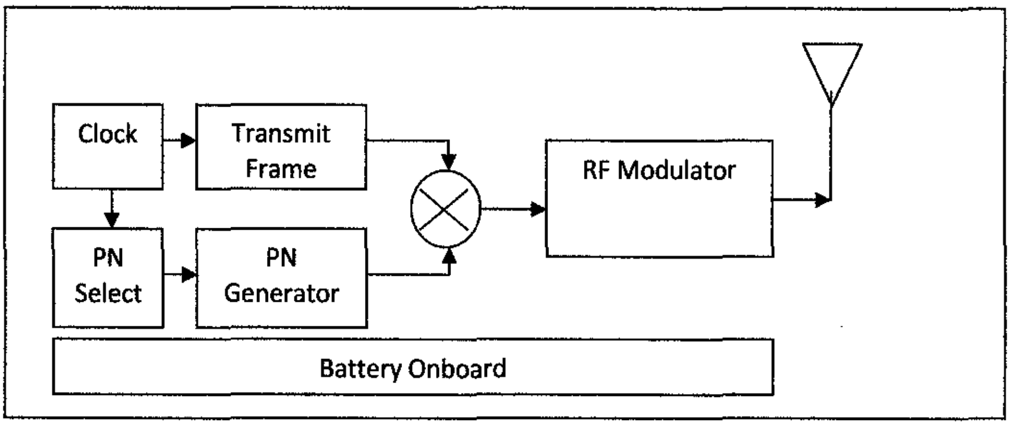


Figure.8. Simplified Tag Structure

The tag has the clock or triggering unit for the setting of Beacon Rate, which allows the transmission of signals periodically. The frame pattern to be transmitted is multiplied with the PN-Sequence generated by PN-Generator. There are 2^{16} available PN-Sequence to use in this RFID system. PN Selector unit will randomly select an available PN-Sequence prior to the transmission. Once the transmitting signal is spread, the spread signal is modulated in the RF Modulator Circuit and transmitted out through the antenna.

The PN-Generator will generate noise like signals of "1" and "-1". The resulting signal after the multiplication has higher frequency and wider energy band. The receiver will decode the spread signal by multiplying with the same sequence used on transmission thus revealing the original signal. The intended receiver will receive the spread signals and the unintended receivers will receive the spread signals as noise.

The PN-Sequence in this transmission scheme allows the reduction of tag collisions in this RFID system, the tag doesn't need any acknowledgement from the reader thus the tag is only equipped with Transmission devices thus the power usage for the tag is very low, allowing longer battery life. The most common anti-collision methods used are based on Time Division Multiple Access (TDMA), and others such as Frequency Division Multiple Access (FDMA) and CDMA. TDMA is an example of a group of people talking one at a time in a room, FDMA is a group of people talking with different pitches at a same time and CDMA is a group of people talking with different language from each other, while only the 2 sources communicating are understood to each other while other sources consider it as a noise.

The steps of the functions of Tag are listed below.

- Clock/Triggering unit lets the transmission take place every T_R second.
- PN-Generator generates N bit PN-sequences which are known to the receiving side.
- PN-Selector randomly selects a PN-sequence from available sequences and that sequence is multiplied with the transmit bit frame.
- The coded bit frame is modulated and transmitted through the RF Modulator, (such as BPSK, PSK, QAM, ASK, OOK).

The transmit frame pattern (transmit signal structure) is stored in ROM and sent out periodically. This DS-CDMA method provides encryption since the spreading code encrypted the transmit signal, thus having greater security and avoiding interferences between tags. The tag structure depicted in Figure.8 is simulated in Matlab/Simulink simulation environment. The detail simulations and results are shown in Result & Discussion section of this report.

3.1.4 Reader Structure

The reader structure is designed to receive the signals sent from tags, demodulate and decode the signal. The reader has a bank of matched filters to match the bipolar representation of incoming signals. Since the reader is to parallel process the tag signals which are received aperiodically thus a buffer is present in the reader structure. After the receive signals are buffered, a frame detection and error detection processes are done. In this process the SYS Field, Tag ID and CRC field of the decrypted signal is going to be checked, only the signal with correct SYS field and relevant CRC checksum, the reader send the ID of this tag to the Middleware. The concept of the reader is depicted in Figure.9.

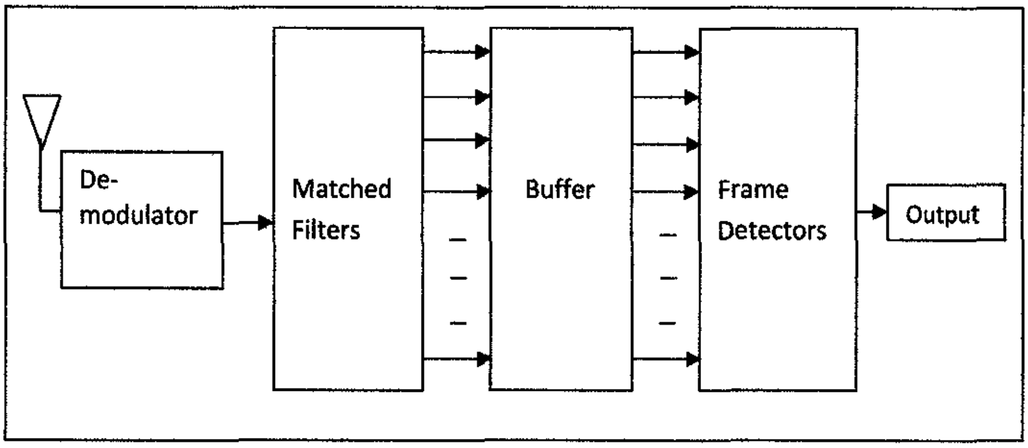


Figure.9. Conceptual Structure of the Reader

The reader or receiving end will receive a modulated signal. It'll be demodulated and transformed into baseband signal in the Demodulator part of the reader. Then the bit stream of the signals goes through the bank of matched filters where there are enough filters for all of the tags present in the system. The PN-sequenced signals are decoded in matched filters and decoded signal is buffered in the buffer. The frame detectors for all the signals detect errors and detect the signal's SYS field. Only the correct SYS field and signals with no error will send to output where the signal is further sent to middleware for processing or storing.

Thus, this method of avoiding the interferences between tags is the use of DS-CDMA technology, where the transmit signal is spread with a noise like sequence called PN-sequence, allowing each tag with a unique code to communicate with the receiver, reducing the interferences between other tags. Figure.10 depicts communication between a tag and the reader.

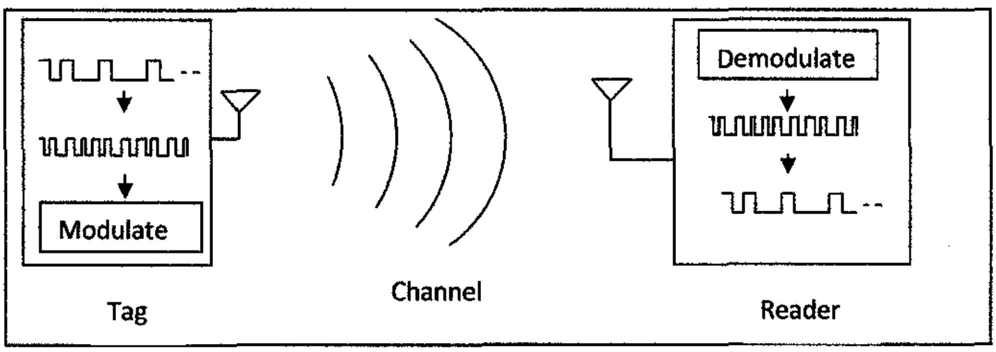


Figure.10. Simplified illustration of tag-reader communication

3.2 Spread Spectrum Techniques

Earlier in this chapter, mentioned the technique of using the spread spectrum technique to send and receive the signals from the tags. This method is widely used in many communication applications since 1940 when the military started using the technique because this technique gives a very secure transmission and reception [10]. The technique spread the original signal hence getting wider bandwidth and allowing the signal with more secure and robust transmission. This achievement is related to Shannon's channel capacity formula. Shannon's formula for channel capacity is a relationship between achievable bit rate, signal bandwidth and signal to noise ratio [11].

$$C = B \log_2 (1 + SNR) \tag{5}$$

Where, C = Capicity

B = Bandwidth

SNR = Signal to Noise Ratio

The equation states that the better the SNR and the more bandwidth a system has, the more bits per second of data can be pushed into the system. If a signal to be sent is treated to have a wider signal bandwidth, the signal's resistance to noise and interferences is higher. This is very useful in situations where the signal power is much weaker than the noise power. We can overcome this problem by using a spread spectrum technique. The spread spectrum technique has many advantages.

According to C. Kopp (1997)

The Ability to Selectively Address: If we are clever about how we spread the signal, and use the proper encoding method, then the signal can only be decoded by a receiver which knows the transmitter's code. Therefore by setting the transmitter's code, we can target a specific receiver in a group, or vice versa. This is termed Code Division Multiple Access.

Bandwidth Sharing: If we are clever about selecting our modulation codes, it is entirely feasible to have multiple pairs of receivers and transmitters occupying the same bandwidth. This would be equivalent to having say ten TV channels all operating at the same frequency. In a world where the radio spectrum is being busily carved up for commercial broadcast users, the ability to share bandwidth is a valuable capability.

Security from Eavesdropping: If an eavesdropper does not know the modulation code of a spread spectrum transmission, all the eavesdropper will see is random electrical noise rather than something to eavesdrop. If done properly, this can provide almost perfect immunity to interception.

Immunity to Interference: If an external radio signal interferes with a spread spectrum transmission, it will be rejected by the demodulation mechanism in a fashion similar to noise. Therefore we return to the starting point of this discussion, which is that spread spectrum methods can provide excellent error rates even with very faint signals.

Difficulty in Detection: Because a spread spectrum link puts out much less power per bandwidth than a conventional radio link, having spread it over a wider bandwidth, and a knowledge of the link's code is required to demodulate it, spread spectrum signals are extremely difficult to detect. This means that they can coexist with other more conventional signals without causing catastrophic interference to narrowband links.

The spread spectrum techniques can be further divided into Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), Time Hopping Spread Spectrum (THSS) and combination of these techniques. The DS-CDMA scheme allows avoiding collisions between transmitters to the base station or tags to the reader, thus using the technology in RFID is an advantage to avoid the collisions. Figure.11 depicts the use of CDMA for 2 different transmitters [12]. One transmitter sends out certain data to the receiver and another transmitter sends a different data to the receiver. Receiver, being known which transmitter is using which code (channel) can decode the received spread signal according to the user and the sent data is encoded.

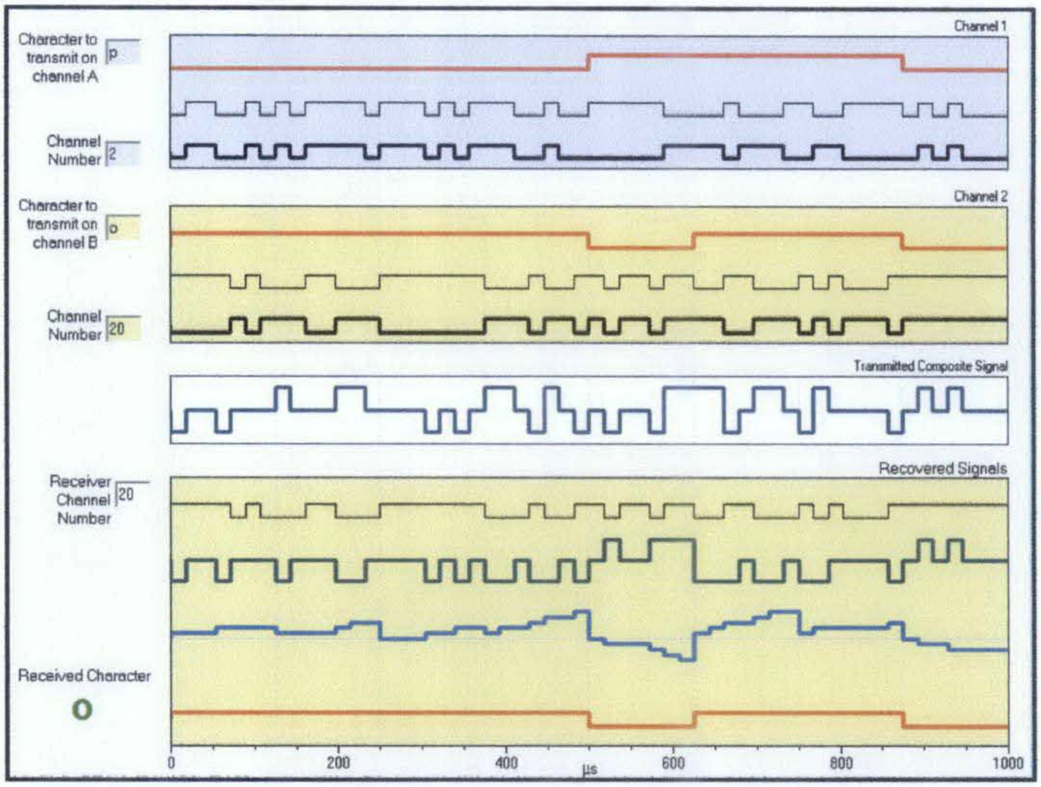


Figure.11. DSSS Encoding and Decoding with 2 Transmitter

In this chapter, approached method of avoiding the collisions and interferences between RFID tags is described. Direct Sequence Spread Spectrum technique is used in many communication networks especially in mobile phone networks. RFID tags are simply introduced with coded and widen bandwidth transmission thus avoiding the interferences between other tags.

CHAPTER 4
RESULTS & DISCUSSION

4. SIMULATION RESULTS AND ANALYSIS

The approached method of avoiding the collisions and interference between RFID tags is simulated and described in detail in this chapter. The simulation environment is in Matlab/Simulink with appropriate matlab codings and Simulink blocks structures. The simulation of DSSS technique, DS-CDMA transmission, the use of DS-CDMA in RFID Tag structure and multiple tag simulations are described in detail.

4.1 Direct Sequence Spread Spectrum Simulation

A 6 bit long sample is generated in Matlab and spread with a PN-sequence then modulated and transmitted. A series of diagrams can be seen to analyze the usage of PN-sequence in this transmission scheme. The Matlab coding used in this simulation is shown on "Appendix 1: Matlab Coding of DSSS".

In this simulation, the focus is on the original bit sequence and the transmit signal bit sequence after the spreading process is done. Since this is not a simulation for complete transmission, the receiving side and channel properties are not considered in the simulation coding.

Figure.12. shows the bipolar representation of the transmitting bit sequence. Figure.13. shows the PN-sequence and we can see that the frequency of this sequence is much higher than the original bit sequence. In order to spread the spectrum, the PN-sequence is multiplied with the original signal. The resultant DSSS signal is shown in Figure.14.

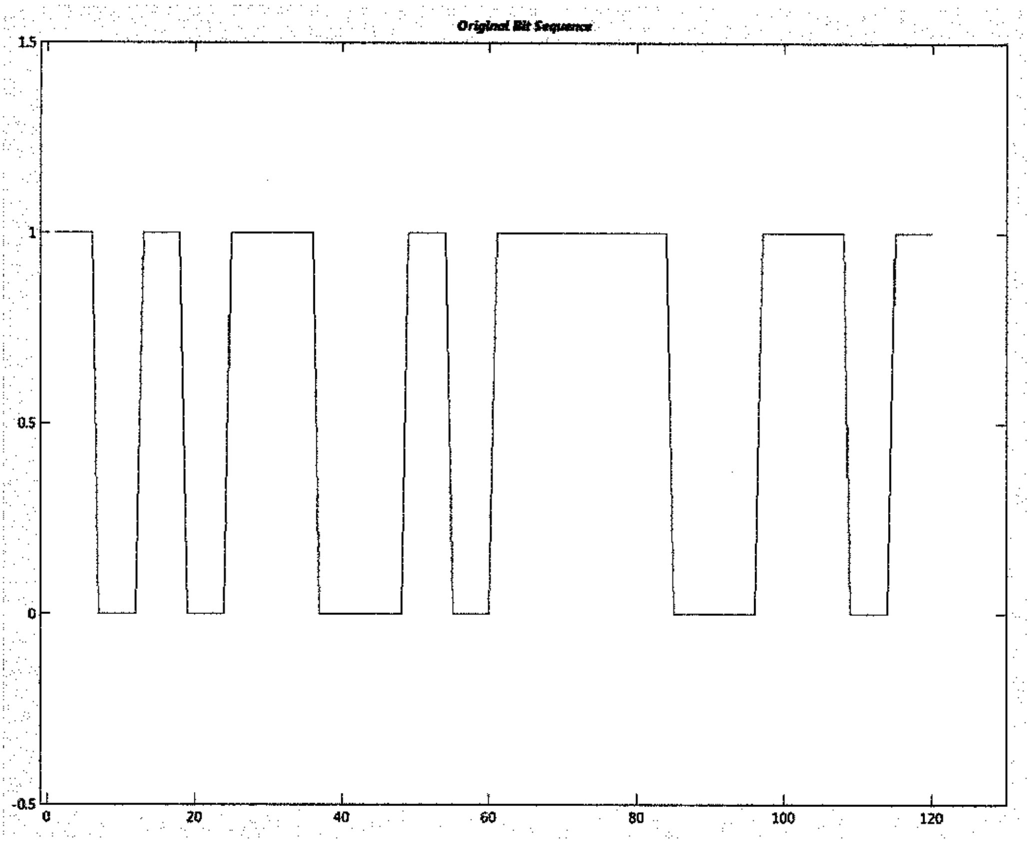


Figure.12. Original Bit Sequence

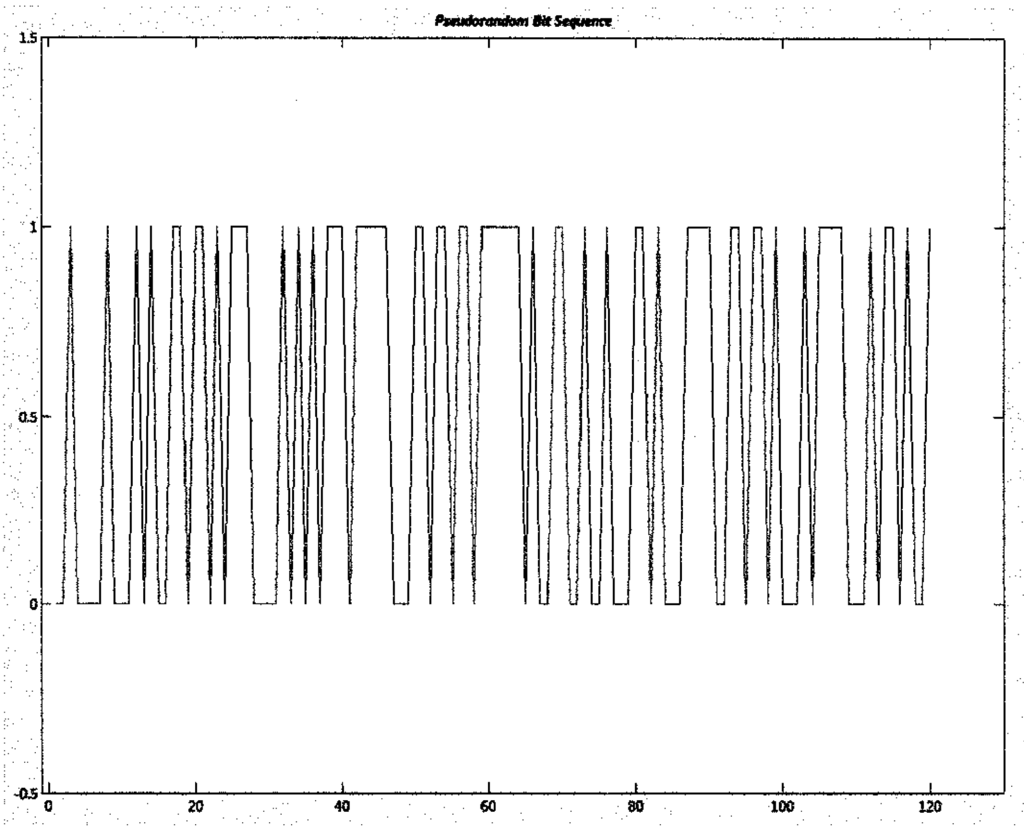


Figure.13. PN-Sequence bits

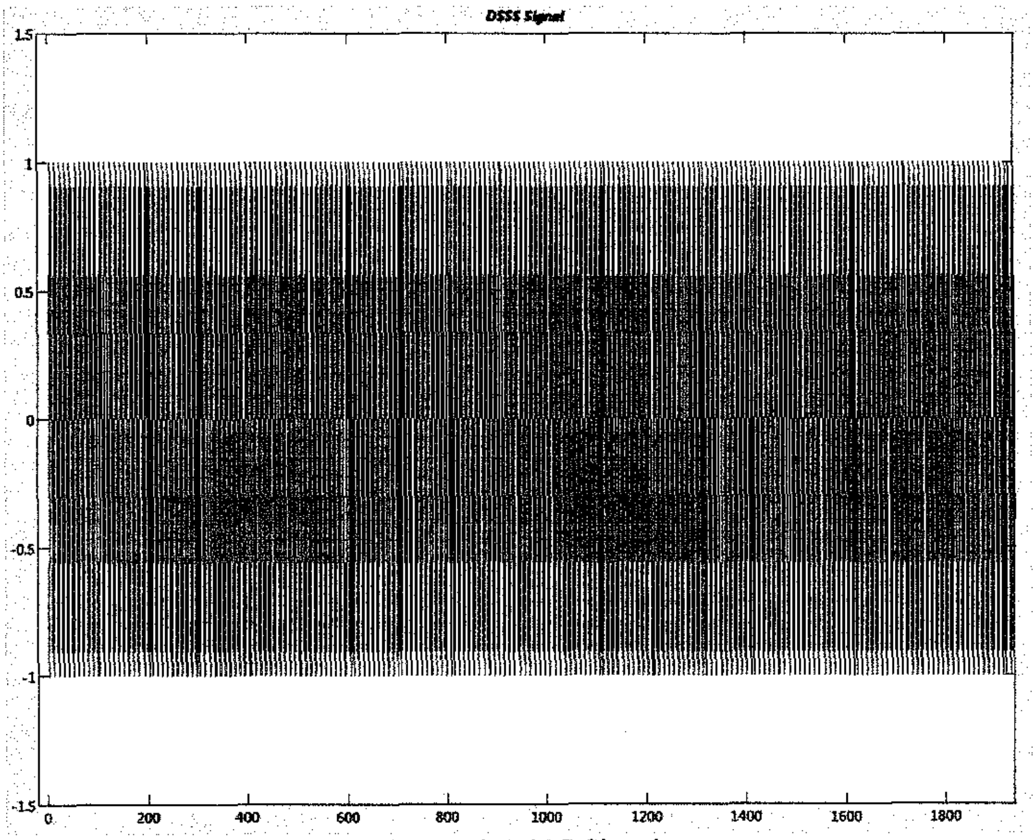


Figure.14. DSSS Signal

Comparing the original signal bit sequence and the signal using the DSSS technique, it is clear that the resultant DSSS signal is having a much more higher frequency and bandwidth than the original signal. This type of signals can communicate with a certain receiver using the same frequency without interfererring against each other. The receiving side can de-spread the signal using the same PN-sequence thus resulting in the original bit sequence. Error can be occurred according to the type of channel and noise level. However this simulation only focused on the DSSS technique without consideration of channel properties and receiving end.

4.2 DS-CDMA Simulation Model in Simulink

4.2.1 Simulation Model Details

The simulation model for DS-CDMA technique is constructed in Simulink using the Simulink Communication Blocks. The purpose of this simulation is to analyze the DS-CDMA technique for its usage of collision avoidance in RFID systems. The figure below shows the simulation model for DSSS technique in simulink.

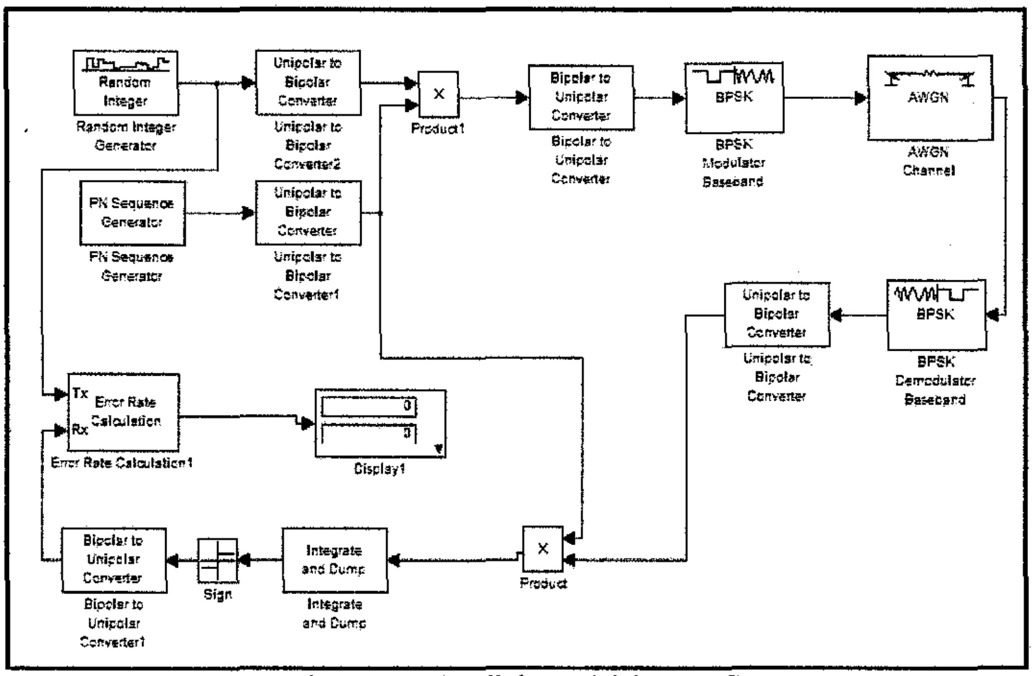


Figure.15. Simulink Model for DSSS

Random Integer generator is used to generate the bit signals to send out. Unipolar to Bipolar block is to represent the unipolar bits as "+" and "-" representations. PN Sequence Generator is used to generate the PN Sequences. After the bit sequence is spread with PN Sequence, the bipolar representation of the spread signal is converted back into Unipolar representation to perform the modulation. In this simulation, BPSK (Bi-Phase Shift Keying) is used to modulate the data and send out through the channel. Additive White Gaussian Noise channel is used as the channel. After the AWGN channel block is the receiving side of the model. Again, demodulation of the received signal is performed and convert into Bipolar representation to decode the Spread Spectrum signal. The Integrate and Dump block sums up the input signals and reset to zero after a certain sample has been outputted from the block. That means the block has set a certain amount of samples to add and after these samples, the block will reset to zero and adds up again, until the simulation time is up. Table.2. describes the simulation parameters for the model shown in Figure.15.

Table.2. Simulation Parameters for DSSS Model

Block	Parameter	Value
Random Integer Generator	Sample Time	1/1000
	M-ary	2
PN Sequence Generator	Sample Time	1/32000
Unipolar to Bipolar	M-ary	2
AWGN Channel	Sample Time	1/32000
	Eb/No	6 dB
Integrate and Dump	Integration Period	32
Error Rate Calculation	Receive Delay	1

4.2.2 Simulation Results

The simulation of the model shown in Figure.15 gives the transmit signal, spread signal and the receive signal. The channel properties in this simulation are set for the simulation as shown in Table.2. The figure below shows the original signal and spread signal for the transmission.

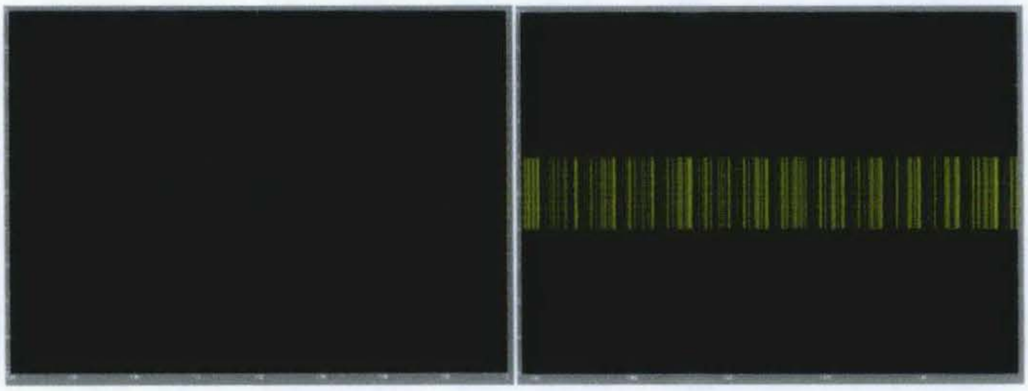


Figure.16. Original Signal and Spread Signal

The original and the receive signals are shown in the figure below. We can see that both signals are the same. This shows that the simulation is a success.

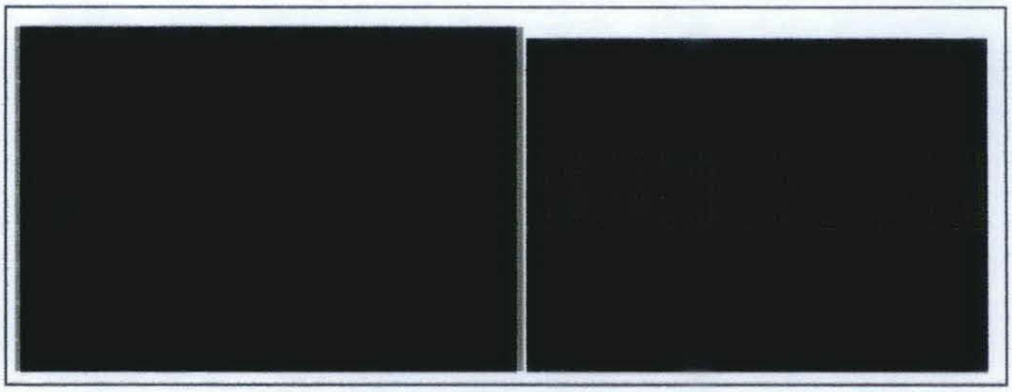


Figure.17. Original signal and received signal

The Error Calculation block shows "0" error, this is because the transmit and received bits are all the same and the channel used in this simulation is not a critical channel simulation thus the noise introduced in this simulation is very low, resulting in all the signals sent and receive are same with no error.

4.2.3 Simulation Model for Multi Tags (DS-CDMA)

The model shown in Figure.18 is the simulation model for Multi Tags (DS-CDMA), considering the transmitting sources as the RFID tags, the 3 tags are sending the signals to the reader with different PN codes. In the simulation, the PN-generators are programmed with different PN Generating sequences for the transmitters to get the unique codes. The random integer generator blocks are also programmed to generate different bits. The channel properties or channel is not considered in this model.

The Tags transmits the signals with a unique spread signals, and to simulate the transmission of the tag to the reader at the same time, the transmit spread signals from all three tags are added together. This addition creates the mixture of the signals from all 3 transmitting sources (Tags) and the reader receives the mixture of the signals. At this point, we can clearly see the advantage of the DS-CDMA technique. The reception of the mixture of the signals from all 3 tags doesn't make any difference to the receiver (reader) since the Direct Sequence Spread Spectrum is used. The using of same PN-sequence to decode the receive-signal can reveal the original transmit signal at the receiver. The Figure.18 below shows the model for 3 transmitting sources (Tags). (Since the model is too large to fit in the page, the larger version of the model is shown in Appendix.2)

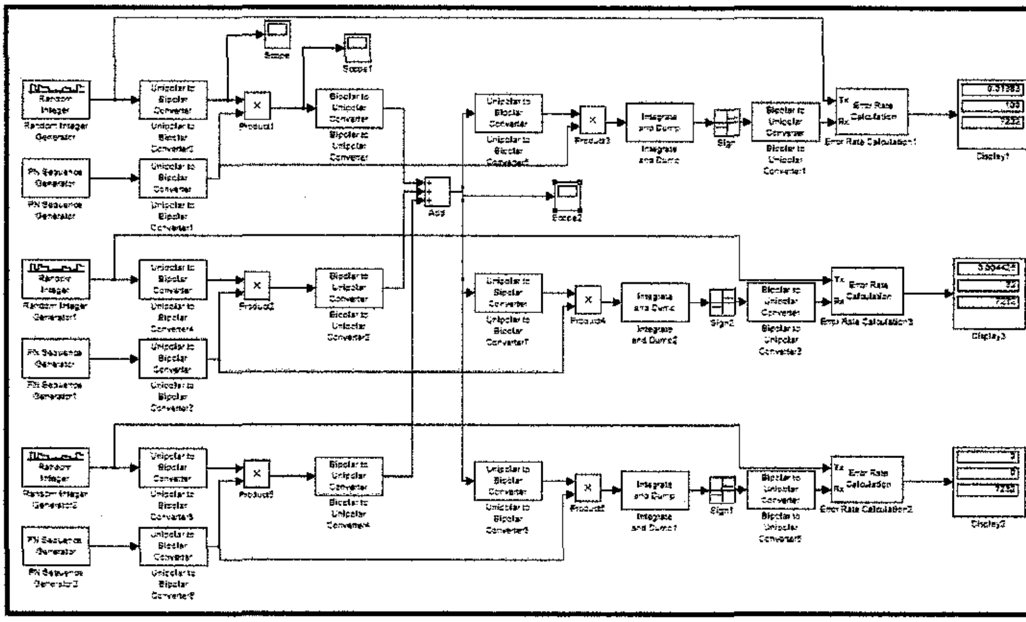


Figure.18. Model for Multi-Tags (DS-CDMA)

4.2.4 Simulation Results

The simulation results depend on how specific the PN-Sequence used in the model, the PN-Sequence with longer bit sequences gives less error in receiver. The original transmitting bits generated from Random Integer blocks are not significantly different from the signal shown in Figure.16, thus only the mixture of three signals after they are spread is shown in Figure.19. The signals transmitted are received as high frequency signals and without the use of DS-CDMA, this type of signals are to be treated as noise. However, DS-CDMA technique decodes this type of signal and the original signals are recovered with very low error rate.

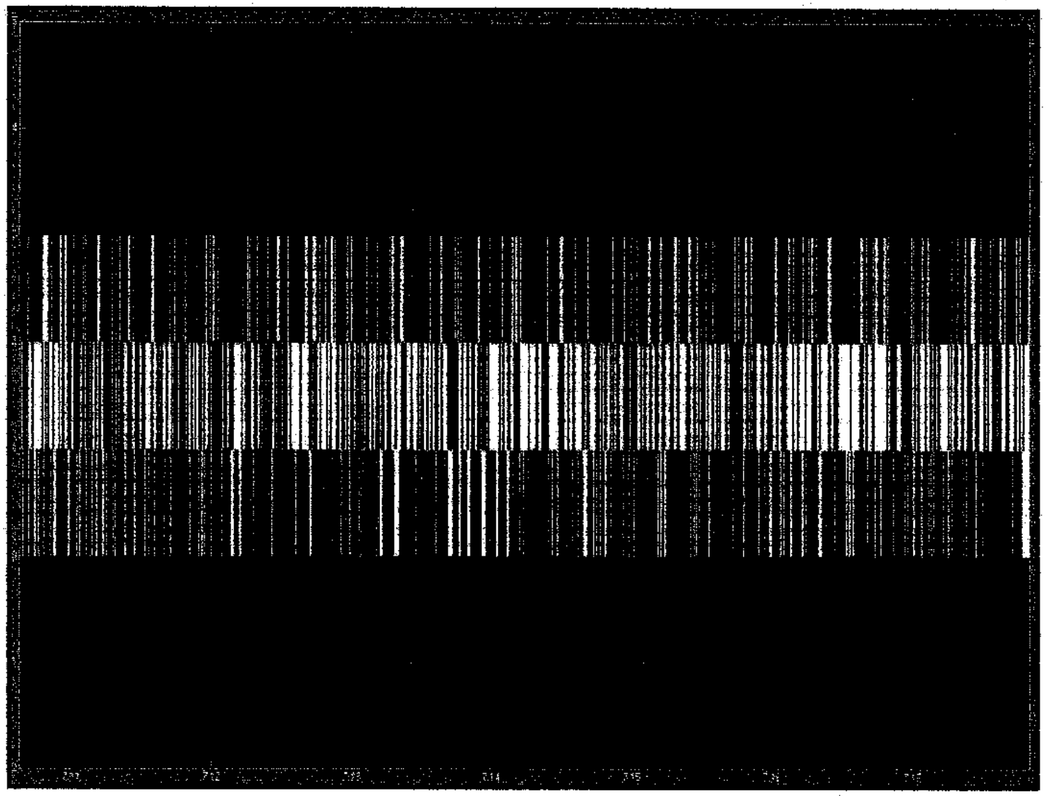


Figure.19. Mixture of Spread Signals from 3 Tags

The error performance in this simulation is relatively good. The error rates for each received signals are 0.01383, 0.004425 and 0. Thus the overall error rate for this simulation is 0.006085.

The case where RFID tags transmit the signals to the reader at a same time without any anti-collision avoidance will simply make the reader confuse or miss read the tags. The simulation shows that the reception of the overlap signals are recovered with minimal error, thus this is the advantage of using DS-CDMA technique as RFID anti-collision method.

4.3 Discussion on the Results

The method and use of DS-CDMA technique in RFID system for collision avoidance and its simulations are described in previous section. The discussion on the effectiveness and difficulties on further more detail simulations and implementation are described in this section. The main concern for the simulation and simulation results done in this report are the accuracy and complexity of the simulation model and simulation environment. The model used in this project is constructed in Simulink simulation environment using the provided blocks. This makes the simulation of this project less accurate, however the concept of applying the DS-CDMA technique in RFID systems is clearly shown. The conceptual structures for Tag structure and Reader structure can be built in further more detail using other simulation environments. However, this paper provides the clear concept of using the spread spectrum in RFID systems to avoid collisions although more detail structures and simulations can be done in future.

As far as the simulations done and results obtained, the analysis of the results shows the collision between the tags are reduced. There are many other methods to avoid the collisions in RFID systems as mentioned in previous sections, the detail comparison of the method mentioned in this report with other methods cannot be made since the simulation works in this paper need more accuracy and detail. However, the advantage of this method is the less complexity in reader and tag structures compare to other RFID systems since the Tag in this method is the transmitter and the reader in this method is the receiver. Since the Active Tag used in this method has transmitter circuits and the reader has the receiver circuit, thus this method uses a very low power for both tag and reader. Since the tag is provided by onboard battery source, less power usage means longer battery life and reliable operation for the tag.

The reader structure for the method is a conceptual design, and further development and detail designs are needed. The basic concept is to allow the reception of the signals sent from tags which are overlapped in time which the use of the bank of matched filters. The matched filters are to decode all possible spread spectrum used in the system with the PN-sequences. The detail circuitry of each components in the simulation such as filters, amplifier, modulation units and gain controls are not considered in the simulations and this is the major disadvantage of this report. The absent of the detail circuitry in the simulations are because of the tight schedule and given time frame for the project. Since this is a research based project, grabbing the background theory and literature review of the project work themselves take longer time, since the collision avoidance techniques are much more advanced and can be considered as higher level studies compare to RFID transmissions, receptions and fundamental theories. Anyhow this project introduces the use of DS-CDMA technique to avoid the collisions in the RFID systems.

CHAPTER 5
CONCLUSION AND RECOMMENDATIONS

5. CONCLUSION AND RECOMMENDATIONS

This section covers the review of the report and summary of all the works done in this project. The recommendations for further research and works are also mentioned.

5.1 Conclusion

The project started with studies on RFID technologies and applications, fundamental theories of RFID and its various advantages over other likely technologies are also studied. The studies on electromagnetic theories and radio communications fundamentals are done to get the background knowledge to work on this project [13][14]. Existing and proposed anti-collision methods are also studied throughout the project work.

The advantage of the method described in this report is that the Active tag and the reader are only the transmitter and receiver. Synchronization between tag and the reader is not necessary thus providing a very straight forward transmission between tag and the reader. Each tags are assigned with unique PN-sequence and spread prior to the transmission. The reader is capable of receiving the tags signals overlapped in time. The designs of reader and tag are conceptual.

The simulations done in the project are shown and analyzed and clearly be seen that the introduced method is very useful for RFID systems. Discussions from the critical point of views are mentioned such as the simulation issues and accuracy of the simulations. Finally, the project work has successfully described the concept of using DS-CDMA technique in RFID systems.

5.2 Recommendations

Future works on this project can be done in many ways including the constructing of the more detail model for tag and reader. The simulations done in this project mainly focus on the theory and concept of the method, thus detail focus on all the aspect of the whole RFID system to simulate can be done in future project work. Since it is very difficult to simulate the whole RFID system using only one model, the tags and reader structures can be constructed separately and linked to the models to get the overall simulation. The Channel of the simulation model also can be further modified to get as close as possible to the real channel thus it will result with much more accurate simulation results. Once the whole simulation for RFID system using DS-CDMA is done, the performance analysis and comparison with other collision avoidance methods can be made.

REFERENCES

[1] RFID Journal , Dec 2010, [online]
Available: http://www.rfidjournal.com/article/glossary/3#125

[2] R. Want, "An Introduction to RFID Technology," in *IEEE CS and IEEE ComSoc* Mar. 2006, pp. 1536-1268.

[3] G. Mazurek, "Active RFID System With Spread-Spectrum Transmission," in *IEEE Transactions on Automation Science and Engineering,* Jan 2009 Vol. 6, No. 1, pp. 5955-5963.

[4] D.M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice,* 2008 Elsevier. ch. 3.

[5] S. Xue, "Multi-tag Content Access Control in RFID System," in *University of Stavanger, Master's Thesis,* Ch.1, 2009.

[6] D.K. Klair, K.W. Chin, R. Raad, "A Survey and Tutorial of RFID Anti-Collilsion Protocols," in IEEE Comm.. Serveys & Tutorial, Vol.12, No.3. 2010, pp. 400-421.

[7] A. Goldsmith, "Wireless Communication," *Cambridge University Press* 2005, Ch.7.4.

[8] Wikipedia, Jan 2011, "Cellular Network," [online]
Available: http://en.wikipedia.org/wiki/Cellular_network

[9] Wikipedia, Jan 2011, "Code Division Multiple Access," [online]
Available: http://en.wikipedia.org/wiki/Code_division_multiple_access

[10] Wikipedia, Jan 2011, "Spread Spectrum," [online]
Available: http://en.wikipedia.org/wiki/Spread_spectrum

[11] C. Kopp, "An Introduction to Spread Spectrum Techniques," in *Ausairpower.net,* May. 1997.

[12] VIAS, Virtual Institute of Applied Science, Feb 2011, "*DSSS Simulation,*" [online] Available: http://www.vias.org/simulations/simusoft_dscdma.html

[13] J.R. Reitz, F.J. Milford, R.W. Christy, "Foundation of Electromagnetic Theory," 4th ed, New York, Wiley. 2009

[14] B. Gardner, "Say Again, Please: Guide to Radio Communication," *Cambridge University Press* 2004.

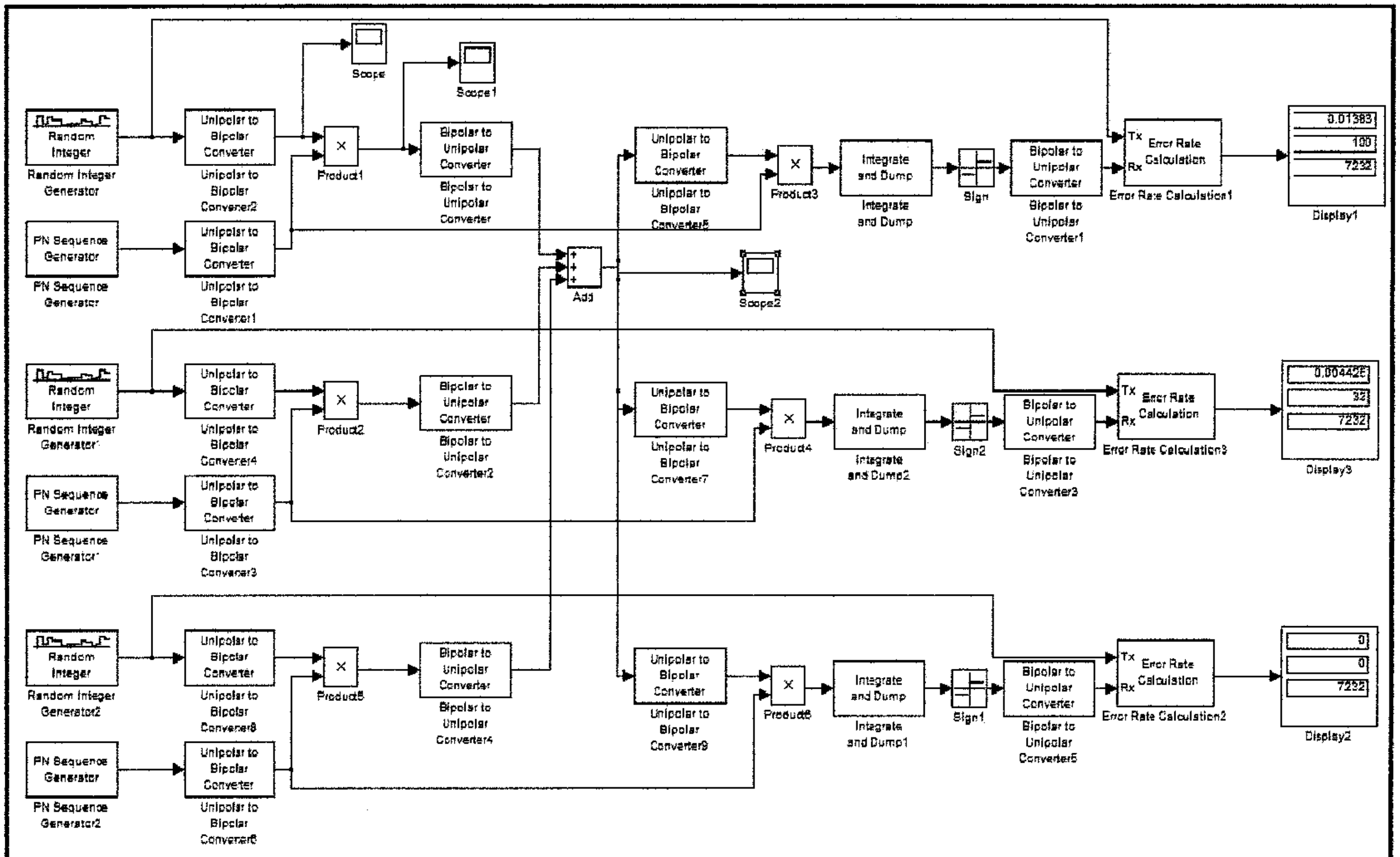
APPENDICES

APPENDIX A

Matlab CODING FOR DSSS

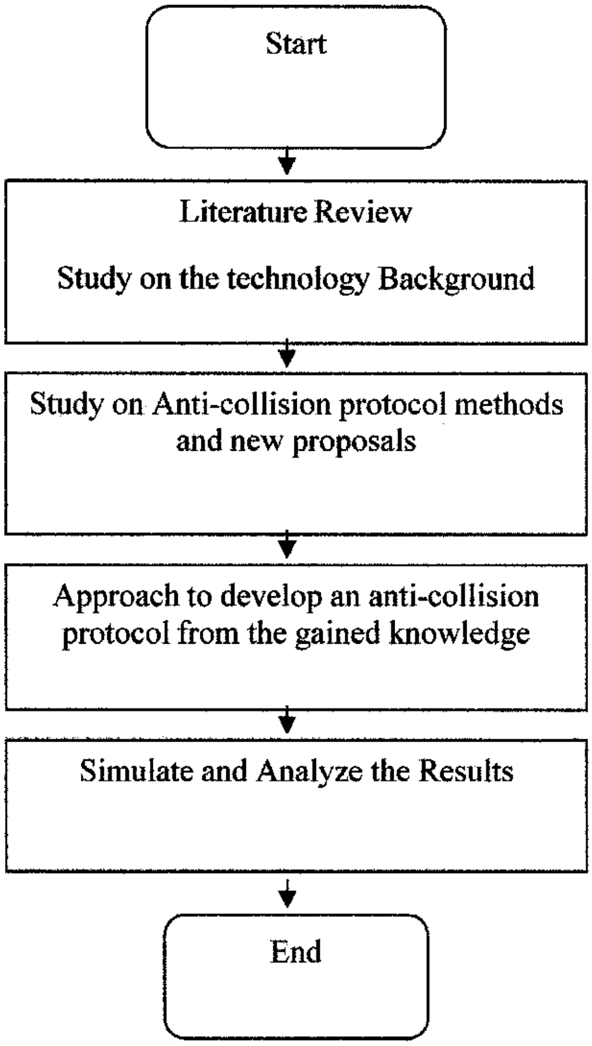
```
% Generating the bit pattern with each bit 6 samples long
b=round(rand(1,20));
pattern=[];
for k=1:20
    if b(1,k)==0
        sig=zeros(1,6);
    else
        sig=ones(1,6);
    end
    pattern=[pattern sig];
end
plot(pattern);
axis([-1 130 -.5 1.5]);
title('\bf\it Original Bit Sequence');

% Generating the pseudo random bit pattern for spreading
spread_sig=round(rand(1,120));
figure,plot(spread_sig);
axis([-1 130 -.5 1.5]);
title('\bf\it Pseudorandom Bit Sequence');

% XORing the pattern with the spread signal
hopped_sig=xor(pattern,spread_sig);

% Modulating the hopped signal
dsss_sig=[];
t=[0:100];
fc=.1
c1=cos(2*pi*fc*t);
c2=cos(2*pi*fc*t+pi);
for k=1:120
    if hopped_sig(1,k)==0
        dsss_sig=[dsss_sig c1];
    else
        dsss_sig=[dsss_sig c2];
    end
end
figure,plot([1:12120],dsss_sig);
axis([-1 12220 -1.5 1.5]);
title('\bf\it DSSS Signal');
```

APPENDIX B
COMPLETE SIMULATION MODEL



APPENDIX C

PROJECT FLOW DIAGRAM



...

APPENDIX D
RFID FREQUENCY RANGE