UNIVERSITY OF NAIROBI
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL AND INFORMATION ENGINEERING

INTERFERENCE CANCELLATION IN RFID SYSTEMS

PROJECT INDEX: PRJ 086

BY

KYULE MARTHA MBENGE

F17/1746/2006

SUPERVISOR: DR. V.K. ODUOL
EXAMINER: DR. GAKURU

A report submitted in partial fulfillment of the requirements for the award of the degree of Bachelor of Science in Electrical and Information Engineering of the University of Nairobi

Date of Submission: 18th May, 2011.
Dedication

This project is dedicated to my sister Grace and my brother Elijah for their support that has kept me going.
Acknowledgment

I take this opportunity to thank my project supervisor, Dr. V.K. Oduol for his valuable suggestions and assistance without which this project could not have been successful.

I am specially grateful to my parents Levin Kyule and Mary Ndinda for their encouragement and support all through my course of study.

Special thanks to my proof reader Ngâru Benjamin and to my friends Julius Kilonzi, Kyalo Victor, Omurayi Clyde, Brian Wambugu and Adam Wanyama for inspiring me in this project.

I would like to express my sincere gratitude to my lecturers for the knowledge they have passed on to me during my course of study.

I am most thankful to God Almighty for this far He has brought me.

God bless all
Declaration of Originality

This Bachelor of Science project is my original work and does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university and that to the best of my knowledge it does not contain any materials previously published or written by any other person except where due reference is made in the text.

é .é .é é é é é

KYULE MARTHA MBENGE

F17/1746/2006

This report has been submitted to the Dept. of Electrical and Information Engineering,
University of Nairobi with my approval as supervisor:

é é é é é é é é

Dr. V.K. Oduol

Date: 18th May 2011
# Table of Contents

**Contents**

Dedication.......................................................................................................................... ii  
Acknowledgment .................................................................................................................. iii  
Declaration of Originality ..................................................................................................... iv  
Table of Contents ................................................................................................................... v  
Abstract ................................................................................................................................ viii  

**CHAPTER 1: INTRODUCTION** ............................................................................................... 1  
1.1 Brief History ..................................................................................................................... 1  
1.2 Problem statement .......................................................................................................... 1  
1.3 Objectives of the Project ................................................................................................. 2  
1.4 Organization of the report .............................................................................................. 2  

**CHAPTER 2: LITERATURE REVIEW** .................................................................................... 3  
2.1 RFID systems .................................................................................................................... 3  
2.2 RFID Tag .......................................................................................................................... 4  
2.3 RFID Reader (Interrogator) ............................................................................................ 5  
2.4 RFID Antenna .................................................................................................................. 6  
2.5 Communication between Reader and Tag ....................................................................... 6  
   2.5.1 Forward link (from reader to tag) .............................................................................. 6  
   2.5.2 Reverse link (from tag to reader) ............................................................................. 6  
2.6 Types of RFID systems .................................................................................................... 7  
   2.6.1 Active RFID Systems ............................................................................................... 7  
   2.6.2 Passive RFID Systems ............................................................................................ 8  
   2.6.3 Semi-Active (Semi-Passive) RFID Systems ............................................................ 9  
   2.6.4 Other Categories of RFID Systems (tags) ............................................................ 10  
2.7 Interference Sources in RFID Systems .......................................................................... 12  
   2.7.1 Collision .................................................................................................................. 12  
   2.7.2 Presence of a Radio Frequency Absorbing Material in Path .................................. 14  
   2.7.3 Electromagnetic Interference (EMI) ...................................................................... 14  
   2.7.4 Harsh environmental conditions .......................................................................... 14
2.7.5 Improper Placement of Tags ................................................................. 14
2.7.6 Physical Obstructions ........................................................................ 15
2.7.7 Transmission Channel Noise .............................................................. 15

CHAPTER 3: INTERFERENCE CANCELLATION .................................................. 16

3.1 Interference Cancellation Techniques in RFID Systems ................................ 16
   3.1.1 Synchronization ................................................................................ 16
   3.1.2 Error Correcting Codes (ECC) ............................................................ 16
   3.1.3 The Active Jamming Approach ........................................................... 16
   3.1.4 Increasing Power and Path-Loss ......................................................... 17
   3.1.5 Use of digital Filters ........................................................................ 17
   3.1.6 Anti-collision ..................................................................................... 19
   3.1.7 Proper Tag and Reader Chip Design .................................................. 20
   3.1.8 The "Kill Tag" approach ................................................................... 21
   3.1.9 The Faraday Cage Approach ............................................................ 22
   3.1.10 The "Hash Lock" Approach ............................................................... 23
   3.1.11 The Encryption Approach ............................................................... 23

CHAPTER 4: DESIGN AND IMPLEMENTATION ................................................ 25

4.1 Design ..................................................................................................... 25
   4.1.1 Interference Cancellation Design using an Adaptive Filter ................. 26
   4.1.2 Simulink Design using a NLMS Adaptive Filter ............................... 28

4.2 Implementation ....................................................................................... 30

CHAPTER 5: RESULTS AND DISCUSSIONS ..................................................... 31

5.1 Results .................................................................................................... 31
5.2 Discussions ............................................................................................. 32

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS .............................. 33

6.1 Conclusion .............................................................................................. 33
6.2 Recommendation for Future Work ......................................................... 34
6.3 APPENDICES .......................................................................................... 35

APPENDIX A ................................................................................................. 35
APPENDIX B ................................................................................................. 36
APPENDIX C ................................................................................................. 37
Abstract

Radio-frequency identification (RFID) is a technology that uses communication via radio waves to exchange data between a reader and an electronic tag attached to an object for the purpose of identification and tracking [1]. The tags can be read from several meters away from the reader. Bulk reading of the tags by a reader enables an almost parallel reading of tags. Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, and other specialized functions. The other is an antenna for receiving and transmitting the signal.

RFID systems are hoped to become a standard tracking and tagging system for various chain management systems. They are flexible since the data contained within a RFID tag can be changed as required. It is also possible to separate the time at which an object is tagged from the time at which information is stored on the tag.

Due to the increased use of RFID systems in the modern day world it is important to understand various RFID systems, study interference sources in these systems and produce accurate information by performing interference cancellation. It is also important to ensure consumer privacy.

In this project, different RFID systems, the sources and nature of interference in the systems have been presented. A design of interference cancellation for performance improvement in RFID systems has also been done. A Normalized Least Mean Square adaptive filter was used in this design. The filter coefficients were adjusted in order to obtain interference cancellation by converging the filter output. For a UHF RFID system (880MHZ), the filter order that gave better noise performance was estimated to be 96. Higher filter ordering caused distortions to the approximated signal.
CHAPTER 1: INTRODUCTION

1.1 Brief History

The history of RFID technology can be dated back to World War II when the Germans, Japanese, American and British were all using coded radar systems which had been discovered in 1935 by a Scottish physicist Alexander Watson-Watt to warn of approaching planes while they were still miles away. The major problem with this system was that it was hard to identify which planes belonged to the enemy from the country’s own planes returning from a mission.

Later the Germans discovered that by the pilots rolling back their planes before returning to the base could change the radio signals reflected back and the radar crew could be alerted that the approaching planes were not allied aircrafts. This marked the first invention of a passive RFID system. The British developed the first active identify friend or foe (IFF) system under Watson Watt. In these systems, a transmitter was put on each of their planes such that when planes received a signal from the radar station on the ground, they began broadcasting a signal back that identified the aircraft as friendly.

Further advancements in RFID technology were accomplished in 1950s and 1960s when scientists and academicians in the United States, Europe and Japan discovered that radio frequency (RF) could be used to identify objects remotely. Companies started commercializing antitheft systems that used radio waves to determine whether an item had been paid for or not.

1.2 Problem statement

Following an increased use of RFID systems for tracking purposes which aid in; ensuring a greater supply chain visibility, tracking product paths in the event of a product recall, allowing inventory of products located in areas that are dangerous or physically difficult to reach and monitoring the safety of perishable items in order to detect spoiled item. It is therefore necessary to understand the type of RFID systems used, their interference sources and the methods used to cancel out the interference.
1.3 Objectives of the Project

The objectives of the project were:

i. To study the RFID systems.
ii. To study the sources of interference in RFID systems
iii. To study interference cancellation techniques
iv. To design interference cancellation for performance improvement in a RFID reader.

1.4 Organization of the report

This report consists of six chapters;

Chapter 2: Describes different RFID systems and the sources of interference in these systems
Chapter 3: Discusses some interference cancellation techniques in RFID systems
Chapter 4: Contains the design and implementation of Interference cancellation for the systems
Chapter 5: Gives the results and the analysis of the design
Chapter 6: Is the conclusion and recommendation for further work.
CHAPTER 2: LITERATURE REVIEW

2.1 RFID systems

Radio frequency identification (RFID) is a technological means of using radio frequencies to transmit information [1, 2]. RFID systems consist of the following components: tags, RFID readers and middleware (a microprocessor). An RFID system allows for data to be transmitted from the tag to the reader, which in turn processes it for a particular use. The data transmitted by the tag may include identification, location information, price, colour or date of purchase. Radio Frequency Identification systems can be used for tracking purposes (asset tracking), logistics and supply chain management.

The tags are usually built using CMOS circuitry and can be powered by a battery or by rectification of the radio signal sent by the reader. Tags can send data to the reader by changing the loading of the tag antenna in a coded manner or by generating, modulating, and transmitting a radio signal. The commonly used modulation techniques used include: ASK, FSK, QAM and PSK [2].

RFID systems can be read only (data is transferred only in one direction, from the tag to the reader but the reader cannot transfer data to the tag) or read write (two-way communication). A typical RFID system uses the principle of modulated backscatter in which to transfer data from the tag to the reader, the reader sends an un-modulated signal to the tag. The tag reads its internal memory of stored data and changes the loading on the tag antenna in a coded manner corresponding to the stored data. The signal reflected from the tag is thus modulated with this coded information. This modulated signal is received by the reader, demodulated using a homodyne receiver, decoded and output as digital information that contains the data stored in the tag. To send data from the reader to the tag, the reader amplitude modulates its transmitted radio signal. This modulated signal is received by the tag and detected with a diode. The data can be used to control the operation of the tag, or the tag can store the data.

An RFID system works in several stages. Items are equipped with a tag, which has a transponder that is assigned a unique electronic product code. A transponder is a special radio transmitter and receiver which is activated on receiving a signal. Typical transponders consist of a microchip
that stores data and a coupling element, such as a coiled antenna, used to communicate via radio frequency communication. The reader antenna has a transceiver and a demodulator, which emits a signal that activates the tag. On activation, data can be read and written to the tag. If a reader is in its read range, it decodes the data being transmitted by the tag’s antenna and relays it to the middleware for processing.

The basic operation of an RFID system can be described by Fig. 2.1

![Fig. 2.1 The block diagram of a typical RFID system](image)

### 2.2 RFID Tag

This is a device that contains the identification number (ID) which is recognized by the reader through consecutive communication. It consists of a microchip programmed with information about a product and a coupling element (an antenna). The size of the tag depends on the size of the antenna. The antenna size increases with the read range of tag and decreases with frequency [1].
2.3 RFID Reader (Interrogator)

It is a device which interrogates the tag and transfers data between the data processing sub-system and the tag. It reads information from the tags and then transmits the information to the middleware (microprocessor) where it is collected, filtered and stored in a database. The antenna transmits radio waves and the tag responds by sending back its data. The read range of a reader can be affected by the frequency of identification, antenna gain, orientation and polarization of both the reader and transponder antennas [1]. RFID communication range (r) is obtained by Equation 2.1

\[ r = \frac{P \lambda G X \eta}{4\pi (R + 4X)P} \]  \hspace{1cm} (2.1)

Where: r is the communication range

- \( P \) is the Effective Isotropic Radiated Power
- \( \lambda \) is the wavelength
- \( G \) is the tag antenna gain
- \( X \) is the reactance introduced by the load modulator
- \( \eta \) is the rectifier efficiency
- \( R \) is the impedance of the antenna
- \( P \) is the tag power consumption

Global rectifier efficiency is given by Equation 2.2

\[ \eta = \frac{DC \text{ output power}}{Incident \ RF \text{ power}} \]  \hspace{1cm} (2.2)

The conversion rectifier efficiency is given by Equation 2.3

\[ \eta = \frac{DC \text{ output power}}{Incident \ RF \text{ power} - Radiated \ RF \text{ power}} \]  \hspace{1cm} (2.3)
2.4 **RFID Antenna**

A RFID system contains two antennas; one at the tag and another at the reader. They are conductive elements that enable the tag to communicate with the reader. Passive RFID systems use coiled antennas which create magnetic fields using the energy provided by the reader’s carrier signal.

2.5 **Communication between Reader and Tag**

For a passive RFID system, the communication between the reader and the tag is fully controlled by the reader because the tag cannot send data unless triggered by the reader. The communication from the reader to the tag is referred to as the forward link, while the communication from the tag to the reader is referred to as the reverse link as shown in Fig. 2.2

![Fig 2.2 A block diagram showing communication between a RFID reader and a tag](image)

2.5.1 **Forward link (from reader to tag)**

A continuous RF wave is transmitted from the reader to the tag through the forward link. The data is sent from the reader to the tag as short gaps in the continuous wave in amplitude shift key (ASK) modulation with Pulse Interval Encoding (PIE) [2].

2.5.2 **Reverse link (from tag to reader)**

The reverse link in a RFID system is done using backscattering scheme. The modulation of the chip impedance can be done using either ASK or PSK [2].

In ASK modulation, the chip impedance is varied between perfect match and complete mismatch. In PSK modulation, the real part of the chip impedance is kept in match with the antenna, while the imaginary part is varied between two capacitive and inductive values.
2.6 Types of RFID systems

There are three main types of RFID systems:-

i. Active RFID systems
ii. Passive RFID systems
iii. Semi-active (Semi-passive) RFID systems

2.6.1 Active RFID Systems

These systems contain a battery and can transmit signals once an external source ('Interrogator') has been successfully identified. They can initiate communication with a tag reader. The internal power source allows for a longer read-range and for a bigger memory on the tag itself. The power source also makes it possible to store information sent by the transceiver. Active RFID tags are relatively large and can be read from many meters away. They generally have a battery life of about ten years. Some active tags contain replaceable batteries for years of use while others are sealed units. It is also possible to connect the tag to an external power source. For this reason, active tags can have some data processing ability, while passive tags are limited to doing only elementary operations and replying to the reader's queries [2].

The major advantages of an active RFID tag are: -

i. It has a long communication range which improves the utility of the device.
ii. Active RFID tags may be equipped with autonomous networking which determine the best communication path.
iii. It may have other sensors that can use tag battery for power.
iv. It has superior performance in adverse environments, such as damp or metallic.
v. They are accurate and reliable

The disadvantages of active RFID tags are:-

i. They cannot function without battery power, which limits the lifetime of the tag.
ii. The tag is typically more expensive than the passive tag.
iii. The tag is physically larger, which may limit applications.
iv. The maintenance costs for an active RFID tag can be greater than those of a passive tag if the batteries are replaced.
v. Battery outages in an active tag can result in expensive misreads.
2.6.2 Passive RFID Systems

Passive RFID systems are composed of an antenna, a simple electronic circuitry and a small memory for storing some information about the object [1, 2]. They have no power source and require an external electromagnetic field to initiate a signal transmission. Instead, a small electric current is created in the antenna when an incoming signal reaches it. This current provides enough power to briefly activate the tag, usually just long enough to relay simple information, such as an ID number or product name.

Passive RFID tags do not contain a power supply thus they can be very small in size. These tags can be activated from a distance of about 6 meters. The limited resources of a passive tag require it to both harvest its energy and communicate with a reader within a narrow frequency band. The center of the frequency band is denoted by $f$. Passive tags typically obtain their power from the communication signal in two major ways; either through inductive coupling or far field energy harvesting. Inductive coupling uses the magnetic field generated by the communication signal to induce a current in its coupling element which is usually a coiled antenna and a capacitor.

The current induced in the coupling element charges the on-tag capacitor that provides the operating voltage and power for the tag. However, inductive coupling works only in the near-field of the communication signal. The near field for the center of the frequency band $f$ extends up to — meters from the signal source.

For a given tag, the operating voltage obtained at a distance $d$ from the reader is directly proportional to the flux density at that distance. The magnetic field emitted by the reader antenna decreases in power proportional to — in the near field. For a circularly coiled antenna the flux density is maximized at a distance $d$ (in meters) when $d = \sqrt{2} \times R$, where $R$ is the radius of the reader's antenna coil. Therefore, by increasing $R$ the communication range of the reader can be increased, and the optimum reader antenna radius $R$ is 1.414 times the demanded read range $d$.

Far field energy harvesting uses the energy from the interrogation far field signal to power the tag. The far field begins where the near field ends, at a distance of — from the emitting antenna. The signal incident upon the tag antenna induces a voltage at the input terminals of the tag. This voltage is detected by the RF front-end circuitry of the tag and is used to charge a capacitor that
provides the operating voltage for the tag. In a lossless medium, the power transmitted by the reader decreases as a function of the inverse square of the distance from the reader antenna in the far field. A reader communicates with and powers a passive tag using the same signal. The fact that the same signal is used to transmit power and communicate data creates some challenging trade-offs. First, the modulation of the signal causes a reduction in power to the tag. Modulating information onto an otherwise spectrally pure sinusoid spreads the signal in the frequency domain [1].

The advantages of Passive RFID Systems are:-

i. The tag is readable for a very long time.
ii. Passive tags are generally more resistant to corrosion and physical damage.
iii. The tag functions without a battery and therefore has a long life compared to active tags.
iv. The tag is typically much less expensive than active tags.
v. The tag is much smaller and it can be easily concealed.
vi. Passive tags have many more potential uses due to reduced size and cost.

The disadvantages of the passive RFID systems include the following:-

i. The tag can be read only at very short distances. This greatly limits the device for certain applications.
ii. It is not possible to include sensors that can use electricity for power.
iii. The tag remains readable for a very long time, even after the product to which the tag is attached has been sold and is no longer being tracked.

The basic differences between passive and active RFID systems are shown in Appendix A.

2.6.3 Semi-Active (Semi-Passive) RFID Systems

They have an independent power supply, but also receive power from a radio scanner when an incoming signal reaches the antenna. They require an external source to wake up but have significant higher forward link capability providing greater range.
The main advantages of these tags are that:

i. They achieve longer read ranges than passive tags but generally at lower costs than active tags.

ii. They have features associated with active tags such as memory which provides passive tag data storage for hierarchical asset tracking systems but with costs nearer to those of passive tags.

The main disadvantage of the semi-active RFID System is that they are more costly than the passive RFID tags.

2.6.4 Other Categories of RFID Systems (tags)

The RFID tags used are categorized by radio frequency in to four most common tags depending on their operation range [1]:

i. Low frequency tags (125 to 134.2 kHz)

ii. High frequency tags (<13.56 MHz)

iii. UHF tags (868 to 956 MHz)

iv. Microwave tags (<2.45 GHz)

2.6.4.1 The Low Frequency (LF) RFID tags

The characteristics of RFID systems at LF are:

i. Short read range (less than 0.5m)

ii. Low reading speed

iii. Very little absorption or reflection problems in the surrounding due to the presence of water or metal.

Applications of LF tags:

i. In access control

ii. In animal, personnel and asset tracking

2.6.4.2 The High Frequency (HF) RFID tags

These tags are used where medium data rate and read ranges up to about 1.5 meters are acceptable. This frequency also has the advantage of not being susceptible to interference from the presence of water or metals.
The characteristics include:

i. Read range of about 3 m.
ii. More problems to penetrate through materials
iii. Better data transfer speed.

Applications:

i. Building access control
ii. Item-level tracking and baggage handling
iii. Libraries.

2.6.4.3 The Ultra High Frequency (UHF) tags
They offer the longest read range of up to approximately 10 meters and a high reading speed. Their characteristics are:

i. They have a read range of about 10 m.
ii. They have a high probability of interferences (consumer devices).
iii. They have a higher probability for problems due to absorption by metals or matter.
iv. Their data transfer rate is high.
v. They have limited portability.

Applications of UHF tags include:

i. Automated toll collection
ii. Warehouse management
iii. Inventory tracking

2.6.4.4 The Microwave tags
They have:

i. A long read distance
ii. A high reading speed and data transfer rate
iii. Poor performance around water and metal

Applications:

In vehicle identification and automated toll collection
2.7 Interference Sources in RFID Systems

2.7.1 Collision
Interference due to collision occurs in three major ways [1]:-
   i. Tag-tag collision
   ii. Reader-tag collision
   iii. Reader-reader collision

2.7.1.1 Tag-tag collision
It occurs in the interrogation zone of a single reader where the signals of each tag cancel out and weak communication occurs between the reader and the tag. Tag-tag collision is shown in Fig. 2.3

![Fig 2.3 A block diagram showing tag-tag collision](image)

2.7.1.2 Reader-tag collision
Reader-to-tag interference occurs when one tag is simultaneously located in the interrogation zones of two or more readers and more than one reader attempts to communicate with that tag at the same time. In this type of interference, each reader may believe it is the only reader communicating with the tag while the tag is in fact communicating with multiple readers at the same time. The simple nature of RFID communication can cause the tag to behave and
communicate in such an undesirable way to interfere with the communicating readers’ capabilities to communicate with that tag and other tags in their respective interrogation zones.

The reader is unable to differentiate these signals, leading to a phenomenon known as tag collision. A tag can listen to any reader in its vicinity, but it can however, communicate with only one reader at a time, and only if the signal arriving from that one reader is stronger than other signals. If a tag is close to one reader and far from another, it will have no trouble communicating with the nearby reader. But when the tag is almost equidistant to both readers, interference is more likely to occur. This collision reduces the system’s performance by producing a delay in the identification. However, some tags leave the interrogation zone unidentified. The TLR (tag loss ratio) determines the unidentified tags and items. Fig 2.4 shows reader-tag collision.

![Fig 2.4 A block diagram of reader tag collision](image)

2.7.1.3 Reader-reader collision

This type of interference occurs when the signal transmitted by a reader is of sufficient strength and is received at a second reader that the signal masks or jams communication from tag to the second reader. Interrogation zones will not be needed to have an overlap for reader-to-reader interference to occur. Reader-to-reader interference occurs when a reader transmits a signal that interferes with the operation of another reader, thus preventing the second reader from communicating with tags in its interrogation zone. It occurs when multiple readers are configured to work within the same frequency band. Reader jamming is inherently more problematic, because it can involve readers that are quite far away relative to the tag. Mitigating factors for reader jamming include using well-designed readers, proper selection of reader mode,
channel-use randomization, shielding the reader, and the appropriate selection of reader antennas for the application.

2.7.2 Presence of a Radio Frequency Absorbing Material in Path
The path-loss through dense materials is greater than through free air and therefore a tag within the vicinity of RF-absorbing material is less likely to receive enough power from a reader far away from the material and cause interference. The existence of the material on the surrounding increases the effective distance between the two readers, which results in smaller dead zones [2].

2.7.3 Electromagnetic Interference (EMI)
This occurs when radio waves of one device or from an external source interfere with the radio waves of the tag [1]. Sources of such radio waves include; an electrical circuit, wireless computers and electromechanical devices.

Radiated electromagnetic interference may be classified as narrow band or broad band. Narrow band interference results due to intentional transmission such as from radio and television stations. Broad band interference is caused by incidental radio frequency emitters such as electric power transmission lines.

2.7.4 Harsh environmental conditions
Harsh causes adverse effects that can affect tag detection in the following ways:-
   i. Extreme temperatures can damage tags, causing them to fail.
   ii. Some materials in the environment can cause interference by reflection, diffraction and scattering, which hinder the reader from communicating with the tag properly.
   iii. Tags can be damaged by mishandling the tagged items.
   iv. Material of the package surface can affect the reading of the tag.
   v. Shadowing effect created by the dense tag environment prevents tag from being read by the reader.

2.7.5 Improper Placement of Tags
Improperly placed tags such as folded tags or wrongly oriented tags cannot be detected by the reader.
2.7.6 Physical Obstructions
They block the communication path between interrogator and reader creating adverse effects such as absorption, reflection and scattering.

2.7.7 Transmission Channel Noise
Noise may be defined as an unwanted form of energy which tend to interfere with the proper reception and reproduction of transmitted signals[3]. There are several sources of noise in a communication system and these include:

- White noise
- Shot noise
- Thermal noise

White noise:- is a random process with a flat power spectral density. This signal contains equal power within a fixed bandwidth that any center frequency

Shot noise:- occurs in active devices due to the random behavior of charge carriers.

Thermal noise: - is usually generated in a resistive component due to rapid and random motion of the electrons in it. This noise is temperature depended and increases with temperature.
CHAPTER 3: INTERFERENCE CANCELLATION

3.1 Interference Cancellation Techniques in RFID Systems

3.1.1 Synchronization
All the readers across an entire location can be synchronized such that potential interferers are not powered at the same time. In a multiple-reader portal, synchronization of antennas ensures that only one is powered at any given time [2].

The disadvantage of synchronization is that it slows down operation because of the reduction in parallelism and synchronization schemes are expensive. Deterministic synchronization can also have the unwanted effect of repeating a sequence of dead-zones so that, in a static application, some tags may never be read.

3.1.2 Error Correcting Codes (ECC)
When product data is placed on an RFID tag, a special piece of data called an error correcting code is created based on the product data using a known algorithm. The algorithm (or rule) used to create the correcting code is called the error correcting protocol. When the tag is activated and read, the reader pulls out the product data as well as the ECC. The reader uses the error correcting protocol on the product data, and compares the result to the ECC. If they match, the reader knows that the data has been read correctly. Similar methods are used in most data transfer systems to ensure the correctness of each data package as it moves from one part of the system to another. A reader that performs this check automatically is said to be in error correcting mode.

3.1.3 The Active Jamming Approach
Active jamming of RF signals increases consumer privacy by shielding the tags. The consumer usually carries a device that actively broadcasts radio signals which blocks the operation of any nearby RFID readers. This method is however not legal in many cases as it can cause severe disruption of all the nearby RFID systems. The regions where tags are jammed are known as dead zones. If the readers are far enough apart, the dead zone lies outside of the read range of the tag. But if they are close together, the dead zone can fall inside a read zone.
A Tag jamming is primarily related to transmission power levels and the proximity of readers, and is a function of transmitter frequency. The impact of tag jamming on a system’s performance depends on: the design of the tag’s chip, the presence of any RF-absorbing material in the communication path, channel frequency selection, the sequencing of the reader antennas, and the type of tag antenna.

3.1.4 Increasing Power and Path-Loss
Increasing path losses by shielding or lowering the reader transmission level decreases the strength of interfering signals from adjacent readers. This approach is especially useful in situations where the read zone never changes, such as in RFID for item-level applications using conveyor belts. Also interference cancellation can be attained by removing the source of interference by ensuring that any electronic appliance that can cause interference does not operate in the interrogation zone.

3.1.5 Use of digital Filters
Filters can be used to allow only selected frequencies to pass through a connected device or tag. Filtering is a process by which the frequency spectrum of a signal can be modified, reshaped or manipulated to achieve some desired objectives [3]. The major objectives of filtering include: - elimination of noise in contaminated signals, removing signal distortion due to imperfect transmission channel, demodulation of the signals which were modulated at the transmitter end converting digital signals into analog signals and limiting the bandwidth of the signals.

Digital filters are built using adders, multipliers and delay elements. They are broadly classified as the FIR and IIR filters

Finite Impulse Response filters (non-recursive filters) contain the feed forward path only. The output is a weighted sum of the present input and a number of the previous sample of the input. A FIR filter is shown in Fig 3.1.
The difference equation is given by:

\[ y[n] = b_0 x[n] + b_1 x[n-1] + \cdots + b_m x[n-m] \] 3.1

Infinite Impulse Response filters (recursive filter) contain both the feed forward and feedback paths. The output is a weighted sum of the present input and a number of previous samples of the input and output. Fig 3.2 shows an IIR filter.

\[ y[n] = a_0 y[n-1] + a_1 y[n-2] + \cdots + a_m y[n-m] \] 3.2
The advantage of IIR filters is that they are economical in their use of adders, multipliers and delay elements as compared to the FIR filters. However, the FIR filters are more stable, and do not have recursive errors.

### 3.1.6 Anti-collision

This involves different ways used to shield radio waves from one device from interfering with radio waves from another device. Anti-collision can be achieved by using multiple access techniques such as [1]:-

i. Frequency Division Multiple Access (FDMA)

ii. Time Division Multiple Access (TDMA)

iii. Space Division Multiple Access (SDMA)

iv. Coded Division Multiple Access (CDMA)

RFID readers may make use of anti-collision algorithms to enable a single reader to read more than one tag in the reader's field.

#### 3.1.6.1 Time Division Multiple Access (TDMA) based schemes

The channel is divided into different time slots that are assigned to different users. The only limitation is that the users must be synchronized to send signal information in the selected slot. The reader and tag communication uses the same frequency in the same read range, and each tag's response is differentiated by the time interval that it used.

#### 3.1.6.2 Code Division Multiple Access (CDMA) based schemes

TDMA based anti-collision schemes can only retrieve one tag's ID at one time slot. The CDMA technology has been extensively used in many modern communication systems because it allows multiple communications to coexist in the same medium using the same time and frequency resources.

#### 3.1.6.3 Space Division Multiple Access (SDMA) based schemes

In this method the available channels are divided in spatial domain and thus the system can increase the channel capacity of the same frequency and the same time slot. Generally the SDMA scheme separates the coexisting transmission sources via the angle of arrival (AOA) of each signal source. The read range is reduced and an array of antennas is formed which provides
a large coverage area. The limitation of this technique is that it has a complicated array of antennas.

3.1.6.4 Frequency Division Multiple Access (FDMA) based scheme

In this technique the channel bandwidth is divided among several simultaneous users such that each user is allocated a channel with a small bandwidth. The limitation of this technique is that it can only be applied in active RFID systems because they can distinguish different frequencies. This scheme allows a number of transmission channels to work together at the same time by using different operating frequencies since in a passive RFID system, the signal from the reader is send in some operating frequencies to provide power to activate the passive tags. The tag receives the power from the reader’s signal and also utilizes the signal as the carrier of its modulated backscatter signals.

3.1.7 Proper Tag and Reader Chip Design

The design of the tag chip influences its ability to reliably receive signals. RFID chips can be well designed to include interference rejection and decrease the size of dead zones. Tags can be designed to have good interference rejection, such that they can receive power from more than one reader and still communicate effectively with the reader of interest. Smaller dead zones results to less time that tags will be inaccessible when they move through a multiple-reader system.

The tag antenna should be designed in such a way that it is able to minimize loss of the power provided by the antenna. The power available at the tag could be obtained by using the Friis EM wave propagation Equation 3.3 in free space [4]

\[
\frac{P}{P_0} = \frac{A}{r \lambda}
\]

Where:
- \( P \) is the received power by the tag
- \( P_0 \) is the transmitted power by the reader
- \( A \) is the effective aperture of the receiving antenna
- \( A \) is the effective aperture of the transmitting antenna
- \( r \) is the distance between the receiving and transmitting antennas
\( \lambda \) is the wavelength

The **Signal to Noise Ratio** is determined by Equation 3.4

\[
\text{SNR} = \frac{p}{r \lambda BkT}
\]  

(3.4)

Where; \( B \) is the bandwidth

\( K \) is the Boltzmann constant=1.38 \times 10^{-23} \text{ JK} 

\( T \) is the system temperature

To reduce interference on the reader side interference rejection is designed into the reader itself.

The effective aperture is obtained by using Equation 3.5

\[
A = \frac{P}{S} = \frac{V}{4SR}
\]  

(3.5)

Where \( P \) is the received power

\( R \) is the radiation resistant

\( S \) is the pointing vector

\( V \) is the supplied voltage

3.1.8 **The “Kill Tag” approach**

In this approach protection of consumer privacy is attained by “killing” RFID tags before they are placed in the hands of consumers [1]. The killed tag can never be re-activated. The standard mode of operation proposed by the Auto ID Center was for tags to be killed upon purchase of the tagged product. A tag can be killed by sending it a special “kill” command. For example; a supermarket might use RFID tags to facilitate inventory management and monitoring of shelf stocks. To protect consumer privacy, checkout clerks would “kill” the tags of purchased goods such that no purchased goods would contain active RFID tags.

This approach however, has a number of limitations; there are many environments in which the “kill” commands are non-workable or undesirable for privacy enforcement.
Some consumers may wish RFID tags to remain operative while in their possession such as microwave oven that reads cooking instructions from food packages. Other applications in which the tag cannot be killed include the following:

i. Stores may wish products to have tags re-scanned if the products are returned as defective.

ii. Products may need to be scanned so they may be categorized for recycling purposes.

iii. Stores may issue receipts with embedded RFID tags, so they can confirm purchase details when a product is returned.

iv. Individuals may wish to have RFID tags embedded in their business cards, to facilitate scanning by recipients. Here the tag ID may be used to create a URL referring to the actual card data.

v. A store may wish to embed RFID tags in store-issued coupons, for ease of scanning at the checkout counter.

vi. A user may wish to scan his possessions when a recall for a specific set of products is issued.

vii. A merchant may wish to scan consumers for marketing purposes.

viii. A refrigerator may be able to tell when some food or drug product has passed its expiry date.

ix. An airline ticket may contain an embedded RFID tag to allow simpler tracking of passengers within an airport.

x. Businesses may include RFID tags on the invoices, coupons, and return envelopes they mail to consumers, for ease of sorting upon return.

Individuals may also be secretly given tags so they can be tracked or identified by an overzealous merchant, by a private detective, by a spouse, parent, or other relative. Thus, while the "kill-tag on purchase" approach may handle many or even most instances of potential concern for privacy, it is unlikely to be a fully satisfactory solution.

### 3.1.9 The Faraday Cage Approach

A Faraday Cage is a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). It is used to shield the RFID tags or readers from interference. The limitation of this method is that a vast range of object cannot be placed conveniently in the
containers, such as human beings. Thieves have been known to use metal-foiled bags to prevent detection.

3.1.10 The “Hash Lock” Approach

In this approach, due to Weis et al, a tag maybe locked so that it refuses to reveal its ID until it is unlocked. When the tag is locked it is given a value/meta-ID and it is only unlocked by presentation of a key or PIN value x such that y = h(x) for a standard one-way hash function h. In supermarkets, tags may be locked at check out time. A consumer could provide a meta-ID y for the tags and then transmit the unlocking PIN x via some special device to unlock tags on returning home. To make this approach workable, it may be necessary for a reader to query a tag to find its meta-ID, so that the reader knows which PIN to use to unlock it. But this may allow tracking of tags via their meta-IDs, defeating their whole purpose. Weis et al. show how to use randomization in the hash function computation to solve this problem. While this is an effective approach, it seems likely that consumers will find it inconvenient to manage the lock/unlock patterns and associated PINs of more than a small collection.

3.1.11 The Encryption Approach

Encryption is a process of protecting the privacy and authentication of information in a hostile environment by converting information so that it is only intelligible only to the people who can decrypt it to obtain the original message [5]. Encryption techniques can be categorized as symmetric or asymmetric. The symmetric techniques are unsecure since any person who knows how to encrypt the information is able to decrypt it. Asymmetric techniques are more secure such as the Public Key Cryptography (PKC) which involves the use of both a private and a public key. Encryption done using a public key can only be decrypted by only the people with the private key and information encrypted using a private key can be decrypted by people with only the public key. The disadvantage of asymmetric encryption is that it is slower than symmetric encryption.

Symmetric encryption involves taking the original message and converting it into cipher text using an encryption algorithm. For instance if the original message was; "Department of
Electrical Engineering encryption can be done using an encryption algorithm that replaces each letter with that at X places to the right of it.

If X=5, the encrypted text would be: ñjufwyrjs tk Jqjhywnhfq Jslnsijwnsl

To convert the encrypted message back to the original message, a decryption algorithm is used. It is done by replacing each letter with the letter five places to the left of it in the alphabet. Main encryption methods are based on transposition ciphers, substitution ciphers and XOR operation ciphers. In substitution ciphers, each letter is replaced by another letter or a group of letters to disguise it. In complex encryption key controlled mapping of one letter to another is done. Poly-alphabet substitution is mostly used because it is more secure than mono-alphabet substitution.

In transposition ciphers the plain text is written in rows under the key which numbers the formed columns. Modern encryption is done using software which is used to provide secure communication over open networks such as Wi-Fi Protected Access (WPA2) which is used to encrypt data send over wireless communication.

The security of the encrypted data depends on the choice of the algorithm and the key length. An encryption key can contain bit lengths of 56, 64 or 128 bits. A key with more bits cannot be easily decrypted. The disadvantage with encryption techniques of interference cancellation is that criminals can use encryption to secure their communication.
4.1 Design

The design was based on the operation of a typical RFID system summarized as shown in Fig 4.1.

**Fig 4.1:** Operation of a typical RFID system
4.1.1 **Interference Cancellation Design using an Adaptive Filter**

An adaptive filter removes noise from a signal by adapting the filter weights. Fig 4.2 shows an adaptive filter.

![Fig 4.2 An adaptive filter](image)

Adaptive filtering was done to the demodulated signal from the reader antenna. This removed noise from the signal in real time. During the noise cancellation process, the desired signal (the one to clean up) combined noise and the desired information. To remove the noise, a signal $n(k)$ which represents noise that is correlated to the noise to be removed from the desired signal was fed to the filter. The filter adjusted its coefficients to reduce the value of the difference between $y[k]$ and $d[k]$ resulting into a clean signal, $e[k]$. Thus the error signal converged to the input signal rather than to zero [6, 7].

The diagram in Fig 4.3 shows a block diagram of the adaptive filter as used in the design.
Fig 4.3 A block diagram of an adaptive filter

Where; $W_k$ was the weights of the adaptive filter as shown in Equation (4.1)

$$W_k = W_0, W_1, ..., W_n$$  \quad 4.1

$d(k)$ was the contaminated signal with both the desired signal and the noise $n(k)$

$$d[k] = s[k] + n[k]$$  \quad 4.2

$p(k)$ was the measure of the contaminated signal, which is correlated with the noise to produce $y(k)$ which was the approximated noise.

$$y[k] = p[k] W_k$$  \quad 4.3

The filter approximation of the desired signal was obtained as shown in equation (4.4)

$$e[k] = d[k] - y[k]$$  \quad 4.4
4.1.2 Simulink Design using a NLMS Adaptive Filter

The design was done using the Normalized Least Mean Square (LMS) algorithm which was used to vary the weights of the adaptive filter as the input signal was varying. Recursive Least Square (RLS) algorithm could also have been used but it has a limitation in that it has computational complexity and suffers stability problems. However using Adaptive Filtering with Averaging (AFA) algorithm could remove these limitations [8].

![Simulink diagram](image)

**Fig 4.3 Interference cancellation design using an adaptive filter (NMLS)**

Noise cancellation was achieved by adapting the filter coefficient with the normalized least-mean-square algorithm (NLMS) according to the filter order. The algorithm adapted the filter coefficients in order to obtain the desired signal by converging the filter output.

4.1.2.1 Block parameters
Block 1- **The sine wave signal generator** was set to produce a sine wave of amplitude 15 and frequency 880 MHZ. The sampling time was determined using the Nyquist sampling rate [3] as shown by Equation 4.5
\[
Fs = 2Fm
\]
(4.5)

\[
Ts = \frac{1}{Fs}
\]
(4.6)

Where; Fm is the message signal
Ts is the sampling time
Fs is the sampling frequency

But Fm = 880MHZ
Therefore, Fs=2(880) MHZ=1760MHZ

\[
Ts = \frac{1}{Fs} \approx 5.68 \times 10^{-7} \text{ S}
\]
(4.7)

The signal was sampled at Nyquist rate because sampling at a frequency lower than the Nyquist rate causes errors called aliasing. This causes loss of the high frequency components of the signal.

Block 2 - The random source generator was set to be Gaussian type with a signal mean of 0 and a variance of 1.0
The sample time was set to as 5.68 \times 10^{-7} \text{ S}

Block 3 - The digital filter was designed with the sampling frequency set to 1760MHZ and the cut-off frequency set to 300MHZ.

Block 4 - The NLMS adaptive filter was designed with the step size (mu) =0.1 and the initial filter weights were set to 0. The filter length (order) was varied to obtain proper noise cancellation.

Block 5 - The Scope was used to display the noise cancellation process.

Block 6 - The time scope was used to display the adaptation in filter weights.

Block 7 - The display was used to measure the mean square error.
4.2 Implementation

The implementation of the design was done using Real time workshop and the generated code was shown in Appendix I.
CHAPTER 5: RESULTS AND DISCUSSIONS

5.1 Results

NLMS adaptive filter was used to improve the error performance of a RFID system. The most suitable filter order for interference cancellation for UHF RFID systems (at 880MHZ frequency) was determined by estimation to be 96 as shown by the graph in appendix H. Results obtained from other filter orders were as shown in appendices B, C, D, E, F and G. Fig 5.0 and Fig 5.1 shows the results obtained from the filter of order 96 and the adaptation in filter weights.

![Graph showing adaptive filter results](image_url)

**Fig 5.0** Time scope display of the adaptive filter results
Fig 5.1 Vector scope display of the adjustment in filter weights

5.2 Discussions

The desired solution range was not reached during the convergence for the filter of orders; 50, 85, 90, 100,120 and 300, a local minimum was instead reached allowing no further convergence which resulted in poor performance as shown by the results in appendices B, C, D, E, F and G. The filter output error could not be further minimized. Therefore a proper filter order was to be set. It was also necessary to adjust the filter order because noise mixing is depended on the environment. The filter order was varied using the estimation method inorder to adjust the convergence constant and to readapt it. The appropriate order was estimated to be 96. It was further observed that higher filter ordering caused distortions of the original signal as shown by appendix G. This was because the error signal did not converge to the input data signal.
CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

RFID systems were found to be categorized into three major types: - Active systems, Passive systems and Semi-passive systems. The main source of noise was determined to be the transmission channel noise (AWGN). Other sources of interference were; Tag-tag collision, tag-reader collision, reader-reader collision, EMI, harsh environmental conditions such as extreme temperatures, improper placement of tags and presence of RF absorbing materials in the transmission path.

Interference could be minimized by reader Synchronization, Error Correcting Coding, the Active Jamming Approach, digital filtering, Anti-collision, the ‘Kill Tag’ Approach, the ‘Hash Lock’ Approach and the Encryption Approach.

In the project, noise cancellation was achieved using an adaptive NLMS filter of order 96. The scope display in appendices B, C, D, E, F and G was used to approximate that the filter order that gave the best noise performance was between the filters of order 85 and 100. The exact filter order was estimated by using the results in appendix H where it was found that the average mean square error of the filter was lowest for a filter of order 96. Higher filter ordering caused distortions to the approximated signal as shown by appendix G.
6.2 Recommendation for Future Work

Even though the objectives of this project were achieved, the design and the implementation were done by software simulation. In future resources should be availed for a hardware design and implementation.
6.3 APPENDICES

APPENDIX A

Basic differences between passive and active RFID systems

<table>
<thead>
<tr>
<th>ACTIVE RFID SYSTEMS</th>
<th>PASSIVE RFID SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Operate on battery</td>
<td>Are battery less</td>
</tr>
<tr>
<td>2 Are more expensive</td>
<td>Are less expensive</td>
</tr>
<tr>
<td>3 Have limited life</td>
<td>Unlimited life</td>
</tr>
<tr>
<td>4 Heavier in weight</td>
<td>Light in weight</td>
</tr>
<tr>
<td>5 Longer read range of about 100m</td>
<td>Shorter read range of about 3-6 m</td>
</tr>
<tr>
<td>6 Better noise immunity</td>
<td>Subject to noise</td>
</tr>
<tr>
<td>7 Uses internal power to transmit</td>
<td>Derive power from EM field generated by</td>
</tr>
<tr>
<td>signal</td>
<td>the reader</td>
</tr>
<tr>
<td>8 Effective with less powerful readers</td>
<td>Require powerful readers</td>
</tr>
<tr>
<td>9 High data transmission rate</td>
<td>Low data transmission rate</td>
</tr>
<tr>
<td>10 More tags can be read simultaneously</td>
<td>Few tags can be read simultaneously</td>
</tr>
<tr>
<td>11 Less orientation sensitivity</td>
<td>Greater orientation sensitivity</td>
</tr>
</tbody>
</table>
APPENDIX B

Appendix B shows the results obtained for a filter of order 50

Time scope display of the results of Adaptive Filter of Order 50

Adaptation in Filter Weights
APPENDIX C

Appendix C shows the results obtained from a filter of order 85

Time scope display of the results of Adaptive Filter of Order 85

Adaptation in Filter Weights
Appendix D shows the results obtained from a filter of order 90.
APPENDIX E

Appendix E shows the results obtained from a filter of order 100.
APPENDIX F

Appendix F shows the results obtained from a filter of order 120

![Time scope display of the results of Adaptive Filter of Order 120](image)

![Adaptation in Filter Weights](image)
APPENDIX G

Appendix G shows the results obtained from a filter of order 300

Time scope display of the results of Adaptive Filter of Order 300

Adaptation in Filter Weights
## APPENDIX H

<table>
<thead>
<tr>
<th>FILTER ORDER</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>85</td>
<td>0.000477</td>
<td>0.004085</td>
<td>0.006397</td>
<td>0.03579</td>
<td>0.011687225</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>0.03682</td>
<td>0.01682</td>
<td>0.007867</td>
<td>0.007796</td>
<td>0.01732575</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>0.001532</td>
<td>0.01027</td>
<td>0.000501</td>
<td>0.01787</td>
<td>0.007543275</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>0.0041</td>
<td>0.001849</td>
<td>0.007921</td>
<td>0.008797</td>
<td>0.00566675</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>0.002027</td>
<td>0.000244</td>
<td>0.02926</td>
<td>0.003592</td>
<td>0.008780625</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>0.002527</td>
<td>0.0287</td>
<td>0.01029</td>
<td>0.01369</td>
<td>0.01380175</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>0.008805</td>
<td>0.02469</td>
<td>0.01493</td>
<td>0.002942</td>
<td>0.01284175</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>0.02199</td>
<td>0.01027</td>
<td>0.00951</td>
<td>0.01142</td>
<td>0.0132975</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>0.005894</td>
<td>0.007794</td>
<td>0.01667</td>
<td>0.007567</td>
<td>0.00948125</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>0.01071</td>
<td>0.0362</td>
<td>0.01817</td>
<td>0.004257</td>
<td>0.01733425</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>0.00287</td>
<td>0.001676</td>
<td>0.004951</td>
<td>0.001147</td>
<td>0.002661</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>0.000207</td>
<td>0.001676</td>
<td>0.004951</td>
<td>0.0121</td>
<td>0.00473355</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>0.003928</td>
<td>0.003123</td>
<td>0.002158</td>
<td>0.007495</td>
<td>0.004176</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>0.005311</td>
<td>0.00096</td>
<td>0.006642</td>
<td>0.005169</td>
<td>0.0045204</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>0.005452</td>
<td>0.0132</td>
<td>0.003771</td>
<td>0.007992</td>
<td>0.00760375</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A graph of average MSE versus Filter order
APPENDIX I

The code generated by the real time workshop was as follows:

```
#include "final.h"
#include "final_private.h"

BlockIO_final final_B;
DWork_final final_DWork;
RT_MODEL_final final_M;
RT_MODEL_final *final_M = &final_M;
static void final_output(int_T tid)
{
    const real_T updateVal = final_P.SineWave_Frequency*3.568492544780050E-009;
    real_T *accFrqNrm = &final_DWork.SineWave_AccFreqNorm;
    final_B.SineWave = final_P.SineWave_Amplitude * sin(*accFrqNrm);
    *accFrqNrm += updateVal;
    if (*accFrqNrm >= 6.2831853071795862E+000) {
        *accFrqNrm -= 6.2831853071795862E+000;
    } else if (*accFrqNrm < 0.0) {
        *accFrqNrm += 6.2831853071795862E+000;
    }
}

MWDSP_RandSrc_GZ_D((real64_T *)&final_B.RandomSource,(real64_T *)
    &final_P.RandomSource_MeanRTP,1,
    &final_P.RandomSource_VarianceRTP,1,
    &final_DWork.RandomSource_STATE_DWORK[0],1,1);

{
    real_T *inputs = (real_T *)&final_B.RandomSource;
    real_T *outputs = (real_T *)&final_B.DigitalFilter;
    real_T *coeffs = (real_T *)&final_P.DigitalFilter_RTP1COEFF[0];
    real_T *scaleVals = (real_T *)&final_P.DigitalFilter_RTP2COEFF[0];
    real_T *states = (real_T *)
        &final_DWork.DigitalFilter_FILT_STATES[0];
    real_T stageIn, stageOut;
    int_T j;
    stageIn = inputs[0] * scaleVals[0];
    for (j = 0; j < 16; j++) {
        int_T memIdx = 2 * j;
        int_T coeffIdx = 5 * j;
        int_T numIdx = coeffIdx;
        int_T denIdx = numIdx + 3;
        stageIn -= coeffs[denIdx] * states[memIdx];
        stageIn -= coeffs[denIdx+1] * states[memIdx+1];
        stageOut = coeffs[numIdx] * stageIn;
        stageOut += coeffs[numIdx+1] * states[memIdx];
        stageOut += coeffs[numIdx+2] * states[memIdx+1];
        states[memIdx+1] = states[memIdx];
        states[memIdx] = stageIn;
        stageIn = stageOut * scaleVals[j+1];
    }
```
outputs[0] = stageIn;
}

final_B.Sum = final_B.SineWave + final_B.DigitalFilter;
{
    MWDSP_lmsn_an_wy_DD(
        (const real_T*)&final_B.RandomSource,
        (const real_T*)&final_B.DigitalFilter,
        (const real_T)((real_T*)final_P.LMSFilter_MU_RTP),
        (uint32_T)(real_T*)final_DWork.LMSFilter_BUF_IDX_DWORK,
        (real_T*)final_DWork.LMSFilter_IN_BUFF_DWORK[0],
        (real_T*)final_DWork.LMSFilter_WGT_IC_DWORK[0],
        (int_T)96,
        (const real_T)/*(real_T*)
        &final_P.LMSFilter_LEAKAGE_RTP),
        (int_T)1,
        (int_T)sizeof(real_T),
        (real_T*)final_B.LMSFilter_o1,
        (real_T*)final_B.LMSFilter_o2,
        (real_T*)final_B.LMSFilter_o3);
}

final_B.Sum1 = final_B.Sum - final_B.LMSFilter_o1;
{
    StructLogVar *svar = (StructLogVar *)final_DWork.Scope_PWORK.LoggedData;
    LogVar *var = svar->signals.values;
    double locTime = final_M->Timing.t[0];
    rt_UpdateLogVar((LogVar *)svar->time, &locTime, 0);
}

real_T up0[1];
up0[0] = final_B.SineWave;
rt_UpdateLogVar((LogVar *)var, up0, 0);
var = var->next;
}

real_T up1[1];
up1[0] = final_B.Sum;
rt_UpdateLogVar((LogVar *)var, up1, 0);
var = var->next;

{
  real_T up2[1];
  up2[0] = final_B.Sum1;
  rt_UpdateLogVar((LogVar *)var, up2, 0);
  var = var->next;
}

{
  real_T up3[1];
  up3[0] = final_B.LMSFilter_o2;
  rt_UpdateLogVar((LogVar *)var, up3, 0);
}

UNUSED_PARAMETER(tid);
}

static void final_update(int_T tid)
{
  if (!(++final_M->Timing.clockTick0))
    ++final_M->Timing.clockTickH0;
  final_M->Timing.t[0] = final_M->Timing.clockTick0 * final_M->Timing.stepSize0
    + final_M->Timing.clockTickH0 * final_M->Timing.stepSize0 * 4294967296.0;
  UNUSED_PARAMETER(tid);
}

void final_initialize(boolean_T firstTime)
{
  (void)firstTime;
  rt_InitInfAndNaN(sizeof(real_T));
  (void)memset((char_T *)final_M,0,
    sizeof(RT_MODEL_final));

  {
    int_T *mdlTsMap = final_M->Timing.sampleTimeTaskIDArray;
    mdlTsMap[0] = 0;
    final_M->Timing.sampleTimeTaskIDPtr = (&mdlTsMap[0]);
    final_M->Timing.sampleTimes = (&final_M->Timing.sampleTimesArray[0]);
    final_M->Timing.offsetTimes = (&final_M->Timing.offsetTimesArray[0]);
    final_M->Timing.sampleTimes[0] = (5.68E-010);
    final_M->Timing.offsetTimes[0] = (0.0);
  }
  rtmSetTPtr(final_M, &final_M->Timing.tArray[0]);

  {
    int_T *mdlSampleHits = final_M->Timing.sampleHitArray;
    mdlSampleHits[0] = 1;
    final_M->Timing.sampleHits = (&mdlSampleHits[0]);
  }
  rtmSetTFinal(final_M, 9.99964E-006);
  final_M->Timing.stepSize0 = 5.68E-010;
}
{ static RTWLogInfo rt_DataLoggingInfo;
    final_M->rtwLogInfo = &rt_DataLoggingInfo;
    rtiSetLogXSignalInfo(final_M->rtwLogInfo, NULL);
    rtiSetLogXSignalPtrs(final_M->rtwLogInfo, NULL);
    rtiSetLogT(final_M->rtwLogInfo, "tout");
    rtiSetLogX(final_M->rtwLogInfo, "");
    rtiSetLogXFinal(final_M->rtwLogInfo, "");
    rtiSetSigLog(final_M->rtwLogInfo, "");
    rtiSetLogVarNameModifier(final_M->rtwLogInfo, "rt_");
    rtiSetLogFormat(final_M->rtwLogInfo, 1);
    rtiSetLogMaxRows(final_M->rtwLogInfo, 1000);
    rtiSetLogDecimation(final_M->rtwLogInfo, 1);
    rtiSetLogY(final_M->rtwLogInfo, "");
    rtiSetLogYSignalInfo(final_M->rtwLogInfo, NULL);
    rtiSetLogYSignalPtrs(final_M->rtwLogInfo, NULL);
}

final_M->solverInfoPtr = (&final_M->solverInfo);
final_M->Timing.stepSize = (5.68E-010);
rtsiSetFixedStepSize(&final_M->solverInfo, 5.68E-010);
rtsiSetSolverMode(&final_M->solverInfo, SOLVER_MODE_SINGLETASKING);
final_M->ModelData.blockIO = (void *) &final_B;

{ int_T i;
  void *pVoidBlockI0Region;
  pVoidBlockI0Region = (void *)&final_B.SineWave;
  for (i = 0; i < 103; i++) {
    ((real_T*)pVoidBlockI0Region)[i] = 0.0;
  }
}

final_M->ModelData.defaultParam = ((real_T *) &final_P);
final_M->Work.dwork = ((void *) &final_DWork);
(void) memset((char_T *) &final_DWork, 0,
              sizeof(D_Work_final));

{ int_T i;
  real_T *dwork_ptr = (real_T *) &final_DWork.SineWave_AccFreqNorm;
  for (i = 0; i < 225; i++) {
    dwork_ptr[i] = 0.0;
  }
}

void final_terminate(void)
{
}

void MdlOutputs(int_T tid)
{
  final_output(tid);
}
void MdlUpdate(int_T tid)
{
    final_update(tid);
}

void MdlInitializeSizes(void)
{
    final_M->Sizes.numContStates = (0);
    final_M->Sizes.numY = (0);
    final_M->Sizes.numU = (0);
    final_M->Sizes.sysDirFeedThru = (0);
    final_M->Sizes.numSampTimes = (1);
    final_M->Sizes.numBlocks = (8);
    final_M->Sizes.numBlockIO = (8);
    final_M->Sizes.numBlockPrms = (104);
}

void MdlInitializeSampleTimes(void)
{
}

void MdlInitialize(void)
{
    {
        const real_T tNorm = (real_T)(final_M->Timing.t[0] / 5.68E-010);

        real_T arg = final_P.SineWave_Phase;
        arg += (final_P.SineWave_Frequency * tNorm *
                6.2831853071795862E+000);
        while (arg >= 6.2831853071795862E+000)
            arg -= 6.2831853071795862E+000;
        while (arg < 0.0)
            arg += 6.2831853071795862E+000;
        final_DWork.SineWave_AccFreqNorm = arg;
    }

    {
        int_T i;
        for (i = 0; i < 32; i++) {
            final_DWork.DigitalFilter_FILT_STATES[i] = final_ConstP.pooled1;
        }
    }

    {
        int_T i;
        for (i = 0; i < 96; i++) {
            final_DWork.LMSFilter_WGT_IC_DWORK[i] = final_ConstP.pooled1;
        }
    }
}

void MdlStart(void)
{
    {
    
}
real_T arg = final_P.SineWave_Phase;
while (arg >= 6.2831853071795862E+000)
    arg -= 6.2831853071795862E+000;
while (arg < 0.0)
    arg += 6.2831853071795862E+000;
final_DWork.SineWave_AccFreqNorm = arg;
}

uint32_T *seeds = &final_DWork.RandomSource_SEED_DWORK;
const uint32_T initSeeds = (uint32_T) (rand()*100000);
MWDSP_RandSrcCreateSeeds_64(initSeeds,seeds,1);
MWDSP_RandSrcInitState_GZ(seeds,&final_DWork.RandomSource_STATE_DWORK[0],1);

RTWLogSignalInfo rt_ScopeSignalInfo;
static int_T rt_ScopeSignalWidths[] = { 1, 1, 1, 1 };  
static int_T rt_ScopeSignalNumDimensions[] = { 2, 2, 2, 2 };  
static int_T rt_ScopeSignalDimensions[] = { 1, 1, 1, 1, 1, 1, 1, 1 };  
static char_T *rt_ScopeSignalLabels[] = { "", "", "", "" };  
static char_T rt_ScopeSignalTitles[] =  
"ORIGINAL TAG SIGNALORIGINAL TAG SIGNAL WITH NOISEAPPROXIMATED  
ORIGINAL SIGNALAPPROXIMATED NOISE SIGNAL";
static int_T rt_ScopeSignalTitleLengths[] = { 19, 30, 28, 25 };  
static boolean_T rt_ScopeSignalIsVarDims[] = { 0, 0, 0, 0 };  
static int_T rt_ScopeSignalPlotStyles[] = { 1, 1, 1, 1 };  
BuiltInDTypeId dTypes[4] = { SS_DOUBLE, SS_DOUBLE, SS_DOUBLE, SS_DOUBLE };  
static char_T rt_ScopeBlockName[] = "final/Scope";
rt_ScopeSignalInfo.numSignals = 4;
rt_ScopeSignalInfo.numCols = rt_ScopeSignalWidths;
rt_ScopeSignalInfo.numDims = rt_ScopeSignalNumDimensions;
rt_ScopeSignalInfo.dims = rt_ScopeSignalDimensions;
rt_ScopeSignalInfo.isVarDims = rt_ScopeSignalIsVarDims;
rt_ScopeSignalInfo.currSigDims = NULL;
rt_ScopeSignalInfo.dataTypes = dTypes;
rt_ScopeSignalInfo.complexSignals = NULL;
rt_ScopeSignalInfo.frameData = NULL;
rt_ScopeSignalInfo.labels.cptr = rt_ScopeSignalLabels;
rt_ScopeSignalInfo.titles = rt_ScopeSignalTitles;
rt_ScopeSignalInfo.titleLengths = rt_ScopeSignalTitleLengths;
rt_ScopeSignalInfo.plotStyles = rt_ScopeSignalPlotStyles;
rt_ScopeSignalInfo.blockNames.cptr = NULL;
rt_ScopeSignalInfo.stateNames.cptr = NULL;
rt_ScopeSignalInfo.crossMdlRef = NULL;
rt_ScopeSignalInfo.dataTypeConvert = NULL;
final_DWork.Scope_PWORK.LoggedData = rt_CreateStructLogVar(
    final_M->rtwLogInfo,
    rtmGetTFinal(final_M),
    final_M->Timing.stepSize0,
    (&rtmGetErrorStatus(final_M)),
    "ScopeData2",
    1,
    1000000,
    1,
    5.68E-010,
    &rt_ScopeSignalInfo,
    rt_ScopeBlockName);
if (final_DWork.Scope_PWORK.LoggedData == NULL)
    return;
}

MdlInitialize();

RT_MODEL_final *final(void)
{
    final_initialize(1);
    return final_M;
}

void MdlTerminate(void)
{
    final_terminate();
}
REFERENCES


[5] WWW.security.homeoffice.gov.uk

