USING CDMA/AIC TO INCREASE ENERGY EFFICIENCY AND REDUCE MULTIPATH EFFECTS IN PASSIVE RFID TAG SYSTEMS

by

Archita Satish Keni, B.S.

A thesis submitted to the Graduate Council of
Texas State University in partial fulfillment
of the requirements for the degree of
Master of Science
with a Major in Engineering
December 2019

Committee Members:

Harold Stern, Chair

William Stapleton

Semih Aslan

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

Duplication Permission

DEDICATION

This thesis is dedicated to my parents and all the professors who educated me. I am grateful for their prayers, blessings and time.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my thesis advisor **Dr. Harold Stern**, for the continuing encouragement, his support throughout my research and his guidance in carrying out this research. It is a genuine pleasure to work with him on this research. Dr. Stern has been always kind with his timely advice, scholarly suggestions and scientific approach that are mainly responsible to complete this research. He has inspired me to become an independent researcher and helped me realize the power of critical reasoning. I will forever be grateful to him.

I would also like to extend my deepest gratitude to my committee members **Dr. William Stapleton** who provided his expert suggestions and valuable insights. **Dr. Semih Aslan** who provided excellent suggestions in developing a presentable thesis. Without their passionate participation and input, the validation and evaluation of the results for this research could not have been successfully conducted. I am grateful for introducing me to all the possible challenges and methodologies during the proposal presentation to accomplish the goals of this research.

I am grateful to **Dr. Vishu Viswanathan**, the graduate advisor of Ingram School of Engineering. His valuable suggestions and commitment to achieve high standards motivated me in all the positive ways throughout my journey at Texas State University.

Finally, I am extremely grateful to my father, Satish Keni for supporting my dreams, my mother Surekha Keni for all the valuable lessons in life. I am grateful for their blessings, care, and sacrifices for educating and teaching me to work hard, be

dedicated to every goal in life. My sister, Shweta Kerkar and brother-in-law Prasad Kerkar for motivating me to study masters and standing as my pillar throughout my journey. My close friend Jayant Mandhare, for always celebrating my performance for me and motivating me to accomplish my dreams. My friends for supporting me emotionally and to help me stay positive in every situation.

I am deeply grateful to every teacher in my life who educated me and have made me a person I am today.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

ABSTRACT

The Radio Frequency Identification [RFID] technology is a novel solution used in supply chain management. A large warehouse consisting of hundreds of objects must be handled effectively and automatically. RFID technology automatically identifies various objects faster, which improves effectiveness in order to create successful stock management systems. Most of today's RFID applications involved in large retailing businesses demonstrate successful results in their businesses. With the requirement of identifying hundreds of objects in a very short amount of time, RFID technology also faces a significant issue known as tag collisions, which raises concerns about high speed, accuracy, and high energy efficiency requirements.

We propose a new CDMA/AIC protocol to improve the performance (speed, throughput, accuracy, and especially energy efficiency) of mobile and handheld RFID tag systems by giving them the ability to overcome the problems associated with signal corruption due to collisions and the multipath environment, and providing a way to cancel the effects of interference from the desired signal. The ability to accurately capture the information from tags with greater throughput and fewer errors will be demonstrated to present a novel solution in this area.

We have developed a CDMA with AIC algorithm which provides a solution yielding energy efficiency in low SNR environments with multipath and shadowing. The CDMA/AIC does not have the inefficiencies of Slotted-Aloha, can handle low SNR environments, and does not have the restriction of conventional CDMA that the backscattered signal from each tag must arrive at the receiver with the same amplitude. The CDMA/AIC protocol ensures accurately read tags even with collisions, successfully removes the negative impacts caused due to noise, near-far, shadowing and multipath and gives the best energy efficiency for the overall system.

I. INTRODUCTION

A. Problem Statement

RFID technology is a novel solution used in supply chain management. A large warehouse consisting of hundreds of objects must be handled effectively and automatically. RFID technology automatically identifies various objects in a brief period of time, which improves effectiveness in order to create successful stock management systems. The current RFID market estimate is over $10 billion annually. The majority of today's RFID applications involved in large retailing business demonstrate successful results in their businesses. **[1]** With the requirement of identifying hundreds of objects in a very short amount of time, RFID technology also faces a significant issue known as tag collisions, which raises concerns about high speed and high throughput. Often times, the device that interrogates the RFID tags is mobile or even hand-held, placing an additional premium on energy efficiency to allow long battery life and/or extended range. **[2]**

The demand for high performance systems constantly inspires researchers to focus on creating solutions that could increase throughput and eliminate errors. Interference in electromagnetic signals has been an issue for many years. The proposed study supports improvements in the performance (speed, throughput, energy efficiency) and accuracy of RFID tag systems by giving them ability to cancel the effects of interference from the desired signal. The ability to accurately capture the information

from tags with greater throughput and fewer errors will be demonstrated to present a novel solution in this area.

The goal of our research is to develop an algorithm which helps to overcome the problems associated with signal corruption due to collisions and the multipath environment without requiring significant processing in the tags.

B. Brief History

The roots of RFID technology can be traced to the period from the beginning of twentieth century through World War II. The Americans, Germans, Japanese and British were using Radar engineering mechanisms to send warning signals about approaching planes from miles away. The crucial problem was that there was no way to define which aircraft belonged to which enemy. Russian physicist Leon Theremin invented a listening device in 1945 for the Soviet Union which retransmitted radio waves with the added information. RFID is a combination of radar and radio broadcast technology. Radar was developed in the United States during 1920. Scientists further connected relationships between electricity and magnetism, which enabled the foundation of radio broadcasting. RFID technology has evolved since then and its standards began to emerge. Further improvements lead to miniaturization, cost of the system began to fall, and authentication and security measures began to develop. Companies started commercializing antitheft systems using radio waves to determine whether an item was paid or stolen. Earlier, in 2000, retail businesses

started implementing RFID technology to manage their inventory. In 2003, the famous retail business Walmart experienced 15 billion loss in their sales, after further investigation it was noted that the main reason for this loss was improper stock management. They implemented RFID tag systems to resolve this issue and experience 99% accuracy and successful results in their business. **[3]** It is believed that in the near future the technology will be further advanced and will attempt to eliminate barcode systems completely.

C. Thesis Objective

Electromagnetic interference caused by collisions from simultaneously transmitting tags makes it challenging to accurately read information for the RFID reader. Interference in communication systems plays a major drawback in the reliability and throughput of the systems. This is especially true for systems with multiple sources attempting to efficiently share a channel. Radio Frequency Identification (RFID) systems are one such example. The failure to capture accurate data from the RFID tags results in degrading the reliability and throughput of the overall system.

The demand for high performance systems constantly inspires researchers to focus on creating solutions that could increase throughput and eliminate errors. The proposed study would support improving the performance (speed, throughput, energy efficiency) and accuracy of RFID tag systems by giving them ability to cancel the effect of interference from the desired signal. The ability to accurately capture the

information from tags with greater throughput and fewer errors will be demonstrated to present a novel solution in this area.

D. Organization of Thesis

This thesis is organized as follows:

Chapter 1 of this thesis provides a background and introduction including a brief history of RFID technology. Chapter 2 focuses on the challenges experienced in RFID tag systems, such as tag collisions, effects of multipath environment, the issue of near-far scenarios, and a discussion on how these factors impact the throughput and efficiency of the overall RFID tag systems. Chapter 3 discusses the various components present in RFID tag systems, describes the different types in RFID tag systems, and discusses the significance of the Electronic Product Code (EPC). Chapter 4 discusses different multiple access techniques available to work in building strong protocols to minimize the negative impacts of collision, multipath, and noise. Chapter 5 gives a brief description about the previous research work in RFID tag systems. The chapter gives an overview about the list of protocols developed so far using various innovative techniques. Chapter 6 is an introduction of our proposed Code Division Multiple Access technique with Adaptive Interference Cancellation (CDMA/AIC) and explains the process with flowchart and design steps to the Adaptive Interference Cancellation algorithm we have developed in this thesis. Chapter 7 describes the comparison of the proposed CDMA/AIC protocol with the

Slotted Aloha method and traditional CDMA method. This chapter gives in depth analysis and assumptions followed to accomplish this research work. The observations and simulation plots of the research are explained at the later section of this chapter. Chapter 8 finally concludes the aims achieved in this research work. Chapter 9 proposes the various possible ideas for future research.

II. CHALLENGES IN RFID TAG SYSTEMS

A. Tag Collision

The most crucial problems linked with RFID tag systems are collisions of signals, dominating effects of multipath, shadowing, and near-far problems. In a dense environment where there are many tags waiting to send their data to the reader, often times multiple tags end up sending their information to the RFID reader at the same time. This results in mixing of signals and creates errors in capturing the data.

In such situations, the tags wait a random period of time and attempt to retransmit the same information to the reader, which wastes the reading time and reader power, and degrades the performance of the overall system. This problem is identified as *tag collisions*. To overcome this interference researchers are continously investing their focus on developing anti-collision algorithms that would help in achieving greater data accuracy and greater throughput. Multiple access techniques are mainly used in the process of allowing concurrent communication between the reader and tags with minimun intereference. In RFID tag systems the reader tries to capture large amounts of information within less time from the tags present in its read range, which means that the reader and tag communication share the same air medium as their communication channel. Thus a variety of multiple access techniques have been proposed for RFID systems including Time Division Multiple Acess (TDMA), Code Division Multiple Access (CDMA), Spatial Division Multiple Access (SDMA), Frequency Division Multiple Access (FDMA), and hybrid multiple access technologies.**[2][3][6]**

Our thesis will mainly focus on utilizing CDMA multiple access technology in developing the algorithm. Currently specified Class 1 Generation II passive RFID systems are based on the TDMA multiple access technology with Slotted ALOHA in the forward link communication (uplink communication) where the interrogator communicates with the tag first **[22]**. The extreme limitation with the approach of TDMA based anti-collision algorithms is that they can retrieve, at most, one tag's information in one time slot, and in case of collision oftentimes no tag information is successfully demodulated and all colliding tags having to delay a random period and then retransmit. Another disadvantage with this approach is the many empty or unused slots which degrade the overall system throughput. In modern communication systems CDMA technology has been extensively used because the algorithms provide the ability to perform multiple communications in the same channel medium using same time and frequency resources. The introduction of CDMA in passive RFID systems helps in minimizing the time required to detect the tag information correctly. The use of CDMA can also improve the system's performance in the presence of multipath and noise. The CDMA technology is classified in two types: Frequency hopping CDMA (FH-CDMA) and direct sequence spreading CDMA (DS-CDMA). The passive tag systems lack the ability to select the communication frequency properly (they just backscatter the radio signal emitted from the RFID reader) and so the FH-CDMA technique is not suitable for such systems. The DS-CDMA technique, however, utilizes a spread sequence method to present a spread version of its signal source **[6]**. Different tags can transmit their signal simultaneously to the reader and the reader is able to isolate each tag's signal from the overall received signal. This

approach is extremely useful in dense scenario situations where there are tens or hundreds of tags present in the reader range.

Since RFID technology utilizes wireless transmission, it is essential to consider the potential problems caused by interference. The effects of interference are probable to be severe. Two kinds of interference should be considered; first, the interference that prevents precise data transmission and/or reception, and second, the risk that signals form one system will be misinterpreted by other systems as valid data. Difficulties were experienced in the past when RFID tags were mounted on metal or on containers of liquids. RFID tags failed to respond to the readers with their actual data, which increased the failure rate and degraded system efficiency. Failure rate is defined by the percentage of time RFID reader failed to capture data from a tag. There exist many potential reasons on the inability to capture tag data in passive ultrahigh-frequency (UHF) RFID tag systems and some scenarios are listed below:**[4]**

Incorrect tag orientations

RFID tag orientation refers to the position of tag with the reader. RFID tags perform well in certain angles and degrade their performance in certain angles reaching to a point called null zone which means zero capability to communicate with reader. When RFID tag and reader are properly aligned with each other the maximum read distance can be achieved. Polarization of antenna plays important role in achieving excellent transmission and reception quality. Reader antenna with circular polarization can read RFID tags easily in any orientation. But if the application

demands of using dipole UHF tag and a linear-polarized antenna with improper orientation it becomes difficult for the tag to enter in active state because of small portion of energy received by tag. A linearly polarized dipole antenna performs well when RFID tags are parallel to axis.

Electromagnetic Interference

Noise or electromagnetic interference from surrounding objects or RF devices such as machines, dust particles, fluorescent lights etc. corrupts transmission by blocking the waves from getting to the tags. Such adverse effects from various surroundings results into creating interference between reader and tag communication and thus reduces the system efficiency.

Absorption of RF energy

When passive tags are used at UHF, objects that contain large amount of water absorb RF energy. This absorbed energy cannot be used by the tag and results into receiving less energy to reflect back a strong signal back to the reader. Such scenarios causes missing tag information and degrades the reliability of the overall RFID tag systems.

Reflection of RF energy

RFID tags placed near metal surface tend to reflect energy away from the tag which results in difficulty for RFID tag to sends its information to the reader. In certain situation energy bounce off a floor, ceiling, metal shelves it can cancel out waves reducing the probability to accurate transmission of data. This causes null spots, and reader would not be able to capture data from tags present in such zones.

B. Multipath Environment

To address multipath issues in RFID tag systems, the received signal's amplitude in the wireless channel is modeled utilizing a Rayleigh Distribution to account for the non-line-of-sight transmission of tag signals. **[5][23]**. In the non-line-of-sight scenario the transmission of signals occurs only by reflections. The Rayleigh fading model assumes that the signal strength or the magnitude of the backscattered signal when it arrives at the reader will vary randomly according to the Rayleigh distribution where the radial component is the sum of the two uncorrelated Gaussian random variables. The effects of reflection of signals caused in different radio environments is modelled using the approach of Rayleigh and Rican fading. The process is characterized by a Rayleigh distribution for signals received from non-line-of-sight zone and Rican distribution for a line-of-sight-path. The amplitude of the received signal from a tag due to multipath can be modelled by treating g C [τ (t), t)] as a random process in t, where 'τ' is the propagation delay. The multipath channel can be illustrated by the theory of time varying, complex, low-pass equivalent impulse response C [τ (t), t]. The assumptions made on the large number of randomly phased components and the scattering model are used to specify the measurements of the received signal variations. The fading components present in the multipath channel arise generally due to countless reflections at UHF frequency or due to scattering from rough surfaces. According to the "Central Limit Theorem" the C [τ (t), t] can be viewed as a complex Gaussian realization. The probability density function of the in phase and quadrature components, which are nothing but the real and imaginary components, are stated as Gaussian. If C [τ (t), t] has a mean equal to zero, then the envelope.

R (t) = |C [τ (t), t] |has a Rayleigh probability density function (pdf)

$$p_r(r) = \frac{r}{\sigma^2} \exp\left(\frac{r^2}{2\sigma^2}\right).\ r \geq 0$$

C. Near Far Problem

One of the crucial effects experienced with CDMA technology when used in RFID tag systems is the "Near-Far" problem. The Near-Far issue is a case where the reader gains the strong signal from tags that are close to the reader but is not able to gain weaker signals transmitted from the tags further away from the reader but still in the proximity of its read range. This problem mainly occurs because the tags in a large facility are scattered at different locations and when two or more tags transmit their signal simultaneously with same power levels, the receiver receives more power from the nearest tag. If there is a large difference between the strengths of the received signals, the reader may sometimes be able to read the stronger signal, but the signal to interference ratio of the tag which is far away from the reader goes much lower which makes it impossible for the reader to read information from the farthest tag. As the distance between the reader and tag doubles the signal strength falls away to a quarter. This phenomenon is known as the inverse square law where

Signal = K * 1/d^2

K = constant

d = distance

D. Shadowing

In a large warehouse which has hundreds of tags lined up with each other, the tag present nearby to the reader receives maximum energy, but the tags lined behind the first tag does not. This effect is known as shadowing.

In wireless communication shadowing of signals results due to the existing obstacles between transmitter and receiver. These impediments unfavorably influence the electromagnetic wave propagation and shadowing is demonstrated as an irregular procedure. In RFID tag systems shadowing is considered as one of the major factors in determining the failure rate to capture data. Assume if RFID passive tags are firmly arranged together, the first tag will receive reader's significant energy, but the tag behind it may not. The effects of the near-far problem, shadowing, and multipath create huge variations in signal strengths of multiple tags at the receiver's end. However, for CDMA to operate efficiently in order to deliver higher accuracy and a reliable system the reader must be able to receive all the signals within the same channel bandwidth and must be able to decode them correctly.

A possibly excellent design scheme with implemented techniques of anti-collision and interference cancellation methods enables resolving the issues mentioned above. Since all the addressed issues are challenging to overcome studies suggest some excellent techniques and approaches which helps to achieve maximum efficiency and precision.

III. BASICS OF RFID SYSTEMS

Radio Frequency Identification technology is continuously upgrading and advancing. With a fast pace of rapidly changing technology, RFID technology has evolved at a higher rate in the past few years. Nowadays RFID systems are finding applications in innumerable fields such as asset tracking, inventory tracking, healthcare, timing in marathons, concerts, materials management, etc. With the need for high throughput systems it is imperative to develop and design systems in a way that is time and energy efficient and highly accurate. From monitoring health equipment to tracking every single item in a huge warehouse, RFID technology has found innovative ways to be implemented in various sectors. **[6]** Not just in human services and retail offices, RFID innovation is even providing creative approaches in the area of display art and culture. For example, in order to measure involvement at a museum, RFID technology is implemented in many places to record and understand the reaction and interest spent on every item of fine art, thus expanding the usage of RFID technology into almost every possible thing we could imagine.

Radio Frequency Identification (RFID) refers to a technology where the digital data is encoded in the RFID tags or smart labels. This encoded data is captured by the RFID reader that stores the data from each label to a database. The RFID reader, also called an interrogator, can locate more than 1000 items per second. The choice of RFID antenna depends on the distance considered between the reader and the tags to be read. This distance is termed as the read range. RFID reader antennas operate in two

ways: near-field (short range) or Far-field (long range). In near-field applications, the antenna uses magnetic coupling so that the reader and tag can transfer power and the readability of the tags is not affected by the presence of dielectric materials such as water or metal. The typical read range in such applications is less than 30 cm. On the other hand, in far-field application systems the antenna uses electromagnetic coupling and the dielectrics may weaken the communication between the reader and the tag. The typical read range in the far-field systems is greater than 30 cm and in certain frequency bands can be up to 36 feet or even greater. **[7]**

There has been a constant ongoing debate in comparing the RFID technology with Barcode technology. The basic barcode system has several limitations such as the requirement of placing the object in line of sight with the reader, label damage, limited read range etc. RFID ensures precise accounting of products in large warehouses or inventories of any retail business organization. RFID technology currently operates in 3 different frequency bands

- (Low 125 – 145 MHz),
- (High 13.56 MHz),
- (Ultra-High 860 – 960 MHz)

The UHF RF band allows the capability to enhance the read range between the tag and reader. Systems operating in the Ultra-High frequency band easily cover distances of 36 feet or greater, and do not require the tag and reader to be in exact line of sight, which bolsters any system to work at greater than double the speed as compared with barcode systems. **[8]**

A. RFID System Components

RFID brings a great value in the entire supply chain management business by giving the ability to effectively collect, manage, and distribute information on inventory and maintain security controls. RFID allows retailers to evaluate potential delays and shortages caused in the business, in grocery stores RFID allows elimination or minimization item spoilage, and RFID allows for suppliers to track shipments and perform authentication measures and verify security on shipped items.

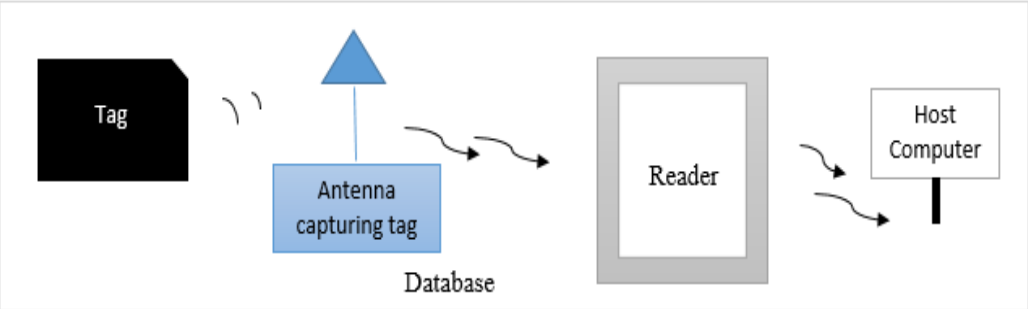


Figure 3.1: Components of RFID tag systems

RFID systems can be read only (data transmitted from tag to the reader) or read write (two-way communication). A typical RFID tag system uses the principle of modulated backscatter. To transmit data from the tag to the reader, the RFID reader sends an electromagnetic signal to the RFID tag. The RFID tags reads the information included in its internal memory and changes the loading on the tag antenna in a coded manner. The reflected signal from the RFID tag is a modulated version including its information. This modulated signal is received by the RFID reader and demodulated using a homodyne receiver. The final output is decoded as digital information containing the actual data stored in the RFID tag. When the RFID reader wants to send data to the RFID tag, the transmitted radio signal is modulated by the reader which is received by the RFID tag. The modulated signal is detected by the tag using a diode, and the data is used to either control the operation of the tag or is stored in the tag's memory. As shown in Figure 3.1, an RFID system consists of three main components, a tag (also called a transponder) with digital memory chip that stores a unique identification number and possibly additional data, an interrogator (also called a reader), and an antenna (included with a transceiver and a decoder). The interrogator captures the information from each tag attached to any object present in the reader range (typically, read time is less than a few hundred milliseconds). **[9]** RFID tag systems can be divided into three types: passive RFID systems, semi-passive RFID systems and active RFID systems. The RFID tags are built by using CMOS circuitary and are powered by using battery or by using the radio signals sent by the reader. The tags send their information to the reader either by transmitting a modulated radio signal to the reader or by changing the loading of antenna in a coded

manner. The modulation technique used in RFID tag systems include: Amplitude Shift Keying (ASK), Phase Shift Keying (PSK), Frequency Shift Keying (FSK), and Quadrature Amplitude Modulation (QAM). **[10]**

The RFID reader performs the air interface functions which includes reading the information from the RFID tag and transmitting the information to the middleware (microprocessor) to allowing storing the information in the database. The read range of a reader is heavily affected by the factors such as frequency identification, orientation of tag and reader, antenna gain and polarization. The read range is usally calculated by:

$$r = \frac{P\ \Delta GXn}{4\pi\ (R + 4X)P}$$

where: r is the communication range

P = Effective Isotropic Radiated Power

Δ = wavelength

G = tag antenna gain

X = reactance introduced by load modulator

n = rectifier efficiency

R = impedence of the antenna

P = tag power consumption

The RFID systems have two antennas; one at the tag and another at the reader. The reader's antenna performs the function to transmit the reader's interrogation signal and, receive the return signal from the tag. The antenna consists of conductive elements which enable the tag to communicate with the reader. The size of an antenna depends on the frequency; as the frequency used in application increases, wavelength and antenna size decrease. **[11]**

B. Active RFID Tag System

Active RFID systems use their own battery source to power the active tags. The active tags constantly transmit their signal using the internal battery power. These tags are mainly used in applications which require a coverage of larger areas such as traffic signals, detecting train signals, security systems, toll booths, system locating, etc. Active tags include a transmitter inside a tag, the transmitted signal is relatively strong and can travel accurately in troublesome environments. With better accuracy and longer coverage distance, active tags are highly expensive when contrasted with the other RFID tags. A typical active tag can cost approximately $10 to $20 per piece and can go considerably higher than $100 depending upon the application. For security-based applications for residential protection, which require high reliability and long battery life, the price range of active tags goes higher that $100. **[20]**

Implementation of Active RFID tag systems has been explored in supply chain management, electronic toll collection, inventory control and object tracking

purposes. Since active tags are equipped with their own battery source and have longer communication range, they are suitable for aerospace industries. Honeywell Aerospace uses active tags for locating tag parts enabled with high memory RFID chips. Active tags with embedded sensors are used in healthcare and harbor logistics systems. Active RFID tag systems are also equipped with autonomous networking which is used to determine the best possible communication paths during information transmission. Apart from accurate and reliable communication they have superior performance in adverse scenarios in presence of liquid and metallic objects.

In RFID tag systems a single tag can transmit its data multiple times which might cause depletion of energy from the batteries used inside the active tags. Active tags cannot perform without battery power, which results in the requirement of either battery replacement or implementation of new active tag. This results in increased maintenance costs of an active RFID tag, further increasing its expense relative to passive tags.

C. Passive RFID Tag System

Passive RFID systems do not have an internal battery source. The reader in a passive RFID system powers up the tag by sending the energy to its RFID antenna. The antenna converts this energy into an electromagnetic wave which, when received by the tag, turns on the tag. The tag energizes the microchip within the tag which generates a signal and restransmits it back to the reader by modulating the tag antenna's impedance. This phenmonon is called backscattering. The change in the

reflected electromagnetic RF wave is detected by the reader which helps to translate the correct data from the tag. Passive tags provide a read range between 8 feet to 40 feet. Although, they are not as fruitful as the active tags in terms of distance they are much less expensive than the active tags. Typically, a passive tag capable of storing 96 bits costs aroung 5 to 15 cents **[15][20][21]**. In order to determine the price range of a particular tag several factors are taken into consideration such as frequency of operation, type of application, area of operation, coverage distance etc.

At the Ultra High Frequency (UHF) range the read range is approximately 12 meters (40 feet). The larger part of new RFID ventures are utilizing UHF range. The UHF innovation has more than 20 billion associated objects giving continuous perceivability and information to a large collection of ordinary objects. These tags are extremely cost effective as the price of one passive tag is, as mentioned earlier, between $ 0.05 to $ 0.15 per tag. They are viewed as the most productive RFID framework for many applications since they give better stock visibilty and eliminate the need of physically perusing labels joined to each thing present in the warehouse of an organization.

Passive tags obtain their power from the communication signal through inductive or by far field energy harvesting. Since passive RFID tags do not have their own power source they are required to harvest the energy and communicate with the reader

within a narrow frequency band. Inductive coupling uses a magnetic field to induce a current in the coupling element of a coiled antenna and a capacitor. This current induced in the coupling element activates the capacitor on the tag which provides an operating voltage and power for the tag to operate. The inductive coupling works well in near field region. Far field begins where the near field ends, which is at the distance from emitting antenna. In far field energy harvesting the energy is used from the interrogation far field signal to power the tag. RFID passive tags are considered as to have longer life, less cost, compact size and more resistant to corrosion and physical damage as compared with the active tag systems.

D. Semi-Passive RFID Tag System

Semi-Passive tag systems also called semi-active or battery-assisted passive (BAP), are based on a similar principle as passive tags, but with battery included to improve communication range. The semi-passive tags require an external power source to activate the integrated circuit inside the tags. The inclusion of batteries expands the offered features of semi-passive tags by additionally enabling application of sensors, reat-time tracking and sound notifications. Because of these features the semi-passive tag systems are mainly used in application such as environment monitoring. The main disadvantage of semi-passive tags is that it is expensive as compared with passive tags and has the same complexity of increasing the requirement of maintenance of such tags.

E. Electronic Product Code (EPC)

For application of RFID technology in the majority of industrial sectors, passive RFID tags are commonly used due to their advantages of being cost effective, small, and physically flexibile. For this thesis we will be considering EPC class 1 generation 2 passive tags for our system **[22]**. EPC or Electronic Product Code is a unique number that distinguishes an explicit object in the inventory network. When RFID tags are attached on any item in a supply chain or retail business environment, the EPC number associated with it is based on the identification scheme. The EPC number can be related with dynamic information about the object such as date of manufacture, type of contents in the item, etc.

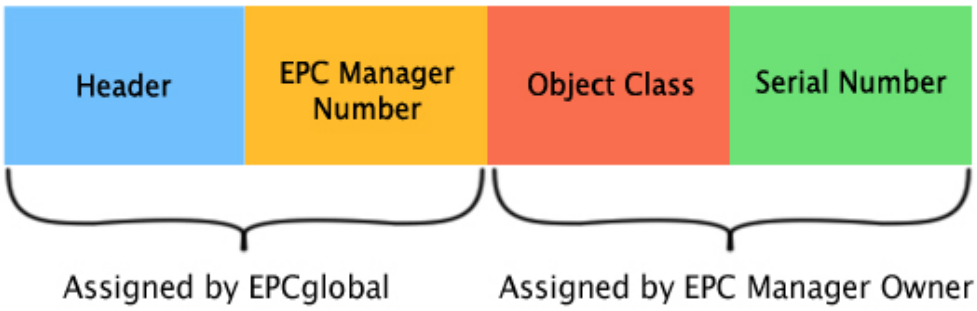


Figure 3.2: Basic Format of Electronic Product Code (EPC)

Figure 3.2 shows the basic format of the Electronic Product Code (EPC) on every RFID tag. The header identifies the length, structure, type, version and generation of the EPC. The EPC manager Number identifies the entity responsible for maintaining subsequent partitions. Object Class identifies class or object of the product and Serial Number identifies the instance of the item. EPC Global is responsible for overseeing

the use of the EPC standards, guidelines and specifications. EPC Global is a non profit joint venture between GS1 (formerly EAN International) and GS1 US (formerly the Uniform Code Council).

The EPC can be viewed in a similar way as the Vehicle Identification Number (VIN) or Global Trade Item Number (GTIN). The gen 2 tags can be compatible with radio frequencies from 860 MHz to 960 MHz, which is the UHF operating frequency range of RFID tag systems.**[1][16]** RFID tags are classified in 6 different class from class 0 through class 5 and their functionality is listed in the table below:

Table 3.1: Classification of RFID tags

Class 0	• These are preprogrammed passive tags used in UHF for read only
Class 1	• Used for UHF and HF range with the feature of write once, read many (WORM)
Class 2	• Passive tags with read-write functionality at any point in the supply chain.
Class 3	• Capable to record parameters like temperatures, pressure, and motion with read-write functionality. They can be active or semi-passive tags with onboard sensors
Class 4	• Active tags with integrated transmitters and read-write functionality.
Class 5	• Comprises Class 4 functionality with the additional feature of providing power to other tags and communicating with devices other than readers.

Class 0 and Class 1 are generation 1 RFID tags in the UHF band. Class 0 is originated as a protocol by Matrics Technology Systems (acquired by Symbol Technologies) and Class 1 is originated as a protocol by Alien Technologies. The generation 2 (GEN 2) RFID tag standards which were adopted in December of 2004 presents expanded data functionality and high performance features. The Gen 2 tags were designed to support 256 bits long EPC code to work with frequency ranging between 860 MHZ to 960 MHZ. The Gen 2 tags were develop as a response to overcome the limitation offered with respect to Gen 1 RFID tags. With additional features of faster, flexible speeds, the Gen 2 tags provide accurate performance acheieved through various anti-collision protocols with enhanced security and privacy. **[1][12]-[13]**

IV. MULTIPLE ACCESS TECHNIQUES USED IN RFID TAG SYSTEM

In wireless communication, a multiple access technique allows more than two terminals to transmit their information using a common transmission channel in the most effective manner. Wireless networks, bus networks, ring networks, etc. are some examples of shared physical media. The channel access method is based on multiplexing, which permits many signals to share the same communication channel or transmission medium. Multiple access techniques mentioned below enables simultaneous transmission and reception of signals from devices present at different locations without any interference. **[25]-[26]**

In attempting to identify multiple RFID tags in the densely populated fields within a short period of time, a typical design of RFID tag systems leads to multiple challenges. The RFID reader communicates with multiple tags using a shared air medium as their communication channel. A variety of multiple access techniques are used to overcome the challenges experienced in communication between RFID tags and readers. **[15]** The following are some fundamental techniques used in RFID tag systems to overcome the common challenges. **[16]**

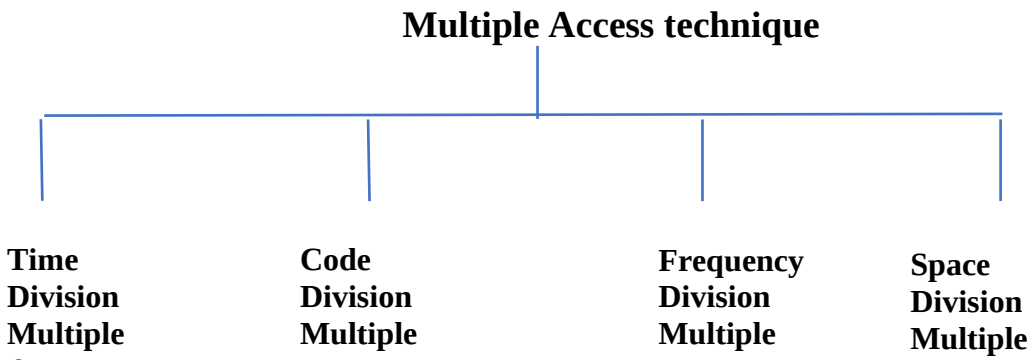


Figure 4.1: Types of Multiple Access technique

A. Time Division Multiple Access (TDMA)

Time Division Multiple Access (TDMA) techniques allow multiple users to share the same frequency channel by dividing the signal into different time slots. Slots allows each user to transmit its response one after another, each using its own time slot. In network communication systems, TDMA can provide a major advantage of enabling the option of listening and broadcasting on the same channel in separate time slots. For times when a user is not transmitting, the user can carry out other network operations such as detecting surrounding transmitters, making network measurements, and processing information. TDMA is a relatively less expensive technology and preferred in various RFID system applications for designing anti-collision algorithms. The transmission channel is divided between the tags participating in the communication and the RFID reader ensures that it identifies each tag indivdually. In RFID tag systems, the protocols based on TDMA technology initially choose an individual tag from a large group using a specific algorithm and then allow communication to take place between the RFID reader and the chosen tag. **[17]**

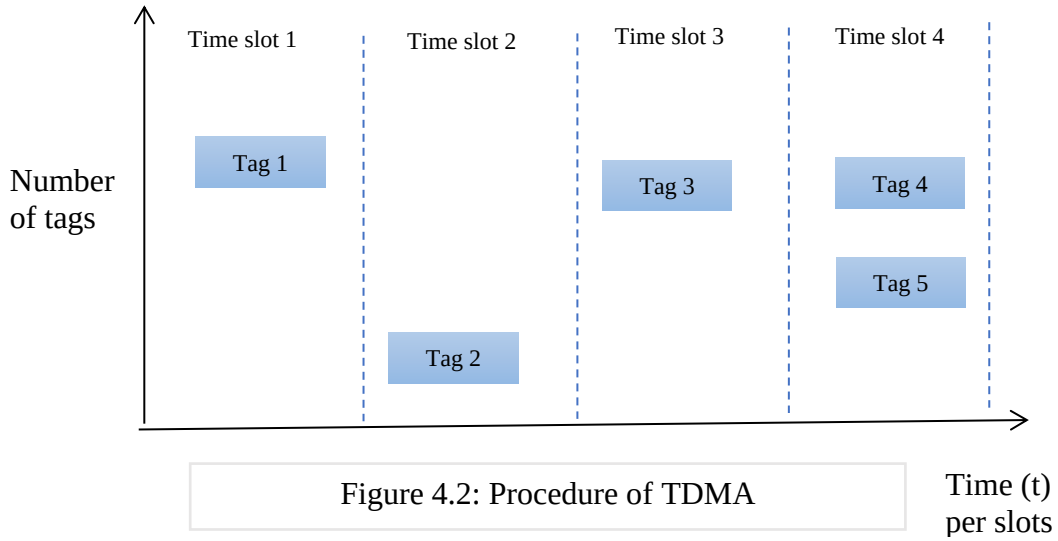


Figure 4.2: Procedure of TDMA

TDMA technologies can be divided into two categories of schemes, the deterministic schemes and probabilistic schemes. The deterministic approaches are usually referred to as binary tree-search schemes. In the binary tree-seach based schemes each root to leaf denotes the information of a unique ID (in our case, a unique RFID tag) and all the ID's are expected to be recovered once all the branches in the tree are completely searched. On the other hand, the probabilistic schemes, of which ALOHA is one of the most popular, do not use a tree-search and allow for the possibility of collisions between two or more tags if they send their response in the same time slots. Information from a tag is successfully recovered only if the tag's reponse is received without collision (and if the response is not corrupted by noise) per time slots. **[1]**

B. The ALOHA Method

The Aloha system was a pioneering computer networking systems developed at the University of Hawaii. **[18][25][28]** The Aloha method provided the first public presentation of a wireless packet data network, and its acronym originally stood for Additive Links On-line Hawaii Area. Later it proved to showcase remarkable performance in wireless broadcast sytems with half-duplex two-way links.

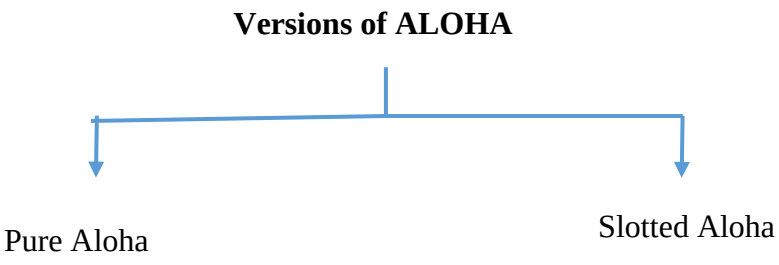


Figure 4.3: Types of Aloha

C. Pure ALOHA Method

The Aloha protocol is based on a simple version of the Time Division Multiple Access technique. The tags automatically start sending their information upon entering the reading field, the first job of the reader is to identify every tag present in its read range and record the data. In many situations some tags trying to communicate with the reader might be interrupted by transmissions with other tags, this interruption would lead to overlapping of their information and therefore data collisions.

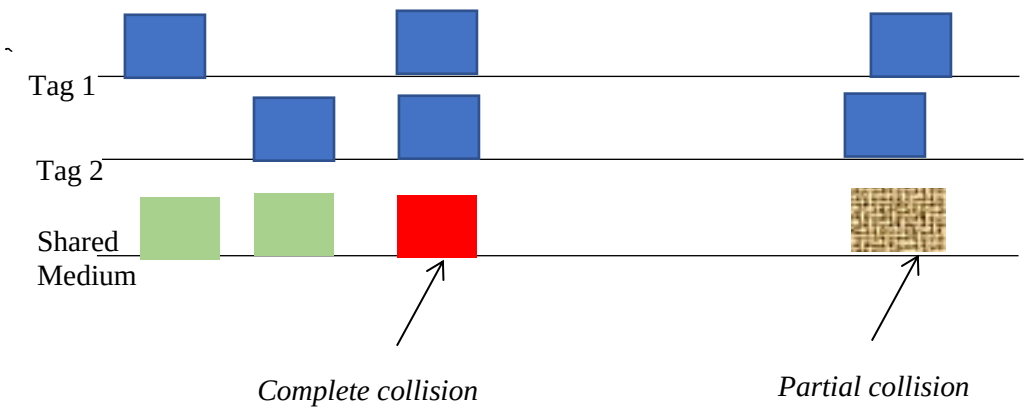


Figure 4.4: Process of Pure Aloha method

As the collision occurs during the communication process, the tags are forced to stop their transmission and retransmit after a random delay period. In the Pure Aloha method, any station can transmit their information at any time. The parameter time is continious and not globally synchronized. The Pure Aloha system does not prioritize to check whether the channel is busy or not. The heavier the load of tags transmitting its information, the worse the collision problem, which results in system efficency degradation.

In the Pure Aloha method, throughput can be predicted by making following simplifing assumptions.

- All frames are assumed to have the same length.
- While transmitting or attempting to transmit, the stations cannot generate a frame.
- The tags will transmit new as well as old data that collided according to a Poisson distribution.**[17]**

Frame time is defined as the time required by the tag to send its information in that frame. Consider "G" as the mean used in Poisson distribution for transmissions attempted per frame time, and "t" the time intended to send a frame. The probability of "k" transmissions occuring during that frame time is given by:

$$\frac{G^k\, e^{-G}}{k!}$$

For two consecutive frame times, the average amount of transmissions attempted is 2G. Therfore, the probability of k transmission-attempts during those two frame-times for any couple of successive frame-times is:

$$\frac{(2G)^k\, e^{-G}}{k!}$$

The probability of successful transmission of data packet is given by

$$G * e^{-2G}$$

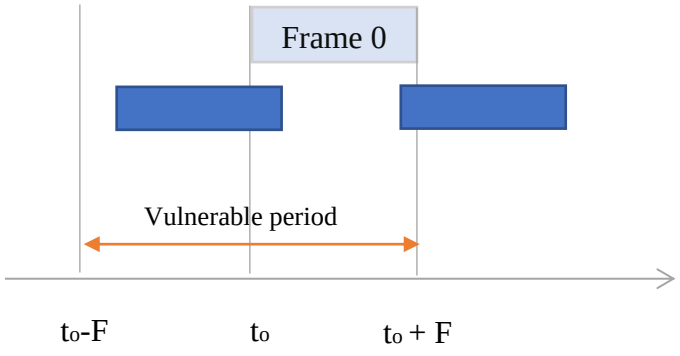


Figure 4.5: Aloha frame vulnerability

The vulnerable period is defined as the time when no tag should transmit its information to the reader. If vulnerable period is equal to frame period, there is a high chance of tag collisions as there is no gap between the time each tag attempts to transmit its information. Since in the Pure Aloha method time is a continous parameter, the number of collisions is maximum. The difficulties raised in Pure Aloha systems makes it a challenging process to capture data efficiently from the tags. Several techniques have been proposed so far to increase the efficiency of data capture with Pure Aloha method. These techniques include the Switch off technique which allows the successfully decoded tags to enter in Quiet state. The tags present in the quiet state no longer transmit their ID to the reader. The second technique is called as the Slow-down technique. It works between the Pure Aloha and the Switch off technique with an aim to dismiss tags. A slow-down command is initiated by the reader when it is overwhelmed by the responses from tags. This results in reducing the rate at which tags transmits their information and maintains reply frequencies. The third technique is called Carrier-sense method, which senses the communication channel to determine the progress of a particular transmission.

D. Slotted-ALOHA Method

Slotted-Aloha was introduced by Roberts in 1972, as an improvement to the original ALOHA protocol. **[28]**. Slotted-Aloha, introduces discrete time intervals called slots and increases throughput of the system.

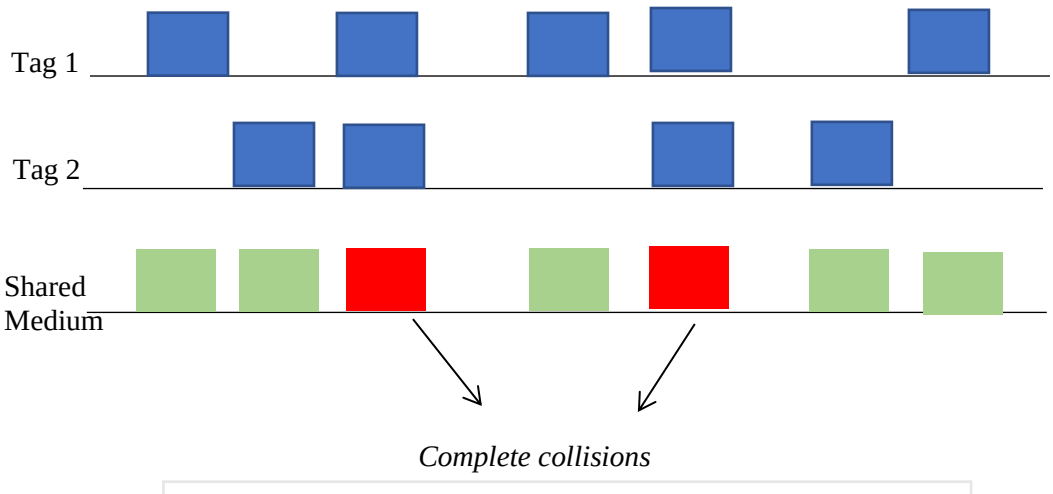


Figure 4.6: Process of Slotted Aloha method

In the Slotted Aloha method tags can begin their transmission only at the beginning of a slot, thus helping to minimize tag collisions. If the beginning of the slot is missed, the tag has to wait to transmit until the next time slot. Tags either collide completely, or do not collide at all. The issue of partial collision as experienced with the Pure Aloha method is eliminated.

The Slotted Aloha method requires a synchronization mechanism to manage the simultaneous tag communications in RFID systems. The mechanism is achieved dynamically by having the reader initiate slot-delimiting beacons, or employing a statically pre-defined timer internal to the tags. The Slotted Aloha approach alleviates many of the problems associated with Pure Aloha approach. The time slots in Slotted Aloha method corresponds to the length of frames, and tags will send their information to the reader in particular time slots which reduces the probability of tag collisions and increases system efficiency. Therefore, the Slotted Aloha protocol is considered better than the Pure Aloha protocol for RFID applications.

The transmission probability requiring precisely k attempts is (k-1 collisions and 1 success) is given by the following equation:

$$Prob\ slotted\ k = e^{-G}(1 - e^{-G})^{k-1}$$

The throughput of Slotted Aloha method is calculated by:

$$Sslotted = Ge^{-G}$$

The highest throughput is 1/e frames per frame-time (attained at G = 1), which is roughly 0.368 frames per frame-time, or 36.8%. Appendix D contains a graph of showing theoritical throughput for both simple Aloha and Slotted Aloha. In environments with significant background noise, errors in the received messages will require retransmissions and make effective throughput much lower. Additionally, in environments where messages arrive in a cluster (as is the case with RFID systems) efficiency also decreases.

Thus the performance of the system is calculated by the number of responses the reader can read in one time slot. The probability of occurrence of successful time slot is written by the equation mentioned below:

$$Prob(success) = n(tag)\left\{\frac{1}{n(frame)}\right\}\left\{1 - \frac{1}{n(frame)}\right\}^{n(tag)-1}$$

Where the n(tag) = number of tags in the reader's field

N(frame) = number of slots from which the tag can select one

In some scenrios where number of tags in the reader's field is large, it can be assumed that the distribution of probability of receiving tag's response is a Poisson distribution. The system's throughput is determined by the proportion of frame size to the amount of tags in the reader's coverage. If the number of tags to be read is unknown, as is often the case in RFID systems, the key factor to estimate the throughtput of the system is accomplished by selecting a appropriate frame size. **[19]**

E. Frame-Slotted ALOHA Method

A Frame-Slotted Aloha (FSA) protocol is widely used in RFID systems, constructed by taking one step further past Slotted Aloha and discrete time division by grouping several slots into frames, each frames having N slots. Various networked systems including satellite networks, wireless LAN, and emerging Machine to Machine (M2M) networks implement an FSA protocol to tackle collisions and maintain effectiveness of their systems. FSA is standarized in EPC Global Class-1 Generation-2 (C1G2) RFID standards. In FSA-based protocols, each tag transmits its data packet in a selected slot of the frame, however only the data packets experiencing no collisions are successfully detected and collided data packets are referred to as backlogged packets (or backlogs) which are retransmitted in the subsequent frames. Packets that do not experience collisions but that are received in error due to high background noise will be backlogged, too.

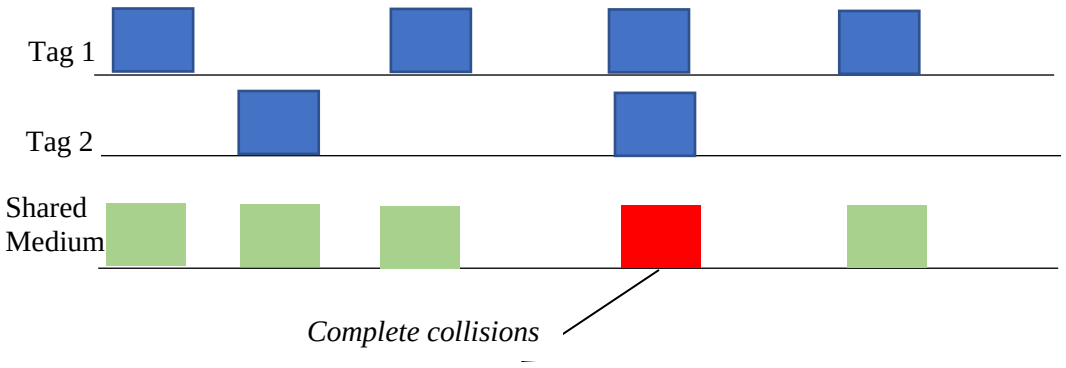


Figure 4.7: Process of Frame Slotted Aloha method

Basic Frame Slotted Aloha (BFSA)is a technique with fixed frame size throughout the reading process. BFSA has four different variants, such as

BFSA-non muting: In this approach an exponetial increase in identification delay is caused when the number of tags is higher than the frame size.

BFSA-muting: In this approach the tags are silenced once they are identified, thus reducing the number of available tags in each read round.

BFSA-non-muting-early-end and BFSA-muting-early end: Both of these BFSA approaches incorporates an early end feature which means the reader is capable of closing a slot early if no response is detected at the beginning of a slot.

The FSA protocol shows significant improvements in performance both in theory and in practical systems, however limited work has been performed with this protocol, because the FSA protocol requires quite exhaustive system design including more precise protocol defination and time handling parameters.

F. Dynamic Frame Slotted ALOHA (DFSA)

Dynamic Frame Slotted Aloha (DFSA) based protocols have varying frame size. The DFSA algorithm operates similarly to the BFSA protocol with implementing the early-end feature. The difference between these two techniques is that in each round, the reader uses a tag estimation function to change the frame size. The tag estimation function calculates the number of tags based on feedback from the reader's frame. This includes information such as multiple tag response (c_k), number of slots with

zero (c_0), and one (c_1). This data is used to estimate the optimal frame size, and to predict the number of tags in that read round. **[20][30]**

Each Aloha protocol is considered to have its own advantages and disadvantages and the table below highlights a few of the major points:

Pure Aloha	
• Adapts easily / quickly to a variety of tags • Simple design	• Low throughput under heavy load conditions. • Maximum channel utilization theoretically is 18.4%
Slotted Aloha	
• Reduced tag collisions • Higher throughput	• Requires queing buffers for retransmission of packets • Maximum channel utilization theoretically is 36.8%
Frame Slotted Aloha	
• Decreases the repetition of tag responses per frame	• Frame size needs to be known • Requires synchronization
Dynamic Frame Slotted Aloha	
• Uses tag estimation functions • Increases the tag identification in each read round	• Extremely complex • Error propogation

Figure 4.8: Overview of Aloha protocols

G. Code Division Multiple Access (CDMA)

Code Division Multiple Access CDMA is an instance of multiple access where multiple transmitters can simultneously send data across a single channel of communication. This enables multiple users to share a frequency band without time slots. **[16]**

H. Traditional CDMA

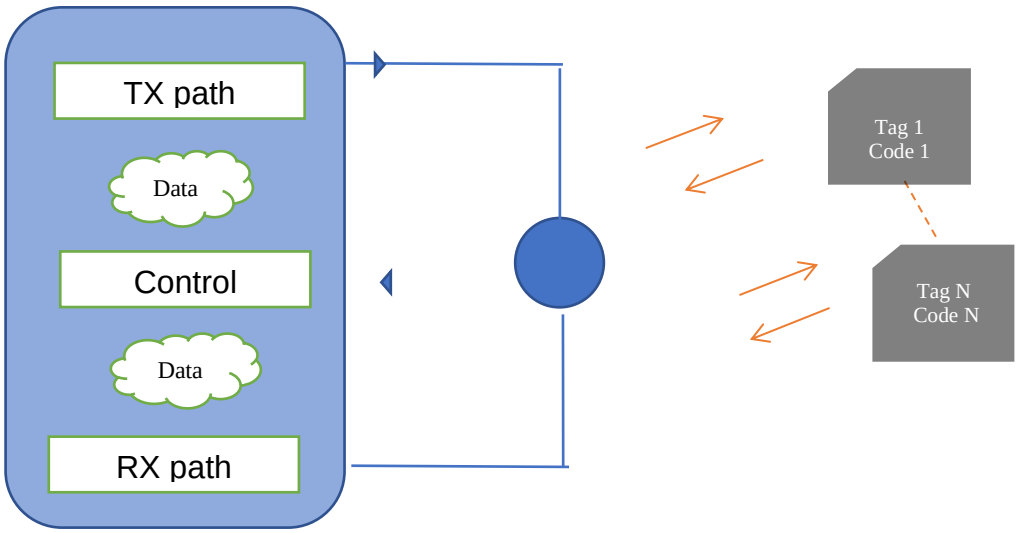


Figure 4.9: Basic architecture of RFID system

The basic architecture of CDMA based RFID tag systems consists of two major parts; a Reader section and a Transponder or Tag section. The CDMA technology requires tags to exclusive-OR their ID by a pseudo-random (PN) sequence before transmission. The basic working principle is shown in Figure 4.10.

The RFID reader has already transmitted a signal over its transmitting antenna TX, which activates various tags in its read field to modulate and reflect an incident wave back to the RFID reader. Therefore, the total backscattered signal represents the aggregated superposition signal from n tags with each tag using a unique sequence of spreading codes. This superimposed signal is acquired by the receiving section which performs the de-spreading process at its end. The de-spreading process allows the reader to separate individual tag signals from each other in order to restore the original transmitted data by each tag. The process of de-spreading is the most intensive complex calculation of the overall RFID communication system.

CDMA technology is considered as the most efficient multiple access technique used to improve the performance of overall RFID tag systems because it can eliminate the need for frequency and timeslot coordination in dense scenarios. Two categories of spread-spectrum CDMA are direct sequence CDMA (DS/CDMA) and frequency hopping CDMA (FH/CDMA). We will focus on DS/CDMA because passive tags cannot implement distinct frequency hopping sequences (they can only backscatter the signal from the reader). There are a variety of spreading sequences for different DS/CDMA applications such as Walsh codes used as orthogonal sequences and Gold codes used as pseudo-random (PN) sequences. Over a period, a PN sequence will have the same number of 1s and 0s. Although the sequence is deterministic due to the limited length of the linear shift register used to generate the sequence, a PN code can be used to provide the required spreading code within a CDMA system. Truly

orthogonal codes are defined such that when two codes are exclusive-ORed together, the result obtained over a period has the same number of 1s and 0s. For example [1 1 1 0] and [0 1 1 1] when exclusive-ORed give [1 0 0 1] which has the same number of 1s and 0s. For the proposed system we will use a set of orthogonal spreading codes generated from the columns of a Hadamard matrix. The spread spectrum technique minimizes the overall interference resulting from other simultaneously transmitting tags using direct spreading codes and from the additive noise experienced between reader and tag communication. The DSSS method produces spread signals from each tag that look like white noise over the bandwidth of the transmission. However, each spread signal can be "despread" at the receiver with the appropriate de-spreading code to retrieve original information.

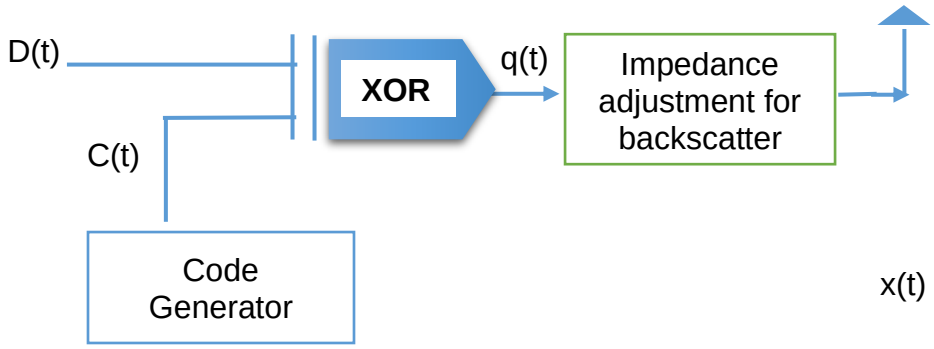


Figure 4.10: RFID Tag incorporating DSSS

The tag data in Figure 4.10 is denoted with D(t), the spreading code is referred to as C(t), and the spread waveform is q(t). The spread waveform q(t) is reflected back to the RFID reader using backscatter.

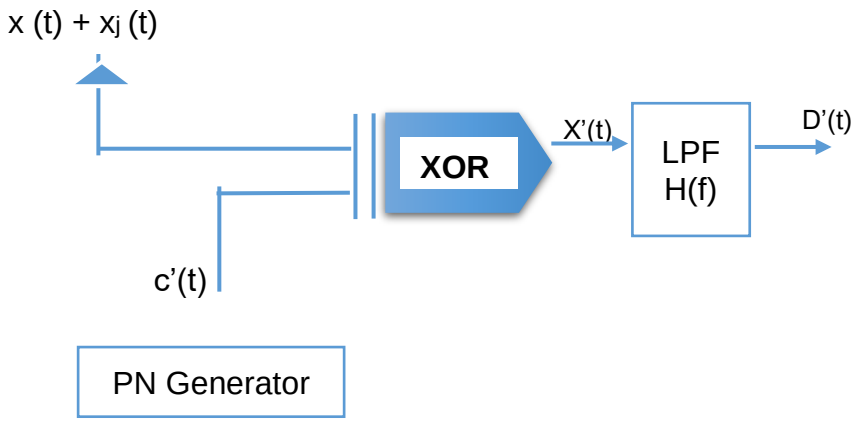


Figure 4.11: DSSS Receiver

The total signal received back at the RFID reader is an aggregation of the transmitted spread spectrum signals from each tag plus noise. Let this received signal be represented by x(t) + xj(t), where x(t) represents the spread spectrum signal received from one particular tag (call it "Tag A" and xj(t) represents the spread spectrum signal received from all the other tags plus noise. When the aggregate received signal is demodulated and then exclusive-ORed with the same spreading code used by Tag A, the result is the data from Tag A plus a relatively low level of bandlimited white noise representing the interference from the other tags plus system noise. The data from Tag A can then be extracted. Using different spreading codes, the RFID reader can de-spread the received signal to reveal the data from each tag represented within the aggregated signal.

In the DSSS approach, the message signal is “spread” in length because the spreading code is many times longer than the original message signal. The ratio of the spreading code’s length to the original message’s length is called the code’s *spreading gain or processing gain* (G_P), which is also referred as the *chip rate*. This ratio should be an integer. Referring back to Figure 4.10, the first bit of the original message is exclusive-ORed with the first G_p bits of the spreading code, the second bit of the original message is exclusive-ORed with the second G_p bits, etc. The resulting encoded message is G_p times as long as the original message, and it can either be transmitted in the same amount of time as the original signal but at a transmission speed G_p times faster, or it can be transmitted at the same speed as the original message but with its transmission time increased by a factor of G_p. The former approach (faster transmission speed and increased bandwidth) is used by most DSSS systems, but the transmission speed of Class I Gen 2 RFID systems is already specified, so our proposed system will use the latter approach and spread the signal’s transmission time. At the receiver the demodulated data is Exclusive OR-ed with the unique spreading code (i.e., “despread”) and then lowpass filtered to regenerate the original transmitted information. When this is done, only the data generated with the same spreading code is regenerated, all interference generated by noise and by other tags, simultaneously transmitting but using different spreading codes, is filtered.

To visualize how the DSSS process works, the simplest technique is to demonstrate an example in terms of information pieces and how the information is spread, transmitted, and then retrieved from the DSSS signal. For example, consider the information from the tag to be 1010, and the chip or spreading code to be 0110. The complete spreading code is used for each data bit in the exclusive-OR operation, and thus the spread or expanded signal consists of four bits for each data bit.

Table 4.1: Example of CDMA spreading process

1	**0**	**1**	**0**	**Data to be transmitted**
0110	0110	0110	0110	Spreading code
1001	0110	1001	0110	XOR output of spread data

The signal obtained after spreading is a 16-bit sequence (G_p=4) and the original data must be decoded by the remote receiver. The following table illustrates the dispreading process to acquire original the information.

Table 4.2: Example of CDMA de-spreading process

1001	0110	1001	0110	Incoming CDMA signal
0110	0110	0110	0110	Spreading code
1111	0000	1111	0000	De-spreading result
1	**0**	**1**	**0**	**Original transmitted data**

Thus, the original transmitted data is recovered exactly at the receiver by using a unique spreading or chip code. If a different spreading code was used in the de-spreading process, then it would produce a 16-bit sequence that would appear to be random and could be visualized as noise in the system, which would then be reduced by lowpass filtering. If noise or interference cause one bit in each 4-bit de-spreading result to be incorrect, filtering still produces the correct recovered data. The spreading code used in the above example was only four bits long. Usually spreading code combinations may be 16, 32, 64 bits, or even 128 bits long to provide the desired performance. The greater the value of $G_{p,}$ the lower the percentage of noise-induced and interference-induced errors in the de-spreading result and the higher the accuracy of the recovered signal after filtering. Accuracy is also dependent on having all of the signals received at roughly the same power level.

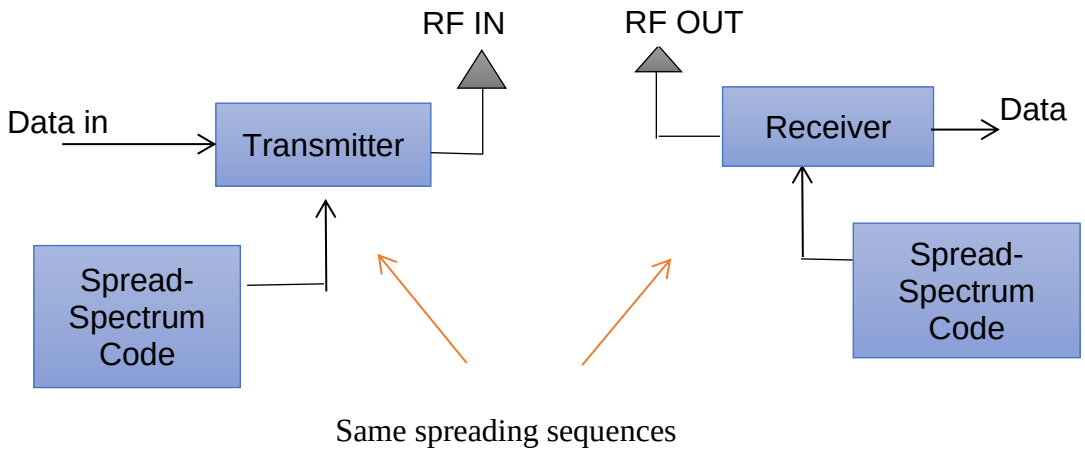


Figure 4.12: Spread-spectrum communication system

In the proposed RFID tag system DSSS is implemented by having each tag select a spreading code from among a set of codes and then spread its data prior to backscattering. At the reader the received signal is depsread by each of the possible spreading codes, and information from each backscattering tag in the system can be read.

I. CDMA With Adaptive Interference Cancellation (AIC)

Destructive tag collision in CDMA based anti-collision protocols occur if two tags use the same spreading code. The issue of empty slots or same slots does not exist with the CDMA system, but there exist adverse effects due to multipath, shadowing and the near-far problem in CDMA. These phenomena cause the tags to send their backscattered signals at significantly different power levels. The signal to noise ratio for the strong signals in this case is so high that it becomes impossible for the RFID

reader to accurately read the signals from the weaker individual tags, even with spreading and de-spreading. In cellular communication systems the variation in power levels is resolved by a control protocol from the base station to the individual cellular users. But adjusting power levels for individual tags is not the option available for passive tag RFID.

In dealing with different power levels for signal-to-noise ratio it is assumed that for extremely low values of SNR the primary problem in the RFID tag system is the errors caused due to noise. With high SNR values the primary reason for errors is not noise but it is tag collisions (two tags selecting same spreading code). The CDMA system gives better capabilities to deal with collisions in the presence of noise. Theoretically, a CDMA based protocol might not give a better performance that slotted Aloha if we are in an environment of zero noise (see section VII Figure 7.5), but practically we will not be dealing with such a case.

The Adaptive Interference Cancellation (AIC) algorithm, which will be proposed in section VI, uses the CDMA techniques as the baseline and provides the additional capability to handle noise by considering the primary goal to conserve more power. Our thesis considers the facts of presence of noise, efficient transmission with low power and accurately read tags that are shadowed and blocked due to the adverse effects of multipath. The AIC algorithm gives the advantages of using CDMA with its

anti-collision and error correction capabilities versus noise while addressing the issue of receiving signals at different power levels. Additionally, if any application requires to operate in lower values of SNR, the AIC protocol gives additional capabilities of cancelling the negative impacts of interference by subtracting its effect from the transmitted signal, interpreting the original tag signal, verifying whether the already interpreted information is correct or not, and accurately identifying the possible signal at the receiver.

J. Frequency Division Multiple Access (FDMA)

Frequency Division Multiple Access (FDMA) is a method which allows multiple users to send data through a single communication channel. The bandwidth of the communication channel is divided into separate non-overlapping frequency sub-channels and each sub-channel is allocated to an individual user. Each user transmits data on a different frequency channel, thus eliminating interference with adjacent users. The FDMA technology used in RFID tag systems allows several transmission channels to operate together at the same time by using distinct operating frequencies.

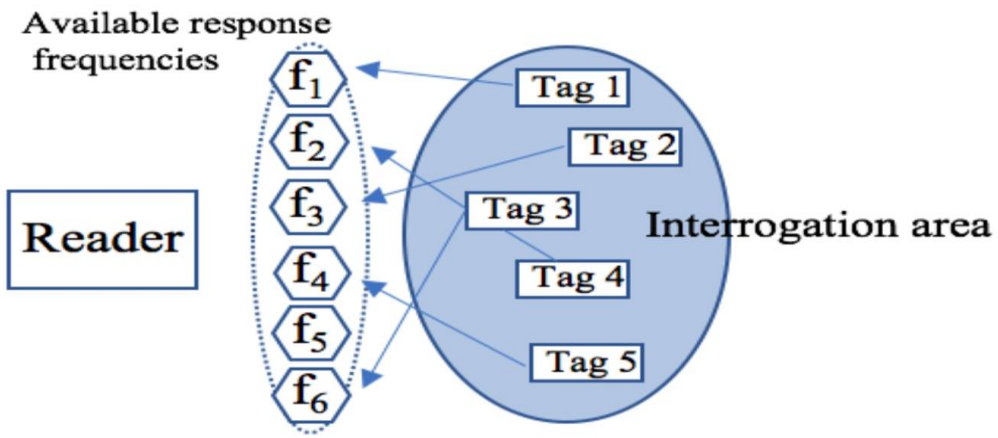


Image source: [21]

Figure 4.13: FDMA technique

In passive RFID tag systems, the signal from the reader is broadcast using some operating frequency to provide power and activate the reader's command to passive tags. A tag receives the power from the broadcast signal sent by the reader and uses the signal as a modulated backscatter signal. In fact, within its operating frequency band, a tag can obtain any signals and use the received signal as a carrier to backscatter a modulated signal. Thus, applying the FDMA technology to passive RFID devices which can use multiple frequencies benefits from this property. The main disadvantage of FDMA schemes in RFID technology is that it gives relatively high cost to design readers capable of working at multiple frequencies. Additionally, it requires a dedicated receiver must be provided for every receiving channel. **[21]**

K. Space Division Multiple Access (SDMA)

Space Division Multiple Access (SDMA) techniques are based on dividing the channel capacity into separate physical areas. A SDMA system allows multiple subscribers or stations associated with the same base station, to use the same Time and Frequency and Code (T/F/C) resources on the grounds of their physical location or spatial separation. RFID protocols based on SDMA technique point the beam at different locations to be able to identify tags. The spatial seperation of the communication channel is achieved by incorporating directional antennas or by the use of multiple readers. The SDMA approach isolates the coexisting transmission sources via an angle of arrival (AOA) of each signal source, which is also referred to as spatial signature. In passive RFID tag systems, this property is beneficial because it does not require any alteration in the physical communication protocol but is achieved by using the reader with array antennas. Therefore, SDMA can be used in conjuction with either the proposed system or with conventional slotted ALOHA systems. A large number of tags can be identified simultenously as a result of spatial distribution over an entire system. Incorporating SDMA into the proposed system is beyond the scope of this thesis but will be suggested as a future research topic in section IX.

V. PREVIOUS RESEARCH WORK

Previous researchers have focused their attention on developing anti-collision algorithms in order to deal with the issues involving reader and tag interference/collisions. These anti-collision algorithms include tree-based protocols adopted from a binary tree algorithm which is based on the identification of particular colliding tags as 0 or 1 **[9]**. In the tree-based algorithms collisions occur in a particular TDMA time slot. The number of colliding tags is separated into subgroups by declaring them either 1 or a 0. The splitting of tags into groups is due to collisions. In this approach the tag that selects a 1 will have to wait until all the tags which have read 0 transmit their ID to the interrogator. This method is suitable in an ideal situation where we know that there will be few collisions of signals from the tags. In a large facility environment such a protocol is not useful because it will either result in waiting for all tags to be read or having more empty slots which will cause a decrease in system performance and accuracy.

Another anti-collision algorithm utilizes the concept of the basic frame slotted aloha method **[5] [6]** where the algorithm selects a fixed frame size and does not change the size until the reading process is completed. In this approach when the interrogator tries to receive information from the tags, the tags offer the information to the reader in the computed time slots in a frame. If while reading, the previous slot detects a collision the entire process to attempt to read information from the tag is repeated and all the tags retransmit in the next read frame. Currently there are several ways to

change the computed frame size and one such popular method is dynamic frame slotted aloha protocol where the interrogator sets an upper threshold and lower threshold value to deal with collisions. If the number of collisions in a frame is above the upper threshold, the interrogator increase the size (number of slots) of the frame for the next read cycle, and if the number of collisions in the first read cycle is below the lower threshold then the interrogator reduces the size (number of slots) of the frame for the next read cycle. **[3]** In the dynamic frame slotted aloha protocol the reader computes the frame length of a cycle by taking into consideration the number of collisions that occurred in the previous read cycle. This approach was again suitable for applications with less coverage area (i.e., fewer tags). In order to modify this approach the improved dynamic frame slotted aloha method was proposed, which is based on several assumptions such as countless tags being present in the read range at a time, reflections from more than two tags are not taken into consideration, and the algorithm identifies only the tags present in the direct line of sight with the reader. In the proposed approach tags were grouped in different frequency channels rather than grouping them in same frequency channel, thus saving the time in estimating the frame size and reducing the number of empty slots in the reading process. Note that the need for simultaneous frequencies increases the complexity of reader. The algorithm was considered a success mainly in the 433 MHz frequency band of RFID application **[5].** Apart from experimenting with the new approaches with the slotted and frame slotted aloha theory there has been a recent approach which presents an enhanced anti-collision algorithm by utilizing the counters and stack to reduce the probability of collision further to improve the system performance and increase the

efficiency. This approach works similarly to the dynamic frame slotted approach where the reader estimates if more than two tags have the same prefix and appends 0 or 1. When a unique match is identified it gains the information from the tag and marks that particular tag as being read. **[25]** This algorithm is called the QT algorithm which consists of executing several rounds of queries and understanding the responses generated in the process.

CDMA technology has been used in structuring various anti-collision algorithms to overcome difficulties experienced in RFID tag systems. But some CDMA based anti-collision algorithms cannot avoid the problem of near far problem in the form of shadowing. The near far problem in RFID tag schemes creates difficulties in reading the information accurately as it causes tag data to be transmitted at distinct energy concentrations, causing certain tags to have SNR values so high that they overpower other tags available in read range. One such example is referenced in **[1]** which effectively displays a novel Bitwise-CDMA (B-CDMA) solution to decrease interrogator power usage by precisely getting data from tags. The Bitwise operation is a straightforward action which operates on one or more-bit patterns at a level of individual bits. Each slot in the algorithm attempts to simultaneously read a maximum number of tags and measures the highest received power. The examination gives strong confirmation of the idea by performing simulations in software and hardware. The B-CDMA protocol is created with a plan to decide the strength of the individual tag's signal from the aggregated version with the presence of interference, turn off

interfering tags until the next read cycle, and recover the original information effectively. The algorithm helps to remove the colliding tags before the tag completes the transmission of EPC bits. **[1][24]** The Bitwise CDMA works for an operation with a smaller number of tags such as 5 and uses modulation technique such as ASK and PSK. The processing gain used in the protocol is 16. Such approach works for small system application. In might show more power consumption in dense scenarios. In order to identify more number of tags the system would require a larger processing gain which may increase the cost of the tag. Another combination explored with CDMA is a hybrid with the Slotted Aloha method, which is proposed to receive better inventory control results. It uses Gold codes for spreading and further helps to maximize the performance of overall RFID tag systems. **[22]**

The best approach for selecting a particular anti-collision algorithm is based on several factors such as how many timeslots (slotted ALOHA) or spreading codes (CDMA) are utilized, what is the estimated frame length of a read cycle, how many times the reading process is repeated in order to identify the number of available tags in the read range, complexity of the algorithm, average signal-to-noise ratio, and how much data is transmitted at a time. All these factors determine the efficiency of an algorithm **[5] [9] [17].** Particular performance metrics used to compare the current slotted ALOHA system with the proposed CDMA/AIC system are established in section 7.

V1. ADAPTIVE INTERFERENCE CANCELLATION MODEL

Our thesis proposes the concept of overcoming collisions and interference by utilizing direct sequence CDMA and an 'Adaptive Interference Cancellation (AIC) technique' to resolve the issues of multipath, shadowing, and near - far problem experienced by the passive RFID tag systems. Improvements provided by the proposed system will help in expanding and upgrading passive tag RFID technology to be used in numerous applications. As mentioned above, the reader receives the signal that was actually transmitted by the tag plus some interference caused by the signals transmitted from other tags and by noise present in the environment.

We began our work by developing a mathematical, small-scale example using Excel to illustrate the situation. We considered data from three tags in the first phase of the research. We applied a direct sequence spreading process to this data by using three different spreading codes – one for each tag. Once the spreading process was completed, we specified a different strength for each tag's signal and an aggregate signal was created and passed through the communication channel, representing the spread signal + interference + (noise was not considered in the first phase). The de-spreading and AIC process determined the strongest signal's amplitude based on de-spreading with each of the three codes, extracted the data for the strongest tag, and the subtracted its signal from the aggregated received signal. The process was repeated iteratively until information from all three tags was extracted. In this manner every iteration gave information about the amplitude for a tag, completed reading

information from that tag, and then removed that tag's effects from the aggregated signal. By examining the behavior of interference in the signal and then subtracting the effects from the strongest tag we accomplished the idea of reducing the negative impact of interference in the communication process. This method increases the performance of the overall operation and provided the ability to eliminate the interference from tags whose information was already acquired by the reader.

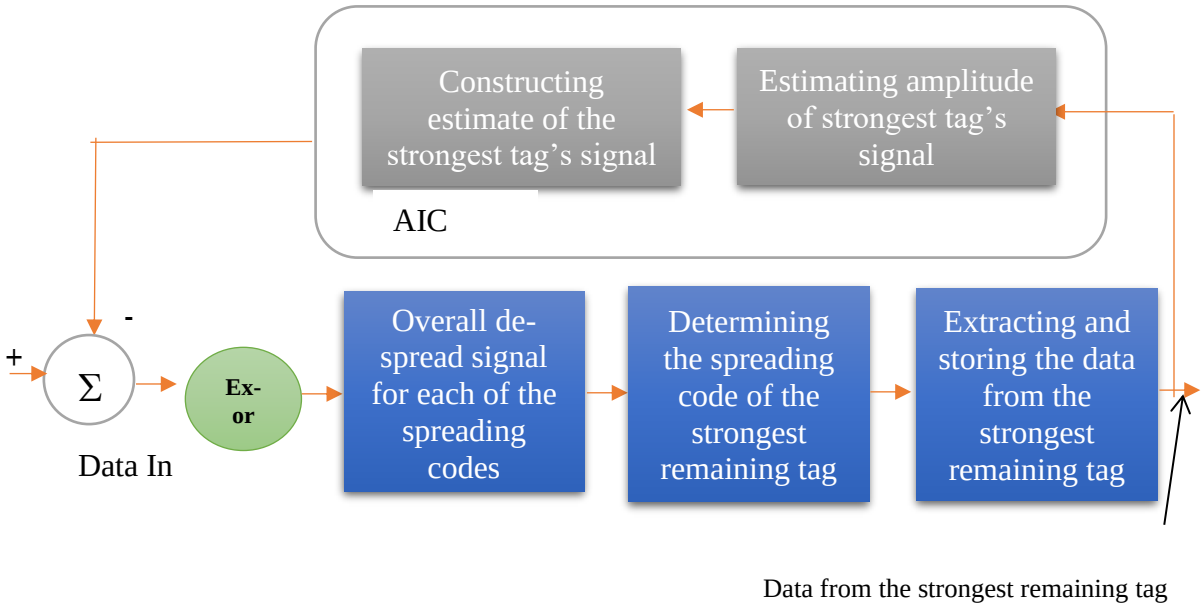


Figure 6.1: Process of AIC protocol.

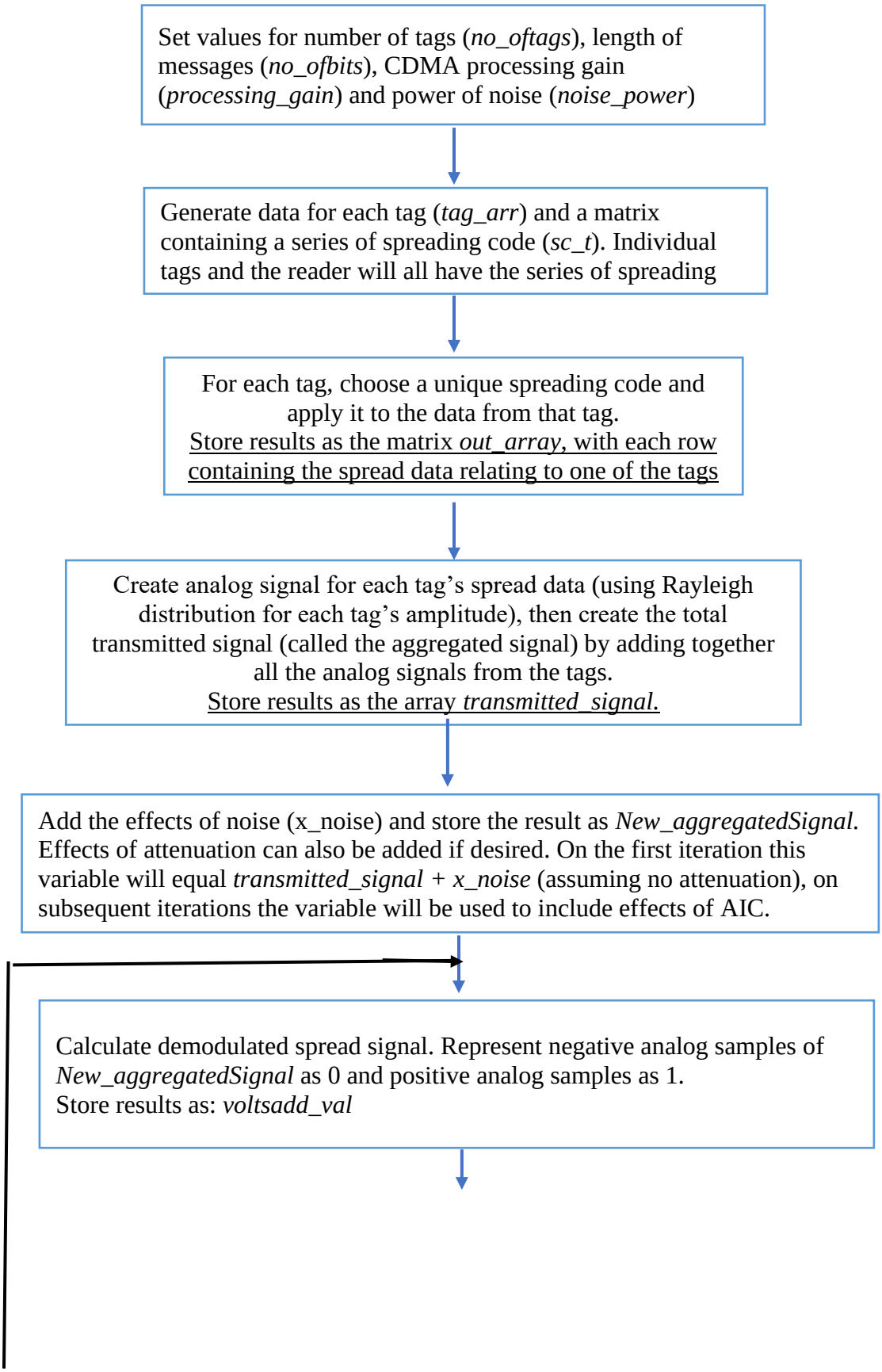
Figure 6.1 illustrates the process of the proposed AIC protocol, and the detailed AIC algorithm is flowcharted later in this section and described in Section 6.2. Adaptive filtering is done to the received signal which removes the interference from the signal by detecting and decoding the signal from the strongest tag, extracting its data, then removing its effects from the aggregated received signal, and then iteratively repeating the process with the remaining signal.

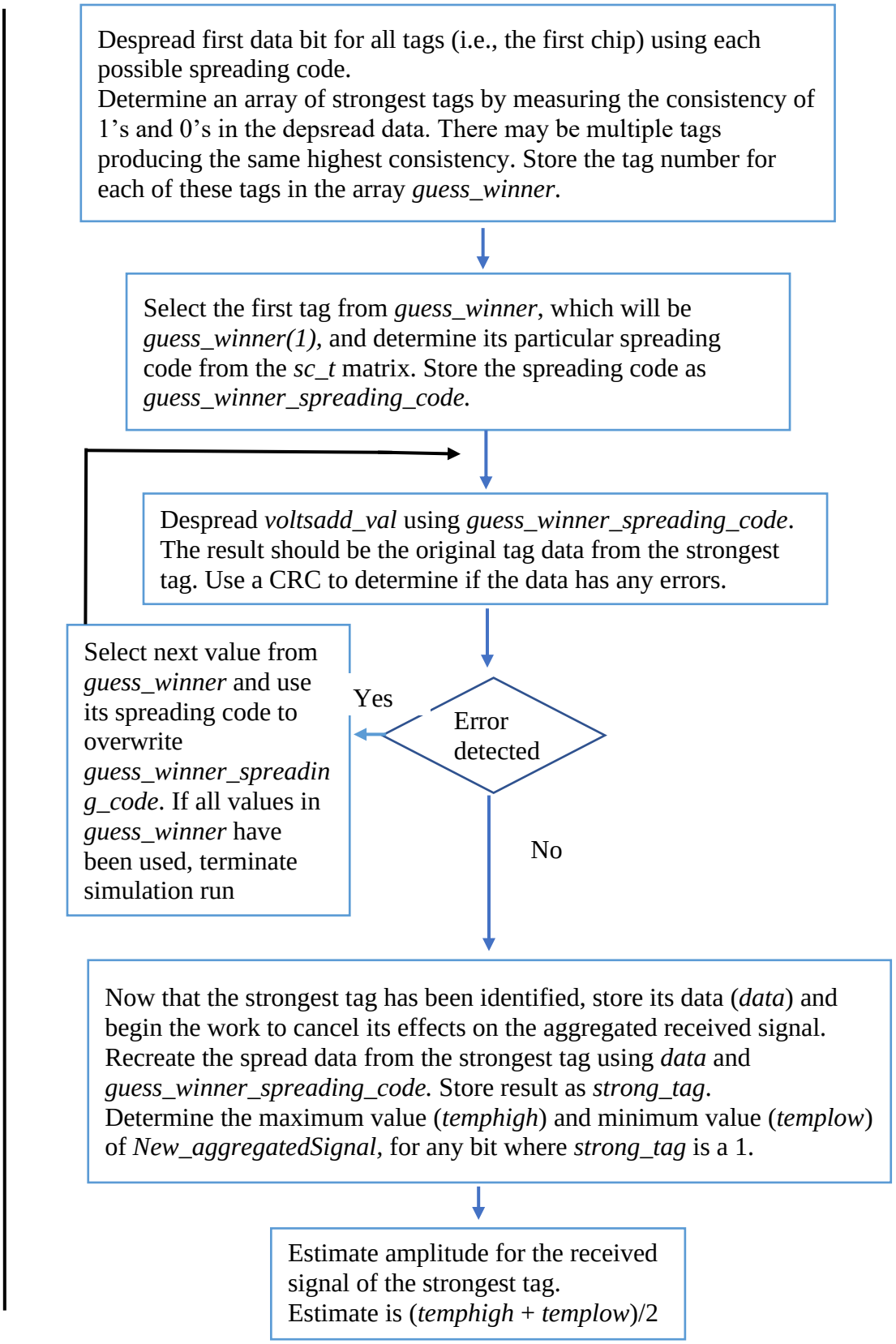
In communication theory, using the process increases the signal-to-interference-plus-noise ratio with each iteration, resulting in successful reception of wireless information. Our approach follows the process of DSSS initially to decode information of the RFID tag. Before starting the interference cancellation process, the protocol compares the values decoded with the originally transmitted bits of a tag. The operation is successful when the values are matched, and the selected tag is identified. If an error occurs in the data comparison process the protocol selects the next tag from the list of strong tags and allows it to pass through the AIC algorithm. The proposed adaptive interference cancellation algorithm helps in adjusting the interference coefficients, subtracts the unwanted information from the signal and presents the recovered signal at its output which is the actual signal containing the data of the transmitter.

Interference due to collisions is something which is uncontrollable but utilizing our proposed approach helps to avoid the potential loss of information and eliminate the need for retransmissions. Also, the quality of signal recovered at the output of the system is more accurate, thus helping to maximize the performance of the overall system and the accuracy.

A. Flowchart of CDMA/AIC Protocol

The second phase of our work was to develop a MATLAB simulation to determine the performance of our proposed system with a larger number of RFID tags and the inclusion of noise. A detailed flowchart of the simulation, including application of direct sequence CDMA, creation of the aggregated signal, inclusion of the effects of noise, de-spreading, and the iterative application of AIC is illustrated in Figure 6.2 below.


Set values for number of tags (*no_oftags*), length of messages (*no_ofbits*), CDMA processing gain (*processing_gain*) and power of noise (*noise_power*)
Generate data for each tag (*tag_arr*) and a matrix containing a series of spreading code (*sc_t*). Individual tags and the reader will all have the series of spreading
For each tag, choose a unique spreading code and apply it to the data from that tag.
Store results as the matrix *out_array*, with each row containing the spread data relating to one of the tags
Create analog signal for each tag's spread data (using Rayleigh distribution for each tag's amplitude), then create the total transmitted signal (called the aggregated signal) by adding together all the analog signals from the tags.
Store results as the array *transmitted_signal.*
Add the effects of noise (x_noise) and store the result as *New_aggregatedSignal.* Effects of attenuation can also be added if desired. On the first iteration this variable will equal *transmitted_signal + x_noise* (assuming no attenuation), on subsequent iterations the variable will be used to include effects of AIC.
Calculate demodulated spread signal. Represent negative analog samples of *New_aggregatedSignal* as 0 and positive analog samples as 1.
Store results as: *voltsadd_val*


Despread first data bit for all tags (i.e., the first chip) using each possible spreading code.
Determine an array of strongest tags by measuring the consistency of 1's and 0's in the depsread data. There may be multiple tags producing the same highest consistency. Store the tag number for each of these tags in the array guess_winner.
Select the first tag from guess_winner, which will be guess_winner(1), and determine its particular spreading code from the sc_t matrix. Store the spreading code as guess_winner_spreading_code.
Despread voltsadd_val using guess_winner_spreading_code. The result should be the original tag data from the strongest tag. Use a CRC to determine if the data has any errors.
Error detected
Yes
Select next value from guess_winner and use its spreading code to overwrite guess_winner_spreading_code. If all values in guess_winner have been used, terminate simulation run
No
Now that the strongest tag has been identified, store its data (data) and begin the work to cancel its effects on the aggregated received signal.
Recreate the spread data from the strongest tag using data and guess_winner_spreading_code. Store result as strong_tag.
Determine the maximum value (temphigh) and minimum value (templow) of New_aggregatedSignal, for any bit where strong_tag is a 1.
Estimate amplitude for the received signal of the strongest tag.
Estimate is (temphigh + templow)/2

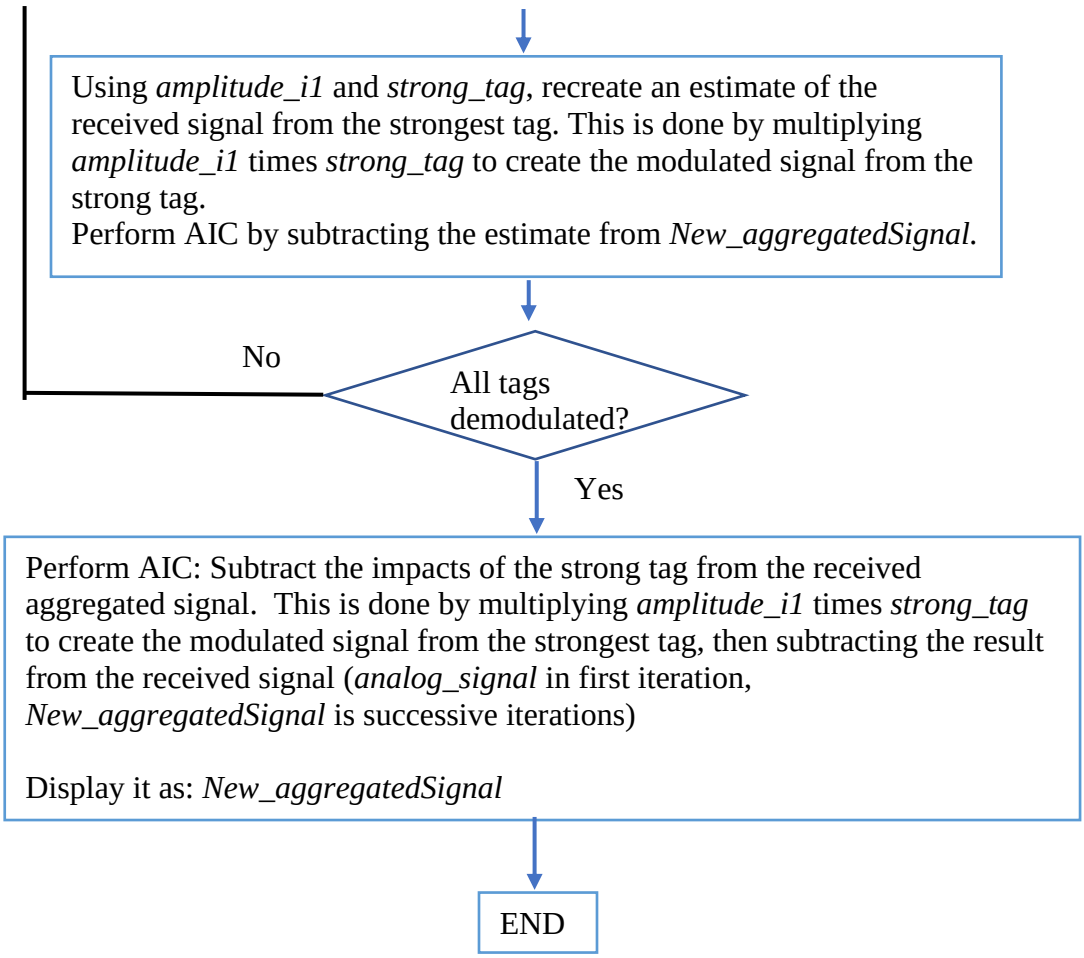


Figure 6.2: Flowchart of AIC

B. Description of Adaptive Interference Algorithm

The proposed algorithm works by combining the idea of Code Division Multiple Access (CDMA) technology with an Adaptive Interference Cancellation technique (AIC). Since tag collisions create a negative impact on the overall performance of the system, spread spectrum technology gives the ability to reduce collisions in the interrogation zone. In this process, the transmitted signal is exclusive OR-ed by a spreading code sequence causing the transmitted signal power to spread over a larger

bandwidth or a longer period of time. The main goals of using this concept are to prevent interference and to reduce the effect of noise, and combined with AIC, to minimize the effects of multipath fading and, shadowing. We consider the following steps in building a simulation to perform and test our algorithm.

1. Initially, select the values for number of tags, length of messages or number of bits, CDMA processing gain ($G_{p)}$ and power of noise.
2. Generate a series of unique spreading code sequences for the selected number of tags, number of bits and processing gain. One spreading code is chosen for each tag, and each tag's data is then Exclusive-OR'ed with that tag's spreading code. The importance of establishing orthogonal spreading codes and balancing out 1's and 0's is considered in this step to avoid the issue of the spreading code getting over-powered.
3. Using Rayleigh Distribution, establish the relative amplitudes of the transmitted signals for each of the tags (tau). This step simulates the effects of multipath and shadowing for each tag.
4. Construct an aggregated signal. This signal represents the transmitted signal which travels through the communication medium. The aggregated signal will be the combination of the transmitted signals from all tags, and it comprises both negative as well as positive interference.
5. Add noise to the aggregated signal and add the effects of attenuation if desired. The result is the received signal.
6. At the receiver, take the received signal (same as the aggregated signal, with noise and possibly attenuation), and demodulate it. Represent the negative analog

samples as 0 and positive analog samples as 1 in the newly constructed aggregated signal.

7. Initiate a de-spreading process on the first spread bit using each possible spreading code to evaluate the consistency of 1's and 0's in the demodulated, despread signal. This helps to identify the signals from strong tag's signal. Note that there may be more than one strong tag. Store the identities of strong tags in guess_winner

8. Select the first strong tag's signal from guess_winner and determine the spreading code used for it.

9. De-spread the transmitted signal using the spreading code of the strong tag and produce a signal which matches with the original signal transmitted by the tag. Using Cyclic Redundancy Check method analyze if the data has any errors. If there are no errors in data bits, proceed with step 11.

10. If one or more errors are detected in step 9, select the second strong tag available and repeat data verification process in step 9 with the information of originally transmitted data bits by that tag. If all the values in *guess_winner* have been used, terminate the simulation run.

11. Once a strong signal is selected, identify the spreading code that was originally used to spread this signal prior to its transmission.

12. Begin de-spreading the received data using only the spreading code of the strong tag.

13. Estimate the original data from the de-spread strong tag signal, record the data, and recreate the spreading code corresponding to the strong tag.

14. Estimate the amplitude of the strong tag's received signal by determining the highest and lowest points of the aggregate received signal for all cases where the spread bit of the strong tag was a "1."

15. Reconstruct the received signal corresponding to the strong tag.

16. Subtract the received signal corresponding to the strong tag from the aggregate received signal (i.e., cancel out the effects of the signal from the strong tag). The result is called the new received signal.

17. The data from one strong tag has now been read and the tag's interfering effects have now been eliminated from the new received signal, so the signals from all other tags have increased in relative strength. Using the new received signal, repeat steps 7 – 16 until data has been extracted from all tags.

The proposed algorithm works successfully to remove negative interference from the signal and predicts the originally transmitted signal. When multiple tags try to send their data to reader at the same time the probability of introducing interference from surrounding objects is high, and intentional or unintentional interferences create detrimental effects on the tag signal. The addition of undesirable effects on the signal makes it problematic for the reader to analyze accurate information from the tags. The AIC algorithm attempts to identify the strongest tag, de-spread it with the corresponding spreading code, calculates its amplitude, and subtract the deleterious impact to retrieve the original signal. Thus, the reader has the capability to decode the data for strongest tag, then the next strongest tag, etc., completing its reading

operation successfully. Results of our simulations, which show the effectivity of CDMA and the AIC algorithm, are given in Section 7.

VII. COMPARISON OF THE PROPOSED CDMA/AIC PROTOCOL VERSUS SLOTTED ALOHA

We have discussed several algorithms, various multiple access technologies in RFID tag systems, which have been established so far. In the Slotted Aloha method, the major disadvantage is the incapability to identify multiple tags with error-free communication between tag and reader. Additionally, it encounters the issue of generating multiple empty slots. In CDMA, tags are concurrently recognized, but if the same spreading code is used by more than one tag, it results in the error propagation issue. Furthermore, the traditional CDMA experiences difficulties in dealing with simultaneously received signals that are at different power levels. The system needs powerful anti-collision protocols in such instances to eliminate or decrease the likelihood of error generation. Combining TDMA and CDMA technology tag collision is less probable to occur, but such combination-based protocols assume that certain portion of slots will read more than one tag at a time. Our CDMA with AIC protocol strategy solves the problem of generating unnecessary slots and dragging out more than the required energy from the system. It also monitors the issue of error propagation by ensuring that the extracted information by the receiver is correct and proceeds with removing the negative impacts caused due to interference and additive noise. The CDMA with the AIC approach does not require complex design of the reader tuned at multiple frequencies as compared to the FDMA technique. The CDMA with AIC protocol works with different combinations of randomly generated spreading codes that help to spread the transmitted signal. The inclusion of interference and noise generated by surrounding objects in any communication system is a challenge that cannot be prevented. But, as will be shown

by the data in this section, the AIC protocol provides significant performance to minimize the adverse effects induced by interference and delivers excellent performance.

A. Handshaking for Slotted ALOHA and CDMA/AIC Protocol

The Class 1 Generation 2 RFID tags use the Slotted ALOHA protocol as their medium access control technique. The number of slots for Slotted Aloha to provide maximum efficiency in RFID systems is a design parameter we shall discuss shortly. As shown in Figure 7.1, the protocol begins when the reader (interrogator) directs the tags to load a random number generator to generate their random slot number. After this step, the RFID reader commands all the tags present in its read range to decrement the slot number by 1 until the randomly generated value becomes 0 (which means the tag's time slot is achieved). The tag generates a temporary ID number which is also known as a "Handle" and reflects the information to the RFID reader. The reader acknowledges this message and instructs the tag to send its EPC data. Once the communication is completed and the required information is transmitted and received the reader instructs the tag to power down. The remaining tags are instructed to decrement further by the reader. If multiple tags generate the same slot number, the tags do not receive an acknowledgment and their data must be transmitted again in next round, using the same approach explained above. This approach has numerous energy inefficiencies. In contrast, for the CDMA/AIC protocol the RFID reader (interrogator) commands all tags to power up and send their data (similar to step 1 in Figure 7.1). The tags then respond by all simultaneously sending their data in DSSS

format (similar to step 4 case 1 in Figure 7.1 but note that message length is increased by G_p). The interrogator then responds by sending a single long acknowledgement identifying all correctly read tags. Any unacknowledged tags will retransmit their data in the next round. The CDMA/AIC approach requires fewer interchanges between the interrogator and tags. The required interchanges are longer, but, as will be shown shortly, lead to greater energy efficiency.

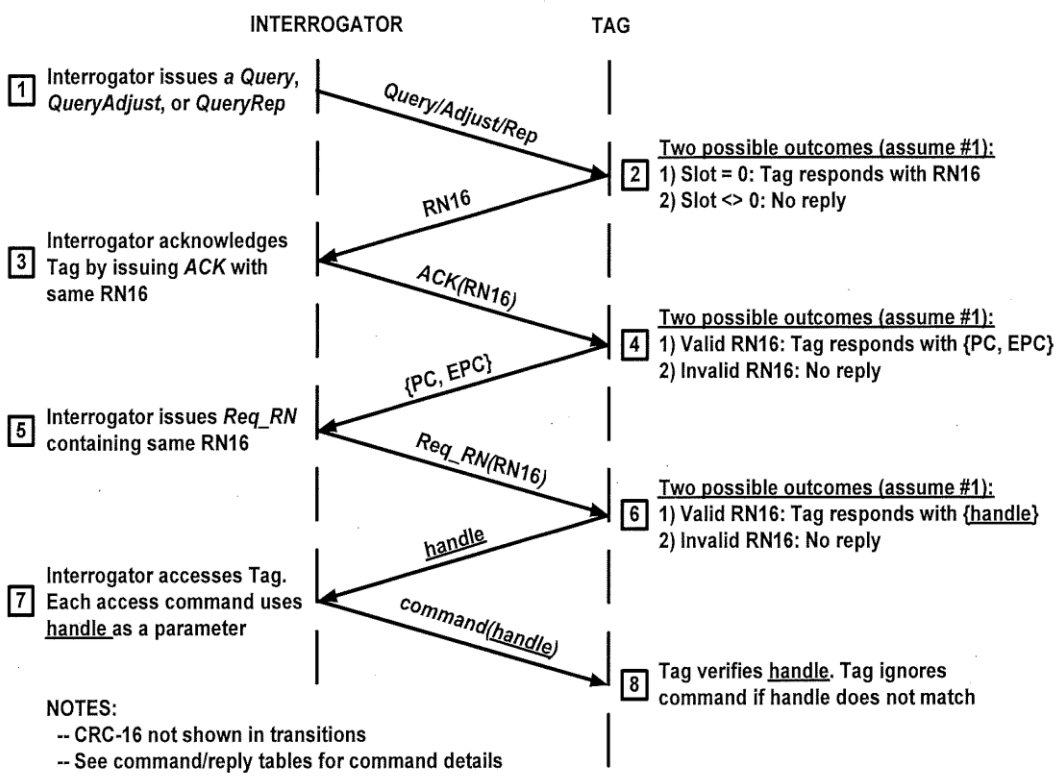


Figure 7.1 Example of tag inventory and access

[31]-[32]

B. Analysis and Assumptions for Comparing Energy Efficiency of Slotted-ALOHA and CDMA/AIC

The proposed CDMA/AIC protocol has been designed to provide energy efficiency for applications where the RFID reader is mobile or handheld. The operating environment can include significant noise, near-far effects, shadowing, and multipath. Increased energy efficiency can translate into more reliable reception, longer battery life between charges (and/or lighter batteries) and extended read range. Since we wish to maximize energy efficiency, the key parameter we will use in comparing the two protocols (proposed CDMA/AIC versus the currently-used Slotted Aloha protocol) is *the minimum total energy that the reader must transmit in order to read a given number of tags with a specified accuracy, within a fixed amount of time.* Accuracy can be expressed as the percentage of tags in the system that are not accurately read (we will call this percentage the *missed tag rate*). For many inventory and supply chain applications, an unread tag rate between 10^{-3} (one unread tag per thousand) and 10^{-4} (one unread tag per ten thousand) is acceptable. **[6][23]-[24]**

Class 1 Gen 2 passive RFID systems are specified to transmit at a maximum of 128 Kbits/sec (which is slow) and, as mentioned earlier, each tag has a maximum of 256 data bits. We will use the maximum transmission speed and maximum number of data bits per tag in our simulations. If our system contains X tags within read range and a maximum read time of Y, to calculate the total energy that must be transmitted by the reader we need to know the following:

For the slotted ALOHA protocol:

- The number of slots per frame
- The number of transmissions required for each slot that contains a message
- The number of transmissions for each slot that does not contain a message
- The maximum number of rounds allowable within the maximum time Y
- And, for various average signal-to-noise ratios,
- The unread message error rate produced by the protocol
- The average number of rounds needed to transmit the X tags

For the CDMA/AIC protocol:

- Processing gain
- The number of transmissions for each round that successfully transmits at least one message
- The maximum number of rounds allowable within the maximum time Y
- And, for various average signal-to-noise ratios
- The unread message error rate produced by the protocol
- The average number of rounds needed to transmit the X tags

We experimented with difference numbers of tags, different processing gains for the CDMA/AIC system, different signal-to-noise ratios, and differing numbers of slots (for slotted ALOHA). We then narrowed our focus to evaluating systems with 9 tags, 10 tags, and 11 tags and, noting the slow maximum transmission speed, we set a 650 msec maximum time to read all the tags. For the CDMA/AIC system we determined

that the maximum practical processing gain, $G_p = 64$, was the most effective (even higher processing gains require more memory then we anticipate being available in the near future for low priced passive tags). We then calculated the time for each CDMA/AIC round as follows:

Number of data bits = 256;

- We require
- 256 * 64 = 16,384 bits
- Each round of CDMA requires approximately

$$\frac{16{,}384}{128{,}000} = 0.\mathbf{128}\ \boldsymbol{seconds}$$

- Therefore, our maximum read time allows up to 5 rounds.

Determining the relative energy efficiency of the CDM/AIC system and the slotted Aloha system was accomplished in 2 steps. First, we determined the SNR vs. missed tag rates for each system, and then we translated the results of performance with missed tag rates of 10^{-3}, 5 x 10^{-4}, and 10^{-4} into energy usage for each system. Using these parameters, we plotted SNR versus Missed Tag Rate (i.e., accuracy) by running the simulation (see Appendix A) 30,000 times for each SNR starting at -1.5 dB and increasing to 7.5 dB in 0.5 dB increments, and then simulating subsequent rounds using the program CDMA2 shown in Appendix B, running that simulation 100,000 times for each SNR value. Results are shown in Figure 7.2.

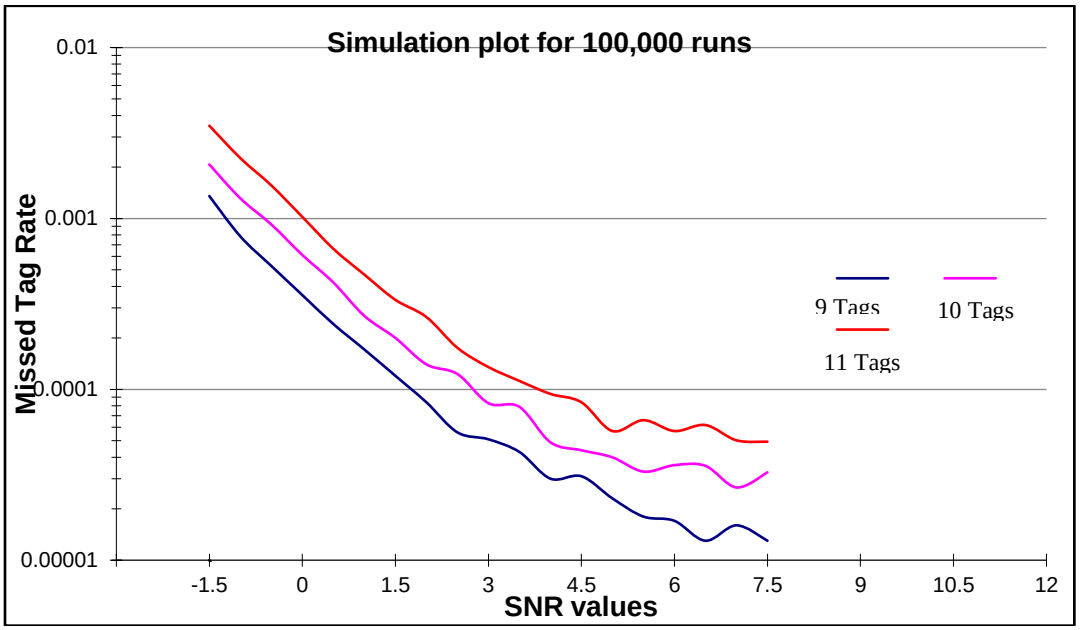


Figure 7.2: Simulation plot of 9 tags, 10 tags, 11 tags for 100,000 runs

We observed that with ***number of tags = 9*** the probability of error was less when compared to ***number of tags = 10 or 11***. This is as expected because a lower number of tags results in less interference and less possibility of tag collisions. Slotted Aloha method, which we will analyze shortly, will also show a decrease in performance if we use a greater number of tags because of more tag collisions (if each frame has only few slots) or more empty slots (if the number of slots per frame is increased). This results in reducing the throughput and efficiency of the system. It may result in more re-transmissions, more usage of power, less accuracy for tag identification. As show in figure 7.2 the curve for 9 tags represents that it has lower error rates for a given SNR. The visibility of low error rates ensures that the amount of energy required to transmit with number of tags = 9 is less. For slightly more power, we can

see that the number of tags could be increased to 10 or 11 tags. The transition from 9 tags to 10 tags is approximately 11% of improvement in throughput, which is about 0.4 dB of improvement, roughly the same as the increase in SNR required to obtain the same error rate for 10 tags as with 9 tags. The enhancement in tag number from 10 to 11 is an additional 10% boost of throughput requiring roughly the same increase in SNR relative to the system with 10 tags. This means that the net energy *per tag* is approximately the same for 9, 10, 11 tag systems.

Our analysis shows the practical processing gain is 64 for standard memory requirements. We performed research for $G_p = 32$ for 9,10,11 tags, but the result showed an increase in the levels of message error rates encountered for the selected SNR values. For different systems with the need to read fewer tags simultaneously (number of tags = 6/7/8), there may be a different scenario where $G_p = 32$ works better but not for our experiments. Based on the above information and the need for high throughput, we selected 10 tags for our system.

Next, we evaluated SNR versus Missed Tag Rate performance of Slotted Aloha for 10 tags with frame size of 4, 6, 8, 10 and 12 slots. We calculated the time for each 8-slot slotted Aloha round as follows:

- *256 bits/tag * 8 slots/frame * 1.5 = 3072 bits*

The factor of 1.5 was used as a conservative value for taking into account the additional overhead caused by the extra handshaking shown earlier in Figure 7.1. Time for one round of 8-slot Slotted Aloha was therefore

$$\frac{3072}{128{,}000} = 0.\mathbf{024}\ \boldsymbol{seconds}$$

Which we rounded up to 0.025 seconds to account for the interrogator's power-up and power-down times during the extra handshaking. Thus, the 650 msec maximum read time allows up to 26 rounds for an 8-slot frame. The maximum number of rounds for 4-slot, 6-slot, 10-slot, and 12-slot frames was calculated in a similar way.

We performed our analysis by running the ALOHA5 simulation by 30,000 times for each frame size for 0.5 SNR increments in appropriate intervals. Results of the simulations are shown in Figure 7.3 Simulation plot of Slotted-Aloha (10 tags; 4, 6, 8, 10 and 12 slot frames)

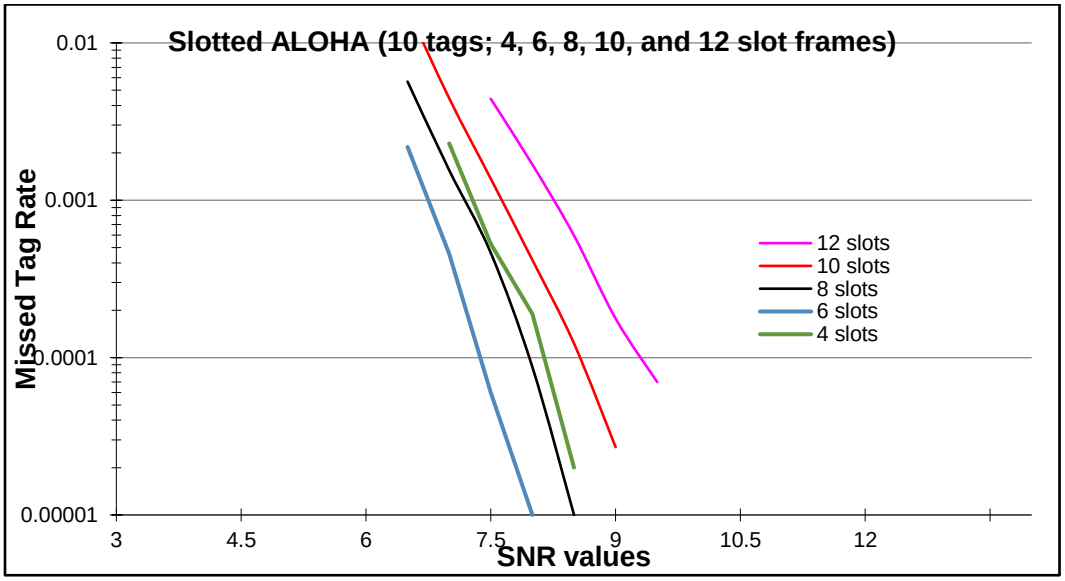


Figure 7.3: Simulation plot of Slotted-Aloha (10 tags; 4, 6, 8, 10 and 12 slot frame)

As will be described in more detail later in this section, maximum energy efficiency for the slotted ALOHA system was achieved for a frame size of 6 slots. Figure 7.4, which shows SNR vs Missed Tag Rates for 8-slot systems with 9, 10, and 11 tags, indicates a slight reduction in performance as the number of tags in the system is increased. We anticipated that the Slotted Aloha method would show a decrease in performance if we use a greater number of tags because of a greater number of tag collisions, resulting in more re-transmissions and more usage of power or less accuracy for tag identification.

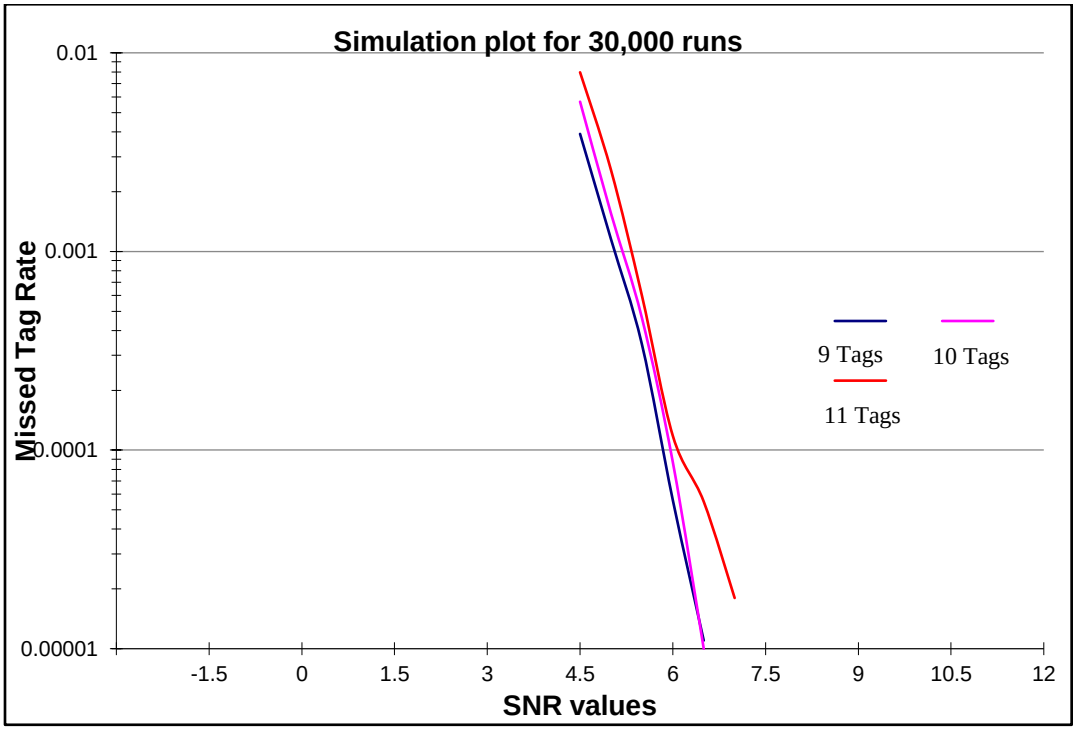


Figure 7.4: Simulation plot for 30,000 runs

The bend observed in the above graph shows a situation of churning (more and more collisions). To establish our initial parameters, we evaluated Figures 7.2, 7.3, and 7.4

for missed tag rates in the range of 10^{-3} to 10^{-4}, and we decided to make a comparison with 10 tags. The comparisons in this case will be very close with number of tags = 9 or 10 or 11 from Slotted Aloha standpoint.

Figure 7.5 compares the 10 tag plots for both CDMA/AIC and Slotted ALOHA. We see that the CDMA/AIC protocol provides approximately 4.9 dB better SNR for missed tag rate of 10^{-3} and approx. 2.75 dB better SNR for missed tag rate of 10^{-4}. Errors in data packets occurs because of two reasons:

a) Tag collisions

b) Presence of noise

If we are in an ideal communication system with noiseless environment the 6-slots Slotted Aloha method would be better than CDMA/AIC, as shown by the crossing of the curves in Figure 7.5 and Slotted Aloha prevailing for higher SNRs. The negative impacts of noise are prominent at lower SNR levels, resulting in more collisions, more power consumption, and greater loss of data. Because CDMA can spread the signal and reduce the effects of noise, the CDMA/AIC system has better performance in the presence of noise.

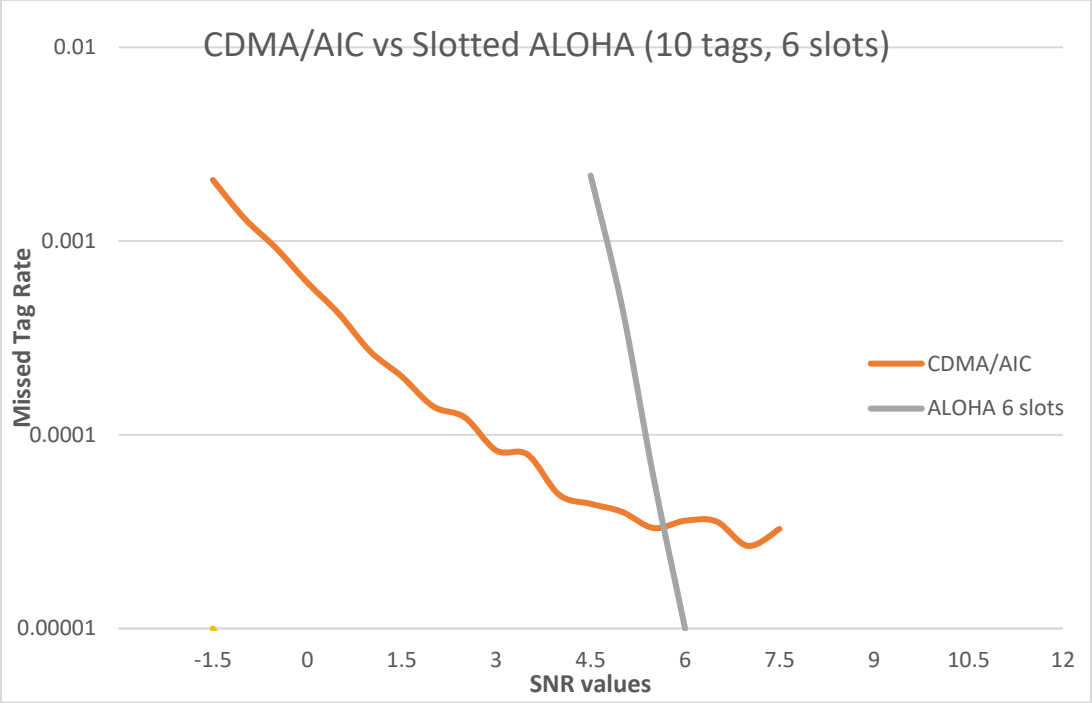


Figure 7.5: Simulation plot for CDMA/AIC vs Slotted ALOHA (10 tags, 6 slots)

In addition to computing missed tag rate versus SNR, the CDMA/AIC and Slotted ALOHA simulation programs also compute the average number of rounds each protocol uses to complete transmission of the data. The table 7.1, which is consistent with Figures 7.5 and 7.3, shows SNRs and average number of rounds for each protocol for missed tag rates of .001, .0005, and .0001. Each system has 10 tags, 256 data bits per tag, and a maximum read time of 650 msec. In addition to a 6-slot Slotted ALOHA system, simulation data is also shown for a 4-slot system and an 8-slot system. This information will be used later in this section to establish that the most energy-efficient frame size is 6 slots.

Table 7.1: SNR & Avg rounds for each protocol with missed tag rates

Missed Tag Rate	8-slot Slotted ALOHA		6-slot Slotted ALOHA		4-slot Slotted ALOHA		CDMA/AIC Gp=64	
	SNR	Avg Rounds	SNR	Avg Rounds	SNR	Avg Rounds	SNR	Avg Rounds
0.001	5.25	13.3	4.85	18.5	5.35	25.8	-0.5	2.7
0.0005	5.5	12.5	5	17.5	5.5	25.1	0.3	2.5
0.0001	6	11.1	5.5	15.4	6	22.4	2.75	2.2

Now that we've established the SNRs necessary for each system to achieve missed tag rates of 10^{-3}, 5 x 10^{-4}, and 10^{-4}, we need to establish a measure to compare the energy efficiency of the two proposed systems at these 3 different levels of accuracy. Let Eb represent the amount of energy that the reader must transmit to receive 1 bit of backscattered signal from a tag with an SNR of 0dB. For the case of slotted ALOHA each tag will need its own transmission from the reader in order to respond in the appropriate slot, but for CDMA/AIC a single transmission from the reader will be sufficient for all tags to simultaneously respond with their backscattered signal. For the Slotted Aloha system, total energy needed from the reader to transmit data for 10 tags is

(number of slots) (256) (avg number of rounds) (SNR) (Eb) (1.5)

where, the factor of 1.5, as explained earlier in this section, is due to extra levels of handshaking required by the Slotted Aloha protocol relative to CDMA/AIC. Prior to its use in the equation, SNR is converted from dB to linear.

For the CDMA/AIC system, total energy needed from the reader to transmit data for 10 tags is

(processing gain) (256) (avg number of rounds) (SNR) (Eb)

Table 7.2 below shows total energy from the reader for each protocol and missed tag rate described in Table 7.1. Energy is given in units of Eb.

Table 7.2: Total energy from the reader of each protocol and missed tag rate

Missed Tag Rate	8-slot Slotted ALOHA	6-slot Slotted ALOHA	4-slot Slotted ALOHA	CDMA/AIC Gp=64
0.001	136859	130213	135835	39426
0.0005	136248	127503	136793	43889
0.0001	135751	125894	136974	67896

Table 7.2 establishes that the 6-slot frame produces the most energy efficient slotted ALOHA system. The table also shows for that the proposed CDMA/AIC system is significantly more energy efficient than the 6-slot Slotted ALOHA system. Table 7.3 summarizes the improvements in energy efficiency offered by CDMA/AIC.

Table 7.3: Improvement in Energy Efficiency of CDMA/AIC vs. 6-slot

Missed Tag Rate	Energy Efficiency Improvement of CDMA/AIC vs. 6-slot Slotted ALOHA
0.001	330.27%
0.0005	290.51%
0.0001	185.42%

As shown in the table 7.3, the proposed CDMA/AIC system is more than 3 times as energy efficient as Slotted Aloha for missed tag rate of one tag per thousand and almost twice as efficient as Slotted Aloha for a missed tag rate of one tag per ten thousand. For mobile and handheld applications, the increase in energy efficiency translates into greater accuracy, extended range, longer operating time between battery charges, and/or smaller/lighter batteries.

VIII. CONCLUSION

The performance limitation caused by various vulnerabilities existing in RFID tag communication with the reader such as the presence of noise, increasing probability of tag collisions, data corruption due to the multipath, shadowing and the near-far issue has been successfully investigated and characterized. The limitation arises due to the lack of anti-collision protocols to accurately identify tags in a large inventory, lack of ability to handle different noise environments, and lack of ability to remove unwanted negative interference in the system which results in consuming more energy.

The Slotted Aloha protocol proves to be energy inefficient for passive tag RFID systems because of the generation of empty slots (if frame size is large) or an increase in retransmissions of tags due to collisions (if frame size is small). With a smaller number of slots per frame and fewer tags, we might believe that there will be fewer empty slots and less probability of collisions, but in low SNR environments the system still fails to correctly read all the available tags within a reasonable time period. Embedding an error correction code in the tag messages will improve accuracy, but at the cost of additional energy and read time and will not reduce the number of tags whose messages are lost due to collision.

A traditional CDMA system with a small number of tags is strong in a low SNR environment if all signals are received at the same level of power, but the protocol has practical limitations in Class 1 Gen 2 RFID systems due to limited number of

spreading codes and the fact that the backscattered signals from the tags reach the reader with a wide variation of different amplitudes due to multipath, shadowing and the near-far effect. We model this variation using a Rayleigh distribution.

There are many applications for energy-efficient passive tag RFID systems, including mobile and handheld applications. Greater energy efficiency could even enable more exotic applications (consider a reader attached to a drone surveying tagged animal livestock from a distance – a high noise environment with interference issues. In a realistic scenario, we might never be in an environment with zero noise. We have proposed, developed, and evaluated a CDMA with Adaptive Interference Cancellation (CDMA/AIC) protocol as a solution yielding energy efficiency in low SNR environments with multipath and shadowing. The CDMA/AIC protocol ensures accurately read tags even with collisions, and successfully removes the negative impacts caused due to noise, near-far, shadowing and multipath. CDMA/AIC does not have the inefficiencies of Slotted-Aloha, has the ability to handle low SNR environments, and does not have the restriction of conventional CDMA that the backscattered signal from each tag must arrive at the receiver with the same amplitude. With missed tag rates in the 10^{-3} – 10^{-4} range, CDMA with AIC can simultaneously read the maximum number of tags and give the best energy efficiency for the overall system. The fluctuations in the amplitude of the signal are closely analyzed and evaluated by the protocol as compared with Slotted Aloha and the traditional CDMA system.

IX. SUGGESTIONS FOR FUTURE RESEARCH

As established in this thesis, the CDMA/AIC protocol shows better energy efficiency than Slotted ALOHA for many applications in the presence of noise, shadowing and multipath. In evaluating the CDMA/AIC protocol there are many areas in which further research can yield additional insights. First, in evaluating the time and energy overhead due to the less efficient handshaking of Slotted Aloha versus CDMA, we used a conservative protocol factor of 1.5, but future analysis is suggested to establish a more precise value. Second, we've established cases where CDMA/AIC excels but we have not established the exact areas of optimization. For the CDMA/AIC to be optimized it is important to know at exactly what point in exactly what profiles the protocol is better than Slotted Aloha and to evaluate the possible reasons for it. The CDMA technique and adaptive interference cancelation process result in excellent energy efficiency, but it is uncertain in which exact possible areas the CDMA/AIC performs better, or the Slotted Aloha method performs better. We also suggest simulations to show how CDMA/AIC performs for a wide range of number of tags and characterize with a wide range of parameters. We also suggest an investigation into research about the exact correlation with a precise number of CDMA/AIC rounds and rounds for Slotted Aloha for a precise number of slots. The CDMA/AIC protocol shows an estimate with 6 slots or 8 slots and successfully shows experimental results with different numbers of slots. But a further investigation on the best possible scenarios with an optimum number of slots can be useful. Third, the Rayleigh fading distribution is worst-case for mobile or handheld RFID applications and gives a significant advantage to our system, but experiments with a different type of

distribution such as Rician fading with exact values for Rice factors and lognormal distribution could be considered for future evaluations. Fourth, in the future, a contrast between CDMA/AIC with dynamic processing gain and Dynamic Frame Slotted Aloha could provide valuable information for the next set of protocol improvements. Additionally, using a different modulation technique to deal with the complexities introduced due to noise, multipath and shadowing in RFID tag systems would be considered valuable. We suggest future experiments can be performed with the development of new protocols and an in-depth investigation with SDMA technique to determine the probabilities of faster recognition of tags. Finally, further evaluation of the CDMA/AIC with more variants of SNR values, number of slots, number of bits, number of tags, and processing gain would be considered an excellent approach to making valuable contributions toward achieving best performance.

APPENDIX SECTION

APPENDIX A
SIMULATION PROGRAM FOR FIRST ROUND OF CDMA/AIC PROTOCOL

```
tic
clear
no_oftags=11
no_ofbits=256;
tau_fail=0;                          %Diagnostic variable
spread_overpowered=0;                %Diagnostic variable
successful_demodulation=0;
sim_runs=10000;
noise_power = 5.600;                 % Scalar value of noise power (sigma)^2 in (mvolts)^2

%The large loop below (using the variable iruncount) spans most of the program and runs the
simulation "sim_runs" times.

for iruncount=1:sim_runs
processing_gain = 64;

tag_arr =                            %Generate array containing original binary data for all tags
randi(0:1,no_oftags,no_ofbits
hadamardmat =
hadamard(processing_gain);
scm=transpose(hadamardmat);

%The rows of scm are now the orthogonal spreading codes.

%The next loop of six lines randomizes (or "scrambles") the rows of scm, which helps remove
correlation between adjacent rows and will subsequently simplify the process of having each tag
randomly choose a spreading code.

for j = 1:no_oftags
scramble=randi(processing_gain);
temp=scm(j,:);
scm(j,:)=scm(scramble,:);
scm(scramble,:)=temp;
  end

sc_t = scm;
sc_t(sc_t == -1) = 0;                %sc_t now contains the different spreading codes in
                                     its rows, converted to
                                     1s and 0s instead of 1s and -1s.
                                     The loops below create the matrix out_array.
                                     Each row of out_array contains the spread data
                                     corresponding to one of the tags.
                                     Because the rows of sc_m (and therefore sc_t)
```

have been "scrambled," the process simulates each tag randomly selecting a spreading code.

```
out_array =
zeros(no_oftags,processing_gain*n
o_ofbits);
  for p = 1:no_ofbits
    for n = 1:no_oftags
      for m = 1:processing_gain
      point=m+(p-
1)*processing_gain;
      out_array(n,point) =
xor(tag_arr(n,p),sc_t(n,m));
      end
    end
end
```

%The next section produces a Rayleigh distribution for the relative amplitude of each tag's transmission.
This simulates the effects of multipath and shadowing.

```
tau = zeros(1,no_oftags);
sigma = 1;
  for n = 1:no_oftags
    tau(1,n) = sigma*sqrt(-2*log(1-
rand(1)));
  end
```

%The next section creates the analog transmitted signals for each tag.

%Nominally, 5 millivolts is used to represent a "1" and -5 millivolts is used to represent a "0," but each tag's signal must then be multiplied by its "tau" to include the effects of multipath and fading.
Each row of the matrix volts_forall will contain the analog signal corresponding to one tag

```
volts_forall = zeros(no_oftags,no_ofbits*processing_gain);
for n = 1:no_oftags
volts_forall(n,:) = (-5 + 10*out_array(n,:))*tau(1,n);
end
```

%Since all the signals are transmitted simultaneously, the total transmitted signal is the sum of all the individual signals.
The section below creates analog_signal, which is the aggregate transmitted signal.

```
volts_add = zeros(1,point);
  for n = 1:no_oftags
  volts_add(1,:) = volts_add +
(volts_forall(n,:));
```

```
  end
transmitted_signal=volts_add;

%Now add the noise to the analog transmitted signal.  Channel attenuation could be added, too,
but won't change the analysis as long as received SNR is the parameter used to evaluate performance.

noise_db =
10*log10(noise_power);                    %remember that signal and noise power measurements
                                          are given in (millivolts)^2
x_noise = wgn(point,1,noise_db);
x_noise=transpose(x_noise);
received_signal=transmitted_signal
+x_noise;

%Now start demodulation, either of the received signal (when z = 1) or of the received signal
after an AIC loop (when z > 1)

New_aggregatedSignal=received_si          % Before AIC is applied, New_aggregatedSignal
gnal;                                     will be the same as received_signal, but not after AIC
                                          is applied

%The large loop below (using the variable z) demodulates, despreads, finds the tag with the
strongest signal, extracts the data from that tag, and then uses AIC to remove the effects
of the strongest tag

  for z=1:no_oftags
%FIRST step: demodulate the received signal.
Later we may want to use different variables to represent the analog received signal
and the demodulated received signal.

  voltsadd_val(1:point) =                 %voltsadd_val is now the demodulated, spread signal
(New_aggregatedSignal(1:point) +          at the receiver (1s and 0s)
abs(New_aggregatedSignal(1:point
))) / 2;
  voltsadd_val(voltsadd_val>0) =
1;
  %SECOND step: despread the first bit of the received signal using each possible spreading code
(we're only despreading the first chip because that information will be sufficient to tell
us which tag sent the strongest signal)

add_signal =                              %add_signal is the first chip of received signal
voltsadd_val(1:processing_gain);
despreading_forall=zeros(processin
g_gain,processing_gain);
for n= 1:no_oftags
    despreading_forall(n,:) =
xor(add_signal,sc_t(n,:));
    end
```

```
%Each row of despreading_forall now contains the first chip of the received signal xor-ed with
one of the possible spreading codes.

despread_results =
despreading_forall;

 %THIRD step: determine which spreading code produced the chip that is most consistent
(i.e., has the most "1"s or the most "0"s).  That code will correspond to the strongest tag.

counting_rows =
zeros(no_oftags,2);
    for n = 1:no_oftags
    counting_rows(n,1) = nnz
(despread_results(n,:) == 1);
    counting_rows(n,2) = nnz
(despread_results(n,:) == 0);
    end

   %Each row of counting_rows contains consistency
information for a particular spreading code.
The first element in the row contains
the number of "1"s, the second element contains
the number of "0"s.

%Now identify the despread tags with the greatest consistency.

  subtract_1 = zeros(no_oftags,1);
    for n = 1:no_oftags
    subtract_1(n,1) =
abs(counting_rows(n,1) -
counting_rows(n,2));
    end

highest_num = max(subtract_1);

%highest_num = maximum differential of 1s and 0s.
The higher this value, the greater the consistency.

guess_winner =
find(subtract_1==highest_num);

%guess_winner is a 1-column array containing the numbers of all tags producing the
greatest consistency (i.e., the strongest tags).
The first element in this array will be used as the strongest tag.

%Note that there may be multiple tags with the same, greatest consistency.

%In most cases, selecting any one of these tags for our first pass through
AIC will allow us to successfully extract the tag's data.
However, if an error occurs, we want to be able to try again using each of the other
"greatest consistency" tags to see if we can extract that tag's data without error


sz=size(guess_winner);

n_strong=sz(1);

%n_strong is the number of tags with the
greatest consistency.

%Create loop for strongest tag
```

```
for n_aic=1:n_strong
    guess_winner_despread_code =
despread_results(guess_winner(n_a
ic),:);
```

%guess_winner_despread_code is the despread code corresponding to the potentially strongest tag (i.e., one of the tags with the greatest consistency)

```
guess_winner_spreading_code =
sc_t(guess_winner(n_aic),:);
```

% guess_winner_spreading code is the spreading code corresponding to the potentially strongest tag.

%***FOURTH step***: Now that a potentially strongest tag has been identified, depsread all the received data using only the spreading code from the potentially strongest tag

```
        for p = 1:no_ofbits
          for m = 1:processing_gain
          point=m+(p-
1)*processing_gain;
          despread_strong_tag(point)
=
xor(voltsadd_val(point),guess_winn
er_spreading_code(m));
          end
        end
```

%***FIFTH step:*** Extract the original unspread data from the potentially strongest tag

```
        for p = 1:no_ofbits
        counting_ones=0;
        counting_zeros=0;
          for m = 1:processing_gain
          point=m+(p-1)*processing_gain;
            if despread_strong_tag(point)==1
            counting_ones=counting_ones+1;
            else
            counting_zeros=counting_zeros+1;
            end
            if counting_ones>=counting_zeros
            data(p)=1;
            else
            data(p)=0;
            end
          end
        end
```

%The array "data" now contains the extracted data from the potentially strongest tag

%***SIXTH step:*** Verify that the extracted data is correct. In practical applications this verification will be done using a small Cyclic Redundancy Check (CRC) code. Since the CRC will be necessary

whether the system uses conventional slotted ALOHA or CDMA, it's easier in this simulation to just check the extracted data against the original data.
This shortcut won't change the performance comparison of the slotted ALOHA system versus CDMA. If extracted data is correct, the code below will set datacheck will equal 0. If the extracted data has one or more errors, *datacheck* will be set equal 1.

```
   datacheck=0;
       for x=1:no_ofbits
         if data(x)-
tag_arr(guess_winner(n_aic),x)==0
         else datacheck=1;
         end
       end
       if  datacheck==1
continue
end
successful_demodulation=successf
ul_demodulation+1;
```

%***SEVENTH step:*** Estimate the amplitude of the received signal corresponding only to the strongest tag.
%First, recreate the spread data corresponding to the strongest tag.

```
       for p = 1:no_ofbits
       for m = 1:processing_gain
       point=m+(p-
1)*processing_gain;
strong_tag(point)=xor(data(p),gues
s_winner_spreading_code(m));
       end
       end
```

% The array "quickcheck" below should contain all zeroes if the respread extracted data matched the original spread data transmitted by the strongest tag. The array will be useful for diagnostics.

```
quickcheck=abs(out_array(guess_w
inner(n_aic),:)-strong_tag);
```

%Second, estimate the amplitude of the received signal corresponding only to the strongest tag. The first part of the estimate involves determining the maximum and minimum values of the received signal for those bits where *strong_tag = 1*.

We start by initializing some variables.
%The variable *temphigh* is initialized to -100 instead of zero because in rare cases all appropriate values of v may be negative, but they will not all be less than -100.
templow is initiated to 100 instead of zero because in rare cases all appropriate values of v may be positive but they will not all be greater than 100. In future, we may want to refine this code

```
    onescount=0;
    temphigh=0;
```

% “over_power” will be nonzero if the extracted data from the strongest tag

```
    templow=0;                                  was in error.  The higher this variable, the more errors.
    highpointer=-100;                           This will be useful in diagnostics
    lowpointer=100;
    over_power=0;
      for p = 1:no_ofbits
        for m = 1:processing_gain
        point=m+(p-
1)*processing_gain;

over_power=over_power+quickche
ck(point);

            if strong_tag(point)==1
            onescount=onescount+1;
              if
New_aggregatedSignal(point)>=te
mphigh

temphigh=New_aggregatedSignal(
point);

highpointer=point;                          %pointer is for diagnostic purposes
              end
              if
New_aggregatedSignal(point)<=te
mplow

templow=New_aggregatedSignal(p
oint);

lowpointer=point;                           %pointer is for diagnostic purposes
              end
            end
          end
        end

%Now we can calculate the estimated amplitude of the strongest tag.

addmaxmin = temphigh + templow;     %amplitude_il is the estimate of the strongest tag's
    amplitude_i1 = (addmaxmin/2);   received signal.

 %The section below provides some debugging diagnostics.
The variable tau_fail will count the number of times in the entire simulation run that
the estimate for tau was in error, and the variable spread_overpowered will show the number
of times in the entire simulation run that the
extracted data from a tag was in error.
```

```
strong_tau_guess =
(amplitude_i1/5);                    %This is the estimate of the strongest tag's tau
strong_tau=tau(guess_winner(1));     %This is the actual value of tau for the strongest tag
                                     %This is the end of the "for n_aic" loop

diagnosis(iruncount,1)=iruncount;

diagnosis(iruncount,2)=strong_tau_
guess;

diagnosis(iruncount,3)=strong_tau;

diagnosis(iruncount,4)=over_power
;
        if abs(strong_tau-
strong_tau_guess) > .001
           tau_fail=tau_fail+1;

diagnosis(iruncount,5)=tau_fail;
        else
        diagnosis(iruncount,5)=0;
        end
        break
      end

%Check to see if all potentially strongest tags have been tried and have failed.
If so, indicate that spreading code has been over_powered and go to the end of the demodulation loop

      flag=0;
      if datacheck==1
        if n_aic>=n_strong
          flag=1;

spread_overpowered=spread_overp
owered+1;
        end
      end
      if flag==1
         break
      end

 %EIGHTH STEP: Subtract effects of strongest tag from received signal.

This step is the actual AIC (cancellation of the effects of the strongest tag)

      for p = 1:no_ofbits
        for m = 1:processing_gain
```

```
        point=m+(p-
1)*processing_gain;
        calculate(point) =
New_aggregatedSignal(point)-((-1
+
2*strong_tag(point))*amplitude_i1)
;
      end
    end

    New_aggregatedSignal =
calculate;
end
end
```

% Storing the values in New_aggregatedSignal
%New_aggregatedSignal now represents the received signal
after the effects of the
strongest tag have been subtracted

% Print the following values for analysis purpose

APPENDIX B
SIMULATION PROGRAM FOR MULTIPLE ROUNDS OF CDMA/AIC PROTOCOL

```
% This simulation models the multiple transmission rounds of the proposed
CDMA system with Adaptive Interference Cancellation.  The simulation
% CDMA with AIC protocol is run first with a given number of bits per packet, a
given processing gain, a given number of tags, and a given noise power.
% The output of CDMA with AIC protocol is the packet error rate at the end of
the first round of transmission.
% The packet error rate is then entered this simulation along with the same
processing gain, number of tags, and noise power as
% CDMA with AIC protocol.  This simulation then determines the number of
rounds needed to successfully transmit all packets without error.  One exception: if
there are still packets that haven't been transmitted without error after the
maximum specified number of rounds ("max"), an overflow counter is
incremented, and the number of un-transmitted packets is added to a total counter
(missed_tags).


tic
processing_gain=64;          %Use value consistent with CDMA with
                             AIC protocol


sigma=1;

max=5;                       %Maximum number of rounds
collisions=0;
message_errors=0;
total_rounds=0;
overflow=0;
missed_tags=0;
sim_runs=100000;

packet_error_rate=0.2905;

 %Output from CDMA with AIC
protocol

for iruncount=1:sim_runs
no_oftags=11;
```

```
%Use value consistent with
CDMA with AIC protocol

%If there are either collisions
(due to two tags choosing the
same spreading code) or packets
received in error, another round
of transmissions will be required
for all the packets involved in
collisions or errors.  The loop
below reduces the number of
tags to only those in collision or
error and provides another round
of transmission.

for irounds=1:max
collisionflag =
zeros(1,no_oftags);

%collisionflag is a 1xno_oftags
array that will be used to indicate
whether or not a particular tag's
packet was involved in a
collision

errorflag = zeros(1,no_oftags);

%errorflag is a 1xno_oftags
array that will be used to indicate
whether or not a particular tag's
packet was received in error

% Randomly choose a
spreading code for each tag

for tag =1:no_oftags
codechoice(tag)=randi(processin
g_gain);
end

% This loop determines the
number of messages that collide
```

```
because their tags chose the
same spreading code

for j=1:no_oftags
      for k=j+1:no_oftags
         if
codechoice(j)==codechoice(k);
         collisionflag(j)=1;
         collisionflag(k)=1;
         end
      end
   end
collisions=collisions+sum(collisi
onflag);

% "collisions" contains total
number of collisions.  This may
be a useful diagnostic.
% The large loop below
determines if an uncollided tag's
message is successfully
transmitted or if noise causes a
packet error

   for j=1:no_oftags
      if collisionflag(j)==1
continue

% If collision occurred there is
no reason to check noise
else
         pick=rand;
         if
pick<=packet_error_rate
            errorflag(j)=1;
         else
            errorflag(j)=0;
         end
      end
   end

no_oftags=sum(collisionflag)+su
m(errorflag);
```

```
    total_rounds=total_rounds+1;
    if no_oftags==0
       break
    end
    if irounds==max
       overflow=overflow+1;

missed_tags=missed_tags+no_of
tags;
       break
    end
    end
Message_errors =                    % "message_errors" contains total
message_errors+sum(error_flag)         % number of message errors due to noise.
;                                   Possibly a useful diagnostic.
End
%The next four lines are just
print-outs for diagnostics
collisions
%Messages_transmitted_without
_collision=(sim_runs*no_oftags)
-collisions
%Messages_in_error_from_nois
e=message_errors
%Message_error_rate=Messages
_in_error_from_noise/Messages
_transmitted_without collision
total_rounds

%The average number of rounds
per simulation will be
total_rounds/sim_runs

Overflow                            %This is the number of times per sim_runs
                                     that there was at least one tag's data still
                                    %in error after the maximum number of rounds.


missed_tags
%It's possible that more than one
tag was still in error after the
maximum number of rounds.
missed_tags is the total number
of tags that were not correctly
```

received after sim_runs
simulations. Percentage in error
=
missed_tags/(no_oftags*sim_run
s).
toc

APPENDIX C
SIMULATION PROGRAM FOR SLOTTED ALOHA PROTOCOL

```
% This simulation models a traditional slotted ALOHA RFID system.  For a given
number of bits per packet, a given number of slots, a given number of tags, and a
given noise power, the simulation determines the average number of rounds
needed to successfully transmit all packets without error.
One exception: if there are still packets that haven't been transmitted without error
after the maximum specified number of rounds,an "overflow" counter is
incremented and the number of untransmitted packets is added to a total counter
(missed_tags)

 tic
 no_ofbits=256;
 no_ofslots=8;
 sigma=1;
 max=26;
 collisions=0;
 message_errors=0;
 total_rounds=0;
 overflow=0;
 missed_tags=0;
 sim_runs=10000;
 noise_power = 14.058;                    % Scalar value of noise power
                                          (sigma squared) in millivolts.
                                          %The large loop below (using
                                          the variable iruncount) spans
                                          most of the program and runs
                                          the simulation "sim_runs" times.
 for iruncount=1:sim_runs
 no_oftags=9;

   %If, after the previous round, there are either collisions or packets received in
error, then another round of transmissions will be required for all the packets
involved in collisions or errors.
The loop below reduces the number of tags to only those in collision or error
and  provides for another round of transmission.
 for irounds=1:max                        %collisionflag is a 1xno_oftags
    collisionflag = zeros(1,no_oftags);   array that will be used to
                                          indicate whether or not a
                                          particular tag's packet was
                                          involved in a collision
```

```
errorflag = zeros(1,no_oftags);          errorflag is a 1xno_oftags array
                                         that will be used to indicate
                                         whether or not a particular tag's
                                         packet was received in error.

 % Randomly choose a slot for each tag

   for tag =1:no_oftags
      slotchoice(tag)=randi(no_ofslots);
   end

% This loop determines the number of messages that collide because their tags
chose the same slot

  for j=1:no_oftags
      for k=j+1:no_oftags
         if slotchoice(j)==slotchoice(k);
         collisionflag(j)=1;
         collisionflag(k)=1;
         end
      end
   end
collisions=collisions+sum(collisionflag);   % "collisions" contains total
                                            number of collisions in all the
                                            simulation runs.  It's not a very
                                            useful number except for
                                            diagnostics

% The large loop below determines if an uncollided tag's message is
successfully transmitted or if noise causes a packet error

for j=1:no_oftags
      if collisionflag(j)==1
continue                                 % If the tab was involved in a
                                         collision there is no reason to
                                         check noise
else
tau = sigma*sqrt(-2*log(1-rand(1)));     %add Rayleigh fading
noise_db = 10*log10(noise_power);
         for k=1:no_ofbits
if errorflag(j)==1                       %skip loop if error has already
                                         been detected in tag
```

```
  break
            end
            bitval=randi(0:1);
            x_noise = wgn(1,1,noise_db
            if bitval==0                          % This IF statement checks to
                                                  see if a 0 was transmitted and
                                                  the noise was large and positive

             if x_noise>=5*tau
               errorflag(j)=1;
             end
Else                                              %This ELSE statement checks
                                                  to see if a 1 was transmitted and
                                                  the noise was large and negative
             if x_noise<-5*tau
              errorflag(j)=1;
             end
           end
         end
       end
   end
                                                  %Calculate the number of tags
no_oftags=sum(collisionflag)+sum(errorflag)       that will need to be transmitted
;                                                 for the next round

total_rounds=total_rounds+1;
   if no_oftags==0
      break
   end
   if irounds==max
      overflow=overflow+1;
      missed_tags=missed_tags+no_oftags;
      break
   end
   end
                                                  % "message_errors" contains
message_errors=message_errors+sum(errorfl         total number of message errors
ag);                                              due to noise

End
%The next four lines are just print-outs for diagnostics collisions
%Messages_transmitted_without_collision=(sim_runs*no_oftags)-collisions
%Messages_in_error_from_noise=message_errors
```

```
%Message_error_rate=Messages_in_error_from_noise/Messages_transmitted_w
ithout collision

total_rounds                    %The average number of rounds
                                per simulation will be
                                total_rounds/sim_runs
Overflow                        %This is the number of times
                                per sim_runs that there was at
                                least one tag's data still in error
                                after the maximum number of
                                rounds

missed_tags                     %It's possible that more than
                                one tag was still in error after
                                the maximum number
                                ofvrounds.  missed_tags is the
                                total number of tags that were
                                not correctly received after
                                sim_runs simulations.
                                Percentage in error =
                                missed_tags/(no_oftags*sim_run
                                s).
toc
```

Design of Slotted Aloha protocol

Slotted-Aloha introduces discrete timeslots and increases maximum throughput by allowing transmission of the tags in individual slots. This approach is followed for designing the Slotted-Aloha protocol.

The simulation results obtained to test the slotted aloha protocol follows the design steps mentioned below:

The protocol begins by selecting the following given information:

a) Number of bits per packets = 256
b) Number of slots = 8
c) Number of tags = 11 (we also tested the protocol for 9 and 10 tags)
d) Number of noise power (from 10.5 DB to -1.5 DB)

Step 1: Enter the given data for no. of bits per packets, no. of slots, no. of tags, number of noise power.

Step 2: Randomly select a slot

Step 3: Determine the number of messages that collide (a scenario when two tags select the same timeslot)

Step 4: Determine the number of tags successfully transmitted. (This step checks the uncollided tags and verifies if noise caused any packet error.)

Step 5: Add Rayleigh fading distribution.

Step 6: Determine the intensity of noise in transmitted signal and analyze whether it creates positive or negative impacts on the efficiency of the system.

Step 7: Calculate the number of tags that will be required for re-transmission of their information.

The protocol successfully gives estimate of the following information:

- Messages transmitted without collisions
- Messages with error due to noise
- Message error rate
- Total number of rounds to complete the reading of available tags
- The number of missed tags

Formulas derived to calculate the message error rate and its relationship with messages successfully transmitted without collision is expressed below:

- *Messages transmitted without collision = [Total simulation runs * Number of tags] – collisions*

- $\textit{Message error rate} = \frac{Messages\ detected\ with\ errors\ from\ noise}{Messages\ transmitted\ without\ collision}$

- $\textit{Total rounds} = \frac{Total\ rounds}{Number\ of\ simulation\ runs}$

From communication theory we know that the probability of bit received with error is expressed using the following equation:

$$Q\left[\frac{5}{sqrt(noise\_power)}\right]$$

Our simulation uses +5 millivolts to represent a 1 and -5 millivolts to represent 0

REFERENCES

[1] R. Z. Doany, C. Lovejoy, K. Jones and H. Stern, "A CDMA-based RFID inventory system: A CDMA approach as a solution for decreased power consumption," *IEEE*, p. 4, 2016.

[2] L. Jun'e, Z. Xiaocui and L. Bingwu, "The application of RFID technology in the inventory management," in *IEEE*, Dalian, China, 2010.

[3] A. N. Nambiar, "RFID Technology: A Review of its Applications," in *Proceedings of the World Congress on Engineering and Computer Science* , San Francisco, USA.

[4] N. L. Siew, "A RELIABILITY STUDY OF THE RFID TECHNOLOGY," NAVAL POSTGRADUATE SCHOOL, MONTEREY, CALIFORNIA , 2006.

[5] J. Liu, "Wireless multipath fading channels modeling and simulation based on Sum-of-Sinusoids," in *IEEE*, Wuhan, China, 2016.

[6] K. Saravanakumar, K. Deepa and N. S. Kumar, "A study on possible application of RFID system in different real-time environments," in *IEEE*, Kollam, India, 2017.

[7] M. K. Lim and M. Winsper, "Exploring value-added applications of RFID systems in industry and service sectors," in *2012 8th International Conference on Information Science and Digital Content Technology (ICIDT2012)*, Jeju, South Korea, 2012.

[8] S. Tedjini and E. Perret, "Radio-frequency identification systems and advances in tag design," in *URSI Radio Science Bulletin (Volume: 2009 , Issue: 331 , Dec. 2009)*, 2009.

[9] L. Chen, H. Ba, W. Heinzelman and A. Cote, "RFID range extension with low-power wireless edge devices," in *2013 International Conference on Computing, Networking and Communications (ICNC)*, San Diego, CA, USA, 2013.

[10] E. P. S. Tedjini, "Radio-Frequency Identification," The Radio Science Bulletin, 2009.

[11] "Radio-frequency identification," [Online]. Available: https://en.wikipedia.org/wiki/Radio-frequency_identification.

[12] "RFID Tags," [Online]. Available: https://www.epc-rfid.info/rfid_tags.

[13] "WHAT IS RFID?," [Online]. Available: https://www.zebra.com/us/en/resource-library/faq/rfid/what-is-rfid.html#gen1-2.

[14] "Channel access method," [Online]. Available: https://en.wikipedia.org/wiki/Channel_access_method.

[15] H.-C. Liu, "Performance analysis of multi-carrier RFID systems," Istanbul, Turkey, 2009.

[16] H.-C. Liu, "The Approaches in Solving Passive RFID," National Taiwan University of Science and Technology , Taiwan.

[17] L. A. Burdet, "RFID Multiple Access Methods," US: FCC Federal Communications Commission, Japan, 2004.

[18] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/ALOHAnet.

[19] S. Maharjan, "RFID and IOT: An overview," Simula Research Laboratory, 2010.

[20] D. K. Klair, K.-W. Chin and R. Raad, "A Survey and Tutorial of RFID Anti-Collision Protocols," in *IEEE Communications Surveys & Tutorials (Volume: 12 , Issue: 3 , Third Quarter 2010)*, 2010.

[21] "A Comparison of RFID Anti-Collision Protocols for Tag Identification," *Research gate*, 2018.

[22] I. A. Andreas Loeffler and F. Schuh, "CDMA-Based UHF-RFID System with Semi-Passive UHF Transponders," *International Journal on Advances in Telecommunications, vol 4 no 1 & 2, year 2011, http://www.iariajournals.org/telecommunications/*, p. 16, 2011.

[23] B. E. I. 9.-1. ©. 2. S. M. L. A. R. Reserved, "Inventory, Inventory Management, Accounting How to Order, Manage, Value, and Report Inventory, step-by-step," 2019. [Online]. Available: https://www.business-case-analysis.com/inventory.html.

[24] "The REAL Shocking costs of dead inventory!," 3 June 2016. [Online]. Available: http://www.cutwatersolutions.com/blog/the-real-shocking-costs-of-dead-inventory/.

[25] A. K. Maini and V. Agrawal, "Chapter 6 Multiple Access Techniques 286," in *Satellite Technology: Principles and Applications, 3rd Edition*, 2014, p. 846.

[26] S. Faruque, Radio Frequency Multiple Access Techniques Made Easy, Springer, 2019.

[27] S. Kang and Z. Prodanoff, "RFID Model for Simulating Framed Slotted ALOHA Based Anti-Collision Protocol for Muti-Tag Identification," 2010.

[28] L. G. .. Roberts, ALOHA PACKET SYSTEM WITH AND WITHOUT SLOTS AND CAPTURE, 1975.

[29] A. C. Dabas, B. M. Balhara and C. J. Gupta, "CDMA based Anti-Collision Deterministic," *International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009* , p. 4, 2009.

[30] S. L. Peng, "Improved Dynamic Frame Slotted ALOHA Algorithm for Anti-collision in RFID System," in *Knowledge Discovery and Data Mining. Advances in Intelligent and Soft Computing,*, Springer, Berlin, Heidelberg.

[31] W. G. B. deMatos, M. Ueda, T. R. d. Camargo and A. Morais, "Inventory control with RFID integration," in *IEEE,* Sao Paulo, Brazil, 2015.