EXTENSION OF THE CDMA/AIC PROTOCOL THROUGH ANALYSIS AND SIMULATION

by

Paul Nicanor Sanasi, B.Tech.

A thesis submitted to the Graduate Council of
Texas State University in partial fulfillment
of the requirement for the degree of
Master of Science
with a Major in Engineering
May 2021

Committee Members:

Harold Stern, Chair

William Stapleton

George Koutitas

COPYRIGHT

by

Paul Nicanor Sanasi

2021

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

This work is protected by the Copyright Laws of the United States (Public Law 94-553, section 107). Consistent with fair use as defined in the Copyright Laws, brief quotations from this material are allowed with proper acknowledgement. Use of this material for financial gain without the author's express written permission is not allowed.

Duplication Permission

As the copyright holder of this work I, Paul Nicanor Sanasi, authorize duplication of this work, in whole or in part, for educational or scholarly purposes only.

ACKNOWLEDGEMENTS

First and above all, I thank **The Lord Almighty** for His wisdom, blessings, guidance and protection over me to undertake this research study and complete it.

I express my sincere gratitude to my thesis advisor, **Dr. Harold Stern**, for his guidance and support. His expertise in the field of wireless communication has enabled me to learn and understand various concepts with ease. I am forever grateful for his timely advice, scholarly suggestions and scientific approach that led me to complete this research. I also thank him for being available online most of the time to communicate concerning my thesis work.

I would like to thank my committee members **Dr. William Stapleton** and **Dr. George Koutitas** for their valuable suggestions all throughout my thesis work. I am grateful for their constant encouragement and introducing me to possible challenges and approaches.

I would also like to thank **Dr. Vishu Viswanathan**, Graduate Advisor at the Ingram School of Engineering for his guidance and motivation during my study here at Texas State University. I especially thank him for his valuable suggestions in both orientation and presentation sessions.

I would like to thank all the faculty of Ingram School of Engineering who have taught me all the required coursework. I also thank the office staff of Ingram school of Engineering for helping me with the required paperwork.

I also thank my beloved parents Dr. Paul Douglas and Vijaya Douglas for all their prayers, love and support. I also thank my twin brother Lt. Paul Nicolas for his love and support all the time. I also thank my grandparents and other family members for their love and encouragement.

Lastly, I thank all my seniors and friends here at Texas State University. I am grateful to Priyanka Kodangi, Venkateshwara Mekha, Tarun Kadukuntla, Preeti Gokhale, Swathi Mekala, Spandana Vottem, Vinod K Subramanyam, Ajay Reddy Gudi, Saketh Kapardi and Mowgli Singaraju for their friendship and encouragement.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

Figure **Page**

LIST OF ABBREVATIONS

Abbreviation	Description
RFID	Radio Frequency Identification
AIC	Adaptive Interference Cancellation
TDMA	Time Division Multiple Access
FDMA	Frequency Division Multiple Access
CDMA	Code Division Multiple Access
SDMA	Spatial Division Multiple Access
MAC	Multiple Access
ALOHA	Additive Links On-line Hawaii Area
UHF	Ultra High Frequency
PDF	Probability Density Function
CDF	Cumulative Distribution Function
DSSS	Direct Sequence Spread Spectrum

ABSTRACT

RFID tags find their application in many areas such as inventory tracking, shipment tracking, vehicle tracking and identification, and animal tracking and identification. Passive RFID tags have been used in most of the applications as they are extremely cost-efficient, and they have a longer lifespan. Previous researchers have developed a CDMA based Adaptive Interference Cancellation protocol to increase energy efficiency and reduce multipath effects. In Adaptive Interference Cancellation, we would read the strongest tag and remove its effect and then read the next strongest, remove its effects and so on. In analyzing the protocol, researchers have used a Rayleigh distribution to establish the relative amplitudes for each of the tags to simulate the effects of multipath and shadowing for each tag. The Rayleigh distribution, which models received signal strength with no line-of-sight component, is the worst case for many applications but is not the worst case for assessing the performance of the protocol.

This research aims to extend the Adaptive Interference Cancellation algorithm to a broader group of applications. We evaluate the CDMA based Adaptive Interference Cancellation Protocol with different types of distributions such as Rician fading and Lognormal distributions. Rician fading technique has less fluctuations and a series of Rice factors due to reflections and Line of Sight which may reduce the performance of the AIC method. We also aim to use standard lognormal distributions to represent extremely strong Line of Sight.

I. INTRODUCTION

Radio Frequency Identification (RFID) is an automatic identification system which we use in our everyday lives. It works on data capturing technology. Capturing accurate data from the tags plays a very important role in managing inventories. An inventory is a space which has thousands of objects with tags attached to it. RFID is one of the fastest techniques to scan, record data and manage inventories. Many retail businesses have seen an increase in their sales with RFID technology [1]. There are other various applications of RFID in different real time environments [2], including transportation, retailing, agriculture, government and military, human identification, health care, clothing and traffic management. According to research conducted by BCC Research, the global market for RFID technologies is forecast to reach $38.0 billion by 2021. This will be from $16.2 billion in 2016 and grow at a compound annual growth rate of 18.6 percent, during that timeframe [3]. In this thesis, we mainly focus on challenges related to RFID tags in supply chain management [4], in particular challenges caused by collisions and reduced signal strength.

Benefits of RFID systems

Solving these challenges is a very worthwhile effort because of the benefits of properly working RFID systems. Some of the benefits of RFID are:

Increases in asset visibility:

RFID tags can be read from anywhere within range in the facility. In facilities like a large warehouse, it is extremely difficult to search for an item using a traditional bar code and a scanner. Employees and customers will also know the status of the item in real-time. RFID tags help in resolving issues like misplaced materials, oversight, poor organization and mistakes made during the manual process.

Improvement in employee productivity:

With the advent of RFID tags, employees no longer have to be within the line of sight of an item to track it. It helps in reducing the time consumed to scan individual bar codes, search for misplaced tools or count inventory amounts. This will lead to an increase in the speed and reductions in labor costs which helps in improving the overall productivity of the facility.

Better security:

With RFID tracking, we can mitigate risk, theft and loss. Misdistribution of the items can be avoided by tracking the movement of each item in the facility. This leads to a much more organized facility which increases the production and revenue.

Challenges of RFID systems

The challenges in RFID tag systems include:

Tag collisions:

Reducing tag collisions plays a huge impact in managing inventories. The two important components in an RFID system are an RFID reader and an RFID tag. The main task of an RFID reader is to capture information from every tag, understand and process it. With multiple tags being present around the reader and with noise, it is harder for the tags to communicate with the reader. Tag collisions happen when these tags simultaneously try to communicate with the reader and the reader tries to capture the tags' data. The impact of this issue is that the reader may drop the information or create a wrong entry. Creating a wrong entry or missing data creates a huge impact in inventory management. Tags that experience collision will wait for a random period of time and then retransmit their data back to the reader. Multiple tag collisions lead to multiple retransmissions which will increase the amount of power consumed by the system. Multiple access techniques are used as anti-collision protocols in the communication between the reader and the tag with minimum interference. A variety of multiple access techniques have been proposed for RFID systems such as Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), Spatial Division Multiple Access (SDMA), Frequency Division Multiple Access (FDMA) and hybrid multiple access techniques [5][6][7]. We will further discuss the CDMA technique as it is used in our thesis.

Noise, Signal Strength Variation, and Interference:

In wireless communication, noise is any natural or man-made energy interference that affects the quality of a wireless signal. Noise in general can be classified as external noise and internal noise. Since RFID technology uses wireless communication, there are certain problems caused by interference. The RFID reader communicates with the tag by using electromagnetic waves, and due to objects present in between the reader and the tag, the electromagnetic waves often do not travel in a direct line. They will reflect from certain objects and will follow different paths. Because of this there will be amplitude variations in the backscatter signal that is transmitted from the tag to the reader. Depending on the RF environment, the amplitude variations can be modeled as one of three different probability distributions: Lognormal, Rice, and Rayleigh. These distributions and the effects of amplitude variation will be discussed in depth in Chapter

3. There are various effects of interference within UHF passive RFID systems. Three types can be considered based on RFID reader and the tag.

Tag-to-tag interference:

This type of interference occurs when multiple tags respond to the same reader simultaneously. This type of interference, referred to as tag collisions earlier in this chapter, will be the main type of interference considered in this thesis. Tag collisions can be reduced by having each tag respond at different times or using multiple access techniques to mitigate the issue.

Tag-to-reader interference:

This type of interference occurs when a tag is in the interrogation zone of multiple readers and more than one reader transmits simultaneously.

Reader-to-reader interference:

This type of interference occurs when signals from neighboring readers interfere. It can be avoided by having different readers operate at different frequencies or in different time slots or by using a multi-reader anti-collision algorithm.

We will be analyzing systems with a single reader and therefore will not be assessing reader-to-reader or tag-to-reader interference in this thesis. However, the analysis we will do for interference between tags in the same system will also be valid for interference between tags in different systems.

Near far problem (a specific type of tag collision):

The Near-far issue is a case where a tag that is present nearby to the reader will send a very strong signal and tags that are far from the reader (or are shadowed) and which send a signal at the same time as the near tag are not captured by the reader. The

Signal to Noise Ratio (SNR) of the near signal will be so high that it will create difficulty to read the tag that is far away from the reader.

Organization of Thesis

The thesis is organized as follows: Chapter 1 of this thesis provides a brief introduction about Radio Frequency Identification. Chapter 2 focuses on the basics of an RFID system and its working principles. It also discusses the various operating frequencies, components and types of RFID tag systems and the types of Multiple Access Techniques that can be used in an RFID system. Chapter 3 explains about different RF environments and fading in wireless communications, its classifications and modelling of various fading systems. Chapter 4 describes previous research, in particular using CDMA/AIC in passive RFID systems. Chapter 5 focuses on extending the limited evaluations of the CDMA/AIC protocol that have been done. These extensions will significantly expand the range of RFID environments for which the protocol may be useful, thereby improving the performance of RFID in an extended set of applications. Chapter 6 gives the results of the extension and in-depth analysis of the results. Chapter 7 concludes the aims achieved in this research work. Chapter 8 proposes various possible ideas for future research.

II. BASICS OF RFID SYSTEMS

Radio Frequency Identification (RFID) uses electromagnetic fields to automatically identify, and track tags attached to objects. An RFID system consists of an RFID reader which captures information from each tag attached to any object present in the read range, antennas which are included with both the reader and the tag and an RFID tag which consists of a digital memory chip to store a unique identification number and additional data. When an electromagnetic signal is generated by an RFID reader, the tag transmits digital data back to the reader [8]. An RFID reader, which is also called as interrogator, can identify more than a thousand items per second. RFID readers can operate in two ways: near-field, where the reader antenna uses magnetic coupling for power transfer and far-field, where the reader antenna uses electromagnetic coupling. The read range of the near-field reader antennas is less than 30 cm, and the read range of the far-field reader antennas is greater than 30 cm. Depending on the operating frequency band, the read range of the far-field RFID system can be 10 meters or greater. An RFID tag system is a boon to the supply chain management business as it helps in effectively collecting, managing and distributing information besides maintaining security control. RFID tag systems can be read-only or can perform two-way communication.

Frequency Bands and Types of RFID Systems

The RFID technology works primarily in three operating frequency bands:

- Low frequency (125-145 KHz) used in applications like animal tracking, access control, and car keys
- High Frequency (~13 MHz) used in applications like personal ID cards, library books and DVDs

- Ultra-high frequency (860-960 MHz) used in applications like inventory management, asset tracking and race timing

RFID tag systems can be classified into three types:

Active tag systems:

In an active RFID system, tags use their own battery to power the device. The tags continuously transmit the signal using the internal battery power. Active RFID tags are mainly used where there needs to be a large coverage of area. Certain toll booths, system locating, train signal detection and traffic signal detection are some of the main areas where active tag systems are used. Active tags are expensive and each tag costs about $10 to $100 depending on the specification and application. In an inventory where there can be thousands of tags attached to objects, attaching an Active RFID tag will be a huge cost. Moreover, the battery in an active RFID tag does not last forever. The batteries have to be replaced or a new active tag must be engaged. Active RFID tags are also used in aerospace industries as they have a long range and can be enabled with a high memory chip which can hold large amounts of data.

Passive tag systems:

Since an inventory can have millions of objects with tags attached to each object, it uses passive tag systems as they are cost efficient. Each passive tag costs about 10-20 cents and they don't need a battery.

Important components of passive RFID system are the RFID reader and the RFID tag. Passive RFID tags do not have a battery. They receive energy from an electromagnetic signal that is transmitted from the reader. The tags reply with a backscatter signal to the reader. In an inventory many tags are identified with a unique ID number called the Electronic Product Code (EPC). The EPC data is compressed in binary form. It gives the product details for that particular tag. There are many standards developed for the EPC data. We will use a modification of the current standards developed for class I generation 2 tags in this research. An RFID reader and a tag communicate with each other. With EPC class 1 generation 2 tags, first, the reader sends a power up signal because passive RFID tags do not have a battery. That will energize the IC circuit present in the tag, and it will ask the tag to generate a random response delay number. The reader will issue a decrementing command and will decrement this delay time by 1. Once the response delay time reaches to 0, the tag will generate a handle number known as temporary ID number and send it to the reader. The reader will then take the number and send an acknowledge signal back to the tag and then ask it to send the original EPC number. If a collision happens, the entire process is repeated from the start.

Fig 2.1 Current Communication Protocol [1]

Semi passive RFID tag systems:

Semi-passive RFID tags are a combination of both the active tag system and the passive tag system. They are also known as semi-active systems or battery-assisted passive systems. The semi-passive RFID tags work on the same principle as the passive RFID tag and will additionally have a battery pack for long range communication. Additionally, sensors, sound notifications and real-time tracking can also be applied in the semi-passive RFID tag systems. Due to all the additional features, this type of tag is mostly used in environmental monitoring applications. A semi-passive tag costs around 50-80 cents [9].

Multiple Access Techniques in RFID Tag Systems

In wireless communication, a Multiple Access (MAC) technique allows more than two terminals to communicate their information using a mutual transmission channel in the most effective approach. A variety of MAC techniques are used to overcome interference faced in communication between RFID tags and readers [10][11][12][13]. Some fundamental techniques used in the RFID tag systems to overcome common challenges are as follows:

Time Division Multiple Access (TDMA)

Time division multiple access can be implemented using two kinds of approaches

Deterministic Approach:

In a binary tree scheme, each node denotes a unique ID number of the tag. This tree increases with an increase in the number of tags and if there is a collision, it has to wait until the entire branch is completely scanned. This protocol delays operation and creates more collisions with an increase in the number of tags.

Stochastic Approaches (ALOHA and its variants):

Pure Aloha: In the pure aloha technique, tags just transmit (via backscatter) their data when illuminated by a reader. Whether the reader is available to read or not, the tags will not wait for the reader to read and they will not wait for any acknowledgement. They will just send their data.

Slotted Aloha: With an increase in the number of tag collisions, there is an increase the number of retransmissions. In order to overcome the inefficiencies of the deterministic approach the slotted aloha protocol was developed. The entire time interval is divided into discrete time slots and each tag transmits in a randomly chosen time slot. The problem with this approach is that sometimes multiple tags respond with same slot number which causes a collision. For retransmission of the packets, the collided packets are retransmitted after a random delay. As was described earlier, the current Class I Generation II uses a slotted aloha protocol as its Multiple Access Technique [12].

Basic Frame-Slotted Aloha (BFSA): Another variant of the slotted aloha protocol is the Frame-Slotted ALOHA Method. This method is an extended version of the slotted ALOHA method and discrete time division by grouping several slots into frames and each frame having N number of slots. FSA protocol is mainly used in satellite networks, wireless LAN and Machine to Machine network implementation. It avoids collisions and maintains the efficiency of the system. In this process, only the data packets with no collisions are detected and the collided data packets (also called backlogs) are retransmitted in the subsequent frames. The basic frame slotted ALOHA method has four different variants such as BFSA-non muting, BFSA-muting, BFSA-non-muting early end and BFSA-muting-early end. Since the FSA protocol requires comprehensive system design, a limited amount of work has been performed using this protocol [14].

Dynamic Frame Slotted Aloha (DFSA): The difference between BFSA and DFSA is that the BFSA uses a fixed frame size. Due to this the system efficiency decreases greatly when the number of tags are not in the anticipated range. The Dynamic frame slotted ALOHA protocol has a varying frame size. The DFSA protocol implements the early-end feature. There are two methods to regulate frame length. They are:

1. Estimate the unread tags and set the next frame length according to the number of unread tags. 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, number of slots corresponding to zero tags (empty slots) and one tag. This data is used to estimate the optimal frame size and to predict the number of tags in that round [15][16].
2. Use the number of empty slots, the slots with collision and the slots filled with one tag, and determine the current collision situation, then give feedback to the next frame.

Code Division Multiple Access (CDMA)

CDMA is a multiple access technique where multiple transmitters simultaneously send data across a single communication channel with each transmitter using a unique spreading code to differentiate its data. This enables users to share a frequency band without time slots [17].

In the CDMA protocol, the tags need to excusive-OR their ID by a pseudo-random sequence before transmission. When an RFID reader transmits a signal over its transmitting antenna, various tags will be activated in the read field and an incident wave is reflected back to the RFID reader. The total backscattered signal is the aggregated signal of all the tags where each tag contains a unique spreading code. The signal is then received by the receiving antenna which will then de-spread the signal. The de-spreading process will allow the reader to separate each transmission to restore the original transmitted data. De-spreading involves complex calculations in the RFID communication system.

CDMA technology is considered as the most efficient multiple access technique used to improve the overall performance of the RFID system. It eliminates the need for frequency and timeslot coordination in dense conditions. There are two categories of the spread spectrum CDMA. They are Direct Sequence CDMA (DS/CDMA) and Frequency Hopping CDMA (FH/CDMA). We will only focus on the DS/CDMA because passive RFID tags cannot implement FH/CDMA as they can only backscatter the received signal. There are a variety of direct spreading sequences such as Walsh code which uses orthogonal sequences and Gold code which uses pseudo-random (PN) sequences. Previous researchers have used orthogonal spreading codes generated from a column of a Hadamard matrix [18]. The spread spectrum decreases the overall interference occurring from other simultaneously transmitted tags using direct spreading codes and also from the additional noise experienced from the communication between the reader and the tag. However, each spreading code should be de-spread at the receiver with the appropriate de-spreading code to retrieve original information.

In the DSSS method, the message of the signal is spread in length because the spreading code contains more bits than the original message signal. The ratio of the length of the spreading code to the length of the original message is called the processing gain (G_p) or spreading gain. Usually spreading codes may be 16, 32, 64 or even 128 bits depending on the desired performance. As the value of G_p increases, the percentage of noise and interference errors decreases.

Frequency Division Multiple Access (FDMA)

Frequency Division Multiple Access is a protocol which allows multiple users to send data through a single communication channel. The total bandwidth of the communication channel is divided into separate non overlapping frequencies with sub-channels where each channel is assigned to a specific user. This is an efficient method to eliminate interference as no overlapping of the data is done. In passive RFID systems, a signal is broadcast in a certain frequency to power up and energize passive RFID tags. In the same operating frequency, the reader and the tag communicate through a backscatter signal. When dealing with multiple frequencies, the reader needs to be designed so that it can capture all the frequencies of the tags. There is a huge cost of design involved in this area. Moreover, a dedicated receiver must be specified for every individual receiving channel [19].

Space Division Multiple Access (SDMA)

Space division multiple access is a technique where each channel capacity is divided into separate physical areas. The system allows multiple users of the same station to use the same resources because of their spatial separation. Directional antennas or multiple readers are used to incorporate the spatial separation of the communication channel. Spatial signature is the isolating of coexisting transmission channels via an angle of arrival of each signal source. In passive RFID systems, array antennas can be used to achieve multiple access in the space division protocol. SDMA can be used with the Adaptive Interference Cancellation protocol [18] or with conventional slotted ALOHA.

III. FADING IN WIRELESS COMMUNICATION

In wireless communication, fading is a stochastic variation of the amplitude of a signal, and it is related to multiple variables. A transmitted signal may or may not have a direct line of sight path to the receiver. If such a path exists, the signal along that path experiences a loss of power due to attenuation and absorption by the intervening medium. Whether or not a line-of-sight path exists, the transmitted signal undergoes scattering, reflection and diffraction between the transmitter and the receiver, and so multiple reflected signals can also be received. This process is called multipath, and the total received signal is the sum of the individual signals, which arrive at different amplitudes and with different phasing. Since phasing for each of the individual signals is dependent on the distance it has traveled, significant changes in constructive and destructive interference, and therefore significant changes in amplitude, can occur between two different locations that are very close together. Since the amplitude and phase of the signal from each of these paths can be treated as random variables, the received power will also be random.[1] This random fluctuation of power is identified as "fading" in wireless systems [20]. Fading can be classified into two types: 1. Large scale fading and 2. Small scale fading [21]. A fading channel is a communication channel that experiences fading.

Large Scale Fading

Large scale fading is caused when there is an obstruction between a transmitter and a receiver. This interference causes a huge loss in signal strength. Large scale fading happens because the electromagnetic wave is shadowed or blocked by the obstacle. This

[1] For this thesis we will not be considering the effects of relative motion between the reader and the tags.

type of fading can be described in terms of mean path loss and a log-normally distributed variation about a mean.

The lognormal distribution is given by

$$f_X(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp\left(-\frac{(\ln x - \mu)^2}{2\sigma^2}\right)$$

where:

μ = mean value of *x* in dBm

σ = standard deviation *of x* in dB

x = signal power in mW

If an RFID system is operating in an environment where the line of sight is very strong relative to reflected signals, we are dealing with virtually no multipath and we then model the received signal using a lognormal distribution. As will be established in Chapter 5, path loss can be estimated as a function of distance, and variance, which is dependent on the particular environment, can be estimated based on empirical measurements made in similar environments.

Small Scale Fading

Small scale fading is caused in a multipath environment by the constructive and destructive interference of the multiple received signals. Depending on the line-of-sight component, multipath fading can be modelled using various distributions [22]. If there is no dominant propagation along the line of sight (LOS) between the transmitter and the receiver, the received signal can be statistically described by a Rayleigh distribution. Line of Sight propagation means the electromagnetic waves travel in a direct path from the source to the receiver.

$$f(x;\sigma) = \frac{x}{\sigma^2} e^{-x^2/(2\sigma^2)}, \quad x \geq 0,$$

Where:

σ = scale parameter of the distribution

If a significant LOS signal exists in addition to the reflected signals, the received signal can be statistically described by a Rician distribution. The Rician distribution has a probability density function (PDF) given by:

$$p(r) = \frac{r}{\sigma^2} e^{-\left(\frac{r^2 + A^2}{2\sigma^2}\right)} I_0\left(\frac{Ar}{\sigma^2}\right) \qquad \text{for } A \geq 0, \quad r \geq 0$$

where:

A = peak amplitude of the dominant signal

I_0 = the modified Bessel Function of the first kind and zero order

$r^2/2$ = instantaneous power

σ = standard deviation of the local power

The Rician distribution is often described in terms of a parameter *K*, known as the Rician factor and is expressed as:

$K = 10\log(A^2/2\sigma^2)$ dB

As $A \rightarrow 0$, $K \rightarrow -\infty$ dB and as the dominant path decreases in amplitude, the Rician distribution degenerates to a Rayleigh distribution. On the other hand, for very large values of K the Rician distribution approximates the lognormal distribution. Various distributions can be used to model and establish the relative amplitudes for each of the tags in an RFID system to simulate the effects of multipath and shadowing for each tag. All three of the environments described above are relevant for various applications involving passive RFID tags in supply chains. Previous analysis of the CDMA/AIC protocol has been based on Rayleigh fading. In our thesis we focus on 1. Lognormal Distribution and 2. Rician Distribution. We will then compare the performance characteristics of both the distributions with Rayleigh fading for a selected number of tags.

IV. PREVIOUS RESEARCH WORK

CDMA is a multiple access technique providing the capability to read multiple tags at the same time. For RFID systems experiencing congestion due to tag collisions, CDMA can be extremely efficient relative to the slotted aloha protocol where only one tag can be read at a time. CDMA based RFID systems collect data from all the tags that are present. Each tag will select a spreading code and spread their original data over a wide range of bandwidth by performing an exclusive-or operation, and it will denote the spread signal that passes through the communication channel. During this process undesirable effects due to collisions and noise get added to the signal, but the signal can often still be demodulated to decode the original transmitted information. One of the keys to successful demodulation in traditional CDMA is having transmitters adjust their power level so that all signals arrive at the receiver with the same power level. In presence of multipath fading and near-far problem, however, the backscatter signal from the RFID tags would not reach the receiver at same power levels. In most mobile communication systems, we have an ability to adjust these levels using power control mechanism at the transmitters, but in the RFID passive tags, we do not have the ability to adjust these power levels.

Previous Passive Tag RFID Research without Adaptive Interference Cancellation

An RFID reader is able to communicate with only one tag at a time but due to the sharing of the same wireless channel, RFID systems experience collisions. In order to solve these collision problems, tree-walking and ALOHA based anti-collision protocols have been proposed and developed [27][28]. A frame-slotted ALOHA based anti-collision protocol called the EPC Gen-2 was standardized and accepted as the main standard by EPC Global. The EPC Gen-2 protocol uses the dynamic frame slotted ALOHA technique to identify nearby tags and uses an adaptive algorithm called Q-algorithm to determine the number of slots required for each query. The EPC Gen 2 protocol operates in the frequency range of 860-960 MHz for passive ultra-high frequency RFID tags [26][32].

In recent times, many researchers have suggested replacing the EPC's dynamic framed slotted ALOHA protocol with the CDMA protocol to enable the reader to read more tags and to accelerate tag identification procedures. For active tags, using Direct Spreading-CDMA techniques have been suggested [29]. Other researchers have also studied warehouse environments in worst case scenarios and have suggested to employ CDMA technique for tag identification purposes [30]. Some CDMA based anti-collision algorithms cannot avoid the near-far problem due to shadowing. The near-far problem faces difficulties in reading the accurate information as it causes tag data to be transmitted at distinct energy levels causing imbalances in the SNR values of certain tags.

In the slotted ALOHA system, the main disadvantage is that a reader cannot read multiple tags at the same time. However, slotted ALOHA performs better than the CDMA in the total number of transmitted bits per tag. Bit-wise CDMA or B-CDMA protocol solves some of the shortcomings of the slotted ALOHA system, the straight CDMA system as well as the combination TDMA-CDMA system. The solution of the B-CDMA is that it generates the number of slots on-the-fly while reading the maximum number of tags during each time from the beginning of the reflection of the first EPC bit to the final EPC bit and also by removing the colliding tags with the transmission of each encoded data bit [31][1]. This process allows the reader to read the maximum number of tags at each slot with the highest power, thereby reducing the issues resulting from the near-far problem (shadowing). Adaptive interference cancellation (or AIC) is a solution that records the tag reflections, reads the highest power tag reflection, subtracts it from the conglomerate signal then continues to read the lower powered tags. We can see that a CDMA based RFID system with DSSS has shown better energy consumption in the interrogator compared to the frame-slotted ALOHA based current EPC RFID system. Various other research has shown that performance of passive UHF RFID systems is highly affected by the multipath fading channels that distort and reduce the power of the continuous waves transmitted by the reader [33][34].

A secure system for RFID tags identification with zero-collision based on CDMA and Hash-chain mechanics has also been proposed. This system assists in several tags sending their data simultaneously without collision and also provides mutual authentication, tag anonymity, robustness and forward secrecy. Hash-chain mechanism is a cryptography approach for safeguarding against password spying. Now, it can be found in other applications such as micropayment systems and RFID authentication due to elegant and versatile low-cost implementations associated to this technique. The CDMA and the hash-chain technologies are integrated to provide a zero-collision and secure channel between tags and a reader (for example, during the identifying process, both the reader and tags can mutually authenticate each other, and attackers cannot infer any tag identity from the exchanged messages) [35].

The CDMA-AIC Process

A. Keni [18] proposed a very promising technique, the CDMA-AIC process, for addressing the issue of noise and improving the energy efficiency of the system. The key parameter is the total amount of energy that the reader requires to get the data from the tag. The accuracy is determined by the percentage of missing tags which is also called the missed tag error rate.

Initially, values are selected for the number of tags, number of slots, number of bits, CDMA processing gain and power of noise. Then a series of unique spreading code sequences are generated and one spreading code is assigned for each tag. Each tag's data is then exclusive-OR'ed with that tag's spreading code. The relative amplitudes variations of the transmitted signals from each tag (tau) are modelled using the Rayleigh distribution. This stimulates the effects of shadowing and multipaths for each of the tags. Then an aggregated signal which is the combination of the transmitted signals from all tags is constructed. This aggregated signal comprises of both positive and negative interferences. Effects of noise and attenuation are then added to the aggregated signal which gives a received signal. This received signal is then demodulated. During the de-spreading process, the first strong tag's signal is selected and the spreading code which was used for it is determined. Using cycle redundancy check method, we analyze if the data contains any errors. Now we estimate the original data from the de-spread strong tag signal, record the data and recreate the spreading code for the strong tag. After that the amplitude of the strong tag's received signal is determined by considering the maximum and minimum points from the interpreted signal and that value represents the interference caused by the strong tag and it is removed from the aggregated signal. Then the received signal corresponding to the next-strongest tag is reconstructed. After reconstruction, the effects of the signal from that strong tag are cancelled out. The result is the new received signal. Data for one strong tag has now been read and the tag's interference effects have been eliminated from the new received signal. This process is repeated until all the tags are read and the data has been extracted. The AIC algorithm attempts to identify the strongest tag, de-spread it with the corresponding spreading code, calculates its amplitude, and subtracts 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.

The CDMA-AIC protocol was evaluated for Rayleigh fading environments. This research investigates CDMA-AIC in Lognormal and Rician Fading environments as these environments are representative of many passive RFID tag applications and CDMA-AIC may not operate as well in these conditions because the received signal strength from the tags is not widely distributed enough and therefore will make the adaptive interference cancellation more difficult. We will learn more about the performance in these environments in later chapters.

V. USING CDMA/AIC PROTOCOL IN LOGNORMAL DISTRIBUTION AND RICIAN FADING ENVIRONMENTS

As discussed earlier, the two types of fading we have considered in our thesis are the Lognormal distribution and the Rician fading environments. We have used MATLAB to model both the simulation environments. Both the Rician fading, and the Lognormal distribution environment are significantly different than the Rayleigh fading environment and so the system performance may also be distinct. We can also say that if the performance in the Lognormal and the Rician fading environments is satisfactory, then it significantly broadens the set of RFID applications for which the CDMA-AIC can offer more power-efficient systems. The modelling of both the environments have been discussed clearly in the later sections of this chapter.

Lognormal Distribution

If the RFID system is operating in an environment where the line of sight is very strong relative to reflected signals, we are dealing with virtually no multipath. We then model the received signal using a lognormal distribution. The lognormal distribution describes the random shadowing effects which occur over a large number of measurement locations which have the same transmitter and receiver separation but have different levels of clutter on the propagation path. Typically, in factory and warehouse environments with lognormally distributed signal strength, the standard deviation, σ_s equals 8 to 10 dB [24[25].

As established in Chapter 3, the lognormal distribution is given by

$$f_X(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp\left(-\frac{(\ln x - \mu)^2}{2\sigma^2}\right)$$

where:

μ = mean value of x in dBm

σ = standard deviation *of* x in dB

x = signal power in mW

Fig 5.1 shows the lognormal probability density function plot with a mean of 1 and a sigma of 8.7 dB. As will be discussed in detail in Chapter 6, two features that will affect how well the CDMA-AIC system performs in a lognormal environment are the spread of the signal (its variance) and the percentage of the pdf that represents received signals of low power levels.

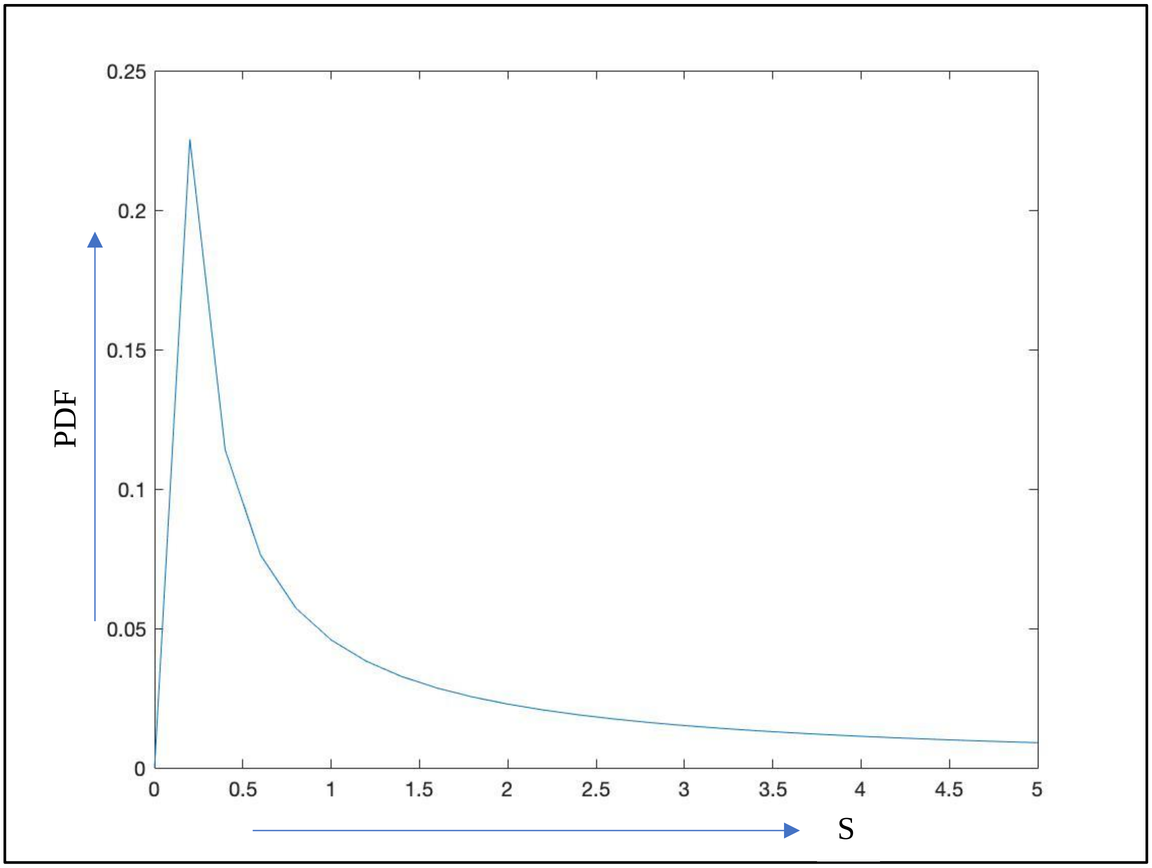

Fig 5.1 Lognormal distribution PDF with σ = 8.7 and Mean=1

To model lognormally distributed signal strength in our simulation, we first pick a random number from 0 to 1. We then determine the Q function of that particular value; the Q function is one minus the cumulative distribution function of the standardized normal random variable being evaluated. We then assign the values of sigma and mu and the other parameters such as number of tags, the number of simulations and the processing gain. We then calculate the amplitude of each tag's signal (represented by the array tau in the simulation). The value of tau determines where that amplitude is in the distribution of all amplitudes for the Lognormal distribution. We then use CDMA with Adaptive Interference Calculation to find out the strongest tag and the next strongest tag and so on. We then finally determine the number of tags successfully demodulated using the lognormal distribution. Appendix A shows the modified code for the CDMA-AIC simulation in a lognormal RF environment.

Rician Distribution

When there is a dominant stationary (nonfading) signal component present, such as a LOS propagation path, the small-scale fading envelope distribution is Rician. As established in Chapter 3, the Rician distribution has a probability density function (PDF) given by:

$$p(r) = \frac{r}{\sigma^2} e^{-\left(\frac{r^2 + A^2}{2\sigma^2}\right)} I_0\left(\frac{Ar}{\sigma^2}\right) \qquad \text{for } A \geq 0, \quad r \geq 0$$

where:

A = peak amplitude of the dominant signal

I_0 = is the modified Bessel Function of the first kind and zero order

$r^2/2$ = instantaneous power

σ = standard deviation of the local power

The Rician distribution is often described in terms of a parameter *K*, known as the Rician factor and is expressed as:

K = 10log($A^2/2\sigma^2$) dB

As $A \rightarrow 0$, $K \rightarrow -\infty$ dB and as the dominant path decreases in amplitude, the Rician distribution degenerates to a Rayleigh distribution. On the other hand, for very large values of K the Rician distribution approximates the lognormal distribution.

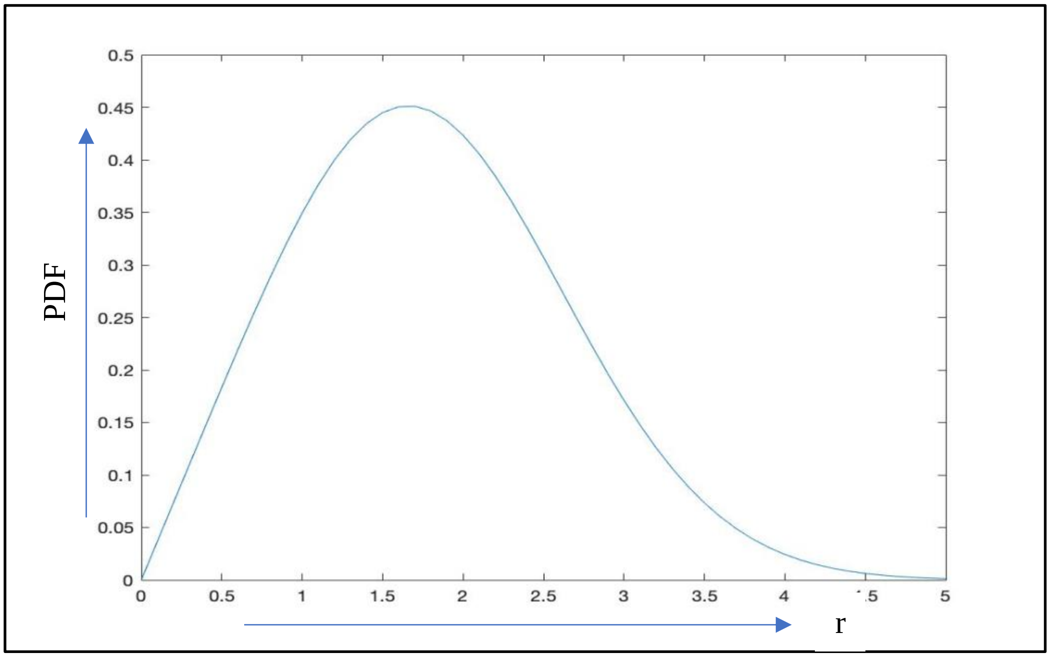

Fig 5.2 Rician fading PDF for K=1

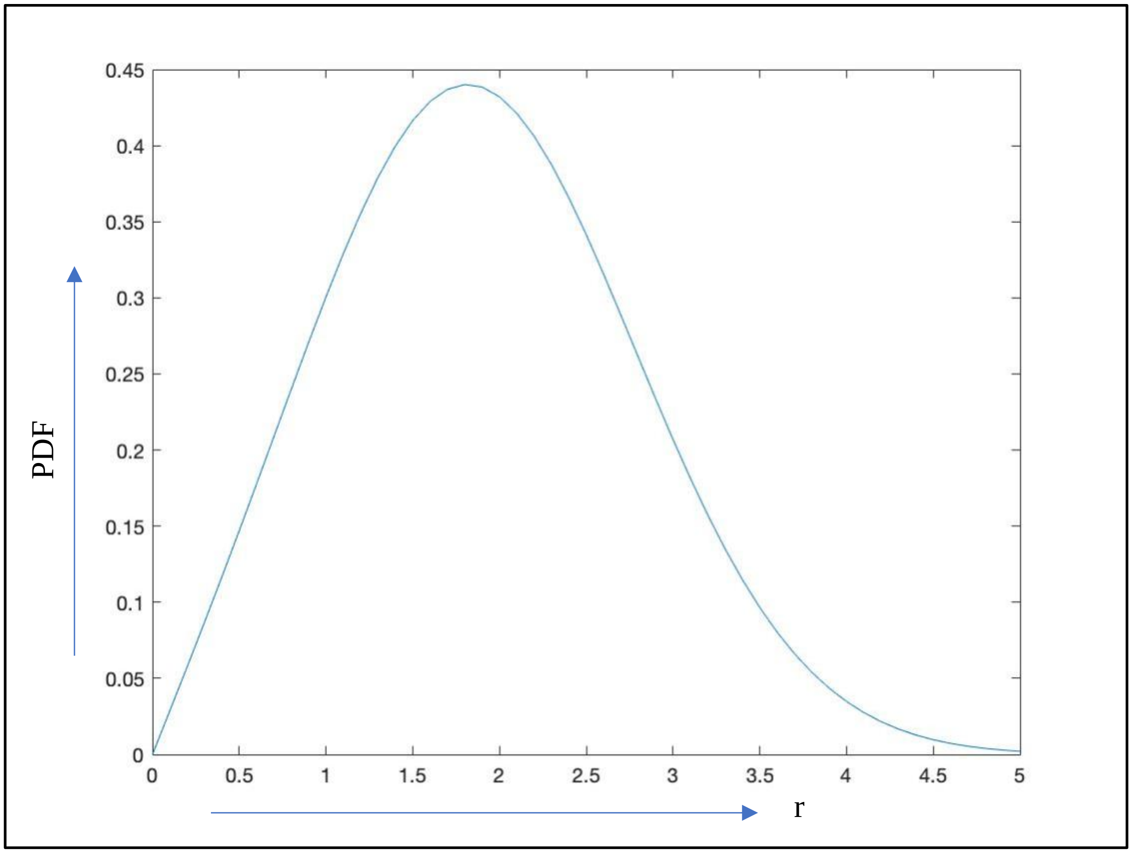

Fig 5.3 Rician fading PDF for K=1.25

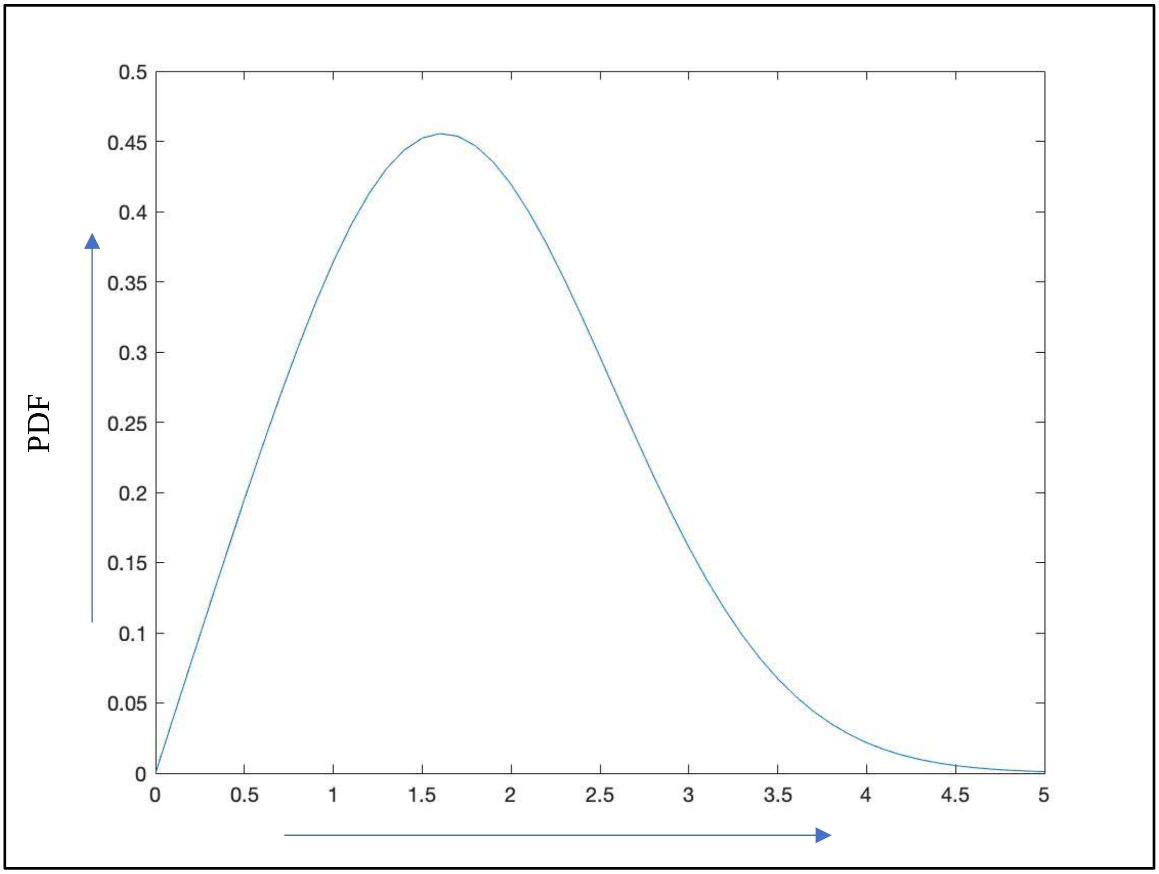

Fig 5.4 Rician fading PDF for K=0.93

A k-factor of 0.93 is consistent with RFID warehouse applications in our research [29] and a sigma value of 8.7 is consistent with the lognormal distribution for warehouse applications as shown in Fig 5.1. The two features that affect how well the CDMA-AIC system performs in a Rician environment are the spread of the signal (its variance) and the percentage of the pdf that represents received signals of low power levels.

In order to model the CDMA/AIC protocol in a Rician fading environment, we first generate the probability density function (PDF) of the Rician distribution using the equation given above, I_0 as modified Bessel function of the first order, a selected value for the line-of-sight amplitude (A) and K. We determine the CDF by taking the PDF curves and finding the area under the curves. We do that by using trapezoidal integration of the PDF function. In mathematics, and more specifically in numerical analysis, the trapezoidal rule is a technique for approximating the definite integral. The trapezoidal rule works by approximating the region under the graph of the function as a trapezoid and calculating its area.

Then we calculate the value of the amplitude of the signal for each tag by first generating a random value from 0 to 1 on our y-axis and calculating the CDF of our Rician distribution. We then draw a horizontal line and interpolate the point which intersects the CDF curve. We can vary the Rice factor K i.e., the relative amplitude of the reflected signals to the direct line of sight signal and create a new set of tau values which are the amplitudes for each of the signals. We finally generate tau values for a Rician distribution with a variety of Rice factors and calculate the number of successful tag demodulations in a Rician fading environment.

Appendix B shows the modified code for the CDMA-AIC simulation in a Rician RF environment.

Rayleigh Distribution

The Rayleigh distribution PDF is given as

$$f(x;\sigma) = \frac{x}{\sigma^2} e^{-x^2/(2\sigma^2)}, \quad x \geq 0,$$

Where σ = scale parameter of the distribution

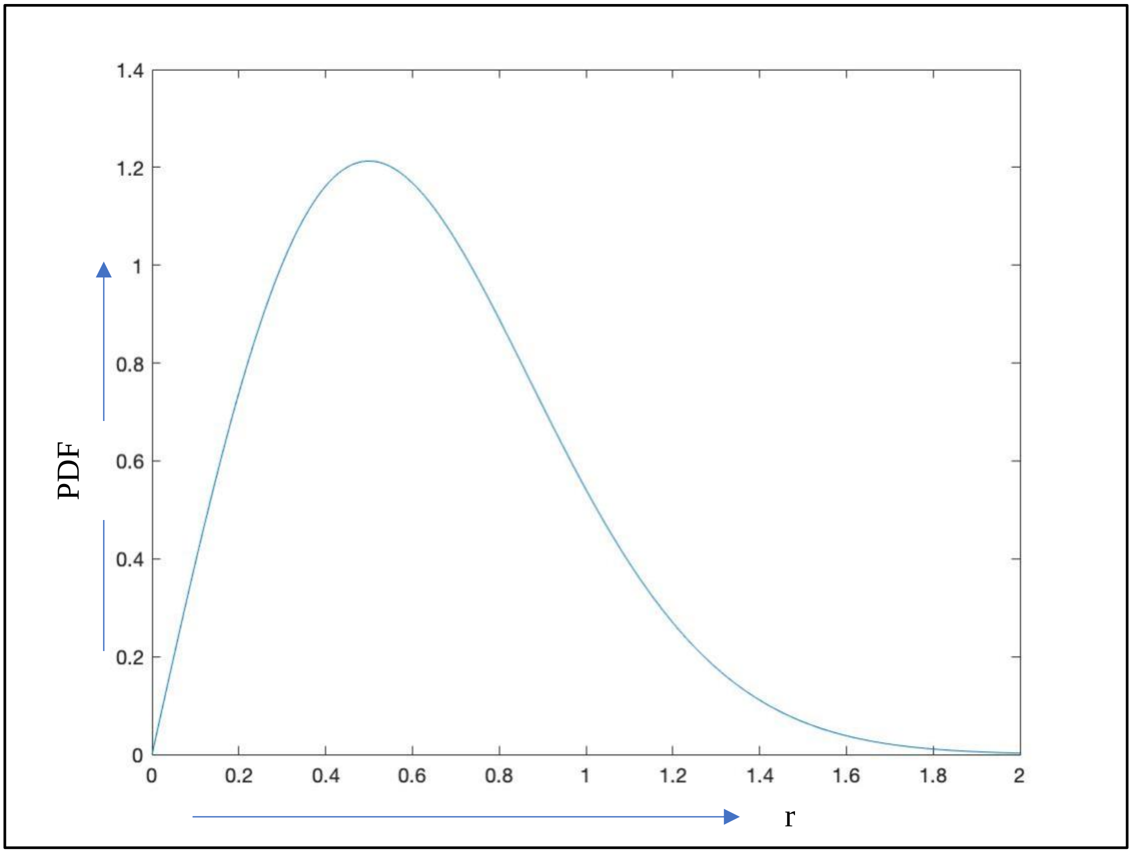

Fig 5.5 Rayleigh distribution PDF with σ = 0.5

The Rayleigh distribution was used by the previous researcher [20] for the CDMA-AIC protocol. The performance comparisons of the Lognormal vs Rayleigh, Lognormal vs Rician and Rician vs Rayleigh environments using a CDMA/AIC protocol are given in the next chapter.

VI. RESULTS AND ANALYSIS

Testing the CDMA/AIC protocol in practical environments:

In this chapter, we will provide simulation results for the CDMA/AIC protocol in various RF propagation environments and then we will provide an in-depth analysis of the results obtained.

There are two different issues that are going to be involved in the successful reception of RFID messages regardless of the different types of fading. They are 1) susceptibility to noise and 2) susceptibility to collisions. What we have found is that there's a balance. Considering Rayleigh fading, where we have the most likely case of getting a lot of weak signals that are more susceptible to noise that others, but with Rayleigh fading we also get the widest distribution of different signal strengths which makes the CDMA-AIC protocol work better and so we are less vulnerable to collisions. When we take a look at Rayleigh fading vs Rician Fading, we can notice that as the average signal-to-noise ratio increases, we can see that Rayleigh works better and when the average signal-to-noise ratio decreases, we can see that Rician works better because the issues with noise become more important than the issues with collisions. With Lognormal distribution, we can see that when we have a larger variation (sigma), the performance goes down because larger variation produces a larger percentage of weak signals which are more susceptible to noise.

We first considered a Rician fading environment to test the CDMA/AIC protocol. We ran 10,000 simulations each for systems with 8 to 12 tags. We considered a large storage hall at 868 MHz with an estimated averaged k-factor of 0.93. Although there are various k-factors for different frequency bands and different environments, we take into consideration 868 MHz since that frequency band is consistent with EPC class 1 generation 2 RFID applications [1], and a k-factor of 0.93 is consistent with RFID warehouse applications in our research [25]. Average signal-to-noise ratio, prior to processing gain, is 3 dB. We have mentioned average signal to noise ratio prior to processing gain because we tested the CDMA/AIC in a true environment with the exact SNR values. It is possible to achieve desired processing gain while dealing with Multiple Access systems like CDMA by altering the amount of spreading used in the codes. For all of our simulations, we used a constant processing gain of 64.

Table 6.1 Rician fading with K= 0.93 (A= 1.3638)

No of Tags	Percentage of messages successfully demodulated
8	92.31
9	90.36
10	88.97
11	87.40
12	86.03

We have also considered a Lognormal distribution environment for the CDMA/AIC protocol. We again ran 10,000 simulations for 8 to 12 tags with a 3 dB signal-to-noise ratio prior to processing gain. We considered a retail store/commercial environment (which is more likely to produce lognormal fading than Rician fading) at 914 MHz with an estimated sigma value of 8.7 dB [25].

Table 6.2 Lognormal distribution with sigma= 8.7 dB

No of Tags	Percentage of messages successfully demodulated
8	81.28
9	79.70
10	78.17
11	77.59
12	76.20

Table 6.3 provides results from 10,000 simulations in a Rayleigh fading environment for 8 to 12 tags with a 3 dB average signal-to-noise ratio prior to processing gain.

Table 6.3 Rayleigh fading

No of Tags	Percentage of messages successfully demodulated
8	90.27
9	88.65
10	87.35
11	85.87
12	84.06

We can observe that for 10,000 simulations, the percentage of successful simulations for tags 8 to 12 in Rician Fading is more than Lognormal distribution. Comparing Rayleigh fading and Rician fading we can observe that Rician fading has a greater number of successful demodulations for all tags. This is because of the effects of low SNR in the Rayleigh fading environment. We can observe the performances of all the three systems with a 3 dB average SNR in figure 6.1

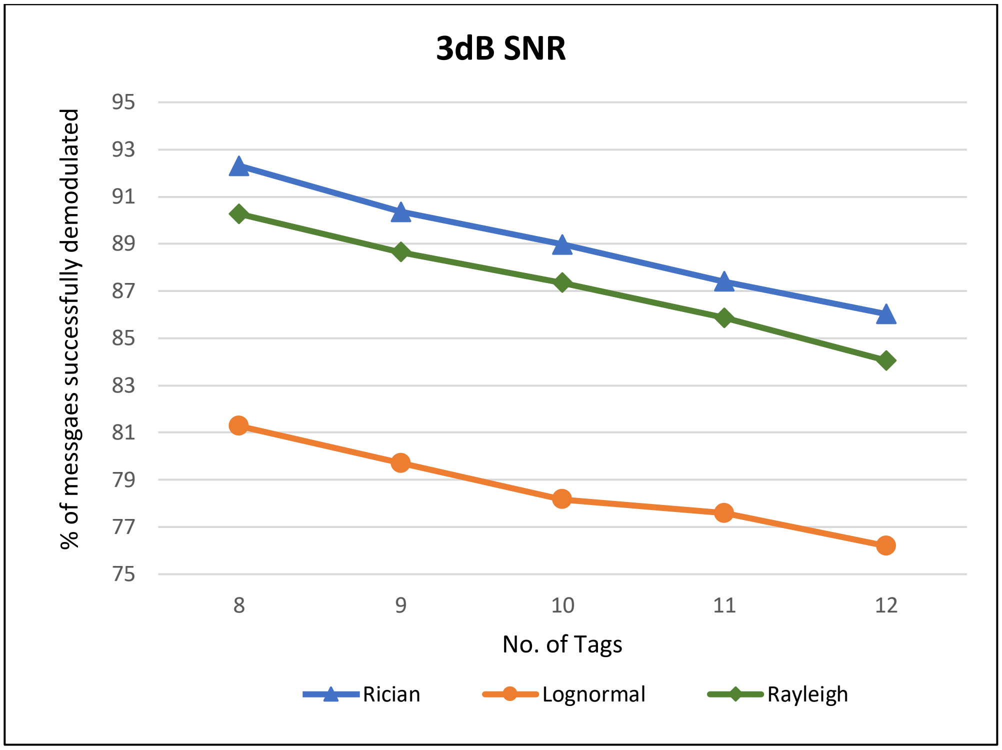

Fig 6.1 Performance comparison of CDMA/AIC with SNR = 3 dB

A wide distribution allows us to compensate for the effects of collisions fairly easily as it helps us in determining the signals of each of the individual tags and removing them using the Adaptive Interference Cancellation. But a wide division of signal strength will hurt the performance as the weaker the signal gets, the more likely it will be damaged by noise and AIC cannot help us that much with noise. What we have observed in this particular case is that the Rician performs best with low average SNR.

Increased average SNR:

Tables 6.1 – 6.3 above represent simulations run with an average SNR of 3dB before processing gain. Tables 6.4 – 6.6 below, average SNR before processing gain is increased to 6 dB. We ran 10,000 simulations each for RF environment with 8 to 12 tags. With the increased SNR we expect that the system will perform better in all three environments. We can observe the performances of all the three systems with a 6 dB average SNR in figure 6.2.

Table 6.4 Rician fading with K= 0.93

No of Tags	Percentage of messages successfully demodulated
8	93.16
9	90.75
10	88.59
11	87.28
12	86.13

Table 6.5 Lognormal distribution with sigma = 8.7 dB

No of Tags	Percentage of messages successfully demodulated
8	86.84
9	85.50
10	84.35
11	83.02
12	81.82

Table 6.6 Rayleigh fading

No of Tags	Percentage of messages successfully demodulated
8	92.90
9	91.49
10	89.89
11	88.37
12	87.51

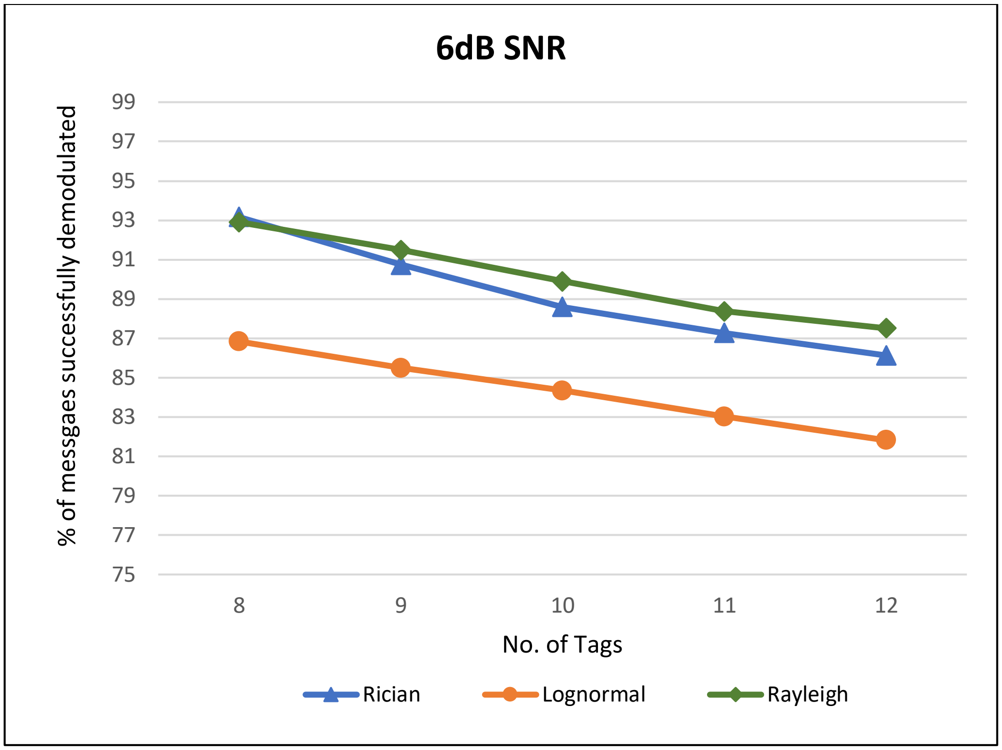

Fig 6.2 Performance comparison of CDMA/AIC with SNR = 6 dB

The tested hypothesis was to increase the average SNR to reduce the effects of noise while not changing the effects of collision. We see that, as expected, all three systems performed better, and we see that the relative improvement in the Rayleigh fading environment is greater than the relative improvement in the Rician fading environment. The relative improvement in the Rayleigh fading environment supports our hypothesis that the greater variation in signal strength, caused by the Rayleigh fading environment, produces an improvement in the CDMA/AIC protocol's handling of collisions.

To further test our hypothesis, we increased SNR again, producing an average Signal-to-noise ratio before processing gain of 9dB. Again, we ran 10,000 simulations each for systems with 8 to 12 tags. We can observe the performances of all the three systems with a 9 dB average SNR in figure 6.3.

Table 6.7 Rician fading with K= 0.93 (A= 1.3638)

No of Tags	Percentage of messages successfully demodulated
8	93.87
9	91.24
10	89.06
11	87.21
12	85.32

Table 6.8 Lognormal distribution with sigma = 8.7 dB

No of Tags	Percentage of messages successfully demodulated
8	91.17
9	90.11
10	89.03
11	87.78
12	86.74

Table 6.9 Rayleigh fading

No of Tags	Percentage of messages successfully demodulated
8	94.00
9	92.31
10	90.87
11	89.40
12	87.84

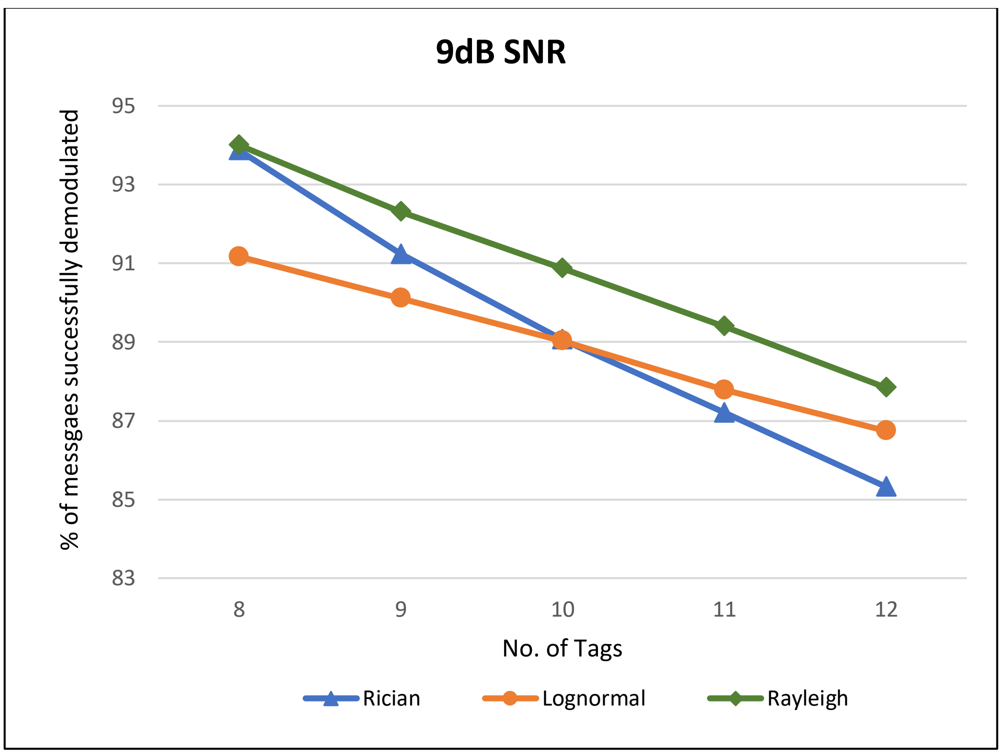

Fig 6.3 Performance comparison of CDMA/AIC with SNR = 9 dB

In Tables 6.7 – 6.9 we see that the system performs better in a Rayleigh fading environment than in a Rician fading environment as we increased SNR to 9dB, we can state that if we increase signal strength, Rayleigh fading works better as collisions are more dominant than the effects of noise. We can also see that for the cases of 10, 11, and 12 tags, the system performs better in a lognormal fading environment than in a Rician environment. Again, this is because the lognormal environment produces a wider variation in signal strength, which increases the effectivity of the CMDA/AIC protocol in reducing the effects of collisions. The larger the number of tags in the system, the greater the probability of collision. We have considered SNR values of 3 dB, 6 dB and 9 dB as they are used in standard communication environments.

Now let's look at how variations in the k-Factor affect the performance of the protocol in Rician fading. Table 6.10 shows the results of Rician Fading Simulations with an average SNR of 6 dB before processing gain and with varying k-Factors (10 tags). 10,000 simulations were run for each k-Factor in the table below.

Table 6.10 Rician fading with varying K-factors

K-FACTORS	PERCENTAGE OF SUCCESFUL DEMODULATIONS
K=0.5 (A=1)	89.08
K=0.75 (A=1.2247)	88.52
K=0.93(A=1.3638)	88.59
K=1.25 (A= 1.5811)	87.84

The lower the value of k, the weaker the line-of-sight signal is relative to the reflections and the more we have a signal that looks more like a Rayleigh environment. Higher k values produce less spread and less variation which leads to effects of collisions becoming greater. To further test the k-factor performances, we have taken 10000 simulations for 8 to 12 tags for three different K-factors.

Table 6.11 Rician simulations for K=0.5 (A=1) and SNR = 3 dB

No of Tags	Percentage of messages successfully demodulated
8	92.08
9	89.86
10	87.46
11	86.40
12	85.10

Table 6.12 Rician fading simulations for K=0.75 (A=1.2247) and SNR = 3 dB

No of Tags	Percentage of messages successfully demodulated
8	92.09
9	90.56
10	88.98
11	87.51
12	85.97

Table 6.13 Rician fading simulations for K=1.25 (A= 1.5811) and SNR= 3 dB

No of Tags	Percentage of messages successfully demodulated
8	92.26
9	90.28
10	89.09
11	87.79
12	86.59

In Tables 6.11 - 6.13 we see that as the K-factor increases, it causes less spread and less variation which leads to an increase in the number of collisions that AIC cannot resolve. We can also see that as the number of tags increase, there is again an increase in the number of collisions which result in decreasing the performance of the systems.

Finally, let's look at how variations in sigma affect the performance of the protocol in Lognormal fading. We have considered lognormal distribution simulations for 10 tags, noise power of 12.58 (SNR = 3dB) and varying sigma values.

Table 6.14 Lognormal distributions with varying sigma values

Sigma Value	Percentage of messages successfully demodulated
6.7	77.94
7.7	78.05
8.7	78.61
9.7	79.88
10.7	80.69
11.7	82.48

From table 6.14, we can see that when we have a larger variation (sigma), the performance of the system is increased. This is because a larger variation makes the AIC more effective, reducing the number of collisions that cannot be resolved.

VII. CONCLUSION

This research aimed to extend the code division multiple access / adaptive interference protocol through analysis and simulation. We have created MATLAB simulations for Rician Fading and Lognormal distributions for the relative amplitudes of each tag's transmission to stimulate the effects of multipath and shadowing. To test the CDMA/AIC protocol in practical environments, we have taken values of sigma for lognormal distribution and k-factor for Rician fading in a factory/warehouse location. For each of the values of sigma and k-factors we have analyzed for simultaneously transmitting tags. The various cases that we have analyzed were comparing Rayleigh fading, Rician fading and Lognormal distributions and taking 10000 simulation runs for each number of tags. We have then increased the noise power and analyzed all three systems. We have also considered how variations in K-factor affect the performance of the CDMA/AIC protocol with Rician fading and how variations in sigma affect the performance of the CDMA/AIC protocol with Lognormal distribution environment.

We can see in the previous chapter that when there is a strong signal, Rayleigh fading works better and when the signal becomes weaker and weaker, Rician fading outperforms Rayleigh fading. With Lognormal distribution we can observe that greater the value of sigma, greater the variation and when the variations become larger, the performance improves. When there is less noise involved in the system, Rayleigh fading works best in dealing with collisions and when there is significant noise involved, Rician fading tends to give better results.

VIII. SUGGESTIONS FOR FUTURE RESEARCH

We have developed both Rician Fading and Lognormal distributions for Code Division Multiple Access - Adaptive Interference Cancellation Protocol. We have also evaluated in-depth how Rayleigh fading, Rician Fading and Lognormal distribution environments affect performance of the CDMA/AIC protocol in a warehouse environment. For future research, firstly, we suggest determining how changes in the processing gain affect CDMA/AIC protocol in all three fading environments. This will help in understanding how the system could work better, leading to a greater number of messages getting successfully demodulated. Secondly, we have only tested the CDMA/AIC protocol and its environments through programming. We suggest laboratory and field testing using a Software Defined Radio interfaced to high-speed Radio Frequency circuitry for transmission and reception. External hardware such as LimeSDR can be used for transmission and reception of signals. Thirdly, we suggest investigating technology to have the RFID tags generate the spreading code and do the spreading rather than requiring the tags to store all of the spread codes. This would provide more flexibility to identify and investigate the best possible scenarios for CDMA/AIC protocols. Fourthly, we suggest research using a dynamic CDMA/AIC (i.e., changing processing gains or retransmissions) versus Dynamic Slotted Aloha and then evaluating Rayleigh, Rician and Lognormal distribution fading in both cases. Lastly, we have seen that the performance of the system i.e., the number of messages successfully demodulated, is dependent on collisions and noise. Experimenting in various RF environments and modifying the simulation to determine what percentage of the messages that couldn’t be demodulated are caused by collisions and what percentage are caused by noise could lead us to new insights.

APPENDIX SECTION

The two simulations that we have developed for the CDMA-AIC protocol are Lognormal distribution and Rician Fading environment. The simulation codes for the Lognormal and Rician fading environments are given below and are marked in pink color. The main simulation program for the CDMA-AIC protocol with Rayleigh fading can be found in the reference [18].

APPENDIX A
SIMULATION PROGRAM FOR CDMA/AIC PROTOCOL USING LOGNORMAL DISTRIBUTION

```
%This is the main simulation program for the CDMA-based RFID
%system with Adaptive Noise Cancellation using a Lognormal distribution.
tic
clear
no_oftags=8;
no_ofbits=256;
tau_fail=0; %Diagnostic variable
spread_overpowered=0; %Diagnostic variable
successful_demodulation=0;
sim_runs=10;
noise_power =12.53; % Scalar value of noise power (sigma squared) in (millivolts)^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 = randi(0:1,no_oftags,no_ofbits); %Generate array containing original
                                   %binary data for all tags
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*no_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 Lognormal 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
   x=rand(1);
   y=qfuncinv(x);
   mu=0;
   sigma=3;
   A=(sigma*y)+(mu);
   B=10^(0.1*A);
   tau(1,n)= B;
  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 it's "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_signal; % Before AIC is applied,
New_aggregatedSignal
%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) = (New_aggregatedSignal(1:point) +
abs(New_aggregatedSignal(1:point))) / 2;
  voltsadd_val(voltsadd_val>0) = 1; %voltsadd_val is now the demodulated, spread
                                     %signal at the receiver (1s and 0s)
  %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 = voltsadd_val(1:processing_gain); %add_signal is the first chip of received
signal
  despreading_forall=zeros(processing_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_aic),:);
  %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, despread
  %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_winner_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 % if extracted data has an error, go to end of loop and start over
    %with another potentially strongest tag.
  end
  successful_demodulation=successful_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),guess_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_winner(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 determing 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.  Later we may want to refine
%this code.
onescount=0;
temphigh=0;
templow=0;
highpointer=-100;
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+quickcheck(point);
    %over_power will be nonzero if the extracted data from the strongest tag
    %was in error.  The higher this variable, the more errors.  This will be
    %useful in diagnostics
      if strong_tag(point)==1
      onescount=onescount+1;
        if New_aggregatedSignal(point)>=temphigh
        temphigh=New_aggregatedSignal(point);
        highpointer=point;%pointer is for diagnostic purposes
        end
        if New_aggregatedSignal(point)<=templow
        templow=New_aggregatedSignal(point);
        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_i1 = (addmaxmin/2);
%amplitude_il is the estimate of the strongest tag's 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
    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 %This is the end of the "for n_aic" loop
  %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_overpowered+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; % Storing the values in New_aggregatedSignal
    %New_aggregatedSignal now represents the received signal after the effects of the
    %strongest tag have been subtracted.  We're now ready to repeat the
    %demodulation loop to extract data for another tag.
  end %This is the end of the demodulation loop
end
successful_demodulation
percent_messages_successfully_demodulated =
successful_demodulation/(no_oftags*sim_runs)
toc
```

APPENDIX B
SIMULATION PROGRAM FOR CDMA/AIC PROTOCOL USING RICIAN FADING DISTRIBUTION

```
%This is the main simulation program for the proposed CDMA-based RFID
%system with Adaptive Noise Cancellation using a Rician Distribution.
tic
clear
no_oftags=12;
no_ofbits=256;
tau_fail=0; %Diagnostic variable
spread_overpowered=0; %Diagnostic variable
successful_demodulation=0;
sim_runs=10000;
noise_power=12.58; % Scalar value of noise power (sigma squared) in (millivolts)^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 = randi(0:1,no_oftags,no_ofbits); %Generate array containing original
                                          %binary data for all tags
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*no_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 Rician 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 m = 1:no_oftags
       A=1.3638;
       k=(A^2)/2;
       x=(0:0.0999:9.999);
       y(1)=0;
       I=besseli(0,A*x);
        for n=(1:101)
            z(n)=x(n)*exp(-((x(n)^2)+(A^2))/2)*I(n);
        end
      %plot(x,z);
       y(1)=0;
        for n=(2:101)
            y(n)=y(n-1)+(.1*(z(n-1)+z(n))/2);
        end
     plot(x,y);
     hold on % used this command to hold the cdf plot
     k=rand(1); % created a random number from 0 to 1
     yline(k);% drew a horizontal line from the random number
     [y,index] = unique(y);
     c = interp1(y,x(index),k); % point where the horizontal line intersects the Rician CDF
curve
     hold off
     %Q=besseli(0,A*c);
     %t=c*exp(-((c^2)+(A^2))/2)*Q;% substituted the value of x i.e (c) in Z(n) and named
it t
     tau(1,m)=c;
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 it's "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_signal; % Before AIC is applied,
New_aggregatedSignal
%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) = (New_aggregatedSignal(1:point) +
abs(New_aggregatedSignal(1:point))) / 2;
  voltsadd_val(voltsadd_val>0) = 1; %voltsadd_val is now the demodulated, spread
                      %signal at the receiver (1s and 0s)
  %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 = voltsadd_val(1:processing_gain); %add_signal is the first chip of received
signal
  despreading_forall=zeros(processing_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_aic),:);
  %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, despread
  %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_winner_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 % if extracted data has an error, go to end of loop and start over
    %with another potentially strongest tag.
  end
  successful_demodulation=successful_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),guess_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_winner(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 determing 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.  Later we may want to refine
%this code.
onescount=0;
temphigh=0;
templow=0;
highpointer=-100;
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+quickcheck(point);
    %over_power will be nonzero if the extracted data from the strongest tag
    %was in error.  The higher this variable, the more errors.  This will be
    %useful in diagnostics
      if strong_tag(point)==1
      onescount=onescount+1;
        if New_aggregatedSignal(point)>=temphigh
        temphigh=New_aggregatedSignal(point);
        highpointer=point;%pointer is for diagnostic purposes
        end
        if New_aggregatedSignal(point)<=templow
        templow=New_aggregatedSignal(point);
        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_i1 = (addmaxmin/2);
    %amplitude_il is the estimate of the strongest tag's 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
    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 %This is the end of the "for n_aic" loop
  %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_overpowered+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; % Storing the values in New_aggregatedSignal
    %New_aggregatedSignal now represents the received signal after the effects of the
```

```
    %strongest tag have been subtracted.  We're now ready to repeat the
    %demodulation loop to extract data for another tag.
  end %This is the end of the demodulation loop
end
successful_demodulation
percent_messages_successfully_demodulated =
successful_demodulation/(no_oftags*sim_runs)
toc
```

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] RFID: Technology, Applications and Global Markets, BCC Publishing, 2016. [Online]. Available: https://www.bccresearch.com/market-research/instrumentation-and-sensors/rfid-technology-applications-markets-report.html

[4] "Benefits and challenges in supply chain management," [Online]. Available: https://lowrysolutions.com/blog/the-3-biggest-benefits-of-rfid-asset-tracking-in-the-supply-chain/.

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

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

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

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

[9] "Price of Passive RFID tags," [Online]. Available: https://www.advancedmobilegroup.com/blog/the-true-price-of-rfid-tags.

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

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

[12] Roberts, L.G. (1975) ALOHA Packet System with and without Slots and Capture. Computer Communication Review, 5, 28-42. http://dx.doi.org/10.1145/1024916.1024920.

[13] 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.

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

[15] 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.

[16] 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.

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

[18] Archita Keni, [Thesis] “Using CDMA/AIC to increase energy efficiency and reduce multipath effects in passive RFID tag systems”, December 2019

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

[20] S.Popa, & N, Draghiciu & R, Reiz. (2008). Fading Types in Wireless Communications Systems. Journal of Electrical and Electronics Engineering.

[21] Riadi, Abdelhamid & BOULOUIRD, Mohamed & Hassani, M.. (2020). Performances of OSIC Detector of an UpLink OFDM Massive-MIMO system in Rayleigh and Ricain fading channels. Wireless Personal Communications.

[22] Ali, Firas. (2010). Simulation of Multipath Fading Effects in Mobile Radio Systems. Microwave Journal. 53. Online Paper.

[23] S.Popa, & N, Draghiciu & R, Reiz. (2008). Fading Types in Wireless Communications Systems. Journal of Electrical and Electronics Engineering.

[24] Andersen, Jørgen & Rappaport, T.S. & Yoshida, Susumu. (1995). Propagation Measurements and Models for Wireless Communications Channels. Communications Magazine, IEEE.

[25] Theodore Rappaport. 2001.Wireless Communications: Principles and Practice (2nd.ed.). Prentice Hall PTR, USA.

[26] E. Vahedi, R. K. Ward and I. F. Blake, "Performance Analysis of RFID Protocols: CDMA Versus the Standard EPC Gen-2," in *IEEE Transactions on Automation Science and Engineering,* vol. 11, no. 4, pp. 1250-1261, Oct. 2014

[27] H. Wu and Y. Zeng, “Efficient framed slotted ALOHA protocol for RFID tag anticollision,” IEEE Trans. Autom. Sci. Eng., vol. 8, no. 3, pp. 581–588, Jul. 2011.

[28] E. Vahedi, V. Shah-Mansouri, V. Wong, I. F. Blake, and R. K. Ward, “Probabilistic analysis of blocking attack in RFID systems,” IEEE Trans. Inform. Forensics Security, vol. 6, no. 3, pp. 803–817, Sep. 2011.

[29] G. Mazurek, “Active RFID system with spread-spectrum transmission,” IEEE Trans. Autom. Sci. Eng., vol. 6, no. 1, pp. 25–32, Jan. 2009.

[30] J. Y. Maina, M. H. Mickle, M. R. Lovell, and L. A. Schaefer, “Application of CDMA for anti-collision and increased read efficiency of multiple RFID tags,” J. Manuf. Syst., vol. 26, no. 1, pp. 37–43, Jun. 2008.

[31] P. Wang, A. Hu, and W. Pei, “The design of anti-collision mechanism of UHF RFID system based on CDMA,” in Proc. IEEE APCCAS, Singapore, Dec. 2006, pp. 1703–1708.

[32] EPCglobal, EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz version 1.2.0, 2008

[33] A. G. Dimitriou, S. Siachalou, A. Bletsas, and J. N. Sahalos, “A site– specific stochastic propagation model for passive UHF RFID,” *IEEE Antennas and Wireless Propagation Letters*, vol. 13, pp. 623–626, 2014.

[34] T. Ben-Jabeur and A. Kadri, "Enhancing passive UHF RFID communication in multipath fading channels using time-varying continuous wave signals," 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 2015, pp. 574-579, doi: 10.1109/WCNC.2015.7127533.

[35] L. Wuu, Y. Chen, C. Hung and W. Kuo, "Zero-Collision RFID Tags Identification Based on CDMA," 2009 Fifth International Conference on Information Assurance and Security, Xi'an, China, 2009, pp. 513-516, doi: 10.1109/IAS.2009.216.