View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

ISTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

ON PERFORMANCE EVALUATION AND ENHANCEMENT OF RFID SYSTEMS COMPLYING WITH ISO 18000-3, ISO 18000-7 STANDARDS

M.Sc. THESIS

Atakan ARSLAN

Department of Electronics and Communications Engineering

Telecommunications Engineering Programme

JANUARY 2013

ISTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

ON PERFORMANCE EVALUATION AND ENHANCEMENT OF RFID SYSTEMS COMPLYING WITH ISO 18000-3, ISO 18000-7 STANDARDS

M.Sc. THESIS

Atakan ARSLAN
(504081348)

Department of Electronics and Communications Engineering

Telecommunications Engineering Programme

Thesis Supervisor: Associate Prof. Dr. Mesut Kartal

JANUARY 2013

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

ISO 18000-3, ISO 18000-7 STANDARTLARINA UYGUN RFID SİSTEMLERİNİN PERFORMANS ANALİZİ VE İYİLEŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

Atakan ARSLAN
(504081348)

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Telekomünikasyon Mühendisliği Programı

Tez Danışmanı: Associate Prof. Dr. Mesut Kartal

OCAK 2013

Atakan ARSLAN, a M.Sc. student of ITU **Graduate School of Science, Engineering and Technology** student ID **504081348**, successfully defended the thesis entitled **“ON PERFORMANCE EVALUATION AND ENHANCEMENT OF RFID SYSTEMS COMPLYING WITH ISO 18000-3, ISO 18000-7 STANDARDS ”**, which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Associate Prof. Dr. Mesut Kartal** İstanbul Technical University	....
Jury Members :	**Prof. Dr. Sedef Kent** İstanbul Technical University	....
	Assistant Prof. Dr. Hamid Torpi Yıldız Technical University	....

Date of Submission : **17 December 2012**
Date of Defense : **21 January 2013**

Anneme ve Büşrama . . .

FOREWORD

I would like to thank all people who have helped and inspired me during my M.Sc. study. I especially want to thank my supervisor Associate Prof. Dr. Mesut Kartal for his guidance during this thesis work.

I would like to sincerely thank to my thesis jury Prof. Dr. Sedef Kent and Assistant Prof. Dr. Hamid Torpi for examining this thesis and providing me helpful comments.

I also would like to thank my friend (a really good friend), Süleyman Kardaş, for his uncountable helps and contributions to this thesis. My deeply thanks to Muhammed Ali Bingöl who always gave me the encouragement that I need for helps, valuable instructions and his great friendship over the years.

My deepest gratitude goes to my family for their unflagging love and support throughout my life; this thesis is simply impossible without them.

January 2013 Atakan ARSLAN

TABLE OF CONTENTS

Page

FOREWORD ..... **ix**
TABLE OF CONTENTS ..... **xi**
ABBREVIATIONS ..... **xiii**
LIST OF TABLES ..... **xv**
LIST OF FIGURES ..... **xvii**
SUMMARY ..... **xix**
ÖZET ..... **xxiii**
1. INTRODUCTION **1**
  1.1 A General RFID Technology Overview 1
    1.1.1 RFID systems 1
    1.1.2 Some basic terms 2
  1.2 Main Contributions 3
  1.3 Organization of the Thesis 3
2. THE PERFORMANCE ANALYSIS OF PASSIVE RFID SYSTEMS FOR ISO 18000-3 STANDARD **5**
  2.1 Introduction 5
  2.2 Related Works On Simulation Environments 7
  2.3 Channel Analysis 8
    2.3.1 Channel types 9
      2.3.1.1 Additive white gaussian noise (AWGN) channel 9
      2.3.1.2 Rayleigh fading channel 9
    2.3.2 The BER analysis of AWGN and rayleigh Channel 11
    2.3.3 The comparison of AWGN channel and rayleigh fading channel 16
  2.4 ISO/IEC 18000-3 Standard 18
  2.5 The Implemented Protocol In Our Simulation Environment 22
    2.5.1 The registration phase 23
    2.5.2 The authentication phase 24
  2.6 Simulation Setup and Result 25
    2.6.1 The analysis of PETRA 25
    2.6.2 Our simulation environment 26
    2.6.3 Our simulation scenario 27
    2.6.4 The simulation results 29
3. PERFORMANCE IMPROVEMENT OF ACTIVE RFID SYSTEMS USING MULTIPLE-ANTENNAS WITH LIMITED FEEDBACK SCHEMES **33**
  3.1 Related Works 33

3.2 ISO 18000-7 Standard 34
3.3 Communication Setup 37
3.4 Channel Models 38
3.5 Limited Feedback Schemes 39
  3.5.1 Trasmit antenna selection (TAS) 39
  3.5.2 Extended balanced space-time block codes scheme (EBSTBCs) 41
  3.5.3 Improved transmit scheme (ITS) 43
  3.5.4 Beamforming (BF) 44
3.6 The Performance Evaluation For Multiple-Antenna At Tag Side 45
3.7 The Performance Evaluation For Multiple-Antenna At Both Tag and Reader Side 48
4. CONCLUSION 51
REFERENCES 53
CURRICULUM VITAE 57

ABBREVIATIONS

AWGN : Additive White Gaussian Noise
BER : Bit Error Rate
CRC : Cyclic Redundancy Code
DSFID : Data storage format identifier
EEPROM : Electrically Erasable Read Only Memory
EPC : Electronic Product Code
FER : Frame Error Rate
FIPS : Federal Information Processing Standards
HF : High Frequency
ISO : International Organization for Standardization
LF : Low Frequency
LSB : Least Significant Bit
MSB : Most Significant Bit
NFC : Near Field Communication
PETRA : Protocol Evaluation Tool for RFID Applications
RFID : Radio Frequency IDentification
UHF : Ultra High Frequency

LIST OF TABLES

Page

Table 2.1 General Request Format 19
Table 2.2 General Response Format 19
Table 2.3 Inventory Request Format 20
Table 2.4 Inventory Response Format 20
Table 2.5 Custom Request Format 20
Table 3.1 Interrogator-to-tag command format (broadcast) 35
Table 3.2 Interrogator-to-tag command format (point-to-point) 35
Table 3.3 Tag-to-Reader Broadcast Response Message Format 35
Table 3.4 Tag-to-Reader Response Message Format (point-to-point) 36
Table 3.5 Frame Error Rate Performance When Single Antenna Presents At The Tag 37
Table 3.6 Frame Error Rate Performance When Three Antennas Present At The Tag 47
Table 3.7 Frame Error Rate Performance When Four Antennas Present At The Tag 47
Table 3.8 Frame Error Rate Performance When Three Antennas Present At The Tag and Two Receive Antennas Present At The Reader 49

LIST OF FIGURES

Page

Figure 1.1 : A Basic RFID System.. 2
Figure 2.1 : The Representation of AWGN Channel 12
Figure 2.2 : Signal Point for Binary Antipodal Signals 12
Figure 2.3 : The Power Spectral Density (PSD) of the Wideband White Noise ... 12
Figure 2.4 : Conditional PDFs of two Signals 13
Figure 2.5 : Bit Error Rate (BER) of AWGN and Rayleigh Fading Channel 16
Figure 2.6 : Frame Error Rate (FER) of AWGN and Rayleigh Fading Channel . 17
Figure 2.7 : The States of a RFID Tag 21
Figure 2.8 : The Proposed RFID Authentication Protocol.................................. 23
Figure 2.9 : RFID System Structure to PETRA 25
Figure 2.10: The Detailed Structure of PETRA 26
Figure 2.11: The Backbone of Our Simulation Enviroment 27
Figure 2.12: The Class Structure of Our Simulation Enviroment 28
Figure 2.13: Num. of Occurred Trials for Auth. Vs. Num. of Generated Tags 31
Figure 2.14: Num. of Successed Tags Vs. Num. of Generated Tags 31
Figure 2.15: Authentication Time [ms] Vs. Num. of Generated Tags 32
Figure 3.1 : A Basic RFID System with Multiple-Antenna Tag........................... 34
Figure 3.2 : Signal Point for Binary Orthogonal FSK Signals 38
Figure 3.3 : FER for three antennas at the tag and frame length is 20 bytes.......... 45
Figure 3.4 : FER for three antennas at the tag and frame length is 255 bytes........ 46
Figure 3.5 : FER for four antennas at the tag and frame length is 20 bytes........... 48
Figure 3.6 : FER for four Antennas at the tag and frame length is 255 bytes........ 49
Figure 3.7 : FER for three antennas at the tag and two receive antennas at the reader and frame length is 20 bytes. 50
Figure 3.8 : FER for three antennas at the tag and two receive antennas at the reader and frame length is 255 bytes. 50

ON PERFORMANCE EVALUATION AND ENHANCEMENT OF RFID SYSTEMS COMPLYING WITH ISO 18000-3, ISO 18000-7 STANDARDS

SUMMARY

This M.Sc. thesis is mainly two folds: First part includes the performance evaluation of passive and active RFID systems complying with ISO 18000-3 and ISO 18000-7 standards respectively. Second part shows the performance improvement of active RFID systems with multiple antennas in ISO 18000-7 standard. It also includes a detailed comparison of different limited feedback schemes for multiple antennas at tag side and both tag-reader side.

Radio Frequency IDentification (RFID) has become very popular in wireless technologies and pervasively deployed in many applications area, such as contactless credit cards, e-passports, ticketing systems, access control, gaming, healthcare, pharmaceuticals, document and media management. This technology provides wireless communication with an object or someone to automatically identify or track by using radio waves. RFID systems can be grouped into three basic ranges by their using operating frequency: Low frequency (LF, 30-300 KHz), high fequency (HF 3-30MHz) and ultra high frequency (300MHz-3GHz) / microwave (>3 GHz).

RFID tags and readers communicate with each other over air interface. This insecure channel and the limited capabilities of RFID tags cause security and privacy vulnerabilities. An adversary may do tag impersonating, tracking, eavesdropping, and denial of service (DoS) attack. Besides the vulnerabilities, a tag might be distinguishable in its life-span by an attacker. If it is once recognized by an adversary, it will be easily able to be traceable. At that situation, there might be two attacks. (i) An attacker might track the previous interactions of the tag or (ii) he may track the future ones. These two attacks are called backward traceability and forward traceability, respectively. The protocol used for RFID system should provide not only resistance against passive attacks, replay attacks, cloning attacks but also resistance against active attacks. There are public-key cryptography solutions in literature but none of them are convenient for the low-cost tags used in lots of applications because of their limitations. It needs to find much light-weight approaches. Therefore, many light-weight authentication protocols are proposed to have a win against the adversaries that deceive the capacity-restricted tags. But, designing light-weight cryptographic authentication protocols with basic cryptographic primitives (xor, hash function) is a challenging task.

A growing security and privacy concerns are most commonly related with high frequency (HF) RFID devices, using near field communication (NFC), such as contactless smart cards (CSC), because they are used to store secure and private

personal information in many RFID applications: e-passport, govern ID, credit cards etc. Many researches offer different protocol designs to overcome the security and privacy problems for the standards. Although, their security and privacy analysis are quite important, their effectiveness is also another vital point for real world RFID applications/systems. Unfortunately, it is a troublesome to physically test every new protocol desings because of cost, time and it is also impractical.

The performance of the protocols affects the quality of HF RFID applications. Therefore, many simulation environments have been improved to evaluate the performance of these kinds of protocols. However, none of them shows the success bounds of the protocols by considering wireless channel effect. Motivated by this need, in this thesis, firstly, we improve the PETRA simulation environment by adding two channel models, AWGN channel, Rayleigh fading channel and show the performance bounds of an RFID authentication protocol in these channels for ISO/IEC 18000-3 standard. For this purpose, we implement a secure authentication protocol in our new simulation environment to understand the effect of the wireless channel in a real life scenario. This work may guide the protocol designers to test their protocols and observe the performance of passive RFID systems before using them on real systems.

We show that RFID protocols perform best performance in AWGN channel. This performance gives us the upper bound performance because the AWGN channel is an ideal case in wireless communication environment. We added the results of Petra simulation environment to evaluate the wireless channel effect. On the other hand, the performance of RFID protocols in Rayleigh fading channels gives the lower bound of the performance. The effects of the Rayleigh fading channel are extremely severe when it is compared to the AWGN channel. The FER curve is inversely linear proportional with the SNR for Rayleigh fading while it is exponentially decreasing for AWGN channel.

RFID tags can also be categorized in three groups by using energy source such as passive, semi-passive and active (battery assisted) tags. Passive RFID tags do not have own internal energy source. Instead, they use the radio energy transmitted by the reader. Semi-passive and active RFID tags have their own energy source. The difference between them is that semi-passive tags do not talk first and they are powered up by the reader's request. The energy source is used after the request. Active tags might talk to RFID reader first or answer its first request.

Active RFID tags are preferred in many applications for their advantages: Visibility, security, quality and high distance communication. An active tag can transmit its data at great range by using its internal source. However, the battery life is decreased by the active parts of the tag. Hence, it causes a trade-off between communication distance and power consumption. In addition to this, the increased transmission distance might also cause interference problem because a large number of tags or multi-reader multi-tag environment within the range of a reader grounds communication difficulties.

ISO/IEC 18000-7 is an active RFID standard that their tags operatea at 433 MHz. We realize that a tag consumes too much energy source to perform a satisfactory communication compliance with the standard in Rayleigh fading channel. In this thesis, secondly, we aim to ameliorate an active RFID system performance from the perspective of better communication and energy efficiency. Our simulation results

show that multiple-antenna designs at tag side and tag-reader side using limited feedback schemes significantly decreases the frame error rates and increases the battery lifetime.

ISO 18000-3, ISO 18000-7 STANDARTLARINA UYGUN RFID SİSTEMLERİNİN PERFORMANS ANALİZİ VE İYİLEŞTİRİLMESİ

ÖZET

Bu Yüksek Lisans Tezi iki ana kısımdan oluşmaktadır. Birinci kısım, ISO 18000-3 ve ISO 18000-7 standartlarına uygun pasif ve aktif RFID sistemlerinin performans değerlendirmesini içermektedir. İkinci kısım ise, 18000-7 standardına uygun RFID sistemlerinin çoklu antenlerle başarım iyileştirilmesini içermektedir. Bu kısım ayrıca değişik sınırlı geri besleme metotlarının çoklu antenlerle birlikte etiket ve okuyucu tarafındaki detaylı karşılaştırmalarını da kapsamaktadır.

Radyo frekans tanımlama (RFID) teknolojisi, kablosuz haberleşme alanında oldukça popüler olmaya başlamış ve birçok uygulama alanında yaygın bir şekilde dağılmıştır: temassız kredi kartları, e-pasaport, bilet sistemleri, giriş-çıkış kontrolleri, oyunlar, sağlık, ilaç, doküman ve basın yönetimi…Bu teknoloji, radyo dalgaları yardımıyla herhangi bir nesne ya da canlıyı tanımlama veya takip etmeyi kablosuz olarak sağlamaktadır. RFID sistemleri, kullandıkları frekans bantlarına göre üç gruba ayrılırlar: Düşük frekans (LF, 30-300 KHz), Yüksek Frekans (HF 3-30MHz) ve ultra yüksek frekans (UHF,300MHz-3GHz) / Mikrodalga (>3 GHz).

RFID etiketleri ve okuyucuları birbirleriyle havadan haberleşirler. Haberleşme kanalının güvensiz olması ve hafif-siklet etiketlerin sınırlı kapasiteleri güvenlik ve mahremiyet açıklarına neden olur. Bir saldırgan etiketi taklit edebilir, izleyebilir, dinleyebilir veya DoS saldırısında bulunabilir. Bu açıklıklara ek olarak, bir etiket, bir düşman tarafından yaşam döngüsü boyunca farkedilememelidir. Eğer bir saldırgan bir etiketi tanıdıysa, artık onu kolayca takip de edebilir. Bu durumda, iki saldırı söz konusudur: (i) Bir saldırgan etiketin bütün geçmiş konuşmalarını deşifre edebilir veya (ii) gelecek konuşmalarında onu takip edebilir. Bu saldırılar sırasıyla geri dönük takip edilebilme ve ileriye dönük takip edilebilme atağı olarak adlandırılmaktadır. Litaratürde güvenlik ve mahremiyet sorunlarına çözüm olacak açık-anahtar şifreleme çözümleri bulunmaktadır, fakat bu çözümlerin hiçbir tanesi, sınırlı kapasiteleri nedeniyle birçok uygulamada kullanılan hafif-siklet etiketler için uygun bir çözüm değildir. Bu yüzden, saldırganların sınırlı kapasitedeki etiketleri kandırmasını engellemek için çok sayıda hafi-siklet asıllama prokolleri önerilmiştir.

Önemi artan güvenlik ve mahremiyet konuları genellikle yakın alan haberleşmelerinde kullanılan (kablosuz akıllı kartlar) HF RFID sistemleriyle ilgilidir. Çünkü bu sistemler, birçok RFID uygulamalarında (e-pasaport, akıllı nüfus kartı, kredi kartları vb.) güvenlik ve mahremiyet gerektiren kişisel bilgileri saklamaktadır. Birçok araştırmacı, standartlara uygun olacak şekilde güvenlik ve mahremiyet problemlerine farklı protokol tasarımlarıyla çözümler sunmuşlardır. Bu protokollerin güvenlik ve mahremiyet konularındaki analizleri oldukça önemli olmasına rağmen, onların gerçek

hayattaki verimlilikleri ise önem arz eden başka bir konudur. Maalesef, her bir yeni protokol tasarımının fiziksel olarak test edilebilmesi maliyet, zaman ve pratik uygulama açısından oldukça zordur.

Protokollerin performansları, HF RFID uygulamalarının kalitesini etkilemektedir. Bu yüzden, farklı protokolleri değerlendirmek için birçok simülasyon ortamları geliştirilmiştir. Bunlardan hiçbiri kablosuz kanal etkisini göz önüne alacak şekilde protokollerin başarı sınırlarını göstermemiştir. Bu motivasyonla biz, bu tez çalışmasında PETRA simülasyon ortamına AWGN ve Rayleigh sönümlemeli kanal modellerini ekleyerek iyileştirmede bulunduk. Bu kanallarda haberleşen ISO/IEC 18000-3 standardına uygun olan RFID sistemlerindeki protokollerin performans sınırlarını gösterdik. Bu amaca yönelik olarak, güvenli ve mahrem bir kimlik tanıma protokolünü, yeni geliştirdiğimiz simülasyon ortamına uyguladık ve pasif RFID sistemlerin gerçek hayatta kullanılmadan önceki performans değerlendirmesini gözlemledik.

Biz RFID protkollerinin en iyi başarıyı AWGN kanalı altında sergilediğini gösterdik. Bu başarım göstergesi bize aslında protokolün başarım üst sınırını vermektedir çünkü AWGN kanal, kablosuz haberleşme ortamları içerisinde ideal kanal olarak kabul edilmektedir. Ayrıca, kablosuz kanalın etiklerini göstermek için Petra simülasyon ortamının sonuçlarını ekledik. Bunun yanı sıra, Rayleigh sönümlemeli kanalda başarım sonuçlarını elde ettik. Bu sonuçlar ise bize RFID protokollerin başarım alt sınırını vermektedir çünkü Rayleigh sönümlemeli kanalın bozucu etikeleri AWGN kanalına göre daha çoktur ve en kötü kanal yapılarında birisidir. AWGN kanalında çerçeve hata oranı sinyal gürültü oranına göre üstsel olarak azalırken, Rayleigh sönümlemeli kanalda linear olarak azaldığı simülasyonlarla gösterilmiştir.

RFID etiketleri aynı zamanda enerji kaynaklarına göre üç gruba ayrılır: pasif, yarı-pasif ve aktif etiketler. Pasif RFID etiketlerin kendi enerji kaynakları yoktur. Bunun yerine bu etiketler, okuyucudan yayınlanan enerjiyi kullanırlar. Yarı-pasif ve aktif etiketlerde ise kendilerine ait bir enerji kaynakları vardır. Aktif etiketlerle yarı-pasif etiketlerin farkı ise yarı-pasif etiketlerin ilk konuşmayı başlatmaması ve okuyucudan gelen sorgu ile konuşabilmesidir. Kendi enerji kaynağını, okuyucudan gelen sorgu ile kullanmaya başlar. Aktif RFID etiketleri ise okuyucu ile kendi konuşma başlatabildiği gibi ondan gelen sorgu ile de konuşmaya başlayabilir.

Aktif RFID etiketleri, birçok uygulamada sahip oldukları görünürlük, güvenlik, kaliteli ve uzak mesafeli haberleşme kabiliyetleri açısından tercih edilebilmektedir. Bir aktif RFID etiketi, içerisindeki veriyi iç enerji kaynağı yardımıyla oldukça uzak mesafelere iletilebilir. Ancak batarya süresi, etiketin aktif parçaları sebebiyle azalmaktadır. Böylece bu, haberleşme mesafesiyle enerji tüketimi arasında kayıp-kazanç dengesine dönüşmektedir (yani mesafe artarken, enerji tüketiminde artma veya tam tersi). Bununla birlikte iletim mesafesinin artması, girişim problemlerine de neden olabilir çünkü bir okuyucunun okuma ortamında olabilecek etiketler ve/veya okuyucular haberleşmede zorluklara zemin hazırlayabilir.

ISO/IEC 18000-7 bir aktif RFID standardıdır. Bu standardın etiketleri 433 MHz frekansında çalışmaktadır. Biz fark ettik ki, bu standartta uyan aktif bir RFID etiketi, Rayleigh sönümlemeli kanalda tatmin edici bir haberleşme gerçekleştirebilmesi için oldukça fazla enerji tüketmektedir. Bu tezde ikinci olarak biz, ISO/IEC 18000-7 standardındaki aktif RFID sistemlerinin haberleşme kalitesi ve enerji verimliliği açısından performanslarını iyileştirdik. Simülasyon sonuçlarımız göstermiştir ki, gerek etiket gerekse hem etiket hem de okuyucu tarafındaki çoklu anten tasarımları, sınırlı geri besleme tekniklerinin kullanılmasıyla çerçeve hata oranlarını düşürmüş ve enerji kaynağının yaşam süresini arttırmıştır.

1. INTRODUCTION

In this chapter, we present vital concepts of this study and give a few basic definitions. These definitions will be useful to support ideas for later chapters. Firstly, we briefly introduce the background information of RFID systems then we describe the major contributions of this thesis.

1.1 A General RFID Technology Overview

1.1.1 RFID systems

Radio **F**requency **ID**entification (RFID) has become very popular in wireless technologies and pervasively deployed in many applications, such as contactless credit cards, e-passports, ticketing systems, access control, gaming, healthcare, pharmaceuticals, document and media management. This technology provides wireless communication with an object or someone to automatically identify or track by using radio waves [1].

A typical RFID system basically consists of a tag *(transponder)*, a reader *(interrogator)* and a back-end system *(database)*. A tag contains an antenna and a microchip. The chip stores data and processes cryptographic functions. The antenna is a transducer that converts radio waves to electric currents or vice versa. It is interrogated by a reader with its modulated radio signals. A tag is attached to target objects and identified by a RFID reader. An RFID reader which has a central role in an RFID system, acquires the data of the tag and convey it to the back-end system for further processing. All relevant information about the tag is stored and managed in server side. Figure 1.1 illustrates a typical RFID system. Moreover, RFID tags can be categorized in three groups by using energy source such as active, passive and semi-passive or active (battery assisted) tags. Passive RFID tags do not have own internal energy source. Instead, they use the radio energy transmitted by the reader [2]. Furthermore, RFID systems can also be grouped into the three basic ranges by their using operating frequency: Low frequency (LF, 30-300 KHz), high fequency (HF 3-30 MHz) and ultra high frequency (300 MHz - 3 GHz) / microwave (>3 GHz) [1].

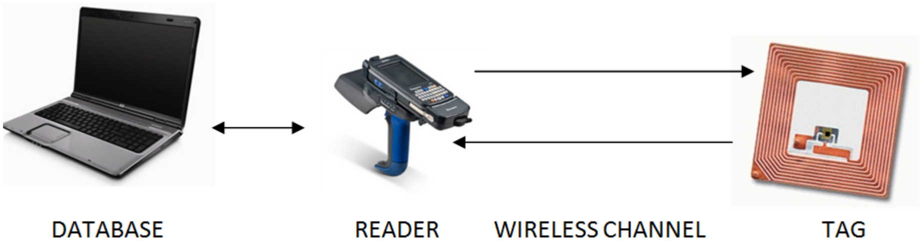


Figure 1.1: A Basic RFID System

1.1.2 Some basic terms

The term 'protocol' is generally used as a shorthand expression for 'cryptographic protocol'. A cryptographic protocol is a distributed algorithm describing precisely the interactions of two or more entities to achieve certain security objectives. The entities interact with each other by exchanging messages over private and/or public communication channels [3, 4]. In other words, it is defined that a certain communication procedure between two parties. In RFID protocols these two interacting entities are mostly an RFID reader (verifier) and a RFID tag (prover).

An *authentication* is a process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (*i.e.*, is active at, or immediately prior to, the time evidence is acquired).

Here the goal of corroborative evidence is that to provide a proposition that is already supported by some initial evidence e.g., something known, something possessed or something inherent (to a human individual). Moreover, mutual authentication refers to the provision of entity authentication for both parties [3].

On the other hand, the term *identification* is used to simply refer to the process of claiming or stating an identity without providing the corroborating evidence required for entity authentication [3].

1.2 Main Contributions

The summary of the contributions of this thesis can be divided in two main branches as:

We present the performance evaluation of passive RFID systems complyig with ISO 18000-3 standard by using simulation enviroment. We improve the PETRA simulation environment by adding two channel models, AWGN channel, Rayleigh fading channel and show the performance bounds of an RFID authentication protocol in these channels for ISO/IEC 18000-3 standard. For this purpose, we implement a secure and private authentication protocol in our new simulation environment to understand the effect of the wireless channel in a real life scenario. The performance analysis of HF contactless smart cards in air are untouched research area. Hence, we decide to enhance a RFID protocol design environment to answer that need. At the end, we observe the performance results, present the best and the worst success rates of the RFID system. This work may guide the protocol designers to test their protocols and see their performance before using them on real systems.

Secondly, we examine the performance of active RFID systems for with ISO/IEC 18000-7 standard. We reformulate that the performance of an active RFID system compliance with ISO/IEC 18000-7 standard is improved by limited feedback methods. The tag is equipped with multiple-antennas and limited feedback is available from the reader to the tag. It can be seen from our detailed simulations that limited feedback schemes yields more than 30 dB better performance with respect to the single antenna case. This improvement is not only extensive amount of battery consumption at the tag side but also diminishing interference at the wireless environment.

1.3 Organization of the Thesis

The remaining body of the thesis is arranged as follows:

In **Chapter 2**, we present the performance analysis of passive RFID systems complying with ISO 18000-3 standard by using a simulation environment. We observe the performance results, show the best and the worst success rates of the RFID system.

In **Chapter 3**, we aim to ameliorate an active RFID system performance from the perspective of better communication and energy efficiency. Detailed and extensive simulations show that multiple-antenna designs at tag side using limited feedback schemes significantly decreases the frame error rates and increases the battery lifetime.

In **Chapter 4**, we conclude the thesis and describes possible directions for future works.

2. THE PERFORMANCE ANALYSIS OF PASSIVE RFID SYSTEMS FOR ISO 18000-3 STANDARD

In this Chapter, we present the performance analysis of passive RFID systems complying with ISO 18000-3 standard by using a simulation environment. The simulation environment includes a complete passive RFID system that contains one reader, one back-end system (database) and many tags. The performance of a passive RFID system depends on the quality of servising an application. The service quality of an application also depends on the effects of wireless channel. Therefore, we visualize that we have a big warehouse which store thousands of products labelled with unique RFID tags. These tags try to authenticate themselves to the reader by using an authentication protocol in a wireless channel. We prefer one of the most private and secure authentication protocol and implement the protocol and run it. At the end, we observe the performance results, present the best and the worst success rates of the RFID system.

2.1 Introduction

Passive RFID tags use authentication protocols in many applications. These protocols take a vital place in RFID world. The performance of the protocols affects the quality of RFID applications. Therefore, many simulation environments have been improved to evaluate the performance of these kinds of protocols. However, none of them shows the success bounds of the protocols by considering wireless channel effect.

Today, passive RFID tags, particularly contactless smart cards, have been still proliferating because of their productivity, efficiency, reliability. But this increased usage of RFID systems brings some serious problems together, security and privacy [5–8]. Especially, using wireless communication and preferring low cost tags, which have restricted capacity and limited computational power, deepen the concerns. Many wireless RFID protocols are proposed to overcome these issues [9–12]. The main aim of each protocol is providing that an adversary cannot impersonate a legal tag to the reader and cannot link a relationships between itself or another tag whenever and wherever they are observed.

A growing security and privacy concerns are most commonly related with high frequency (HF) RFID devices, using near field communication (NFC), such as contactless smart cards (CSC), because they are used to store secure and private personal information in many RFID applications: e-passport, govern ID, credit cards etc. Furthermore, CSCs are divided into some groups based on the standards that describe the physical characteristics, signal interface, anti-collision and transmission protocol for vicinity coupling smart cards with a range from 10 cm up to 1-1.5 m. Many researches offer different protocol designs to overcome the security and privacy problems for the standards. Although, their security and privacy analysis are quite important, their effectiveness is also another vital point for real world RFID applications. Unfortunately, it is a troublesome to physically test them because of cost, time and it is also impractical.

In fact, simulation environments are helpful tools to test the performance of the new innovative protocol designs. Most of simulator designers are interested in UHF RFID systems. However, the performance analysis of HF contactless smart cards in air are untouched research area. Hence, we decide to enhance a RFID protocol design environment to answer that need. We realise that PETRA simulation environment suits well to ISO/IEC 18000-3 standard MODE 1 but there is a deficiency in transmission layer. It is assumed that there isn't any destructive effect against to real life applications. Actually, this situation impedes the protocol designers to test the performance of their protocols in real world scenarios. Motivated by this need, in this chapter, we ameliorate the simulations environment by adding two channel models, AWGN channel and Rayleigh fading channel. We determine the performance bounds of a RFID authentication protocol in a wireless channel for ISO/IEC 18000-3 standard [13]. We determine the upper bound of the success rate by running the protocol in AWGN channel and the lower bound in Rayleigh fading channel which is the worst environment for an RFID communication.

In this chapter, we improve the PETRA simulation environment by adding two channel models, AWGN channel, Rayleigh fading channel and show the performance bounds of an RFID authentication protocol in these channels for ISO/IEC 18000-3 standard. For this purpose, we implement a secure authentication protocol in our new simulation environment to understand the effect of the wireless channel in a real life scenario. This work may guide the protocol designers to test their protocols and see their performance before using them on real systems.

The last of the paper is as follows: In the next section, we briefly talk about the related previous works. Then, we analyse the AWGN and Rayleigh channels. In section 2.4, we explain ISO/IEC 18000-3 standard MODE 1. Later on, in Section 2.5, we give a detail description of the implemented protocol in our simulation. In section 2.6, we give the simulation setup and show the results.

2.2 Related Works On Simulation Environments

Many wireless network simulators have been developed to model the behavior of a network. In the long history of networking research, it is seen that different attributes of real life scenarios can be tested in a software platform and performance analysis can be obtained. It also provides to test the most popular protocols, such as Wireless LAN, Wi-Max, and TCP. Ns-2 (Network simulator) is a discrete event network simulator popularly used in the simulation of routing and multicast protocols, which began to develop in 1989 as a variant of the real network simulator [14]. GloMoSim [15] (Global Mobile Information System Simulator) which uses the Parsec (C-based simulation language) compiler to compile the simulation protocols and OPNET Modeler [16, 17], which is a software tool, for network modeling and network performance, are a few examples of wireless network simulators. Although RFID is one of the most popular technologies in wireless area, there are not enough available simulation platforms for RFID communication protocols.

One of the simulation environment tool, mentioned above, ns-2 is used by Balakrishnan [18] for network engineers to investigate how various protocols perform with different configurations and topologies. The simulation models tags and readers in a RFID system. Han et al. [19] presented a system simulation environment in

Matlab/Simulink of RFID. In this work, a system model of the forward link and return link of RFID was constructed. The system simulation mentioned to reader side. It has a detailed model of the receiver part of the reader with a simple wireless channel and a simple reflection model of a tag to evaluate the performance of the reader. In the simulation, a protocol example conforming with EPC Class 1 Generation 2 (EPC C1G2) standard was given.

In 2007, Guang Xu [20] studied on RFID Application Simulation Environment in SDR Workbench in his master thesis. In this work, EPC C1G2 standard was chosen for RFID air interface. Four modulation schemes (ASK, BPSK, QPSK and 8-PSK) are used to simulate the transmission line (tag-to-reader) in Matlab. Then, the performance comparison of four methods were presented.

RFIDsim [21] uses the discrete event simulator to simulate a physical RFID environment with signal propagation and RFID communication protocols for real-world application. In this simulator, ISO 18000-6C UHF RFID communication protocol and some features (characteristics) of a typical wireless channel and various models such as pathloss, fading, backscattering and capture, tag mobility were implemented.

Dominikus and Aigner [22] developed the RFID simulation engine Protocol Evaluation Tool for RFID Applications (PETRA) in IAIK institute at the Graz University of Technology. In this tool, ISO/IEC 18000-3 HF RFID protocol implemented without modeling the physical layer. The Java program PETRA was designed for simulating the communication between RFID reader and tags conforming the ISO/IEC 18000-3 standard [23].

2.3 Channel Analysis

Additive White Gaussian Noise (AWGN) and Rayleigh at fading are simple and well-known models. These models which show the performance of wireless communication systems are best ones to determine the performance bounds of RFID protocols.

2.3.1 Channel types

2.3.1.1 Additive white gaussian noise (AWGN) channel

AWGN channel is the simplest and an ideal channel model. The model is preferred to compare the performance of wireless channel models and wireline channel models. It never models a real-life radio channel. The transmitted signal is corrupted by an additive white noise with a constant spectral density and a Gaussian distribution of amplitude.

$$r(t) = s(t) + n(t) \tag{2.1}$$

In an AWGN channel, $s(t)$ is transmitted and corrupted by an additive white Gaussian noise $n(t)$. $n(t)$ does not have imaginary component and obeys the a Gaussian distribution with zero mean and one standard deviation. Its power spectral density functions is a constant over whole spectrum. $s(t)$ is received as $r(t)$ by receiver (Equation **2.1**).

2.3.1.2 Rayleigh fading channel

AWGN channel model makes easier to interpret Rayleigh flat fading channel. In wireless communication, the fading effects can be basically divided into two types: Large-scale fading (or path loss) and small scale fading (multipath fading). Addition to these two mutually independent propagation phenomena, shadowing effect represents the medium-scale effect. For a detail information, the following source can be examined [24], [25]. We can assume that frequency flat Rayleigh fading channel where channel gains are circularly complex Gaussian random variables and statistically independent from each other. The fading coefficients remain constant over the duration of one frame.

In following sections, these wireless channel characteristics between a transmitter and receiver will be given in a detail.

- **Large scale fading (path loss)**

  In the study of wireless communications, path loss (or path attenuation) is one type of the large-scale fading effects [24]. The strength of the signal attenuation is caused by many effects: free-space loss, refraction, diffraction, reflection etc. In fact, it includes all the lossy effects which are related to distance and the environmental obstacles between two parties. Path loss can be represented by the path loss exponent. In general, the value is in the range of 2 to 4. It is 2 for free space and 4 for lossy environments or for the case of full specular reflection from the earth surface (flat-earth model). Path loss is usually expressed in logarithmic (see Equation (**2.2**)).

$$L = 10 \cdot \alpha \cdot \log(d) + C[dB] \tag{2.2}$$

L is the path loss in decibels, α is the path loss exponent, d is the distance between the transmitter and the receiver in terms of meter and C is a constant for system losses. The free space path loss is propositional with the distance between transmitter and receiver (Equation (**2.3**)).

$$L = \left(\frac{4\pi d}{\lambda}\right)^2 \tag{2.3}$$

where λ is the wave-length of the signal in terms of meter.

- **Shadowing**

  The large objects on between transmitter and receiver cause to impede the transmitted signals to reach the receiver. In other words, the obstacles shadowing the receiver. In the simulation, this phenomenon is not considered.

- **Small-scale fading (multipath fading)**

  The amplitude of a transmitted signal in a wireless channel over a short period time might be rapidly fluctuated [26]. This is called small-scale fading effect of the channel. The transmitter transmits the signal but the signal might reach to receiver in more than one path because of channel characteristics. Hence, the receiver obtains the superposition of the multiple copies of the signal. These reflections are called multipath waves. Each multipath wave is exposed attenuation, phase shift and delay. The small-scale fading has a Rayleigh distribution (Equation **2.4**) if there isn't any line of sight (LOS) between the transmitter and receiver. In other words, there is absence of the strong signal between two parties. On the other hand, this fading suites a Ricean distribution when there is LOS between them. The small-scale fading can be categorised in some groups based on multipath time delay spread, based on doppler spread [25].

$$P(x) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}, x \geq 0 \tag{2.4}$$

Before grouping the fading channels, some definitions enlighten the fading types.

*Coherence bandwidth (Bc):*The coherence bandwidth is a statistical measure of the range of frequencies over which the channel passes all spectral components with approximately equal gain and linear phase. Based on multipath time delay spread:

- **Flat Fading:** Flat fading is occurred when the coherence bandwidth (Bc) of the channel is larger than the bandwidth of the transmitted signal. Under this fading, the all frequency components of the signal are exposed the same amount of attenuation. The gain of the channel fluctuated in times. This type of fading channel is sometimes referred to as a 'narrow-band' channel.
- **Frequency Selective Fading:** Frequency selective fading is occurred when the coherence bandwidth (Bc) of the channel is smaller than the bandwidth of the transmitted signal. Under this fading, the different frequency components of the signal are exposed the different amount of attenuation. The gain of the channel is fluctuated in time and frequency.

The fading channel can be also grouped based on doppler spread; fast fading and slow fading but in our simulation environment we don't consider them.

2.3.2 The BER analysis of AWGN and rayleigh Channel

In this section, we calculate the probablity error for AWGN and rayleigh fading channel. Figure 2.1 shows the representation of AWGN channel.

ASK signals are one-dimensional. Therefore, their geometric representation is simply one-dimensional vector. Figure 2.2 shows the signal points for binary antipodal signals. ASK signal represantation corresponds to the error propablity of binary antipodal signals. Therefore, we prefer to present the antipodal signal notation.

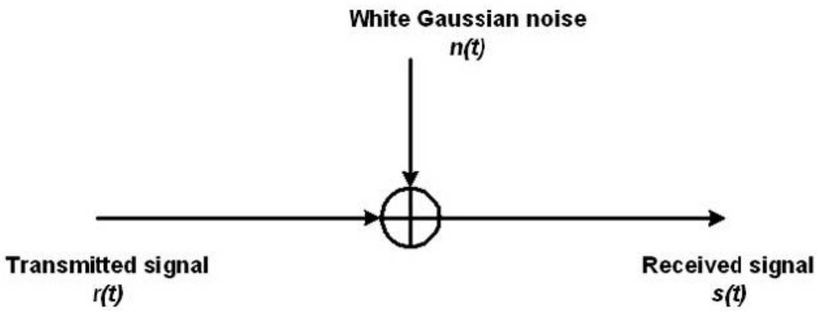


Figure 2.1: The Representation of AWGN Channel

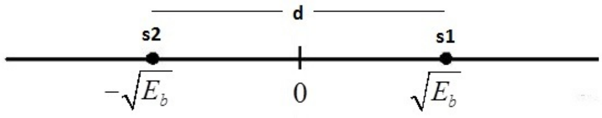


Figure 2.2: Signal Point for Binary Antipodal Signals

Let us assume that two signals are equally likely and the signal s_1 was transmittted. Then, the received signal from the demodulator is shown in Equation **2.5** where n represents the additive Gaussion noise component, which has zero mean and variance $\sigma_2 = \frac{1}{N_0}$. Figure 2.3 shows the power spectral density (PSD) of the wideband white noise.

$$\begin{aligned} r &= s_1 + n = \sqrt{E_b} + n \\ p(r \mid s_1) &= \frac{1}{\sqrt{\pi N_0}} e^{-\frac{(r-\sqrt{E_b})^2}{N_0}} \\ p(r \mid s_2) &= \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(r+\sqrt{E_b})^2}{N_0}} \end{aligned} \qquad \textbf{(2.5)}$$

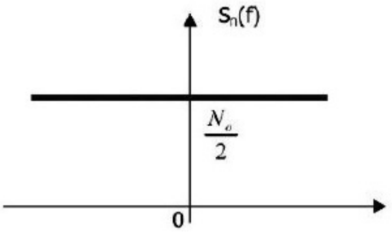


Figure 2.3: The Power Spectral Density (PSD) of the Wideband White Noise

In this stage, the decision rule is chosen that if $r \geq 0$, the decison is s_1 message is transmitted, and if $r \leq 0$, the decison is s_2 message is transmitted. Figure 2.4 shows the conditional PDFs of two signals. Equation **2.5** also shows the PDFs.

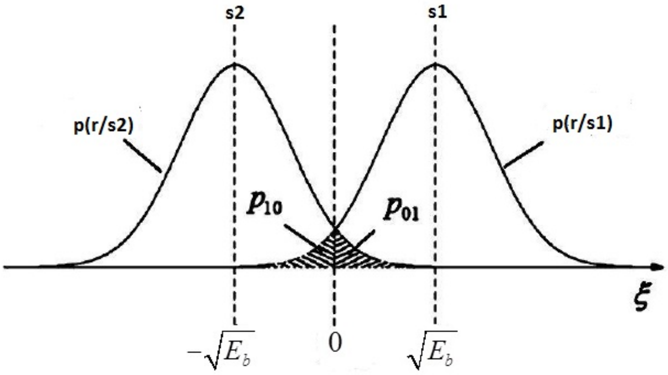


Figure 2.4: Conditional PDFs of two Signals

Given that s_1 message is transmitted, the probability error rate is shown in Equation **2.6** where Q and erfc error functions are defined in Equation **2.7** and Equation **2.8** respectively.

$$\begin{aligned} p(e \mid s_1) = p_{10} &= \int_{-\infty}^{0} \mathrm{p(e \mid s_1)}\,\mathrm{d}r \\ &= \frac{1}{\sqrt{\pi N_0}} \int_{-\infty}^{0} \mathrm{e}^{-\frac{(\mathrm{r}-\sqrt{\mathrm{E_b}})^2}{\mathrm{N_0}}}\,\mathrm{d}r \\ &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\sqrt{2E_b/N_0}} \mathrm{e}^{-\frac{\mathrm{x}}{2}}\,\mathrm{d}x \\ &= \frac{1}{\sqrt{2\pi}} \int_{\sqrt{2E_b/N_0}}^{\infty} \mathrm{e}^{-\frac{\mathrm{x}}{2}}\,\mathrm{d}x \\ &= Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \end{aligned} \tag{2.6}$$

$$Q(x) = \int_{x}^{\infty} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{\mathrm{y}^2}{2}}\,\mathrm{d}y \tag{2.7}$$

$$erfc(x) = \int_{0}^{x} \frac{2}{\sqrt{\pi}} \mathrm{e}^{-\frac{\mathrm{y}^2}{2}}\,\mathrm{d}y \tag{2.8}$$

Similary, if s_2 message is trasnmitted, the same error rate is obtained. Since the signals are equally likely to be transmitted, the average probability of error is shown in Equation **2.9**.

$$\begin{aligned}P_e &= \frac{1}{2}p(e \mid s_1) + \frac{1}{2}p(e \mid s_2)\\ p(e \mid s_1) &= p(e \mid s_2) = p_{10}\\ P_e &= Q\left(\sqrt{\frac{2E_b}{N_0}}\right)\\ P_e &= \frac{1}{2}erfc\left(\sqrt{\frac{E_b}{2{\sigma_n}^2}}\right)\end{aligned} \tag{2.9}$$

The probabilit of error might be express in terms of the disance between to signals s_1 and s_2. The distane between to signals is $d_{12} = 2\sqrt{E_b}$. By substituting that relation into the Equation **2.9**, we've got the Equation **2.10**

$$P_e = Q\left(\sqrt{\frac{d_{12}^2}{2N_0}}\right) \tag{2.10}$$

In this simple case, the actual communication only involves one antenna on the transmitter and receiver sides. We'll reach a general formulae of ASK modulation to obtain bit errror rate for AWGN and rayleigh channel. For this reason the complex channel gain from the transmit antenna to the receive antenna is simply denoted by h in the following Equation **2.11**. The received signal during a given symbol cycle is obtained with using match filter. Noise is invariant to rotation in the complex plane. The constellation is quadratically symmetric and the symbols are equally probable. We've already give these assumptions above. Let d be the euclidian distance between two nearest neighbor signals s_1, s_1 and ${\sigma_{\tilde{n}}}^2$ the variance of the noise.

$$\begin{aligned}y &= hs + n\\ z &= \mid h \mid^2 + hn\\ \tilde{s} &= s + \tilde{n}, \tilde{n} = \frac{n}{\mid h \mid}\\ {\sigma_{\tilde{n}}}^2 &= \frac{{\sigma_n}^2}{\mid h \mid^2} = \frac{N_0}{2\mid h \mid^2}\end{aligned} \tag{2.11}$$

We obatin the Equation **2.12** from the Equation **2.11**.

$$P_e = \frac{1}{2}erfc\left(\sqrt{\mid h \mid^2 \frac{E_b}{N_0}}\right) \tag{2.12}$$

Real and imaginary parts of h are modelled as independently identically distributed (i.i.d.) real valued gaussian random variables with zero mean and the pdfs of X and Y are given in Equation **2.18**. Hence, the PDFs of X and Y are also given in Equation **2.13** by [27].

$$\begin{aligned} h &= X + jY \\ f_x &= \frac{1}{\sigma\sqrt{2\pi}} e^{\left(\frac{-x^2}{2\sigma_2}\right)} \\ f_y &= \frac{1}{\sigma\sqrt{2\pi}} e^{\left(\frac{-y^2}{2\sigma_2}\right)} \end{aligned} \qquad (\mathbf{2.13})$$

Since both random variables are statistically independent and zero mean the mean and variance of h

$$\begin{aligned} \mu_h &= E[X] + jE[Y] = 0 \\ \sigma_h^2 &= E[X^2] + E[Y^2] = 2\sigma^2 \end{aligned} \qquad (\mathbf{2.14})$$

An additional conclusion from statistical independent and zero mean X and Y is that $\mid h \mid^2 = X^2 + Y^2$, see Equation **2.15**, is central chi-squared distributed with two degrees of freedom [28].

$$\mid h \mid^2 = X^2 + Y^2, \quad \text{chi-square dist.} \qquad (\mathbf{2.15})$$

Hence, we obtain the Equation **2.16**

$$pdf_{|h|^2}(x) = \frac{1}{2\sigma^2} e^{\left(\frac{-x}{2\sigma_2}\right)}, \quad 0 \leq x \qquad (\mathbf{2.16})$$

Furthermore, $\mid h \mid$ follows a Rayleigh distribution. When x is Raleigh distributed, x^2 has a chi-square probability distribution.

$$pdf_{|h|}(x) = \frac{x}{2\sigma^2} e^{\left(\frac{-x^2}{2\sigma_2}\right)}, \quad 0 \leq x \qquad (\mathbf{2.17})$$

By using the central chi-squared distribution (Equation **2.16**) and results in the following double integral in Equation **2.16**. If we evaluate the Equation **2.18**, we have the BER of two channels.

$$\begin{aligned} BER &= \int_0^\infty BER_{|h|^2} \mathrm{pdf}_{|\mathrm{h}|^2}(y)\, \mathrm{d}y \\ &= \frac{1}{\sqrt{\pi}} \int_0^\infty e^{-y} \int_{\sqrt{y\frac{Eb}{N_0}}}^\infty e^{-x^2}\, \mathrm{d}x\, \mathrm{d}y \end{aligned} \qquad (\mathbf{2.18})$$

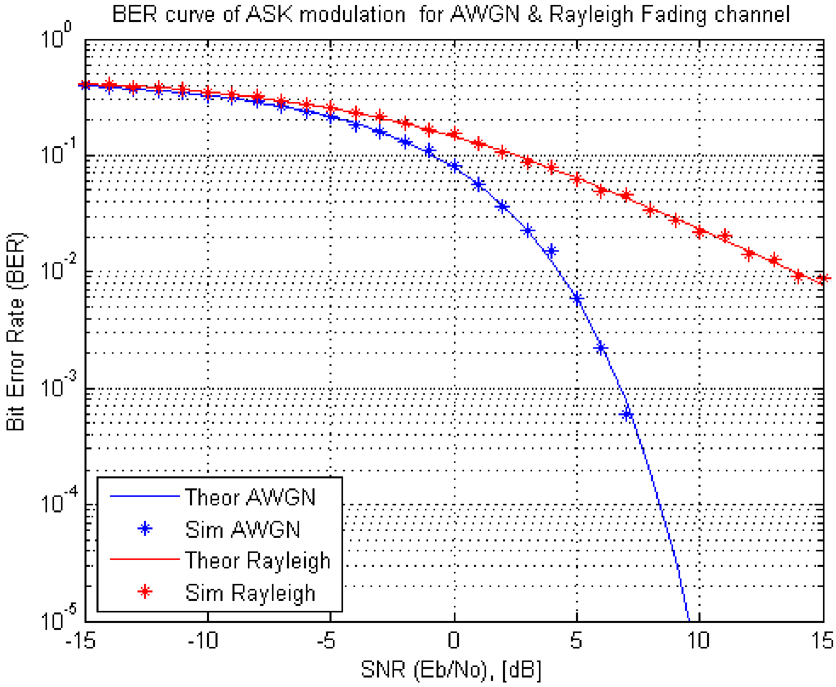


Figure 2.5: Bit Error Rate (BER) of AWGN and Rayleigh Fading Channel

We calculate the BER of rayleigh fading channel by using above equation and the analytical result is given by [28] that Equation **2.19** shows the BER of rayleigh fading channel. By the way, if $h = 1$, that channel is AWGN.

$$BER = \frac{1}{2}\left(1 - \sqrt{\frac{\frac{Eb}{N_0}}{1+\frac{Eb}{N_0}}}\right) \qquad (\mathbf{2.19})$$

2.3.3 The comparison of AWGN channel and rayleigh fading channel

The theoritical bit error rate (BER) of AWGN and Rayleigh channels is shown in Equation **2.20** and Equation **2.21**, respectivly where SNR denotes to signal-to-noise ratio.

Figure 2.5 shows the both theoritical and simulation bit error rate results.

We simulate AWGN and Rayleigh Fading channel to compare their exact performance before implementing wireless layer into the simulation environment and plot the frame error rates (FER) for varying SNR levels that in range from $0B$ to $15dB$ (see Figure 2.6) with one byte frame length. We assume the channel is flat fading so the multipath channel becomes only one tap and it is randomly varying in time.

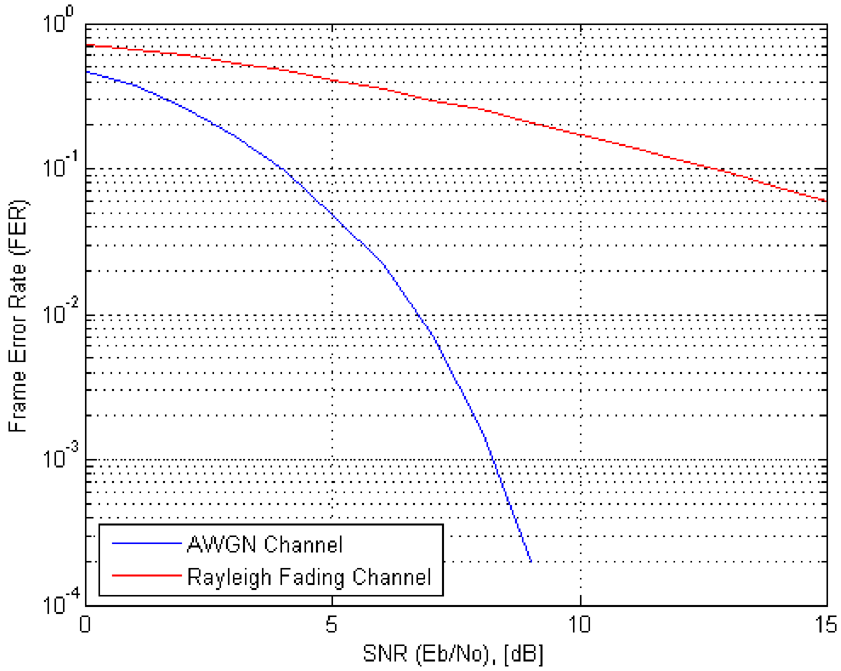


Figure 2.6: Frame Error Rate (FER) of AWGN and Rayleigh Fading Channel

$$Pe_{awgn} = \frac{1}{2} erfc\left(\sqrt{SNR}\right) \tag{2.20}$$

$$Pe_{ray} = \frac{1}{2}\left(1 - \sqrt{\frac{SNR}{1+SNR}}\right) \tag{2.21}$$

Figure 2.6 shows the theoretical and simulation plots of the both channels.

It can be clearly seen that a communication system in the AWGN channel is much better than the Rayleigh fading channel.

$$Pe_{(FER)} = 1 - (1 - Pe)^{L\times 8} \tag{2.22}$$

On the other hand, the Figure 2.6 shows the FER with 1-byte frame length. Equation **2.22** formulate the frame error rate (FER) with respect to the length of the frame, where $L \times 8$ is the length of the frame and L represent the how many bytes are sent in the frame. This Equation states that the length of the frame is increased, the FER curves become worser.

2.4 ISO/IEC 18000-3 Standard

High frequency (HF) has the most established and commonly used frequency among all the RFID systems. ISO/IEC 15693 is an ISO standard for vicinity cards. ISO/IEC 15693 defines parameters for RFID tags/cards, generally preferred in applications which require read ranges of more than 10 cm [29]. ISO/IEC 14443 is one of the most pervasively used standards at the same frequency for proximity RFID tags [30]. The vital difference is that vicinity tags can be read from a greater distance as compared to proximity ones. Furthermore, the version ISO/IEC 18000-3 based upon ISO/IEC 15693 for providing physical layer, collision management system and protocol values operating at 13.56 MHz [23].

Furthermore, ISO/IEC 18000-3 standard provides physical Layer, collision management system and protocol values for RFID systems for item identification operating at 13.56 MHz in accordance with the requirements of ISO 18000-1.

Most people are confuse with proximity and vicinity RFID tags. Although, both of two standards are very similar, their intended application is the main difference between them and vicinity tags can also be read from a greater distance as compared to proximity ones supported by ISO/IEC 14443. Later on, ISO organization started a more specific process for RFID standardization under the SC31 roof. ISO/IEC 18000-3 published in 2004, is the new standard for 13.56 MHz RFID systems [23]. ISO/IEC 18000-3 standard defines 3 non contending MODES. MODE 1 is a comprehensive standard which has been built on the ISO/IEC 15693. The physical, collision management and transmission protocols determined in this MODE are consistent with the approach taken in ISO/IEC 15693. In other words all features for the MODE 1 air interface at 13.56 MHz shall be compliant with ISO/IEC 15693. The version ISO/IEC 18000-3 based upon ISO/IEC 15693 for providing physical layer, collision management system and protocol values is used in PETRA simualtion environment. Therefore, after this introductive informantion about the standards at 13.56MHz for RFID systems, we explain ISO/IEC 15693 standard.

ISO/IEC 18000-3 standard provides physical Layer, collision management system and protocol values for RFID systems for item identification operating at 13.56 MHz in accordance with the requirements of ISO 18000-1.

ISO/IEC 15693 is an ISO standard for vicinity cards. Most people are confuse with proximity and vicinity RFID tags. The vital difference is that vicinity tags can be read from a greater distance as compared to proximity ones.

Tags are uniquely identified by their own Unique identifier (UID) which is composed of 64 bits. This ID provides for addressing each tag uniquely and individually during anti-collision and communication stages.

A protocol defines the communication steps between a reader and tag by using request and response. A request is transmitted by the reader to the tag. The tag responses to the request. The instructions between both parties are started by the reader. It is known that this standard is for passive tags which don't have internal energy source. They are powered up by the reader's request. Each request consists of 5 fields and each response consists of 4 fields (see Table 2.1 and Table 2.2). Moreover, the request and the response are transmitted in a frame structure. Each frame starts with SOF (Start of frame) and end EOF(End of frame) delimiters. The tag responses after the request of the reader and it continues with consequent request and response frames (see Table 2.3, Table 2.4 and Table 2.5). For further information about each fields and more, ISO/IEC 15693-2,3 standards can be examined [29].

Table 2.1: General Request Format

SOF	Flags	Comman Code	Parameters	Data	CRC	EOF
1 Byte	1 Byte	1 Byte	1 Byte	0-8 Bytes	2 Bytes	1 Byte

Table 2.2: General Response Format

SOF	Flags	Parameters	Data	CRC	EOF
1 Byte	1 Byte	1 Byte	N Bytes	2 Bytes	1 Byte

Moreover, each request and response includes two bytes *CRC*(Cyclic redundancy check), defined in ISO/IEC 13239, within each frame before EOF. All of the bytes in a frame, after the *SOF* byte or from the start of the flags to the end of the frame, are used to calculate the *CRC* bytes. When a request is received by a tag from a reader, it verifies that the *CRC* value is valid or not. If it is invalid, a tag discards the request and does not respond. But in the same situation, the responsibility is left to reader designer. The initial state of the *CRC* is 'FFFF' with $x^{16} + x^{12} + x^5 + 1$ polynomial and backward direction.

Table 2.3: Inventory Request Format

SOF	Flags	Inventory	Optional AFI	Mask Length	Mask Value	CRC	EOF
1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	0-8 Bytes	2 Bytes	1 Byte

Table 2.4: Inventory Response Format

SOF	Flags	DSFID	UID	CRC	EOF
1 Byte	1 Byte	1 Byte	0-8 Bytes	2 Bytes	1 Byte

Table 2.5: Custom Request Format

SOF	Flags	Custom	IC Mfg Code	Custom Request Parameter	CRC	EOF
1 Byte	1 Byte	1 Byte	1 Byte	Custom Defined	2 Bytes	1 Byte

Tags can be in four different states. These are power-off, ready, quiet and selected states. Figure 2.7 specified the transition of the states. In the power-off state (*A*), the tags are not powered up. They are inactive. In ready state (*B*), tags are activated by reader and they are ready to answer any request whose selected flags is not set. In the quite state (*C*), if inventory flag of a request is not set and at the same time its address flag is set, the tags process this request. These are mandatory states in the standard. In the optional state (*D*), tag only responses to the request with set the selected flag. A tag keeps its current state for other transitions. Moreover, anti-collision term is one of most important procedure in passive RFID tags. A further explaination with a illustrated clear example can be examined in ISO/IEC 15693 Part-3 document.

A RFID tag in this standard harvest its power which is used for internal operations by radio frequency via coupling antennas. The communication from the reader to tag

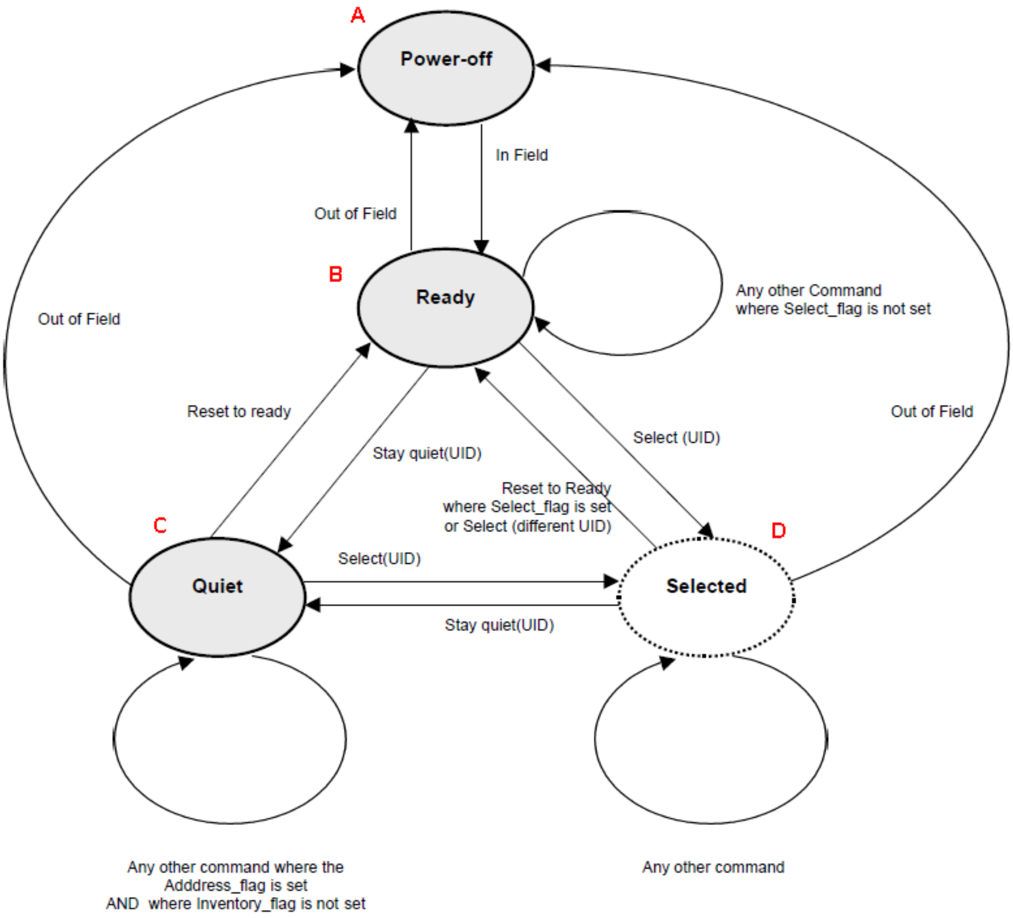


Figure 2.7: The States of a RFID Tag

is accomplished by modulating this RF field. The carrier frequency (fc) of the RF field is 13,56 MHz. Reader side uses an amplitude-shift keying (ASK) with 10% or 100% modulation index and tag side decodes both. On the other side, tag side, uses ASK or frequency shift keying (FSK) in this standard. Furthermore, both parties use Manchester coding as line code in which the encoding of each data bit has at least one transition and occupies the same time without DC component. Moreover, the communication is occurred step by step. Firstly, the tag in the reading field of a reader is on power-off state. The conversation is started with the activation of the tag by the RF field of the reader. Secondly, the tag is on ready state and waits silently for a request from the reader. The tag responses after the request of the reader and it continue with consequent request and response frames (see Figure 2.3, Figure 2.4 and Figure 2.5).

2.5 The Implemented Protocol In Our Simulation Environment

We explain an authentication protocol which is used in our simulation environment to determine the effect of the wireless channel. This authentication protocol is proposed to meet almost all security and privacy features in the literature. The Figure 2.8 clearly shows the protocol.

Previously, we give a brief description of the assumptions and notations. Then, we talk about initialization and the authentication phases in a detail.

The notations of the proposed protocol:

- $\in_R$: A choice operator which randomly choice an element from a finite set.
- $\oplus, ||$: XOR and concatenation operator, respectively.
- h, H : A hash function s.t. $h : \{0,1\}^* \to \{0,1\}^n$, $H : \{0,1\}^* \to \{0,1\}^{2n}$.
- N : The number of tags in the database.
- N_a, N_b : n-bit random nonce generated by the reader and the tag, respectively.
- K : n-bit secret shared between the tag and the reader.
- val_1, val_2 : n-bit the server validator of the tag and the reader, respectively.

- K^{old_1}, K^{old_2} : Previous n-bit secret shared between the tag and the reader.
- val_1^{old}, val_2^{old} : Previous n-bit the server validator of the tag and the reader, respectively.
- L, S : The seed value of val_1 and val_2, respectively.
- r_1, r_2 : n-bit random bit strings produced by $h(N_a)$, $h(N_b, K)$, respectively.
- v_i : n-bit random bit strings produced by $h(K, r_1, r_2)$.
- M_1, M_2 : $M_1 = V_1 \oplus L$, $M_2 = V_2 \oplus S$.

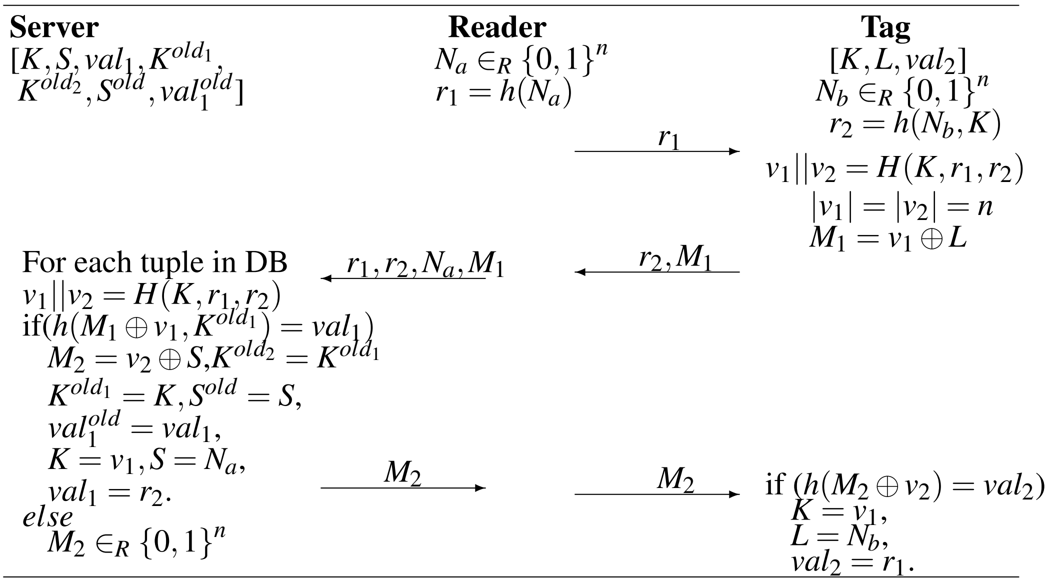


Figure 2.8: The Proposed RFID Authentication Protocol

2.5.1 The registration phase

The following steps must be performed by the registrar for each tag T_i, before the starting of the protocol:

1. Three n-bit random nonces (K, S, L) are generated by the registrar. At the same time, it computes $val_1 = h(L, K)$, $val_2 = h(S)$. Initially, K^{old_1} = K^{old_2} = K, S^{old} = S, and val_1^{old} = val_1.
2. The registrar creates an entry in its database. The entry has (K, S, val_1, K^{old_1}, K^{old_2}, S^{old}, val_1^{old}).

3. The registrar assigns (K, L, val_2) to the tag T_i.

2.5.2 The authentication phase

Each tag stores its own triple values K, L, and val_2 and the reader stores the K, S, val_1 for that tag in the protocol (see figure 2.8). The protocol steps are performed as follows.

Step 1. A reader generates a random n-bit nonce N_a and calculates hash of it $r_1 = h(N_a)$. Then, it tranmits r_1 to the tag T_i.

Step 2. The tag T_i generates a random n-bit N_b nonce and calculate hash of it, $r_2 = h(N_b, K)$. Then, the tag uses a pseudo-random function that hashes r_1, r_2 messages with shared secret key K to calculate $v_1 || v_2 = H(K, r_1, r_2)$. The length of each v_1 and v_2 are equal to n. Later on, the tag calculate M_1 message by XORing v_1 with secret L. Finally, the tag transmits r_2 and M_1 messages to the reader.

Step 3. The reader transmits N_a, r_1, r_2, and M_1 to the server.

Step 4. The server performs an exhaustive search among all tags in the database. It computes $v_1 || v_2 = H(K, r_1, r_2)$ and $h(M_1 \oplus v_1, K)$. The server checks that $h(M_1 \oplus v_1, K^{old_1})$ is equals to val_1.

If one match is found, then the server computes M_2 message by XORing v_2 with S and then sends M_2 to the reader. After that, it updates $K^{old_2} = K^{old_1}$, $K^{old_1} = K$, $S^{old} = S$, $val_1^{old} = val_1$, $K = v_2$, $S = N_a$, and $val_1 = r_2$.

If no match is found, then the server performs another exhaustive search. In this instance, it calculates $v_1 || v_2 = H(K^{old_1}, r_1, r_2)$ and it checks that $h(M_1 \oplus v_1, K^{old_2})$ is equals to val_1^{old}.

If one match is found, the server calculates M_2 message by XORing v_2 with S and transmits M_2 to the tag. After that, it updates $K = v_2$, $S = N_a$, and $val_1 = r_1$.

However, if there is no match, the server generates an n-bit random bit string and transmits to the reader. The random bit string is transmittes to that foreclose any attacker to validate M_1 for random nonces r_1 and r_2.

Step 5. The reader forwards M_2 message to the tag T_i. When T_i receives M_2 , it calculates $h(M_2 \oplus v_2)$ and checks that it is equal to val_2. If it is equal, then the tag complete updates as $K = v_2$, $L = N_b$, and $val_2 = r_1$.

2.6 Simulation Setup and Result

In this section, we discuss how to design our simulation environment, present some our observations and give the simulation results. We first define the PETRA simulation environment platform and improved it, Then, we give the parameters used in our simulation design.

2.6.1 The analysis of PETRA

Dominics and Aigner implements the ISO/IEC 18000-3 standard MODE 1 which operates at HF frequency band and try to represent the behaviour of a real world scenario of a RFID system [22]. There are four main separate layers in the simulation PETRA. These are database, RFID reader, transmission line and RFID tags. The transmission layer provides communication between reader and tags by instructions of the requests of the database (see Figure 2.9). The simulation flows in a time line and it is assumed that the time starts at 0 ms. Database generates appropriate requests to lead the reader to interrogate the tags which are inside its reading field. Reader sends requests as interrogation frames structure by using transmission layer.

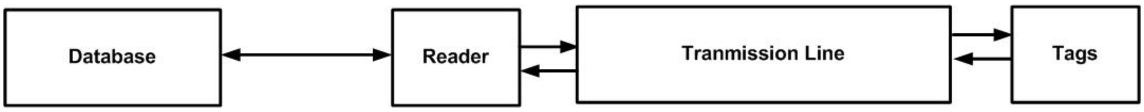


Figure 2.9: RFID System Structure to PETRA

The transmission layer passes the requests to the tags and collects their responses. The transmission layer also holds the availability information of the tags at the during the valid request period. At this point, there are three different scenarios. Firstly, in the reading field, there might be no tag so the transmission layer passes any response to reader. Hence, the reader only informs the DB once. Secondly, if there is only one answer, the reader starts to talk the tags. Thirdly, if there is more than one tag, the anti-collision procedure must be processed. Therefore, the informed DB sends a collision frame to the reader to request the all tags and tags response to every request. The current time is updated by the transmission layer within each request and response and each tag has own timing information. They keep the entering time information to the field and leaving time information from the field. The transmission layer decides the tag availability by considering that time stamps of the tags.

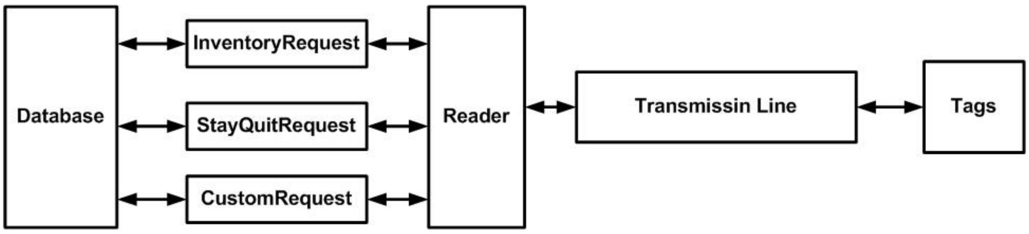


Figure 2.10: The Detailed Structure of PETRA

The program fulfils the timing definitions of the standard well. Figure 2.10 shows the detailed structure of PETRA. It is suggested that the usage manual can be examined to gather further information about the Petra simulation environment [22]. Although, the program is well designed, there is a vital deficiency in transmission layer from the point of real life scenarios. It is designed that the messages between a reader and a tag is never corrupted by any noise. In other words, it is assumed a perfect channel between them but it is an unreal situation. Therefore, we decide to design the best and worst channel models to see the performance bounds of a RFID authentication protocol. In the next section, we will explain our simulation design.

2.6.2 Our simulation environment

We use AWGN or Rayleigh channel models to simulate the transmission layer Figure 2.11 shows the backbone of our simulation enviroment. Hence, the messages are corrupted with the characteristics of the channel while two parties are talking. A message, request or response, refers to a frame in our simulation. If a party received a frame with invalid cyclic redundancy check (CRC), it discards the frame. Moreover, a reader and a tag use ASK modulation with Manchester coding as described in the standard. We also assume that the reader has isotropic antenna that radiates equal power in all directions (omnidirectional patterns). AFI (Application family identifier) byte is not used. Although, one time slot or 16 time slots are supported to use for inventory request in the standard, 16 time slots are preferred in our simulations. This choice causes getting more tags' IDs by a reader in the anti-collision procedure. We make radical changing over PETRA environment, although we comply ISO/IEC 15693 standard. Besides improving by adding the real physical layer in the environment, we change the scenario. We have simulated an authentication protocol for RFID over different simulation scenarios.

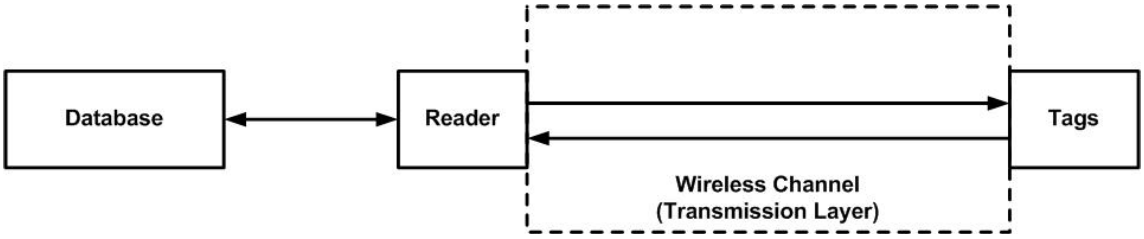


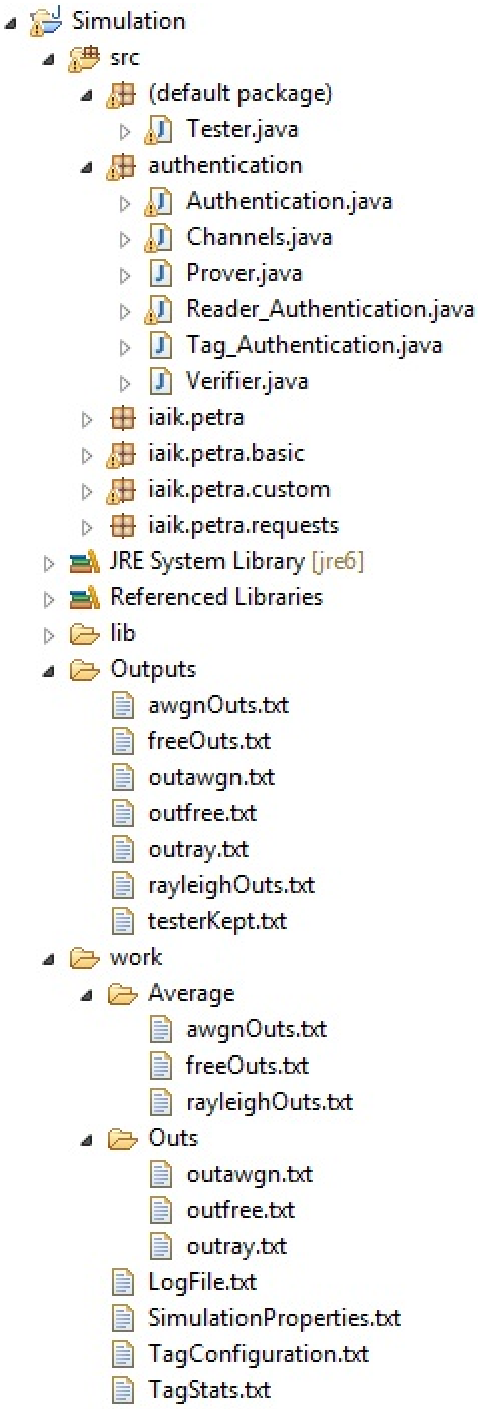
Figure 2.11: The Backbone of Our Simulation Enviroment

We change the PETRA class structure with obeying the standard. We just add a wireless channel and adjust the timing parameters. We also add authentication property to communication of reader and tags in this wireless channel.

Figure 2.12 shows our class structure of the simulation. In this class map, there are six different code parts. We avoid to explain the each class in a deatil not to be boring. However, we give a brief explanation about them below We use prover and verifier classes to represent the tags side and reader side, respectively. Our authentication protocol is implement in authentication class. Each steps of the protocol is given in Figure 2.8. Reader_Authentication and Tag_Authentication include every single step of the authentication protocol at tag and reader side. For instance, a hashing operation may be occured in a step. Wireless channel model is simulated in channel class.

2.6.3 Our simulation scenario

For describing the design and the parameters used in our simulations, it might be visualized that we have a big warehouse which store thousands of products labelled with unique RFID tags. All the products are wanted to be counted in a specified simulation time ***T*** (this may change for each simulation). We have only one person ***P*** who has the legitimate mobile RFID reader to identify the products in the warehouse. This reader is securely connected to a trusted database which stores the credential of each tag. A simulation scenario for counting process is done as follows. First of all,



- Simulation
  - src
    - (default package)
      - Tester.java
    - authentication
      - Authentication.java
      - Channels.java
      - Prover.java
      - Reader_Authentication.java
      - Tag_Authentication.java
      - Verifier.java
    - iaik.petra
    - iaik.petra.basic
    - iaik.petra.custom
    - iaik.petra.requests
  - JRE System Library [jre6]
  - Referenced Libraries
  - lib
  - Outputs
    - awgnOuts.txt
    - freeOuts.txt
    - outawgn.txt
    - outfree.txt
    - outray.txt
    - rayleighOuts.txt
    - testerKept.txt
  - work
    - Average
      - awgnOuts.txt
      - freeOuts.txt
      - rayleighOuts.txt
    - Outs
      - outawgn.txt
      - outfree.txt
      - outray.txt
    - LogFile.txt
    - SimulationProperties.txt
    - TagConfiguration.txt
    - TagStats.txt

Figure 2.12: The Class Structure of Our Simulation Enviroment

the person ***P*** starts to move in warehouse in order to identify tags by the help of the reader. The person walks around in all part of the warehouse for ***T*** seconds. During this period, the person uses reader to identify the tags. When a tag is identified and authenticated, the target tag will be silent. For simulation, we divide the simulation time in the time interval and a tag is assumed to appear in front of the reader with Exponential distribution in a time interval. The number of tags will appear in any time interval is distributed with Poisson distribution. In addition, any tag in front of the reader will stay ***x*** seconds where ***x*** is a number with Gaussian distribution.

We choose that the mean of the exponential time interval is 1,000 ms. The simulation is runned for different simulation of the time intervals and each period of the simulation time interval with this exponential time, averagely 5 tags come across with the reader. For instance, if the simulation time interval is chosen 8 s and the period interval is chosen 1 s, it means that in this simulation interval there will be 8 periods and each period 5 tags might be in the reading field at average. Therefore, possibly 40 tags might be ready to talk to the reader in that simulation time interval. Moreover, when a tag is inside the reading field of the reader, it stays there according to the Gaussian distribution with 500 ms average and 10 ms standard deviation. It is also assumed that a hash calculation is done averagely in 30 ms and a protocol is permitted to wait for only 60 ms. The other timing constraints are already defined in the standard.

For each simulation time interval, we regenerate the parameters and the restarted simulation is trailed ***N*** times. After ***N*** = 100 trials, the average results are obtained. This procedure is done for two wireless channel models over and over.

2.6.4 The simulation results

We obtain three graphs which explain the results well. The first graph, see Figure 2.13, shows the number of occurred trials for authentications versus the number of generated tags in the time interval (x-axis). In other words, it presents the number of identification during simulation time. The second graph, see Figure 2.14, shows the number of successes tags versus the same x-axis. It means that in that time interval those numbers of tags are successfully authenticated. The third graphs, see Figure 2.15, show the authentication time versus (x-axis), too.

The number of generated tags represents the simulation of time interval. The simulation time is linearly increased as 8, 16, 32, 40, 48 and 56 seconds and the characteristics of the two channels are observed. For Figure 2.13, 38 tags are approximately generated during the first time period, 8 seconds. This number is actually 38.3 but we round the number not to disrupt the consistency. It can be visualize that in the field of the reader there are 38 tags are ready to talk. At this point, the Figure 2.13 shows that 31, 28.1 tags are identified for AWGN channel, Petra simulation enviroment, respectively. On the other hand, 37 tags are identified in Rayleigh fading channel. In the fading channel, there are more tags are identified because more tags can't be authenticated. The unauthenticated tags have a second chance for a new authentication so they are identified again and again. But if a tag is authenticated, it is never re-identified. By the way, it takes too much time for authentication rather than the identification. These results tell us that the corrupted effect is much dominant in Rayleigh fading channel, an authentication is generally dropt while the tag can be authenticated in AWGN channel. Hence, it causes more authentication trials in fading channel. Furthermore, the numbers of the trials are also related the length of frames defined in the authentication protocol varied for costumer decisions (see customer request format, Figure 2.5).

The inventory process is another important parameter that should be considered to express this result. The anti-collision procedure isn't deterministic. This randomness may consume the tag time within the time interval in front of the reader, inside the reading range. Therefore, the identification number varies with respect to the reader's obtaining time of the tag ID list. This problem is overcome by increasing the trails. We run the simulation a hundred times with the same parameters and average the results.

The second graph, see Figure 2.14, shows the performance bounds of the protocol. In the Petra simulation environment, 25.4 tags are successfully authenticated among 28.1 identified tags. In the AWGN channel, 21 tags are also successfully authenticated among 31 identified tags; however, it is 16 in Rayleigh fading channel in 37 ones. The success ratio between two channels is more or less constant while the simulation time is gradually increasing. In fact, the exact performance will be between two bounds if the protocol is runnned in real-life environment.

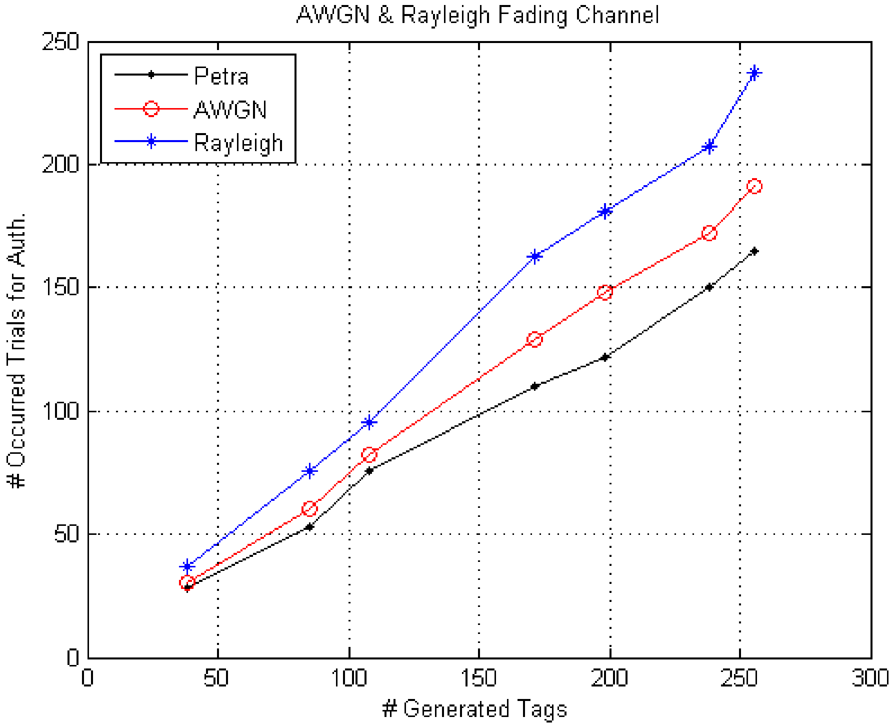


Figure 2.13: Num. of Occurred Trials for Auth. Vs. Num. of Generated Tags

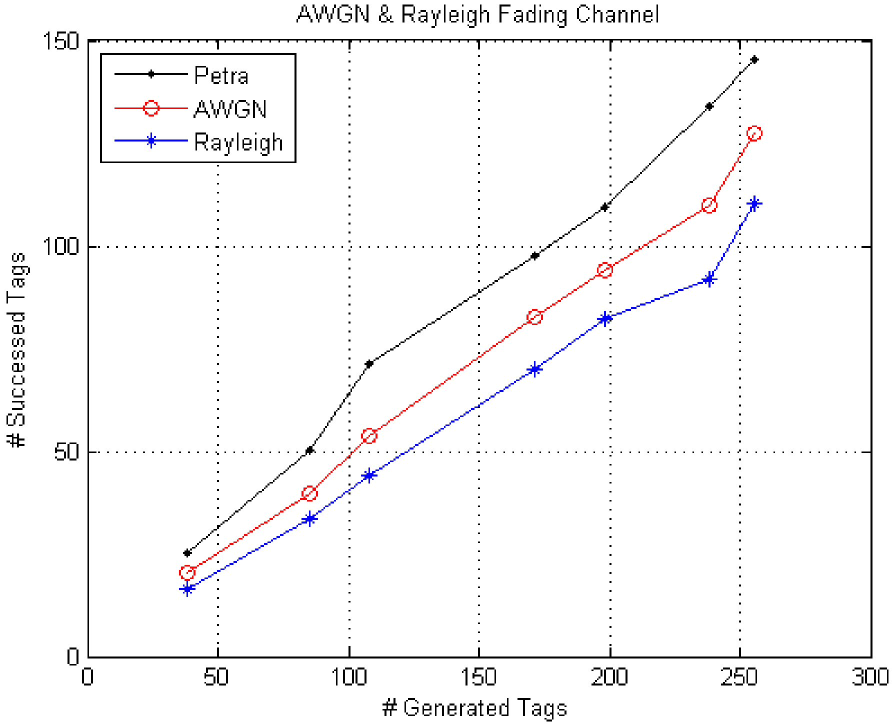


Figure 2.14: Num. of Successed Tags Vs. Num. of Generated Tags

The third graph, see Figure 2.15, shows that how much time is roughly passed for all authentications. There are more successful authentications take place in AWGN channel so much more time is consumed for the authentication procedures. But the most successful authentications are occured in the Petra simulation environmet. 25.4 tags are successfully authenticated in this environment and it takes 8.81 seconds. It can be clearly seen that authentication time is also linearly increasing with the number of authenticated tags.

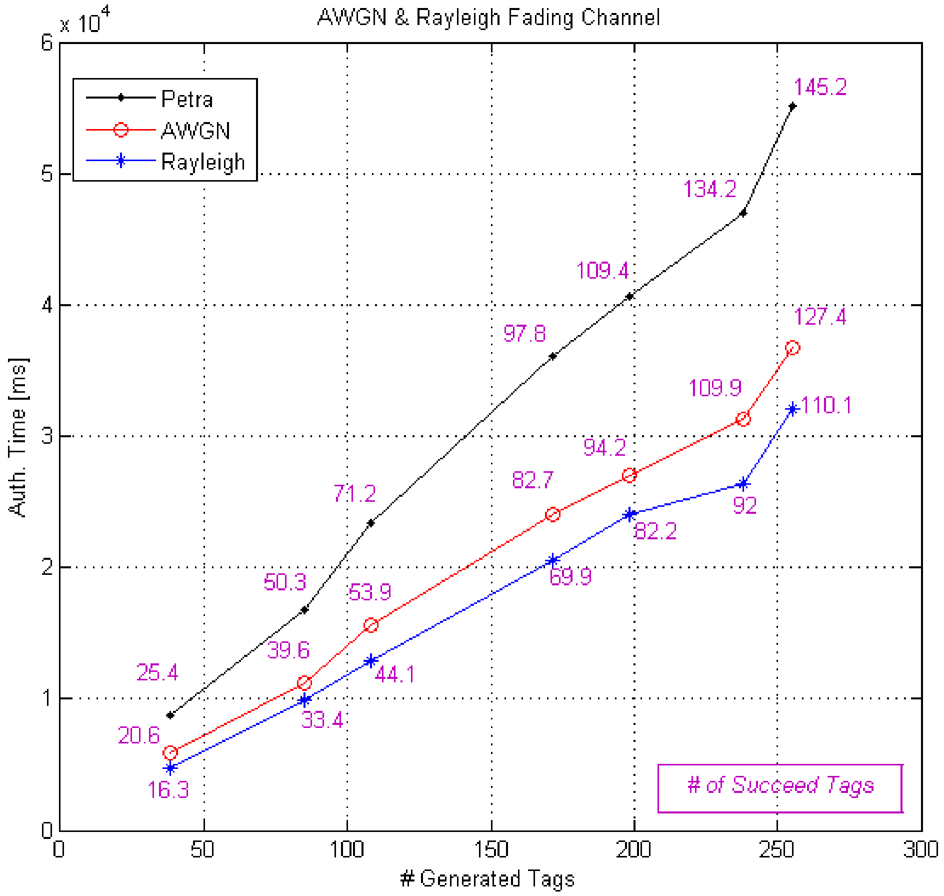


Figure 2.15: Authentication Time [ms] Vs. Num. of Generated Tags

3. PERFORMANCE IMPROVEMENT OF ACTIVE RFID SYSTEMS USING MULTIPLE-ANTENNAS WITH LIMITED FEEDBACK SCHEMES

Active RFID tags are preferred in many applications for their advantages: Visibility, security, quality and high distance communication. ISO/IEC 18000-7, operating at 433 MHz, is one of themost popular active RFID standards. We realize that a tag consumes too much energy source to perform a satisfactory communication compliance with the standard in Rayleigh fading channel. We aim to ameliorate a RFID system performance from the perspective of better communication and energy efficiency. Detailed and extensive simulations show that multiple-antenna designs at tag side using limited feedback schemes significantly decreases the frame error rates and increases the battery lifetime. High energy efficiency and effective communication in Rayleigh fading wireless channels can be reached by using limited feedback with multiple antennas at the tag side and both tag-reader side. We also make a detail comparison of different limited feedback schemes.

The remainder of this chapter is organized as follows. In Related Work Section, we briefly describe the system model. Then, we explain ISO/IEC 18000-7 standard. Later on, we talk about the limited feedback schemes. In Evaluation Section, we show the simulation results and evaluate the system performance. Lastly, we conclude the chapter and present our opinion for future work.

3.1 Related Works

Active RFID tags might be used to increase transmission distance in many applications for long range distance such as container identification and location estimation. However, the battery life is decreased by the active parts of the tag. Hence, it causes a trade-off between communication distance and power consumption. In addition to this, the increased transmission distance might also cause interference problem because a large number of tags or multi-reader multi-tag environment within the range of a reader grounds communication difficulties. The frames are also corrupted by fading because RFID systems at UHF and microwave frequency band are exposed to fading [31,32]. Coding schemes or multiple-antenna techniques can be solutions to overcome these troubles (see Figure 3.1).

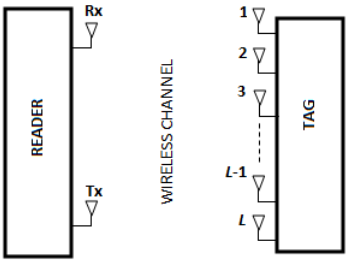


Figure 3.1: A Basic RFID System with Multiple-Antenna Tag

Griffin et al. model forward channel and backscatter channel as a cascaded channel for passive RFID systems [33]. They also show that these channels can be modeled by Rayleigh fading in a non-line-of-sight (NLOS) environment and analyze the performance effects of using multiple antennas at both reader and tag sides [34]. Using multiple antennas at the tag side or both tag and reader sides would ameliorate the system bit error rate (BER) performance without space-time coding is shown in [33,34]. He and Wang derive a close-form BER expression of non-coherent frequency shift keying (FSK) for passive RFID systems with using multiple antennas at the tag side in double Rayleigh Channel [35]. They show that RFID systems with multiple tag antennas causes a vital BER performance improvement without using space-time coding. Their simulation and analytical results present that almost 6 dB improvement in BER performance is provided by using two tag antennas.

3.2 ISO 18000-7 Standard

There are four available international standards for building active RFID systems: ISO/IEC 18000-7, IEEE 802.15.3 (or UWB), IEEE 802.11 (or WLAN or Wi-Fi), IEEE 802.15.4 (or WPAN, related to Zigbee). The ISO 18000-7 standard [4] is based on the Savi active RFID protocol, which was the first commercial active RFID system employed by the US military in the early 1990s [36].

ISO/IEC 18000 consits of 7 parts. The series from part-2 to part-7 is related to air interface communication parameters for different frequency bands. ISO/IEC 18000-7 standard was prepared by committee of ISO/IEC JTC-1 to address the air interface for an active RF tags at operating 433 MHz band in item management application. Later on, it is revised and the third edition cancels and replaces the second edition in 2008 [37]. An RF tag in this standard has its own on-board source. Hence, the communication may be started by tag or reader. The carrier frequency (fc) is 433,92 MHz with ±50kHz deviation. The transmitted signal is modulated by using FSK method. Data between two parties is transmitted in packet format by using Manchester coding. The data from reader-to-tag is sent by choosing one of two formats depending on the type of the message (frame or packet). The reader-to-tag message format is described in Table 3.1 and Table 3.2. There are two possible message response formats from the tag-to-reader. In the first response shown in Table 3.3, tags response to the reader's broadcast command within its reading range. The second one, shown in Table 3.4, is the response message format to the reader's point-to-point command.

Table 3.1: Interrogator-to-tag command format (broadcast)

Protocol ID	Frame Options	Frame Length	Session ID	Command Code	Command Arguments	CRC
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	*N* Bytes	2 Bytes

Table 3.2: Interrogator-to-tag command format (point-to-point)

Protocol ID	Frame Options	Frame Length	Tag Manufacturer ID	Tag Serial Number	Session ID	Command Code	Command Arguments	CRC
1 Byte	1 Byte	1 Byte	2 Bytes	1 Byte	2 Bytes	1 Byte	*N* Bytes	2 Bytes

Table 3.3: Tag-to-Reader Broadcast Response Message Format

Protocol ID	Tag Status	Frame Length	Session ID	Tag Manufacturer ID	Tag Serial Number	Command Code	Data	CRC
1 Byte	2 Bytes	1 Byte	2 Bytes	2 Bytes	4 Bytes	1 byte	*N* Bytes	2 Bytes

For broadcasting, the length of the reader message is 8+*N*. It is 13+*N* for point-to-point communication, where *N* denotes the length of the command arguments in bytes.

Table 3.4: Tag-to-Reader Response Message Format (point-to-point)

Protocol ID	Tag Status	Frame Length	Session ID	Tag Manufacturer ID	Tag Serial Number	Command Code	Response Data	CRC
1 Byte	2 Bytes	1 Byte	2 Bytes	2 Bytes	4 Bytes	1 byte	N Bytes	2 Bytes

Arguments are defined for some specific command. A command is not able to require a command argument. Hence, the minimum length of the frame in reader side is 8 bytes and the maximum length can possibly reach to 255 bytes. On the other hand, a tag can use a frame within a range from 20 bytes to 255 bytes as a response. Tags can prefer a different frame length but the length never exceeds the maximum frame length. In addition to this, the length of the frame determines the performance of an RFID system. When the length of a frame is increased, the frame error rate (FER) curves become worse. Hence, a healthy communication can not be provided and the system consumes the battery for another transmission.

In the study of wireless communications, path loss (or path attenuation) is one type of the large-scale fading effects [24]. This term is a decreasing the intensity of an electromagnetic wave while it propagates through space. The amplitude of a transmitted signal in a wireless channel over a short period time might be rapidly fluctuated [26]. This is called 'small-scale fading effect' of the channel. The transmitter transmits the signal but the signal might reach to the receiver in more than one path because of the channel characteristics. Hence, the receiver obtains the superposition of the multiple copies of the signal. These reflections are called multipath waves. Each multipath wave is exposed attenuation, phase shift and delay.

The theoretical bit error rate (BER) of single transmitting antenna at the tag and single receiving antenna at the reader (1Tx:1Rx) RFID systems for coherent FSK in Rayleigh channels is shown in Equation **3.1**. The Equation **3.2** formulates the FER with respect to the length of the frame, which is $M \times 8$ is the length of the frame, where M represents the number of bytes sent in the frame. This formulae says that the length of the frame is increased, the FER curves become worse shown in Table 3.5.

$$Pe = \frac{1}{2} erfc\left(\sqrt{SNR}\right) \qquad \textbf{(3.1)}$$

$$Pe_{(FER)} = 1 - (1 - Pe)^{M \times 8} \qquad \textbf{(3.2)}$$

In (1Tx:1Rx) RFID systems, the required Signal-Noise Ratio (SNR) for various FER values can be found in Table 3.5.

Table 3.5: Frame Error Rate Performance When Single Antenna Presents At The Tag

(FER)	Frame Length (20 Bytes)	Frame Length (255 Bytes)
FER=10^{-1}	25.80 dB	36.86 dB
FER=10^{-2}	36.00 dB	47.07 dB
FER=10^{-3}	46.00 dB	57.07 dB

3.3 Communication Setup

The RFID system model is similar to the He and Wang's model where the reader has one transmitting and one receiving antenna and the tag is equipped with L transmit antennas [35]. We can assume that all channels are frequency flat Rayleigh fading channel where channel gains are circularly complex Gaussian random variables and statistically independent from each other. The parameter h_i is the channel coefficient from the i^{th} antenna of the tag to the reader receiving antenna where $i = 1, 2, \dots, L$.

We also assume that the channels are quasi-static. That is to say, the fading coefficients remain constant over the duration of one frame. The reader is assumed to have perfect knowledge of its own channels with using a Protocol ID (see in Table 3.1) section of the tag response. The noise can be modeled as additive white Gaussian whose components are circular complex random variable(CCRV), has a probability distribution that is invariant under rotation in the complex plane, with zero-mean and variance σ^2. A single-dimensional complex random variable Z is called circular if for any angle ϕ both Z and $Ze^{j\phi}$, that is its rotation by angle ϕ, have the same probability distribution.

$$BER = Q\left(\sqrt{\frac{E_b}{N_0}}\right) \qquad \textbf{(3.3)}$$

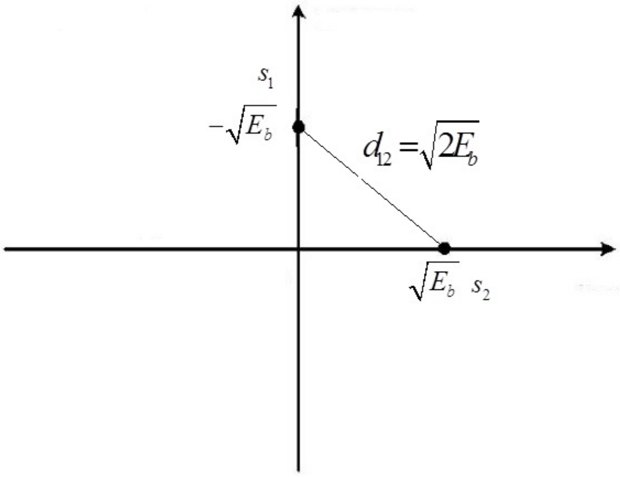


Figure 3.2: Signal Point for Binary Orthogonal FSK Signals

The tag transmits data bits with using frequency shift keying (FSK) modulation. Figure 3.2 shows the signal points for FSK signals. Consequently, the BER of FSK modulation is given in Equation **3.3** by using Equation **2.10**.

3.4 Channel Models

The wireless channel is considered non-frequency selective. Therefore, every instant channel realization is characterized by a single complex number in the SISO (**3.4**) setup, a row vector of complex numbers in the MISO (**3.5**) case, a column vector of complex numbers in the SIMO (**3.6**) case and a complex two-dimensional matrix for MIMO (**3.7**) considerations. In (**3.7**) the first index of the elements h_{ij} refers to the respective receive antenna, the second index identifies the associated transmit antenna.

$$\mathbf{h_{SISO}} = h \tag{3.4}$$

$$\mathbf{h_{MISO}} = \begin{pmatrix} h_1, & h_2, & h_3, & ,\ldots, & ,h_{N_t} \end{pmatrix} \tag{3.5}$$

$$\mathbf{h_{SIMO}} = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ \ldots \\ h_{N_t} \end{pmatrix} \tag{3.6}$$

$$\mathbf{h_{MIMO}} = \begin{pmatrix} h_{11}, & h_{12}, & h_{13}, & ,\ldots, & ,h_{N_{1t}} \\ h_{21}, & h_{22}, & h_{23}, & ,\ldots, & ,h_{N_{2t}} \\ h_{31}, & h_{32}, & h_{33}, & ,\ldots, & ,h_{N_{3t}} \\ & & \ldots & & \\ h_{N_r1}, & h_{N_r2}, & h_{N_r3}, & ,\ldots, & ,h_{N_rN_t} \end{pmatrix} \qquad \mathbf{(3.7)}$$

The time-dependent statistical properties are defined according to the block fading definition. Thus for M successive symbol cycles the instant channel realization, given by one of (Equation **3.4**) - (Equation **3.7**) is considered fixed. At block boundaries a completely new realization is randomly generated with no statistical relation to the previous channels. This model is also referred to as quasi-static [38]. The (pdfs) of the channel coefficients are kept constant over all blocks, i.e the same pdfs are realized for the whole duration of the transmission.

Our simulation includes several independent sub-simulations for different values of signal-to-noise ratio (SNR). At the end of each sub-simulation the average frame error ratio (FER) for the current SNR value is calculated by dividing the number of defected frames by the total number of transmitted frames. E_b references the average energy per transmitted bit, emitted by the sum of all active transmit antennas per discrete symbol cycle.

3.5 Limited Feedback Schemes

In this section, we explain the limited feedback methods with multiple antenna designs.

3.5.1 Trasmit antenna selection (TAS)

Multiple-antenna systems, known as multiple-input multiple-output, can enhance the capacity and reliability of RF communication. However, using the multiple antennas is costly in terms of size and power. Antenna selection is a low-cost low-complexity alternative to capture many of the advantages of MIMO systems [39]. Transmit antenna selection method needs a feedback path from the receiver to the transmitter. For single antenna selection, this feedback rate is rather small. The antenna is selected to obtain the highest equivalent receive SNR. Hence, little else need be talked about single transmit antenna selection.

Transmit antenna selection method needs a feedback path from the receiver to the transmitter. For single antenna selection, this feedback rate is rather small. The antenna is selected to obtain the highest equivalent receive SNR. Let we assume that there are N_t, which denotes the number of the selected antennas, $(L_t \geq N_t)$ antennas at the transmitter and one antenna at the receiver. L_t denotes number of the transmit antennas. Then we have to choose the most suitable N_t out of L_t antennas. We prefer the transmitting antennas that maximizes SNR when the superposition of their transmitted signals at the receiver. In this situation, we select the N_t transmit antennas with the highest channel gain. The subset, which consists of indices for selected transmit antennas, is denoted by S. For example, when all available transmit antennas are selected, we obtain $N_t = L_t$ and $S = 1, 2, ..., N_t$ [40].

There are several well-known limited feedback schemes in multiple-input multiple-output (MIMO) systems. One of the schemes is transmit antenna selection (TAS) which is an effective way to obtain good system performance with low complexity [40]. Using TAS, a single antenna or a subset of the antenna array is optimally selected for the transmitter.

In [41], space-time block coding with optimal antenna selection scheme which is called transmit antenna selection with Alamouti's scheme has been proposed. They keen on orthogonal space-time block coding (OSTBC),in particular, on the Alamouti code. They propose the algorithm for the case of joint antenna subset selection with fading. The antennas are picked out to minimize the instantaneous probability of error in the process with maximizing the received SNR. The transmit antenna selection with Alamouti's scheme selects highest channel gain pair out of L transmit antennas and transmits Alamouti's code. The mobile user needs $L(L\text{-}1)/2$ feedback bits $(L \geq 3)$. In the transmit antenna selection, the best of the transmit antennas is selected based on the channel state information (CSI) at the base station in order to minimize the instantaneous error probability. The mobile user needs ceil($log_2 L$) feedback bits $(L \geq 2)$ where the operator ceil$\{.\}$ rounds to the smallest integer greater than or equal to its argument.

3.5.2 Extended balanced space-time block codes scheme (EBSTBCs)

Orthogonal space time block codes (OSTBCs) is a member of the space-time coding scheme. Full diversity might be achieved with a low decoding coplexity by using OSTBCs. However, OSTBCs does not provide full diversity and full rate for more than two antennas. The extended balanced spacetime block codes (EBSTBCs) was proposed scheme in [42, 43]. In this scheme, an arbitrary numbers of codes can be produced for improved coding gain and all available transmit antennas are also employed to achieve full diversity and to maximize the coding gain.The symbol error rate (SER) and the bit error rate (BER) upper bounds for the EBSTBCs are also derived. Moreover, the performance of the EBSTBCs is investigated for both multi-input single output (MISO).

The extended balanced space time block codes (EBSTBCs) scheme can be attaained by multiplying the an OSTBC with a matrix [42]. We know that Alamouti's code is the only orthogonal code with rate one and minimum delay so the EBSTBCs can be obtained as an extension of the Alamoutis code [42] (Equation **3.8**).

$$\mathbf{C} = \mathbf{X}\mathbf{W} \tag{3.8}$$

Where **X** denotes the Alamouti's code and **W** denotes the $2 \times N$ matrix where $N \geq 2$ and the rank of **W** must be 2. The following example shows how to generate the EBSTBCs for three transmitters. Consider the EBSTBC pair with transmission matrix [42].

$$\mathbf{C} = \begin{pmatrix} s_1 & s_2 & as_2 \\ -s_2{}^* & s_1{}^* & as_1{}^* \end{pmatrix} \tag{3.9}$$

where $a = e^{j\pi m/q}$, q is the extention level and $m = 1, 2, \ldots q-1$ The columns and rows of C_1 denote symbols transmitted from three transmit antennas in two signalling intervals, respectively. C_1 is obtained from the Alamouti code using Equation **3.8** where

$$\mathbf{X} = \begin{pmatrix} s_1 & s_2 \\ -s_2{}^* & s_1{}^* \end{pmatrix} \tag{3.10}$$

$$\mathbf{W} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & a \end{pmatrix} \tag{3.11}$$

- **For three transmit antennas**

When three transmit antennas are at the transmitter, then, C_1, C_2 and C_3 are available EBSTBC matrices [42]. These matrixes are:

$$\mathbf{C_1} = \begin{pmatrix} s_1 & s_2 & as_2 \\ -s_2{}^* & s_1{}^* & as_1{}^* \end{pmatrix} \tag{3.12}$$

$$\mathbf{C_2} = \begin{pmatrix} s_1 & s_2 & as_1 \\ -s_2{}^* & s_1{}^* & -as_2{}^* \end{pmatrix} \tag{3.13}$$

$$\mathbf{C_3} = \begin{pmatrix} s_1 & as_1 & as_2 \\ -s_2{}^* & -as_2{}^* & s_1{}^* \end{pmatrix} \tag{3.14}$$

The EBSTBC C_j, $j = 1,2,3$, is selected to give the maximum coding gain and the feedback a. Two bits of feedback is needed to select the EBSTBC matrices and k bits of feedback is needed to select the feedback a where $k = \lceil dlog2 \rceil$ [42].

- **For four transmit antennas**

When four transmit antennas are present at the transmitter, then, seven different EBSTBC matrices can be obtained [42]. These matrices are

$$\mathbf{C_1} = \begin{pmatrix} s_1 & as_1 & bs_1 & s_2 \\ -s_2{}^* & -as_2{}^* & -bs_2{}^* & s_1{}^* \end{pmatrix} \tag{3.15}$$

$$\mathbf{C_2} = \begin{pmatrix} s_1 & as_1 & s_2 & bs_1 \\ -s_2{}^* & -as_2{}^* & -s_1{}^* & -bs_2{}^* \end{pmatrix} \tag{3.16}$$

$$\mathbf{C_3} = \begin{pmatrix} s_1 & s_2 & as_2 & bs_2 \\ -s_2{}^* & s_1{}^* & -as_2{}^* & -bs_2{}^* \end{pmatrix} \tag{3.17}$$

$$\mathbf{C_4} = \begin{pmatrix} s_1 & s_2 & as_2 & bs_2 \\ -s_2{}^* & s_1{}^* & as_1{}^* & bs_1{}^* \end{pmatrix} \tag{3.18}$$

$$\mathbf{C_5} = \begin{pmatrix} s_1 & as_1 & s_2 & bs_2 \\ -s_2{}^* & as_2{}^* & s_1{}^* & bs_1{}^* \end{pmatrix} \tag{3.19}$$

$$\mathbf{C_6} = \begin{pmatrix} s_1 & s_2 & as_1 & bs_2 \\ -s_2{}^* & s_1{}^* & -as_1{}^* & bs_1{}^* \end{pmatrix} \tag{3.20}$$

$$\mathbf{C_7} = \begin{pmatrix} s_1 & s_2 & as_2 & bs_1 \\ -s_2{}^* & s_1{}^* & as_1{}^* & -bs_1{}^* \end{pmatrix} \tag{3.21}$$

where $a = e^{j2\pi m/q}$ and $b = e^{j2\pi m/q}$.

The EBSTBC matrix C_j, $j = 1,2,\ldots,7$ is selected to give the maximum coding gain and the feedbacks a and ba. Three bits of feedback is needed to select the EBSTBC matrix and $2k$ bits of feedback is needed to select feedbacks a and ba.

3.5.3 Improved transmit scheme (ITS)

Another limited feedback method is an improved transmit scheme (ITS) which has been proposed in [44]. The ITS of the EBSTBC can be obtained as an extension of Alamouti's code first or second column. To obtain minimum decoding delay, the first column extension is selected. Since one of the path gain antenna does not contribute the coding gain, to maximize the received SNR of the EBSTBC, the ITS uses $L-1$ transmit antennas out of L transmit antennas and doubles the power of an antenna which maximizes the received SNR [44].

$$\mathbf{C_1} = \mathbf{X_1 W_1} \tag{3.22}$$

Here X_1 is the Alamouti's code first column and W_1 is the $1 \times L$ matrix. The following example shows how to generate the ITS of the EBSTBC for three transmit antennas. Consider the ITS of the EBSTBC pair with transmission matrix [44].

$$\mathbf{C_1} = \begin{pmatrix} s_1 & 0 & as_1 \\ -s_2{}^* & 0 & -as_2{}^* \end{pmatrix} \tag{3.23}$$

The columns and rows of C_1 denote symbols transmitted from first and third transmit antennas in two signaling intervals, respectively. X_1 is obtained from the Alamouti's code first column using Equation **3.23** where [44].

$$\mathbf{X_1} = \begin{pmatrix} s_1 \\ -s_2{}^* \end{pmatrix}, \quad \mathbf{W_1} = \begin{pmatrix} 1 & 0 & a \end{pmatrix} \tag{\textbf{3.24}}$$

The performance of the ITS approaches less than 1 dB to the ideal beamforming performance [44].

3.5.4 Beamforming (BF)

Beamforming (BF) needs ideal CSI at the base station and it requires unlimited feedback from the mobile user [45]. However, the bandwidth of the feedback channel is limited. In this case, the mobile user should quantize the CSI in the form of transmit beamforming vector and informs the base station through a low-rate, limited bandwidth feedback channel [46].

In [46], the authors also consider the problem of quantized beamforming for independent and identically distributed (i.i.d.) Rayleigh flat-fading channels when the transmitter has access to a low-bandwidth feedback channel from the receiver and the receiver employs maximum ratio combining (MRC). To support the limitations of the feedback channel, they assume the use of a codebook of possible beamforming vectors known to both the transmitter and receiver.

When the second row of Equation **3.23** is replaced by $[s2 \quad 0 \quad as2]$, then we obtain the Equation **3.25** [44].

$$\mathbf{C_1} = \begin{pmatrix} s_1 & 0 & as_1 \\ s_2 & 0 & as_2 \end{pmatrix} \tag{\textbf{3.25}}$$

The C_6 is equivalent to the code in (Equation **3.23**), in terms of error rate probability. Then, this is equivalent to choosing 2 antennas out of 3 transmit antennas, using beamforming with beamforming vector $[\sqrt{2} \quad a]$ and $[a \quad \sqrt{2}]$ [44].

The same reasoning applies to N antenna case: Choose the antenna with lowest gain, and do not transmit from that antenna. For the remaining $N-1$ antennas, choose the one with the highest gain, double its power and apply beamforming vector $[\sqrt{2} \quad a_1 \quad a_2 \quad a_3 \quad \dots \quad a_{N-2}]$ [44].

3.6 The Performance Evaluation For Multiple-Antenna At Tag Side

The frame error rates of the EBSTBC, the ITS, the transmit antenna selection (TAS *L*:1), and the transmit antenna selection with Alamouti (TAS *L*:2) are evaluated for FSK modulation by computer simulations. The wireless channel is already explained in Section 2. The frame length is either 20 bytes or 255 bytes. The reader checks cyclic redundancy check (CRC) of the frame and discards the frame if the received CRC in the frame does not match the calculated CRC. For comparison, FER curves of the Alamouti's code (2Tx:1Rx), single antenna at the tag (1Tx:1Rx) and ideal beamforming (Ideal BF) are also included in Figures 3.3-3.6

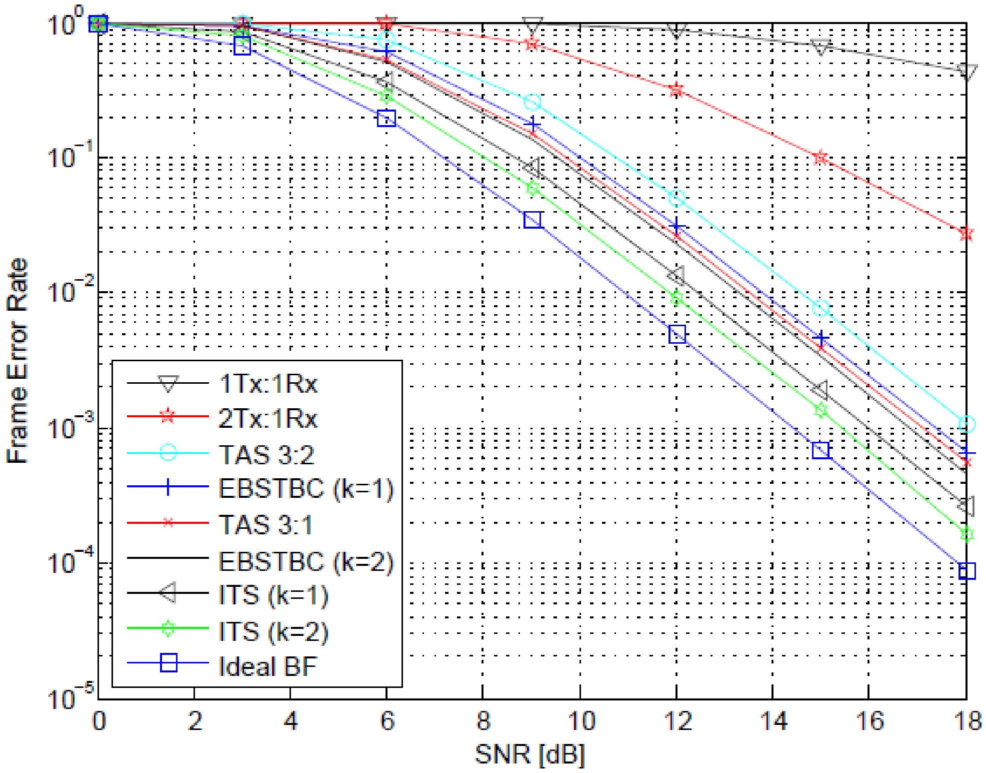


Figure 3.3: FER for three antennas at the tag and frame length is 20 bytes

Figure 3.3 presents frame error rates of the ITS with one bit extension of feedback (ITS (*k*=1)), the ITS with two bit extension of feedback (ITS (*k*=2)), the EBSTBC with one bit extension of feedback (EBSTBC (*k*=1)), the EBSTBC with two bit extension of feedback (EBSTBC (*k*=2)), the transmit antenna selection (TAS 3:1), the transmit antenna selection with Alamouti (TAS 3:2) when tag transmitted frame length is equal to 20 bytes and the tag is equipped with three transmit antennas. When 18 dB SNR is available, FER performances of the single antenna at the RFID tag (1Rx:1Tx), the

Alamouti's code (2Tx:1Rx) and the transmit antenna selection with Alamouti (TAS 3:2) yield 0.4352, 2.72×10^{-2} and 1.04×10^{-3}, respectively. For a FER value of 1×10^{-3}, the required SNR values can be found in Table 3.6. Compared to the single antenna at the tag (1Tx:1Rx), the ITS with two bit extension of feedback (ITS (k=2)) provides approximately 30.58 dB better performance. It is not only extensive amount of battery consumption but also diminishing interference at the wireless environment.

Figure 3.4 shows frame error rates of several limited feedback schemes when tag transmitted frame length is equal to 255 bytes and the tag is equipped with three transmit antennas. When 18 dB SNR is available FER performances of the single antenna at the RFID tag (1Rx:1Tx), the Alamouti's code (2Tx:1Rx) and the transmit antenna selection with Alamouti (TAS 3:2) yield 0.9994, 0.2968 and 1.32×10^{-2}, respectively. For a FER value of 1×10^{-2}, the required SNR values can be found in Table 3.6. Compared to the single antenna at the tag (1Tx:1Rx), the ITS with two bit extension of feedback (ITS(k=2)) provides approximately 31.31 dB better performance which is extensive amount of battery consumption at the tag.

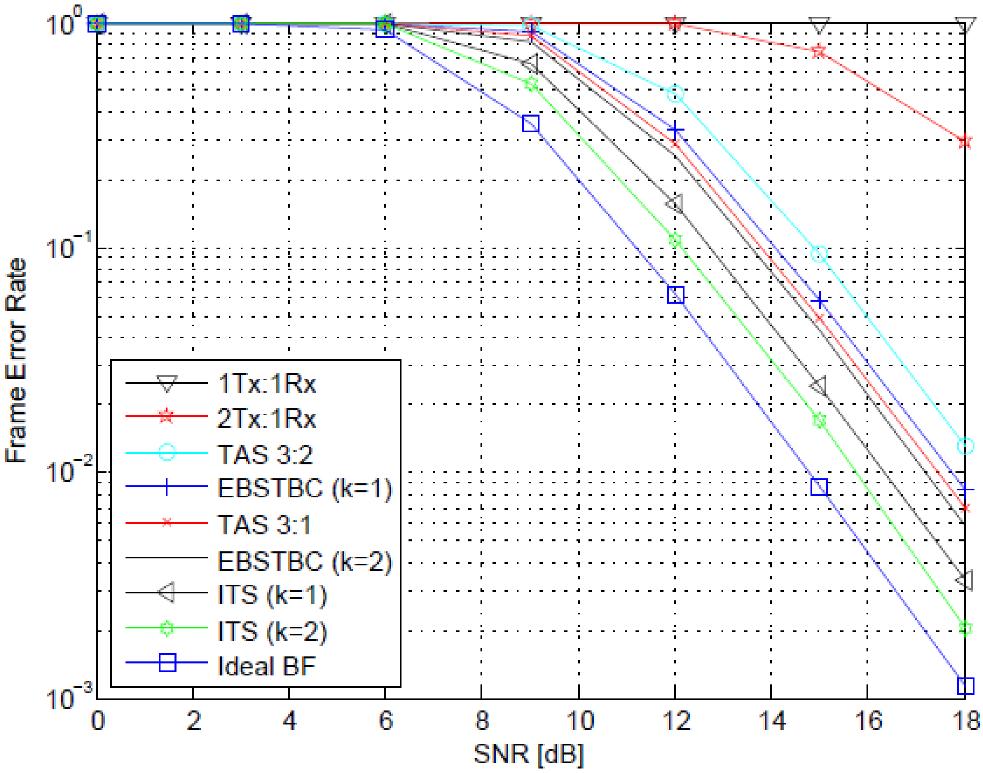


Figure 3.4: FER for three antennas at the tag and frame length is 255 bytes

Table 3.6: Frame Error Rate Performance When Three Antennas Present At The Tag

Limited Feedback Schemes	Frame Length=20 Bytes, FER=10^{-3}	Frame Length=255 Bytes, FER=10^{-2}
EBSTBC (*k*=1)	17.35 dB	17.71 dB
TAS 3:1	17.08 dB	17.44 dB
EBSTBC (*k*=2)	16.82 dB	17.17 dB
ITS (*k*=1)	15.98 dB	16.33 dB
ITS (*k*=2)	15.42 dB	15.76 dB
Ideal BF	14.44 dB	14.80 dB

Figure 3.5 presents the frame error rates of the ITS with one bit extension of feedback (ITS (*k*=1)), the ITS with two bit extension of the feedback (ITS (*k*=2)), the EBSTBC with one bit extension of feedback (EBSTBC (*k*=1)), the EBSTBC with two bit extension of the feedback (EBSTBC (*k*=2)), the transmit antenna selection (TAS 4:1), the transmit antenna selection with Alamouti (TAS 4:2) when tag transmitted frame length is equal to 20 bytes and the tag is equipped with four transmit antennas. When 15 dB SNR is available, FER performances of the single antenna at the RFID tag (1Rx:1Tx) and the Alamouti's code (2Tx:1Rx) yield 0.6766 and 9.88×10^{-2}, respectively. For a FER value of 1×10^{-3}, the required SNR values can be found in Table 3.7. Compared to the single antenna at the tag (1Tx:1Rx), the ITS with two bit extension of feedback (ITS (*k*=2)) provides approximately 34.79 dB better performance which is not only extensive amount of battery consumption but also diminishing interference at the wireless environment.

Table 3.7: Frame Error Rate Performance When Four Antennas Present At The Tag

Limited Feedback Schemes	Frame Length=20 Bytes, FER=10^{-3}	Frame Length=255 Bytes, FER=10^{-2}
TAS 4:2	14.68 dB	14.97 dB
TAS 4:1	13.94 dB	14.22 dB
EBSTBC (*k*=1)	13.56 dB	13.85 dB
EBSTBC (*k*=2)	12.66 dB	12.92 dB
ITS (*k*=1)	12.13 dB	12.42 dB
ITS (*k*=2)	11.21 dB	11.48 dB
Ideal BF	10.33 dB	10.62 dB

Figure 3.6 depicts frame error rates of several limited feedback schemes when tag transmitted frame length is equal to 255 bytes and the tag is equipped with four transmit

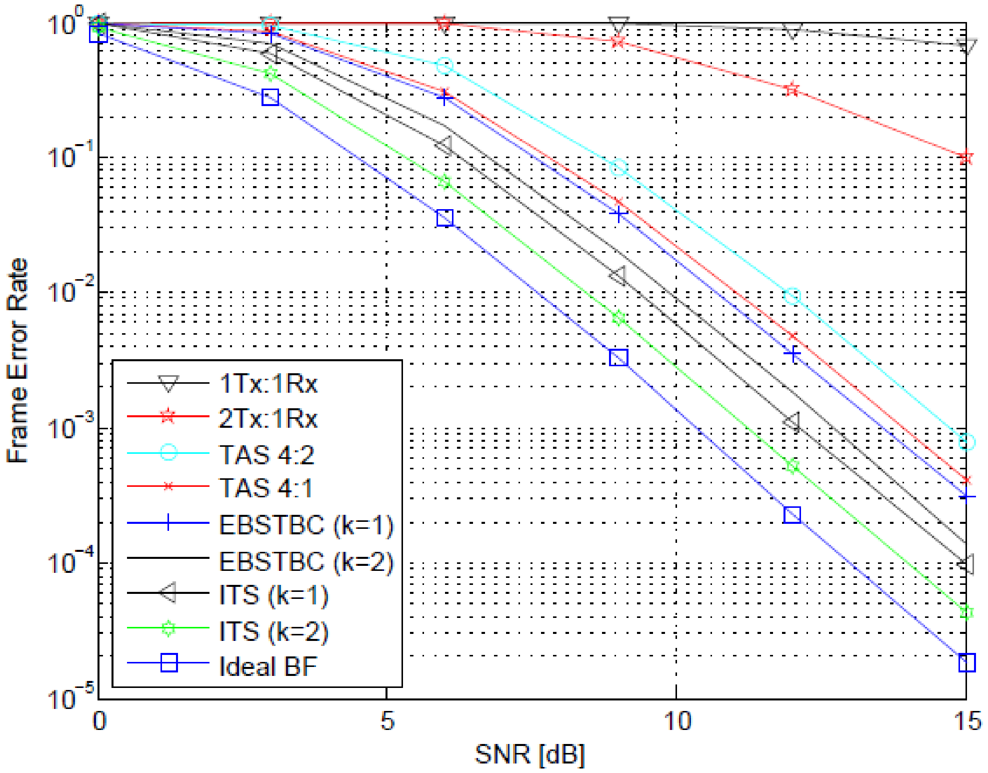


Figure 3.5: FER for four antennas at the tag and frame length is 20 bytes

antennas. When 15 dB SNR is available, FER performances of the single antenna at the RFID tag (1Rx:1Tx) and the Alamouti's code (2Tx:1Rx) yield 1 and 0.7341, respectively. The tag and the reader do not communicate. For a FER value of 1×10^{-2}, the required SNR values can be found in Table 3.7. Compared to the single antenna at the tag (1Tx:1Rx), the ITS with two bit extension of feedback (ITS (k=2)) provides approximately 35.59 dB better performance which is extensive amount of battery consumption at the tag.

3.7 The Performance Evaluation For Multiple-Antenna At Both Tag and Reader Side

Owing to insufficient antenna space and hardware limitations, the tag may not be equipped a higher number of transmit antennas. To improve the FER performance, the reader may be equipped more than one receive antenna. In the sequel, we assumed that the reader is equipped with two receive antennas. Figure 3.7- 3.8 show frame error rates for several limited feedback schemes when tag transmitted frame length is equal to 20 bytes and 255 bytes, respectively and the tag is equipped with three

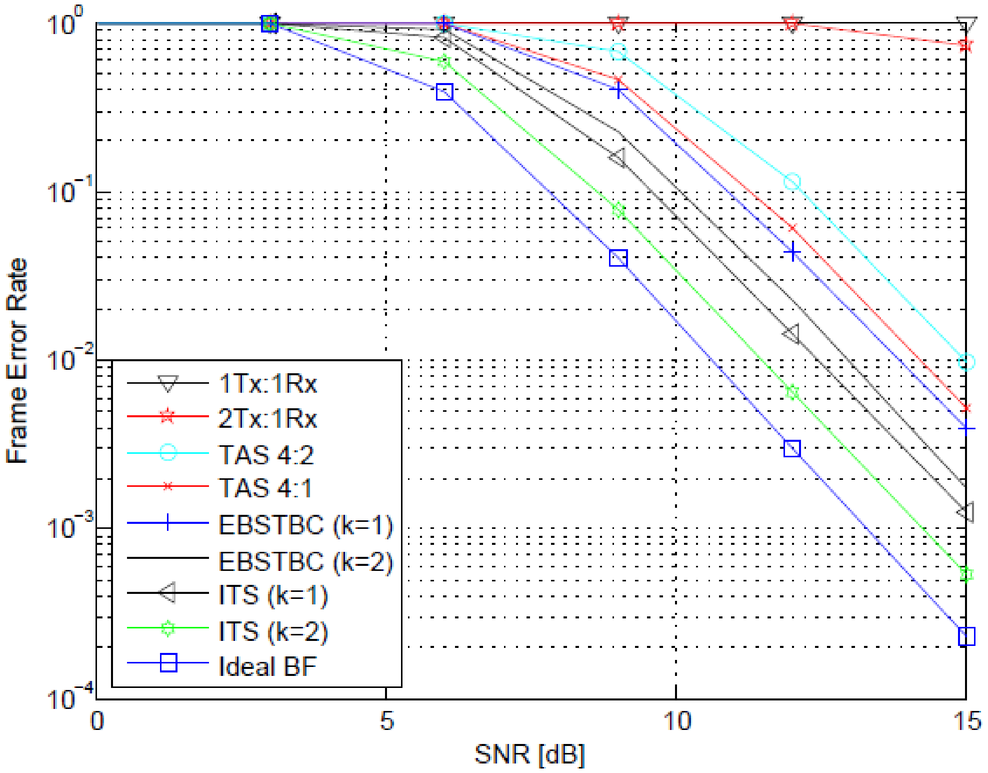


Figure 3.6: FER for four Antennas at the tag and frame length is 255 bytes

transmit antennas. For a FER value of 10^{-3}, the required SNR values can be found in Table 3.8.

Table 3.8: Frame Error Rate Performance When Three Antennas Present At The Tag and Two Receive Antennas Present At The Reader

Limited Feedback Schemes	Frame Length=20 Bytes, FER=10^{-3}	Frame Length=255 Bytes, FER=10^{-3}
TAS 3:2	11.94 dB	14.06 dB
EBSTBC (*k*=1)	11.74 dB	14.09 dB
EBSTBC (*k*=2)	10.82 dB	13.04 dB
TAS 3:1	10.74 dB	12.93 dB
ITS (*k*=1)	9.73 dB	12.00 dB
ITS (*k*=2)	9.17 dB	11.27 dB
Ideal BF	8.27 dB	10.50 dB

Compared to the single antenna at the tag and at the reader (1Tx:1Rx), the ITS with two bit extension of feedback (ITS (*k*=2)) provides approximately 36.83 dB and 45.8 dB better performance when frame length is equal to 20 bytes and 255 bytes, correspondingly.

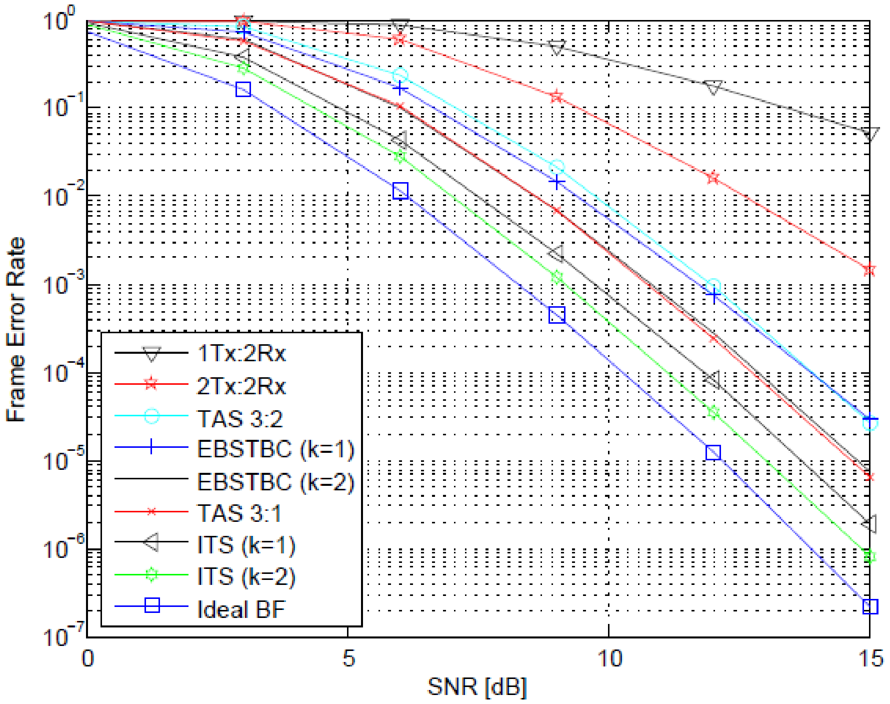


Figure 3.7: FER for three antennas at the tag and two receive antennas at the reader and frame length is 20 bytes.

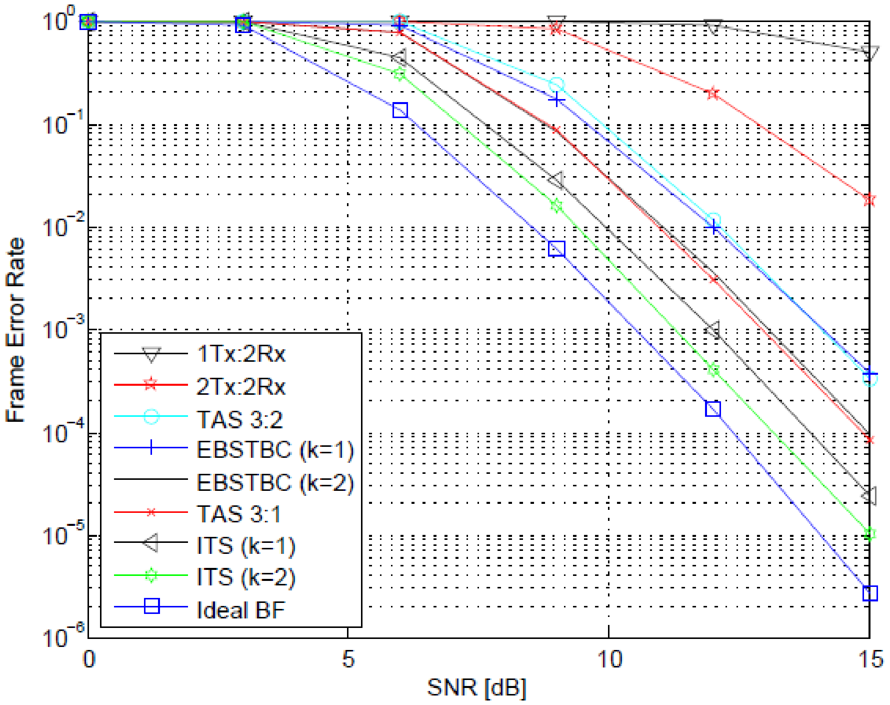


Figure 3.8: FER for three antennas at the tag and two receive antennas at the reader and frame length is 255 bytes.

4. CONCLUSION

We design a simulation environment of a passive RFID system complying with 18000-3 standard that may guide the protocol designers to test their protocols and see their RFID system performance before using them on real systems. We have some observations based on our simulation. In the Rayleigh fading channel, there are more tags are identified because the unauthenticated tags have a second chance for a new authentication so they are identified again and again. But if a tag is authenticated, it is never re-identified. By the way, it takes too much time for authentication rather than the identification. These results tell us that the corrupted effect is much dominant in Rayleigh fading channel, an authentication is generally dropt while the tag can be authenticated in AWGN channel. Hence, it causes more authentication trials in fading channel.

We also show that the simulation results match the theoritical calculations and expectations. RFID protocols perform best performance in AWGN channel. This performance gives us the upper bound performance because the AWGN channel is an ideal case in wireless communication environment. We added the results of Petra simulation environment to show the wireless channel effect. On the other hand, the performance of RFID protocols in Rayleigh fading channels gives the lower bound of the performance. The effects of the Rayleigh fading channel are extremely severe when it is compared to the AWGN channel. The FER curve is inversely linear proportional with the SNR for Rayleigh fading while it is exponentially decreasing for AWGN channel. It is difficult to achieve low FER at Rayleigh fading channels. The reason behind this result is quite clear. In Rayleigh fading channel, RFID tags cannot directly communicate with readers and multiple copies of the same signal are received by the receiver. In other words, the signal in the air is exposed to fading. Furthermore, FER curves show more realistic performance, compared to the BER curves because two parties communicate with each other with frame structures. In a nutshell, RFID system designers can easily use our simulation environment to test their desings before implementing an application on passive RFID systems.

Secondly, we examine the performance of active RFID systems for with ISO/IEC 18000-7 standard. We reformulate that the performance of an active RFID system compliance with ISO/IEC 18000-7 standard is improved by limited feedback methods. The tag is equipped with multiple-antennas and limited feedback is available from the reader to the tag. We also use multi-antenna designs for both tag and reader sides. It can be seen from our detailed simulations that limited feedback schemes yields more than 30 dB better performance with respect to the single antenna case. This improvement is not only extensive amount of battery consumption at the tag side but also diminishing interference at the wireless environment. Moreover, we assumed that channel gains are circularly complex Gaussian random variables and statistically independent from each other. Due to the tag's size, the channel gains may be correlated with the each other. We leave the performance of the multiple-antennas RFID tags with using limited feedback schemes in correlated channels as an interesting future work.

REFERENCES

[1] **Finkenzeller, K.**, (2003). RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, John Wiley & Sons, Inc., New York, NY, USA.

[2] **Garfinkel, S. and Rosenberg, B.**, (2005). RFID: Applications, Security, and Privacy, Addison-Wesley.

[3] **Tilborg, H.C.A.V.**, (2005). Encyclopedia of Cryptography and Security, Springer.

[4] **Menezes, A.**, **Oorschot, P.C.V. and Vanstone, S.A.**, (1996). Handbook of Applied Cryptography, CRC Press, Boca Raton, FL.

[5] **Juels, A.**, (2005). Minimalist Cryptography for Low-Cost RFID Tags, SCN, volume3352 of *Lecture Notes in Computer Science*, Springer, pp.149–164.

[6] **Henrici, D.**, (2008). RFID Security and Privacy: Concepts, Protocols, and Architectures, Springer–Verlag.

[7] **Deursen, T.V. and Radomirovic, S.**, (2008), Attacks on RFID Protocols, Cryptology ePrint Archive, Report 2008/310.

[8] **Ranasinghe, D.C. and Cole, P.H.**, (2008). Addressing Insecurities and Violations of Privacy , Networked RFID Systems and Lightweight Cryptography, Springer Berlin Heidelberg, pp.101–145.

[9] **Song, B. and Mitchell, C.J.**, (2008). RFID authentication protocol for low-cost tags, WiSec '08: Proceedings of the first ACM conference on Wireless network security, volume 0, ACM, pp.140–147.

[10] **Dimitriou, T.**, (2005). A Lightweight RFID Protocol to protect against Traceability and Cloning attacks, SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, IEEE Computer Society, Washington, DC, USA, pp.59–66.

[11] **Chien, H.Y. and Chen, C.H.**, (2007). Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards, *Comput. Stand. Interfaces*, **29(2)**, 254–259.

[12] **Weis, S.A.**, **Sarma, S.E.**, **Rivest, R.L. and Engels, D.W.**, (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, Security in Pervasive Computing, volume2802, Springer-Verlag, pp.201–212.

[13] **Kardaş, S.**, **Levi, A. and Murat, E.**, (2011). Providing Resistance against Server Information Leakage in RFID Systems, New Technologies, Mobility and Security – NTMS'11, IEEE, IEEE Computer Society, Paris, France, pp.1–7.

[14] **Fall, K. and Varadhan, K.**, (2009). The NS Manual, Notes and Documentation.

[15] **Zeng, X.**, **Bagrodia, R. and Gerla, M.**, (1998). GloMoSim: A Library for Parallel Simulation of Large-scale Wireless Networks, in Workshop on Parallel and Distributed Simulation, pp.154–161.

[16] **Kaparti, R.**, (n.d.). Opnet It Guru: A Tool For Networking Education.

[17] **Malhotra, R.**, **Gupta, V. and Bansal, D.R.K.**, (2011). Article: Simulation and Performance Analysis of Wired and Wireless Computer Networks, *International Journal of Computer Applications*, **14(7)**, 11–17, published by Foundation of Computer Science.

[18] **Balakrishnan, A.**, **Krishnan, S.**, **Advanced, C. and Banerjee, I.S.**, (n.d.), Abstract Simulation of RFID platform on NS-2.

[19] **Han, Y.**, **Li, Q. and Min, H.**, (2006), System Modelling and Simulation of RFID.

[20] **GuangXu**, (2007), Application Simulation Environment in SDR Workbench.

[21] **Floerkemeier, C. and Sarma, S.E.**, (2009). RFIDSim - A Physical and Logical Layer SimulationEngine for Passive RFID, *IEEE T. Automation Science and Engineering*, **6(1)**.

[22] **Dominikus, S. and Aigner, M.**, (2006). Petra Software Institute for Applied Information Processing and Communications (IAIK).

[23] **ISO/IEC Std. 18000-3**, (2004), RFID for item management -Air interface, Part 3: Parameters for Air interface communication at 13.56 MHz.

[24] **Sklar, B.**, (1997). Rayleigh Fading Channels In Mobile Digital Communication Systems. Part I: Characterization and Part II: Mitigation, *Communications Magazine, IEEE*, **35(7-9)**.

[25] **Rappaport, T.**, (2001). Wireless Communications: Principles and Practice, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2nd edition.

[26] **Sklar, B.**, (1997). Rayleigh Fading Channels In Mobile Digital Communication Systems. Part II: Mitigation, *IEEE Communications Magazine*, **35(9)**.

[27] **Weinrichter, H. and Hlawatsch, F.**, (1991). Stochastische Grundlagen Nachrichtentechnischer Signale, Springer.

[28] **John, P.**, (2000). Digital Communications, 4 edition.

[29] **ISO/IEC 15693**, (2000), Identification Cards Contactless Integrated Circuit(s) Cards, Proximity Cards.

[30] **ISO/IEC 14443**, (2000), Identification Cards Contactless Integrated Circuit(s) Cards, Proximity Cards.

[31] **Angerer, C.**, **Langwieser, R. and Rupp, M.**, (2010). Experimental Performance Evaluation of Dual Antenna Diversity Receivers for RFID Readers, La Manga del Mar Menor, Cartagena, Spain, pp.5–10.

[32] **Kim, D.**, **Jo, H.**, **Yoon, H.**, **Mun, C.**, **Jang, B. and Yook, J.**, (2010). Reverse-Link Interrogation Range of a UHF MIMO-RFID System in Nakagami-Fading Channels, *IEEE Transactions on Industrial Electronics*, **57(4)**, 1468–1477.

[33] **Griffin, J. and Durgin, G.**, (2010). Multipath Fading Measurements at 5.8 GHz for Backscatter Tags With Multiple Antennas, *Antennas and Propagation, IEEE Transactions on*, **58(11)**, 3693 – 3700.

[34] **Griffin, J. and Durgin, G.**, (2008). Gains For RF Tags Using Multiple Antennas, *Antennas and Propagation, IEEE Transactions on*, **56(2)**, 563 –570.

[35] **He, C. and Wang, Z.J.**, (2011). Closed-Form BER Analysis of Non-Coherent FSK in MISO Double Rayleigh Fading/RFID Channel, *IEEE Communications Letters*, **15(8)**, 848–850.

[36] **Amanna, A.**, **Agrawal, A. and Manteghi, M.**, (2010). Active RFID for Enhanced Railway Operations.

[37] **ISO/IEC Std. 18000-7**, (2008), Information Technology - RFID for Item Management-Part 7: Parameters for Air Interface Communication at 433 MHz.

[38] **Fuxjäger, P.**, (2004). Antenna Selection for MIMO Systems With Space-Time Coding.

[39] **Sanayei, S. and Nosratinia, A.**, (2004). Antenna Selection in MIMO Systems , volume 42, IEEE Press, Piscataway, NJ, USA, pp.68–73.

[40] **Park, C.S. and Lee, K.**, (2008). Statistical Multimode Transmit AntennaSselection for Limited Feedback MIMO Systems, *IEEE Transactions on Wireless Communications*, **7**, 4432–4438.

[41] **Gore, D. and Paulraj, A.**, (2002). MIMO Antenna Subset Selection With Space-Time Coding, *IEEE Transaction on Signal Processing*, **50**, 2580–2588.

[42] **Ekşim, A. and Çelebi, M.E.**, (2009). Extended Balanced Space-Time Block Coding for Wireless Communications, *IET Signal Processing*, **3**, 476–484.

[43] **Ekşim, A. and Çelebi, M.E.**, (2010). Performance Improvement of Binary Sensor Based Statistical STBC Cooperative Diversity Using Limited Feedback,, *IETE Technical Review*, **27**, 60–67.

[44] **Ekşim, A.**, (2012). Extended Balanced Space-Time Block Coding With Transmit Antenna Selection, *Transaction on Emerging Telecommunication Technologies*, **23**, 163–171.

[45] **Andersen, J.B.**, (2000). Antenna Arrays In Mobile Communications: Gain, Diversity, and Channel Capacity, volume 42, pp.12–16.

[46] **Love, D.J.**, **Member, S.**, **Heath, R.W. and Strohmer, T.**, (2003). Grassmannian Beamforming for Multiple-Input Multiple-Output Wireless Systems, *IEEE Trans. Inform. Theory*, **49**, 2735–2747.

CURRICULUM VITAE

Name Surname: Atakan ARSLAN

Place and Date of Birth: Eskisehir / 01.01.1986

E-Mail: atknarsln@gmail.com

B.Sc.: Anadolu University, Management, June 2012.

B.Sc.: Istanbul Technical University, Control Engineering, June 2008.

University of Sheffield, Control Engineering, 2005-2006.

List of Publications

- **Arslan A.** , Celik S., Kartal M.: The Performance Bounds Of Protocols In Wireless Channel For ISO 18000-3 Standard, *International Conference on Software, Telecommunications and Computer Networks-SoftCom2012*, September 2012
- Eksim A., **Arslan A.**, Celik S., Kartal M.: Performance Improvement of Multiple-Antenna RFID Tags Using Limited Feedback Schemes In ISO 18000-7 Standard, *International Conference on Software, Telecommunications and Computer Networks -SoftCom2012*, September 2012
- Gurel Ali., **Arslan Atakan**, Mete Akgun, 2010: None-Uniform Stepping Approach to RFID Distance Bounding Problem, *Data Privacy Management (DPM 2010)*, Lecture Notes in Computer Science, , pages 64-78, 2010. ©Springer Verlag.