ISTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

DESIGN AND IMPLEMENTATION OF A SECURE UHF RFID PROTOCOL ON FPGA

M.Sc. THESIS

Okan Emre ÖZEN

Department of Electronics and Communications Engineering

Electronics Engineering Programme

OCTOBER 2013

ISTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

DESIGN AND IMPLEMENTATION OF A SECURE UHF RFID PROTOCOL ON FPGA

M.Sc. THESIS

Okan Emre ÖZEN
(504111213)

Department of Electronics and Communications Engineering

Electronics Engineering Programme

Thesis Advisor: Dr. H. Bülent YAĞCI

OCTOBER 2013

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

GÜVENLİ BİR UHF RFID PROTOKOLÜNÜN FPGA ÜZERİNDE TASARIMI VE GERÇEKLENMESİ

YÜKSEK LİSANS TEZİ

Okan Emre ÖZEN
(504111213)

Elektronik ve Haberleşme Mühendisliği Bölümü

Elektronik Mühendisliği Programı

Tez Danışmanı: Dr. H. Bülent YAĞCI

EKİM 2013

Okan Emre ÖZEN, a M.Sc. student of ITU Institute of Science and Technology 504111213 successfully defended the thesis entitled **"DESIGN AND IMPLEMENTATION OF A SECURE UHF RFID PROTOCOL ON FPGA"**, which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Dr. H. Bülent YAĞCI** Istanbul Technical University	.....
Jury Members :	**Dr. H. Bülent YAĞCI** Istanbul Technical University	.....
	Assoc. Prof. Dr. S. Berna Örs YALÇIN Istanbul Technical University	.....
	Prof. Dr. Osman Nuri UÇAN Istanbul Aydın University	.....

Date of Submission : **17 September 2013**
Date of Defense : **4 October 2013**

To my family,

FOREWORD

I would like to specially thank to my advisor professor Bülent Yağcı for his contributions to my professional and academic career and moral and material support in last two years. Moreover it would be very shame on me if I would not thank to my project advisor Berna Ors Yalcin, who has always trusted in my efforts and has been patient for the outputs of such a hard work.

Furthermore, thanks to my father and mother for their support in the duration of my master studies, to my sister who has always been the source of energy for me. Lastly, I would like to specially thank to Giedre Gaidelyte, for her greater and forever support!

October 2013 Okan Emre ÖZEN

TABLE OF CONTENTS

Page

ABBREVIATIONS

CDMA : Code Division Multiple Access
EDK : Embedded Development Kit
DOS : Denial of Service
FET : Field Effect Transistor
FSK : Frequency Shift Keying
GFSK : Gaussian Frequency Shift Keying
GHz : Gigahertz
HF : High Frequency
kHz : Kilohertz
LF : Low Frequency
MHz : Megahertz
NFC : Near Field Communication
OOK : On-Off Keying
PSK : Phase Shift Keyingg
QAM : Quadrature Amplitude Modulation
RF : Radio Frequency
RFID : Radio Frequency Identification
SDK : Software Development Kit
SNR : Signal to Noise Ratio
SPI : Serial Peripheral Interface
TEA : Tiny Encryption Algorithm
UHF : Ultra High Frequency
VHF : Very High Frequency

LIST OF TABLES

Page

LIST OF FIGURES

Page

DESIGN AND IMPLEMENTATION OF A SECURE UHF RFID PROTOCOL ON FPGA

SUMMARY

Latest technological improvements led to increase in production of numerous different products and applications in different stages of daily life. As a these products and applications became industrial, the number of users has increased and feasibility of operations became harder. In order to prevent failure of these systems due to high number of users, identification systems are developed as a solution in order to determine an optimum quiescent point for operations considering number of users and efficiency. The use of Radio Frequency Identification System (RFID), which is one of mentioned identification systems, is scaling up day by day as a result of ease of applicability and efficiency.

RFID technology is involved in many different systems and applications nowadays. Since RFID systems give chance for user processes to be completed rapidly, they are applied for many different purposes such as toll collection systems in highways, card readers in public transportation vehicles, product bar-codes in shops, patient follow-up in hospitals, container follow-up in ships and etc.

RFID systems are composed of reader and tag structures. Considering the tag architectures, RFID systems might be examined in three different categories as passive, semi-active and active systems [4]. In passive systems, the tag is not supplied. DC supply is provided by incoming RF signals. Tag powers up and responds when it is in the range of the reader, but can not start communication with the reader by itself. In semi active systems, both the reader and the tag are supplied. Communication between the tag and reader is controlled by reader as in passive systems. The advantages of the semi active systems over passive systems is higher range. In active systems reader and tag are supplied and both have ability to start communication between.

While RFID systems increase efficiency of applications, they lead to an important problem, user security [5].Security gaps that might occur in use of RFID systems may lead to undesired disclosure of identity ofindividual users, inadvertent access to databases of companies and organizations that may result in capture of important data by undesired third-party individuals or companies and financial losses. Accordingly, security has gained more important in RFID technology and design of secure RFID systems came into prominence.

Under consideration of above mentioned facts, design and implementation of a secure UHF RFID system was accomplished in first phase of the thesis, by proposing new reader and transponder hardware. Active tag architecture was preferred in system design to keep the communication range long and security level high. 868 MHz center frequency is selected for system operation considering European UHF band

RFID regulations defined by European Telecommunication Standards Institute (ETSI). RFM22B transceiver modules were decided on and used for RF front-end stages of reader and tag taking into low power consumption and flexible operating features. FPGA boards formed up microcontroller part of designed reader and tag to keep the computational power substantially high. A communication protocol with two way authentication mechanism was used between receiver and transmitter devices. Tiny Encryption Algorithm was preferred in the design to secure the transmitted data. As a result, a secure RFID system with 64 byte authentication procedure was implemented.

In second part, attack studies were held on designed system. The aim of the attacks were to impersonate the original tag with an attack device and convince the reader that original tag is in range of communication. To accomplish replay attacks, an attack device similar to the reader and tag architecture, was designed and prepared for operation. Firstly, reader and tag data was listened by attack device and sent to a personal computer for storage over serial communication link. Later on, stored data is replayed back to the reader when the original tag was out of communication range.

GÜVENLİ BİR UHF RFID PROTOKOLÜNÜN FPGA ÜZERİNDE TASARIMI VE GERÇEKLENMESİ

ÖZET

Teknolojinin son yıllardaki hızlı gelişimi birçok ürün ve uygulamanın kullanımını büyük ölçüde arttırmıştır. Kullanıcı sayısındaki artışa bağlı olarak da çalışmaların uygulanabilirliği daha zor kontrol edilebilir hale gelmiş ve kısıtlanmıştır. Sistemler için kullanıcı sayısı ve etkinlik arasında optimum bir çalışma noktası için ise belirli Kimlik Belirleme Sistemleri geliştirilmiştir. Bu sistemlerden biri olan Radyo Frekansı ile Kimlik Belirleme (RFID) teknolojisinin kullanım alanları da kolay uygulanabilen ve etkin bir sistem olmasından dolayı gün geçtikçe artmaktadır. Söz konusu sistemler kullanıcı işlemlerinin hızlı bir şekilde gerçekleştirilmesine olanak sağladıkları için günümüzde otoyollardaki ücret ödeme noktaları, toplu taşıma araçlarındaki kart okuyucular, giyim mağazalarında ürün barkodları, hastahanelerde hasta takibi, gemilerde konteyner takibi gibi birçok farklı uygulamada kullanılmaktadır.

RFID sistemlerinin kullanımı uygulamaların etkinliğini arttırırken kullanıcı güvenliği gibi önemli bir sorunu da beraberinde getirmektedir [2]. RFID sistemlerinin kullanılması sırasında oluşabilecek güvenlik açıkları, bireysel kullanıcıların kimlik bilgilerinin açığa çıkması, kurumsal kullanıcıların veritabanlarına erişilmesi sonucu önemli bilgilerin istenmeyen kişi ve kurumların eline geçmesi, finansal verilerde yapılabilecek değişikler sonrası maddi kayıplar oluşması gibi önemli sonuçlara yol açabilir [6]. Bu nedenle güveli RFID sistemlerinin tasarımı büyük önem kazanmıştır.

RFID sistemleri, birçok tasarım parametresine sahip olmalarından dolayı değişik açılardan incelenebilirler. Çalışma frekansı, haberleşme mesafesi, güvenlik gereksinimleri, ve bellek kapasitesi RFID sistem tasarımında en önemli parametrelerdir. Çalışma frekansı seçiminde birtakım kıstaslar söz konusudur. Near Field Communication (NFC) aygıtları LF ve HF gibi düşük frekans bantlarında çalışırken uzak alan bazlı sistemler daha yüksek frekanslarda çalışır. Bununla birlikte, frekans standardizasyonu da çalışma frekansının belirlenmesinde etkilidir. Haberleşme mesafesi, güvenlik gereksinimleri ve bellek kapasitesi daha çok uygulamaya özel parametrelerdir. Eğer uygulama sırasındaki okuyucu-etiket mesafesi yüksekse, sistem tasarımı buna uygun olarak yapılmalıdır. Tam tersi bir durumda da sistem maliyetini arttıracak donanımın kullanılmasından kaçınılmalıdır. Güvenlik gereksinimleri aynı zamanda gerek duyulan bellek kapasitesini etkilemektedir. Yüksek güvenlik gerektiren bir uygulamada daha geniş bellek alanına ihtiyaç duyulmaktadır.

Bir RFID sistemi okuyucu, etiket ve veritabanından oluşur. Etiketler pasif, yarı-aktif ya da aktif olarak 3 farklı gruba ayrılır. Bir etiketin aktif ya da pasif yapısı güç besleme tekniğine göre belirlenir. Pasif etiketlerde dahili bir güç kaynağı bulunmaz. Okuyucu tarafından gönderilen AC işaretler DC'ye çevrilir ve etiket içerisindeki çipin beslemesinde kullanılır. Bununla birlikte, aktif etiketlerde dahili bir güç kaynağı

bulunur ve etiket sürekli olarak aktif durumda tutulur. Bir etiketin aktif ya da pasif yapısı, sistemin haberleşme mesafesi ile birlikte güvenlik seviviyesine de etki eder. Aktif sistemlerde haberleşme mesafesi ve güvenlik seviyesi pasif sistemlere göre daha yüksektir.

IDTechEx tarafından yapılan bir pazar araştırmasına göre, 2011 yılında 6.51 trilyon $ olan pazar payı 2012 yılında 7.67 trilyon $'a yükselmiştir. Buna göre, RFID, radyo teknolojileri arasında en hızlı gelişen sektör haline gelmiştir. RFID sistemlerinin dünya genelindeki kullanım oranına bakılırsa, yüksek ve hızla artan pazar değerinin şaşırtıcı olmadığı görülmektedir. RFID teknolojisi dünya üzerindeki birçok şirket ve organizasyon tarafından stok ve tedarik zinciri, otomatik geçiş sistemleri, fatura ödeme, yolcu takip sistemleri gibi birçok alanda artan bir oranla kullanılmaktadır.

RFID teknolojisinin çok farklı alanlarda uygulanabilirliğe sahip olması ve kullanılması sonucu Güvenlik ve Gizlilik son zamanlarda tartışılan konular haline gelmiştir. Bazı durumlarda etiketler, ait oldukları kişi veya eşyalar hakkında önemli bilgi taşımaktadırlar. Çoğu uygulamada etiketlerin doğrulama olmadan okuyuculara cevap vermesi sonucu RFID etiketlerin taşıdığı bilgiler istenmeyen kişilerin eline geçebilir ve bilgi sızımı gerçekleşebilir. Bu durumda, etiketleri taşıyan kişiler ya da sistemler takip etme ve gizlilik ataklarına karşı korumasız hale gelmiş olurlar. Bu nedenle, bazı kuruluş ve organizasyonlar RFID teknolojisinin endüstriyel anlamda kullanımına karşı çıkmaktadır. Yarıiletken üreticisi Philips 2003 yılında Benetton firması için RFID etiketler üretimine başladığını bildirmişti. Bu durum tüketici gizliliğine önem veren kuruluş ve organizasyonlar tarafından öğrenildiğinde Benetton firmasına karşı bir boykot eylemi başlatıldı ve eylemin yayılımını arttırmak için www.boycottbenetton.com adında bir websitesi açıldı. Sonraki zamanlarda Metro, Tesco, Gillette gibi ürünlerine RFID etiketler yerleştirmek isteyen firmalara karşı da benzer protestolar yapıldı.

Tartışmalar değerlendirildiğinde güvenli bir RFID haberleşmesinin önemli bir sorun olduğu açıkca görülmektedir. Geçmişte, istenmeyen 3.şahıslar tarafından yapılan ataklara karşı sistem güvenliğinin arttırılması amacıyla bazı çalışmalar yapılmıştır. 2005 yılında, bir grup Japon araştırmacı yeniden şifreleme yöntemini kullanarak etiket kimliğini değişken hale getirerek takip etme ataklarına karşı güvenilir bir etiket tasarımı gerçekleştirmiştir. Başka bir çalışmada, okuyucu ve etiket veri çerçeve yapılarına zaman bilgisinin eklenmesiyle Ortadaki Adam ve Yeniden Oynatma ataklarına karşı güçlü bir kimlik doğrulama protokolü geliştirilmiştir.

Bazı araştırma grupları etiket ve okuyucu arasındaki kimlik doğrulama protokollerine odaklanırken, kripto algoritmaları üzerine de önemli miktarda çalışma yapılmaktaydı. Israena, 2006 yılında Tiny Encryption Algorithm ve bu algoritmanın RFID sistemlerdeki uygulamaları üzerine önemli bir çalışma gerçekleştirdi. Araştırmacı, TEA algoritmasının RFID sistemlerdeki avantaj ve dezavantajlarını 3 farklı yöntem kullanarak ortaya koydu. Sonuçlara göre, algoritmanın paralel mimari kullanılarak uygulanması karmaşık bir doğrulama algoritması 0.21mm2lik bir alanda tasarlanabilmiş ve güç tüketimi 7.37uW olarak belirlenmiştir. Wang tarafından yürütülen bir başka çalışmada ise asimetrik anahtar kullanana Tame Transformation Signatures ile yeni bir kimlik doğrulama sistemi geliştirilmiştir.

Bu tezin ilk aşamasında, yeni okuyucu ve etiket yapılarının geliştirilmesinin ardından güvenli bir UHF RFID sisteminin FPGA üzerinde tasarımı yapılmış ve gerçeklenmiştir. Haberleşme mesafesini geniş ve güvenlik seviyesini yüksek tutmak amacıyla sistem tasarımında aktif etiket yapısı kullanılmıştır. Avrupa UHF RFID standartları göz önüne alınarak merkez frekansı 868MHz olarak belirlenmiştir. Düşük güç tüketimi ve ayarlanabilir çalışma noktası özelliklerine bağlı olarak Okuyucu ve etiket yapılarının alıcı verici katlarında RFM22B modülleri kullanılmıştır. İşlem kapasitesinin yüksek tutulması amacıyla mikroişlemci katında FPGA kitleri kullanılmıştır. Haberleşme protokolünde 2 yönlü doğrulama yapan bir protokol tercih edilmiştir. İletilen verinin kritografik olarak şifrelenmesi Tiny Encryption Algorithm ile gerçekleştirilmiştir. Sonuç olarak 64 bit veri ile kimlik doğrulama işlemi gerçekleştiren bir RFID sistemi başarıyla gerçeklenmiştir.

Tezin ikinci aşamasında okuyucuya karşı "yeniden oynatma" atakları yapılmıştır. Bu ataklar ile asıl etiketin yerine geçilerek okuyucunun gerçek etiket ile haberleştiğine inandırılması amaçlanmıştır. Bu amaçla, daha önceden tasarlanan okuyucu ve etiket yapılarına benzer bir atak birimi tasarlanmış ve öncelikli olarak okuyucu-etiket arasındaki haberleşme 1000 defa dinlenmiştir. Dinleme sonucu elde edilen verilen bilgisayar ortamında saklanmıştır. Sonrasında, asıl etiketin aktif olmadığı durumda, atak birimi okuyucudan gelen veriyi daha önceden kaydedilen veriyle karşılaştırmış ve eşleşme olduğu takdirde bahsedilen okuyucu verisine cevap olan etiket verisini okuyucuya geri göndermiştir. Sonuç olarak tasarlanan RFID sisteminin yeniden oynatma ataklarına karşı güvenilirliği arttırılmıştır.

1. INTRODUCTION

In recent years automatic identification procedures (Auto-ID) has taken great attention of manufacturers in industry due to great advantages and easiness they provide in production, distribution and marketing of goods [4]. Generally, Auto-ID systems duty is to provide information about an item in manufacture or goods in transit. However, these systems might also be used for tracking and identifying vehicles, animals, or individuals.

Nowadays there are several different identification systems used in applications. Bar-coding technology has taken the lead after the invention of identification systems since they are very cheap [4]. However the low data storage capacity distracted the designers to find a new solution. Storing the data on a silicon chip while keeping the design cost at low levels is the main idea behind the evaluation of smart cards [4]. Smart cards provide a lot more data storage possibility compared to bar-code labels. Yet smart cards are unable to meet the requirements of all applications because of their short communication range and impractical mechanical structures. Considering mentioned systems and deficiencies, Radio Frequency Identification (RFID) systems came into prominence as a solution due to possibility of long range communication and ease of manufacture.

RFID systems might be investigated in many different aspects [4]. Operating frequency, communication range, security requirements and memory capacity are most important criterions in RFID system design. Several issues are involved in choosing frequency of operation. Near Field Communication (NFC) devices operate at low frequency levels, in Low Frequency and High Frequency bands, while far field devices operate at higher frequency bands due. Moreover, governmental frequency allocations are effective on the selection of frequency. Communication range, security requirements and memory capacity are much more application specific criterions. To give example, if the distance between reader and tag is far in the application, system

is built-up to be a long range communication system or vice-versa. Besides, security requirements of an rfid baggage handling systems of an airport and rfid credit card are not same as well as required memory capacity.

An RFID system consists of a reader and a tag. Tags are classified into three different groups as active, semi-active or passive. The term active or passive is defined according to the power supply technique of the tag. Passive tags do not have an internal power source. Received reader signals are rectified and used to supply the tag chip. Active tags have an internal power source and the energy is used to keep tag chip powered on all the time. Active or passive structure of tag determines the communication range of the system as well as the security level. Active systems provide longer range and higher security as a result of higher power consumption while passive systems are insufficient in both compared to active systems.

As mentioned above, many features and capabilities of RFID technology makes itself stand out as the best identification system solution among all, resulting in high user numbers. An RFID market research from IDTechEx claims that in 2012 the value of the entire RFID market has raised to $ 7.67 billion, up from $6.51 billion in 2011. The RFID market therefore belongs to the fastest growing sector of the radio technology industry, including mobile phones and cordless telephones [7]. Higher market share is not surprising considering the use of RFID systems used in many identification systems all over the world. RFID technology is preferred by numerous companies and organizations for stock and supply chain management, vehicle tracking, shipment tracking, patient follow-up, book and document tracking, toll collection, bill payment, passenger follow up purposes and etc.

1.1 Purpose of Thesis

Security, privacy and tracking in RFID has become hot issues recently as a result of such a wide application spectrum of the technology [5]. Leakage of information is a problem that occurs when data sent by tags reveals sensitive information about the labeled items. In some cases RFID tags carry information about the objects they are implemented on and usually, readers are not authenticated and tags answer in a transparent and indiscriminate way. In this case, people carrying objects with RFID

tags are vulnerable to tracking and privacy attacks. An attacker can easily find out by reading the tags on a person's clothes where she is shopping, or what kind of medicines she uses and what kind of illnesses she has, where she lives, what her identity number is, how much money she has and etc. In such a situation, personal privacy rights are considered to be easily violated. Hence, some groups and organizations protest against use of RFID technology in industry. In 2003, semiconductor manufacturer Philips announced that it would supply RFID tags to clothing manufacturer Benetton [5]. When privacy advocates and organizations heard about the act, they called for a boycott of Benetton and they even set up a web page (www.boycottbenetton.com) to inform people about the boycott [5]. Similar acts were observed against Metro, Tesco, Gillette in the past as they wanted to apply RFID tags in manufactured goods.

Considering the arguments, securing the communication in RFID stands to be a problem of high importance. In first stage of this thesis, implementation of a secure RFID protocol was carried out. To decide the communication frequency, RFID frequency standards were researched firstly. 869MHz UHF communication for active RFID tags used in Europe was defined as the operating frequency. Then reader and tag stages were implemented and RF interface was completed. Following, Tiny Encryption Algorithm (TEA) was implemented on back-end stage to take encryption precautions and secure the data [8]. As a result design and implementation of a secure RFID protocol is completed.

In the second stage, replay attacks were carried out on reader. By replay attacks, it was aimed to take place of the original tag and convince the reader that original tag is in communication range. For this purpose, an attacker device, which was similar to reader and tag stages, was designed and the communication between reader and original tag was listened. 1000 sample data were recorded for both 176 bit reader data and 168 bit tag response. Later on when the original tag was out of communication range, the attacker device was used to analyze the data sent by the reader, find the proper answer from the sample list and replay the proper answer. Lastly, some precautions were suggested against replay attacks.

1.2 Related Work

To increase security against attacks by third party people and implement secure RFID protocols, many different studies have been completed in the past. Qualified literature research were expressed in [9] and [1]. Hash-lock scheme, randomized hash-lock scheme and hash chain schemes were developed as early solutions to security problems [9]. However, these schemes were vulnerable to tracking, replay and denial of service attacks. Besides, computational cost of of randomized hash lock scheme was high. Another proposed solution was challenge-response protocols with symmetric key encryption schemes. Unfortunately, this method has high implementation cost and use of single secret key technique decreases the system security against attacks. Then, use of different secret key for each tag in the protocol was proposed as an alternative approach. However, matching a secret key and a tag during the authentication stage came up as a problem, and in case of large number of tag existence, computational cost brought due to entire system operation increases.

Detailed information on existing RFID protocols is given on Table 1.1.

Cryptographic algorithms are also used for privacy and security protection of RFID communications. Several lightweight authentication protocols have been proposed in literature. As an early study, Hopper and Blum [15] developed the HB protocol in 2001. The protocol provides security based on learning parity with noise problem. However, this study provides security only against passive eavesdroppers. To implement a protocol also secure against active eavesdropping attacks, Jules and Weis [16] proposed HB^{+} protocol, an enhanced version of previous HB protocol. In 2005, a new study proved the vulnerability of HB^{+} against a computational complex attack by adversaries [17]. Also in [18], a new attack study on both protocols was proposed. Later on, HB^{++} protocol was developed by Bringeret et al. [19], claiming security against all known attacks. The main idea behind the protocol is increasing the number of secret keys in both the tag and the reader. However, the HB^{++} protocol was also vulnerable to active attacks [20]. Then, research of Munilla and Peinado [21] has ended up with new HB-MP protocol, which is resistive to active attacks. In [22] [23],

Table 1.1: Evaluation of different RFID Authentication Protocols [1].

Protocol Name	Hardware Requirement	Protocol Features	
		Advantages	Disadvantages
Hash-Lock Protocol [10]	Hash function	ID is secured	Vulnerable to replay and tracking attacks
Randomized Hash Lock Protocol [10]	Hash function PRNG	ID is secured with random process	Vulnerable to replay and tracking attacks, Computational cost is high
Hash-Chain Agreement [11]	Two different Hash function	Hardly tracked, Forward secure	Vulnerable to replay attacks
Distributed RFID Challenge-Response Protocol	Hash function PRNG	Secure transmission	High computational cost due to Pseudorandom number generation
Digital Library RFID Protocols	Pseudorandom function, PRNG	Secure transmission	High computational cost due to Pseudorandom number generation
Y. C. Lee and others, Authentication Protocol [12]	Hash function	Information hiding achieved, Hard to be tracked	One-way authentication protocol, Vulnerable to impersonation attacks
HASP Protocol [13]	Hash function PRNG	Secure transmission	Needs Tag-Hash calculation and pseudorandom number generation. Hence, computational cost is high
LCAP Protocol	Hash function	Secure against Tracking, Replay and Counterfeiting Attacks	Vulnerable to Denial of Service Attacks
Hash Based ID Variation Protocol	Hash function	Secure against Tracking, Replay and Counterfeiting Attacks	Vulnerable to Denial of Service Attacks
SASI Protocol [14]	Bit operations and shift operation	Strong authentication and integrity	Algorithm is weak and may be cracked

HB-MP protocol's unreliability against man-in-the-middle attacks was explained. In 2008, HB# was proposed which is more secure and efficient than the HB+protocol, but requires larger secrets and storage [24].

More protocols studies with cryptographic algorithms were analyzed in a study completed by Safkhani et. al. [25]. Several lightweight authentication protocols have been proposed in [26], [27], [28], [29], [30], [31], [32], [33], [34], [35]. However, most of these protocols do not meet the security needs in RFID according to analyzes in [36], [37], [38], [39], [40], [41] and [42].

In this study, a new communication protocol is developed and for UHF RFID applications. Proposed work is a challenge-response protocol using cryptographic means to secure the communication. The Tiny Encryption Algorithm is thought to be one of the fastest and most efficient lightweight cryptographic algorithms [43] and suitable for embedded systems that require ease of implementation, high speed, low power consumption and low cost beside security [44]. Although equivalent keys lead to weaknesses in related-key attacks, it still provides good security in RFID. Besides, compared to other encryption algorithms such as DES and AES, TEA has a simpler structure, which leads to less computational cost on microprocessors.

On the other hand, resistivity of the protocol against replay attacks was aimed. Therefore, replay attacks were accomplished against the study. Eventhough there has been theoretical approaches to resistivity of the proposed protocols to replay attacks in several studies such as [45], [46], [47], [48], [49], [50], [51], [9], [52], [53] and [54], to our knowledge, there have not been any practical studies of replay attacks accomplished before. Hence, proposed work has a vital role for future use in literature.

2. RFID SYSTEMS

RFID systems are complex identification systems [55]. Therefore, many different design parameters exist designers should pay attention to. Considering the purpose of application such as animal identification, item management, container identification, vehicle tracking and the application environment such as indoor,outdoor, main parameters are defined.

The most important differentiation parameters are operating frequency of the reader, physical coupling method between reader and tag and the range of the system.

2.1 Frequency, Range and Coupling

In radio communications, the main idea is to separate communication channels with frequency allocation and so to operate many different systems in a frequency interval [55]. This operation is mainly controlled by governmental organizations all around the world, with different parts of electromagnetic spectrum being assigned for different purposes.

RFID systems operate in widely different frequencies, ranging from 135kHz to 5.8GHz. Most commonly encountered frequency bands are 125/135 kHz, 13.56 MHz, 860-960 MHz, 2.4-2.5 GHz and 5.4-6.8GHz [2].

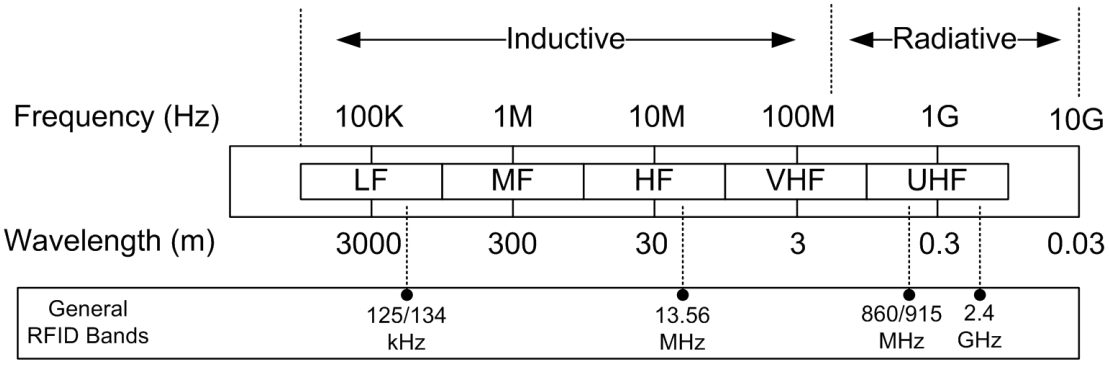


Figure 2.1: RFID Frequency Bands [2].

The most important differentiation criteria for RFID systems are the operating frequency of the reader, the physical coupling method and the range of the system [4]. Actually, operating frequency of a system has a big influence on defining the coupling method between reader and tag. Electromagnetic waves travel in space at the speed of light, c=300.000 km/s. Considering also the frequency of operation, wavelength of an electromagnetic wave is defined by,

$$\lambda = c/f \tag{2.1}$$

Thus the wavelength of a wave will be 3km in 100kHz and 1 cm in 5GHz. As clearly seen, the wavelength is very long in short frequencies. Therefore, low frequency systems and high frequency systems differ in coupling techniques.

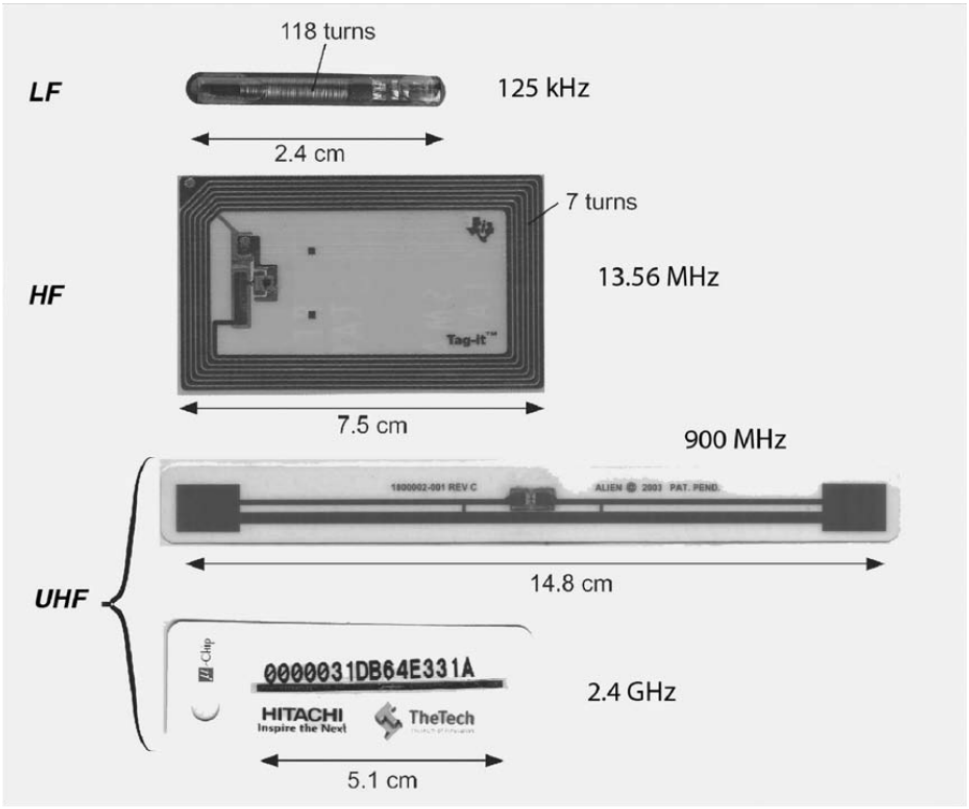


Figure 2.2: Antenna type difference in passive tags depending on frequency and coupling [2].

2.1.1 Inductive Coupling

Inductive coupling systems are near field communication systems. Energy is transferred from reader to tag via the mutual inductances of the antennas. When a tag is in proper range of antenna, a voltage level is induced in tag and tag powers up with

rectification of the voltage [4]. To transmit data from tag to reader, tag changes the load on its coil and magnetic changes are detected by reader. LF and HF systems mainly operate on inductive coupling basis [4]. Because of enormous sizes of wavelengths in LF and HF bands, implementation of a suitable antenna for RFID applications is not possible, considering the varying lambda/4 lengths above 100m.

2.1.2 Radiative Coupling

Certain RFID systems operate on radiative coupling basis [4]. In this type of a coupling, the reader emits radio waves through a dipole antenna to the tag, which is in meters distance. All of RFID systems with radiative coupling function performs at UHF frequencies and microwave frequencies. In passive tags, data transmission from tag to the reader is be done by modulating and backscattering received signals and communication ranges of 3-4m are achieved, while ranges of above 15m can even be achieved using semi-active backscatter transponders [4]. Active transponders are capable of transmitting radio waves using power supply. In these systems, communication ranges of 100m and above is possible regarding to the receive sensitivity.

2.2 System Components

RFID systems are categorized into three main subsystems, reader, tag and database [2].

Database: Database is data storage where the useful information is stored to be used by the reader. Registered Tag ID numbers are stored in database. No further details will be given about database since it is not an important design parameter in this thesis.

Reader: Readers are the devices used for control, verification and tracking of tags. In general, main structure and operation of readers do not differ much in different systems. Readers consists of an RF front-end stage for RF communication and a baseband stage, where useful data is processed. Readers are used for tracking, receiving information from tags and authentication control purposes. Production

of portable and stable readers is possible. Selection of the proper type of reader depends on the aim of application.

Tag: On the other hand, RFID tags are the devices which defines important parameters in an RFID system. According to the structure of a tag, range, coupling and antenna type and communication protocol changes in RFID systems. RFID tags are also called transponders, a term comes from TRANSmitter and resPONDER, and the most important distinction between RFID systems is how the transponders are supplied in terms of energy [2].

Passive and active transponders are two main transponder types in RFID.

2.2.1 Passive Tags

Passive transponders do not have a power supply [2]. In this structure, tags are supplied by regulating the incoming signals of readers. Data transmission from tag to reader is done by backscattering the signals sent by reader. Received signals are analyzed by transponder chip after power is supplied. Then the tag activates and deactivates a Field Effect Transistor (FET) through a pin depending on the data stored on it. When the FET is active, received signal is short-circuited to the ground and there is no backscattering, but when the FET is inactive, received signal is backscattered to the reader. Hence, modulation of the received data is completed and data transmission from tag to reader is completed.

This type of communication between transponder and reader may also be called passive communication [4]. In passive type of communication, tag and reader are coupled inductively. Hence, if the tags are not in close proximity to reader, there is no data transmission from tag to reader since the tag can not be supplied. Very simple protocols must me used in readers to minimize power consumption, hence the computational power of a passive tag is low. Link improving techniques such as error-correcting codes, interleaving, gain adjustment and retransmission are not practical for passive tags due to limited computational power. Moreover, security and privacy are compromised in passive tags as implementation of complex cryptographic algorithms are not possible due to limited resources [2].

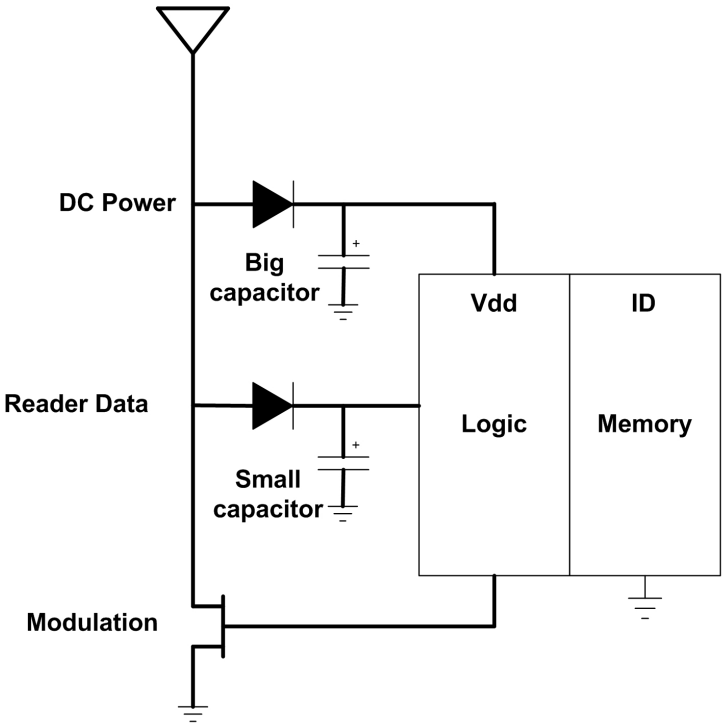


Figure 2.3: Passive Tag Structure [2].

There is also semi-passive type of RFID transponders, but the subject is not examined in this thesis. Basically, semi passive tags are advanced types of passive tags with power supply implementation, provide larger communication range with larger memory size.

2.2.2 Active Tags

In active transponder structure, a power supply unit is implemented in the circuit [2]. Active transponders have an RF front-end to receive-transmit signals. When the reader signal is received, firstly the signal is downconverted to baseband signals. Following, data is analyzed by microcontroller stage and the response data is encrypted and transmitted to the radio stage. In the radio stage, baseband signal is attached on RF carrier signal and then transmitted to air by antenna to the reader.

When compared to passive tags, the electromagnetic field may be much weaker than the field required for operating a passive transponder [2]. Therefore, communication range is higher in active transponders. Due to other physical mechanisms and taking into account the permitted transmitting power, short-range devices can have a range of

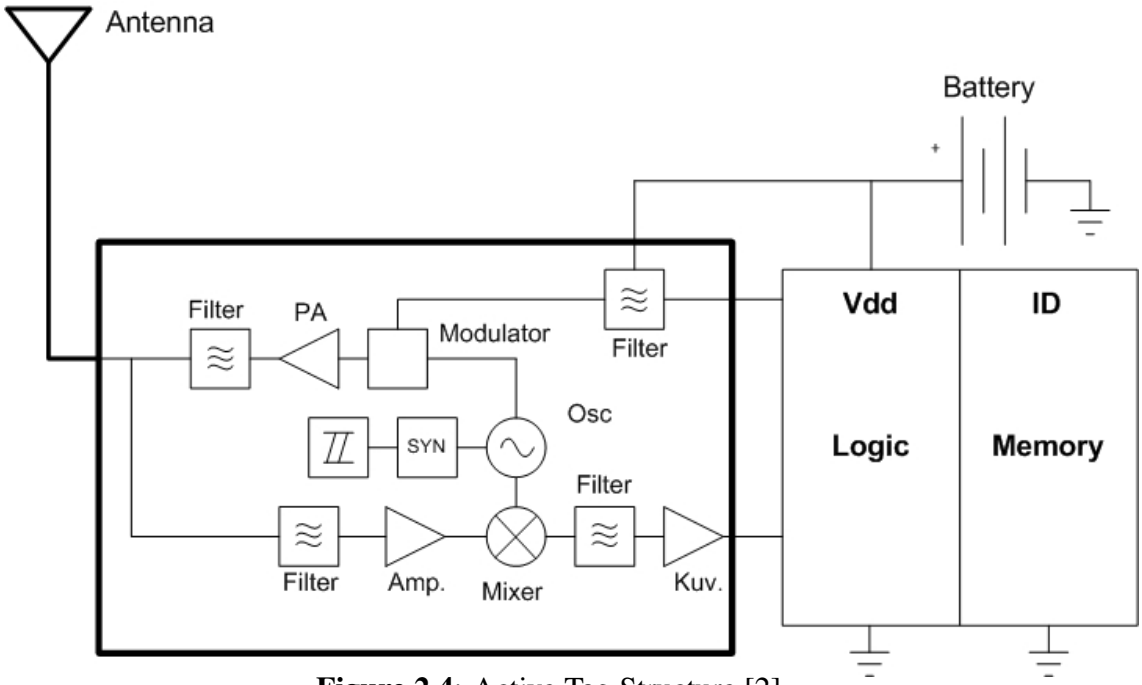


Figure 2.4: Active Tag Structure [2].

up to several hundred meters. Moreover, active transponders have larger data storage capacity.

Active tags have capability of communicating with amplitude modulation as passive tags and modulation and demodulation of more sophisticated phase-based modulations(phase-shift keying, PSK, frequency shift keying, FSK, and quadrature amplitude modulation, QAM), which provides more efficient use of spectrum and better Signal to Noise Ratio (SNR) values [2]. Application of high-rate Code-Division Multiple Access (CDMA) techniques are possible in active tags to allow multiple tags reuse the same frequency band.

2.3 Summary

In this chapter, the most important parameters in an RFID system were presented, which are frequency of operation, coupling method and tag architectures. Firstly, RFID frequency bands were presented and features of these bands were revealed. Effects of frequency on coupling method between reader and tag was expressed. Following, RFID system components were mentioned and different tag architectures were presented. Frequency of operation is the primary matter of selection. Coupling method and tag selections are defined according to the frequency and possible

communication range of the systems. In high frequency bands, active tags are used and radiative coupling method is applied to provide high communication range. However, in systems operating in HF and VHF band, inductive coupling is preferred due to long wavelengths. Besides, passive tag structure is preferred for systems operating in low frequency ranges.

3. RADIO BASICS FOR UHF RFID

Radio frequency planning is a key part of network deployment and is essential for wireless networks [56]. Insufficient network planning leads to decrease in system performance and network quality and increase in power consumption. Furthermore, total cost of the whole system may also increase. To prevent mentioned disadvantages, designers should pay enough attention to RF planning of a communication link.

Link budget and Free Space Path Loss parameters should be understood very firstly to have a good understanding of propagation of radio waves.

3.1 Link Budget

Link Budget is the sum of calculations of all gains and losses in the environment a wave travels from the transmitter, through medium to the receiver in a wireless communication system [2]. Link budget is a way of quantifying the link performance. The received power in a communication link is determined by four different factors, which are transmit power, transmitting antenna gain, losses in medium and receiving antenna gain. If transmitted power minus the losses in the link path is greater than the receive sensitivity of the receiving radio, then communication is possible.

Link margin is a result of link budget calculations and is used for telling the difference between required power level and system power level. Link margin can be expressed as:

$$LinkMargin = EIRP - L_{path} + G_{R_x} + TH_{R_x} \tag{3.1}$$

where

- EIRP is the effective isotropically radiated power in W or dBm,

- L_{path} is the total path loss, including miscellaneous losses, reflections, and fade margins in dB,
- G_{R_x} is the receive gain in dB,
- TH_{R_x} is the receiver sensitivity.

3.2 Propagation of Radio Waves

Propagation of radio waves may interrupted by the materials in the area of propagation.Hence, to make a true analyze, propagation of radio waves can be researched in two different category.

3.2.1 Free space path loss (FSPL)

Free space path loss is the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space with no obstacles nearby to cause reflection or diffraction.

Free-space path loss is proportional to the square of the distance between the transmitter and receiver, and also proportional to the square of the frequency of the radio signal, hence to the wavelength. Free space path loss formula is:

$$FSPL = \frac{P_t}{P_r} = (\frac{4\pi}{\lambda})^2 d^n \tag{3.2}$$

where

- d is distance from transmitter in meters,
- λ is wavelength in meters,
- P_t is transmitted power from transmitter,
- P_r is received power.

Considering the Friis transmission equation, free space path loss of a signal in a communication system becomes:

$$FSPL = \frac{P_t}{P_r} = \frac{1}{G_t}\frac{1}{G_r}(\frac{4\pi}{\lambda})^2 d^n \quad (\mathbf{3.3})$$

where

- G_t is transmitter antenna gain,
- G_r is receiver antenna gain.

Equation can be expressed in dB as:

$$FSPL = \frac{P_t}{P_r} = 20\log(\lambda) - 20\log(d) - G_t - G_r + 22 \quad (\mathbf{3.4})$$

In given equations here, receiver and transmitter antenna gains are calculated, but mostly free space path loss formula is given without antenna gains, as in Equation **3.2**. Propagation constant, n, in free space path loss formula which effects attenuation due to distance differs in different mediums. In spaces where the number of objects that effect propagation is less, n gets the value 2.

3.2.2 Propagation in real world

Wireless communication channels have many parameters and are much more complex compared to wired communication systems. Due to high number of interrogators, communication links and environments are modeled with specific techniques. Signal power levels and environmental effects are researched and analyzed in these models. Three main effects are considered in large scale propagations. Alongside with attenuation of signal in free space due to path loss, reflection, scattering and diffraction of radio waves effect the continuity of propagation. On the other hand, in small scale propagations, multipath effects comes into prominence in indoor environments.

3.2.2.1 Reflection

During the propagation, if the waves crash to an object larger than the wavelength, some part of the wave reflects back while remaining part penetrates into the crashed object. If the object is a perfect conductor, all the wave is reflected back and no attenuation occurs on signal strength. In other case, if the material is not a perfect conductor, attenuation occurs on the signal strength and reflection is calculated by

Fresnel Reflection Coefficient (Γ)17. Value of fresnel coefficient depends on reflection angle, frequency and radio wave polarization type18.

3.2.2.2 Scattering

Scattering happens at the corners of the objects which have greater dimensions than the wavelength and leads to diffraction. It can provide communication link without line of sight. Scattering provides many advantages in GSM applications and some other closed area applications where radio waves face a lot of barriers.

3.2.2.3 Diffraction

In some cases, objects, which radio waves meet, may have equal dimensions close to the wavelength19. If radio waves crash to the objects, waves spread away in a lot more directions than in scattering. Diffraction is the hardest parameter in modeling studies.

3.2.3 Indoor propagation

Most important characteristics of an indoor RF propagation environment are existence of multipath reflections, absence of line-of-sight path and possible change of environment characteristics over a very short time or distance [56]. Communication ranges generally tend to be short. Walls, doors, furniture, and people may be the source of attenuation on signal strength. In this kind of an environment, propagation is much more related to reflection, scattering, diffraction and penetration. Delay and Doppler Effect are not of great importance since the range is significantly short and the speed of field transceiver is not much.

Many different models were developed for indoor propagation modeling up to date in wireless communications. In this study, path loss model prepared by International Telecommunications Union is mentioned.

3.2.3.1 The ITU indoor path loss model

The ITU model for site-general indoor propagation path loss prediction is:

$$L_{total} = 20\log_{10}(f) + N\log_{10}(d) + Lf(n) - 28dB \qquad \textbf{(3.5)}$$

where

- N is the distance power loss coefficient,
- f is the frequency in MegaHertz,
- d is the distance in meters (d > 1m),
- $Lf(n)$ is the floor penetration loss factor,
- n is the number of floors between the transmitter and the receiver.

Calculated N and $Lf(n)$ values are given in tables below.

Table 3.1: Power Loss Coefficient Values, N, for the ITU Site-General Indoor Propagation Model.

Frequency	Residential	Office	Commercial
900 MHz	-	33	20
1.2-1.3 GHz	-	32	22
1.8-2 GHz	28	30	22
4 GHz	-	28	22
5.2 GHz	-	31	-
60 GHz	-	22	17

Table 3.2: Floor Penetration Loss Factor, $Lf(n)$, for the ITU Site-General Indoor Propagation Model.

Frequency	Residential	Office	Commercial
900 MHz	-	9(n=1)	-
	-	19(n=2)	-
	24(n=3)	-	
1.8-2 GHz	4n	15+4(n-1)	6+3(n-1)
5.2 GHz	-	16(n=1 only)	-

N=20 power loss coefficient value corresponds to free space loss, which is applied in open areas. In corridors, RF signal is channeled by the walls. Hence, power loss coefficient equals to N=18, which is less than free space loss. On the other hand, N=40 value is used for propagation through walls or over corners since the attenuation is higher.

The ITU indoor path loss model is a site-general model for indoor path loss calculation. There are several more site-general models and also many site-specific models exist in research history. Site-specific models are generally application based empirical models.Hence, they are not further investigated in this thesis due to disinterest with thesis subject. ITU model is preferred for future link margin calculations in the thesis.

3.3 Bit Error Rate Analysis

In an ideal case, a bit sequence transmitted into a transmission channel is expected to be received at output without any errors. However, in real conditions, it is hampered by undesired noise signals in transmission channels. The ratio of bit error number in entire transmission channel to the number of transmitted bits gives bit error rate [57].

$$BER = \frac{numberoferroneousbits}{numberoftotalbits} \tag{3.6}$$

Signal to noise ratios and Eb/No figures are parameters that are more associated with radio links and radio communications systems [58].

$$\frac{E_b}{N_0}(dB) = C - N_0 - 10\log(f_b) \tag{3.7}$$

where

- E_b is energy per bit (dBm/Hz)
- N_0 is noise spectral density (dBm/Hz)
- C is carrier power (dBm)
- f_b is transmission bit rate

Errors occurring in a transmission channel has a random nature, meaning the errors may not be constant [57]. Therefore, to detect the real bit error rate, infinite number of bits should be transmitted in the channel which is not possible. Accordingly, different techniques have been used to detect bit error rates. Bit error rate calculation is a statistical method used to detect bit error rates. A BER calculated with the

method converges to real case as the number of transmitted bits converges to infinite. Nowadays, BER calculation of most systems is defined with calculated BER's being higher or lower than a predefined threshold BER, considered not to be much effective on the communication, and there exist a Confidence Level term related to this comparison. Confidence level is the ratio of tests, in which measured BERs is lower than the threshold BER level.

$$CL = 1 - e^{N_{bit} * BER^{'}} \tag{3.8}$$

where

- N_{bit} is the number of transmitted bits
- $BER^{'}$ is predefined threshold level

It should be noted that each different type of modulation has its own value for the error function [58]. Each different modulation type performs different in presence of noise signals. Modulation types which can carry higher data rates are as robust as lower order modulation formats that offer lower data rates. Hence, BER of a communication link differs in different modulation types while preserving the range.

3.4 Summary

In this chapter, link calculation of radio systems were presented. At the beginning, basic term of link budget was expressed. Following, propagation of radio waves was mentioned and free space effects on a radio wave was given in details. Considering the free space path loss, a radio wave's power level decreases proportional to the square of distance due to Friis equation. Besides, reflection, scattering and diffraction are three important parameters that effect a propagating radio wave in real world environment. Radio waves do not behave as in free space while propagating in real world. Hence, different parameters are considered in real world link budget calculations. To make generalization, there are two possible environment of propagation in real world, indoor and outdoor. Outdoor calculations are relative or almost same as free space calculations. However, many effects are considered on indoor propagation. To

make precise calculations, indoor links are often modeled specifically. Wide variety of indoor propagation models exist in literature. However, the site-general model proposed by International Telecommunications Union is presented in this study. Lastly, bit error analysis in communication systems are explained.

4. SECURITY IN RFID

Compared to rest of automatic identification systems, RFID systems have substantial advantages, most importantly providing communication without the need of line of sight and easy tracking [3]. In parallel with these features, use of RFID systems is increasing day by day in every corner of daily life. Patient tracking systems in hospitals, vehicle tracking, supply chain management and stock tracking in warehouses, toll collection systems in highways are several examples of RFID applications.

Despite RFID is blooming without restraint in automatic identification systems industry, security and privacy have become hot issues recently [5].

4.1 Main Security Concerns

4.1.1 Privacy

Leakage of information is a problem that occurs when data sent by tags reveals sensitive information about the labeled items. In some cases RFID tags carry information about the objects they are implemented on and usually, readers are not authenticated and tags answer in a transparent and indiscriminate way. In this case, people carrying objects with RFID tags are vulnerable to tracking and privacy attacks. Several types of RFID tags are very small in dimensions and these tags can be embedded in clothes, shoes, books, key cards, prescription bottles and a stranger in public can easily find out by reading the tags where she is shopping, or what kind of medicines she uses and what kind of illnesses she has, where she lives, what her identity number is, how much money she has and etc. In such a situation, personal privacy rights are considered to be easily violated.

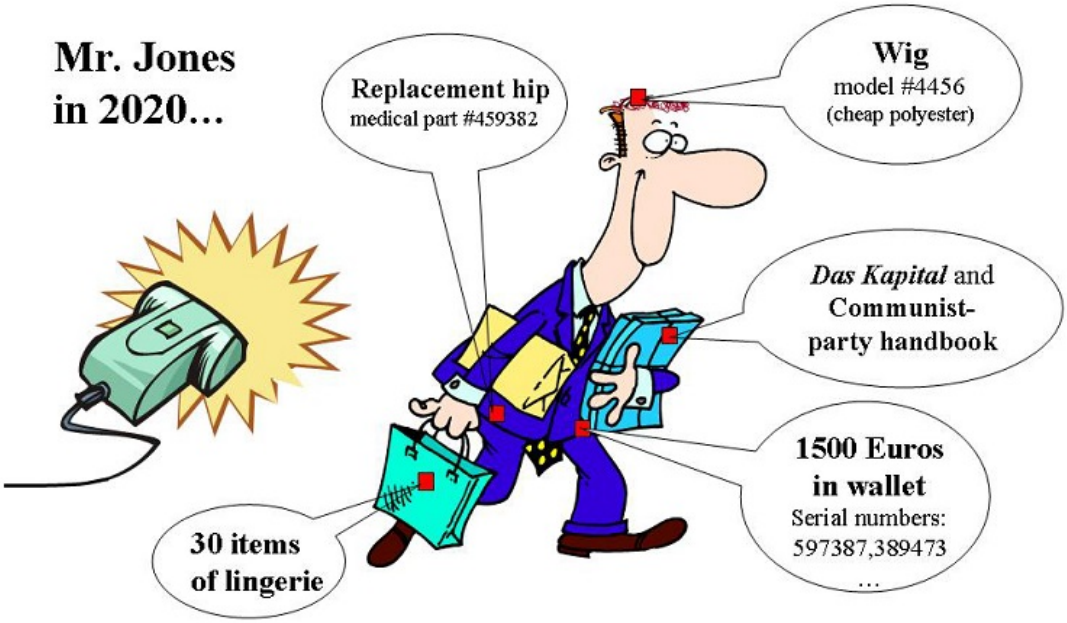


Figure 4.1: Manufactured goods with RFID tags [3].

4.1.2 Tracking

Location privacy is another subject in consideration of privacy [3]. Certainly RFID systems are not the only possible way of tracking individuals. Tracking an individual is quite easy if the person has a mobile phone. Each time a cell phone makes reasonable location change, it connects to a new cell in that region. By this means, a mobile phone operator can easily track customers. In means of RFID, by suitably placing readers, tracking people with RFID transponders becomes very easy. To give example, RFID chips are placed in your shoes by vendor, the company can easily track individuals location, when the individual go or quit home, which malls she visits and can sell this information to third party organizations. Collecting the location data of people, these organizations could send the person personalized advertising information depending on her shopping habits [59].

Recently, a high school student's refusal to wear the school's badge with RFID chip in Texas, USA has been the center of debates in RFID tracking [60]. Andrea Hernandez, 16 year old student, refuses to wear RFID enabled school badge since she doesn't want to be tracked during school time. In November, she was notified by the district that she

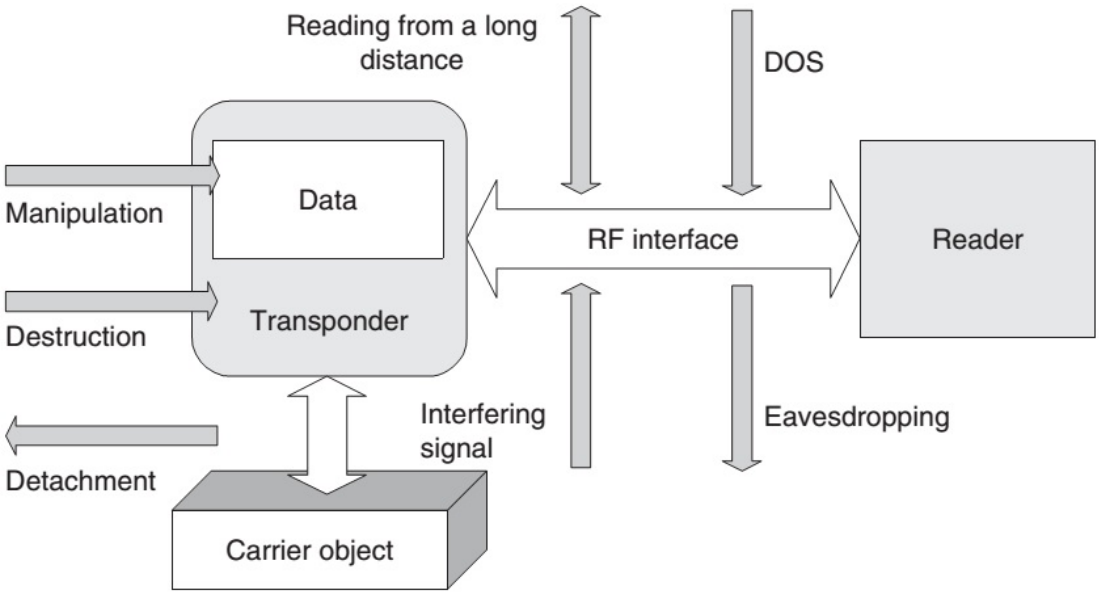


Figure 4.2: RFID Attacks [4].

will not be able to attend her current John Jay High School if she refuses to wear school badge.

On the other hand, implementation of individual product codes on manufactured goods are being considered nowadays. If the technology is presented to the market in following years, every individual will be easily matched with product that has the specific RFID code and tracking will become so easy as finding a needle in haystack.

4.2 RFID Attacks

It is mentioned in earlier stages that an RFID system consists of different stages and these stages should be considered separately to fully analyze radio frequency identification systems. In this section, possible attack on RFID systems are presented. Classification of RFID attacks are visualized in Figure3.2.

4.2.1 Attacks on transponder

Transponders are easily accessed part of RFID systems. Hence, vulnerability of transponders against attacks is high. Several attacks on RFID transponders are considered in this section.

4.2.1.1 Permanently disabling tags

Tag Removal-Transponders that are not embedded in goods may easily be removed or placed in another product. Switching price tags of manufactured goods is an example of this kind of an attack. An attacker can easily replace the price tag of an expensive product with a cheaper one and pay less at the cash point. Tag removal is not a complex process and does not require high technical skills for an individual to carry out, hence this is a mostly faced problem in shopping malls and markets.

Tag Destruction- Operating features and physical limitations of RFID tags are defined considering predefined standards with proper power regulations [61]. Generally, readers are prohibited to emit higher power level radio waves than a predefined limit and inductive systems are set to induct sufficient voltage level on tags. An attacker with suitable technical equipment can transmit high power level signals to a radiatively coupled RFID tag and destroy the tag. Similarly inductively coupled tags also suffer from high voltage levels induced by coil antenna. Moreover, electrostatic discharge also leads to malfunction of RFID tags [61].

4.2.1.2 Temporarily disabling tags

RFID tags may disappear for a short period of time instead of malfunctioning at all [59]. Temporarily disabling may be either intentionally or unintentionally. A stealer may cover the RFID tag of a product with a material to constitute faraday cage and can pass any security check without any alert. Furthermore, radio interference can lead to temporarily disabling of a tag. Moreover, it is possible to tune receiver antenna of a tag. In inductive coupling systems, a simple piece of a metal in contact with the coils of the antenna changes the resonant frequency and so the inductance. In backscattering systems, antennas are tuned to a different frequency by the help of different materials such as air, water, etc8 [4].

In general, RFID systems operate in a noisy environment and the communication between tag and reader is susceptible to any interference and collisions from other radio transmitters close to the system. On the other hand, an attacker can place a

transmitter system close to the reader, and interfere with the communication of reader and tag.

4.2.1.3 Spoofing and cloning tags

Read-only transponders suddenly responds when they enter to a electromagnetic field without any authentication of the reader [59]. Hence, an attacker with proper reader can possibly listen to the response of the tag and store the received data. After embedding the data in another tag and counterfeiting the original one, manipulating the reader becomes possible. If the copy tag enters communication zone of the reader, it sends the same data as the original tag and reader does not notice any difference since the data sent by read-only tags does not change by time.

In transponders with accessible memories, the chance of cloning the tag relies on authentication protocols used by tag. Possibility of counterfeiting is reduced or even prevented by implementation of authentication protocols or password, key techniques in tags [4].

4.2.2 Attacks on RF interface

In RF interface, as the data transmission between tag and reader is completed through air, communication link between is open to several types of attacks. An attacker could pose threats to the system even from distances away without the knowledge of the operator.

4.2.2.1 Eavesdropping

According to the frequency of communication and reader-tag output power levels, the communication can be eavesdropped from distance, ranging from 3-4 meters for near field communication systems to a few hundred meters for active communication systems in UHF band [4].

It is observed that communication of inductively coupled systems can be intercepted from 3 meters distance [4]. An attacker can record the communication and store it for later attacks called Replay Attacks. Data transmission between reader and tag occurs in two ways, from reader to tag and from tag to reader. As reader transmits more

powerful signals to have a wider range, it may be eavesdropped farther than tag to reader.

On the other hand, in active RFID communication in UHF band, readers and tags outputs high power levels, which in turn allows for eavesdropping from a hundred meters or a few kilometers away. However, reflection of radio waves from metallic surfaces in the environment and walls in indoor areas, the range is limited in shorter distances.

4.2.2.2 Jamming

Jammer devices are used to produce noise signals in a definite frequency band, hence prevents operation of any other transmitters in that frequency interval. Jamming a system relies on many different parameters. An attacker either should be in close range of the communication link to suppress the signals between reader and tag, or should transmit signals with high power level. To jam inductively coupled systems, the field strength between coil antennas should be suppressed.

Applying jamming techniques has other downsides. Using jammers is illegal and often forbidden by law. As an addition, the jammer signal is easy to detect and can be located easily.

4.2.2.3 Denial of service

Modern RFID systems have capability of dealing with many transponders in their interrogation fields. These kind of multitag systems use anticollision algorithms to communicate with a specific transponder in once. Even some systems determine which transponder to communicate with through use of serial numbers.

Exactly in this kind of applications, some specific tags called blocker tags interfere with the system. A blocker tag always sends ones and zeros simultaneously and simulates collision at each bit location of the tree, hence mislead the reader. Taking into account the received information, the reader presumes that there are 2^k tags, where k is the number of bits in serial number. As a result such large number of tags block the reader [4]. This type of an attack is called Denial of Service attack.

4.2.2.4 Relay attacks

In relay attacks, attacker convinces the reader that the transponder is still in field interrogation even though transponder is somewhere else. The operation relies on extending the communication range by using transceiver equipment that transmit signals from reader to transponder and vice versa.

Relay equipment has two stages to communicate with reader and tag. The component located close to the reader is ghost, which is capable of receiving reader's signals and create load modulation to communicate with reader instead of transponder. Other component close to the transponder, called leech, transmit signals to power up the tag and receives modulated signal, so the information stored on the tag.

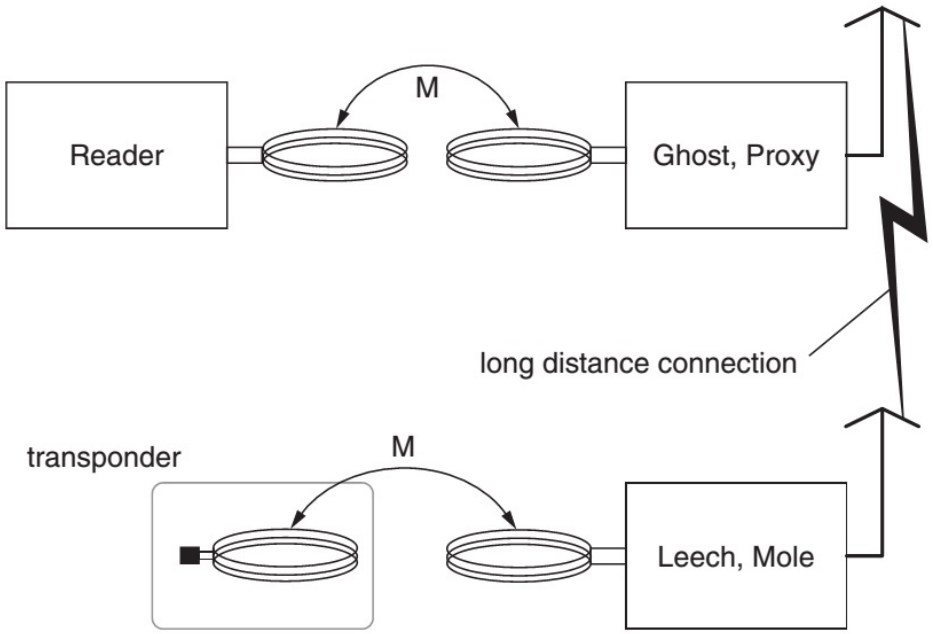


Figure 4.3: Relay attack [4].

In relay attacks, runtime for the transmission of data forth and back might be a problem. As the distance between ghost and leech increases, transmission duration of data increases identically. Hence, relay attacks may fail in a time-critical protocol like ISO/IEC 14442 Type A [2].

To give an example, a relay attack could be used to charge a victim's RFID card for the payments. In 2007, Roel Verdult, an MSc. student from Raboud University

of Nijmegen has successfully performed relay attacks on Dutch Public Transport Cards [62].

5. READER AND TRANSPONDER DESIGN

Security concerns in RFID systems are deeply investigated in previous section. Moreover, RFID attack techniques are mentioned and some examples are given for proposed attacks. Considering the shortfalls of RFID systems in security, design and implementation of a secure RFID protocol on FPGA is proposed in this thesis and replay attacks were completed on the protocol.

In this section, design and implementation of the communication system, which consists of reader and tag, is revealed step by step.

5.1 Determination of Operating Frequency

In RFID systems, frequency of operation is defined considering the purpose of application and the conditions in the environment where the system will operate.

In this study, communication system was desired to have long communication range together with low reflection compared to high frequency applications. Therefore, UHF frequency band is selected as communication frequency between reader and tag. UHF band is wide frequency band ranging from 300 MHz to 3GHz. Exact center frequency of the systems is determined considering RFID regulations in UHF band. Frequency intervals used for UHF applications in RFID are different all around the world due to regulations and restrictions of governments. In Europe, 865-868 MHz frequency band is defined as UHF RFID communication frequency range. To comply with the regulation, 868MHz center frequency is selected for the system.

5.2 Communication Protocol

In order to secure the communication between tag and reader and apply authentication, several authentication protocols are used in RFID systems suitable with the standards. Data transfer between reader and tag must be accomplished in definite data frame in

accordance with the protocols. In this study, a simple two way challenge-response communication protocol is used for authentication. The basis of the study is the authentication protocol proposed by Martin Feldhofer in 2004.

Start of Frame	Flags	0xA0	MfgCode	User ID	Random Number	CRC	End of Frame
	8 bit	8 bit	8 bit	64 bit	128 bit	16 bit	

Figure 5.1: Data frame of reader signal.

Figure 5.1 reflects the structure of reader signal data frame. Each meaningful data presented within the frame is explained below.

Flags: Flags form up the first byte of transmit data frame. They are used to indicate to transponder what data rate and carrier frequency should be used for the response signal.

Command Code: Following byte is called command code which is used to give information about the required command.

Manufacturer Code (IC Mfg Code): Any custom command contains as its first parameter the IC manufacturer code (IC Mfg code). This allows IC manufacturers to implement specific custom commands without risking duplication of command codes and thus cause misinterpretation.

User Identity (UID): 64 bit UID data addresses a unique tag to respond to the transmitted data. This UID must first be retrieved from the tag by the inventory request.

Cyclic Redundancy Check (CRC): CRC is a technique used for detecting errors in digital data, but not for making corrections when errors are detected. In the CRC method, transmitter calculates a checksum value on data to be sent using a predefined polynomial before sending the message and attaches the value to the transmit data frame. Upon receiving the data, receiver completes the same calculations using the same polynomial and creates a checksum. If the received and calculated checksum values match in the receiver stage, the message sent by the

reader is received without any errors. Any other case is a result of errors in received data and if an error occurred, the receiver sends a negative acknowledgement back to the sender, requesting the message to be retransmitted. 16 bit CRC value is placed at the end of frame before the delimiter.

As seen in Figure 5.2, tag data frame is shorter than reader data frame. In tag data frame, command code and manufacturer code bytes are not included since tag operates as a slave device. It can only accomplish the proposed tasks but give commands to the reader.

Start of frame	Flags	User ID	Encrypted Data	CRC	End of frame
	8 bit	64 bit	64 bit	16 bit	

Figure 5.2: Data frame of tag signal.

5.2.1 Authentication

To give details on authentication, a random 64bit number is firstly sent to the transponder in a proper data frame. Received data is encrypted and then sent back to the reader. Following, the reader decrypts the received data and compares with the data sent to transponder. If received and sent data match with each other, reader authenticates the transponder.

5.2.2 Encryption Algorithm

Tiny Encryption Algorithm (TEA) is a cryptographic algorithm used to secure data transfer between reader and tag. TEA is an advantageous algorithm due to quite short runtime and low memory use. TEA produces two different 32 bit output data, using a 128 bit encryption key.

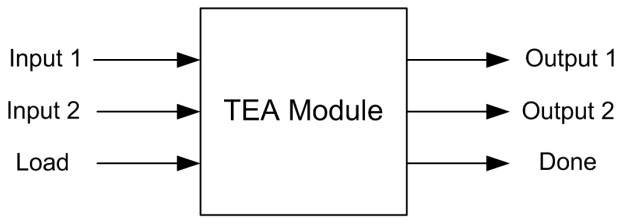


Figure 5.3: Visualization of input and outputs of TEA module.

64 byte input data enters the algorithm as two different 32 byte signals. The load data entered together with the input data enhances the transfer of input data from registers to variables and initiates the algorithm. The data is encrypted or decrypted with the use of 128bit key hidden in the design and sent to the output as two different 32 byte data. Completion of process is verified by done bit. TEA is used in this study to secure the transferred data.

5.3 RF Front-End Modules

RFM22B Transceiver Modules manufactured by Hope Microelectronics are used as RF front-end modules in the system. The modules have -121dBm receive sensitivity and are capable of outputting signal with +20dBm power level at maximum. Calculating the free space path loss at frequency of operation, maximum communication range of the modules is quite long in free space.

Table 5.1: RFM22B RF Module Features.

Parameter	**Value**
Frequency Range	433/470/868/915 MHz ISM Bands
Receive Sensitivity	-121dBm
Max Output Power	100mW
Supply Voltage	1.8-3.6V
Receive Power Consumption	60mW
Transmit Power Consumption	280mW (max case)
Modulation	FSK, GFSK, OOK
Data Rate	0.123 to 256 kbps

RFM22B modules are versatile devices to be used in a wide frequency range for different purposes. As seen in table below, modules are capable of operating at different ISM bands. Moreover, using the frequency deviation feature, device can be programmed to operate in different carrier frequency bands ranging from 240MHz to 960MHz. Due to high capabilities of the chips, RFM22B modules may be used in many applications such as remote control, home security and alarm, telemetry, personal data logging, tire pressure monitoring, wireless PC peripherals, tag readers and etc.

Modules were used as RF front-end modules in reader-tag devices in this project. Devices were connected to FPGA boards to be programmed and supplied in terms of power. Microblaze, which is software based microcontroller on FPGA board, was used as microcontroller to program the modules and set the desired operation parameters. Required program was designed in C programming language. Modules were programmed to work at 868MHz center frequency with GFSK modulation. Data rate was set to 9.6 kbps.

Table 5.2: Specified operation values.

Parameter	**Value**
Center Frequency	868MHz
Output Power	100mW
Supply Voltage	3.3V
Receive Power Consumption	18.5mA (60mW)
Transmit Power Consumption	85mA (280mW)
Modulation	GFSK
Data Rate	9.6kbps
Bit Error Rate	BER < %0.1

RFM22B modules have a characteristic data frame to decrease the number of processes on microcontroller and increase the communication speed. Bytes sent before the data handles detection, synchronization and addressing issues. Automatically adding these fields to the data payload greatly reduces the amount of communication between the microcontroller and the RFM22B/23B and reduces the required computational power of the microcontroller.

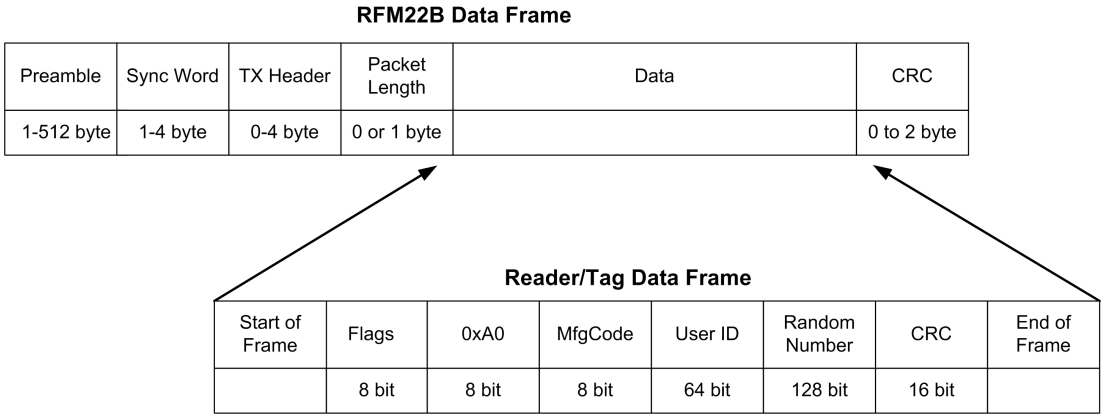


Figure 5.4: Implementation of reader/tag data frame to RFM22B data frame.

Desired data to be sent is placed in data part of RFM22B frame as a whole reader/tag frame. As visible, RFM22B's are also capable of calculating the CRC value of the data being sent. However, this option is not preferred in order to have ease of design within the designed algorithm.

5.4 Reader and Tag Design

An RFID reader device consists of front-end and back-end stages. As already mentioned before, RFM22B modules were used in front-end stage. On the other hand, an FPGA was preferred in microcontroller stage due to high computational power. Hence, Spartan-3E starter board constitutes baseband stages of transponder and tag. Following sections give detailed info about the hardware and software design of reader.

5.4.1 Hardware

Xilinx Embedded Development Kit(EDK) was used to define the hardware specifications of FPGA kits. In this program, user selects the desired features of FPGA board and sets up the hardware configuration. EDK is a platform to create and change hardware configuration of the board using algorithms designed in Hardware Description Language like Verilog and VHDL. On the other hand, Software Development Kit (SDK) of Xilinx is used to control the hardware configuration by software. For this feature, hardware design in EDK should be transferred to SDK. After transferring process, it is possible to develop an algorithm to control the configuration using C programming language. A board support package is provided for communicating and programming with hardware submodules through Microblaze.

5.4.1.1 TEA-Microblaze communication

In this study, TEA algorithm is proposed as a hardware submodule (IP Core) in FPGA design. An IP Core should be firstly defined to Microblaze to allow data transmission in between. For this purpose, TEA module is defined in EDK as a peripheral firstly. TEA algorithm is integrated to the design by changing verilog file created by the template in EDK. Utility of TEA module is tested and verified in Project Navigator using test vectors.

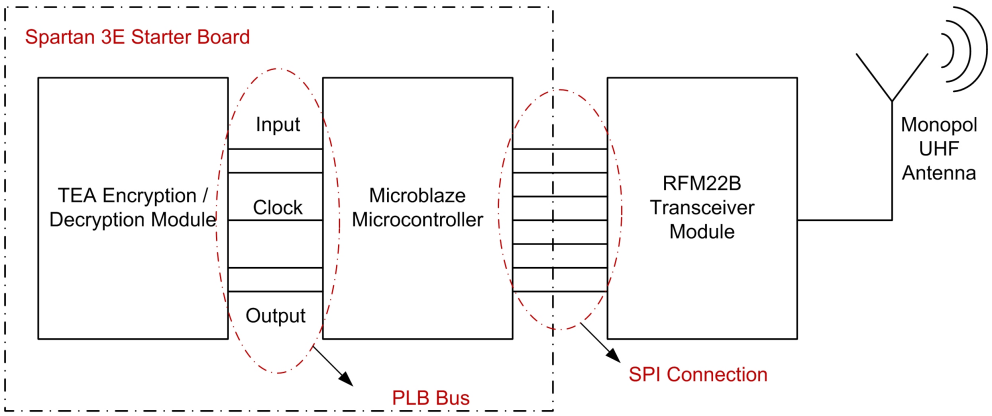


Figure 5.5: Microblaze and TEA communication block diagram.

In order to transmit data generated by TEA module to the outside world, the data should be sent to RF transceiver modules through Microblaze. Hence, addressing of the module is done in EDK and the hardware design is transferred to SDK for software based controlling tests. In this section, designed TEA module is connected via Microblaze by a simple code that is created by using the functions defined in board support package libraries of SDK design.

5.4.2 Reader Algorithm

Reader algorithm starts with initial functions. After running the functions and making slave devices such as RFM22B RF modules and other submodules ready for operation, algorithm enters to communication mode. After the initial section, reader algorithm consists of two different parts, Data Send Loop and Data Receive Loop which are actually two different for loops running in another common for loop.

Data Send Loop: Send loop is the first loop between two loops, since the reader is responsible for starting the communication with the tag. Random number data should be sent periodically for any tag that might appear in the range. Below diagram is the flow chart of data send loop of reader algorithm.

In data send loop, reader firstly generates random numbers and prepares the data frame with bitwise operations. Then, CRC checksum is calculated by implemented CRC algorithm. Calculated value is added as last two bytes of the frame just before the EOF delimiter for CRC comparison operation in tag stage. Upon completing CRC operations, data is written to RFM22B first-in-first-out(FIFO) registers over SPI

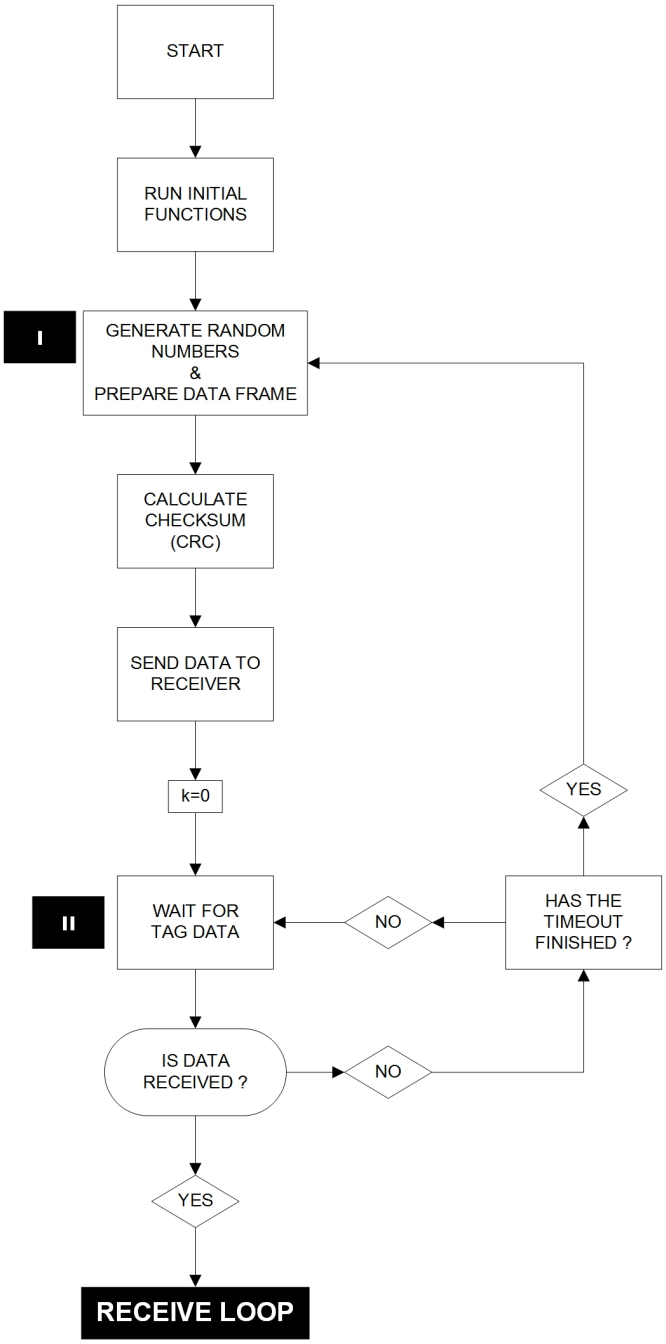


Figure 5.6: Reader algorithm, data send loop flow chart.

link. When all frame, 176 bit reader data, is written on FIFO, "data ready to sent acknowledgement" is sent to RFM22B and the module transmits the data to the air over an UHF antenna.

Next, reader starts to wait for an incoming tag response. The length of timeout is set to be higher than the total duration of forward transmission, data process in tag and

backward transmission. In case of data reception, RFM22B generates an interrupt and pulls down the NIRQ pin. If any data is received during timeout, reader enters to the next loop, data receive loop. Else, waits till the end of timeout, when parameter k reaches 10000, and goes back to the beginning of the loop, position I.

Data Receive Loop: Receive loop is the second loop that comes after send loop. During the operation, reader algorithm does not run the receive loop section all the time. Receive loop runs only in case of received data presence. Block diagram below reflects the flow chart of receive loop.

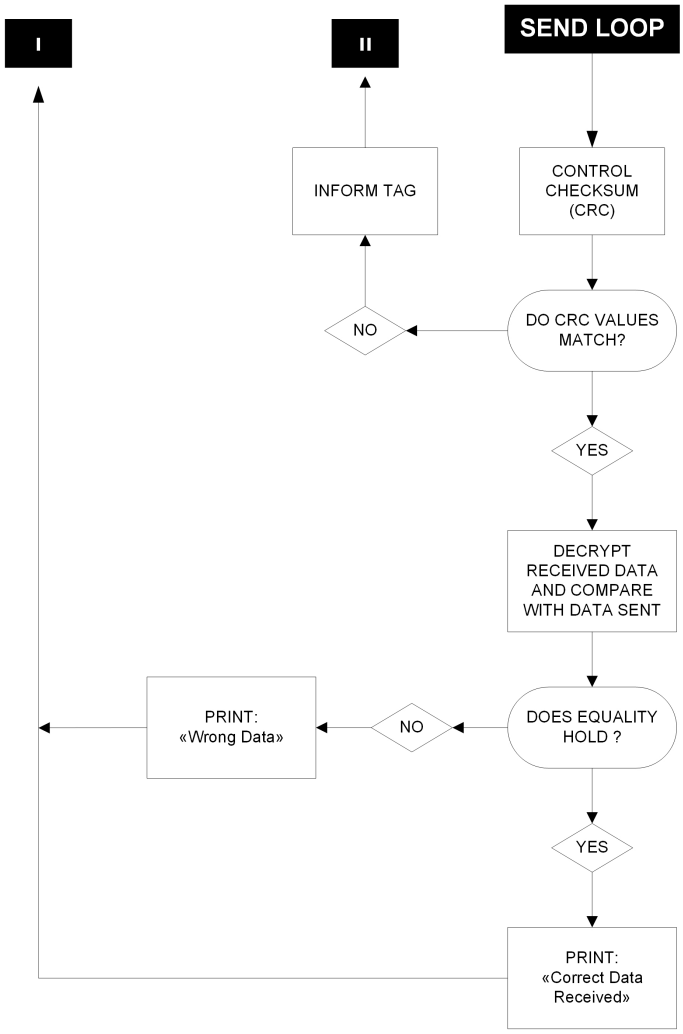


Figure 5.7: Reader algorithm, data receive loop flow chart.

In receive loop, reader firstly checks for CRC value of received data and takes the next action considering the result of comparison between received and calculated checksum

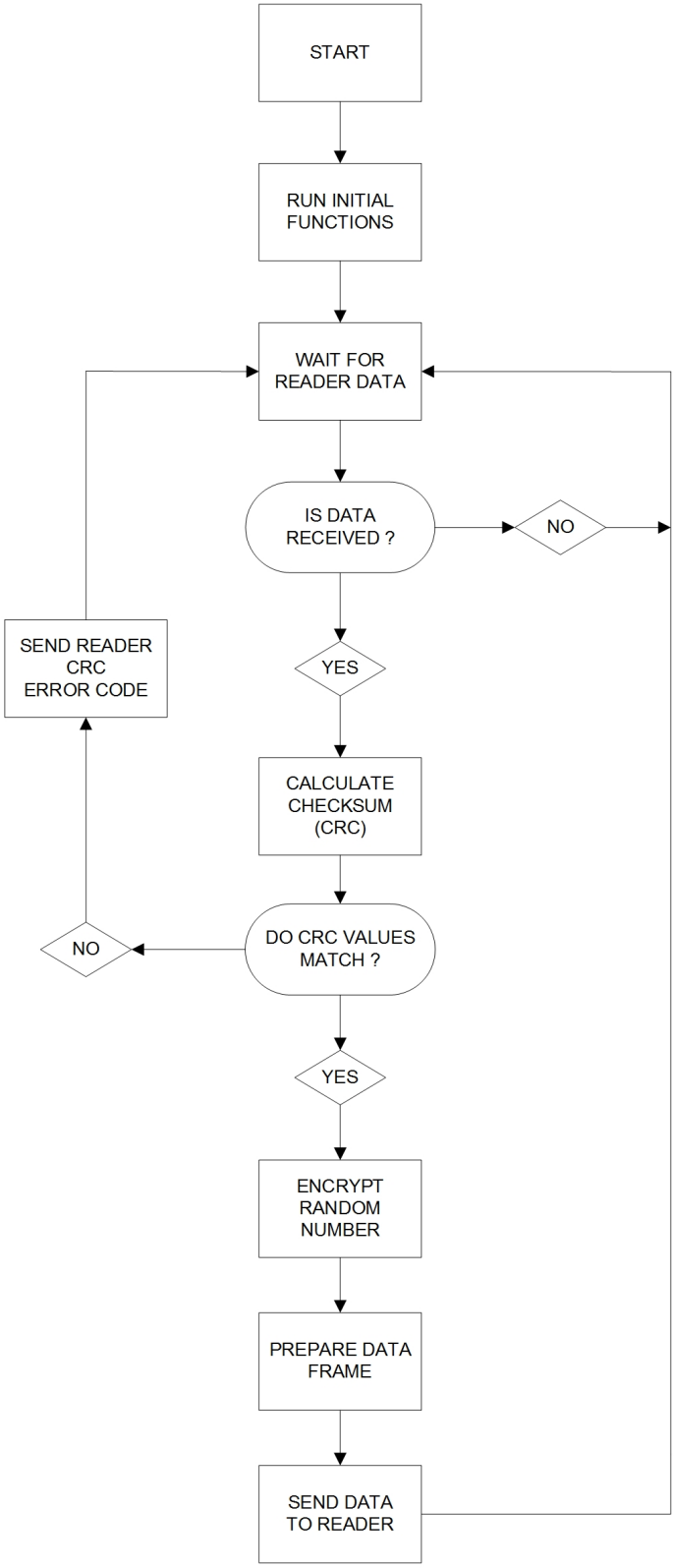


Figure 5.8: Tag algorithm flow chart block diagram.

values. If equality does not hold between two values, reader informs the tag and algorithm goes back to command II in send loop. However, as the match occurs between CRC values, reader decrypts the tag data and compares is with the data sent. Authentication ends positively in case of correct data reception. In any other cases, tag is not authenticated, reader exits the receive loop and goes back to command I in send loop.

5.4.3 Tag Algorithm

Tag is the listener device in the communication protocol. Since communication starts with the data sent by reader, tag waits for the proper signal to respond. Flow chart of the tag algorithm is given in Figure 5.8.

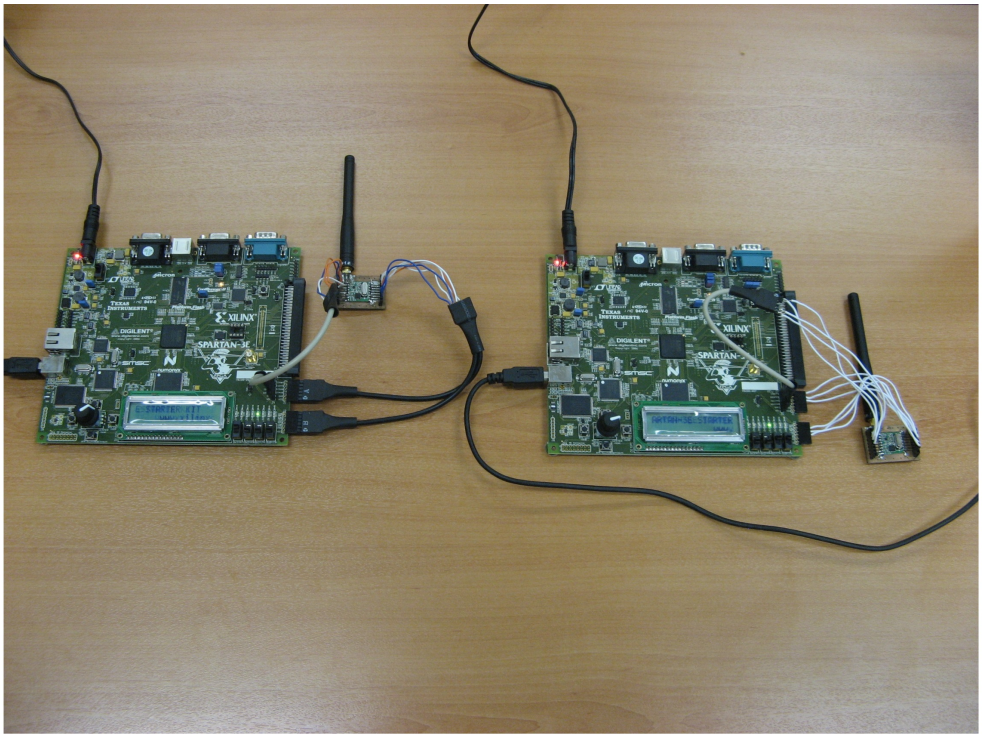


Figure 5.9: Reader and Tag Structures.

Upon running the initial functions after start command, tag starts to wait for reader data. If any 176 bit data is received, CRC checksum calculation is done and received-calculated values are compared by tag. In positive match case, 64 bit random number data sent to TEA IP Core by Microblaze, and encrypted data is saved on a buffer after the process. Then, tag prepares the data frame to send response to reader device. Just before sending, CRC value of the new data is calculated and added as last

two bytes of the frame before the EOF delimiter. Upon completing CRC operations, data is firstly sent to RFM22B and then transmitted to the reader.

5.5 Overall Design

Completed design is visible in 5.9. RFM22B modules are connected to the suitable ports of FPGA boards. To make the FPGA operate, bitmap of the designed architecture should be embedded. By embedding the reader and tag codes at each FPGA, RFID system gets ready for operation.

Indoor area communication range of the system is approximately 100m. Power supply of the RF transceivers are provided by FPGA board. Dipole antennas are used on RF modules. Output power of each transceiver is set to 100mW.

6. ATTACKS ON THE PROTOCOL

In this section of thesis, completed replay attack studies on proposed communication protocol are explained. At first, theory of attack operation is mentioned. Following, attack device design stages are explained. Lastly, attack implementations are given in details and results are reflected.

6.1 Fundamentals of Operation

The aim of the replay attacks was to spoof the reader as the original tag is in range and protocol runs correctly. In other words attacker device acted as the original tag. To accomplish the attacks, the data sent over communication between reader and tag was recorded in first phase. In second phase collected data were replayed by attacker device in the second phase.

Figure 6.1 delineates the attacking operation.

6.2 Attack Device Design

Attack device is almost same as reader and tag structures, but there is an additional personal computer (PC) stage, which is used to record and save the data for replay attacks.

6.2.1 Hardware

Attack device is formed up using RFM22B module at RF front end and Spartan3E FPGA board for baseband processes. In order to implement the proposed replay attacks, received data needed to be saved, but the memory blocks on Spartan3E board are not enough for this kind of an operation. Hence, collected data needed to be saved on external memory device. To overcome the storage problem, data received by attacker device is transferred to a PC to be stored.

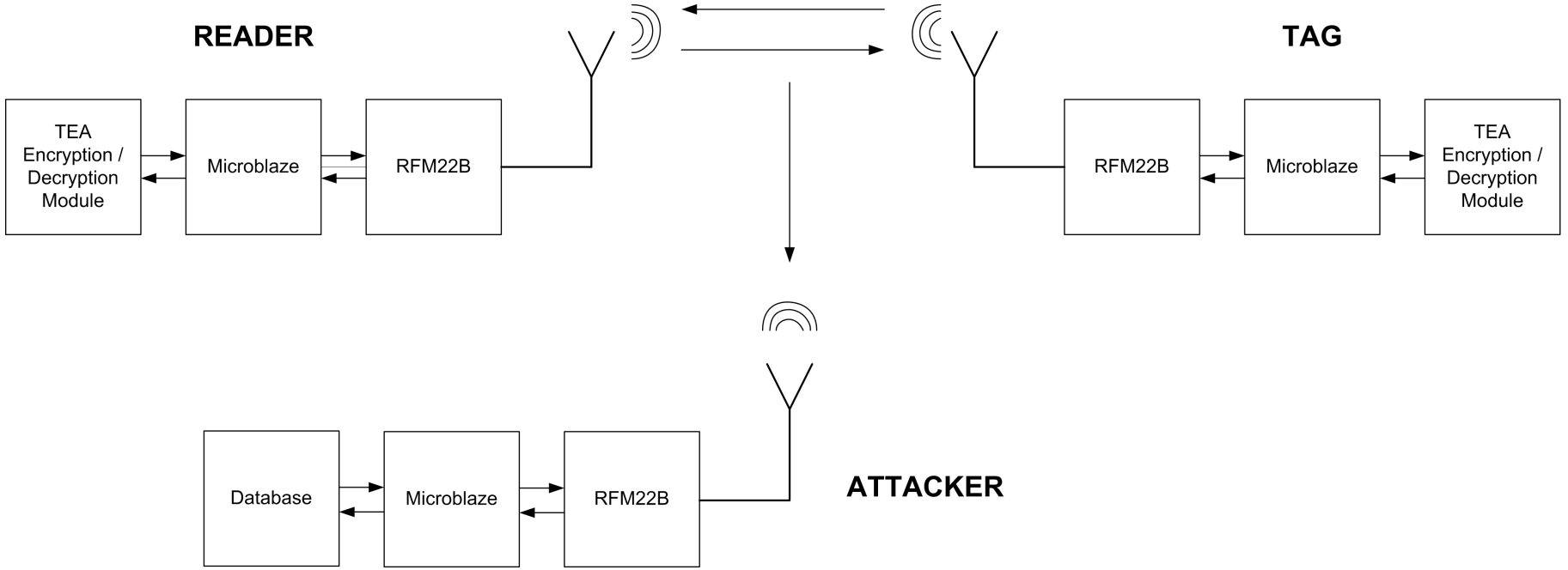


Figure 6.1: Attack setup.

RS232 communication is used to transfer data from FPGA board to PC. Serial port data received by PC is further processed by MATLAB.

6.2.2 Software

Two different code designs were implemented for both Microblaze processor of FPGA stage and MATLAB. MATLAB controls the serial port at PC stage. At first, the system is programmed to record and save the communication between reader and tag.

According to the communication protocol, reader starts the communication with the reader by sending a frame of 176 bits including 64 bits of random number. Upon receiving the data, the tag encodes the random number and sends back 168bits including 64bits of encoded data. Hence, the communication, protocol is a two way authentication protocol.

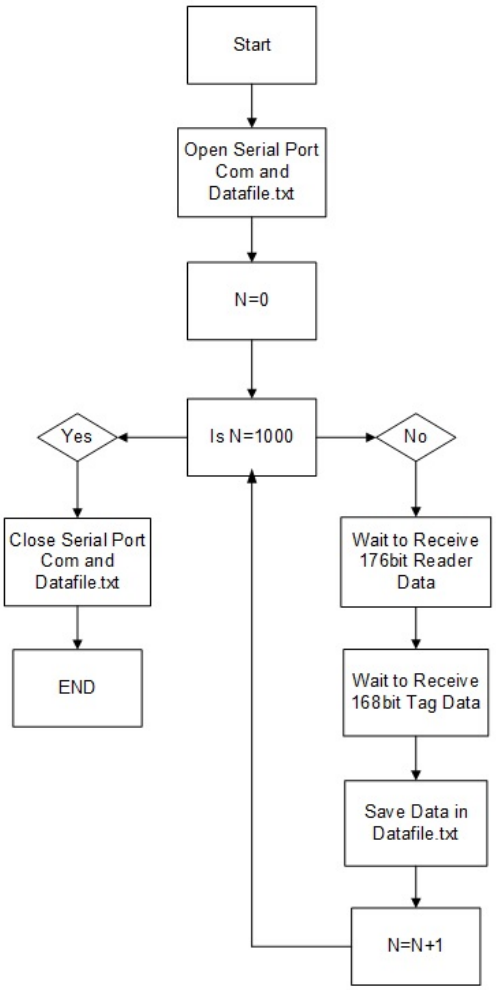


Figure 6.2: Matlab code record case flow chart.

Considering the protocol, the attacker should be capable of recording both the data sent by reader and tag and save it for a definite number of communication periods. To accomplish a replay attack by taking all probabilities into account, the communication has to be saved 2^n times where n represents the number of bits, which means saving all possible random numbers in n bit order and so forming up a complete sample context. Since n is 64 for the protocol used in this project, it means $(176bits + 168bits)2^{64}$ times, which corresponds to a huge size of data. It is not possible to record and handle so huge size of a data due to memory limitation and some precautions against replay attacks. Hence, communication record number was limited to 1000 times in this project.

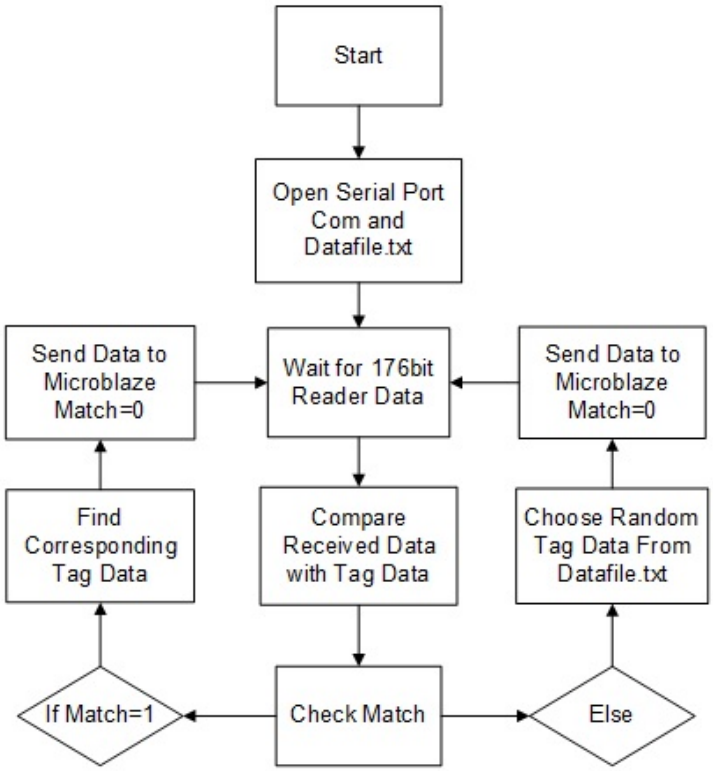


Figure 6.3: Matlab code attack case flow chart.

Figure 6.2 and 6.3 MATLAB codes for recording and saving the communication. Firstly, Microblaze waits for the interrupt from RFM22B which indicates 176 bit reader data is received. Then, reader data is sent to MATLAB over serial communication. MATLAB receives the data and saves it in a txt file called "DataFile.txt" and starts to wait for the next 168 bit tag data. Simultaneously, Microblaze, waiting for the reader data, sends it to the PC upon receiving and MATLAB saves the tag data to the same line in txt file after reader data and goes to next line for incoming data.

Table 6.1: Stored data.

Reader Data	Tag Data
r_{R1}	$E_{K1}(r_{R1})$
r_{R2}	$E_{K2}(r_{R2})$
r_{R3}	$E_{K3}(r_{R3})$
.	.
.	.
.	.
.	.
.	.
.	.
r_{R1000}	$E_{K1000}(r_{R1000})$

In second part, Microblaze and MATLAB were programmed to realize replay attacks. In this action, attacker waits for reader to send the data with the random number. When the data is received by attacker, it is directly sent to MATLAB and compared with the previously saved reader data. If the data matches with stored data, then MATLAB sends the corresponding tag data to Microblaze. At last, Microblaze sends it to reader and waits for authentication.

6.3 Replay Attacks and Results

Attacks were accomplished two times with different communication distances between reader and attacker in indoor environment.

6.3.1 Short range attacks

In short range attack applications, the distance between reader and attacker device was 3 meters with a clear line of sight (LOS). The devices were performing in office environment. Since the distance between devices is very short, possible reflection sources were underestimated.

Replay attacks were carried out 10 times. Each specific time, 176 bit r_R data sent by the reader is received by attacker device and compared with the previously saved data in database. The comparisons did not match any time and in this case, attacker device returned a random tag data, $E_{Kn}(r_{Rn})$, from the database to reader as reply. Unfortunately returned tag data was denied at reader stage at all trials. Since the CRC

check failed all time, reader did not further continue to process the received tag data and resend reader data to the receivers around, which is only the attacker device in this case.

6.3.2 Long Range Attacks

During the long range attack applications, attacker device was placed in a different room where the LOS was absent. The placement configuration is seen below.

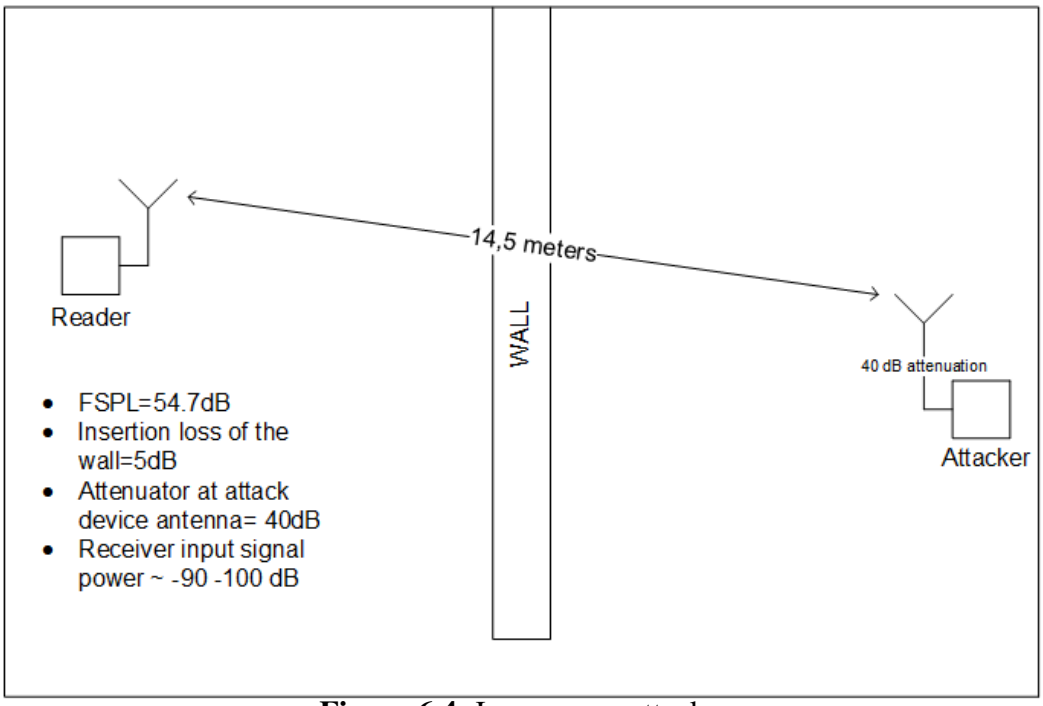


Figure 6.4: Long range attacks.

At frequency of operation, calculated free space path loss is 54.7dB. If the reader outputs max power level signals, which is 20dBm, the power level of the signal at attack device antenna would be $-34.7dBm$. Also, considering the losses caused by the wall, which is approximately 5dB, power level becomes $-40dBm$. Under these conditions, it is observed that the system can operate normally without any change in the operation.

To find the minimum signal level attacker can operate, signal attenuators were connected to attack device antenna in an increasing order. Starting from 10dB, attenuation level was increased to 40dB by time. Attacker was still able to receive reader signals without error, analyze and respond back till 40dB attenuation. But if the attenuation level was increased more, errors were observed in data received by attack

device. The reason of the errors in received data is the receive sensitivity level of the attacker front-end. Since the level was reached, data was not received properly by the device.

As seen in the Table 6.2, there is 40dB difference between receive sensitivity level of transceiver module and received signal level. Possibly, the reason of the difference is reflections caused by walls, metal stuff and etc. in the area of experiment. Moreover, another option is the existence of a signal source operating in close frequency range.

Table 6.2: Link budget calculation.

Source	**Level**
Output power	20dBm
FSPL	$-54.7dB$
Attenuation on wall	$-5dB$
Attenuation at receiver	$-40dB$
Received signal power	$-80dBm$
Receive sensitivity	$-120dBm$
Received signal power	$-80dBm$
Losses caused by other sources	40dB

Long range attack studies were completed in mentioned conditions, when the original tag was out of communication. Process of the attack is the same as in short range attacks. r_R data sent by the reader is received and compared with stored data. If there is a match, corresponding tag data is sent. Attack was handled 10 different times, but the result was negative. No matching occurred between the reader data and stored data. Therefore, authentication failed.

6.4 Possible Precautions

Some simple countermeasures exist in RFID as solutions to protocol or system security against replay attacks.

6.4.1 Timestamps

Use of timestamps within transmitted data frame stands as the easiest solution. In this technique, reader attaches time information to the transmitted data which relates the time of transmission. Tag do not changes the time information but places the

information in the response frame. Upon receiving the tag data, reader checks for the time variant parameter and compares it with the receive time value. If $\Delta t \leq t'$ equality holds, where t' represents the pre defined max possible communication duration, the reader evaluates the received information. In other cases, the tag is not authenticated.

Timestamps might be implemented using any other techniques to provide more security. Moreover, use of encrypted timestamps provides higher security in protocols against several attacks as replay and counterfeiting, but the system must be capable of meeting the computational power requirements in such a case.

6.4.2 RF Directivity

Another approach is the use of RF shielding on readers in order to limit the directionality of radio signals. In a simple case, radio waves propagate to any direction from the antenna with power levels in any direction proportional to directivity of the transmitting antenna. In this cases, an adversary with very low receive sensitivity might eavesdrop the communication from long distances. However, by applying shielding techniques in reader and tag structures and increasing the propagation directivity of transmitted waves, omnidirectional propagation might be prevented. Thus, communication security can be increased against eavesdropping and replay attacks.

6.4.3 Received Signal Strength Indication (RSSI)

RSSI is basicly a technique used in RF systems and calculations to indicate the power level of received signal. RSSI technique might be used to increase the security in RFID systems against attacks. RSSI information could definitely be used in order to make a discrimination between authorized and unauthorized readers or tags and subsequently mitigate replay attacks. Otherwise, reader decides that However to apply the technique, readers might be capable of indicating received signal strength, which increases the design cost.

7. CONCLUSION AND FUTURE STUDIES

Security and privacy are main blockades in front of radio frequency application systems being injected into daily life. RFID systems are widely being used in every corner of life nowadays. While large retail companies use RFID systems to control live stocks and supply chains, companies and even high schools started to use RFID tags to control workers and students in work hours. In most cases, given tags carry important personal information or critical reports about the products in the stock. Vulnerability of the protocols used by mentioned systems against attacks, leads to a decrease in trust to the technology. Having known the fact, scientists have completed thousands of different research studies on increasing the security in RFID protocols. Large number of new protocols were developed and great efforts were given on strengthening the weak points of the protocols. Moreover, very important cryptographic algorithm were also developed by designers to increase data security in RFID systems. However, research and development on design of more secure RFID systems is required.

Under consideration of above mentioned facts, design and implementation of an UHF RFID system was accomplished in first phase of the thesis, by proposing new reader and transponder structures. Active tag architecture was preferred in system design to keep the communication range long and security level high. As a result of detailed investigation of RFID frequency bands and regulations, frequency of operation was selected in UHF band. Low frequency systems are generally Near-Field Communication systems and maximum allowed communication range in specified ISM bands is very low. Therefore, 868 MHz center frequency is selected for system operation considering European UHF band RFID regulations. RFM22B transceiver modules were decided on and used for RF front-end stages of reader and tag taking into low power consumption and flexible operating features.

Spartan3E Starter FPGA boards formed up microcontroller part of designed reader and tag to keep the computational power substantially high. A communication protocol

with two way authentication mechanism was used between receiver and transmitter devices. In the protocol, reader sends 64 byte random number to the tag without encryption. Received data is then encrypted by tag and sent back to the reader. Upon receiving the tag data, reader does the decryption and compares it with sent data. If the match is positive, tag is authenticated, else not. Tiny Encryption Algorithm was preferred in the design to secure the transmitted data. As a result, a secure RFID system with 64 byte authentication procedure is implemented.

In second part, attack studies were held on designed system. The aim of the attacks were to impersonate the original tag with attack device and convince the reader that original tag is in range of communication. To accomplish replay attacks, an attack device similar to the reader and tag architecture, was designed and prepared for operation. Firstly, reader and tag data was listened by attack device and sent to a personal computer for storage over serial communication link. Later on, stored data is replayed back to the reader when the original tag was out of communication range. Reader data was received by attack device, sent to MATLAB for comparison with stored data and if there was a match, corresponding 168 bit reader data was replayed back. If the match fails, a random tag data was replayed back to the reader.

Attack studies were carried out two times with different distances between reader and attacker. First case was short range attacks, where the distance between reader and attacker was 3m in distance with clear line of sight. Attacker listened to reader 10 times and compared received data with the previously saved data, but the match was negative. Random tag data was sent back to the reader had failed in authentication. It was proven that proposed system is secure against short range replay attacks.

In second case, long range attacks were carried out, where the receive sensitivity limit of the receiver was reached. Long range attacks were done in same procedure as short range attacks. Every time authentication failed and the result of the attacks was negative. It was proven that proposed system is secure against long range replay attacks.

All in all, a secure RFID system was designed, implemented and system security against replay attacks from short and long ranges was proven. Designed system can be used in long range identification systems with high security needs.

Completed study is a part of TUBITAK project named Design and Implementation of A Secure RFID System. In future steps of the study, new attack scenarios will be prepared against the system and trials will be completed. Hence system security against different RFID attacks will be seen and possible precautions will be taken.

REFERENCES

[1] **Hong Li, Y.C.**, 2006. Security and privacy aspects of low-cost radio frequency identification systems, Security in Pervasive Computing, SPC, 2003. in Proceedings of International Conference on, pp.4 pp.–.

[2] **Dobkin, D.M.**, 2006. The RF in RFID, Elsevier Inc.

[3] **Juels, A.**, Feb. 2006. RFID Security and Privacy: A Research Survey, *Selected Areas in Communications, IEEE Journal on*, **24(2)**, 381 – 394.

[4] **Finkenzeller, K.**, 2010. RFID Handbook, John Wiley & Sons, Ltd., 3. edition.

[5] **Thornton, F.**, **Haines, B.**, **Das, M.A.**, **Bhargava, H.**, **Campbell, A. and Kleinschnidt, J.**, 2006. RFID Security, Syngress Publishing, Inc.

[6] **Feldhofer, M.**, 2004. An Authentication Protocol in a Security Layer for RFID Smart Tags, Proceedings of The 12th IEEE Mediterranean Electrotechnical Conference (MELECON), volume 2, IEEE, Dubrovnik, Croatia, pp.759 – 762.

[7] **Das, R.**, `http://www.piworld.com`, accessed on: 2013.04.24.

[8] **Garrets, T.**, `http://www.cs.rit.edu/~ark/spring2010/482/team/u9/report.pdf`, accessed on: 2013.07.30.

[9] **Xiao, M.**, **Shen, X.**, **Wang, J. and Crop, J.**, 2011. Design of a UHF RFID tag baseband with the hummingbird cryptographic engine, ASIC (ASICON), 2011 IEEE 9th International Conference on, pp.800–803.

[10] **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, Springer-Verlag, pp.201–212.

[11] **Ohkubo, M.**, **Suzuki, K. and Kinoshita, S.**, 2003. Cryptographic Approach to "Privacy-Friendly" Tags, IN RFID PRIVACY WORKSHOP.

[12] **Lee, Y.C.**, **Hsieh, Y.C.**, **You, P.S. and Chen, T.C.**, 2008. An Improvement on RFID Authentication Protocol with Privacy Protection, Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on, volume 2, pp.569–573.

[13] **Heng, L.**, **Fei, G.**, **Yanming, X. and Shuo, F.**, 2010. Research of RFID Authentication Protocol Based on Hash Function, **Q. Luo**, editor, Advances in Wireless Networks and Information Systems, volume 72 of *Lecture*

Notes in Electrical Engineering, Springer Berlin Heidelberg, pp.177–182, http://dx.doi.org/10.1007/978-3-642-14350-2_22.

[14] **Chien, H.Y.**, 2007. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity, *Dependable and Secure Computing, IEEE Transactions on*, **4(4)**, 337–340.

[15] **Blum, M.**, 2001. Secure human identification protocols, In Asiacrypt, Springer, pp.52–66.

[16] **Juels, A. and Weis, S.A.**, 2005. Authenticating Pervasive Devices with Human Protocols, Springer-Verlag, pp.293–308.

[17] **Gilbert, H.**, **Robshaw, M. and Sibert, H.**, 2005. Active attack against HB+: a provably secure lightweight authentication protocol, *Electronics Letters*, **41(21)**, 1169–1170.

[18] **Katz, J.**, **Sun, J. and Smith, S.A.**, 2010. Parallel and concurrent security of the HB and HB+ protocols, *Journal of Cryptology*.

[19] **Bringer, J.**, **Chabanne, H. and Dottax, E.**, 2005. HB++: a Lightweight Authentication Protocol Secure against Some Attacks, *IACR Cryptology ePrint Archive*, 440–440.

[20] **Piramuthu, S.**, 2006. HB and related lightweight authentication protocols for secure RFID tag/reader authentication, In CollECTeR 2006.

[21] **Munilla, J. and Peinado, A.**, 2007. HB-MP: A further step in the HB-family of lightweight authentication protocols, *Computer Networks*, **51(9)**, 2262 – 2267, http://www.sciencedirect.com/science/article/pii/S1389128607000242, <ce:title>(1) Advances in Smart Cards and (2) Topics in Wireless Broadband Systems</ce:title>.

[22] **Leng, X.**, **Mayes, K. and Markantonakis, K.**, 2008. HB-MP+ Protocol: An Improvement on the HB-MP Protocol, RFID, 2008 IEEE International Conference on, pp.118–124.

[23] **Yoon, B.**, **Sung, M.Y.**, **Yeon, S.**, **Oh, H.**, **Kwon, Y.**, **Kim, C. and Kim, K.H.**, 2009. HB-MP++ protocol: An ultra light-weight authentication protocol for RFID system, RFID, 2009 IEEE International Conference on, pp.186–191.

[24] **Gilbert, H.**, **Robshaw, M.J.B. and Seurin, Y.** Hb#: Increasing the security and efficiency of hb, of LNCS, Springer, pp.361–378.

[25] **Safkhani, M.**, **Bagheri, N.**, **Naderi, M.**, **Luo, Y. and Chai, Q.**, 2011. Tag Impersonation Attack on Two RFID Mutual Authentication Protocols, Availability, Reliability and Security (ARES), 2011 Sixth International Conference on, pp.581–584.

[26] **Tan, C.**, **Sheng, B. and Li, Q.**, 2008. Secure and Serverless RFID Authentication and Search Protocols, *Wireless Communications, IEEE Transactions on*, **7(4)**, 1400–1407.

[27] **Xueping, R. and Xianghua, X.**, 2010. A Mutual Authentication Protocol for Low-Cost RFID System, Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific, pp.632–636.

[28] **Sun, H.M. and Ting, W.C.**, 2009. A Gen2-Based RFID Authentication Protocol for Security and Privacy, *Mobile Computing, IEEE Transactions on*, **8(8)**, 1052–1062.

[29] **Peris-Lopez, P.**, **Hernandez-Castro, J.**, **Tapiador, J. and Ribagorda, A.**, 2009. Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol, **K.I. Chung**, **K. Sohn and M. Yung**, editors, Information Security Applications, volume5379 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, pp.56–68, `http://dx.doi.org/10.1007/978-3-642-00306-6_5`.

[30] **Cho, J.S.**, **Yeo, S.S. and Kim, S.K.**, 2011. Securing against brute-force attack: A hash-based {RFID} mutual authentication protocol using a secret value, *Computer Communications*, **34(3)**, 391 – 397, `http://www.sciencedirect.com/science/article/pii/S0140366410001040`, <ce:title>Special Issue of Computer Communications on Information and Future Communication Security</ce:title>.

[31] **Chien, H.Y.**, 2006. Secure Access Control Schemes for RFID Systems with Anonymity, Mobile Data Management, 2006. MDM 2006. 7th International Conference on, pp.96–96.

[32] **Song, B. and Mitchell, C.J.**, 2008. RFID authentication protocol for low-cost tags, Proceedings of the first ACM conference on Wireless network security, WiSec '08, ACM, New York, NY, USA, pp.140–147, `http://doi.acm.org/10.1145/1352533.1352556`.

[33] **Chen, Y.Y.**, **Tsai, M.L. and Jan, J.K.**, 2011. The design of {RFID} access control protocol using the strategy of indefinite-index and challenge-response, *Computer Communications*, **34(3)**, 250 – 256, `http://www.sciencedirect.com/science/article/pii/S0140366410002471`, <ce:title>Special Issue of Computer Communications on Information and Future Communication Security</ce:title>.

[34] **Sadighian, A. and Jalili, R.**, 2009. AFMAP: Anonymous Forward-Secure Mutual Authentication Protocols for RFID Systems, Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on, pp.31–36.

[35] **Sadighian, A. and Jalili, R.**, 2008. FLMAP: A fast lightweight mutual authentication protocol for RFID systems, Networks, 2008. ICON 2008. 16th IEEE International Conference on, pp.1–6.

[36] **Phan, R.W.**, 2009. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol x02014;SASI, *Dependable and Secure Computing, IEEE Transactions on*, **6(4)**, 316–320.

[37] **Li, T. and Deng, R.**, 2007. Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol, Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on, pp.238–245.

[38] **Safkhani, M. and Naderi, M.**, 2010. Cryptanalysis and Improvement of a Lightweight Mutual Authentication Protocol for RFID system, Information Security and Cryptology 2010(ISCISC'10). In7th International ISC Conference on,, pp.57–59.

[39] **Safkhani, M., Naderi, M. and Bagheri, N.**, 2010. Cryptanalysis of AFMAP, *IEICE Electronics Express*, **7(17)**, 1240–1245, `http://ci.nii.ac.jp/naid/130000324248/en/`.

[40] **M. Safkhani, M.N. and F.Rashvand, H.**, 2010. Cryptanalysis of the Fast Lightweight Mutual Authentication Protocol (FLMAP), *International Journal of Computer & Communication Technology (IJCCT)*, **2(2,3,4)**, 182–186.

[41] **Rizomiliotis, P., Rekleitis, E. and Gritzalis, S.**, 2009. Security analysis of the song-mitchell authentication protocol for low-cost RFID tags, *Communications Letters, IEEE*, **13(4)**, 274–276.

[42] **Safkhani, M., Bagheri, N. and Naderi, M.**, 2011. Cryptanalysis of Chen et al.'s RFID Access Control Protocol., *IACR Cryptology ePrint Archive*, **2011**, 194, `http://dblp.uni-trier.de/db/journals/iacr/iacr2011.html#SafkhaniBN11`.

[43] **Israsena, P.**, 2006. Securing ubiquitous and low-cost RFID using Tiny Encryption Algorithm, Wireless Pervasive Computing, 2006 1st International Symposium on, pp.4 pp.–.

[44] **M. B. Abdelhalim, M. El-Mahallawy, M.A. and Elhennawy, A.**, March/June 2012. Design & Implementation of an Encryption Algorithm for use in RFID System, *RFID Security and Cryptography (IJRFIDSC). International Journal of,*, **1(1/2)**, 51–57.

[45] **Abawajy, J.**, 2009. Enhancing RFID Tag Resistance against Cloning Attack, Network and System Security, 2009. NSS '09. Third International Conference on, pp.18–23.

[46] **Liu, Y.**, 2008. An Efficient RFID Authentication Protocol for Low-Cost Tags, Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on, volume 2, pp.180–185.

[47] **Chien, H.Y.**, **Lee, C.I.**, **Chen, S.K. and Hou, H.P.**, 2011. New RFID Authentication Protocol with DOS-attack Resistance, Parallel and Distributed Systems (ICPADS), 2011 IEEE 17th International Conference on, pp.605–609.

[48] **Gao, L.**, **Ma, M.**, **Shu, Y. and Liu, C.**, 2011. RFID security protocol trace attack and desynchronizing attack deep research, Computer Science and Network Technology (ICCSNT), 2011 International Conference on, volume 2, pp.918–922.

[49] **Akgun, M.**, **Caglayan, M. and Anarim, E.**, 2009. A new RFID authentication protocol with resistance to server impersonation, Parallel Distributed Processing, 2009. IPDPS 2009. IEEE International Symposium on, pp.1–8.

[50] **Karabat, C.**, 2009. A Novel Secure RFID System to Ensure Privacy, Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP '09. Fifth International Conference on, pp.442–445.

[51] **Chen, C.**, **Qian, Z.**, **You, I.**, **Hong, J. and Lu, S.**, 2011. ACSP: A Novel Security Protocol against Counting Attack for UHF RFID Systems, Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on, pp.100–105.

[52] **Chung, H. and Miri, A.**, 2012. On the hardware design and implementation of a chaos-based RFID authentication and watermarking scheme, Information Science, Signal Processing and their Applications (ISSPA), 2012 11th International Conference on, pp.460–465.

[53] **Morshed, M.**, **Atkins, A. and Yu, H.**, 2012. Efficient mutual authentication protocol for radiofrequency identification systems, *Communications, IET*, **6(16)**, 2715–2724.

[54] **Devadas, S.**, **Suh, E.**, **Paral, S.**, **Sowell, R.**, **Ziola, T. and Khandelwal, V.**, 2008. Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications, RFID, 2008 IEEE International Conference on, pp.58–64.

[55] **Dowla, F.U.**, 2003. Handbook of RF & Wireless Technologies, Newnes Pubblications.

[56] **Seybold, J.S.**, 2005. Introduction to RF Propagation, John Wiley & Sons, Inc., 1. edition.

[57] **Editorial, A.T.**, How do i measure bit error rate (BER) to a given confidence level on N490xA/B serial BERTs?, `http://www.radio-electronics.com/info/rf-technology-design/index.php`, accessed on: 2013.04.25.

[58] **Poole, I.**, BER Bit Error Rate Tutorial and Definition, `http://www.radio-electronics.com`, accessed on: 2013.09.07.

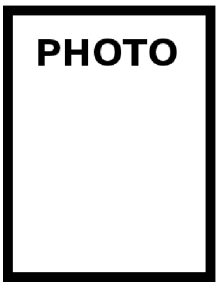
[59] **Lopez, P.P.e.a.**, 2009. Attacking RFID Systems, Taylor & Francis Group.

[60] **Kravets, D.**, `http://www.wired.com`, accessed on: 2013.04.26.

[61] **Mitrokotsa, A., R.M.R. and Tanenbaum, A.S.**, 2008. Classification of RFID Attacks, Proceedings of the Second International Workshop on RFID Technology, pp.73–86.

[62] **Tanenbaum, A.**, `http://www.cs.vu.nl/~ast/ov-chip-card/`, accessed on: 2013.04.27.

CURRICULUM VITAE



Name Surname: Okan Emre Özen

Place and Date of Birth: Zonguldak, 30.03.1988

Adress: Beyazevler Mahallesi 557 Sok. No:21 Gaziemir / İzmir

E-Mail: okanemreozen@gmail.com

B.Sc.: Electronics Engineering Undergraduate Programme, Istanbul Technical University

M.Sc.: Electronics Engineering Master Programme, Istanbul Technical University

List of Publications and Patents:

Ozen, O.E., et al., Design and Implementation of a High Linearity Low Noise Amplifier for 1.57 GHz GPS Applications, Mediterranean Microwave Symposium (MMS 2012), Sept 2-5, 2012, Istanbul / Turkiye

Ozen, O.E., et al., TURKSAT-3USAT Satellite Computer Design and Satellite Management System, 9th International Acedemy of Astronautics Symposium on Small Satellite for Earth Observation (IAA), April 08-02 2013, Berlin / Germany

Ozen, O.E., et al., High Gain, Linear, Low Cost, Digitally Controlled VHF-UHF Analog Transponder for Nano Satellites, 2013 Asia-Pacific Microwave Conference, November 5-8, 2013, Seoul / South Korea

PUBLICATIONS/PRESENTATIONS ON THE THESIS

- Özen, O. E., Örs, S.B., and Yağcı, H. B., 2013: Design and Implementation of a Secure RFID System on FPGA *21. IEEE Sinyal İşleme ve İletişim Uygulamaları Kurultayı*, April 24-26, 2013 Girne, Northern Cyprus Turkish Republic.