

The Integration of IEEE 802.11 (WLAN) with RFID Systems in ISM (2.45 GHz) Frequency Band Environment using Framed Slotted ALOHA and IEEE 802.15.4

by

Haleh Khojasteh

Bachelor of Science, Shahid Beheshti University, Iran, 1997

A thesis presented to
The Faculty of Graduate Studies of
Ryerson University
in partial fulfillment of the requirements
of the degree of

Master of Science

Department of Computer Science
Ryerson University
Toronto, Ontario, Canada, 2011

©Haleh Khojasteh 2011

Author's Declaration

I hereby declare that I am the sole author of this thesis.

I authorize Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

Signed:_____

I further authorize Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Signed:_____

The Integration of IEEE 802.11 (WLAN) with RFID Systems in ISM (2.45 GHz)
Frequency Band Environment using Framed Slotted ALOHA and IEEE 802.15.4

Master of Science 2011

Haleh Khojasteh

Computer Science

Ryerson University

Abstract

In this thesis, we attempt to solve the problem of WLAN/RFID coexistence and integration in frequency band of 2.45 GHz or ISM band. Our solution to this problem is to allow the WLAN access and RFID access in a time-sharing manner by making the WLAN Access Point aware of the RFID neighbor-network at MAC layer. The time-sharing function is implemented using IEEE 802.11 PCF mechanism. RFID network is implemented using two different standards. The first one is Framed Slotted Aloha standard and the second one is IEEE 802.15.4 standard. We have simulated both models using Artifex simulator and compared their performance using some performance metrics like collision probability and average number of collision in each superframe. It is shown that IEEE 802.15.4 based model outperforms the Framed Slotted Aloha based model.

Contents

Author's Declaration	iii
Abstract	v
Table of Contents	viii
List of Figures	ix
List of Tables	xi
Acknowledgments	xiii
Dedication	xv
1 Introduction	1
2 Related Work and Background	6
2.1 RFID	9
2.1.1 Coupling Techniques	10
Near-Field Coupling	10
Far-Field Coupling	12
2.1.2 Tag Memory	15
2.1.3 Programming Interface	15
2.1.4 The Life Cycle of a Typical RFID Tag	17
The calculations of sleeping period and probability	18
2.1.5 Anti-collision protocol for RFID network: Framed Slotted Aloha	19
Pure Aloha Protocol	20
Slotted Aloha Protocol	20
Framed Slotted Aloha Protocol	23
2.1.6 Anti-collision protocol for RFID network: IEEE 802.15.4 . . .	26
Slotted CSMA-CA Medium Access	29
Uplink and Downlink Communication in Beacon Enabled Mode	33
2.2 IEEE 802.11 DCF	37
2.3 Point Coordination Function (PCF)	42
3 The Proposed Solution and Simulation Model	46
3.1 Time schedule in the proposed solution	50

3.2	Basic Parameters and Calculations of Solution	53
3.2.1	Parameters for Wi-Fi and IEEE 802.15.4	53
	Tags' Sleeping Patterns and Parameters	55
3.2.2	Parameters for Framed Slotted Aloha	56
	Tags' Access Probability	56
	Tags' Sleeping Patterns and Parameters	58
	Tags' Collision Probability	58
3.3	The Simulation Model	61
3.3.1	Access Point	64
3.3.2	Wi-Fi Medium	66
3.3.3	Wi-Fi Device	67
3.3.4	RFID Reader	71
3.3.5	RFID Medium	74
3.3.6	RFID Tag: Framed Slotted Aloha version	75
3.3.7	RFID Tag: IEEE 802.15.4	78
4	Simulation Results and Analysis	82
4.1	Simulation Results of both models for the First Scenario	84
4.2	Simulation Results of both models for the second scenario	89
5	Conclusion	94
A	Abbreviations	97
	Bibliography	106

List of Figures

1.1	WLAN/RFID coexistence.	3
2.1	The channel assignment of 802.11b and 802.15.4 networks.	7
2.2	Near-field communication using inductive coupling [8].	11
2.3	Different types of near-field RFID tags [8].	12
2.4	Different types of far-field RFID tags [8].	13
2.5	The life cycle of a typical tag.	18
2.6	Structure of the superframe in beacon enabled mode [27].	28
2.7	Operation of the slotted CSMA-CA algorithm [27].	31
2.8	Uplink packet transmission, beacon enabled mode [27].	34
2.9	Downlink packet transmission, beacon enabled mode [27].	36
2.10	Example of basic access mechanism [6].	40
2.11	RTS/CTS Access Mechanism [6].	41
2.12	MAC Architecture of IEEE 802.11 [3].	42
2.13	Example of PCF frame transfer [3].	43
2.14	CFP/CP alternation [3].	44
3.1	The overview of proposed topology.	47
3.2	The overall of proposed solution.	51
3.3	A typical cycle in the proposed solution.	52
3.4	An example of $P_{slot[k]}$	60
3.5	The overview of simulated model and its classes.	62
3.6	Main page of simulation.	63
3.7	Measurement page.	64
3.8	Access point class.	65
3.9	Wi-Fi medium class.	67
3.10	Wi-Fi device: Main page.	68
3.11	Wi-Fi device: Data generating and waiting page.	69
3.12	Wi-Fi device: CSMA/CA page.	71
3.13	RFID reader: Main page.	72
3.14	RFID reader: Data generating and waiting page.	73

3.15	RFID reader: CSMA/CA page.	74
3.16	RFID medium class.	75
3.17	RFID tag: Main page for Framed Slotted Aloha.	76
3.18	RFID tag: Data generating and waiting page for FSA.	77
3.19	RFID tag: Anti Collision page for Framed Slotted Aloha.	78
3.20	RFID tag: Main page.	79
3.21	RFID tag: Data generating and waiting page.	80
3.22	RFID tag: CSMA page.	81
4.1	Simulation results for the first scenario: Collision probability.	85
4.2	Simulation results for the first scenario: Average no. of collisions. . .	85
4.3	Simulation results for the first scenario: Average waiting time of tags. .	86
4.4	Simulation results for the first scenario: Average no. of awoken tags. .	86
4.5	Simulation results for the first scenario: Average collision position. . .	87
4.6	Simulation results for the first scenario: Average sucessful position. .	88
4.7	Simulation results for the second scenario: Collision probability. . . .	89
4.8	Simulation results for the second scenario: Average no. of collisions. .	90
4.9	Simulation results for the second scenario: Average waiting time of tags. .	91
4.10	Simulation results for the second scenario: Average no. of awoken tags. .	91
4.11	Simulation results for the second scenario: Average collision position. .	92
4.12	Simulation results for the second scenario: Average sucessful position. .	92

List of Tables

2.1	Frequency characteristics of RFID systems [8].	14
2.2	An example of Framed slotted Aloha protocol [41].	25
2.3	Timing parameters in beacon enabled operating mode [27].	29
2.4	Defined Timings for IEEE 802.11 Standard [6].	38
3.1	Timing parameters in beacon enabled operating mode [27].	54
3.2	Sleeping parameters for ZigBee protocol.	55
3.3	Basic parameters for ZigBee and Framed Slotted Aloha protocols. . .	56
3.4	Sleeping parameters for Framed Slotted Aloha.	58

Acknowledgments

My utmost gratitude goes to my supervisor, Dr. Jelena Mišić for accepting me as her Master's student and guiding me with patience and encouragement. She has been abundantly helpful and has assisted me in numerous ways. Without her continual support and thoughtful mentoring, this thesis would not be possible.

Furthermore, I would like to appreciate Dr. Vojislav B. Mišić for his valuable ideas and advices on my simulation problems and Artifex simulator issues.

Moreover, my appreciation goes to my friends in our lab who were there when I needed help.

I dedicate this thesis to my family: my husband, my son and my parents who supported me unconditionally and have been the source of motivation and inspiration for me and made my time more enjoyable during past couple of years.

To my beloved family for their kindness and encouragement.

Chapter 1

Introduction

Radio Frequency Identification (RFID) systems and WLANs are emerging as two of the most ubiquitous computing technologies due to their important advantages and their broad applicability. RFID communication is fast, convenient and its application can substantially save some time, improve the services, reduce the labor cost, reduce the possibility of fraudulent copies of product and theft, increase the productivity gains and maintain the quality standards. Common applications are highway toll collection, transport payment, supply chain management, public transportation, tracking in mines, controlling building access, animal tracking (livestock ID), smart home appliance development and remote keyless entry development for automobiles (i.e. automotive security), e-passports, automated libraries, health care and locating children. RFID systems are mainly used to identify objects or to track their location without providing any indication about the physical condition of the object [41]. RFID uses the Radio Frequency (RF) technology for establishing the communication among its nodes, including the reader and tags. The complete definition of these

nodes along with their communication mechanism is presented in Chapter 2.

On the other hand, a wireless local area network (WLAN) is a flexible data communications system that can use either infrared or Radio Frequency (RF) technology to transmit and receive information over the air. A typical wireless LAN comprises of an Access Point (AP) and Network Interface Card (NIC) installed on the wireless device in that area. The AP is essentially the wireless equivalent of a LAN hub in wired networks. An AP is typically connected with the wired backbone through a standard Ethernet cable, and communicates with wireless devices by means of an antenna. The coverage area of the AP determines the boundary of the LAN (Local Area Network) and it forms a cell. The size of the cell depends on the strength of the propagated infrared or radio signal and some other environmental features.

Therefore from the two last paragraphs, we can conclude that nowadays, there are several different wireless networks available in the same vicinity and in Radio Frequency based technologies, air is used as the common medium. Using this common medium has its own advantages, whereas it can also cause interference among networks. Interference issue has been a source of motivation for establishing or presenting several practical models, industrial developments and reports and academic articles and consequently, it is saving hot topics for presenting remarkable theses. Interference can occur in different frequency bands which are unlicensed and not pre-assigned to specific networks or systems.

The scope of this thesis is 2.45 GHz frequency band which is also known as Industrial, Scientific and Medical (ISM) band. ISM band is an unlicensed frequency band and different networks can use this free frequency band for their signal trans-

mission. Thus, interference is probable in this frequency range. The following thesis is specifically suggesting a solution for Wi-Fi and RFID network coexistence issue in the mentioned frequency band. With our model, we are trying to decrease the number of collided signals in these networks.

The most important parameter for evaluating RFID system performance is tag range which is the maximum distance a RFID reader can either read or write information at the tag. Tag range can be strongly affected by interference from other wireless networks, especially Wi-Fi WLANs due to their large transmission power and transmission range that can exceed hundred meters. In Figure 1.1, the coexistence of WLAN and RFID networks has been displayed.

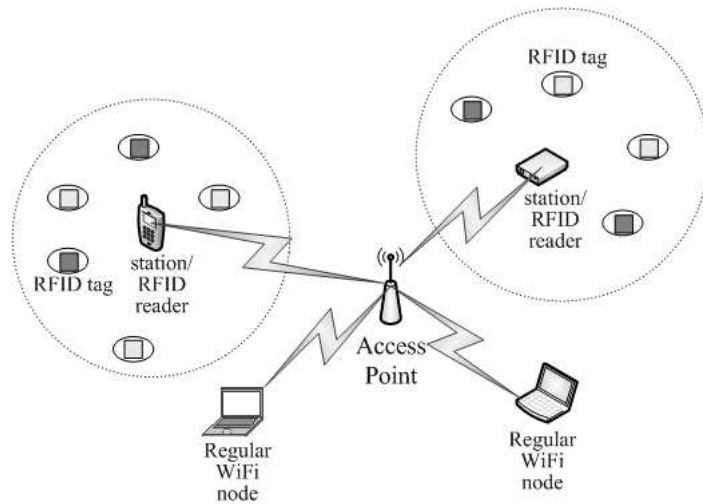


Figure 1.1: WLAN/RFID coexistence.

In our project, we attempt to solve the problem of WLAN/RFID coexistence and integration in frequency band of 2.45 GHz or Industrial, Scientific and Medical (ISM) band. In other words, we are willing to propose a way to allow fast and

accurate RFID tag identification in physical spaces with co-located Wi-Fi WLANs, using existing hardware in the mentioned frequency range.

In this project, we present our solution for the coexistence of IEEE 802.11b and IEEE 802.15.4 networks. Also, our solution is applicable to IEEE 802.11 and Framed Slotted Aloha networks in the same vicinity. Thus, for the Medium Access Control (MAC) layer and Anti-collision issues in RFID network, we will use two different standards in two attempts: The first model includes Framed Slotted Aloha standard [1] which is being used widely in RFID networks in industry. The second model uses IEEE 802.15.4 standard [2] which is famous for its usage in ZigBee networks.

In summary, these are our contributions in this thesis:

- This project aims to solve the WLAN/RFID coexistence problem in 2.45 GHz or ISM frequency band. In our model, WLAN and RFID networks are allowed to work together in a time sharing manner using Point Coordination Function (PCF) mechanism of IEEE 802.11 standard. PCF is a suitable mechanism for time sharing models at MAC layer level.
- We will use two different medium access standards in RFID networks: Framed Slotted Aloha standard and IEEE 802.15.4 standard. It should be mentioned that we are using these two standards separately in two simulation models. At end, we will evaluate the performance of these two models and compare their simulation results.
- In order to simulate our two models, we use Artifex simulation environment which is based on Extended Petri Nets. The Artifex simulation environment

is integrated with standard programming languages like C and C++. In mentioned environment, we simulate our models from scratch and the simulation results (measurements) will go to some text files directly. Afterward, we are using the Maple environment to draw the related plots.

The thesis is organized as following:

In Chapter 2, we present some related works and studies in this area. Moreover, we briefly introduce the RFID infrastructure and its functionality. Also, two anti-collision standards i.e. Framed Slotted Aloha and ZigBee (IEEE 802.15.4) are presented for RFID networks. Moreover, we introduce the basic protocol of Medium Access Control (MAC) layer of WLANs: the IEEE 802.11 Distributed Coordination Function (DCF) and the Point Coordination Function (PCF). In Chapter 3, we discuss our proposed solution and simulations and related issues. We have two versions of our model: the first one which uses Framed Slotted Aloha standard to prevent collisions in RFID networks and the second model which uses the IEEE 802.15.4 (also known as MAC layer of ZigBee) standard for the same matter. In Chapter 4, simulation results are presented and analyzed for both models. Finally, Chapter 5 concludes our work.

Chapter 2

Related Work and Background

The frequency band of 2.45 GHz or ISM band (also known as Microwave band) is a free frequency band and it is assigned to several wireless networks such as Wi-Fi (802.11b), ZigBee (802.15.4), Bluetooth (802.15.1), high rate WPAN (802.15.3) and Microwave RFID. Even some microwave ovens and hand held phones are working in this frequency range. Therefore, ISM band is a very busy frequency band and the signals of different wireless networks can collide with each other. Interference in the 2.4 GHz band has been discussed in some papers like [11] since last decade.

In Figure 2.1, only the assigned channels for 802.11b and 802.15.4 networks are illustrated.

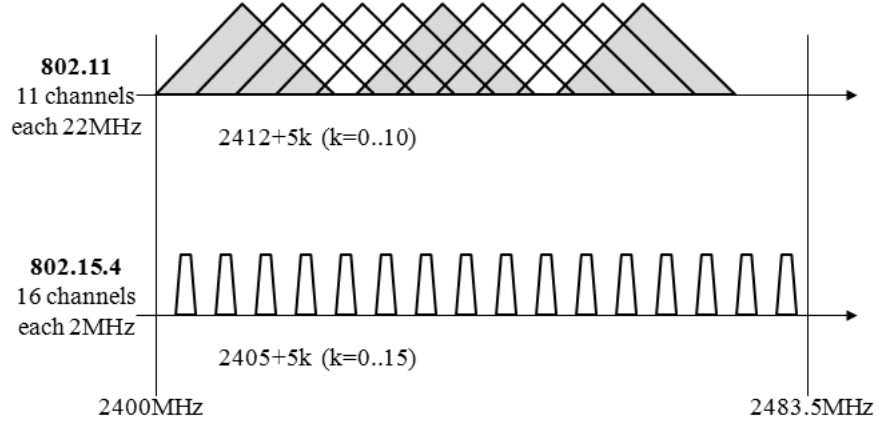


Figure 2.1: The channel assignment of 802.11b and 802.15.4 networks.

There are a lot of papers available in literature which were specifically discussing the interference issues between IEEE 802.11b and IEEE 802.15.4 [15, 31–33, 35–37, 39, 40]. For example in [21], A mathematical model was proposed to analyze the mutual interference of 2.45GHz RFID and 802.11b systems, and Packet Error Rate (PER) was used as the performance metric to evaluate the mutual interference. According to the theoretical analysis and the simulation in [21], the mutual interference can significantly degrade the performance of the mentioned systems. In another example presented in [14], authors have discussed the interference in ISM band and in order to study the behavior this interference, they have perposed and simulated a noise model which acts like an external interference.

Some of the solutions for the coexistence problem rely on the reader being integrated with the Access Point which limits the RFID network coverage. The solution presented by AeroScout [17] is an example of these solutions which is used in some

Industrial models such as the architecture suggested in [34] for underground mine mapping. Furthermore, in some solutions, researchers were trying to fix the interference problem at RFID tag's side. In [7], the author has proposed a hybrid RFID tag design that is protocol-compatible with existing IEEE 802.11b and/or Bluetooth standards as well as existing RF-tag standards.

Moreover, some manufacturers such as AeroScout [18], Ekahau [19], PanGo [20] and Radionor Communications [9] presented Wi-Fi RFID tags. Although we did not have access to the details and technical specifications of these tags (which are part of proprietary information of these companies), we generally found that these RFID tags comply with IEEE 802.11 standards and have been used in the health industry, especially in hospitals to track patients and staff and to locate expensive medical equipment. In [13] which describes the RFID Implementation at the University of Pittsburgh Medical Center, the passive tags of 915 MHz were used to track patients and surgical instruments. Also, active Wi-Fi RFID tags of 2.45 GHz were used to track staff and visitors because of their wide range. Furthermore, Wi-Fi RFID tags have been used for tracking in citywide wireless networks or outdoor Location-Based Services. The model suggested in [29], [28] is an example of using Wi-Fi RFID tags for tracking in Wireless Trondheim, Norway. The Wireless Trondheim location based infrastructure has used Cisco Systems' equipments, such as access points, access point controllers and a location server. The Wi-Fi RFID tags used in the location tests were AeroScout T2 tags. The authors claimed that they have experienced some location errors in their test results and they believed that the interference in ISM frequency band could be a considerable error source to their obtained test results.

Therefore we can say that developing a comprehensive solution will facilitate the development of much-needed or potential RFID applications and allow the use of existing, readily available Wi-Fi hardware. The deployment of such RFID solutions in practice would thus contribute to even wider applications of RFID, including areas in which RFID is not used currently due to the outlined problem.

Furthermore, some wireless standard developing organizations are attempting to match their primary standards with RFID networks. For example, IEEE has recently made an effort to adapt the primary standard of IEEE 802.15.4 for Active RFID and the Task Group 4f (TG4f) has been assigned to prepare IEEE 802.15.4f standard for Active RFID. TG4f have had several meetings and they have discussed Active RFID issues and parameters and presented some findings which are available for public, but the prospect standard or its draft is not available as of yet.

In the following sections of this chapter, we will describe the required standards in our models:

2.1 RFID

A Radio Frequency Identification (RFID) system consists of readers (also called interrogators) and tags (or transponders). A typical system has a few readers, either stationary or mobile, and many tags, which are attached to objects, such as pallets, cartons, bottles, etc. A reader communicates with the tags in its wireless range and collects information about the objects to which tags are attached. Depending upon their operating principle, tags are classified into three categories: passive, semi-passive, and active.

A passive tag is the least complex and hence the cheapest. It has no internal power source but uses the electromagnetic (EM) field transmitted by a reader to power its internal circuit. It does not rely on a transmitter but on "backscattering" to transmit data back to the reader. A semi-passive tag has its own power source but no transmitter. Also, it uses backscattering. An active tag has both the internal power supply and an on-tag transmitter.

Without a power supply of their own, passive RFID tags depend on the electromagnetic field of the reader. The coupled energy is rectified and the voltage is multiplied to the power up internal circuits. A multi-stage Greinacher half-wave rectifier or a derivative is commonly used for such purpose [8].

2.1.1 Coupling Techniques

Two different coupling techniques, near and far fields, are used by passive tags.

Near-Field Coupling

The electromagnetic (EM) field in the near-field region is reactive in nature-the electric and the magnetic fields are orthogonal and quasi-static. Depending upon the type of antenna, one field (such as the electric field for a dipole or magnetic field for a coil) dominates the other. Most near-field tags rely on the magnetic field through inductive coupling to the coil in the tag. This mechanism is based upon the Faraday's principle of magnetic induction (Figure 2.2).

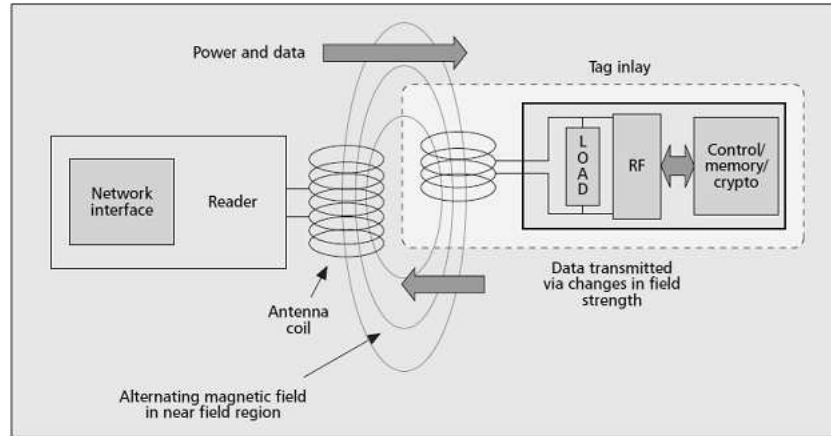


Figure 2.2: Near-field communication using inductive coupling [8].

A current flowing through the coil of a reader produces a magnetic field around it. This field causes the generation of a small current (by the tag's coil in the vicinity).

Communication between a reader and a tag is through a mechanism called load modulation. Any variation of the current in a tag's coil causes a small current variation in a reader's coil due to the mutual inductance between the two, and the variation is detected by reader. A tag varies the current by changing the load on its antenna coil, and hence the mechanism is called load modulation. Because of its simplicity, inductive coupling was initially adopted for passive RFID systems.

Depending upon the application, near-field tags come in many form factors. Some examples are shown in Figure 2.3:

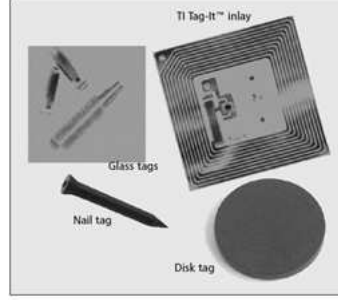


Figure 2.3: Different types of near-field RFID tags [8].

The boundary between near-field and far-field regions is inversely proportional to frequency and approximately equal to $c/2\pi f$, where c is the speed of light [38]. Therefore, only low carrier frequencies are used in near-field coupling tags; the two most common are 128 kHz (LF) and 13.56 MHz (HF).

For example, the boundary distances are 372 m for 128 kHz and 3.5 m for 13.56 MHz. One problem with use of low frequencies is that a large antenna coil is required. Also, the power of magnetic field of a magnetic dipole loop drops as $1/r^6$ the near-field region, where r is the distance between a reader and a tag. Another downside is the low bandwidth and, hence, the low data rate.

Far-Field Coupling

The EM field in the far-field region is radiative in nature. Coupling here captures EM energy at a tag's antenna as a potential difference. Part of the energy incident on a tag's antenna is reflected back due to an impedance mismatch between the antenna and the load circuit. Changing the mismatch or loading on the antenna can vary the amount of reflected energy, a technique called backscattering. Figure 2.4 illustrates

the mechanism.

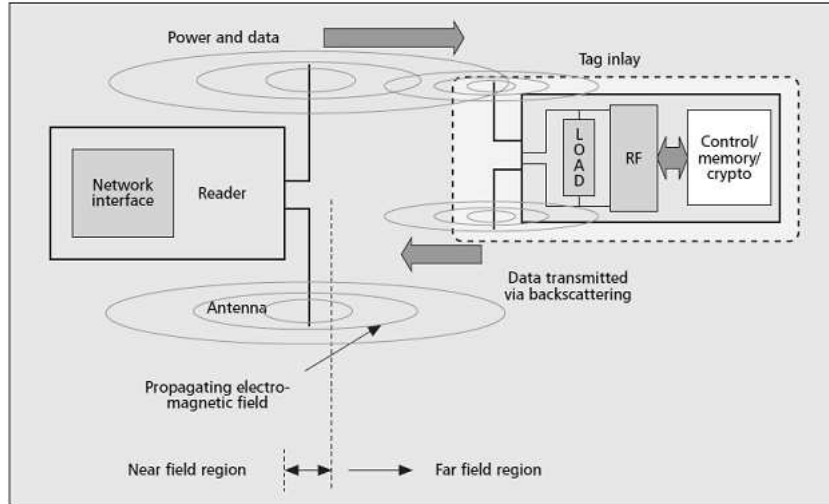



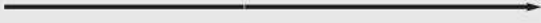

Figure 2.4: Different types of far-field RFID tags [8].

Far-field coupling is commonly employed for long-range (5-20 m) RFID, and, in contrast to near-field, there is no restriction on the field boundary for far-field RFID. The attenuation of the EM field in far-field region is proportional to $1/r^2$, which is smaller by orders of magnitude than in the near-field range (which is $1/r^6$). An advantage of a far-field tag operating at a high frequency is that the antenna can be small, leading to low fabrication and assembly costs. Innovative circuit designs combined with advances in silicon technology have made far-field passive tags, which consume only a few microwatts, practical.

Far-field tags usually operate in the 860-960 MHz UHF band or in the 2.45 GHz Microwave band. Various form factors and antenna shapes are used for far-field tags to meet application requirements.

Several emerging technologies in the UHF and LF bands try to exploit advantages of both near-field and far-field tags. UHF proponents are promoting near-field

Table 2.1: Frequency characteristics of RFID systems [8].

Frequency range	< 135 KHz [LF]	13.56 MHz [HF]	860–960 MHz [UHF]	2.45GHz [Microwave]
Relevant standards	<ul style="list-style-type: none"> • ISO 11784 & 11785 • ISO/IEC 18000-2 • ISO 14223-1 	<ul style="list-style-type: none"> • ISO/IEC 18000-3 • EPC class-1 • ISO 15693 • ISO 14443 (A/B) 	<ul style="list-style-type: none"> • ISO/IEC 18000-6 • EPC class-0, class-1 	<ul style="list-style-type: none"> • ISO/IEC 18000-4
Typical read range	<0.5 m	~1 m	~4–5 m	~1 m
Tag type	Passive-inductive coupling	Passive-inductive coupling	Passive or active	Passive or Active
Typical applications	Access control, animal tagging, vehicle immobilizer	Smart cards, access control, payment ID, item-level tagging, baggage control, biometrics, libraries, transport, apparel	Supply chain pallet- and box-level tagging, baggage handling, electronic toll collection	Electronic toll collection, cold chain management, environment monitoring
Multiple tag read rate	Slower			
Ability to read near metal or wet surfaces	Better			
Passive tag size	Larger			

UHF tags for label tagging, which has been the sole domain of HF near-field tags. The advantage of using UHF here is the low tag cost, resulting from small antenna size. RuBee, a relatively new active RFID technology, operates in the LF band and employs long-wave magnetic signaling. It can achieve a read range of 30 m. Long-wave magnetic signaling has a great advantage: it is highly resistant to performance degradation near metal objects and water, a serious problem for UHF and Microwave far-field RFID.

Non-conductors with a high dielectric constant can cause severe performance degradation for UHF and Microwave RFID, yet have little impact on low-frequency RFID. Therefore, LF or HF tags are preferred for animal tagging or those involving humans. A summary of RFID bands, frequency characteristics, and corresponding standards are tabulated in Table 2.1:

RFID tags and readers fall under short range devices, which normally do not require a license for operation. However, their frequency emissions are governed by regulations varying from one country to another. Currently, only the 13.56 MHz and

2.45 GHz bands are globally accepted, but the 2.45 GHz band regulations are not as uniform as for the 13.56 MHz band. Regulations for the 900 MHz band vary the most among RFID bands. However, with adoption of EPC Class-1 Gen-2 as a global UHF RFID standard for supply chain management, countries throughout the world are amending their spectrum allocations and/or opening up portions of spectrum in the UHF band for RFID.

2.1.2 Tag Memory

In [38] a commercially available RFID system naming "I-Code" by Philips Semiconductors has been used. An I-Code tag provides 64 bytes memory which is addressable in blocks of 4 bytes. All blocks can be read from, but writing to some blocks is inhibited, indicated by a set of write protection bits. This prevents changes to the serial number and similar data. The write protection bits themselves cannot be deactivated after activation.

Of the 64 bytes, 46 are available for application data. The rest is reserved for a 8 byte serial number and the following functionality: write protection; one bit for indicating electronic article surveillance; one bit indicating the "quiet" state of the tag. If the latter bit is set, the tag will not engage in communication with the reader unless a "reset quiet bit" procedure is executed.

2.1.3 Programming Interface

The programmatic interface of the system is provided by the reader device. It comprises commands for setting configuration parameters of the reader device itself,

e.g. the speed of the serial connection, and commands for handling communication with tags that are in range [38]. Communication commands include the following:

- Anti-collision/select (ACS). This command causes all tags that are in range to send their serial numbers. Afterwards, these tags become "selected" and keep quiet in following ACS cycles as long as they are in range. After a tag moves out of the field it becomes "unselected". When it comes back again, it re-sends its serial number. This command can be used to detect tags that are in range, since a list of serial numbers is returned. It is also a prerequisite for writing to tags, since the write command affects only selected tags. However, we are not going to use this command since one ACS cycle takes significantly longer than a Read unselected command.
- Write. This command is used to write data to a number of tags. One data block (4 bytes) can be written to at a time, but multiple tags may be affected. The tags are selected by the time slot (discussed in the next subsection) they have used while the ACS command. This requires that tags don't move in and out of range while writing is in progress.
- Read. This command causes only "selected" tags to send their data. It is performed after an ACS command.
- Read unselected. This is similar to read but all tags are triggered regardless of their selection status. By specifying the blocks 0 and 1 to be read, this command can be used to read the serial numbers as well. This is our preferred reading command.

2.1.4 The Life Cycle of a Typical RFID Tag

Active RFID tags switch to a power saving mode for most of the times, this is often referred to as 'sleeping.' Power saving typically involves turning off the radio subsystem which is the single greatest power consumer; in most hardware implementations, this will reduce power consumption by two to three orders of magnitude and allow prolonged operation on battery power. Moreover, as most of the tags are sleep at the same time, the awaken tags will rarely collide with each other. So, this sleeping order will reduce the overall collision of the system.

In Figure 2.5, the life cycle of a typical tag has been shown: RFID tag will wake up after an average sleeping time (like once an hour) and it will search for the reader's signal. After sensing the beacon or request signal from reader, it will send back its ID in format of a data frame toward reader and it will go back to sleeping phase. In this project, The request/reply process will be done in two attempts: In first one we will use Framed Slotted Aloha standard and in second one, we will use IEEE 802.15.4 standard (ZigBee protocol). It should be mentioned that in our proposed model which will be presented in Chapter 3, RFID tags will choose a random sleeping time using the Geometric distribution with a specific average sleeping time (as input argument for Random Geometric function). Geometric distribution will return a random number (in this case a random sleeping time) which is mostly close to that specific average sleeping time. So the RFID tags will not wake up at the same time, Therefore they will not collide with each other and this is the reason we are using Geometric distribution in our sleeping time selection.

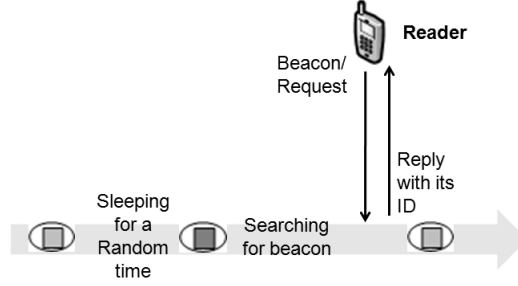


Figure 2.5: The life cycle of a typical tag.

The calculations of sleeping period and probability

In this section we want to introduce some parameters and calculate some of them according to the requirements of this project. We begin by defining the probability generating functions (PGFs) for the variables to be used in our analyses. Since the cluster uses the slotted CSMA-CA algorithm, all state changes may be considered to happen at the boundaries of backoff intervals. Therefore, all variables have discrete probability distributions and can be represented as weighted sums of multiples of backoff periods. For all variables, the corresponding PGFs will then be polynomials in z [12], e.g.,

$$V(z) = \sum_{k=1}^{\infty} p_k z^k$$

for a given variable V .

As to the choice of sleep time distribution, a simple solution is to use Geometric distribution which is controlled with a single adjustable parameter. Let us denote this

parameter with P_{sleep} ; the duration of the vacation period may, then, be expressed as:

$$V(z) = \sum_{k=1}^{\infty} (1 - P_{sleep}) P_{sleep}^{k-1} z^k = \frac{(1 - P_{sleep})z}{1 - zP_{sleep}}$$

and its mean duration is $\bar{V} = (1/1 - P_{sleep})$

Now let's calculate the sleeping probability of the tags. In this example we are using the ZibBee standard for communication in RFID networks. Tags are sleep for most of the time and in our model they will wake up for example once per hour and search for beacon signal. From calculations we found $T_{sleep} = \bar{V} = (1/1 - P_{sleep})$.

So we have: $T_{sleep} = 3600/0.00032 = (1/1 - P_{sleep})$

In this equation, 0.00032 is the size of each IEEE 802.15.4 time slot in Second, thus for one hour average sleeping time, T_{sleep} or average sleeping time in time slots is calculated like that.

Thus we have: $P_{sleep} = 0.99999991111111111111$, which means for most of the time the tags are sleep with the probability of P_{sleep} , then they will wake up in different order.

2.1.5 Anti-collision protocol for RFID network: Framed Slotted Aloha

Aloha-based anti-collision protocols are based on a backoff mechanism that operates in a probabilistic manner. They try to arrange the response times of tags in the interrogation zone periodically. In below, we introduce several Aloha-based protocols: Pure Aloha [5], slotted Aloha [25] and framed slotted Aloha [38]. In general, Aloha-based protocols are simple and have fair performance. However, they have the tag

starvation problem that a tag may never be identified because its responses always collide with others’.

Pure Aloha Protocol

Pure Aloha protocol [5] is the simplest Aloha-based anti-collision protocol. When a reader requests tags to respond to their IDs, each tag in the interrogation zone chooses a random backoff time individually and responds with its tag ID to the reader after the backoff time. If no collision occurs during the transmission of a tag ID, this ID is identified successfully and acknowledged by the reader. A tag with acknowledged ID will stop responding to the reader and a tag will repeatedly select a random back-off time and send its ID until the ID is identified and acknowledged by the reader.

Slotted Aloha Protocol

In slotted Aloha protocol [25], the random backoff time must be a multiple of a pre-specified slot time. Note that a slot time is usually set to be a time period that is long enough for a tag to send out its ID and for the reader to recognize the ID and acknowledge the ID. The reader needs to synchronize the slot times for all the tags in the interrogation zone. If only one tag transmits its ID in a period of a slot time, it can be identified and acknowledged by the reader properly. Tags not identified by the reader will repeatedly select a time slot randomly for transmitting their IDs. The performance of slotted Aloha protocol is twice of the Aloha protocol because there is no partial collision of tag ID responses in slotted Aloha protocol. In this protocol:

- All frames consist of exactly L bits.
- Time is divided into slots of size L/R seconds (that is, a slot equals the time to transmit one frame).
- Nodes start to transmit frames only at the beginnings of slots.
- The nodes are synchronized so that each node knows when the slots begin.
- If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends.

The derivation of the maximum efficiency of Slotted Aloha: In this section, we want to outline the derivation of the maximum efficiency of slotted Aloha. In first step we will have some definitions [23]: Let p be the probability of transmission; that is a number between 0 and 1. The operation of slotted Aloha in each node is simple:

- When the node has a fresh frame to send, it waits until the beginning of the next slot and transmits the entire frame in the slot.
- If there isn't a collision, the node has successfully transmitted its frame and thus need not consider retransmitting the frame. (The node can prepare a new frame for transmission, if it has one.)
- If there is a collision, the node detects the collision before the end of the slot. The node retransmits its frame in each subsequent slot with probability p until the frame is transmitted without a collision.

By retransmitting with transmission probability p , we mean that the node effectively tosses a biased coin; the event heads corresponds to retransmit, which occurs with probability p . The event tails corresponds to skip the slot and toss the coin again in the next slot; this occurs with probability $(1 - p)$. All nodes involved in the collision toss their coins independently. Unlike channel partitioning, slotted Aloha allows a node to transmit continuously at the full rate, R , when that node is the only active node. (A node is said to be active if it has frames to send.) Slotted Aloha is also highly decentralized, because each node detects collisions and independently decides when to retransmit.

Slotted Aloha works well when there is only one active node, but how efficient is it when there are multiple active nodes? There are two possible efficiency concerns here. First, when there are multiple active nodes, a certain fraction of the slots will have collisions and will therefore be wasted. The second concern is that another fraction of the slots will be empty because all active nodes refrain from transmitting as a result of the probabilistic transmission policy. The only unwasted slots will be those in which exactly one node transmits. A slot in which exactly one node transmits is said to be a successful slot. The efficiency of a slotted multiple access protocol is defined to be the long-run fraction of successful slots in the case when there are a large number of active nodes, each always having a large number of frames to send. Note that if no form of access control were used and each node were to immediately retransmit after each collision, the efficiency would be zero. Slotted Aloha clearly increases the efficiency beyond zero, but by how much? We now proceed to outline the derivation of the maximum efficiency of slotted Aloha. To keep this derivation simple, let's

modify the protocol a little and assume that each node attempts to transmit a frame in each slot with probability p . (That is we assume that each node always has a frame to send and that the node transmits with probability p for a fresh frame as well as for a frame that has already suffered a collision.) Suppose first there are N nodes. Then the probability that a given slot is a successful slot is the probability that one of the nodes transmits and that the remaining $N - 1$ nodes do not transmit. The probability that a given node transmits is p ; the probability that the remaining nodes do not transmit is $(1 - p)^{N-1}$. Therefore the probability a given node has a success is $(1 - p)^{N-1}$. Because there are N nodes, the probability that an arbitrary node has a success is $N(1 - p)^{N-1}$.

Thus when there are N active nodes, the efficiency of slotted Aloha is $N(1 - p)^{N-1}$. To obtain the maximum efficiency for N active nodes, we have to find the p^* that maximizes this expression. And to obtain the maximum efficiency for a large number of active nodes, we take the limit of expression as N approaches infinity. After performing these calculations, we'll find that the maximum efficiency of the protocol is given by $1/e = 0.37$. That is, when a large number of nodes have many frames to transmit, then at best only 37 percent of the slots do useful work.

Moreover in pure Aloha protocol, the probability that a given node has a successful transmission is $p(1 - p)^{2(N-1)}$. Thus the maximum efficiency of pure Aloha is $1/2e$.

Framed Slotted Aloha Protocol

In framed slotted Aloha [38], the whole interrogation procedure is divided into a set of frames, each having several time slots. On receiving the reader's REQUEST

command, each tag can respond just in one randomly chosen slot during a frame period. If there is only one tag response in a slot, the reader can identify the tag successfully. Tags not identified successfully will reselect a time slot in the next frame for retransmitting their IDs. At the time when no tag responds, all tags are identified successfully. The frame rounds continue until that time.

In Table 2.2, we show an example of framed slotted Aloha protocol in which each frame has four time slots. Suppose that there are six tags with unique 5-bit IDs in the interrogation zone of a reader. The execution procedure of the protocol is described as follows:

1. The reader sends REQUEST command first to synchronize the beginning of a frame.
2. Each tag randomly chooses one of the four available time slots in frame 0 to respond to its tag ID after receiving REQUEST command. In our example, in frame 0, only tag ID (01110) in time slot 1 can be identified successfully. Collisions occur in time slots 2 and 4 and no tag responds in time slot 3.
3. The identified tag can be selected by SELECT command for reading or writing data. It will stop responding to REQUEST commands in later frames.
4. The reader sends REQUEST commands repeatedly until all tags are identified successfully as shown in frames 1 and 2.

It should be mentioned that reader can vary the frame size, e.g. for maximizing throughput; the actual size of a slot is chosen according to the amount of requested data.

Table 2.2: An example of Framed slotted Aloha protocol [41].

	Frame 0					Frame 1					Frame 2				
		Time slot 1	Time slot 2	Time slot 3	Time slot 4		Time slot 1	Time slot 2	Time slot 3	Time slot 4		Time slot 1	Time slot 2	Time slot 3	Time slot 4
Reader	Rqst					Rqst					Rqst				
Tag1			10010						10010						
Tag2		01110													
Tag3					00101		00101							00101	
Tag4			11011				11011						11011		
Tag5			10110					10110							
Tag6					01001					01001					
State		Succ	Coll	Idle	Coll		Coll	Succ	Succ	Succ		Idle	Succ	Succ	Idle

Moreover, one drawback of framed slotted Aloha protocol is that its performance will degrade when the number of slots in the frame does not match properly the number of tags in the interrogation zone. Dynamic framed slotted Aloha protocols try to eliminate the drawback by dynamically adjusting the frame size according to the estimated number of tags. Their performance is better than that of framed slotted Aloha protocol [41].

Different variations of Framed slotted Aloha: Two main variations of Framed slotted Aloha exist in the literature: Basic Framed Slotted ALOHA (BFSA) and Dynamic Framed Slotted ALOHA (DFSA). BFSA algorithms use a fixed frame size and do not change the frame size until the process of tag identification is over. When an RFID reader attempts to read tags, the reader offers necessary information to the tags, such as the frame size and the random numbers. Receiving this information, tags transmit their IDs at the computed timeslots in the frame. If a timeslot has collision, the tags transmitted at the timeslot retransmit in the next read frame [24].

DFSA algorithms can actively deal with the problem of BFSA by changing the frame size for efficient tag identification. To determine the frame size, it uses the probability of collision in the previous frame [24].

The simplest DFSA changes the frame size based on the number of timeslots collided. If the number of timeslots collided is larger than a threshold, a reader increases the frame size at the next frame. When, however, the number of collisions is smaller than a threshold, a reader decreases the frame size at the next frame. This algorithm can solve the problem of BFSA, but this algorithm still has many collisions when the difference between the number of tags and the frame size is large.

Another version of DFSA is based on the tag estimation. Performance of DFSA is known to be optimal when the frame size equals to the number of tags. So, a reader decides the next frame size as the number of tags in the current frame [10].

It should be mentioned that in our solution we are using BFSA algorithm, So we are using fixed frame size in whole of the process. Moreover, we are using ISO18000-4 standard which includes RFID Parameters for air interface communications at 2.45 GHz [1]. according to ISO18000-4 standard , we are choosing the smallest available frame size which is 14 time slots.

2.1.6 Anti-collision protocol for RFID network: IEEE 802.15.4

As it was denoted before, in our second attempt we will use ZigBee or IEEE 802.15.4 standard for Anti-collision issues [2].

Let's start with the physical layer of IEEE 802.15.4 standard. In this project, our scope of work is in ISM band (2.45 GHz). In the ISM band, Orthogonal Quadrature

Phase Shift Keying (O-QPSK) modulation is used before spreading. In this modulation, four data bits comprise one modulation symbol which is further spread with the 32-bit spreading sequence. As a result, the maximum raw data rate in this band is 250 kbps [27].

Channel allocation in the ISM band for IEEE 802.15.4 standard is illustrated in Figure 2.1. In an IEEE 802.15.4-compliant RFID network, a controller device commonly referred to as the RFID reader builds a star topology network with RFID tags as it is shown in Figure 1.1. The networks with the star topology use the so-called beacon enabled operating mode, in which the coordinator periodically emits a special frame or packet known as the beacon frame. The time between two successive beacon frames is known as the superframe or (more precisely) as the *beacon interval*. It is divided into an active portion and an optional inactive period. The structure of the superframe is shown in Figure 2.6(a).

All communications in the cluster take place during the active portion of the superframe. Individual nodes can send their data to the coordinator, or receive data from it; these two directions of communication are referred to as *uplink* and *downlink*, respectively.

The active portion of the superframe is divided into equally sized slots, each of which lasts for exactly $2^{so} * aBaseSlotDuration$ symbols; the *aBaseSlotDuration* contains exactly three backoff periods. The duration of the backoff period is always equal to the time it takes to transmit 20 symbols. In our case, it is equal to $320\mu s$.

The beacon frame is transmitted at the beginning of slot 0, and the contention access period (CAP) of the active portion starts immediately afterward. During

the CAP, channel access is contention-based and all nodes, including the coordinator, must use the slotted CSMA-CA access mechanism. Furthermore, a device must complete all of its contention based transactions within the CAP of the current superframe. The CAP is optionally followed by the contention-free period (CFP), in which an individual device may be granted exclusive access to the medium.

Figure 2.6(b) shows the structure of the active portion of the superframe.

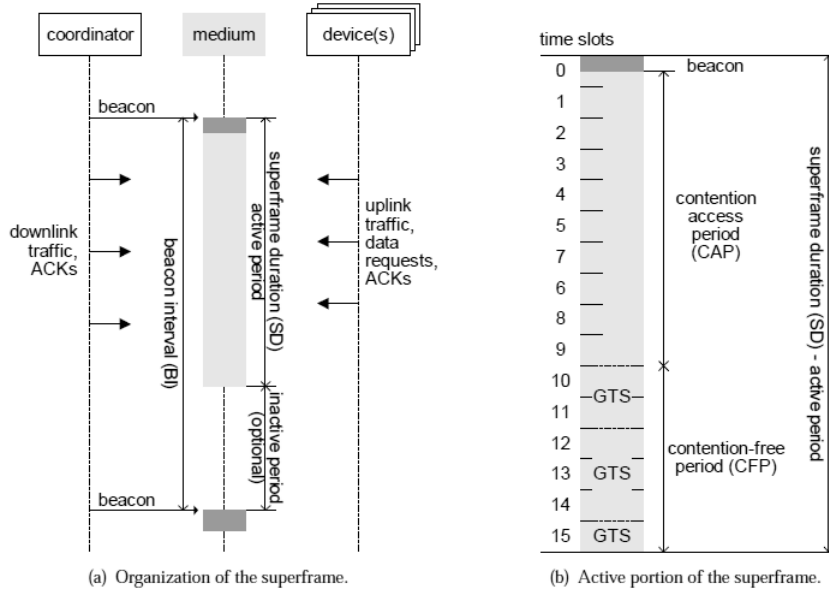


Figure 2.6: Structure of the superframe in beacon enabled mode [27].

The duration of the beacon interval and the active portion of the superframe are controlled through two MAC layer attributes known as the beacon order, BO , and superframe order, SO , respectively, using the simple formulae presented in Table 2.3. Note that the values of these two attributes must satisfy the constraint $0 \leq SO \leq BO \leq 15$, but the formulae are valid only for values of 14 or below. Namely, when BO is set to 15, the coordinator does not transmit beacon frames unless specifically

requested to do so, which means that the superframe, strictly speaking, does not exist; in that case, the value of superframe order SO is conventionally set to 15. This feature is used in the peer-to-peer topology which is not applicable in our case.

In order to synchronize with the beacon, each node in a beacon enabled cluster must listen for the beacon for $aBaseSuperframeDuration * (2^{BO} + 1)$ symbols. If a valid beacon frame is not received during that time, the procedure is repeated. If the number of missed beacons exceeds $aMaxLostBeacons = 4$, the MAC layer assumes that synchronization is lost and notifies the higher layers of the protocol stack.

Table 2.3: Timing parameters in beacon enabled operating mode [27].

Time period	MAC attribute	Duration (symbols)
Unit backoff period	$aUnitBackoffPeriod$	20
Basic superframe slot	$aBaseSlotDuration$	$3 * aUnitBackoffPeriod = 60$
Superframe slot		$aBaseSlotDuration * 2^{SO}$
Superframe duration	SD	$aBaseSuperframeDuration * 2^{SO}$
Beacon interval	BI	$aBaseSuperframeDuration * 2^{BO}$

All packet transmissions must be synchronized with backoff periods derived from the periodic beacon frames. Consequently, the so-called slotted carrier sense multiple access mechanism with collision avoidance (CSMA-CA) is used as the main medium access mechanism, as described below.

Slotted CSMA-CA Medium Access

Nodes in clusters that operate in beacon enabled mode must utilize the slotted CSMA-CA access mechanism, with a few exceptions. The flowchart shown in Figure 2.7 describes the slotted CSMA-CA algorithm which is executed when a packet is

ready to be transmitted. The algorithm begins by setting the appropriate variables to their initial values:

1. Retry count NB , which refers to the number of times the algorithm was required to back off due to the unavailability of the medium during channel assessment, is set to zero.
2. Contention window CW , which refers to the number of backoff periods that need to be clear of channel activity before the packet transmission can begin, is set to 2.
3. Backoff exponent BE is used to determine the number of backoff periods a device should wait before attempting to assess the channel. If the device operates on battery power, in which case the attribute *macBattLifeExt* is set to true, BE is set to 2 or to the constant *macMinBE*, whichever is less; otherwise, it is set to *macMinBE*, the default value of which is 3.

Then, the boundary of the next backoff period is located, and a random number in the range $0..2^{BE} - 1$ is generated. The algorithm then counts down for this number of backoff periods; this period is referred to as the Random Backoff Countdown or RBC. During the RBC period, channel activity is not assessed and the backoff counter is not stopped if such activity takes place, unlike the similar CSMA mechanism utilized in 802.11 networks. For obvious reasons, the countdown will be suspended during the inactive portion of the beacon interval, and will resume immediately after the beacon frame of the next superframe.

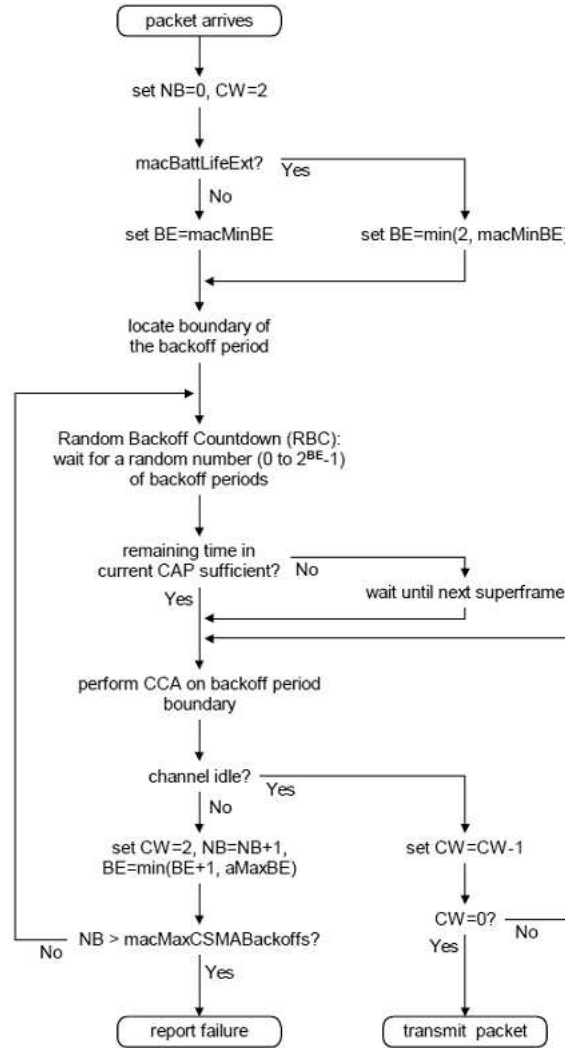


Figure 2.7: Operation of the slotted CSMA-CA algorithm [27].

Once the backoff count reaches zero, the algorithm first checks to see whether the remaining time within the CAP area of the current superframe is sufficient to accommodate the necessary number of CCA checks, the actual packet transmission, and subsequent acknowledgment. If this is the case, the algorithm proceeds to perform

the CCA checks; otherwise, it pauses until the (active portion of the) next superframe. This feature poses an actual performance risk.

CCA check is repeated on CW successive backoff period boundaries. If all CCA checks pass, the channel is deemed idle and the packet may be transmitted. Otherwise, if any of the CCAs detect activity on the channel, the node concludes that there is an ongoing transmission by another node and the current transmission attempt is immediately aborted. The CSMA-CA algorithm is then restarted; the number of retries, NB , and the backoff exponent, BE , are incremented by one, while the CCA count, CW , is reset to two. Note that the backoff exponent BE cannot exceed $macMaxBE$, the default value of which is 5.

However, if the number of unsuccessful backoff cycles NB exceeds the limit of $macMaxCSMABackoffs$, the default value of which is 5, the algorithm terminates with channel access failure status. Failure is reported to higher protocol layers, which can then decide whether to abort the packet in question or re-attempt to transmit it as a new packet. Together, the limit on the number of retries and the manner in which the backoff exponent is incremented, impose a restriction on the range of allowable backoff countdown values. In non-battery powered operation (when the variable $macBattLifeExt$ is false), the random backoff countdown values will not exceed 7, 15, 31, 31, and 31, in successive retries. However, if the node is operating on battery power, the limits of the available range will be between zero and 3, 7, 15, 31, and 31, respectively. Presumably, smaller countdown values will lead to shorter countdowns and, by extension, to lower power consumption and longer battery lifetime.

Note that the backoff unit boundaries of every device should be aligned with the superframe slot boundaries defined by the beacon frame, i.e., the start of first backoff unit of each device is aligned with the beginning of the beacon frame. The MAC layer should also ensure that the PHY layer starts all of its transmissions on the boundary of a backoff unit.

Uplink and Downlink Communication in Beacon Enabled Mode

Uplink transmissions in the star topology cluster operating in beacon enabled mode always use the CSMA-CA mechanism outlined above. A node initiates an uplink transmission whenever an application executing on it prepares a packet to be sent to the coordinator. Furthermore, both the original uplink transmission from a node to the coordinator and the subsequent acknowledgment must occur within the active portion of the same superframe. The overview of uplink transmission has been presented in Figure 2.8.

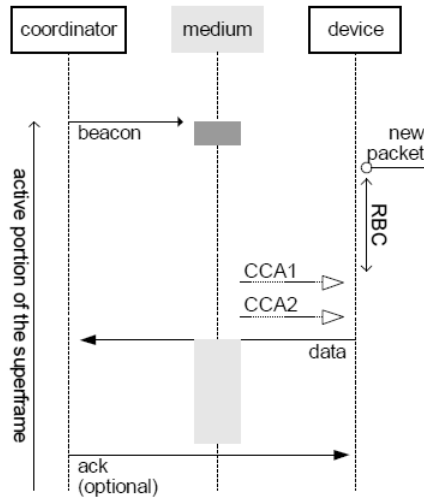


Figure 2.8: Uplink packet transmission, beacon enabled mode [27].

Data transfers in the downlink direction from the coordinator to a node which we are using this case for communication between RFID reader and tags, are more complicated.

When a downlink packet is received by the MAC layer of the coordinator, it must first announce it to the destination node. The announcement is made through the beacon frame, in the form of a list of nodes that have pending downlink packets. When the destination node learns about a data packet to be received, it undertakes the so-called downlink data extraction procedure as follow. The node transmits a data request packet, which the coordinator must acknowledge by transmitting an appropriate acknowledgement packet. After receiving the acknowledgement, the destination node listens for the period of $aMaxFrameResponseTime$, during which the coordinator must send the data frame. An optional acknowledgment is sent upon suc-

cessful reception of the downlink data packet. This message exchange is schematically depicted in Figure 2.9.

If the coordinator does not receive a proper acknowledgment for a downlink packet, it will not attempt retransmission; instead, the destination node must explicitly request the data frame using a data request packet. The standard allows the coordinator to send a data frame 'piggybacked' after the request acknowledgment packet, i.e., without using CSMA-CA. However, such transmission is contingent upon the following conditions:

- The coordinator must be able to commence the transmission of the data packet within the interval between $aTurnaroundTime$ and $aTurnaroundTime + aUnitBackoffPeriod$.
- The remaining time in the CAP of the current superframe must suffice to send the data frame and receive the acknowledgment, together with the appropriate inter-frame spacing.

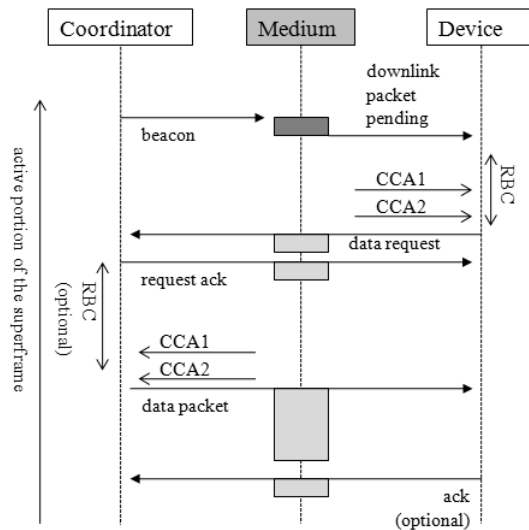


Figure 2.9: Downlink packet transmission, beacon enabled mode [27].

If either of these conditions does not hold, the data frame must be sent using the CSMA-CA mechanism (IEEE 2006). The former condition depends on the capabilities of the coordinator hardware, but the latter depends on the actual traffic. Thus, piggybacking of downlink data frames onto the request acknowledgment packets cannot be guaranteed, and some downlink data will ultimately have to be sent using CSMA-CA.

It is worth noting that the node that does not have a pending downlink packet or a queued uplink packet at the time the beacon frame ends, may achieve further power savings by simply disabling its receiver until the next beacon frame.

2.2 IEEE 802.11 DCF

The primary medium access control (MAC) technique of 802.11 is called Distributed Coordination Function (DCF). DCF is a carrier sense multiple access with collision avoidance (CSMA/CA) scheme with binary slotted exponential backoff [6]. An optional four way handshaking technique, known as request-to-send/clear-to-send (RTS/CTS) mechanism has been standardized for DCF. Before transmitting a packet, a station operating in RTS/CTS mode reserves the channel by sending a special Request-To-Send short frame. The destination station acknowledges the receipt of an RTS frame by sending back a Clear-To-Send frame, after which normal packet transmission and ACK response occurs. Since collision may occur only on the RTS frame, and it is detected by the lack of CTS response, the RTS/CTS mechanism allows increasing of the system performance by reducing the duration of a collision when long messages are transmitted. Moreover, as an important side effect, the RTS/CTS scheme designed in the 802.11 protocol is suited to combat the so-called problem of Hidden Terminals, which occurs when two mobile stations are unable to hear each other and they are transmitting data to the same (third) station.

A station with a new packet to transmit monitors the channel activity. If the channel is idle for a period of time equal to a distributed interframe space (DIFS), the station transmits. Otherwise, if the channel is sensed busy (either immediately or during the DIFS), the station persists to monitor the channel until it is measured idle for a DIFS. At this point, the station generates a random backoff interval before transmitting (this is the Collision Avoidance feature of the protocol), to minimize the probability of collision with packets being transmitted by other stations. In addition,

to avoid channel capture, a station must wait a random backoff time between two consecutive new packet transmissions, even if the medium is sensed idle in the DIFS time.

For efficiency reasons, DCF employs a discrete-time backoff scale. The time immediately following an idle DIFS is slotted, and a station is allowed to transmit only at the beginning of each slot time. The slot time size is set equal to the time needed at any station to detect the transmission of a packet from any other station. This time depends on the physical layer, and it accounts for the propagation delay, for the time needed to switch from the receiving to the transmitting state and for the time to signal to the MAC layer the state of the channel (busy detect time).

DCF adopts an exponential backoff scheme. At each packet transmission, the backoff time is uniformly chosen in the range $(0..w)$. The value w is called contention window, and depends on the number of transmissions failed for the packet. At the first transmission attempt, w is set equal to a value CW_{min} called minimum contention window. After each unsuccessful transmission, w is doubled, up to a maximum value $CW_{max} = 2^m CW_{min}$. The values CW_{min} and CW_{max} reported in the final version of the standard [31] are PHY-specific and are summarized in Table 2.4.

Table 2.4: Defined Timings for IEEE 802.11 Standard [6].

PHY	Slot Time	CW_{min}	CW_{max}
FHSS	$50\mu s$	16	1024
ISM	$20\mu s$	32	1024
IR	$8\mu s$	64	1024

According to previous chapter, ISM band is the scope of our project and we are using its parameters in all of our designs and calculations.

The backoff time counter is decremented as long as the channel is sensed idle, "frozen" when a transmission is detected on the channel, and reactivated when the channel is sensed idle again for more than a DIFS. The station transmits when the backoff time reaches zero. Figure 2.10 shows this mechanism. Two stations A and B share the same wireless channel. At the end of the packet transmission, station B waits for a DIFS and then chooses a backoff time equal to 8, before transmitting the next packet. We assume that the first packet of station A arrives at the time indicated with an arrow in the figure. After a DIFS, the packet is transmitted. Note that the transmission of packet A occurs in the middle of the Slot Time corresponding to a backoff value, for station B, equal to 5. As a consequence of the channel sensed busy, the backoff time is frozen to its value 5, and the backoff counter decrements again only when the channel is sensed idle for a DIFS. Since the CSMA/CA does not rely on the capability of the stations to detect a collision by hearing their own transmission, an ACK is transmitted by the destination station to signal the successful packet reception. The ACK is immediately transmitted at the end of the packet, after a period of time called short interframe space (SIFS). As the SIFS (plus the propagation delay) is shorter than a DIFS, no other station is able to detect the channel idle for a DIFS until the end of the ACK. If the transmitting station does not receive the ACK within a specified ACK Timeout, or it detects the transmission of a different packet on the channel, it reschedules the packet transmission according to the given backoff rules.

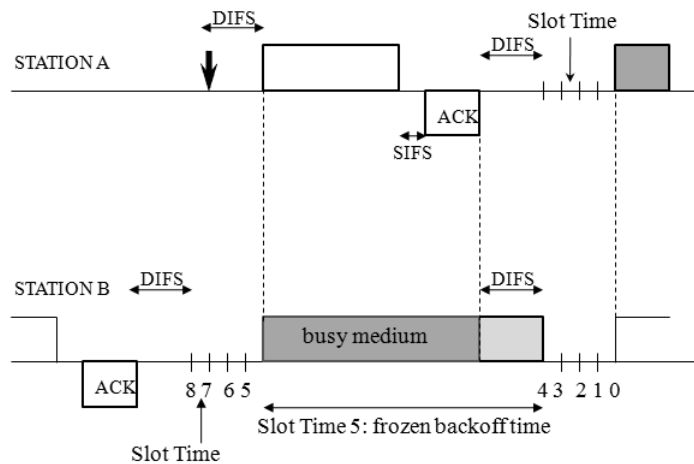


Figure 2.10: Example of basic access mechanism [6].

The above described two-way handshaking technique for the packet transmission is called basic access mechanism. DCF defines an additional four-way handshaking technique to be optionally used for a packet transmission. This mechanism, known with the name RTS/CTS, is shown in Figure 2.11. A station that wants to transmit a packet, waits until the channel is sensed idle for a DIFS, follows the backoff rules explained above, and then, instead of the packet, preliminarily transmits a special short frame called request to send (RTS). When the receiving station detects an RTS frame, it responds, after a SIFS, with a clear to send (CTS) frame. The transmitting station is allowed to transmit its packet only if the CTS frame is correctly received. The frames RTS and CTS carry the information of the length of the packet to be transmitted. This information can be read by any listening station, which is then able to update a network allocation vector (NAV) containing the information of the period of time in which the channel will remain busy. Therefore, when a station is hidden from either the transmitting or the receiving station, by detecting just one

frame among the RTS and CTS frames, it can suitably delay further transmission, and thus avoid collision.

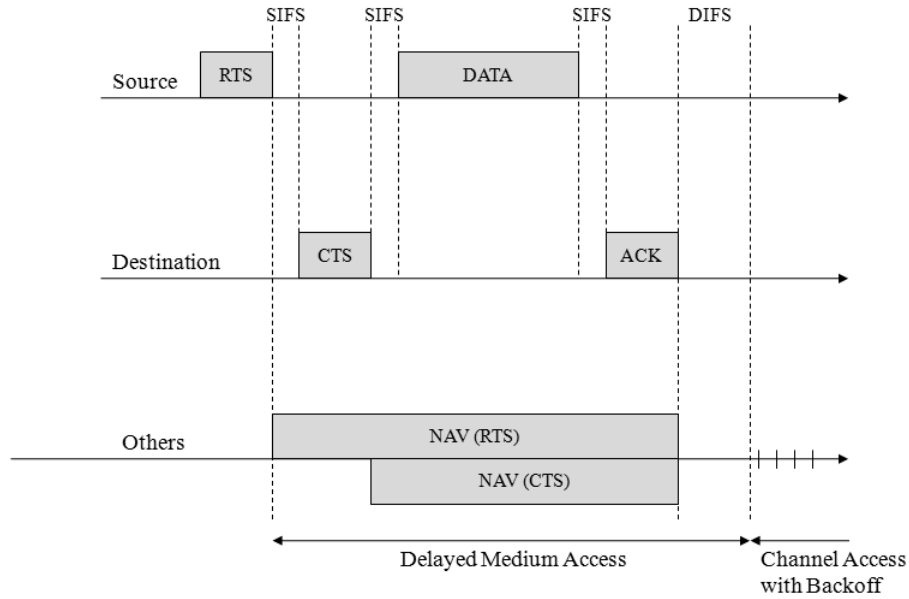


Figure 2.11: RTS/CTS Access Mechanism [6].

The RTS/CTS mechanism is very effective in terms of system performance, especially when large packets are considered, as it reduces the length of the frames involved in the contention process. In fact, in the assumption of perfect channel sensing by every station, collision may occur only when two (or more) packets are transmitted within the same slot time. If both transmitting stations employ the RTS/CTS mechanism, collision occurs only on the RTS frames, and it is early detected by the transmitting stations by the lack of CTS responses.

2.3 Point Coordination Function (PCF)

The IEEE 802.11 MAC may incorporate an optional access method called Point Coordination Function (PCF), which is only usable on infrastructure network configurations [3]. This method has been used to solve some network problems such as presenting Real-time Multimedia Services and addressing QoS issues over 802.11 Wireless Networks [16] or Voice transmission in an IEEE 802.11 Network [22] or supporting the multi-channel operation for Dedicated Short Range Communication (DSRC) in VANETs [26] or defining a central controller which can put its node into doze mode for energy efficiency issues [36]. PCF method uses a Point Coordinator (PC) to determine which station currently has the right to transmit. The operation is essentially based on polling, with the PC performing the role of the polling master.

The variations of available medium access mechanisms and the MAC layer stack of IEEE 802.11 standard is displayed in Figure 2.12.

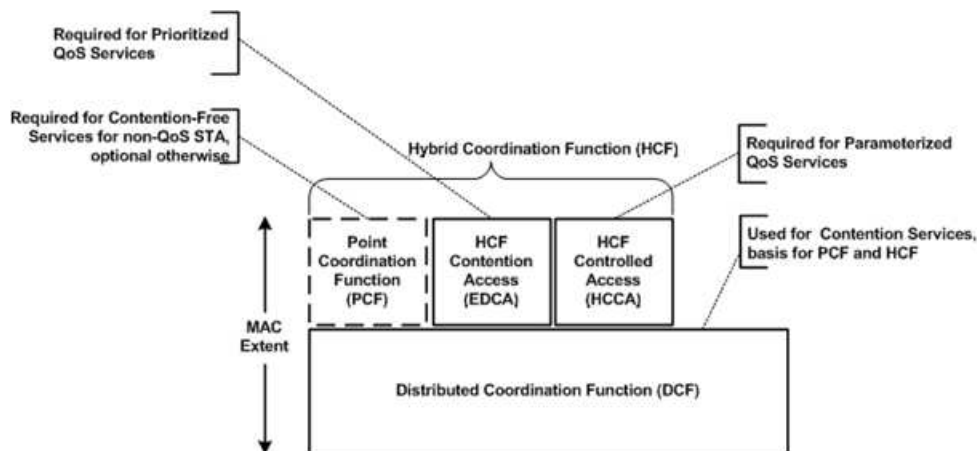


Figure 2.12: MAC Architecture of IEEE 802.11 [3].

As shown in Figure 2.12, the PCF is built on top of the CSMA/CA-based DCF, by utilizing the access priority provisions provided by this scheme.

The PCF uses a virtual carrier sense (CS) mechanism aided by an access priority mechanism. The PCF shall distribute information within Beacon management frames to gain control of the medium by setting the Network Allocation Vector (NAV) in stations. The access priority provided by a PCF may be utilized to create a CF access method. The PC controls the frame transmissions of the STAs so as to eliminate contention for a limited period of time.

The PCF provides Contention Free (CF) frame transfer. The PC shall reside in the AP. All stations inherently obey the medium access rules of the PCF, because these rules are based on the DCF, and all stations set their NAV at the beginning of each Contention Period (CFP). It is also an option for a station to be able to respond to a CF-Poll received from a PC. Figure 2.13 depicts the details of the frame transfer during a typical CFP.

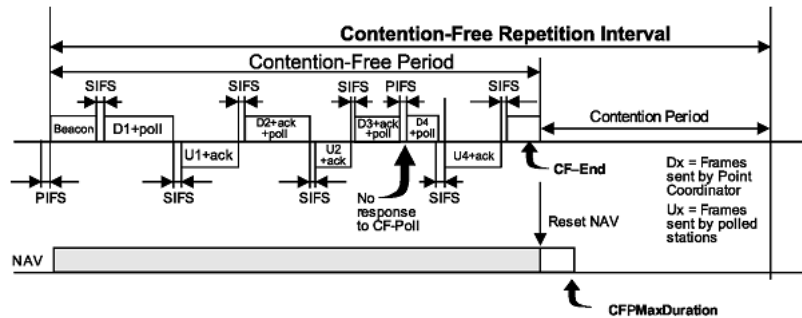


Figure 2.13: Example of PCF frame transfer [3].

A station that is able to respond to CF-Polls is referred to as being CF-Pollable, and may request to be polled by an active PC. CF-Pollable stations and the PC

do not use RTS/CTS in the CFP. When polled by the PC, a CF-Pollable station may transmit only one data unit, which can be sent to the PC but may have any destination, and may "piggyback" the acknowledgment of a frame received from the PC using particular data frame subtypes for this transmission. If the data frame is not in turn acknowledged, the CF-Pollable station shall not retransmit the frame unless it is polled again by the PC, or it decides to retransmit during the Contention Period (CP). If the addressed recipient of a CF transmission is not CF-Pollable, that station acknowledges the transmission using the DCF acknowledgement rules, and the PC retains control of the medium. A PC may use CF frame transfer solely for delivery of frames to stations, and never to poll CFPollable stations.

As it was denoted before, PCF controls frame transfers during the CFP. The CFP shall alternate with a CP, when the DCF controls frame transfers, as shown in Figure 2.14. Each CFP shall begin with a Beacon frame. The CFPs shall occur at a defined repetition rate, which shall be synchronized with the beacon interval.

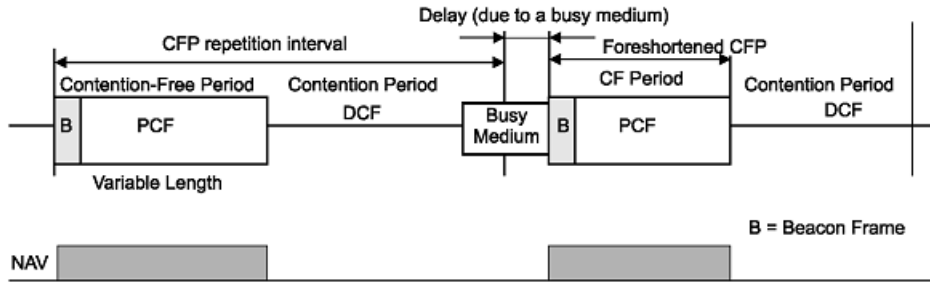


Figure 2.14: CFP/CP alternation [3].

The PC may terminate any CFP at or before the `aCFPMaxDuration`, based on

available traffic and size of the polling list. Because the transmission of any Beacon frame may be delayed due to a medium busy condition, a CFP may be foreshortened by the amount of the delay. In the case of a busy medium due to DCF traffic, the Beacon frame shall be delayed for the time required to complete the current DCF frame exchange. This case has been illustrated in Figure 2.14.

Chapter 3

The Proposed Solution and Simulation Model

One solution to RFID and Wi-Fi co-existence problem is to allow WLAN access and RFID access in a time-sharing manner by making the WLAN Access Point (AP) aware of the RFID neighbor-network at the Medium Access Control (MAC) layer. In this approach, RFID readers act also as Wi-Fi nodes and they are performing the bridging function between RFID and WLAN networks and a single AP is covering Wi-Fi network and multiple RFID networks. In this solution, the AP will periodically broadcast beacon frames with information about the duration of Contention-Free Period (CFP) and contention Period (CP), which will be used by RFID and Wi-Fi access, respectively. No polling is performed at the beginning of the CFP. Instead of that, all RFID readers will read the ID of tags in their area. After reading, the RFID reader within the bridges will pass the collected data to its WLAN interface through a shared buffer. At the end of CFP (or at the beginning of the subsequent

CP), the RFID/Wi-Fi bridge will transmit information obtained from tags to the AP. The AP will collect RFID readings from all the bridged readers and will forward them to the application server where they will be stored and subsequently analyzed. This approach requires suitable but not very complex modifications to be made on both the RFID readers and AP MAC parameters but it does not require any modification on existing RFID tag hardware or software. This property makes the solution economically feasible and thus readily applicable in practice. Furthermore, the use of off-the-shelf Wi-Fi hardware allows for easy transmission of RFID readings to the AP in manner that is transparent to ordinary WLAN nodes.

In Figure 3.1 the general plan for the solution is illustrated.

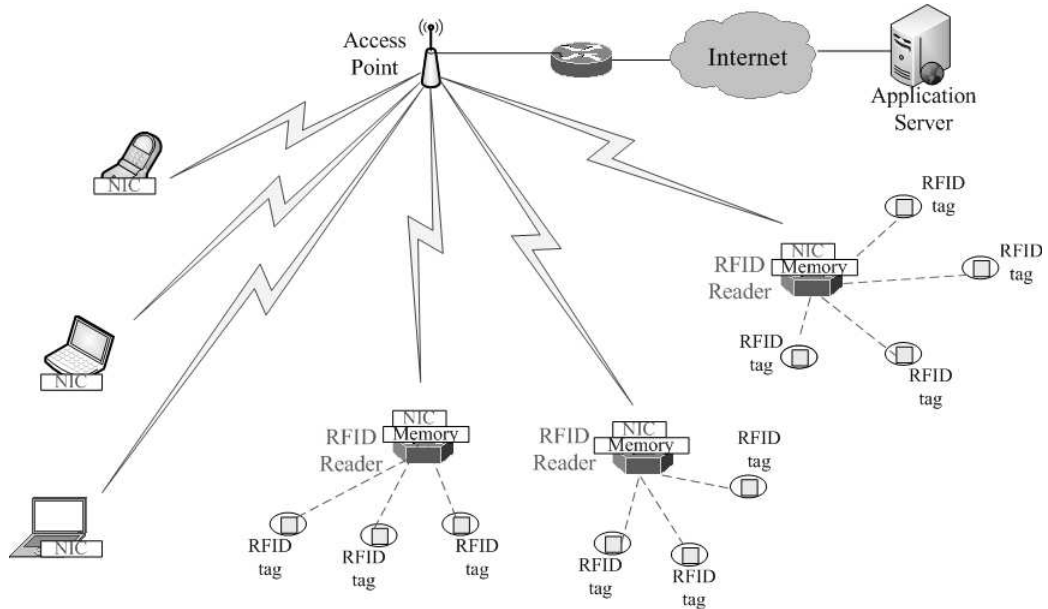


Figure 3.1: The overview of proposed topology.

As it is shown in the figure, wireless devices and RFID readers and tags exist in the same area. RFID readers will collect tags' data and send it to AP. Furthermore, AP

will collect all the data from wireless terminals and RFID readers which are considered as wireless devices themselves. Moreover, all wireless devices are connected to the WLAN via their embedded Network Interface Card (NIC). RFID readers will also have NIC and extra memory.

Let's define the communication cycle according to the IEEE 802.11 definitions: As it was defined in Section 2.3, during the CFP or PCF period, the whole wireless devices will be silent and only RFID readers will collect data from RFID tags in their range using Framed Slotted Aloha or IEEE 802.15.4 protocol (it depends on which anti-collision protocol we are using in our solution, as we are suggesting two separate solutions at the RFID side: one solution using Framed Slotted Aloha, another using ZigBee protocol. At the Wi-Fi side for both solutions, we use IEEE 802.11). After that, during the CP or DCF period, wireless devices including the RFID readers (which will act like other wireless devices in the area) will send their data to AP. During this period, AP and wireless devices will communicate with each other via the DCF technique.

In this project, some parameters will be chosen or calculated in order to obtain the best overall performance in the network. Some of these parameters which are the most challenging part of the network design can be summarized as finding answer to the following questions:

- What is the optimum duration for PCF period (CFP), DCF period (CP) and Beacon size in order to balance the data collection from Tags to readers and also the reader to AP (If PCF is too short, readers cannot read tags' ID properly and if DCF is too short, the devices and readers can not send their data and

saturation occurs)?

- How to define the length of the reading frames?
- What is the best value for probability P_{sleep} (discussed at Section 2.1.4: The calculations of sleeping period)?
- How to integrate the polling commands with the start of IEEE 802.15.4 super-frame?
- What will the answer to that polling be?

In our solution, we are trying to give the medium possession to RFID and Wi-Fi networks in a fairly order and duration to enhance the performance of this multiple network environment. As we mentioned in Chapter 2, IEEE 802.11b and IEEE 802.15.4 and Microwave RFID have interference issues in ISM frequency band. One of the possible solutions which we are using is IEEE 802.11 PCF protocol. By using PCF protocol, during the PCF period, all of Wi-Fi devices will be stopped from sending and receiving frames, so RFID nodes can communicate with their reader using Framed Slotted Aloha or IEEE 802.15.4 standard without the interference of Wi-Fi nodes and after PCF period, the medium possession will be given to Wi-Fi nodes and they should compete with each other to access the medium using IEEE 802.11b DCF.

3.1 Time schedule in the proposed solution

Now let's take a closer look at the proposed solution. Figure 3.2 illustrates the overall solution. Each cycle starts with a Beacon from Access point (AP). This beacon includes cycle length. Then AP will send the polling frame and it will poll the prospect RFID reader. In this solution, during each PCF period, only one RFID reader will be polled and readers are polled in a round robin order (one reader during each cycle). Then the polled reader will send an acknowledge frame to AP. After that the Medium is dedicated to the polled reader until the end of PCF period. At the end of PCF period, the active reader will send a CF-END frame to AP to announce the end of its activity. If the CF-END frame is not received after CFPMaxDuration, the AP will terminate the PCF period itself. During the PCF period other readers and all Wi-Fi devices are waiting in a NAV state and they are not trying to send anything. As the Wi-Fi nodes are not active, the RFID network can work properly during PCF period. During this period the active reader will collect the information frames from the RFID tags and at the end of PCF period, it will aggregate those frames and create a new data frame which includes all collected IDs of that cycle. During DCF period, RFID reader will act as a Wi-Fi device and it will compete for the medium to send aggregation data frame. During DCF period, all Wi-Fi devices and RFID readers will totally work according to the IEEE 802.11b definitions.

It should be mentioned that the last cycle of each complete Beacon Interval is reserved for the future use and adding a new reader to the overall design. During this time the Wi-Fi network will be active so the system is working in DCF mode.

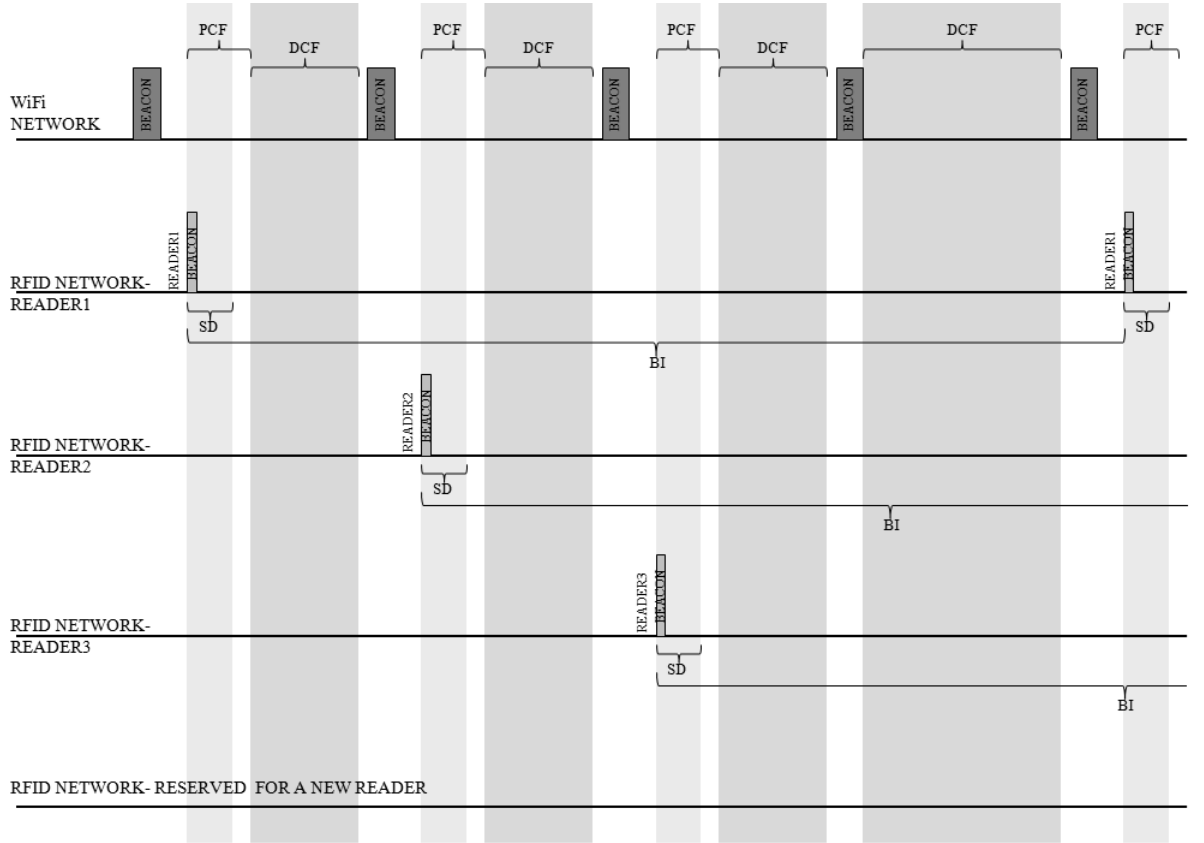


Figure 3.2: The overall of proposed solution.

In Figure 3.3, a cycle of transmission has been shown in details. After the synchronization beacon signal from AP and waiting for SIFS time period, AP will poll the target reader (readers are polled in a round robin order.) with a polling frame and after SIFS time period, AP will receive an ACK frame from the prospected reader. Then the chosen reader will send a beacon signal to its covered area and the awake tags in that area will try to send their IDs according to the described pattern in next paragraph. After the SD period, active reader will send a CF-End frame to AP and then Wi-Fi devices will start working. At the end of this DCF period, AP will wait for PIFS time period and another cycle will start with another beacon signal. It

should be mentioned that readers are working in two modes: During the SD period they will collect IDs of tags which are active in their area and during the DCF period they will work as a Wi-Fi device and they will aggregate the collected data from tags and compete with other Wi-Fi devices for access to medium and they will try to send the aggregated frame to AP.

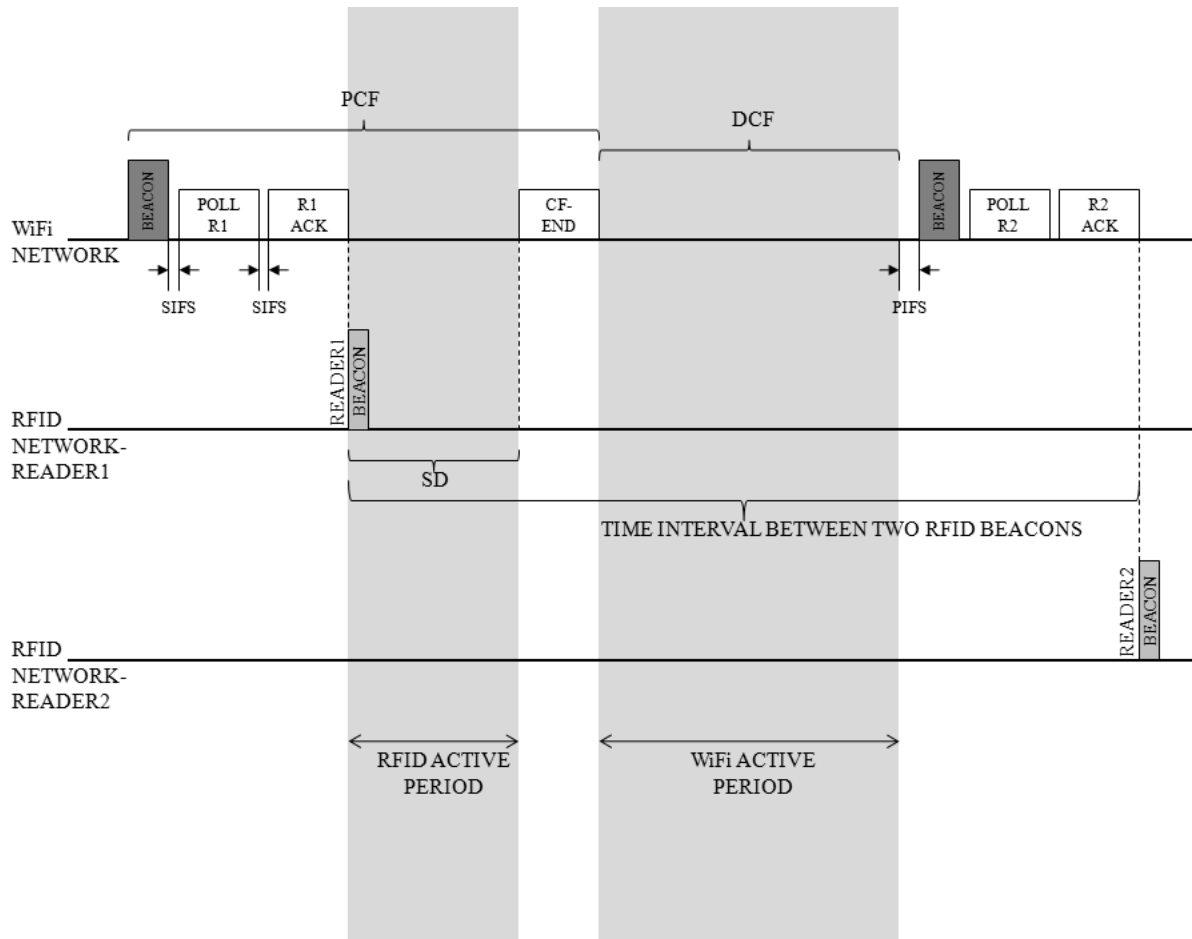


Figure 3.3: A typical cycle in the proposed solution.

Moreover, RFID tags are mostly sleep due to the energy consumption and also collision issues and they will wake up periodically and not synchronous with each other

(eg. one time each hour) and search for a beacon signal. If no beacon is found they will wait for beacon signal. When finding a beacon signal the tag makes a back-off for a random time and then in ZigBee based model, performs a carrier sense according to the IEEE 802.15.4 protocol definitions. If no other carrier is sensed, the tag transmits its payload packet, waits for acknowledge from the reader, and then returns to sleep until the next cycle starts. In the Framed Slotted Aloha based model, the tag will wait for a random time and after sending its packet, it will wait for acknowledgement from reader and it will return to sleeping mode. In some solutions tag will go back to sleeping mode if no beacon signal is sensed [30], but in our solution it will wait for sensing the next beacon signal.

3.2 Basic Parameters and Calculations of Solution

In this subsection, we will present the used parameters and calculations for our simulation. The main parameters and their values are exactly derived from the standards and other required values and timings in this project are calculated by using the basic parameters.

3.2.1 Parameters for Wi-Fi and IEEE 802.15.4

Table 3.1 illustrates most of the parameters and timings which are used in our solution.

The size of Wi-Fi beacon interval is $100TU$ by default while TU is $1024\mu s$. So, if we put $SO = 0$, then $SD = 480 * 2^0 Bytes = 480 Bytes \equiv 15.36ms$. As it is shown in Figure 3.2, the size of the superframe at the RFID side is four times the superframe

Table 3.1: Timing parameters in beacon enabled operating mode [27].

Wi-Fi time slot	$20\mu s$
Wi-Fi Time Unit (TU)	$1024\mu s$
SIFS	$10\mu s$ or $0.5 Wi - Fi$ time slot
PIFS	$30\mu s$ or $1.5 Wi - Fi$ time slots
DIFS	$50\mu s$ or $2.5 Wi - Fi$ time slots
Wi-Fi data rate	$2Mbps$
Wi-Fi beacon size	$2 Wi - Fi$ time slots
Polling frame	$14 Wi - Fi$ time slots or $20Bytes$
Polling ACK frame	$14 Wi - Fi$ time slots or $20Bytes$
CF-END frame	$14 Wi - Fi$ time slots or $20Bytes$
RTS frame	$14 Wi - Fi$ time slots or $20Bytes$
CTS frame	$13 Wi - Fi$ time slots or $14Bytes$
DCF ACK frame	$13 Wi - Fi$ time slots or $14Bytes$
Contention Window in Wi-Fi network	$CW_{min} = 32$ $CW_{max} = 1024$
RFID time slot	$320\mu s$ or $16 * Wi - Fi$ time slots
RFID beacon size	$2 RFID$ time slots
RFID data rate	$250kbps$
Contention Window in RFID network	$CW_{min} = 7$ $CW_{max} = 31$
Total size of ID transmission frame for RFID	$30Bytes$ or $3 RFID$ time slots
Wi-Fi superframe	$122.88ms$ or $120TU$ or $6144 Wi - Fi$ time slots or $384 RFID$ time slots
RFID superframe or BI	$491.52ms$ or $480TU$ or $1536 RFID$ time slots or $24576 Wi - Fi$ time slots

size in Wi-Fi side and the size of a typical RFID cycle is equal to superframe size in Wi-Fi side and it is only shifted. Therefore if we have $BI = 2^{BO}SD \approx 4 * 100TU$, then $BO \approx 4.7$ and if we round BO to 5 then $BI = 32 * 15.36 = 491.52ms$ which will be the superframe size. In other word we can say $BI = 32 * 48 * 16 * 20\mu s = 15 * 2^{15} = 480 * 2^{10} = 480TU$ which is a close amount to default value of $400TU$. Also in RFID scaling we have $BI = 32 * 48 * RFIDtimeslot = 1536RFIDtimeslot$. Moreover in Wi-

Fi scaling, $Wi-Fi_{superframe} = 8*48*16*Wi-Fi_{timeslot} = 6144Wi-Fi_{timeslot}$.

Furthermore, according to the first presentations of IEEE 802.15.4f [4] and parameter suggestions, Total size of the ID frame (with headers and etc) for Active RFID is 30 Bytes. Thus we have $30 * 8/250kbps = 0.96ms$ and $0.96ms/0.320ms = 3RFID$ time slots for the total size of mentioned frame.

Tags' Sleeping Patterns and Parameters

Sleeping patterns of RFID tags and their average sleeping time and sleeping probability (P_{sleep}) were defined in Section 2.1.4 and we discussed about how to calculate sleeping probability (P_{sleep}).

In Table 3.2, Average Sleeping Time in minutes or hours and in time slots and also their corresponding sleeping probability for ZigBee protocol are presented.

Table 3.2: Sleeping parameters for ZigBee protocol.

Average Sleeping Time in hours or minutes	Average Sleeping Time in Time slots	Sleeping Probability (P_{sleep})
1 minute	115207.3733	0.9999913200
2 minutes	230414.7465	0.9999956600
5 minutes	576036.8864	0.9999982640
10 minutes	1152073.733	0.9999991320
15 minutes	2812500	0.99999964444444444444
0.5 hour	5925000	0.99999982222222222222
1 hour	11250000	0.99999991111111111111
1.5 hour	16875000	0.99999994074074074074
2 hours	22500000	0.99999995555555555556

3.2.2 Parameters for Framed Slotted Aloha

When we decided to use Framed Slotted Aloha instead of IEEE 802.15.4, we were trying to provide an environment which is similar to the ZigBee model. Otherwise, we would not be able to compare or evaluate the performance of two models. Table 3.3 is presenting our selected parameters for two models and it is showing how we tried to choose parameters carefully which are not only totally matching their related standards, but also close enough to each other to prepare similar conditions for both models and further comparison.

Table 3.3: Basic parameters for ZigBee and Framed Slotted Aloha protocols.

Basic Parameters	ZigBee Protocol (IEEE 802.15.4)	Framed Slotted Aloha Protocol (ISO18000-4)
Data Rate	250 <i>kbit/s</i>	384 <i>kbit/s</i>
Time slot Size	320 μs	520.8 μs
bits/Bytes per Time slot	80 <i>bits</i> or 10 <i>Bytes</i>	200 <i>bits</i> or 25 <i>Bytes</i>
No of Time slots per active period	48	14
Packet Size	3 <i>Timeslots</i> or 30 <i>Bytes</i>	1 <i>Timeslot</i> or 25 <i>Bytes</i>
Minimum Active period	15.36 <i>ms</i>	7.2912 <i>ms</i>

It should be mentioned that Wi-Fi parameters are the same as what we defined in Section 3.2.1 for both versions of the solution.

Tags' Access Probability

As it was defined in Section 2.1.5, The RFID reader will send its beacon toward the tags in its vicinity and the awaken tags will compete to access the RFID medium during the active period (which in our case is 14 RFID time slots). Tags that have sent their IDs successfully will go back to sleep. After active period time is over for

unsuccessful tags, they should wait for next active period to send their data to their related reader.

It is mostly probable that at the start of each active period, most of the awaken tags will try to access the RFID medium. In reality, most of collision are occurring at the beginning of the active period or few first time slots of that period. In order to simulate this behavior properly in our model, we came to the idea of using the Geometric distribution for simulating the tags behavior for Medium possession/access. So, in our model, at the beginning of active period, awaken tags will choose a random delay time using the Geometric distribution with a specific access probability (as input argument for Random Geometric function) and after that random delay time, it will send its data toward the RFID medium and the transmission result can be successful or unsuccessful. In latter case, Tag will try to retransmit during the next active period and will try with another random delay.

After using different access probabilities as input argument for Random Generator function (which is using Geometric distribution) and doing some calculations, we are currently using 0.75 as the chosen access probability. According to our calculations and trials, it seems that 0.75 access probability (P_a) is providing a proper distribution for the random chosen delays for tags before sending their data to RFID medium and it will reduce the several trials of tags at the beginning of active period and spread the access trials toward the middle and end of active period, (whereas it is still not far from the mentioned behavior of tags at the start of active period). Thus, we are using "*Rnd Geom(Access Probability (P_a) = 0.75) mod 14*" as the random delay generator for tags' access trials. we are rounding the random delay to 14 because

we want to be sure our access trials are not occurring after the active period (which is limited to 14 time slots), although with choosing 0.75 as access probability (P_a) this case will rarely happen in our simulation and this argument is mostly producing reasonable random delays itself without using modulation operator.

Tags' Sleeping Patterns and Parameters

In Table 3.4, Average Sleeping Time in minutes or hours and in time slots, Also their corresponding sleeping probability for Framed Slotted Aloha protocol are presented.

Table 3.4: Sleeping parameters for Framed Slotted Aloha.

Average Sleeping Time in hours or minutes	Average Sleeping Time in Time slots	Sleeping Probability (P_{sleep})
1 minute	187500	0.9999946667
2 minutes	375000	0.9999973333
5 minutes	937500	0.9999989333
10 minutes	1875000	0.9999994667
15 minutes	1728110.59	0.99999942133333333333
0.5 hour	3456221.98	0.99999971066666666667
1 hour	6912442.39	0.99999985533333333333
1.5 hour	10368663.59	0.9999999036
2 hours	13824884.79	0.99999992766666666667

Tags' Collision Probability

One of the most important parameters in a network is collision probability and the network designers are trying to minimize this parameters in their design to enhance the network's performance. In this section, we will discuss about how to calculate

these parameters and in the following chapter, we will evaluate the measured results for collision probability and some other parameters.

As the tags are mostly sleep according to the mentioned pattern, So the access probability for awaken tags (P_{av}) can be calculated as:

$$P_{av} = (1 - P_{sleep}) * P_a$$

Which P_{sleep} and P_a are sleeping probability and access probability relatively.

Moreover, according to definitions in Section 2.1.5, transmission probability in k^{th} slot ($P_{slot[k]}$) can be calculated as:

$$P_{slot[k]} = P_{av} * (1 - P_{av})^{((k-1) \bmod 14)}$$

In Figure 3.4, the output graph of latter formula ($P_{slot[k]}$) has been plotted for different slots while P_a is changing. In this example, average sleeping time is 15 minutes (Therefore $P_{sleep} = 0.99999942133333333333$).

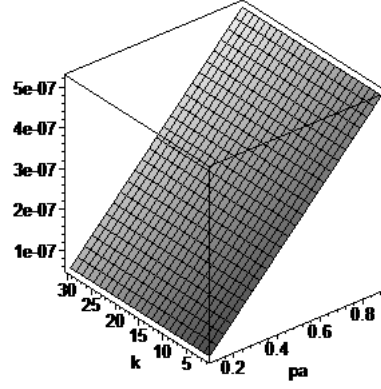


Figure 3.4: An example of $P_{slot[k]}$.

According to Figure 3.4, transmission probability in slot k is not dependant on k ,
Thus after this, we will denote it as P_{slot} or:

$$P_{slot} = P_{slot[k]}$$

and collision probability (P_{coll}) can be calculated as:

$$P_{coll} = 1 - \text{Idle probability} - \text{Success probability}$$

As:

$$\text{Idle probability} = (1 - P_{slot})^N$$

Which N is the number of tags in each network and:

$$\text{Success probability} = N * P_{slot} * (1 - P_{slot})^{(N-1)}$$

Thus:

$$P_{coll} = 1 - (1 - P_{slot})^N - N * P_{slot} * (1 - P_{slot})^{(N-1)}$$

3.3 The Simulation Model

In order to measure the performance of our model, we are trying to simulate our solution using Artifex simulation environment. Artifex simulation environment is based on Extended Petri Nets and it is integrated with standard programming languages like C and C++. In mentioned environment, we simulate our models from scratch and the simulation results (measurements) will go to some text files directly. Afterward, we are using the Maple environment to draw the related plots. Artifex provides a flexible environment for the implementation of different models and according to the definition of several details and features in wireless network protocols and standards, it is a proper environment for simulating these features and observing the behavior of different elements. In Figure 3.5, we have presented the structure of our simulation model, different elements or classes and the related links. According to our model, the access point is controlling the schedules and the transmissions. RFID readers act as both Wi-Fi device and RFID coordinator. Tags are connected to their Readers via RFID medium and Wi-Fi devices and RFID readers are connected to AP via Wi-Fi medium.

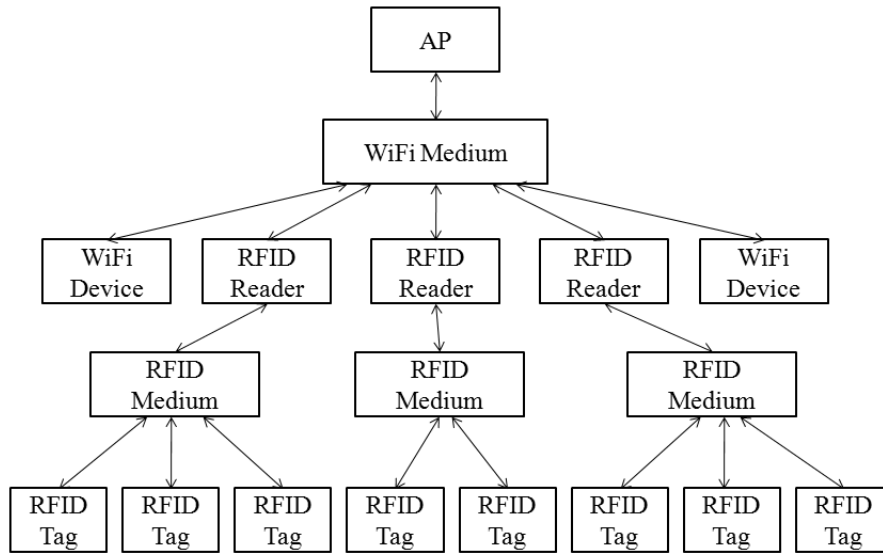
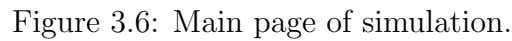


Figure 3.5: The overview of simulated model and its classes.

In Figure 3.6, the main page of our simulation is illustrated. Classes presented in this figure and the communication between classes are same as they were defined in Figure 3.5. Moreover, the classes are connected to the Measurement page via RECORD:MEASUREMENT place.



- Collision probability
- Average number of collision in each superframe
- Average waiting time of tags for beacon after waking up

- Average number of awake tags in each superframe
- Average collision position in each superframe
- Average successful position in each superframe

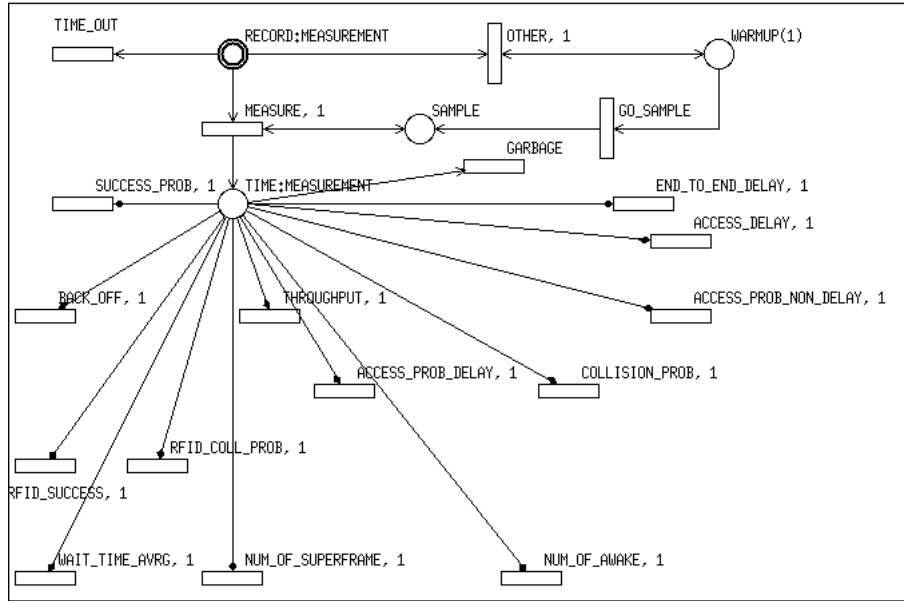


Figure 3.7: Measurement page.

3.3.1 Access Point

Access point is the coordinator of Wi-Fi nodes and RFID readers and it will communicate with it Devices via PCF mechanism. Figure 3.8 shows the flow of sent and received packets for Access Point. In this page, four types of packet from Devices will be received: Data, RTS, ACK and CTS. After receiving each of these packets, the coordinator will react differently and in most cases, it will prepare a response

3.3.2 Wi-Fi Medium

This class includes the simulation of Wi-Fi medium and it is displayed in Figure 3.9. This page includes two parts: The backoff generation part and packet transmission part. The backoff generation part generates one backoff each time slot and the timing of PCF and DCF period will be kept. This generated backoff will be sent to other classes for announcing the medium status (whether it is busy or idle) and to measurement page for statistic issues and also for establishing synchronization in the model. The packet transmission part is relaying packets from Wi-Fi device/RFID reader to Access Point and vice versa. It is also checking if collision has occurred during packet transmission or not. In case of collision occurrence, This page will report it to measurement page. Otherwise if collision does not occur, the received packet will be send to the specified destination. Furthermore, this page will generate appropriate delay with the time length of packet size (in timeslot) and during this time, the medium is set to busy. Otherwise, the medium is idle.

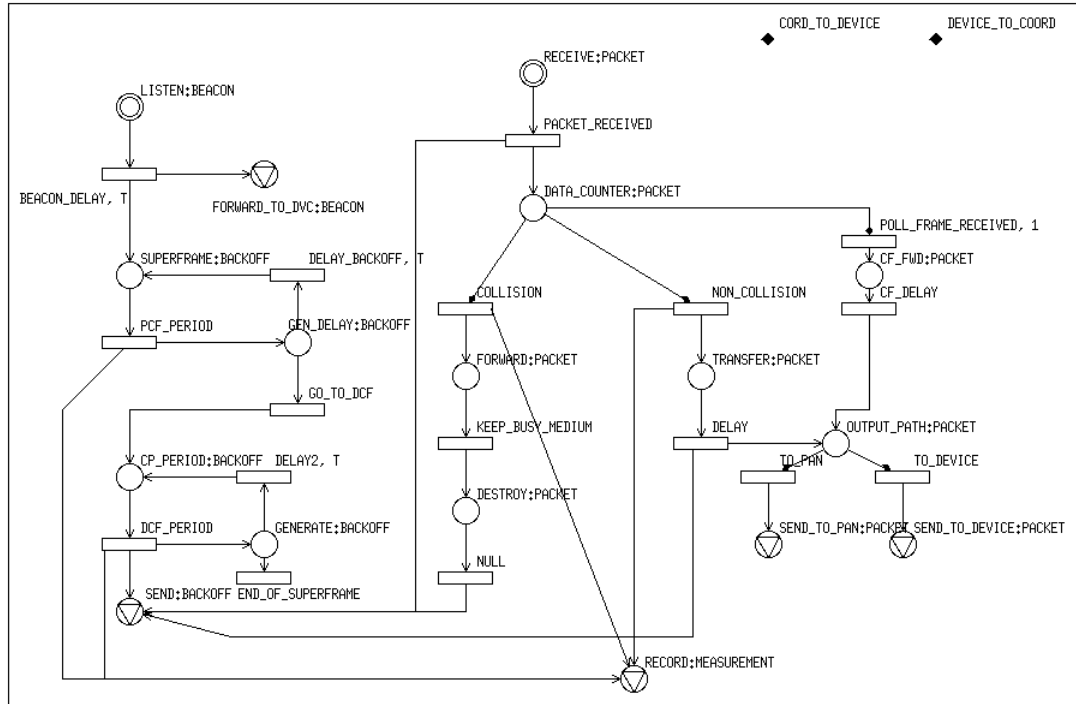


Figure 3.9: Wi-Fi medium class.

3.3.3 Wi-Fi Device

Wi-Fi Device class includes three pages: Main page, Data generating and waiting page and CSMA/CA page. Figure 3.10 presents the Main page of Wi-Fi Device class which shows the flow of sent and received packets for a station. Similar to the main page of Access Point class, in this page, four type of packets can be received by the Wi-Fi Device: Data, RTS, ACK and CTS. After receiving each of these packets, the Wi-Fi Device will react differently and in most cases, it will prepare a response packet for Access point and send it through Wi-Fi Medium.

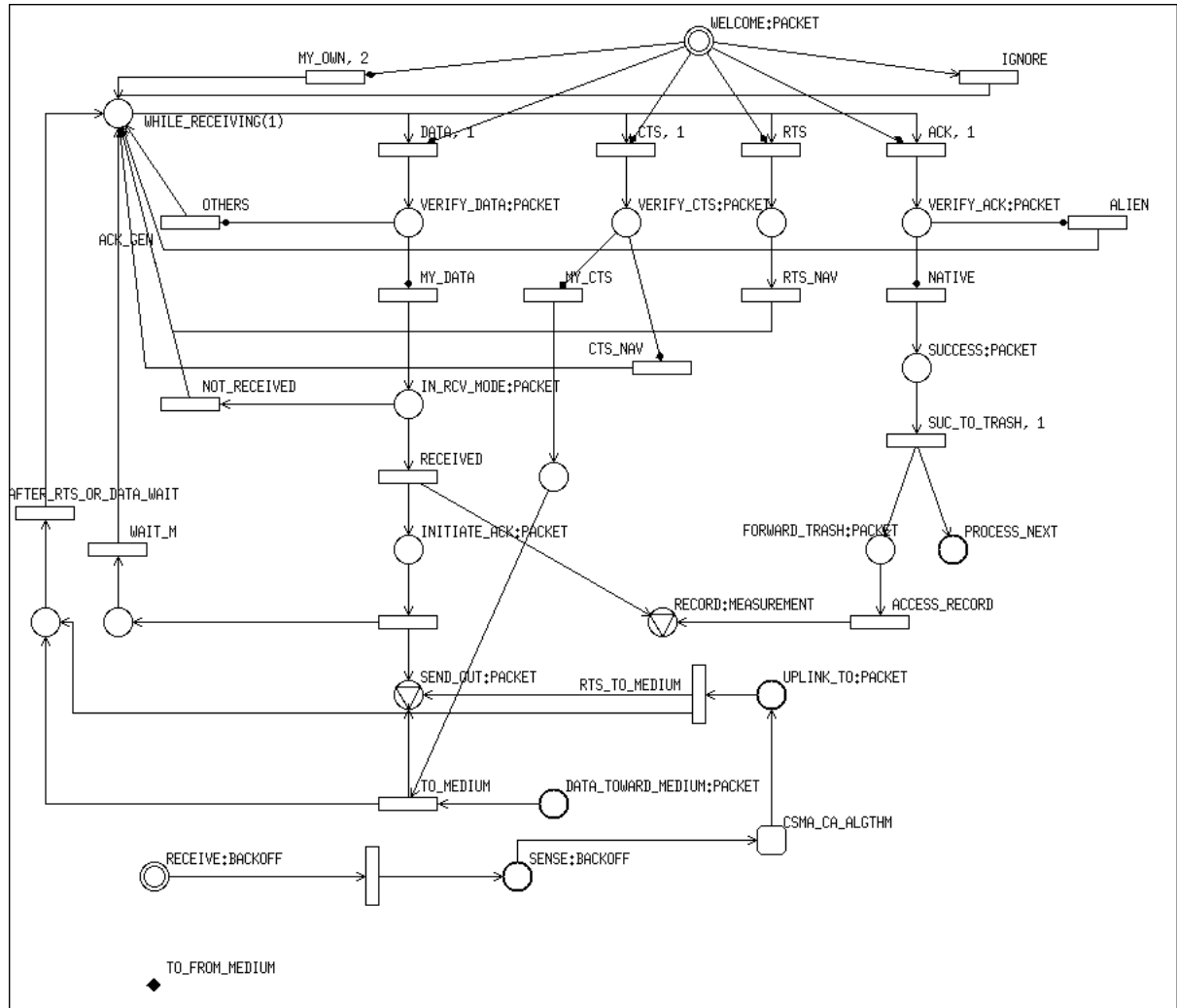


Figure 3.10: Wi-Fi device: Main page.

In Figure 3.11 Data generating and waiting page have been displayed which is where data and RTS packet is generated for station. The data will be generated with a negative exponential distribution timing. After that, if there is no other data packet

in process, it will be ready to go toward the medium (though after the CSMA/CA process for its RTS packet). But if another data packet is in process, the generated data packet should go to the WAIT-DATA and wait in a queue until the previous data packet transmission cycle is done. Moreover, when data is generated and it is ready to go toward medium, according to the standard, a RTS packet will be generated in this page and it will be sent to CSMA/CA page for the CSMA/CA process.

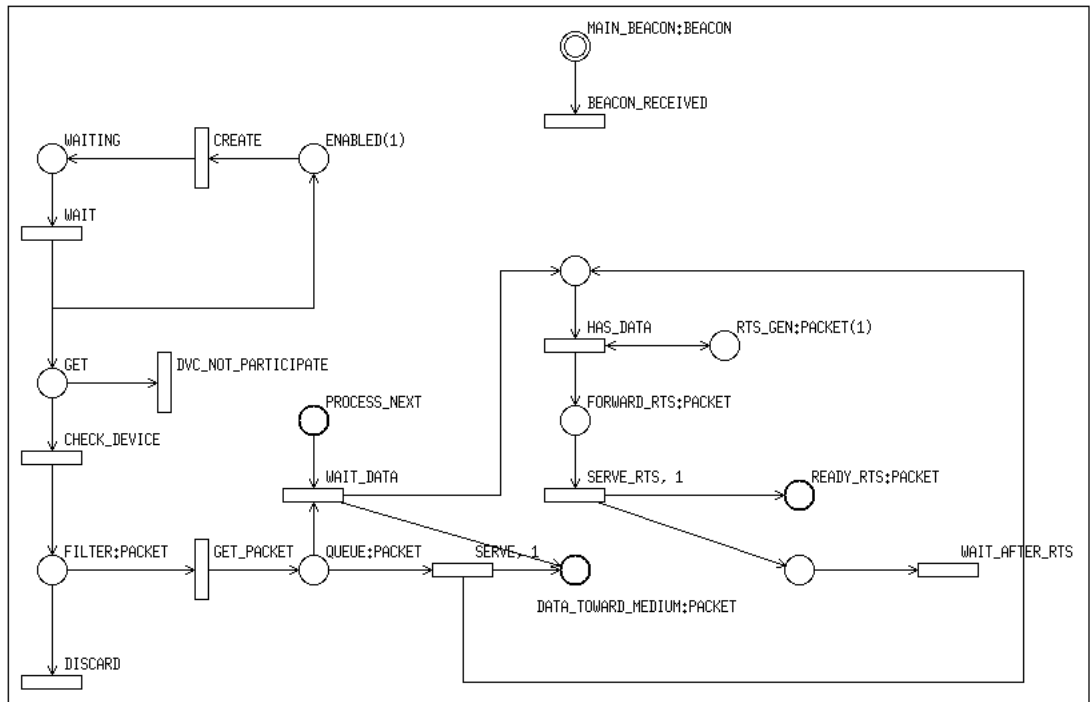


Figure 3.11: Wi-Fi device: Data generating and waiting page.

Figure 3.12 presents the CSMA/CA page for device which is where the CSMA/CA logic is implemented for station. The CSMA/CA logic used in this page works similar to the relevant page in Access Point: Firstly, the generated RTS will be received from READY-RTS place and after that in INITIALIZE process, a random number will be chosen for random counter. then this random counter will be decremented one by one and for each time slot, the medium status will be checked. if the medium is idle, it will continue on decrementing and after the counter becomes zero, if the medium is still idle, it will send the RTS packet toward the medium. otherwise if the medium becomes busy at this moment, packet will go to the RETRANSMIT phase and the contention windows will be doubled and the random countdown process will be repeated. This process can be repeated up to seven times. Moreover, if during the countdown process, medium becomes busy, the counter will go to a freezing mode and after the medium becomes idle, it will continue the countdown process from the frozen amount. Moreover, the initial amount for contention window in this protocol is 32 and its maximum amount can be 1025.



This class is similar to Wi-Fi Device, but it is connected to both Wi-Fi and RFID network. It includes three similar pages: Main page, Data generating and waiting page and CSMA/CA page. As it is illustrated in Figure 3.13, which is the main page of RFID reader, the packet transmission part is same as Wi-Fi Device's main page.

RFID reader's main page also includes the coordinator part for RFID network.

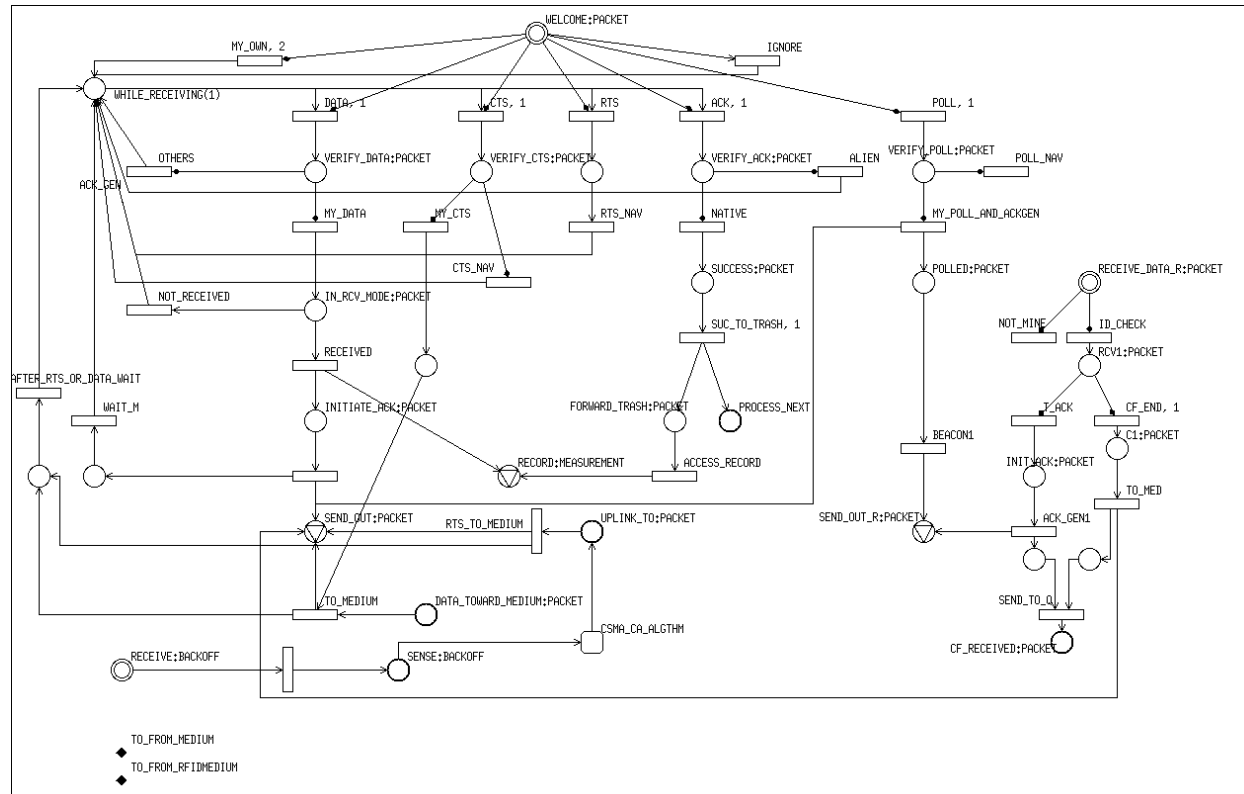


Figure 3.13: RFID reader: Main page.

The Data generating and waiting page for RFID reader is similar to the Wi-Fi Device's version, but the data will be generated using the collected data from RFID tags. Moreover, this page will receive the periodic beacons from Access Point to know which reader should be active during this period.

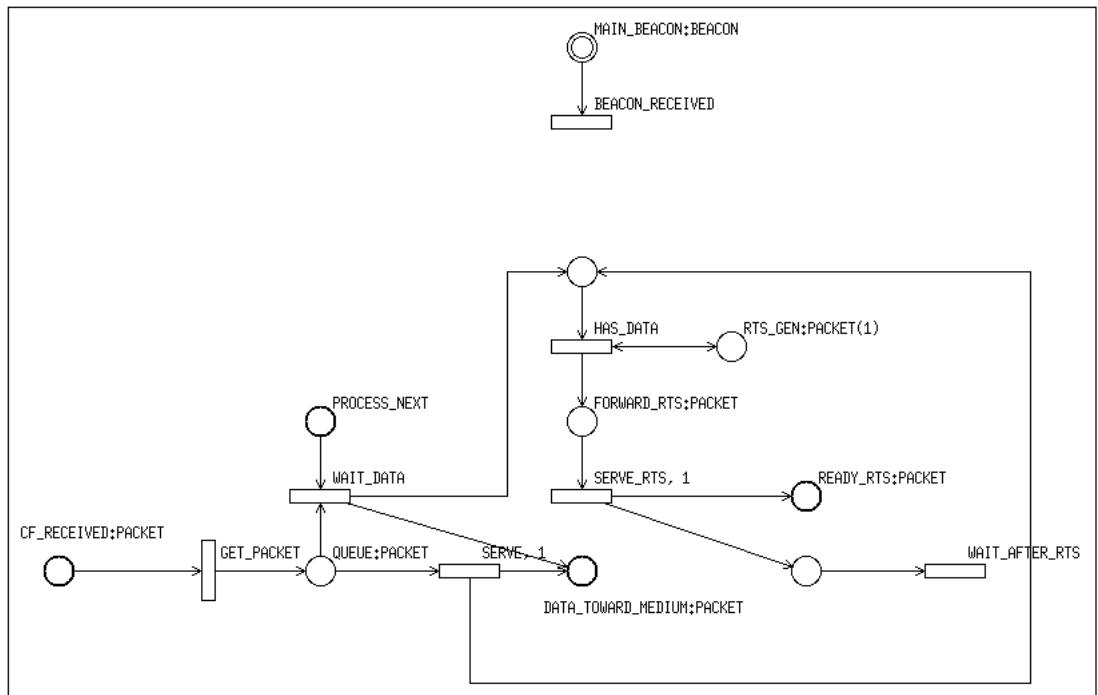


Figure 3.14: RFID reader: Data generating and waiting page.

Figure 3.15 presents the CSMA/CA page for RFID reader and it is similar to the Wi-Fi device's version of CSMA/CA page and the processes are same as CSMA/CA processes in Wi-Fi device.

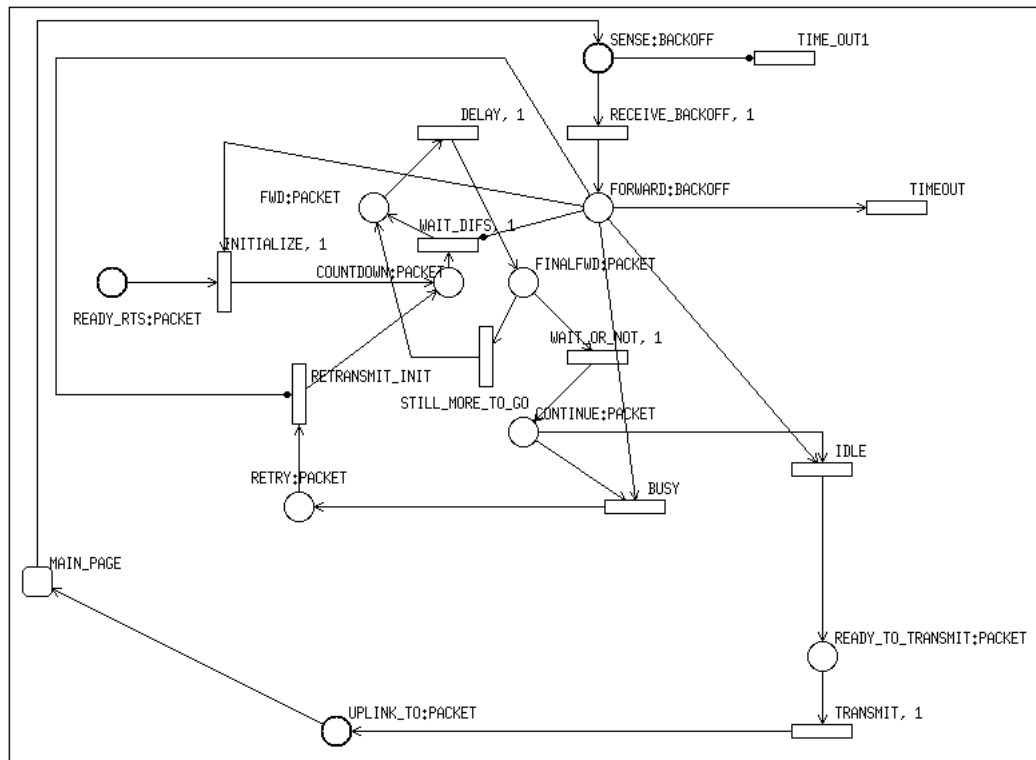


Figure 3.15: RFID reader: CSMA/CA page.

3.3.5 RFID Medium

In Figure 3.16 RFID medium is illustrated which is similar to Wi-Fi Medium page, but in RFID Medium only RFID timings will be kept.

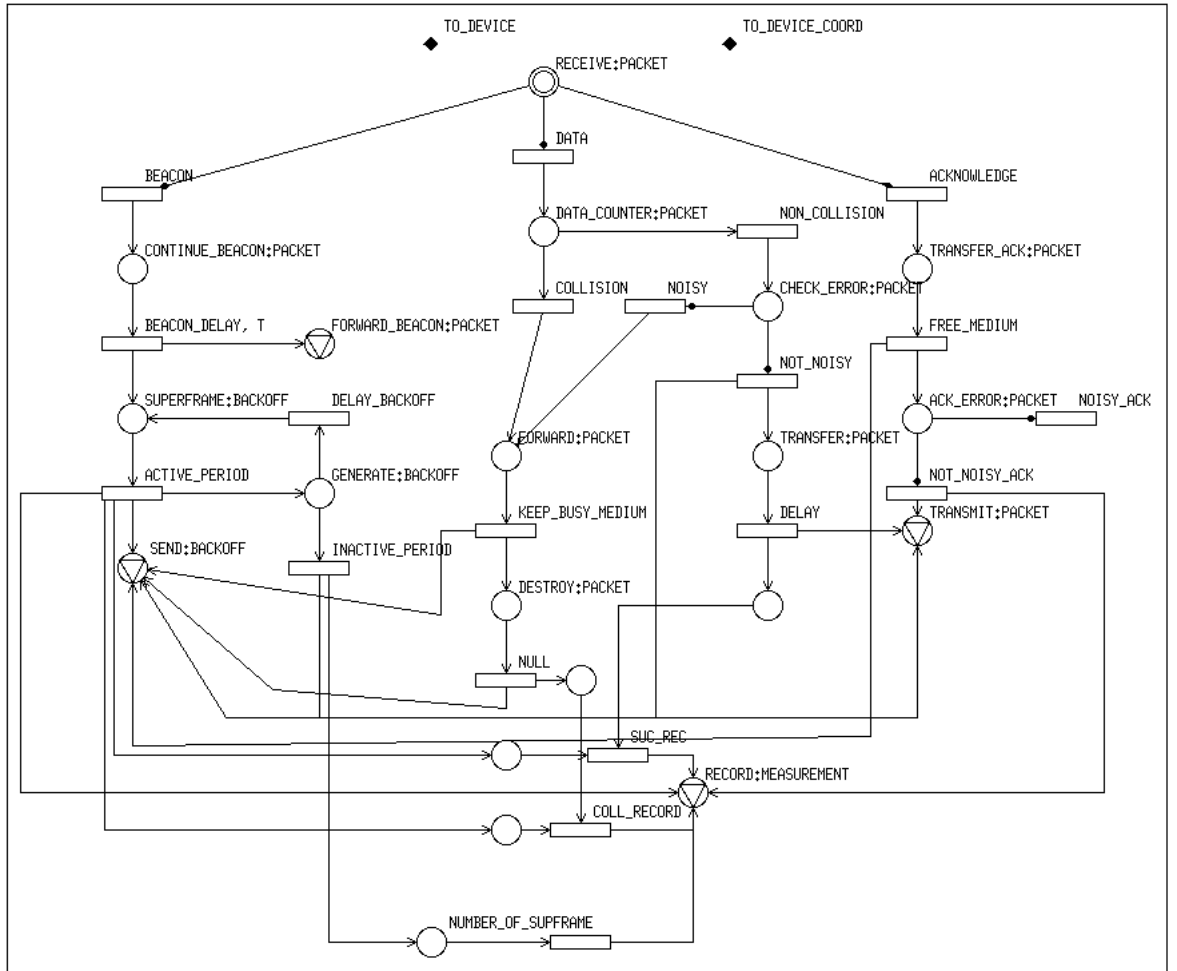


Figure 3.16: RFID medium class.

3.3.6 RFID Tag: Framed Slotted Aloha version

In both Framed Slotted Aloha and ZigBee versions of simulation, the six classes (Main, Access Point, Wi-Fi Device, Wi-Fi Medium, RFID Reader and RFID Medium classes) are same and the connections among classes are same and only the RFID Tag class is different for these two models.

RFID tag class includes three pages: Main page, Data generating and waiting page and Anti collision mechanism page. In Figure 3.17 which is the main page of this class, data packet will be send to RFID Medium and its acknowledgement will be received. Moreover, the sleeping timing and vicinity checking for tag are simulated in this page.

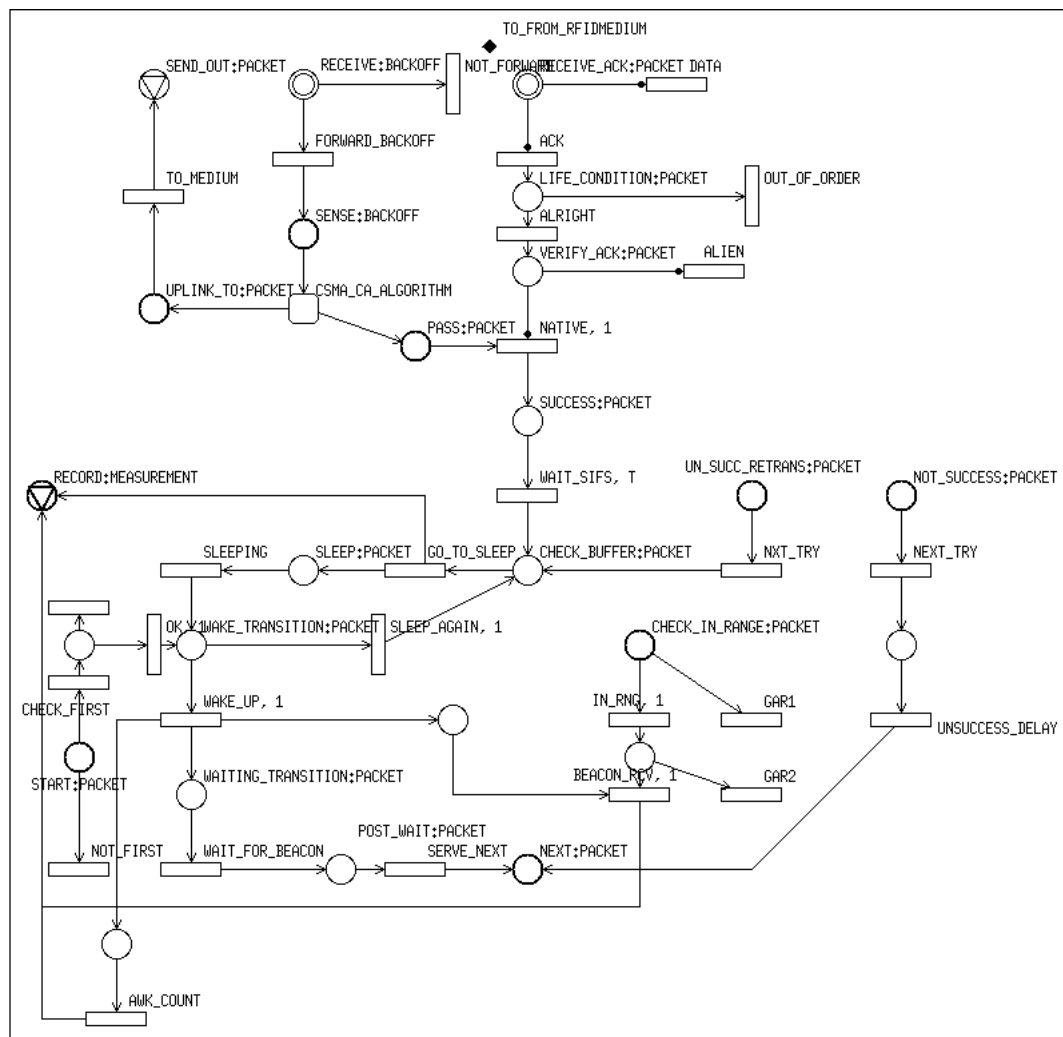


Figure 3.17: RFID tag: Main page for Framed Slotted Aloha.

In Figure 3.18, the data generating and waiting page is presented and it is similar to Wi-Fi Devices version. Furthermore, this page is receiving the periodic beacon from RFID Reader and according to the active reader, the availability of the tag (according to its vicinity) will be checked.

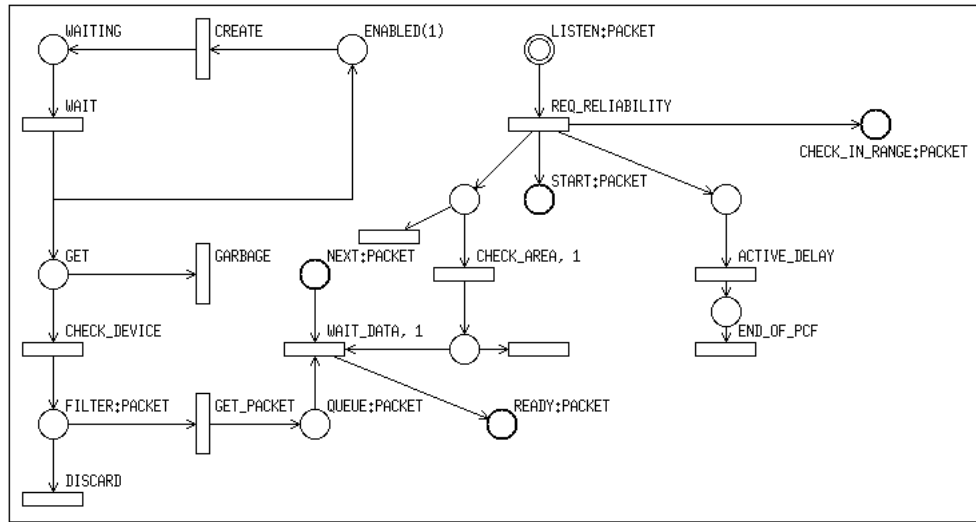


Figure 3.18: RFID tag: Data generating and waiting page for FSA.

Figure 3.19 presents the Anti collision mechanism page for RFID tag and it is implementing Framed Slotted Aloha protocol.

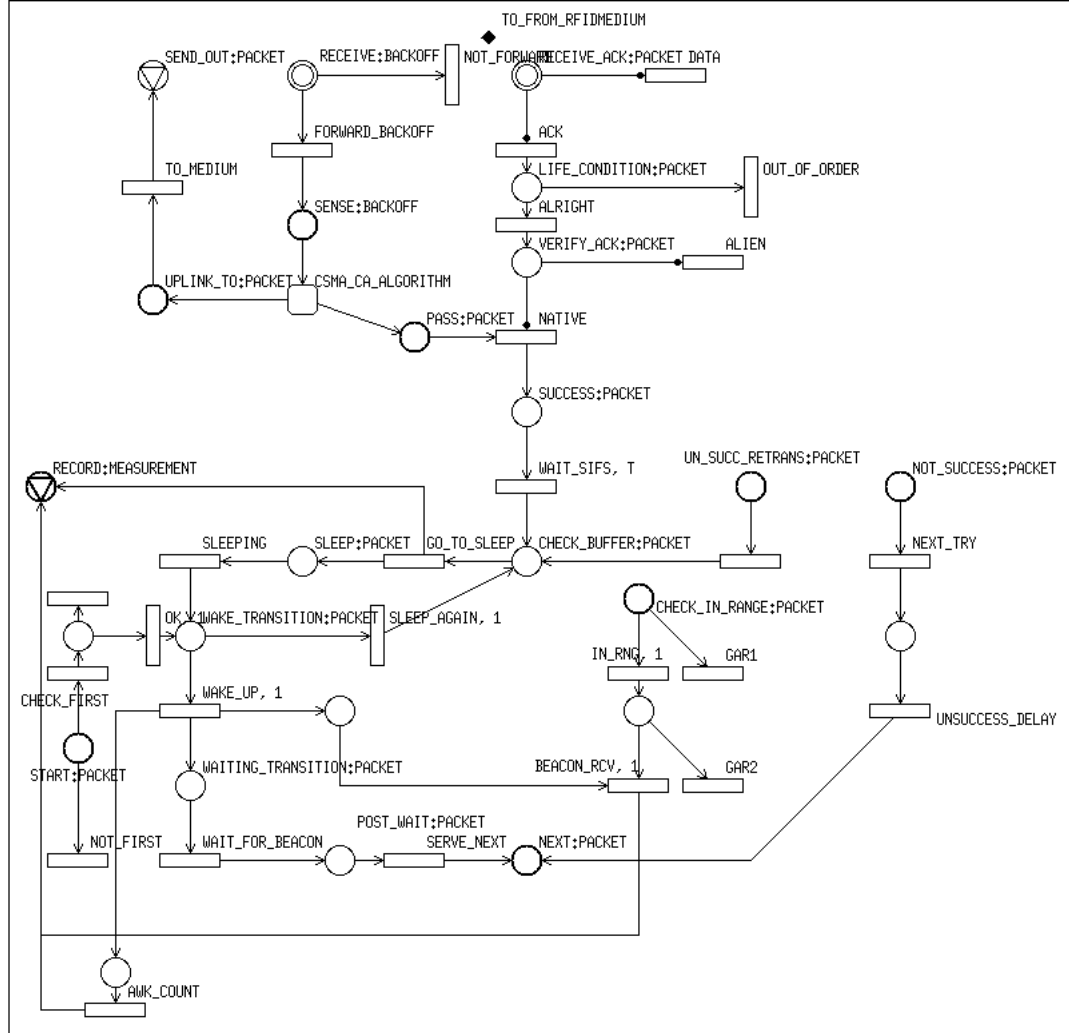


Figure 3.20: RFID tag: Main page.

In Figure 3.21, the data generating and waiting page is presented and it is similar to corresponding page in RFID tag class of Framed Slotted Aloha model. Furthermore, this page is receiving the periodic beacon from RFID Reader and according to the active reader, the availability of the tag will be checked.

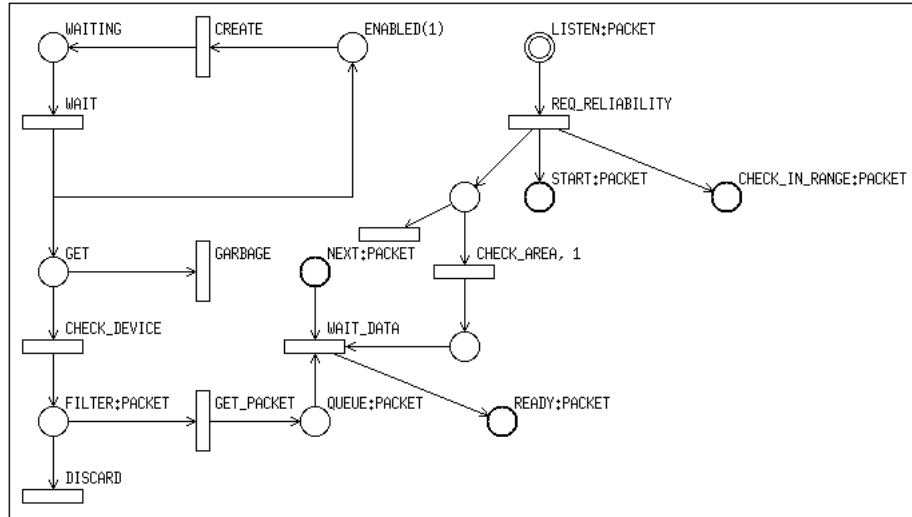


Figure 3.21: RFID tag: Data generating and waiting page.

Figure 3.22 presents the CSMA page for RFID tag and it is implementing IEEE 802.15.4 or ZigBee protocol. The details of CSMA mechanism for IEEE 802.15.4 standard has been defined in Section 2.1.6.

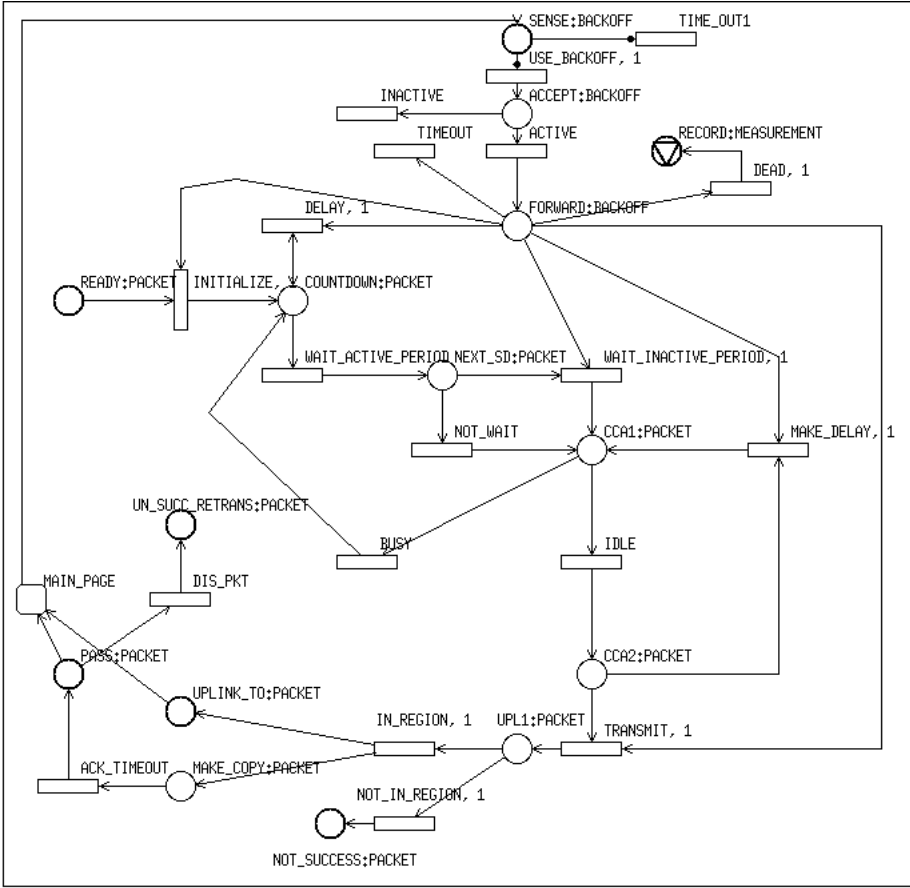


Figure 3.22: RFID tag: CSMA page.

Chapter 4

Simulation Results and Analysis

In this section, the simulation results have been shown. As we mentioned in previous chapter, we are testing two scenarios: In the first one, we are using Framed slotted Aloha as the anti-collision standard for RFID networks and in the second scenario, we are using ZigBee MAC standard(IEEE 802.15.4 standard) for RFID networks. The Wi-Fi network for both solution is same and it is using IEEE 802.11 standard for communication among the nodes. In both models we are testing two scenarios:

1. Constant average sleeping time for RFID tags (average sleeping time = 1 minute) and variable number of tags in each RFID network (10,30,60,90,120 nodes).
2. Constant number of tags in each RFID network (90 tags in each RFID network) and variable average sleeping time for RFID tags (1,2,5,10,15 minutes).

It should be mentioned that in our tests, we should use average sleeping time of one hour or two hours which is more realistic, But in that range there were some restrictions in our simulation. In case of choosing one hour average sleeping time, we would hardly experience any collisions (e.g. one collision in 200 million time slots of running the simulator, which means one week run time for only one sample. On the other hand, we should add the warm up time of the system to the total run time. This warm up time is the required time to have a stable system and it takes several complete cycles of our Beacon Interval(BI) and it can exceed several million time slots of run time). Thus, in that case, we would have some limitations in getting proper and reliable samples. Therefore we are considering shorter times for average sleeping time and in most samples, we were using few minutes for average sleeping time (such as 1 minute; In worst case we were using 15 minutes).

Furthermore, at the beginning of each sample, we were only starting with 0.1 of RFID tags available in that specific case and the other available tags were sleep and they would wake up after a random chosen time based on P_{sleep} . Moreover, according to the previous paragraph, we were considering some warm up time for the system and in each sample, we were discarding that time and its collected measurements to obtain more accurate results.

In both models (Framed Slotted Aloha based model and ZigBee based model) we are measuring and evaluating same parameters.

The evaluated parameters in our solution are:

- Collision probability which is the ratio of the number of collided packets to the number of transmitted packets (whether collided or not).

- Average number of collisions in each superframe
- Average waiting time of tags for beacon after waking up
- Average number of awoken tags in each superframe
- Average collision position in each superframe
- Average successful position in each superframe

Moreover, for simulation and evaluating these parameters we were considering two scenarios:

1. Constant average sleeping time (average sleeping time = 1 minute) and variable number of tags in each RFID network (10,30,60,90,120 nodes).
2. Constant number of tags in each RFID network (90 tags in each RFID network) and variable average sleeping time (1,2,5,10,15 minutes).

In this chapter, we will first present the simulation results of both models for the first scenario and after that, we will show the simulation results of both models for the second scenario.

4.1 Simulation Results of both models for the First Scenario

In this section, we are presenting the simulation results of both models for the first scenario in each RFID network (Constant average sleeping time (1 minute) and variable number of tags (10,30,60,90,120 tags in each RFID network)):

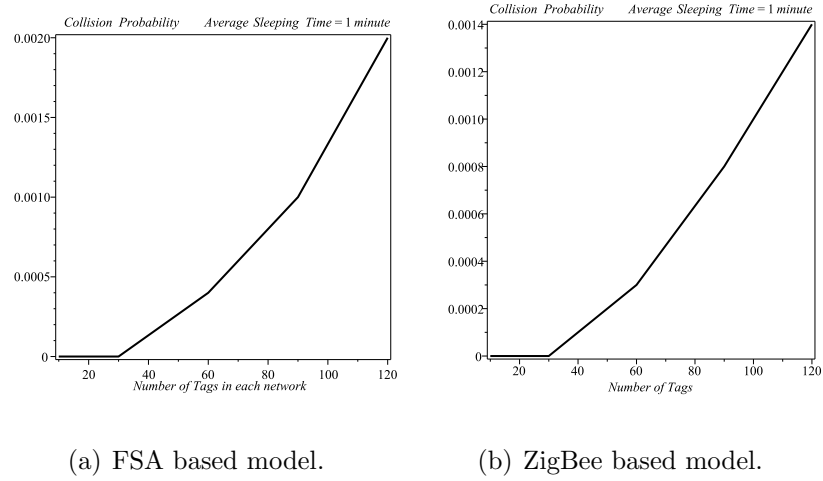


Figure 4.1: Simulation results for the first scenario: Collision probability.

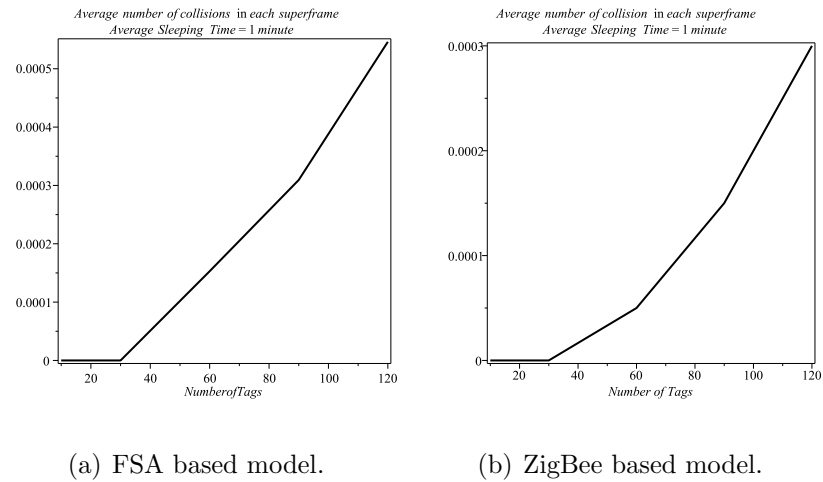


Figure 4.2: Simulation results for the first scenario: Average no. of collisions.

According to Figure 4.1(a), 4.1(b), 4.2(a) and 4.2(b), there was no collision detected in both models before 30 tags in each RFID network; Moreover, increasing the number of tags in each network is increasing the collision rate in both models. Furthermore, in Framed Slotted Aloha based model, the collision probability for 120

tags in each RFID network (which is the worst case in our tested cases) is equal to 0.002, whereas in ZigBee based model, the collision probability in the same case is equal to 0.0014. Thus, in the same condition, ZigBee based model has lower collision rate.

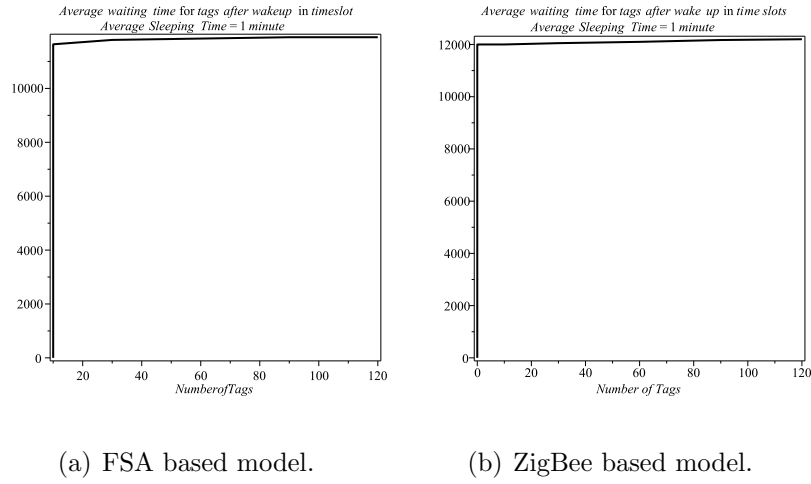


Figure 4.3: Simulation results for the first scenario: Average waiting time of tags.

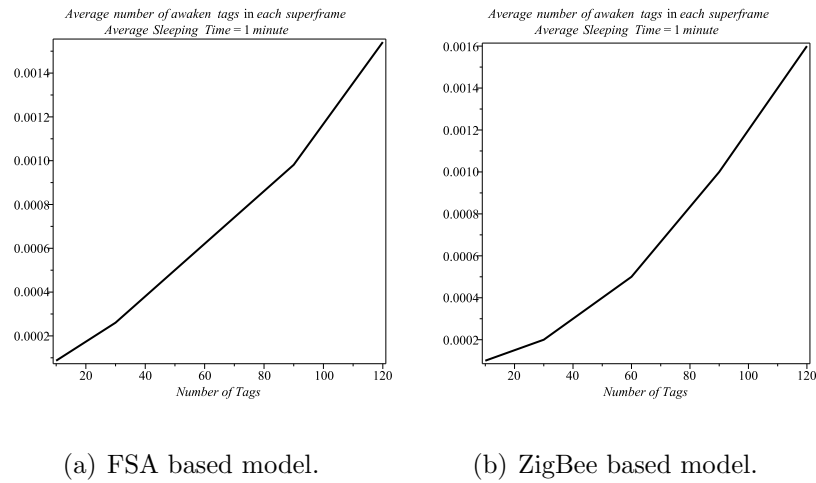


Figure 4.4: Simulation results for the first scenario: Average no. of awaken tags.

According to Figure 4.3(a) and 4.3(b), increasing the number of tags is not causing dramatic change in the average waiting times after wake up for tags but as it is shown in Figure 4.4(a) and 4.4(b), number of awoken tags in each superframe are increasing with the positive change in number of tags.

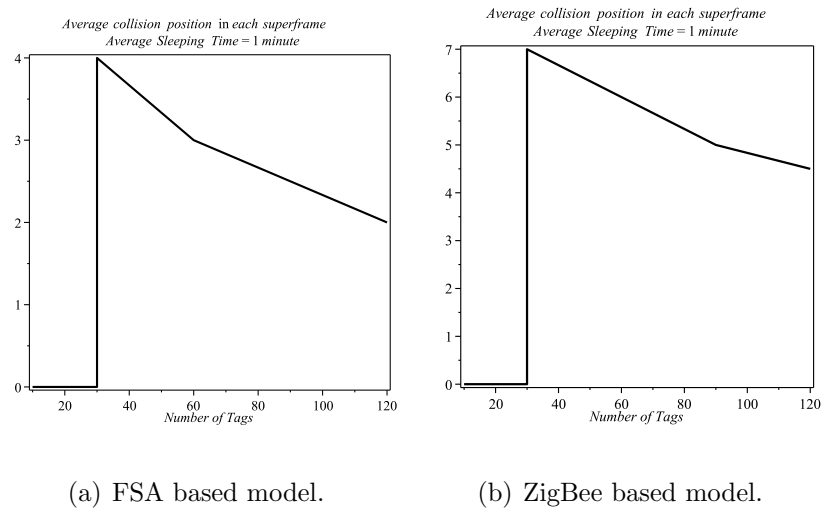


Figure 4.5: Simulation results for the first scenario: Average collision position.

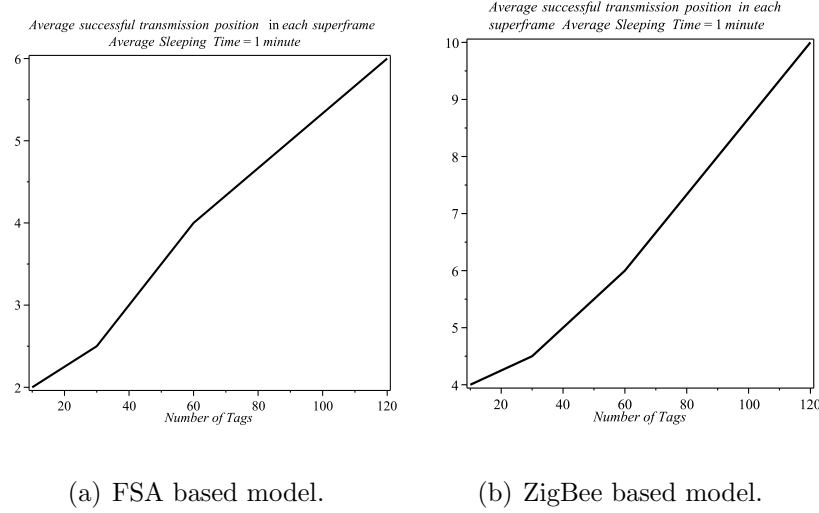


Figure 4.6: Simulation results for the first scenario: Average successful position.

According to Figure 4.5(a) and 4.5(b), with increasing the number of tags, collisions are moving toward the beginning of the superframe; Although in ZigBee based model, the average collision position is farther than Framed Slotted Aloha based model. Also, In Figure 4.6(a) and 4.6(b), with increasing the number of tags, successful access position is getting far from the start of the superframe, but in ZigBee based model, the average successful position is farther than Framed Slotted Aloha based model. Moreover, in Figure 4.5(a) and 4.5(b), as there is no collision before 30 tags in each network, the value is set to zero intentionally.

As it is shown in the figures of this section, increasing the number of tags in each RFID network has a negative effect on the system and it will increase the collision in RFID networks for both models.

4.2 Simulation Results of both models for the second scenario

In this section, we are presenting the simulation results of both models for the second scenario in each RFID network (Constant number of tags (90 tags) and variable average sleeping time (1,2,5,10,15 minutes)):

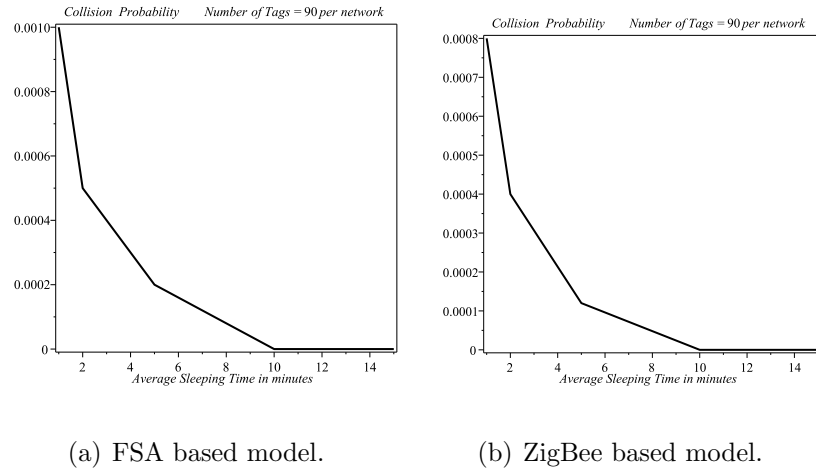


Figure 4.7: Simulation results for the second scenario: Collision probability.

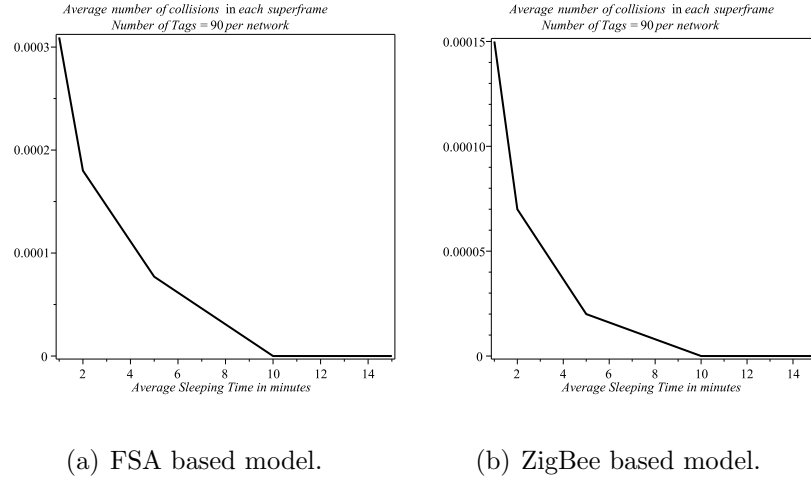


Figure 4.8: Simulation results for the second scenario: Average no. of collisions.

According to Figure 4.7(a), 4.7(b), 4.8(a) and 4.8(b), increasing the average sleeping time in each network is decreasing the collision rate in both models. Furthermore, in Framed Slotted Aloha based model, the collision probability for 1 minute average sleeping time (which is the worst case in our tested cases) is equal to 0.001, whereas in ZigBee based model, the collision probability in the same case is equal to 0.0008. Thus, in the same condition, ZigBee based model has lower collision rate. Moreover, in both models no collision was detected after 10 minutes average sleeping time.

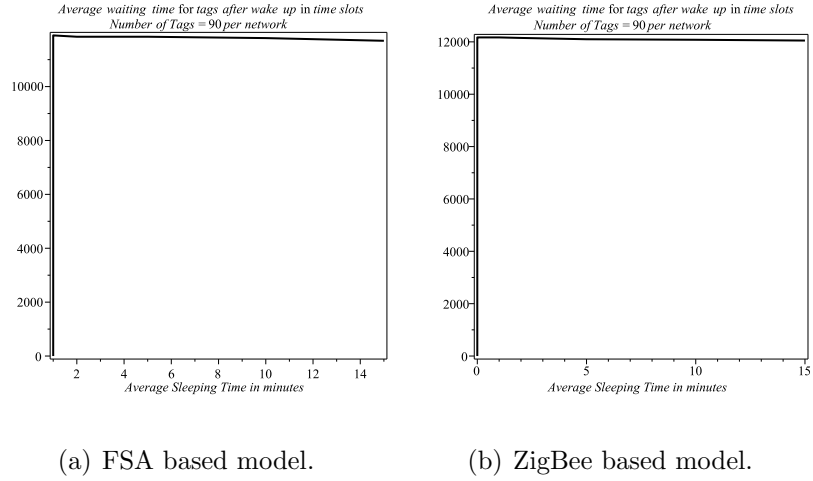


Figure 4.9: Simulation results for the second scenario: Average waiting time of tags.

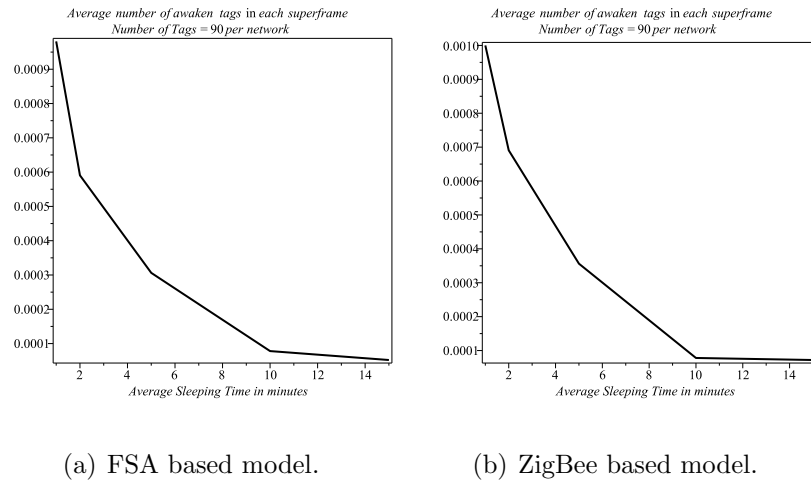


Figure 4.10: Simulation results for the second scenario: Average no. of awoken tags.

According to Figure 4.9(a) and 4.9(b), increasing the average sleeping time is not causing dramatic change in the average waiting times after wake up for tags but as it is shown in Figure 4.10(a) and 4.10(b), number of awoken tags in each superframe are decreasing with the positive change in the average sleeping time.

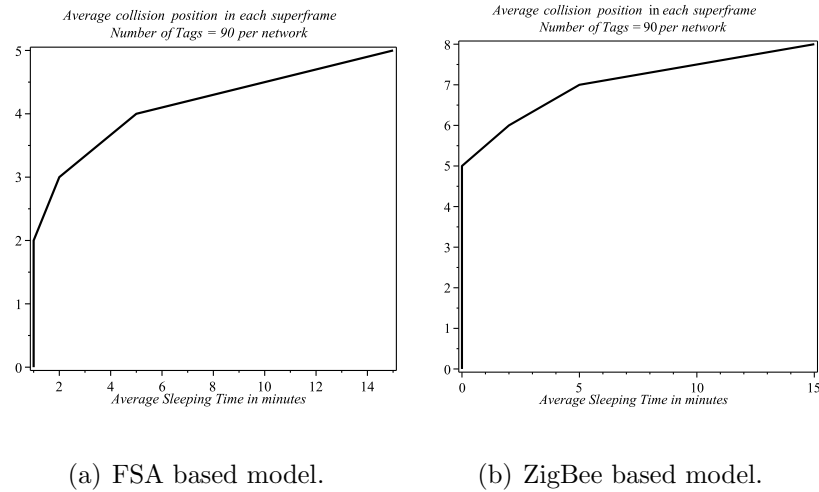


Figure 4.11: Simulation results for the second scenario: Average collision position.

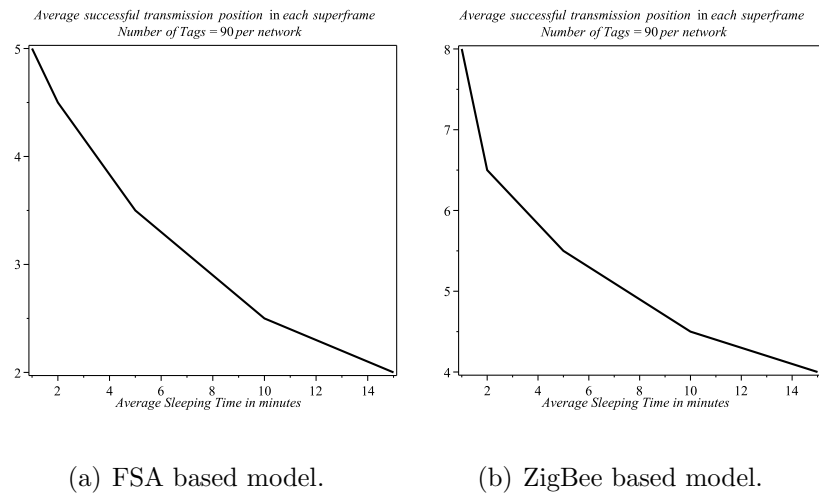


Figure 4.12: Simulation results for the second scenario: Average successful position.

According to Figure 4.11(a) and 4.11(b), with increasing the average sleeping time, collisions are moving farther from the beginning of the superframe; Although in ZigBee based model, the average collision position is farther than Framed Slotted

Aloha based model. Also, In Figure 4.12(a) and 4.12(b), with increasing the average sleeping time, successful access position is getting closer to the start of the superframe, but in ZigBee based model, the average successful position is farther than Framed Slotted Aloha based model.

As it is shown in the figures of this section, increasing the average sleeping time has a positive effect on the system and it will decrease the collision in RFID networks for both models.

Chapter 5

Conclusion

In this thesis, we have suggested a solution for the WLAN/RFID coexistence problem in frequency band of 2.45 GHz or ISM band. A feasible solution should suggest minimum change in current networks and it should be compatible with international standards. In our solution, our changes are mostly limited to RFID readers and it is totally compatible with well-known standards. Our model meets these requirements: It is working in time-sharing manner between Wi-Fi network and RFID networks and it is making the WLAN Access Point (AP) aware of the RFID neighbor-network at the Medium Access Control (MAC) layer. AP is polling these networks in a round-robin order and only one network is active at the same time. With an appropriate time schedule, given time to each network is sufficient to keep collision probability low and Wi-Fi network can not affect the RFID networks by its strong transmission power. Wi-Fi network's Access Point is following the Point Coordination Function(PCF) mechanism of IEEE 802.11 standard which is defined for time sharing models. AP is putting different networks in a waiting state, polling them one-by-one

(in a round-robin fashion) and giving the medium to the polled network. For RFID networks, we have two versions of the model: In the first model, we are using Framed Slotted Aloha standard which has been widely used in industry. After that, in order to improve the performance, we have suggested a second version which in that model we have used IEEE 802.15.4 for anti-collision communication. We have simulated these two models using Artifex simulator and we have measured and evaluated some parameters in both models. Our results are totally approving that the performance of IEEE 802.15.4 based model is better than the Framed Slotted Aloha based model.

According to what we have observed in our result (illustrated in Chapter 4), generally we can conclude that the performance of our ZigBee based model is better than the Framed Slotted Aloha based model. The collision probability of Zigbee based model is around 75% of the Framed Slotted Aloha based model. Furthermore, average number of collision in each superframe in Zigbee based model is almost 60% of the Framed Slotted Aloha based model. In addition, the collision position in superframe in ZigBee based model is moving farther from the beginning of superframe in comparison to Framed Slotted Aloha based model which means in ZigBee based model, the collisions are less likely to occur in comparison to Framed Slotted Aloha based model. Moreover, in ZigBee based model, the successful transmission position is moving farther from the beginning of superframe due to the CSMA mechanism (random delay time and CCAs) used in this model.

Although we can not forget that Framed Slotted Aloha based model has its own advantages: Its standard is being used in industrial RFID products and solutions; Framed Slotted Aloha is easy to implement (according to what we have seen in the

details of the standard which was described in Section 2.1.5): For example there is no CMSA mechanism; In Framed Slotted Aloha based model, data packet size is one timeslot whereas in ZigBee based model, data packet size is 3 timeslots and moreover, we have the delay of two timeslots for each successful data packet transmission. Thus we can say Framed Slotted Aloha based model is easier to deploy, but it has lower performance.

Appendix A

Abbreviations

ACK	Acknowledgement
ACS	Anti-collision/select
AID	Association Identifier
AP	Access Point
BE	Backoff Exponent
BFSA	Basic Framed Slotted ALOHA
BI	Beacon Interval
BO	Beacon Order
BSS	Basic Service Set
CAP	Contention Access Period
CCA	Clear Channel Assessment
CF	Contention Free
CFP	Contention Free Period

CP	Contention Period
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear-To-Send
CW	Contention Window
DCF	Distributed Coordination Function
DFSA	Dynamic Framed Slotted ALOHA
DIFS	Distributed Interframe Space
DSRC	Dedicated Short Range Communication
DSSS	Direct Sequence Spread Spectrum
DTIM	Delivery Traffic Indication Message
EM	electromagnetic
EPC	Electronic Product Code
FHSS	Frequency Hopping Spread Spectrum
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
ISM	Industrial, Scientific and Medical
LLC	Logical Link Control
MAC	Medium Access Control
MLME	MAC Sub-layer Management Entity
MPDU	MAC Protocol Data Unit
NAV	Network Allocation Vector

NB	Number of retries
NIC	Network Interface Card
O-QPSK	Orthogonal Quadrature Phase Shift Keying
PC	Point Coordinator
PCF	Point Coordination Function
PER	Packet Error Rate
PGF	Probability Generating Function
PHY	Physical Layer
PIFS	Point coordination function Interframe Space
QoS	Quality of Service
RBC	Random Backoff Countdown
RFID	Radio Frequency Identification
RTS	Request-To-Send
SD	Superframe Duration
SIFS	Short Interframe Space
SO	Superframe Order
STA	Station
TBTT	Target Beacon Transmission Time
TU	Time Unit
TX	Transmit
UHF	Ultra High Frequency

WLAN	Wireless LAN
WPAN	Wireless Personal Area Network
VANET	Vehicular Ad-hoc Network

Bibliography

- [1] ISO/IEC 18000-4, Information technology - Radio frequency identification for item management - Part 4: Parameters for air interface communications at 2,45 GHz. 2004.
- [2] IEEE 802.15.4 Working Group. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). *IEEE Standard*, 2006.
- [3] IEEE 802.11 Working Group. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. *IEEE Standard*, 2007.
- [4] IEEE 802.15 Task Group 4f. IEEE 802.15-09-0616-00-004f. *Ubisense 2.4 GHz PHY Proposal to 802.15TG4f*, September 2009.
- [5] N. Abramson. The Aloha system-another alternative for computer communications. In *Proceedings of Fall Joint Computer Conference of AFIPS*, volume 37, pages 281–285, Houston, TX, 1970.
- [6] Giuseppe Bianchi. Performance Analysis of the IEEE 802.11 Distributed Co-

- ordination Function. In *IEEE Journal on selected areas in communications*, 18(3):535–547, March 2000.
- [7] R. Bridgelall. Bluetooth/802.11 Protocol Adaptation for RFID Tags. In *Proceedings of the 4th European Wireless Conference*, Florence, Italy, February 2002.
- [8] V. Chawla and D. Sam Ha. An Overview of Passive RFID. In *Communications Magazine, IEEE*, volume 45, pages 11–17, 2007.
- [9] Radionor Communications AS. Website. <http://www.radionor.no/>, Last visited June,20 2011.
- [10] J. Eom and T. Lee. Framed-Slotted ALOHA with Estimation by Pilot Frame and Identification by Binary Selection for RFID Anti-collision. In *International Symposium on Communications and Information Technologies (ISCIT07)*, pages 1027–1031, 2007.
- [11] N. Golmie. Interference in the 2.4 GHz ISM Band: Challenges and Solutions. *White Paper, National Institute of Standards and Technology*, June 2001.
- [12] GR Grimmett and DR Stirzaker. *Probability and Random Processes. 2nd Edition*. Oxford University Press, Oxford, UK, 1992.
- [13] FILA MedIT Consulting Group. Proposal for RFID Implementation in University of Pittsburgh Medical Center. 2009. White Paper. Available from www.ifanchu.com/myDocuments/MSIT.
- [14] S. Han and N. Abu-Ghazaleh. A Realistic Model of Co-Located Interference for Wireless Network Packet Simulation. In *7th IEEE International Conference on*

- Mobile Adhoc and Sensor Systems (MASS)*, pages 472–481, San Francisco, CA, November 2010.
- [15] S. Han, S. Lee, and Y. Kim. Coexistence Performance Evaluation of IEEE 802.15.4 Under IEEE 802.11b Interference in Fading Channels. In *The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC07)*, pages 1–5, Athens, Greece, 2007.
- [16] M. Hsu and Y. Chen. Enhanced PCF Protocols for Real-time Multimedia Services over 802.11 Wireless Networks. In *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW06)*, pages 56–59, 2006.
- [17] AeroScout Inc. Utilizing Wi-Fi Standard Wireless Networks for Active RFID. June 2007. White Paper. Available from <http://www.mas-rfid-solutions.com/Utilizing%20WiFi%20.pdf>.
- [18] AeroScout Inc. Website. <http://www.aeroscout.com/>, Last visited July,5 2011.
- [19] Ekahau Inc. Website. <http://www.ekahau.com/>, Last visited June,20 2011.
- [20] PanGo Inc. Website. <http://www.pango.com/>, Last visited June,20 2011.
- [21] W. Jiang and Y. Ma. Interference Analysis of Microwave RFID and 802.11b WLAN. In *International Conference on Wireless Communications, Networking and Mobile Computing (WiCom07)*, pages 2062–2065, 2007.
- [22] A. Kopsel and A. Wolisz. Voice transmission in an IEEE 802.11WLAN based ac-

- cess network. In *Proceedings of the 4th ACM international workshop on Wireless mobile multimedia (WOWMOM 2001)*, pages 23–32, Rome, Italy, 2001.
- [23] J. Kurose and K. Ross. *Computer Networking: A top-down approach featuring the Internet, 2nd Edition*. Addison-Wesley publication, 2003.
- [24] S. Lee, S. Joo, and C. Lee. An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification. In *Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous05)*, pages 166–172, 2005.
- [25] L. Liu and S. Lai. Aloha-based anti-collision algorithms used in RFID system. In *Proceedings of Conference On Wireless Communication, Networking and Mobile Computing 2006 (WiCOM 2006)*, pages 1–4, 2006.
- [26] T. Mak, K. Laberteaux, and R. Sengupta. A MultiChannel VANET Providing Concurrent Safety and Commercial Services. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET05)*, pages 9–15, Cologne, Germany, 2005.
- [27] J. Mišić and V.B. Mišić. *Wireless Personal Area Networks: Performance and Interconnections and Security with IEEE 802.15.4*. John Wiley and Sons, 2008.
- [28] H.L. Moen. A Study of Wi-Fi RFID Tags in Citywide Wireless Networks. *Masters thesis, Department of Telematics, Norwegian University of Science and Technology*, June 2001.
- [29] H.L. Moen and T. Jelle. The Potential for Location-Based Services with Wi-Fi

- RFID Tags in Citywide Wireless Networks. In *4th International Symposium on Wireless Communication Systems (ISWCS07)*, pages 148–152, October 2007.
- [30] B. Nilsson, L. Bengtsson, P. Wiberg, and B. Svensson. Protocols for Active RFID - The Energy Consumption Aspect. In *International Symposium on Industrial Embedded Systems (SIES'07)*, pages 41–48, Lisbon, Portugal, July 2007.
- [31] B. Polepalli, W. Xie, D. Thangaraja, M. Goyal, and et al. Impact of IEEE 802.11n Operation on IEEE 802.15.4 Operation. In *International Conference on Advanced Information Networking and Applications Workshops (WAINA'09)*, pages 328–333, 2009.
- [32] S. Pollin, M. Ergen, M. Timmers, A. Dejonghe, and et al. Distributed cognitive coexistence of 802.15.4 with 802.11. In *1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pages 1–5, 2006.
- [33] S. Pollin, I. Tan, B. Hodge, C. Chun, and et al. Harmful Coexistence Between 802.15.4 and 802.11:A Measurement-based Study. In *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, pages 2–7, 2008.
- [34] G. Radinovic and K. Kim. Feasibility Study of RFID / Wi-Fi / BlueTooth Wireless Tracking System for Underground Mine Mapping - OKLAHOMA. In *Incorporating Geospatial Technologies into SMCR Business Processes*, pages 1–34, Atlanta, GA, March 2008.
- [35] A. Sikoral and V. Groza. Coexistence of IEEE802.15.4 with other Systems in the

- 2.4 GHz-ISM-Band. In *Proceedings of the IEEE Instrumentation and Measurement Technology Conference (IMTC'05)*, volume 3, pages 1786–1791, Ottawa, Canada, May 2005.
- [36] J. Stine and G. De Veciana. Improving Energy Efficiency of Centrally Controlled Wireless Data Networks. *Kluwer Academic Publishers*, 8(6):681–700, 2002.
- [37] M. Timmers, S. Pollin, A. Dejonghe, L. Van der Perre, and et al. Exploring vs Exploiting: Enhanced Distributed Cognitive Coexistence of 802.15.4 with 802.11. In *IEEE Sensors 2008*, pages 613 – 616, 2008.
- [38] H. Vogt. Efficient object identification with passive RFID tags. In *Proceedings of Pervasive Computing*, pages 98–113, 2002.
- [39] D. Yoon, S. Shin, W. Kwon, and H. Park. Packet Error Rate Analysis of IEEE 802.11b under IEEE 802.15.4 Interference. In *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*, volume 3, pages 1186–1190, 2006.
- [40] W. Yuan, X. Wang, and J. Linnartz. A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g. In *14th IEEE Symposium on Communications and Vehicular Technology in the Benelux*, pages 10–15, 2007.
- [41] Y. Zhang, L. Yang, and J. Chen. *RFID and Sensor networks: Architectures, Protocols, Security and Integrations*. CRC Press publication, 2010.