Integration of RFID with WLAN

by

Nargis Khan
Ryerson University,2011

A Thesis
Presented to Ryerson Univesity
in partial fulfillment of the
requirements of the degree of
Master of Science
in the Program of
Computer Science

Toronto, Canada,2011

Author's Declaration

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

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

Signed:_____

I further authorize 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:_____

Thesis advisor

Dr. Jelena Mišić

Author

Nargis Khan

Integration of RFID with WLAN

Abstract

Radio Frequency Identification (RFID) and Wi-Fi WLANs have achieved widespread applicability in different application domains. However, tag range of RFID systems is very short. Hence, integrating RFID with WLAN networks can contribute to wider application of RFID since Wi-Fi nodes have much larger communication range. However, both RFID and WLAN use the same frequency band and incurs interference by each other for channel utilization.

In this thesis, an efficient approach to solve the coexistence and integration problem of RFID and Wi-Fi WLAN is proposed. This solution allows these networks to access the medium in a time sharing manner by making the WLAN Access Point (AP) aware of the RFID neighboring network at the Medium Access Control (MAC) layer. Thus, it is possible to locate and identify the RFID tags in the physical space, with co-located Wi-Fi WLANS. Simulation results show that both networks work together by maintaining the performance such as higher throughput and lower collision probability, as is desired.

Contents

List of Figures

List of Tables

Acknowledgments

I would like to begin by thanking my advisor, my committee, my parents, my husband, and all the people who have supported me along the way.

This thesis is dedicated to my parents ,my husband and to my beloved daughter.

Chapter 1

Introduction

Background information, motivation, research statement, proposed solution and contribution are briefly presented in the following sections.

1.1 Background

Recently, Radio Frequency Identification (RFID) and IEEE 802.11 Wireless Local Area Network (WLAN) technologies have achieved widespread applicability in different application areas such as manufacturing, healthcare, public transportation, telecommunications, airline bagging and are considered as an alternative of barcode system in the distribution industry adn access control. Thus, using RFID technology increases the security in identification of a product. Moreover, RFID technology is simple, easy to use, and provides faster communication speed and hence, reduces processing time, increases productivity and improves the quality of service. RFID technology work at the 2.45 GHz Industrial Scientific Medical Band (ISM) and uses radio frequency to transfer data between readers and tags.

RFID tags are placed into objects such as cars, products in grocery stores. RFID readers in the vicinity of a tag read tag's data whenever is required. However, there is still no standard published for RFID. IEEE is working on a standard called IEEE 802.15.4f, which is still under processing. They adopt the IEEE 802.15.4 Zigbee protocol for the active RFID that is specially designed for low cost and low power applications.

On the other hand, the IEEE 802.11 standard defines one Media Access Control (MAC) and several physical layer specifications for WLANs connectivity for fixed, portable, and movable stations that require rapid deployment. The MAC procedure supports quality of service (QoS) requirements of the local area networks applications such as transport of voice, audio and video. This standard allows computers to communicate three physical layer specifications: two in the 2.4-GHz band (ISM) and one in the infrared, all operating at 1 and 2 Mbps. The IEEE 802.11 logical architecture contains several components: Station (STA), Wireless Access Point (AP), Independent Basic Service Set (IBSS), Basic Service Set (BSS), Distribution System (DS), and Extended Service Set (ESS). Some of these components map directly to hardware devices, such as stations STAs and wireless APs. The wireless STA contains an adapter card, PC Card, or an embedded device to provide wireless connectivity. The wireless AP functions as a bridge between the wireless STAs and the existing network backbone for network access. The ordinary nodes within WLAN use the basic medium access protocol, namely, Distributed Coordination Function (DCF) having 4-way RTS/CTS handshaking mechanism to access the medium. DCF is a contention based mechanism and easy to implement. However, many studies [24] suggest that DCF is quite inefficient and can be improved by Enhanced Distributed Channel Access (EDCA) to provide the QoS in the networks. Another access control mechanism, Point Co-

ordination Function (PCF) is used to access the medium with controlled delay. PCF works by polling scheme where, a single station gets the uninterrupted time to access the medium. All other stations are polled by round robin fashion and get the chance to transfer the frame. The detailed frame structure of PCF, DCF, and EDCA will be discussed with their working mechanism in Chapter 3.

RFID network uses the IEEE 802.15.4 Zigbee protocol. Both Zigbee and WLAN work in the ISM 2.4 GHz frequency band. Figure 1.1 illustrates the available channels for WLAN and Zigbee standards. Channels 11 to 26 (16 channels) are allocated to LR-WPANs. Each channel has a bandwidth of 2 MHz and is separated by 5 MHz in the 2.4 GHz ISM frequency band. Orthogonal Quadrature Phase Shift Keying (O-QPSK) technique is used as a transmit scheme with the transmission rate of 250 Kbps. The channel usage depends on the regulatory domain [17] for WLAN. On the other hand, the IEEE 802.11 standard defines 14 channels. Most of the adjacent channels are partially overlapped as shown in Figure 1.1. Thus, channel interference might occur when two or more 802.11 nodes operate using the adjacent channels. In USA and Canada, 11 channels are used each having a bandwidth of 22 MHz in the 2.4 GHz ISM band. The IEEE 802.11b standard recommends using non overlapping channels 1, 6 and 11 for North America. Channels 13 and 14 are not used that allows LR-WPAN channels to operate without any interference of Wi-Fi (Figure 1.1). However, the 2.4 GHz applications allow larger bandwidth and more channels. Table 1.1 summarizes some of the important properties of the wireless standards that work in the 2.4GHz frequency band.

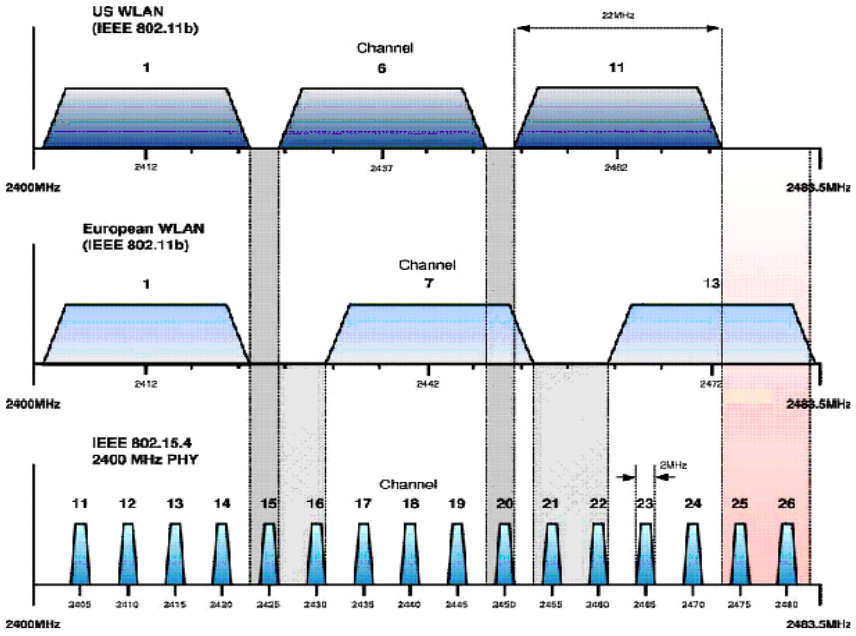


Figure 1.1: The IEEE 802.11 and IEEE 802.15.4 channels in the 2.4GHz ISM band [17]

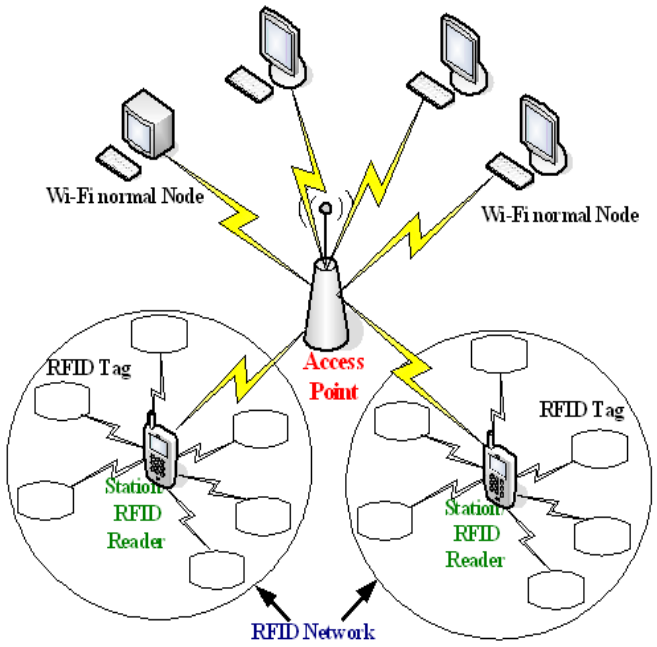


Figure 1.2: The Co-existance problem of RFID and WLAN

Table 1.1: Wireless technologies working in 2.4GHz ISM frequency band [17]

IEEE Standard	Frequency Band	Reserved Bandwidth	Number of Channels	Maximum Data Rate(Mpbs)	Transmission Range	Applications
802.11b/g	2.4GHz	22MHz	11	11/54	100m	WLAN
802.15.1	2.4GHz	1MHz	79	0.72	10m	WPAN
802.15.3	2.4GHz	15MHz	5	55	10m	HR-WPAN
802.15.4	2.4GHz	2MHz	16	0.25	20m	LR-WPAN

1.2 Thesis Motivation

Tag range that measures the performance of RFID system is the maximum distance a RFID reader can either read or write information at the tag. According to the US regulation for ISM 2.45 GHz microwave sub-band, tags can cover up to 11 meters, whereas it is 30 meters for the 860-960 MHz ultra high frequency sub-band. Wi-Fi WLAN can cover the larger area upto to hundred meters.

Due to the short reading range of RFID readers they cannot read RFID tag's from a distant place and thus, cannot be used for many large scale applications. To alleviate this problem RFID networks can be integrated with Wi-Fi WLAN to increase the network coverage because of their large transmission range and power. This would also contribute to even wider applications of RFID, including areas such as security, public safety, emergency responses and health care, where RFID is currently not used due to the problems outlined above. However, both WLAN and RFID networks use the same unlicensed free ISM bands 2.4 GHz frequency band. Working in the same frequency bands results the interference and co-existence problems between the IEEE 802.15.4 Zigbee and 802.11 WLAN standards that requires to be managed and controlled properly to ensure the desired performance requirements. Existing solutions to the co-existence and integration problems rely on readers to be integrated with the Access Point (AP) and are not considered efficient. Moreover,

the IEEE 802.11 DCF MAC protocol does not provide Quality of Service (QoS)and performance degrade at heavy data traffic load. DCF controlled stations have same priority to access the medium and use same distributed interframe space (DIFS) value so there are no differences among the data traffic. Figure 1.2 demonstrates the physical proximity collision domain of RFID and WLAN network.

1.3 Research Statement

The proposed research statement is how to provide quality of service (QoS) such as higher throughput, lower collision probability while integrating Wi-Fi WLAN with RFID network so that a large network area can be covered to extend the application domain of RFID networks. Thus, the proposed research would develop a framework to solve WLAN/RFID co-existence and integration problem using existing hardware, which is compatible with the IEEE 802.11 Wi-Fi standard. Thus, this solution would be economically feasible and readily applicable in practice.

1.4 Solution Approach

To solve the proposed research problem and achieve QoS, we design and implement an approach that uses a two tiered network architecture: (i)RFID networks and (ii) Wi-Fi WLAN. This approach works using Time Division Multiple Access (TDMA) between WLAN and RFID. In the first tier, RFID tags send data to RFID readers using the IEEE 802.15.4 Zigbee protocol. Zigbee provides more flexible and universal functionality than other available wireless standards. An alternative of Zigbee can be slotted ALOHA but it

is trends to be less adoptive to the load.In the second tier of Wi-Fi WLAN, RFID readers integrate two networks and work as special WLAN node having higher priority to extend the RFID transmission range. The IEEE 802.11 PCF protocol is used which allows contention free access and contention based access of the medium. More specifically, RFID networks mainly work in the Contention Free Period (CFP) of PCF and WLAN remains in sleep mode during this period. In the DCF or Contention Period (CP), readers of RFID network and Wi-Fi nodes compete to win the medium to transfer their frames to the AP.

The IEEE 802.11 protocol provides QoS by introducing the IEEE 802.11e Enhanced Distributed Channel Access (EDCA) mechanism. Thus, we would use EDCA instead of DCF to achieve QoS. In the EDCA protocol, we assume that stations have two different priorities to access the medium. Readers (special station) have the highest priority and WLAN STAs have the lowest priority. We measure the performance of these proposed framework to observe how both networks work together and maintain the performance as required level.

1.5 Thesis Contribution

We simulate the proposed scheme using the Artifex simulator tool and measure its performance in terms of different QoS metrics such as throughput, frame collision probability, frame access delay, average backoff phase, and access probability. From the simulation results, we find the proposed scheme achieves the network accuracy as the desired level when readers work as the highest priority station and Wi-Fi nodes as the lower priority station. This represents our contribution to alleviate the co-existence and interference problems between RFID and Wi-Fi networks.

1.6 Thesis Organization

The remainder of this thesis is organized as follows. In chapter 2, we briefly describe the RFID technology, IEEE 802.15.4 WPAN and IEEE 802.11e EDCA protocol. Chapter 3 presents the proposed approach that solves the co-existence and integration problems. In chapter 4, we present the simulator model that is implemented using Artifex simulation tool. Performance of the proposed solution is presented in Chapter 5. Finally, Chapter 6 concludes the thesis.

Chapter 2

Background and Related work

2.1 Related Work

Integration of RFID and WLAN has been heavily investigated recently [12] [13] [15] [39]. Existing solutions do not solve the coexistence problem in a satisfactory manner. Some solutions rely on the readers being integrated with the Access Point (AP) [39]. This increases the network complexity and cost and limits the RFID network coverage. If the coexistence and integration problem is solved this would facilitate the development of much needed RFID applications. This would also allow the use of existing available hardware that makes the system economically feasible.

The work done in paper [39] suggests three types of network integration architecture. These are: (i) smart stations mixed with RFID readers and Wireless Sensor Network (WSN) base stations, (ii) network with RFID readers and WSN base station deployment, and (iii) a smart active tag network architecture. The first case limits the number of reader being integrated whereas for the second case, integration increases the number of readers in the

networks. For the third case, data is transmitted among the tags before transmitting to readers that makes it more flexible to use. However, the integration method is selected based on the cost and application requirements. In our proposed scheme, readers are not integrated with the AP. Hence, the network complexity and cost are reduced. Active tags are used in our proposed framework that cover a large communication area.

The work done in [15], [12] analyze the coexistence impact of an IEEE 802.15.4 network on the IEEE 802.11b devices. In [12], the interference problem between the signals of WPAN (Zigbee) and health care medical equipments is discussed. In [34], channel conflict and interference issues of the IEEE 802.11b and 802.15.4 is discussed. The authors of this paper show that if the number of 802.11b networks increases the conflict among channels increases. The work done in [13] discusses the interference and co-existence impact of the IEEE 802.11 and 802.15.4 in terms of throughput. In [28], the authors address the interference problem between WPAN and WLAN in terms of overlapping channels. By simulation they show that about 90% of WPAN frames are destroyed by the interfering WLAN frames. Interference and coexistence problems of Zigbee and WLAN are discussed in paper [27]. They analysis the interference between Zigbee and WLAN by measuring the throughput of the framework. They demonstrate that the Zigbee interference has more effect on IEEE 802.11 uplink communication than that of the downlink communication. They consider Zigbee peer-to-peer network topology that work at 115 kbps data transmission rate. However, in our proposed scheme, we consider the IEEE 802.15.4 star topology network that work at 250 kbps data transmission rate. The work done in [30] proposes a RFID/WLAN integration scheme to solve the problem of location estimation in indoor environment. This scheme estimates the accurate client position. On the other hand, in our

proposed scheme, a RFID reader works as a bridge to integrate two networks to send tag IDs to the coordinator.

In recent years, the IEEE 802.11 WLAN becomes a dominant technology. The Distributed Coordination Function (DCF) that is considered as the main MAC protocol, does not provide any QoS [16] [8] [18]. Hence, the new version of the standard IEEE 802.11e provides QoS by improving the DCF MAC protocol by Enhanced Distributed Channel Access (EDCA) protocol. Many researchers analyze the performance of the coexistence of DCF and EDCA. In [16], the authors analyze the coexistence problem of DCF and EDCA. They show that QoS stations of EDCA that have lower inter frame space value (AIFS) work better in heavy load than that of the DCF controlled stations. The EDCA protocol provides super QoS performance for real-time applications. In [8], authors analyze the earlier legacy IEEE 802.11 DCF access method. They measure the performance of both protocols using NS-2 simulation tool. The limitations of DCF protocol are discussed in [18]. Stations working using the DCF protocol have same priority to access the medium and use same Contention Window (CW) value. As a result, stations and their traffic cannot be differentiated and QoS is not maintained. The data frame of DCF is best effort [24], which does not provide QoS. Thus, the performance degrades at heavy load. In our proposed scheme, we consider RFID readers as QoS stations work with ordinary WiFi stations to send their stored data. Thus, the performance of both networks is achieved as is desired.

2.2 Protocol Background

2.2.1 Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a fast developing automatic identification technique that consists of two components: readers and tags [35]. A tag stores a bit string in its memory as an identification (ID) of an object. The reader can read the IDs of the neighboring tags using a link-layer protocol over the wireless channel. Tags are normally attached or embedded into objects for the identification or tracking purposes. Tags work as alternatives to UPC barcode in most common application of RFID, such as supply-chain management. By reading all the tag IDs in the neighborhood and then consulting a back-end database that provides a mapping between IDs and objects, the reader learns the existence of the corresponding objects in the neighborhood. RFID tags are classified as active, passive and semi passive based on the types of power usage (e.g., electromagnetic, battery.

Passive tags: Passive tags have no tag power source and transmitter. They are powered by the signals that are sent by reader to the tags. These tags are cheaper and have shorter reading range, about 4 inches - 15 feet. The power needed for passive tags to transmit their IDs to the interrogating reader is supplied by the reader itself. The reader ”energizes” the tags in the vicinity with Radio Frequency (RF) power continuously for the entire read operation, which consists of a query from the reader and followed by the tag response. For the tag response, part of RF power is transmitted back to the reader (using a process called backscattering) after appropriative modulation and coding via the tag’s electronics. The electronics can also perform simple computations and has a small amount of memory.

Semi-Passive tags: They have on tag power source (e.g., batteries) but do not have an on tag transmitter. Thus, tags use the energy transmitted from the reader for communication. Semi-passive tags have greater communication range than that of passive tags.

Active tags: These tags use batteries to power the digital logic as well as transmissions. Thus, they have larger communication range as compared to passive tags, at a higher complexity and cost [35]. We plan to use active tags in the proposed research.

Based on the radio frequency used RFID systems can be divided into Low Frequency(LF), High Frequency(HF), Ultra High Frequency (UHF) and Microwave. A summary of the frequency characteristics, transmission rang and their applications are tabulated in table 2.2.

Table 2.1: RFID systems Frequency characteristics [32]

	LF	HF	UHF	Microwave
Frequency	Typically 125 or 134.2Khz	Typically 13.56Mhz	Typically 868Mhz – 928Mhz	2.45Ghz and 5.8Ghz
Tag types	Passive-inductive coupling	Passive-inductive coupling	Passive or active	Passive or active
Reading/Writing data rate	Slower	Moderate	Fast	Faster
Ability to read/write multiple tags in field	No tag will be read if multiple tag present	Can read/write moderate dense tags	Ability to read/write high-dense tags	Similar to UHF
Approximate range	Up to ~1 meter	Up to ~1.2 meter	Up to ~6 meters	Up to ~2 meter
Applications	Animal Tracking, Access Control, Vehicle Immobilization	Smart Card, Access Control, Item Level Tagging (Supply Chain, Asset Tracking, Library Application, Pharmacy Application, Personnel Identification etc)	Pallet and Case Tagging (Supply Chain). Item Level Tagging is working in progress.	Electronic toll collection, cold chain management, environment monitoring

Basic Infrastructure

The purpose of a RFID system is to collect information of objects that are available in a portable device called a tag. Readers collect and process data based on the application requirements. The collected information from tags are location information, product price, color, date of purchase and other application specific information. Now a days, RFID

technology has been used by many companies because of it's ability to track stationary or mobile objects quickly.

A basic RFID system consists of three components [1].

1. An antenna or coil.
2. A transceiver (with decoder)
3. A transponder or RFID tag which is electronically programmed with unique information.

Antenna

The antenna emits RF to activate the tag and read/write information from/to the tag. Antenna is connected with the reader. Mainly passive tags are powered by the RF signal transmitted from readers whereas active tag has it's own on-board power.

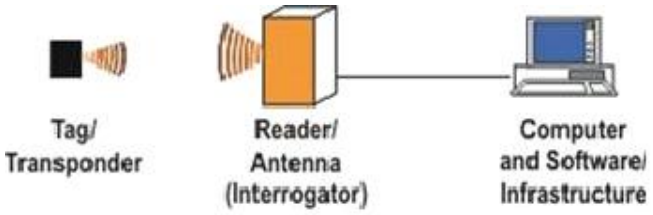


Figure 2.1: Basic components of RFID system [1]

Reader

To collect data from the tag, RFID readers emit radio wave in the range of one inch to 100 feet or even more that depends on the communication range of tags and also on the ra-

dio frequency used. When tags are within the communication range of readers and receive the electromagnetic(EM) signal it detects the activation signal from the reader. Readers decode data that are encoded in the tag's integrated circuit (silicon chip) and transmit data to the host computer for further processing.

Transponder/Tag

A typical RFID tag is an integrated circuit which is actually a microchip attached to a radio antenna mounted on an object. The chip can store upto 2 kilobytes of data.

Figure 2.2 shows the basic sequence of communication between the reader and tag. A reader sends data to a host computer that displays the commands of the reader [40]. The sequence of operation by RFID readers is presented as follows.

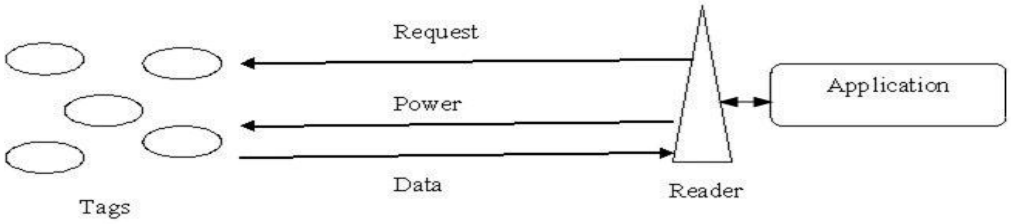


Figure 2.2: Communication techniques of RFID System

1. Host computer manages readers and sends message to the readers.
2. Readers and tags communicate through the RF signal.
3. Request message generated by a reader is in the form of carrier signal.
4. Carrier signals are sent through antennas.

5. Tags receive the carrier signal.

6. Tag antenna receives the modulated signal and then sends the signal containing information of objects to the reader antennas.

7. The Reader decodes the radio waves reflected from the RFID tag.

8. Decoded data are sent back to the host computer.

2.2.2 Operating principles of RFID systems

There are many different operational methods and several ways in which RFID reader and tag communicate with each other.Passive tags use two different coupling techniques: near and far field coupling techniques. These techniques are presented as follows.

Near-Field Coupling

The RFID tags having low communication range and low frequency range use near field coupling techniques. The EM field in the near field region is reactive in nature [10]. The electric and magnetic field are orthogonal and quasi-static. They dominate each other depending on the type of antenna used. However, passive tags mostly rely on the magnetic field. Current flows through the coil of the reader and produces a magnetic field around it. This magnetic field induces the coil of tags to generate a small current. This technique is based upon Faraday's principle of magnetic induction figure (2.3). A tag is able to change the current of its field by changing the antenna load. This mechanism is called load modulation. Readers and tags communicate through this mechanism. Due to the mutual inductance between reader‘s coil and tag‘s coil any changes to the tag‘s current results in

changes to the reader‘s coil. It is a simple technique and used by most of the passive RFID systems. However, a large antenna coil is required for the low frequency band.

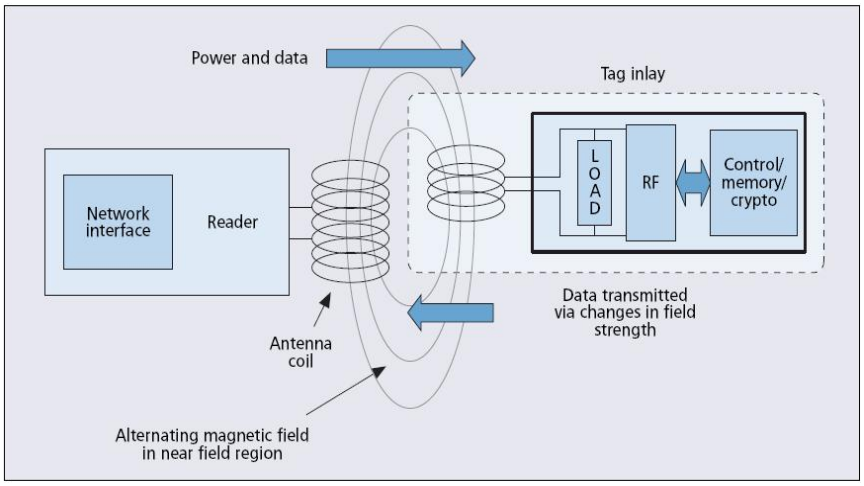


Figure 2.3: Near-field communication using inductive coupling [10]

Far-Field Coupling

The EM field of far field coupling is radiative in nature and uses a technique called backscattering as shown in Figure 2.4. A part of the generated current around the tag‘s coil is reflected back due to the mismatch of antenna and load circuit. Far field coupling is used by a long range (5-20 meters) and high frequency (860-960 MHz UHF or 2.45 GHz microwave) RFID systems. Far field coupling usees small antennas that reduces cost as compared to the near field coupling techniques.

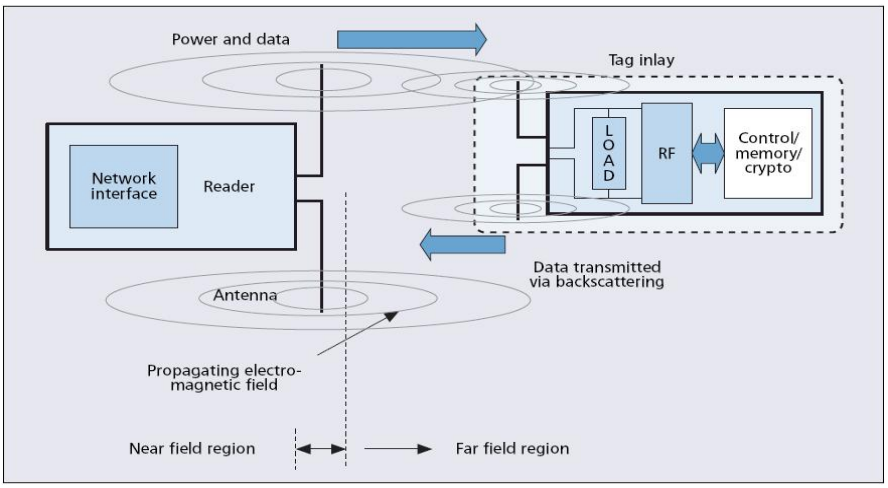


Figure 2.4: Far-field communication using backscattering [10]

2.2.3 Tag Memory

Passive tags typically have 64 bits to 1 kilobyte of non-volatile EEPROM memory. However, some passive tags can store up to 1 kilobyte of data on the tag depending on the amount of data required and application purpose. Active tags have 128 kilobytes of SRAM memory.

I-Code is a commonly used RFID system [36] where, a tag provides 64-bytes memory that is addressable in blocks of 4 bytes. All blocks are readable but writing to some blocks is protected by a set of bits. This prevents changes to the serial number and similar data. 46 bytes of the memory are used for application data. The remaining 18 bytes are reserved for a serial number, write protection, indicating electronic article surveillance (one bit) and indicating the quiet state of the tag (one bit). The tag cannot communication with the reader if the quiet bit is set.

2.2.4 Programming Interface

The RFID reader device provides the programming interface of the system. It comprises commands for configurations setting of the reader such as commands for setting the speed of the serial connection, and handling communication with tags that are in the range of readers. Communication commands have the following functionalities.

Anti-collision/Select (ACS): On the activation of ACS commands all the tags in the communication range send their serial numbers and become selected as long as they are in the range. If any tag moves out of the range it becomes unselected. Then the tags needs to send the serial number again to become selected. This command can be used to locate the neighboring active tags. It is a prerequisite for writing to tags, since the write command affects only selected tags. However, an ACS cycle takes significantly longer period of time.

Write: Write command is used to write data to a selected tag indicated by ACS commands. While writing to tags, they cannot move in and out of the range. However, only one data block of 4 bytes can be written at a time.

Read: Only the tags selected by ACS commnad can send their data using READ command.

Read Unselected: This command is similar to read command. Only difference is that all tags can be triggered without checking their selection status.

2.3 RFID Communication protocol: IEEE 802.15.4 or Zigbee

The main objective of a RFID system is to identify tags that are in the communication range of an active reader. There is a possibility of collision among readers if reading range of multiple readers overlaps. Similarly, collision between tags occurs if more than one tag tries to send their id at the same time. To avoid the collision many anti-collision protocols have been proposed such as ALOHA [7], slotted ALOHA protocols [25], tree based protocols [9], and frame slotted ALOHA [37]. In this thesis, we consider IEEE 802.14.5 or Zigbee protocol as a collision avoidance protocol since it is suitable for low cost and low power applications. We only consider tag-tag collision.

The IEEE 802.15.4 technology provides low complexity, low power consumption, low data rate, and energy efficient battery powered devices. Wireless Personal Area Networks (WPAN) and Wireless Sensor Networks (WSN) are low data rate, and short range wireless networks that build on the IEEE 802.15.4 standards. These networks are mostly infrastructure less and used for applications based on their requirements for data rate, power consumption and QoS. The IEEE 802.15.4 works on three frequency bands: 868 MHz, 915 MHz and 2.45 GHz (Table 2.2). 2.45GHz frequency band is known as ISM band and used by various WPAN standards such as IEEE 802.15.1, 802.15.3 and also by microwave ovens. The maximum data transmission rate of this band is 250 kbps. In WPAN networks, there is a central controller called PAN coordinator that builds personal area networks with other nodes within a small space. PAN coordinator mainly supports two types of topologies: star and pair-to-pair. In star topology, a device must go through PAN coordinator

to communicate with other devices. In pair-to-pair topology, a device can communicate directly with others if they are in the communication range. In our simulator model, we use the star topology.

Devices are classifies based on the level of complexity: Full Functional Device (FFD) and Reduced-Functional Device (RFD). A FFD can function as a PAN coordinator or as a cluster coordinator or as an ordinary device and can communicate with any device of the networks. On the other hand, a RFD can only function as an ordinary device but not as a coordinator and can only communicate with one FFD at a time. RFD is used only for simple applications where individual nodes perform basic communications and have little computational capability.

Table 2.2: Frequency bands and data rates of IEEE 802.15.4 [23]

PHY option	Frequency Band(MHz)	Type of modulation	Maximum Data rate(kpbs)
865/915	868-868.6	BPSK	20
	902-928	BPSK	40
865/915	868-868.6	ASK	250
(2006)	902-928	ASK	250
865/915	868-868.6	O-QPSK	100
(2006)	902-928	O-QPSK	250
2450	2400-2483.5	O-QPSK	250

2.3.1 Star Topology and Beacon Enabled Operation

The way of communication between device to device or device to PAN coordinator depends on whether the network supports beacon or not. The beacon synchronizes the whole networks transmission procedure. The IEEE 802.15.4 standard defines two MAC channel access mechanisms: (i) beacon-enabled and (ii) non-beacon-enabled channel ac-

cess. The network with the star topology uses beacon-enabled channel access mechanism. This mechanism is also known as slotted carrier sensed multiple access mechanism with collision avoidance (CSMA-CA). On the other hand, non-beacon-enabled networks use non-slotted CSMA-CA mechanism. In this thesis, we use the beacon-enabled slotted channel access mechanism. The tags are synchronized with the beacon frame after they wake up from sleeping mode.

In beacon-enabled mode, the coordinator periodically transmits a beacon frame. The PAN coordinator divides the channel time. The time between two beacon frames is called beacon interval (BI) or superframe. Each superframe starts with a beacon frame and is divided into an active and inactive portion as shown in Figure 2.5. All the devices communicate with their PAN coordinator during the active portion of the superframe. They send their data to the coordinator through uplink transmission and receive data from the coordinator through downlink transmission. After the active portion of the superframe, the coordinator and individual node goes to the sleep mode to save energy in the inactive portion of the superframe. The active portion of a superframes is equivalent to the superframe duration (SD), where SD cannot be longer than the BI. The active portion of the superframe is divided into a number of equal sized slots. Each slot lasts for exactly $2^{SO} * aBaseSlotDuration$ symbols [23]. The $aBaseSlotDuration$ symbols contains 3 backoff periods, which is the duration to transmit 20 symbols. The beacon frame is transmitted at the beginning of slot 0 and then the contention access period (CAP) starts. During the CAP, all nodes including the coordinator must use the slotted CSMA-CA channel access mechanism. It is a contention-based channel access mechanism and every device completes for it‘s transaction within the CAP period of the current superframe. After the CAP

period, there is one optional contention free period (CFP), where each device can have guaranteed timeslot to access the medium. The beacon interval and active portion of the superframe duration is controlled by two important MAC parameters: superframe order (SO) and beacon order (BO). The duration ($0 <= SO <= BO <= 15$) is calculated by using the formula listed in Table 2.3. In the real scenario, the formula is valid only for the values less than and equal to 14. Every synchronized node should listen for the beacon for $aBaseSuperframeDuration * (2^{BO} + 1)$ symbols. This procedure is repeated if no valid beacon frame is received during this period. The maximum retry limit is 4. Once this limit exceeds, the MAC layer sends the message regarding the loss of synchronization in the higher layer of the protocol stack.

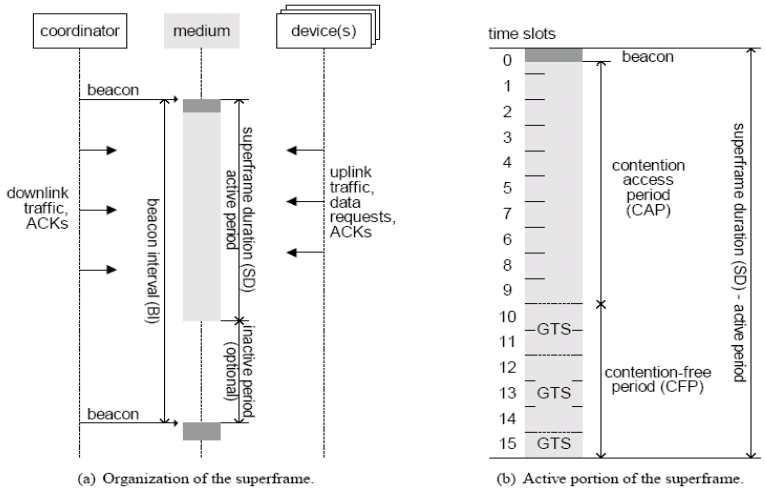


Figure 2.5: Structure of the superframe operating in beacon enabled mode [23]

2.3.2 CSMA-CA Medium Access Control Mechanism

Uplink transmissions in the star topology always use the CSMA-CA mechanism in beacon-enabled mode. In simulation, we only consider the uplink data communication

Table 2.3: Timing parameters in beacon enabled operating mode [23]

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	$aBaseSuperframeDuration * 2^{BO}$

and so, data is only transmitting from nodes to the Access Point but not the vise versa. The working principle of CSMA-CA algorithm is shown in Figure 2.6. The algorithm starts when the ready queue holds at least a packet to transmit. The value of the following parameters are initialized as follows.

1. Retry count or NB refers to the number of times, a station needs to retry to access the medium when it becomes idle.It is set to 0.

2. Contention Window (CW) refers to the number of backoff periods or slots a station senses the channel to become idle before the packet transmission begins. It is set to 2

3. Backoff exponent BE is the number of backoff times a device should wait before attempting to access the medium. If the device is operating in battery power (i.e., when $macBattLifeExt$ is set to true) the value is set to 2. Otherwise, the value is set to 3.

In this algorithm, transmission occurs only at the boundary of the backoff slots. The algorithm locates for the boundary of the next backoff period and all operations must be synchronized with the backoff periods. In the next step, a random number is generated at

backoff periods in the range $0 \ldots 2^{BE} - 1$. The value is then decremented at the boundary of each backoff period, which is called Random Backoff Countdown or *RBC*. During RBC, the channel is not sensed and if it is not available backoff countdown is not frozen. If the current superframe do not have enough time to finish the RBC, the station needs to wait until the next superframe active period. The counter only keeps frozen in the inactive portion of the superframe and resumes again in the active portion of the next superframe. If the value of RBC reaches to zero before transmitting the packet the algorithm needs to check the status (idle or not) of the channel. This is done by listening to the channel by Clear Channel Assessment (CCA) procedure in two backoff periods. Before starting the CCA the algorithm also needs to check if the current CAP have enough time to complete the necessary number of CCA checks, the packet transmission time, and acknowledgement. If there is enough time for all these activities the algorithm starts CCA check. Otherwise, the station needs to wait until the active period of the next superframe. If the channel is busy during the CCA checks the value of *NB* and *BE* are increased by one, and *CW* and *CCA* are reset to 2. The algorithm is also restarted, generates a new *RBC* value and, keeps retrying until the value of *NB* is less than or equal to $macMaxCSMABackoffs$ (its default value is 5). If the value of *NB* exceeds $MaxCSMABackoffs$ the algorithm reports the failure of packet transmission to the higher layer of the protocol. The algorithm then decides whether to retransmit as a new packet or drops the packet. It is also mentioned that the value of *BE* value cannot exceed *macMaxBE*, which is set to 5 as default. Once the medium is found IDLE after checking *CCA* twice, the packet is transmitted. It is noted that the backoff countdown value is restricted by the *NB* and *BE* values. If the device is operating in non-battery power that is determined by $macBattLifeExt$ (if it is set to false)

the value of *RBC* does not exceed 7, 15, 31, 31, and 31, in successive retries. If the device is operating in battery power (if *macBattLifeExt* is set to true) the value of *RBC* remains between zero and 3, 7, 15, 31, 31 on successive retries [23]. The smaller the value of *RBC* the larger the lifetime of batter is.

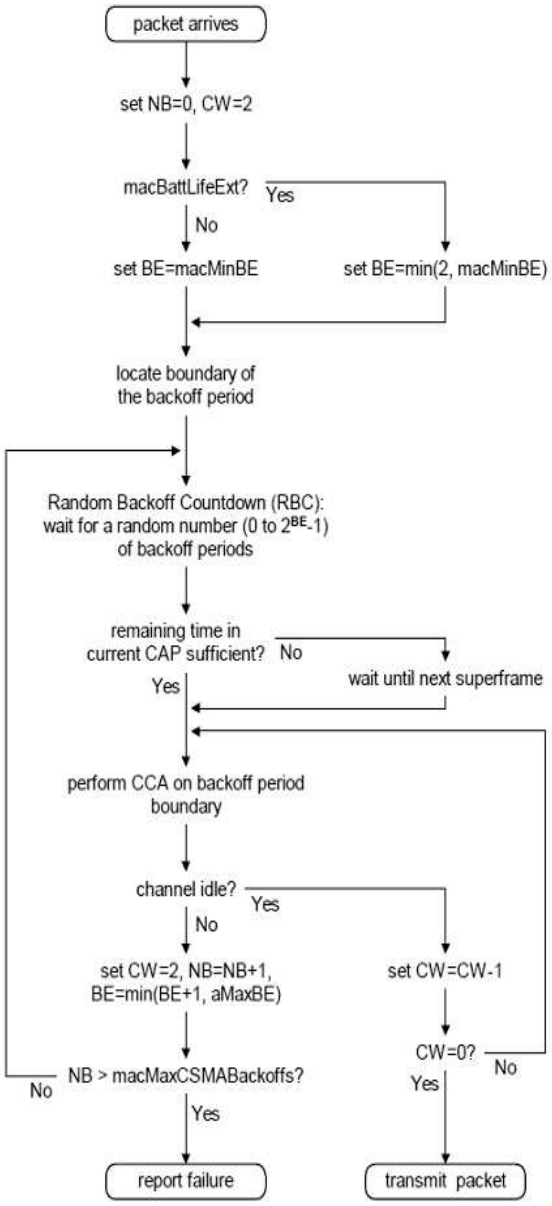


Figure 2.6: Flow chat of slotted CSMA-CA algorithm [23]

2.3.3 Acknowledgment of Successful Transmissions

The use of acknowledgment (ACK) frame is optional. This frame is sent by the coordinator on the request of subsequent devices. After sending the data packet the device should wait for the duration of $macAckWaitDuration$, which amounts to 54 or 120 symbols depending on the PHY option. If the frame is not received within that period the device assumes that the data frame is lost and hence, initiates a retransmission. To retransmit a lost frame there should have enough time in the CAP of the current superframe. Otherwise, the device needs to wait for the CAP of next superframe. The standard allows for the retransmission of a lost frame upto $macMaxFrameRetries$ times, which is set to 3. If $macMaxFrameRetries$ exceeds its maximum value without the successful retransmission, the frame is dropped and the failure is reported to the higher layer of the protocol stack. To transmit an ACK frame the standard allows piggybacked that means it can transmit without using CSMA-CA mechanism. However, two conditions must be fulfilled: (i)the coordinator must transmit the ACK packet by $aTurnaroundTime + aUnitBackoffPeriod$ period after receiving the data frame and (ii) there should be enough time in the current CAP for the data frame, interframe space value, and acknowledgement frame. If both conditions are not fulfilled then the ACK packet needs to be transmitted through the CSMA-CA procedure. In this thesis, we allow frames to be transmitted by following the CSMA-CA procedure and ACK frame is expected by the sender after data transmission. According to the standard, the ACK transmission should start at $aTurnaroundTime + aUnitBackoffPeriod$ after the transmission of data frame, which results in the delay of 12 to 32 symbol periods depending on the PHY option. One backoff period is equal to 20 symbol. Thus, for this period, the channel is kept idle for one backoff period.

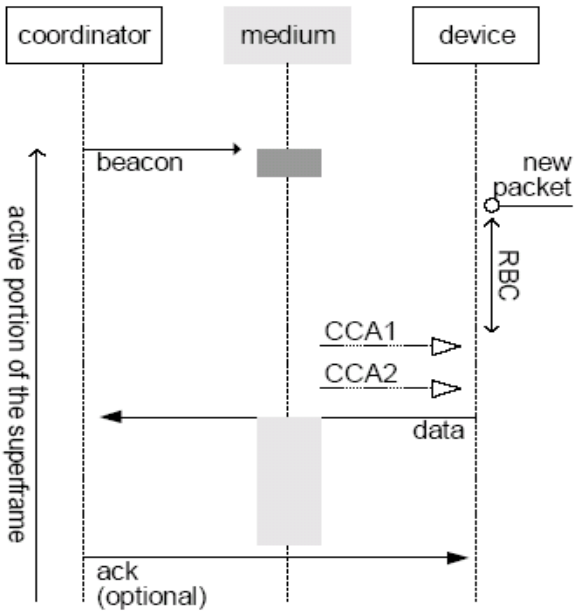


Figure 2.7: Uplink successful packet Transmission, beacon enabled mode [23]

2.3.4 Guaranteed Time Slots

After CAP, there could be a contention free period (CFP) within the time period of active portion of the superframe. In some applications, contention-based access may not work properly due to collision. If a node needs CFP it requests for this period and PAN coordinator may reserve some timeslots for this node for dedicated access to the medium. This contention free dedicated timeslots is called guaranteed timeslots (GTSs) illustrated in Figure 2.5. The coordinator may or may not accept the request. If the request is accepted the node can access the medium without any interference resulted by other nodes. During that period other nodes are not allowed to transmit any data. It is noted that the node that gets GTSs can still use the CAP with all other nodes. In this thesis, we do not consider any guaranteed timeslot in the active period. In the superframe, we consider only the CAP and

inactive period.

2.3.5 Probability of Sleeping for Tags

Energy efficiency is a great challenge for RFID and Sensor Networks. Active tags that have on board energy go to power saving mode or sleeping mode when the network is not active or reader is not available or there are no data to send. By turning off the radio subsystem sensor nodes and tags save the energy consumptions. In this thesis, we consider that RFID tags go to sleeping mode at the end of CFP period. They search and wait for the reader's signal when wake-up again. Thus, idle waiting time is reduced. To avoid synchronized wake-up time, the sleeping time of tags is randomized using geometric probability distribution [23]. Hence, the probability of more than one tags wake-up at the same time that results collision is reduced. The duration of sleeping period [23] can be expressed by Equation 2.1.

$$V(Z) = \sum_{k=1}^{\infty} (1 - P_{sleep}) P_{sleep}^{k-1} Z^k = (1 - P_{sleep}) Z / 1 - z P_{sleep} \tag{2.1}$$

The mean duration of sleeping period is expressed in Equation 2.2.

$$\bar{V} = V\acute{(}1) = 1/1 - P_{sleep} \tag{2.2}$$

In Equations 2.1 and 2.2, P_{sleep} denotes the probability of sleeping. However, if the buffer of a node is empty the node again goes to the sleeping mode. In a beacon enabled 802.15.4 cluster, a node that returns from the sleeping state and have packet to transmit will have to synchronize with the beacon.

2.4 IEEE 802.11 Medium Access Control (MAC) Protocol

The IEEE 802.11 is a set of standard that ensure that both radio-based network interface cards (NICs) and access points implement access methods for sharing the air medium [4]. This standard implements the Wireless Local Area Networks (WLAN) that use the frequency bands of 2.4, 3.6 and 5 GHz. This standard also allows for multiple modulation schemes, and high data rates. The fundamental method of IEEE 802.11 standard to access the medium is called Distributed Coordination Function (DCF) that is also known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). It uses an optional access method, called Point Coordination Function (PCF) and also hybrid access mechanism, called Hybrid Coordination Function (HCF) as shown in Figure 2.8.

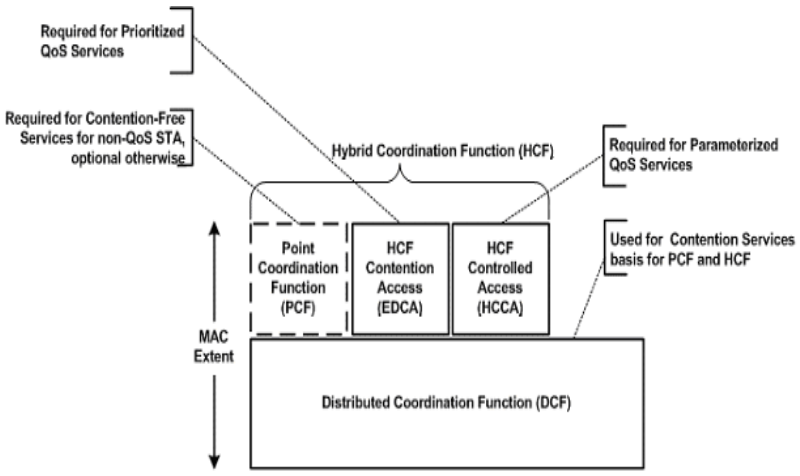


Figure 2.8: Medium Access Control Architecture [5]

2.4.1 Distributed Coordination Function (DCF)

DCF protocol is the fundamental method to access the medium using CSMA/CA medium access control algorithm. CSMA/CA works by sensing the medium before transmit. This

means that if a station wishing to transmit must first sense the radio channel to determine if another station is transmitting. The CSMA/CA scheme implements a minimum time gap exist between contiguous frames sequences.

A station that has packet to transmit first sense the channel status.If the medium is not busy, the transmission may proceed.If the medium is sense busy then the station differ it‘s transmission and needs to wait until medium becomes idle again.Stations need to sense medium being idle for distributed inter frame space(DIFS) period of time.The time after the idle DIFS is slotted and station is allow to transmit on the beginning of the time slot. Once the time has passed, the station selects a random amount(random backoff) of time to wait before sensing again to verify a clear channel on which to transmit. The CSMA/CA protocol avoids collisions among stations that share the medium by utilizing a random back-off time if the station’s physical or logical sensing mechanism indicates a busy medium.The random backoff time is decremented until the medium sensed idle and frozen if the medium becomes busy. The backoff counter is resume again after medium is sensed idle for more than $DIFS$ period of time. When the random counter reaches zero then the packet is ready to transmit. Figure 2.9 present the IEEE 802.11 DCF medium access control mechanism .

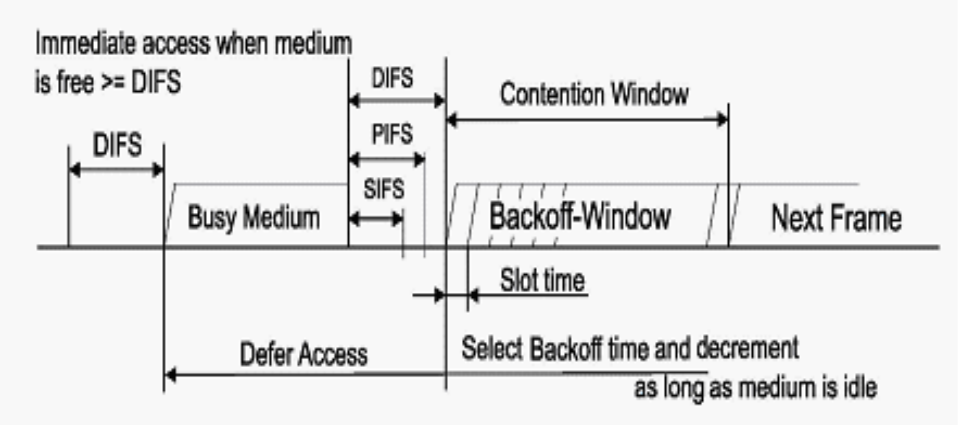


Figure 2.9: Basic Access Method of DCF [5]

The receiver of the packet acknowledge the successful transmission by sending a acknowledgement (ACK) packet after short interframe space *SIFS* to the sender station. The transmission is reported as unsuccessful if the ACK is not received during *SIFS* after the completion of current transmission. The unsuccessful packet needs to retransmit with doubling the CW until it reaches the retransmit limit.Once a frame has been sent from a given transmitted station then that station needs to wait until DIFS time interval to transmit again. When a station is transmitting than all other stations differ their access by setting Network allocation Vector (NAV) value.NAV use virtual carrier sense mechanism to determine the state of the medium. The NAV contains the duration information announced in frames prior to the actual exchange of data. The duration of NAV indicates the BUSY or IDLE state of the medium. If the medium is sensed BUSY when a station has started to transmit it should wait until the current transmission ends which duration is the amount of time set by other transmitting station in their NAV. Figure 2.10 presents the flowchart of the IEEE 802.11 DCF medium access control mechanism.

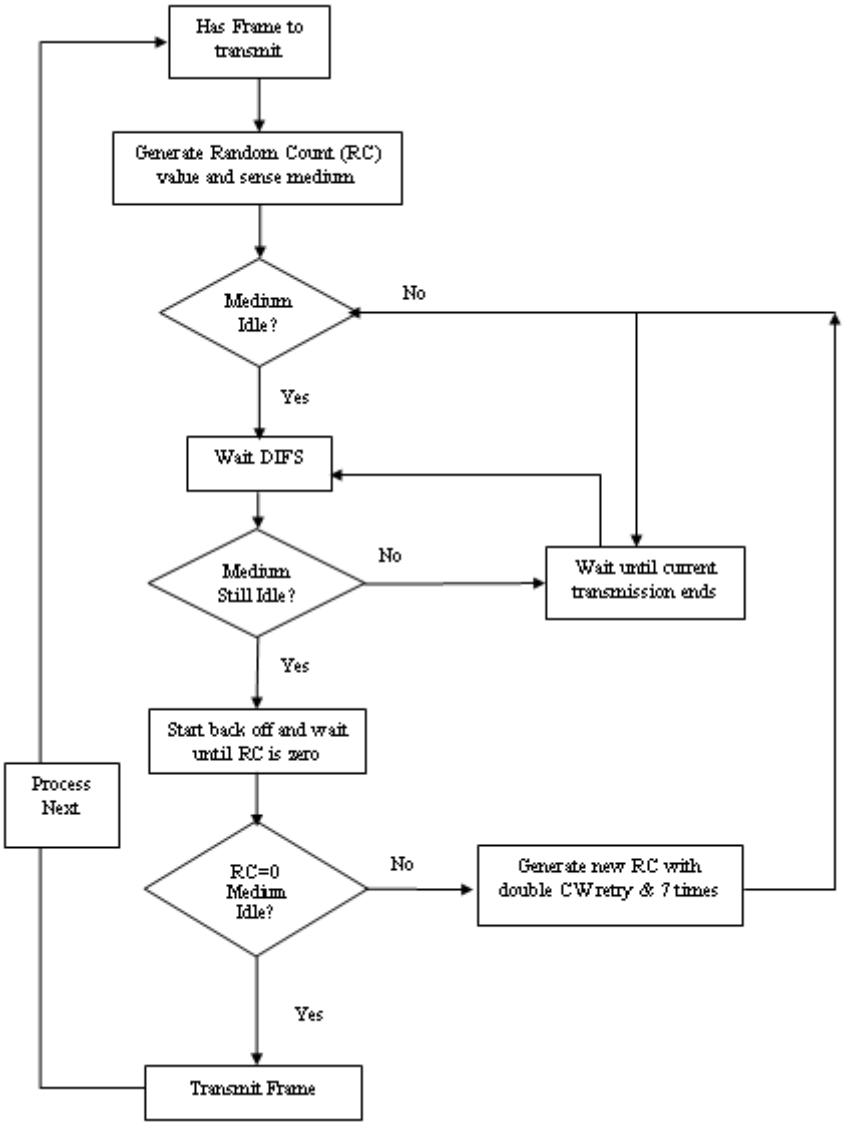


Figure 2.10: IEEE 802.11 DCF Medium Access Control Logic

DCF describes two techniques for packet transmissions: Basic Access mechanism with two-way handshaking and RTS/CTS mechanism with four-way handshaking. In our simulation model, we consider the RTS/CTS mechanism, where after the random counter reaches zero then before sending the data packet the station reserves the channel by send-

ing a short RTS frame . The destination station acknowledge (ACK) the receipt of the RTS frame by sending back a CTS frame. Then, the transmitting station sends the actual data packet and receiving stations replies with an ACK if it receives the data packet. Since no other station can transmit RTS or data packet after a successful transmission of RTS and receipt of CTS by a station, the collision can only occur on the RTS frame and is detected by the lack of CTS frame. The NAV contains the duration information announced in RTS/CTS frames prior to the actual exchange of data. All the other stations set their NAV value accordingly. Detailed working principle of this mechanism is illustrated in Figure 2.11.

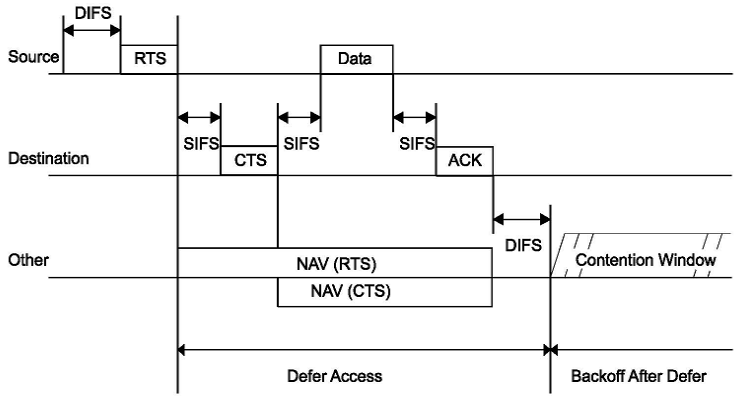


Figure 2.11: RTS, CTS,DATA, ACK and NAV settings [5]

2.4.2 Point Coordination Function (PCF)

The IEEE 802.11 standard also defines an optional access method called Point Coordination Function (PCF), which is a centralized MAC protocol. PCF is built on top of the CSMA/CA-based DCF, by utilizing the access priority provisions, as illustrated Figure 2.8. PCF enables the transmission of time sensitive information [4]. In PCF, a point coordinator

(PC) which can be the AP, controls the network and decides which stations can transmit for a certain period of time. It is an opportunity for the AP to become a PC. PCF provides contention free frame transfer in contention free period (CFP) and a PC goes through all the stations and poll one station at a time. The operating characteristics of PCF are that all stations get the chance to work in the same basic service set (BSS) under one PC. For instance, in CFP period, a station is being polled by PC and that station transmits data frame for a specific period of time when no other station can transmit. Then, the PC polls the next station. This process continues for all stations in the polling list. In PCF, stations are selected to transmit based on the round robin algorithm. At the beginning of the CFP all other stations set their NAV value and do not try to access the medium. The station being polled by a PC is called contention free(CF)-pollable station. PC and CF-pollable station transmit frame without using RTS/CTS mechanism. In CFP, a CF-pollable station may only transmit one MPDU to the PC or may be for other destination and may piggy-back the acknowledgement of received frame from the PC. If the acknowledgement of the transmitted frame is not received by the CF-Pollable station, the station cannot retransmit the frame unless it is polled again by the PC in the CFP or can retransmit in CP. If the frame receiver station is not CF-Pollable then the station replies to the recipient of the frame by sending an ACK frame following the DCF acknowledgement rules. A PC may retransmit an unacknowledged frame when the particular frame association identifier (AID) is in top of the polling list. A PC retransmits the unacknowledged frames during CFP after PIFS time. The transmitted data frame or acknowledged polling frame that are sent by PC or CF-Pollable station during CFP use the appropriate data sub-types based on the following rules. [5].

1. (i)Data and CF-Poll, (ii) Data, CF-ACK and CF-Poll, (iii) CF-Poll, and (iv) CF-ACK and CF-Poll-Frames are only sent by a PC.

2. (i) Data, (ii) Data and CF-ACK, (iii) Null Function, and (iv) CF-ACK frames may be sent by a PC or any CF-Pollable STA.

CFP Frame Structure and Timing

The PCF uses virtual carrier sense (CS) mechanism to access the medium which has access priority mechanism over other access method of IEEE 802.11 standard. The PCF sends information about getting control of the medium through beacon management frame and all the stations set their NAV value accordingly. The interframe space value use in PCF frame (PIFS) transfer is smaller than the DCF (DIFS) frame transfer, which gives the PCF point coordinator more priority to access the medium and transfer frame over DCF access method. This access priority provides CF access period and all the stations can transmit framed without contention for a limited period of time.

IEEE 802.11 protocol supports to alternate between the PCF and DCF access mechanism. Time is divided into CFP and CP as shown in Figure 2.12. In DCF time period, stations compete for using the CSMA algorithm. In PCF time period, stations wait for the poll to be selected as CF-Pollable station by PC before sending data. During CFP, frame transfer is controlled by PCF and each CFP begins after the beacon frame. The beacon frame contains Delivery Traffic Indication Message (DTIM) element and information regarding the CFP duration. All the stations set their NAV value based on these information. Beacon management frame also contains the CF parameter setting elements and Prob Response frames that are transmitted by stations. CFP duration is generated by PC regularly

at the CFP repetition interval, which is define as a number of DTIM intervals as shown in Figure 2.13. PC of the PCF controls the length of the CFP. The maximum length of CFP is calculated by the parameter *CFPMaxDuration* that is defined in the CF parameter setting elements of PC. *CFPMaxDuration* should be long enough to send and receive one data frame and short enough to send one frame during the CP period. The duration of CFP duration is as long as the length of several beacon frames. If this duration is greater than the beacon interval, PC should transmits the beacon in the appropriate time of the CFP. Then the time remaining field of CFP calculates the time left to reach it *CFPMaxDuration*. If the CFP starts after the beacon frame then the *CFPMaxDuration* is equal to the remaining duration of *CFPDurRemaining*. All the stations set their NAV value according to the value of *CFPDurRemaining*.

CFPDurRemaining specifies the maximum time duration of CFP, starting from the target beacon transmission time (TBTT) to the end of CFP. *CFPDurRemaining* is represented in time-unit(TU). After CFP, the beacon frames that are sent in CP should contain a zero value in *CFPDurRemaining*. Figure 2.13 illustrates the relationship of all parameters, where the CFP period and CFP repetition interval are twice and thrice of DTIM intervals, respectively. DTIM intervals is equal to 3 beacon intervals and aCFPMaxDuration is approximately equal to 2.5 beacon intervals. Depending on the size of the polling list and traffic in the network, PC has the ability to terminate any CFP before *aCFPMaxDuration*. If the medium is busy there is a possibility of delay in transmission of beacon frame in TBTT. This delay results the CFP to be foreshortened by the amount of beacon transmission delay as shown in Figure 2.14. If the medium becomes busy during the exchange of DCF frames the beacon is delayed until the end of the frame transmission. In this case,

$CFPMaxDuration$ specifies a value at the beginning of CFP that causes the end of CFP within the time period of $TBTT + aCFPMaxDuration$.

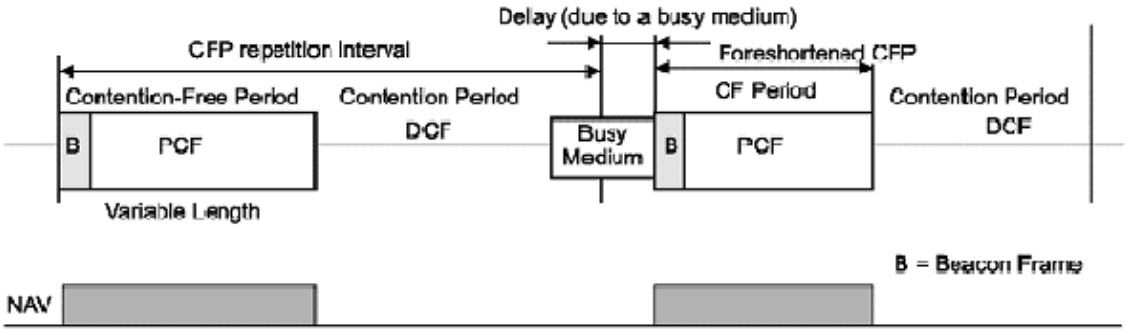


Figure 2.12: operation of PCF(CFP) and DCF(CP) in the same BSS [5]

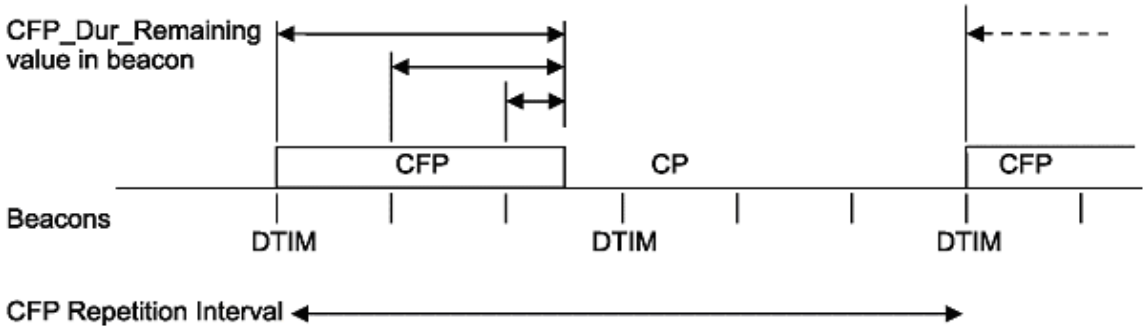


Figure 2.13: Beacon frames and CFPs [5]

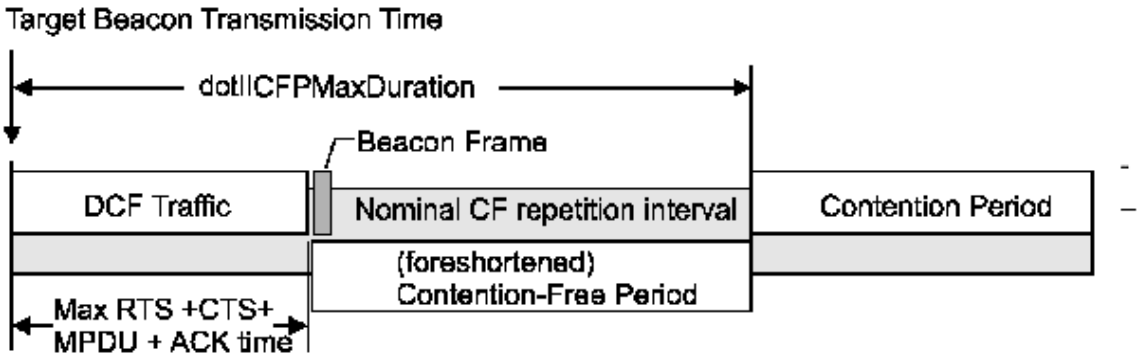


Figure 2.14: Example of delayed beacon and foreshortened CFP [5]

PCF Frame Transfer Procedure

PCF is a contention free protocol that provides contention free frame transfer and all the stations can transmit frames synchronously. Figure 2.15 illustrates the detailed description of a typical CFP cycle of PCF. At the beginning of the CFP, the station senses the medium for PIFS period of time. If the medium is sensed idle the beacon frame containing the CF parameter set element and a DTIM element is sent. A beacon frame also contains the information about the *CFPMaxDuration* and the remaining *CFPDurarion* and all the stations set their NAV value accordingly. After waiting for SIFS period of time of the beacon frame PC sends any of the following frames : data, CF-Poll, Data containing CF-Poll, management, or CF-End frame. As the response to the CF-Poll frame a station sends an acknowledgement frame (optional) after waiting for SIFS period of time. If a PC finds any data for that polled station it sends data containing CF-Poll. Otherwise, it only sends CF-Poll frame. After polled by the PC the station calculates if there is enough time in CFP to transmit a MPDU and receive its subsequent acknowledgement. If there is not enough

time remaining the station should defer the access and sends a Null or CF-ACK frame. In a condition when a station is being polled but there is no data to send the CF-End frame should transmitted immediately after the Beacon frame.After being polled, a station gets SIFS + timeToTxDataFrame interval of time to response to the poll in normal condition, but after waiting for again PIFS period of time the PC regain the control and moves to the next station of the polling list. In the response of the Poll if the station has data to send reply with Data+CFAck otherwise reply simply CFAck. . PC goes through it's polling list one by one and the station on top of list is being polled first. If there is enough time remaining then PC can poll another station and continue until the MinimumDataTransferTime left in the CFP. After that PC sends a CF-End frame to announce the end of the CFP and all the stations set their NAV value as null. Figure 2.16 shows the flowchart of the medium access procedure of the PCF.

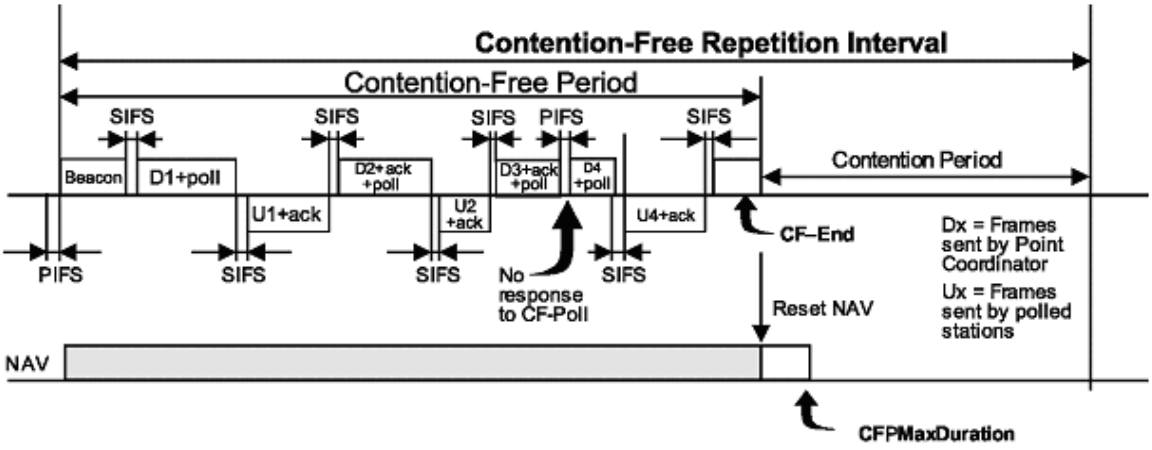


Figure 2.15: Example of PCF frame transfer [5]

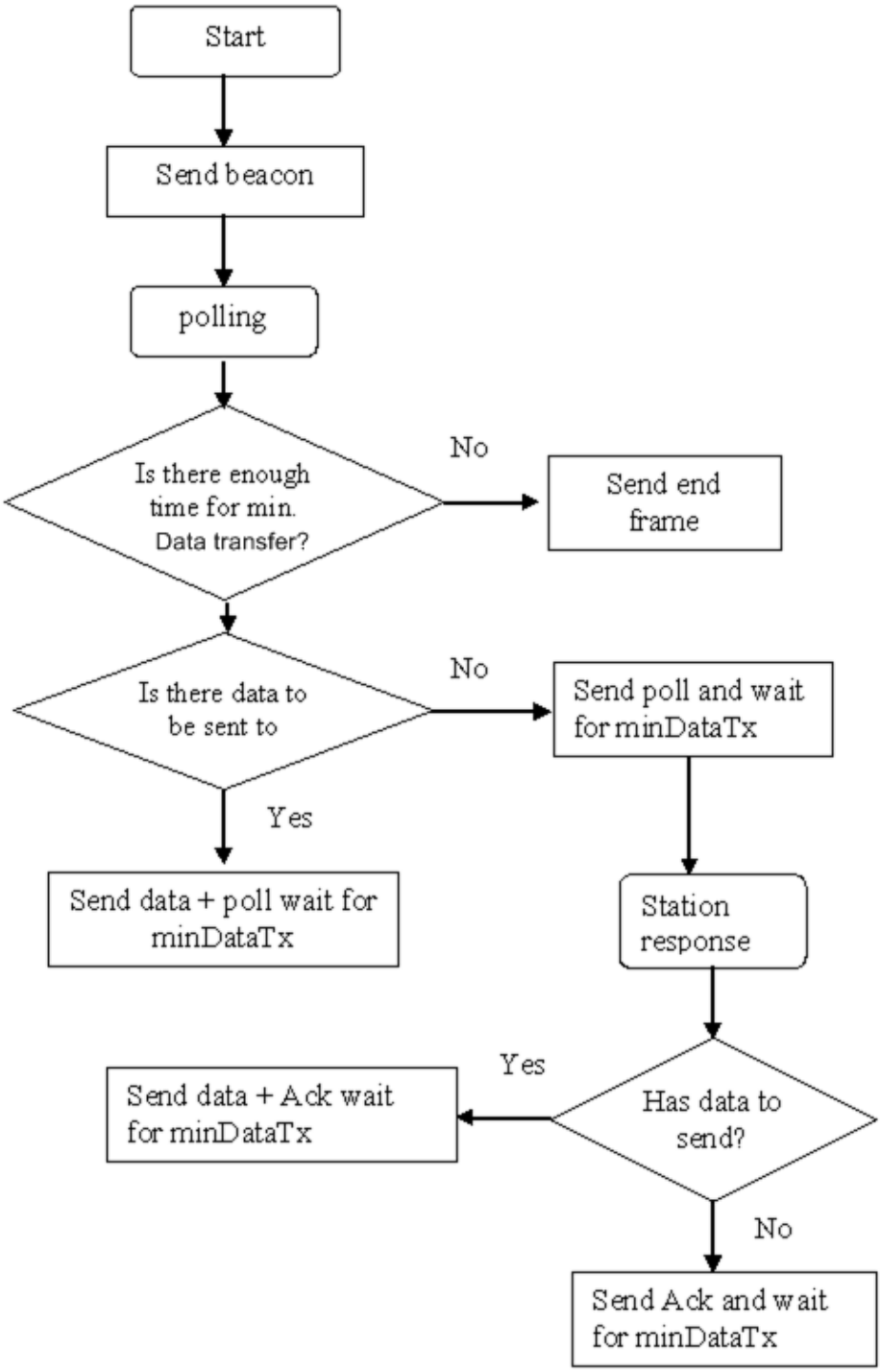


Figure 2.16: Flowchart of PCF medium access procedure

2.4.3 Limitation of IEEE 802.11

DCF: Using the DCF basic access mechanism a station determines the time to access the medium. This decision making process is distributed to all stations. All stations have the same minimum value of contention window and same priority to access the medium. Hence, there is no difference between the higher and lower priority stations and their traffic. Thus, no QoS support exists in DCF.

PCF:The IEEE 802.11 PCF provides QoS for time bounded services. Medium access for the PCF controlled stations have higher priority than that of the DCF controlled stations. PCF provides the limited QoS to the networks due to beacon delay and unknown transmission time for polled stations. Stations can start transmission before TBTT even if the current MSDU has not been finished. Because of the beacon delay from the TBTT a transmission delay occur for the time bounded MSDUs. This delay affects QoS since it causes irregular delay in each CFP. Moreover, PCs have no control of polled stations as they are allowed to transmit fragmented MSDU or MSDU with the maximum length of 2304 bytes. This reduces the QoS of the stations, which are polled in the remaining time period of CFP.

2.5 QoS support mechanisms of IEEE 802.11e

The improved version of the IEEE 802.11 called IEEE 802.11e standard supports priority schemes. To ensure QoS in stations it provides user access priorities among the stations. The IEEE 802.11e supports CP and CFP within one superframe. IEEE 802.11e supports Contention-based channel access method that provides contention based frame

transfer called Enhanced Distributed Channel Access (EDCA) mechanism. EDCA is used only in CP.

2.5.1 Enhanced Distributed Channel Access Protocol (EDCA)

To avoid unpredictable transmission delay, the IEEE 802.11e MAC is improved by using the transmission opportunity (TXOP) value. This value ensures that an IEEE 802.11e station that obtains medium access should not use the medium longer than the defined TXOP limit value. A TXOP is a interval of time during when a station gets an uninterrupted transmission opportunity to transmit MSDUs to the medium. Frames initiate transmission if there is enough time to complete the transmission. This also reduces the beacon delay, as no frame is permitted to transmitted across the Target Beacon Transmission Time (TBTT). Which gives HC better control of the medium. EDCA provides distributed and differentiated access to the medium by the stations which use 8 different user priorities (UPs). These UPs are categories into 4 Access categories (ACs). For each AC, an enhanced DCF medium access mechanism is used, which follows the same rules of DCF. However, three major changes to the operation of the original DCF are listed below.

Priority	UP (Same as 802.1D user priority)	802.1D designation	AC	Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	—	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
Highest	7	NC	AC_VO	Voice

Figure 2.17: UP-to-AC mappings [23]

1. Instead of distributed inter-frame space (DIFS), an inter-frame space (AIFS) is used. AIFS is the minimum idle time after which a station is permitted to access the medium.

2. Contention window (CW) pair minimum/maximum size is not same for every ACs. Using the CW random backoff value is computed.

3. During the maximum channel holding time or transmission opportunity time (TXOP) a station can access medium and send more than one packet. If the value of TXOP is set to 0 then only one frame can be sent.

The QoS support is provided to the stations by introducing these AC‘s with different and multiple independent backoff procedures. Each stations can transmit parallel 4 MSDU‘s using 4 different backoff entity as categorize according to their target application. Each of the backoff entity is prioritized according to AC specific contention parameters which is

define in EDCA parameter set. The EDCA parameter set defines the AC‘s priority as in order of AC_VO(voice), AC_VI(video), AC_BE(best effort) and AC_BK(background). The EDCA parameter set differentiate the AC‘s chance of medium access by setting individual interframe space value, contention window, TXOP value and many other parameter values per AC.

2.5.2 Queuing Structure

Each of the stations has 4 queue and data frames are prioritized according to the 4 access categories as mentioned earlier. If a station has data frames ready to send, it is classified and placed in to the appropriate queues. The inter frame space value and contention window value is calculated independently for each AC queues and decremented in parallel when medium is sense idle. In case of internal collision which happens when two or more queues are ready to transmit at the same time, the higher priority queue can transmit where as, the other queues act as physical collision happen during the transmission. The collided queue needs to double their CW value and increase retry counter. Thus each physical station works as 4 logical stations and hold 4 queues, each for one type of traffic queue. The following figure 2.18 illustrates these priority queues.

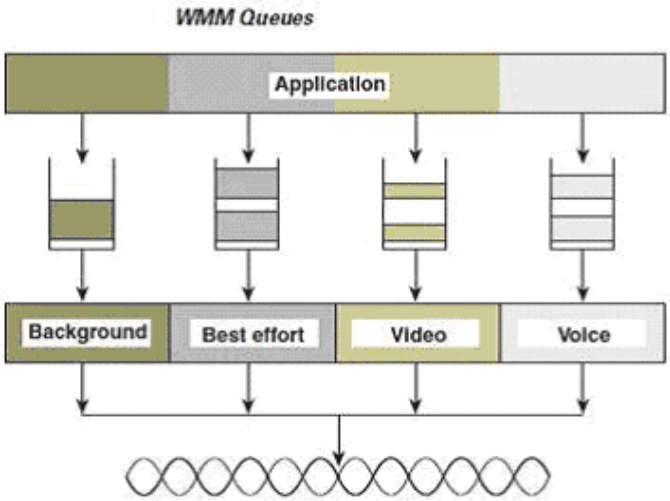


Figure 2.18: Queuing Structure of IEEE 802.11e EDCA [23]

2.5.3 Interframe space value

Each backoff entity needs to wait for a small amount of time before start down counting the backoff value. The time interval between the frames is defined by interframe space (IFS) value. During this value a station should determine that medium is idle through carrier sensing (CS). Five different types of IFS value is used which provides the different priority to access the wireless medium-

1. SIFS short interframe space
2. PIFS PCF interframe space
3. DIFS DCF interframe space
4. AIFS arbitration interframe space (used by the QoS facility)
5. EIFS extended interframe space

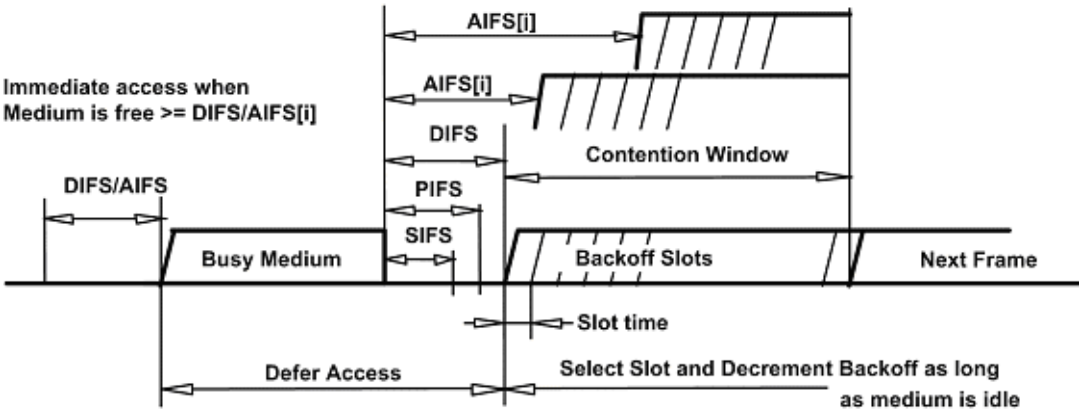


Figure 2.19: Some IFS relationships [23]

The different IFSs used by different stations depend on their bit rate and these values are determined by the PHY according to their attributes.

AIFS: The IFS defined for EDCA is called Arbitration Interframe space (AIFS) which is different according to AC (AIFS[AC]). The QoS stations use AIFS to transmit MPDUs, all management frames (MMPDUs) and for the PS-POLL, RTS, CTS,BlockAckReq and BlockACK control frames. The AIFS[AC] value should be at least Duration of DIFS and can be vary depending on AC priority which is determine by the help of arbitration inter-frame space number (AIFSN[AC]). AIFSN[AC] value is selected for QoS STA by HC for each AIFS[AC] from the dot11QAPEDCATableAIFSN attributes in its MIB.For non -AP QoS STA this value is determine for each AIFS[AC] from the dot11QAPEDCATableAIFSN attributes in its MIB. The AIFSN [AC] defines the duration of AIFS [AC] according to the following formula-

AIFS[AC] = SIFS+AIFSN[AC] x aSlotTime, AIFSN[AC] $= 2$

The smallest access time of medium is DIFS, aSlotTime is the duration of a slot. The AC with small AIFSN[AC] gets the higher priority to access the medium.

2.5.4 Contention Window (CW) value

CW value is the another parameter value depend on which AC gets the priority to access the medium. The random backoff counter value is defined by the CW. The EDCA parameter set define the CWmin and CWmax value for each AC . The smaller the CWmin[AC] value the higher the medium access probability. The EDCA contention window value varies according to AC and derived from DCF base values which is according to standard [5] for IEEE 802.11b $aCWmin$ is 31 and $aCWmax$ is 1023.

AC_VO *Voice* CWmin = $aCWmin + 1/4 - 1$, CWmax = $aCWmin + 1/2 - 1$

AC_VI *Video* CWmin = $aCWmin + 1/2 - 1$, CWmax = aCWmin

AC_BE $BestEffort$ CWmin = aCWmin , CWmax = aCWmax

AC_BK *Background* CWmin = aCWmin , CWmax = aCWmax

Following table 2.4 shows the default values of AIFSN[AC] and CW[AC] for IEEE 802.11b PHY in a QoS BSS according to standard [5]

Table 2.4: EDCA parameter set element value

Priority	UP (Same as 802.11 UP)	AC (informative)	Designation	CWmin	CWmax	AIFSN [AC]
low	0	AC_BE	Best Effort	31	1023	3
low	1	AC_BK	Background	31	1023	7
high	2	AC_VI	Video	15	31	2
high	3	AC_VO	Voice	7	15	2

In a QoS BSS each queue of the AC has different access time to the medium. The frames of the voice queue which is AC[3] will initially select a random backoff timer between 0-3, frames in the video queue which is AC[2] will select a random backoff timer between 0 - 7,other ACs (AC[1] and AC[0]) will also select their backoff value according the above table. In this way, frames of the voice queue which have higher priority, have the

grater chance of selecting lower random backoff value compared with video, best effort and background. There are chances of lower priority frames can select lower random backoff value, but normally it doesn't happen. From the table we can see that , the maximum and minimum CW values of voice and video are smaller then best effort and background queue. The CWmin and CWmax values are encoded in exponent from with base 2. Each filed of the values are 4 bit long and decremented by 1 in the EDCA parameter set information element. Accordingly the CWmin values is 0 and CWmax is 32,767 [1] but practically the CWmax value always set as 1,023 and never above this.

2.5.5 Contention Window Scaling

Following figure 2.20 shows the increment of CW values with number of retries. Initially for the first attempt of transmission the random backoff timer it is set to a value between 0 - Cwmin. In case of collision indicated by lack of acknowledge frame the CW value will be increase. For each number of retries the CW value will double by a power of 2 which is called binary exponential backoff. When the CWmax value reaches the maximum limit it will remain unchanged until the subsequent retransmission attempt reached the retry limit or frame is successfully transmitted.. The maximum number of retries is 7 according to this standard.

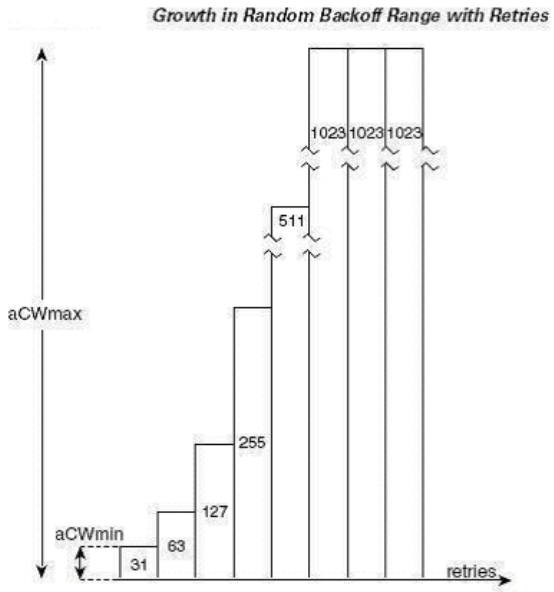


Figure 2.20: Contention Window Scaling [23]

The IEEE 802.11e AIFS and CWmin values are illustrated in the following figure 2.21, based on the 802.11b PHY.

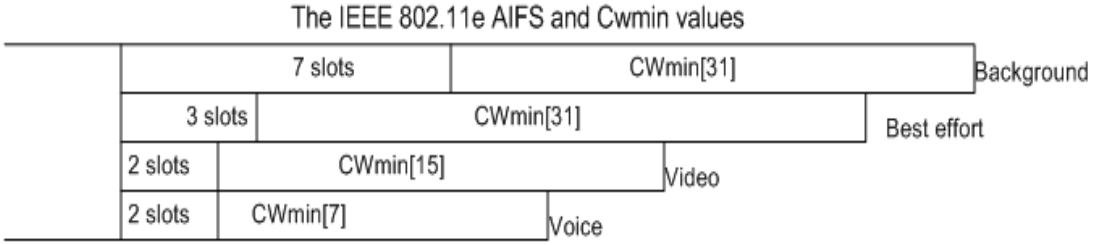


Figure 2.21: The IEEE 802.11e AIFS and CWmin values

2.5.6 EDCA TXOPs

EDCA uses two modes of TXOP first one is initiation of the EDCA TXOP and another one is multiple frame transmission within one EDCA TXOP. The first mode is present

when EDCA rules permit to access to the medium. Multiple frame transmission within one EDCA TXOP duration is occur when the EDCAF(Enhanced Distributed Channel Access Function) obtain the right to access the medium and complete the frame sequence. The TXOP limit value is broadcast by AP in the EDCA parameter set information element through the Beacon and Probe response frames. TXOP limit value 0 means that a single MSDU or MMPDU can be transmitted.

2.5.7 EDCA Medium Access Control mechanism

In EDCA for each ACs an enhanced DCF is used which follow the same rules of DCF four way hand shaking (RTS-CTS)medium access mechanism only some operational rules and parameters changes in the channel access method discussed above. If a node with AC[k](where k indicating the access category number) wants to transmit a packet it needs to sense the medium for the duration of AIFSk(AIFS number for ACk).If the medium is still idle after AIFSk it can transmit the packet without backoff procedure. In this protocol medium can become busy during the AIFSk period then it needs to restart the AIFSk value and wait for the medium becomes idle again. After the medium becomes idle carrier sensing needs to restart from the beginning of the AIFSk. For interrupted AIFSk each AC can not transmit the packet without backoff procedure. The backoff procedure is necessary for an EDCAF, if

1. for that AC an attempt to transmit the packet after sensing medium idle for AIFSN[AC] without backoff was not successful;

2. packet needs to retransmit as fail of transmission due to collision, indicated by failure of receiving of CTS in response of RTS and receiving of ACK in response of MPDU;

3. A frame of that AC is ready to transmit but medium is not idle indicated by physical or virtual carrier sense and backoff countdown becomes zero.

4. The AC with TXOP finished the final transmission and was successful.

5. For the internal collision when two or more EDCAFs of the same stations get the TXOP at the same time and collide one with another that has higher priority.

The CW [AC] value is reset to CWmin [AC] if the frame is successfully transmitted by that AC. If the backoff procedure is invoked because of the above condition 3 the value of CW [AC] shall be left unchanged. If the backoff procedure is called because of the above condition 2 and 5 the CW [AC] value shall be updated as follows:

1. If the QoS station reached the retry limit of EDCA parameter set element indicated value ,CW[AC] shall be reset to CWmin[AC]

2. If CW[AC] is less than CWmax[AC], it shall be increase by double in every retries as (CW[AC]+1)*2-1.

3. If CW [AC] is equal to CWmax [AC], the CW [AC] value shall remain unchanged for the rest of the reties.

After the AIFSk period if medium is still idle then a random backoff number is generated.The backoff number is decremented in each idle backoff slot.If the medium becomes busy during the backoff countdown, the backoff counter will be remain frozen until the medium becomes idle again for the duration of AIFSk = AIFSNk * aSlotTime. When the medium sense idle and backoff counter becomes zero frame transmission starts.After backoff phase 0 (uninterrupted) if there is no packet in the queue then without backoff it can not

be transmitted. When another packet will be in the queue than the previous packet can be transmitted. If the collision occurs the frame needs to retransmit and repeat backoff procedure with doubling the contention window. In this protocol transmission of a frame can be retry 7 times after that that frame is dropped. There are 7 backoff phase starting from phase 0 and CW value can be double until it reaches the CWmax value. After CWmax the value remain unchanged until the end of the transmission. Figure shows 2.22 the flow chart of EDCA CSMA/CA medium access mechanism.EDCA protocol also use RTS/CTS four way handshaking technique to transit a frame. Where before sending the data packet it first send the RTS frame. After sensing the medium idle for AIFS [AC] it starts backoff counting.

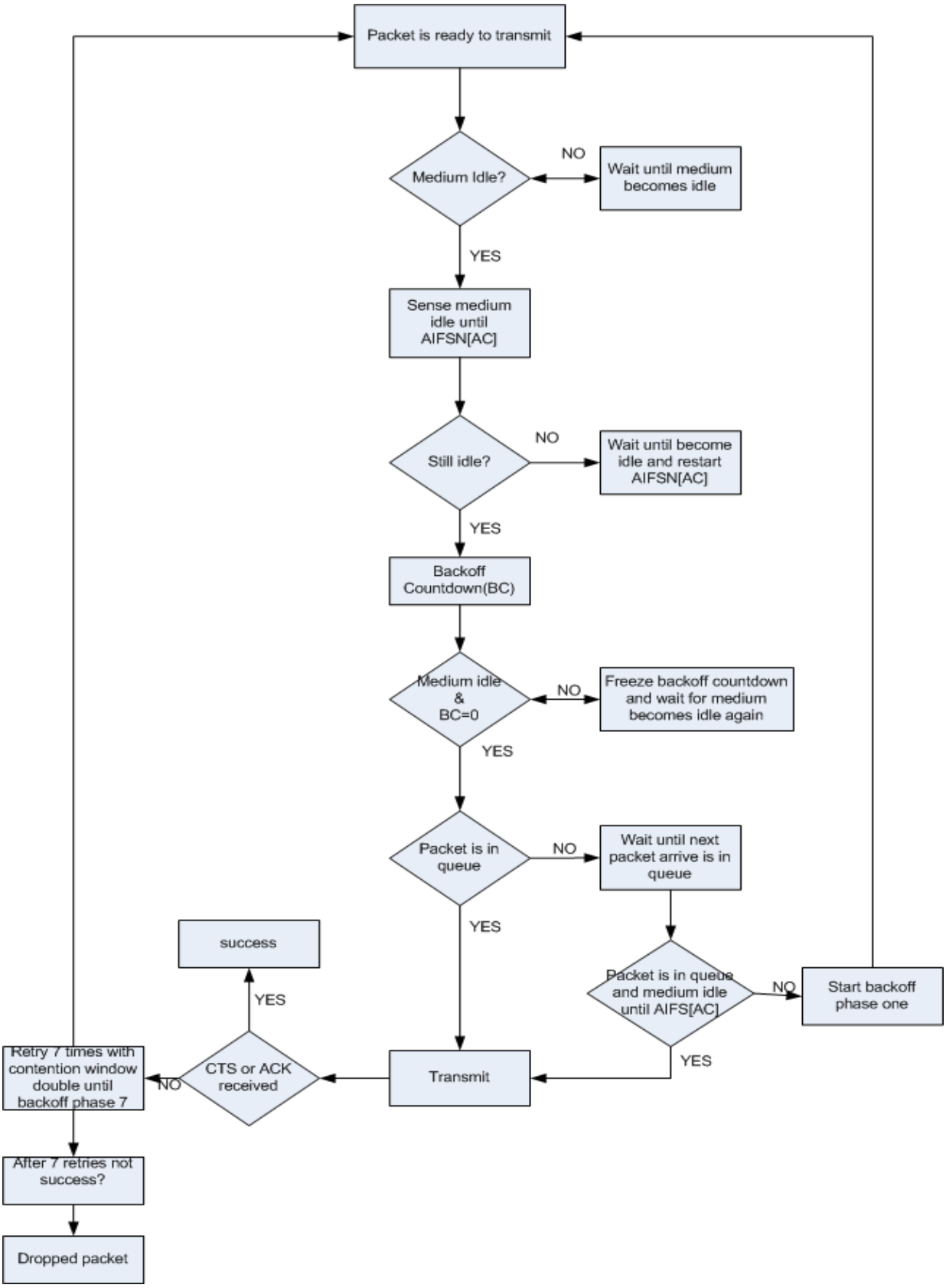


Figure 2.22: Flowchart of the EDCA CSMA/CA mechanism

When the backoff counter reaches zero and there is another packet in the queue of that AC then it can send the RTS and wait for the CTS. After receiving the CTS the data packet is transmitted and waits for the ACK frame. In case of collision, which is indicated by failure to receive a CTS or ACK, the packet is retransmitted until backoff phase 7 after that the packet id dropped. If there is a internal collision, because of the fact that two or more traffic queue transmit at the same time, the higher priority queue will get the chance to transmit, whereas other queues will retry upto 7 times with double CW values.

Chapter 3

Scheme for WLAN and RFID Coexistence

Timing mechanism within the IEEE 802.11 standard supports that stations on the Wireless Local Area Network (WLAN) alternate between the use of Distributed coordination function (DCF) and Point coordination function (PCF) [4]. Time is divided in to contention free period (CFP) and contention period (CP). As a result, the WLAN can support both asynchronous and synchronous information flows. To solve the problem of WLAN/RFID co-existence, the proposed solution allows the WLAN and RFID to access the medium in a time sharing manner by making the WLAN Access Point (AP) aware of the RFID neighboring network at the Medium Access Control (MAC) layer. In this approach, RFID readers act as Wi-Fi nodes. Thus, a RFID readers works as bridge between RFID and WLAN networks and allows a single AP to cover multiple RFID networks. We consider the IEEE 802.15.4 protocol to transmit tags ID from tag to the reader. In the WLAN side, we consider Quality of Service (QoS) stations in the networks by improving the basic ac-

cess protocol of the IEEE 802.11 DCF to access the medium with Enhanced Distributed Channel Access (EDCA). EDCA provides QoS among the stations by dividing 8 user priorities into 4 Access Categories (AC).The objective of the proposed research is to provide QoS while integrating RFID with Wi-Fi WLAN so that there will be differentiation between the data of RFID and ordinary WLAN nodes. We are expecting RFID reader will not be affected by ordinary Wi-Fi nodes while they are accessing medium to send their data packet. We only consider 2 traffic classes. The data traffic from the RFID network is the $AC[3]$, which gets the highest priority to access the medium, whereas the data traffic from WLAN is the $AC[0]$ which has the lowest priority to access the medium.

In the proposed solution,we consider that the RFID active tags and WLAN networks work on 2.4GHz microwave band with data transmission rate of 250 kbps for RFID and 2 Mbps for WLAN. At the beginning, the AP periodically broadcasts beacon frames. These frames contain information about the duration of Contention-Free Period (CFP) and Contention Period (CP), which are be used to access the medium by RFID and Wi-Fi, respectively. In CFP or PCF period only RFID networks (tags) work and all other networks such as WLAN remain silent. After the PCF or CFP period, Wi-Fi nodes of WLAN along with RFID readers work and send data to AP in the CP or DCF period. No polling is performed at the beginning of the CFP instead all RFID readers start reading the tags in their vicinity. Then, the readers transfer data to the Wi-Fi nodes 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. For faster and more reliable access, one reader can be co-located with the AP. The AP collects RFID readings from all the bridged readers and forwards them to the application server. This approach might require a simple mod-

ification on both the RFID readers and AP MAC parameters but it does not require any modification on the existing RFID tag hardware or software. This makes this approach economically feasible and thus, readily applicable in practice. Furthermore, the use of off-the-shelf Wi-Fi hardware provides an easy transmission of RFID readings to the AP that is also transparent to the ordinary WLAN nodes.

The primary prototype of the proposed model is shown in Figure 3.1. We consider 3 RFID networks each with one reader and up to 200 tags. The reader collects data from the tag and sends to AP where, a single AP is able to cover the whole RFID and WLAN networks.

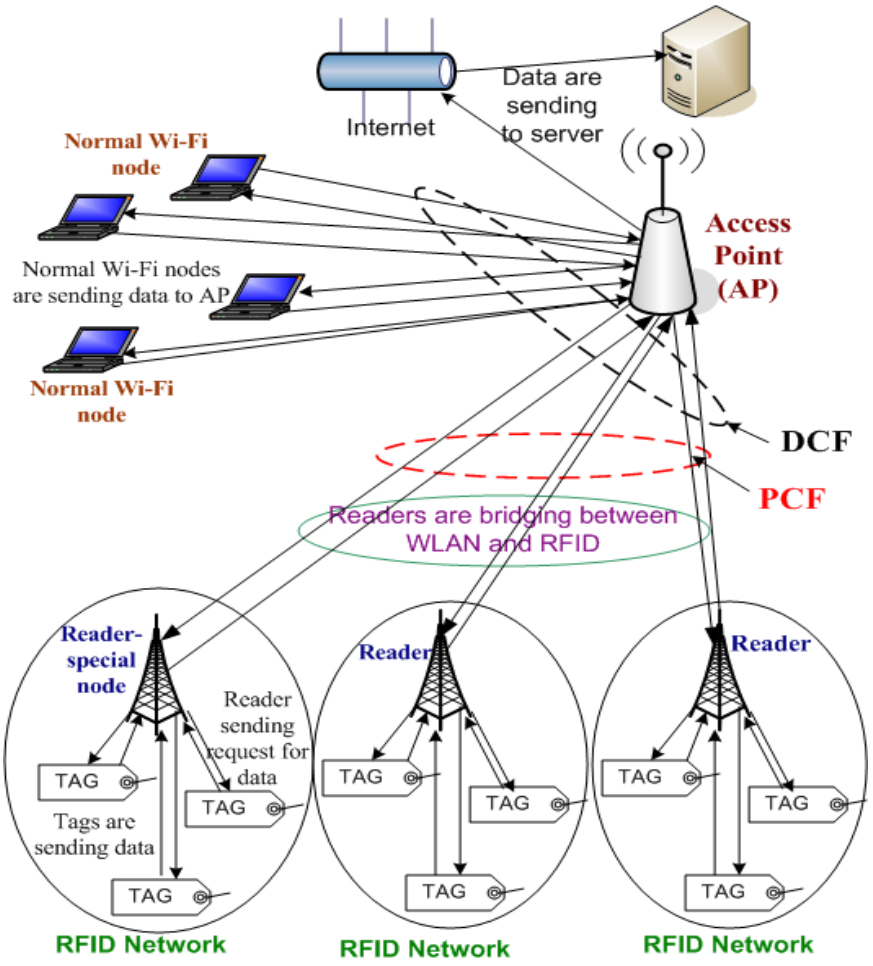


Figure 3.1: Model of RFID and WLAN Integration

The composition frame structure of two networks is illustrated in Figure 3.2. IEEE 802.11 PCF periods is mapped with the IEEE 802.15.4 superframe CFP and DCF is mapped with the IEEE 802.15.4 superframe inactive period. Readers send data to AP as well as other Wi-Fi nodes that work in the CP period. In the CFP or active period of 802.15.4 superframe, data is sent from tags to readers. Inactive period starts when a CF-End frame is received at the end of CFP period. Then the tags go into the sleeping mode. After the CP period, again beacon frame is sent that repeatedly starts the new superframe. In the

following section, we present both networks in detail.

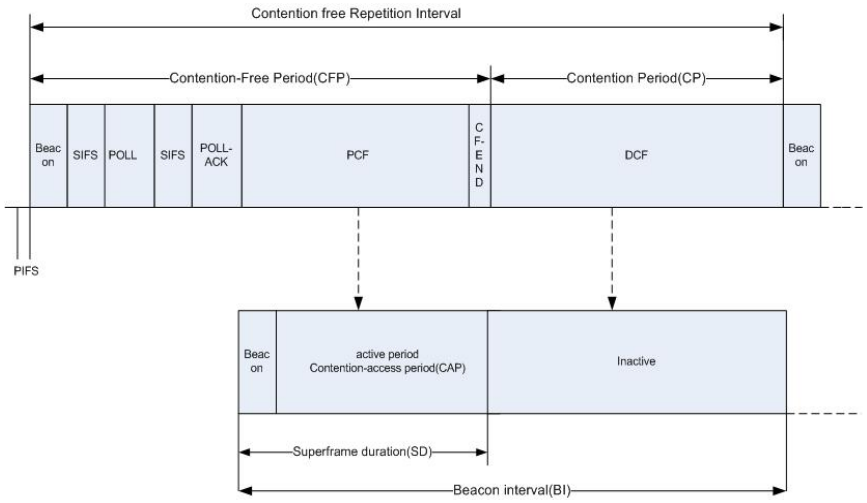


Figure 3.2: The composition of frame structures of IEEE 802.11 and 802.15.4 standard

3.1 Uplink Communication of RFID Networks in Contention Free Period

One of the objectives of the proposed solution is to consider the IEEE 802.11 and IEEE 802.15.4 interference problem. The possible solution is to use the IEEE 802.11 PCF medium access mechanism. RFID networks only work in the CFP period of PCF and other networks remain in sleep mode in that period. This phenomenon reduces the interference problem greatly.

In the proposed simulation model, we only consider the uplink communication using the IEEE 802.15.4 protocol, where data is only transmitting from tags to readers but not vise versa. AP sends beacon messages at the beginning of the CFP. The beacon contains information regarding CFP period. Readers initiate transmission whenever they receive

polling from AP and send them to the tags. Readers also send ACK to the AP if they receive polling. One reader work at a time that is selected on round robin fashion. As soon as a reader finishes transmission controlled is transferred to the next reader of the polling list. If there is not enough time to complete the data transmission a frame indicating the end of CFP is sent. If a station can send all data within the specified time period the polled station control is transferred to another station at the end of current transmission.

Tags transmit data to a reader which also work as a coordinator for the RFID networks. RFID use Slotted CSMA-CA medium access mechanism to transfer data from tags to a reader. A few modification of the current IEEE 802.15.4 standard's MAC frame is required for the RFID network that work in the frequency band of 2.45GHz with data transmission rate of 250kbps (Figure 3.5, and 3.4). IEEE proposes a new standard IEEE 802.15.4f which mentions the necessary MAC frame changes. For the proposed simulation model, we consider 3 BSS, where each BSS consists of one reader and up to 200 tags. In the IEEE 802.15.4 standard, values for two important parameters, beacon order (BO) and superframe order (SO) are chosen carefully and are listed in Table 2.3. The *SO* is used to calculate the super Frame Duration (SD) period and *BO* is used to calculate the Beacon Interval (BI) period. The slot time of the IEEE 802.15.4 is 16 times larger than that of the IEEE 802.11. The backoff value in one superframe is 2 and all slots are equally divided.

Whenever tags receive beacon from the polled readers, CAP/active period of 802.15.4 superframe starts working. If a tag has data to send it sets the initial parameters value as mentioned in the Section 2.3 of Chapter 2 and starts to countdown *RBC*. When the value of *RBC* reaches zero the tag requires to perform two clear channel assessments (CCA). In the first CCA, if the medium is free, the tag performs the second CCA. If the medium is

found free in both CCAs the tag can transmit the packet and wait for the acknowledgement. Transmission occurs only at the boundary of the slot. Hence, if the transmission requirement is fulfilled in the middle of the slot the tags needs to wait for the boundary of the slot to make it happen. Before the two CCA, it requires to check if the current superframe has sufficient time to send the packet. Otherwise, the tags needs to wait until the active period of next superframe. A CF-END frame is sent to tags that indicates the end of active and CFP period. At the end of active period, the inactive period starts when the tags remain in sleep mode. Each tag has an input buffer which store 2 packet in our simulation model. In the active period, if a new packets arrives but finds the buffer full that packet is dropped. When the server is in the sleep state, the 'push-out' policy is used, where a newly arrived packet is always admitted to the buffer. If the buffer is full at that time, admission is accomplished by discarding the packet at the head of the buffer and moving all other packets in the buffer one position so as to make space for the newly arrived packet. Thus, the server that returns from the sleep state always finds the most recent packets in its buffer, which is beneficial in many sensing applications.

2 Octets	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10	Variable	2
Frame Control	Sequence Number	Dest. PAN ID	Dest. Address	Source PAN	Source Address	Security Header	Payload	CRC

Figure 3.3: General 802.15.4 MAC Frame format [2]

2	1	2	0/2/8	Variable	2
Frame Control	Sequence	Dest. PAN	Source Address	Payload	CRC

Figure 3.4: Blink Frame format [2]

3.2 Uplink Communication of WLAN Network in Contention Period

Another objective of the proposed solution is to integrate RFID and WLAN networks. RFID reader acts as a special station and integrates two networks. After the CFP period of PCF, CP of DCF starts. In DCF, all normal Wi-Fi stations and RFID readers compete for the medium to transmit data packets to AP. Data packets are transferred only when the medium is found idle by following the DCF medium access mechanism. The CP or active period of DCF protocol of WLAN is mapped with the inactive period of the IEEE 802.15.4 superframe (Figure 3.2). At the end of CFP, CP starts when RFID network remains in sleep mode and set there NAV value.

During the uplink communication of WLAN, data is transferred from a station to AP

but not vise versa. The IEEE 802.11e contention-based channel mechanism, EDCA protocol is used as a medium access mechanism. CSMA-CA algorithm and DCF four-way handshaking (RTS/CTS) packet transmission technique is used in CP period. If a station has data to transmit it checks the status of the medium and also whether it is CP or CFP. If the station senses the medium as idle for the duration of inter-frame space of time (AIFS) in CP or active period of Wi-Fi mode then the station generates a random number. The random number/backoff is decremented if the station receives idle backoff value (i.e., idle medium). Whenever the random backoff value reaches zero the station transmits if there is any packet in the queue. Before sending the data packet the station sends the RTS packet and waits to receive CTS packet from the AP. The station sends data packet to AP after receiving CTS. If AP receives data successfully it replies with an ACK packet that notifies the end of current transmission. At the end of CP period, the WLAN station sets its NAV value according to the CFP period of PCF.

3.3 Superframe Timing Schedule of Proposed Solution

Figure 3.5 illustrates the total communication cycle of the proposed solution. In the first cycle of superframe, AP sends a beacon frame that contains information about the CFP period and then reader one (R_1) is polled to start working. During this period, only R_1 uses the medium and collects tag IDs and store them for further use. All other stations set there NAV value accordingly. At the end of CFP or $CFPMaximum$, R_1 sends CF-END frame to AP to notify the end of its activity. If R_1 still have frames to transmit but the CFP period ends and reaches to $CFPMaximum$ the AP switches to CP of DCF when WLAN networks start working. R_1 also works with all other normal Wi-Fi nodes to send its stored tag IDs to

AP since it is a special node that works as an interface between two networks. At the end of the CP period of DCF, the second cycle of superframe starts when reader two (R_2) is polled. Similarly, R_3 works in the third cycle. Since we consider only three RFID networks, only stations of WLAN work in the whole fourth cycle. Then R_1 will be polled again in the fifth cycle. The time duration between the first cycle of R_1 and the next cycle for R_1 polled cycle is called beacon interval (BI). The default value of BI between PCF and DCF is 100TU.

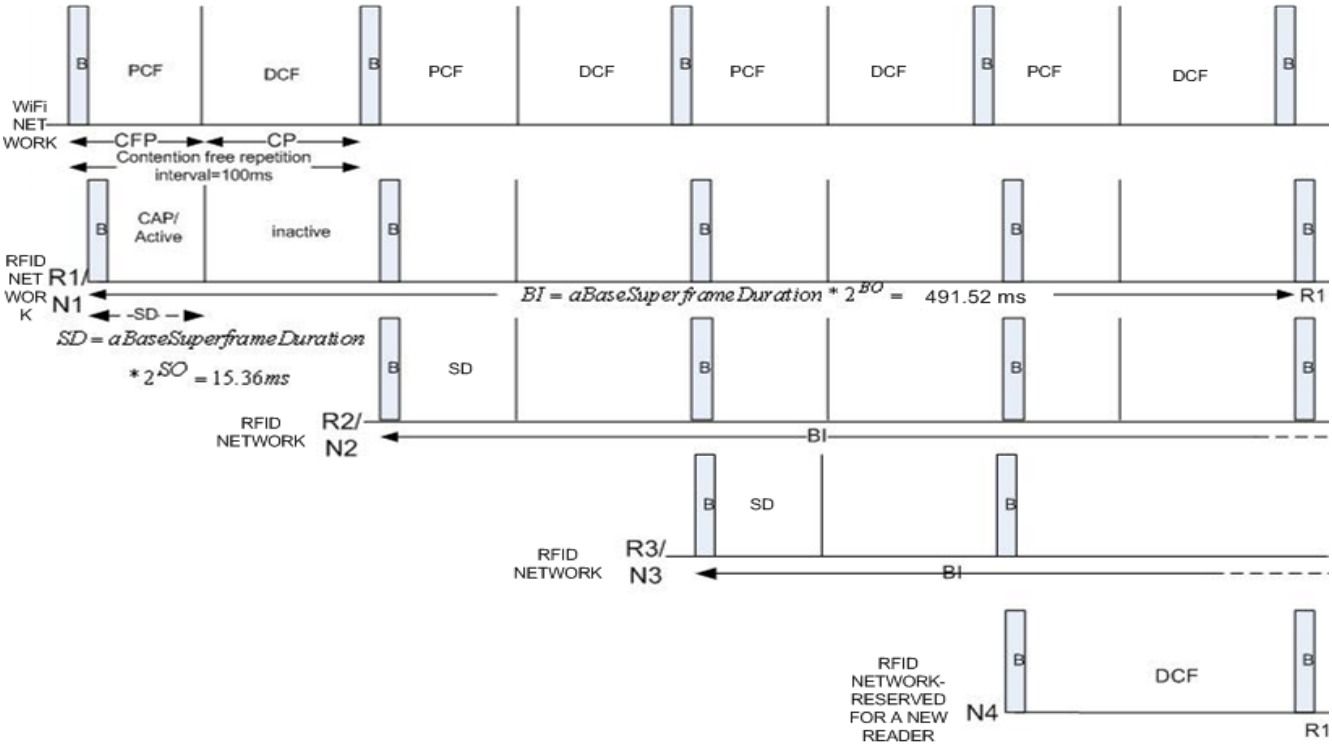


Figure 3.5: Timing structure of the proposed solution

The detailed description of a cycle is illustrate in Figure 3.6. In a typical cycle, CFP and CP alternates. At the beginning of CFP, AP sends a beacon and R_1 is polled and replies

with a Poll-ACK frame. Then R_1 sends a beacon frame to its vicinity to announce the presence of it. The active tags response by sending their IDs. Tags sleep according to their sleeping probability and after wakeup they wait for the specific beacon frame containing the information of active reader. At the end of CFP, R_1 sends CF-END frame to the AP. Then the control is transfer to the CP of DCF form AP where WLAN networks along with the R1 reader sends their data to AP. At the end of the first cycle, CFP period is announced again by the AP. Then, AP sends the beacon frame after waiting for duration of the point coordination function interframe space (PIFS). This process continues synchronously. During the first cycle, when R_1 works other RFID networks ($R2$, and $R3$) set their NAV value according to the PCF period.

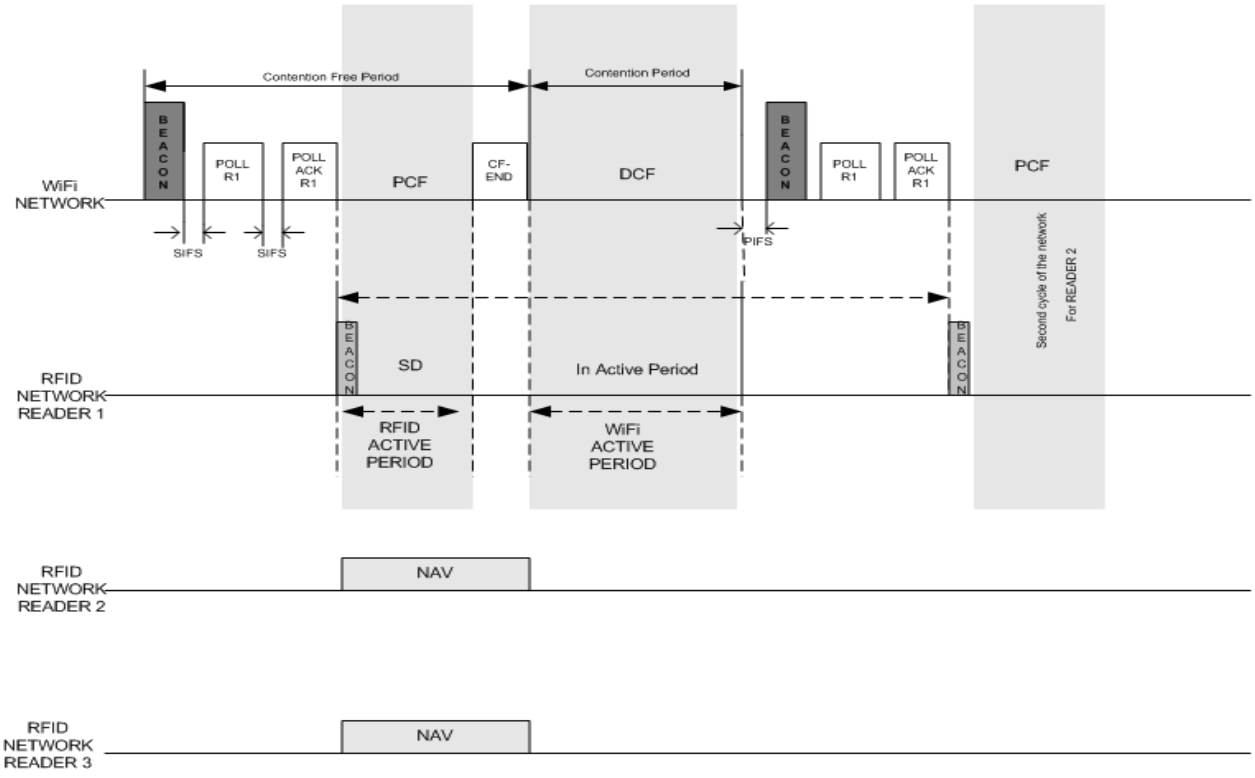


Figure 3.6: Timing structure of one full cycle

3.4 Challenges

It is very important and challenging to identify the values of parameters that provide the best overall performance of the networks. The DCF protocol causes many troubles in WLANs. RF interference is probably the most vulnerable problem. If a source of RF interference (e.g., cordless phone or other WLAN stations) is present, data transmissions are blocked by DCF as long as the interfering signal is present. The stations sense enough energy on the medium and wait patiently, in most cases for just a few seconds or minutes. This also causes the throughput of the network to drop significantly. We consider the following limitations and try to find appropriate values for the following parameters in order to design an efficient approach in this regard.

Tag Range: The most important parameter for evaluating the performance of an RFID system is tag range. It is defined as the the maximum distance at which a RFID reader can either read or write information at a tag. We consider active tags with the tag range up to 11 meters that work in the 2.45 GHz microwave sub-band.

Collision: The collision problems occur when multiple tags send the packet at the same time. To avoid the problem, tags go to sleep mode based on the value of its sleeping probability value after sending one successful packet. We need to calculate the average sleeping time properly. If the wakeup time is set as random the possibility for a number of tags wakeup at the same time is less. The possibility of using multiple readers in the same physical space gives rise to the problem [2] that two readers may simultaneously try to read tags. If the readers are in close vicinity they may interfere with each other directly. The transmitted RF power from one reader may result the tag to response to another reader in the vicinity (reader-tag collision) if they are on the same channel. Even when two readers

on different channels, if there are tags within the coverage of these two readers, tags might not be able to respond to either reader‘s query reliably upon receiving signal from both readers (reader-reader collision). This problem can be sloved by using different frequency for the interfering reads. However, frequency coordination problem arises when number of frequency is limited. In the proposed approach, one reader works in one active period since the IEEE 802.11 PCF medium access mechanism works by polling one node at a time. All other nodes are selected in round robin fashion. Thus, the probability of reader-reader collision is less.

Tag Density: To find the actual number of tags that send data packets in one active period is a great challenge. We assume that the data size is 4 slots and active period is 48 slots. Thus, 12 tags can send data packet to readers.

Contention Free Period (CFP) and Contention Period (CP): We need to find the actual duration of PCF period (i.e., CFP) and DCF period (i.e., CP).Superframe duration (SD) and beason interval (BI) are chosen by two important parameter values *BO* and *SO*. If PCF (CFP) or DCF (CP) periods are too short then tags will have not much time to send their IDs or stations and readers will have not enough time to send their data packets that results a saturation.

TimeSlot: The duration of a timeslot that is used in the IEEE 802.11 is 20 microseconds and in the IEEE 802.15.4 is 320 microseconds (16 time larger than 802.11). Thus, we need to adjust the timeslots duration for two networks properly.

The deployment of such RFID/WLAN solutions in practice would thus contribute to even more wider applications of RFID, including areas where RFID is currently not used due to the coexistence problems mentioned above. We try to share the access of medium

among the RFID and WLAN networks in a fair way to solve the coexistence problem. There can be more issues arise during the design and deployment. Hence, we need to assign the appropriate values and features to them.

3.5 Simulation Parameters and their Values

The parameter values that we use in the simulation are calculated using the specification of the IEEE 802.11 and IEEE 802.15.4 standards. In this section, we define the parameters, and calculate their values. Tables 3.2 and 3.3 present most of the parameters we use in the simulation.

aCFPMaxduration

aCFPMaxDuration is defined as the maximum duration of the CFP period of PCF. The limit of this value allows the coexistence between contention and contention free traffic. Once this time is reached, PCF access method ends and DCF period starts. If the end of the CFP period is not announced by PCF but it reaches to *aCFPMaxduration* the AP terminates the CFP period and transfers control to the DCF period.

We calculate *aCFPMaxduration* in microsecods according to the following formula.

$CFPMaxDuration = (BeaconPeriod * DTIMPeriod * CFPRate) - (MaxMPDUTime + 2 * SIFSTime + 2 * SlotTime + 8 * ACKSize)$

Where,

$MaxMPDUTime = TimeToTxMaxSizedMACFrame + TimeToTx * (Preamble + header + trailer + expansionBits)$

The minimum value of $CFPMaxDuration$ is $MinCFPMaxDuration$ that provides sufficient time for the AP to send one data frame to a station, polling that station and allow the

polled station to respond with one data frame.

$$MinCFPMaxDuration = 2*MaxMPDUTime + TimeForBeaconFrame + TimeForCFEndFrame.$$

$$MinimumDataTransferTime =$$

$$TimeToTxOneDataFrameToST + TimeForSTAToRespondWithOneDataFrame$$

The maximum duration of CFP is defined by the beacon interval. The default value of beacon interval is 100 milliseconds.

Sometimes PC may terminate any CFP before the *aCFPMaxduration* period based on the available traffic and size of the polling list. Beacon frames must wait if the medium is busy. In this case, they need to wait in CP untill the DCF frame transfer ends. This results the late arrival of beacon frames.

Target Beacon Transmission Time (TBTT)

If it is the time for CFP but the frames of CP are in still transmission then the CP frames should finish their transmission that shortens the CFP time. Thus, CFP time starts whenever CP frames finish. Thus, TBTT is defined as the maximum time between foreshortened and actual CFP time.

Superframe Duration (SD) and Beacon Interval (BI)

A slot time in Wi-Fi scale is equal to 20μs whereas, a slot time in RFID scale is 320μ, that is 320/20 = 16 times larger than that of the Wi-Fi scale. A superframe of IEEE 802.15.4 or Zigbee consists of active and inactive periods which are 48 slots in total. SD of RFID scale contains 16 timeslots, each having the same length. A timeslot is divided into $aBaseSlotDuration * 2^{SO}$ symbols, where *aBaseSlotDuration* denotes the minimum number of symbols in a slot (e.g., *aBaseSlotDuration* has 60 symbols if *SO* is equal to 0). The value of *aBaseSuperframeDuration* is fixed to 960 symbols (i.e.,

$aBaseSlotDuration * 16 = 960$ symbols). The symbol time is 16μs in the 2.4GHz ISM band of the IEEE 802.15.4 standard. The BI and SD are defined by the BO and SO, respectively. The range of the BO is between 0 and 14, and the range of the SO is between 0 and BO. The nodes can only communicate with the coordinator during an active period of RFID netwrok, while the coordinator and nodes may enter the idle state during an inactive period. If we consider $SO = 0$ then

$$ActivePeriod/SD = aBaseSuperframeDuration * 2^{SO} \tag{3.1}$$

= (960 * 16) * $2^0\mu$s [when SO = 0]

= 15360 μs

= 15.36 ms

The size of RFID superframe is 4 times larger than the Wi-Fi superframe. However, a typical cycle of the RFID superframe is equal to the superframe size of Wi-Fi network. Beacon Interval (BI) of Wi-Fi superframe is 100TU. Hence,

$$BI = 2^{BO} * SD \tag{3.2}$$

$\approx 4 * 100TU$

$and, BO \approx 4.7$

Other way, we can calculate,

$BI = 32 * 48 * 16 * 20\mu s = 480TU$ $(1TU = 1024\mu s)$

Here,

RFID scaling is 16 times larger than the Wi-Fi scaling ($aSlot = 20\mu s$), superframe size in

slot = 48

480TU is close to the default value of 400TU. If we assume the the BO value is equal to 5, BI value of RFID is expressed as

$$BI = aBaseSuperframeDuration * 2^{BO} \tag{3.3}$$

= (960 * 16) *$2^5 \mu$s [when BO = 5]

= 491.52 ms

This is the super frame size of RFID side and superframe size of WiFI is = 8*48 *16 *WiFitimeslot= 6144WiFi timeslot.We need to fit this active period in IEEE 802.11 PCF, CFP period and then inactive period in DCF, CP period.

Data Packet Size

According to the IEEE 802.15.4f standard working group‘s parameter suggestions, the size of active tag ID including MAC header is $((38 * 8/250kbps)/0.032timeslot) = 384bytes$, i.e., $\approx 4RFIDtimeslot$. On the other hand, the data size of Wi-Fi normal nodes that includes MAC and Physical header is 117 $WiFitimeslot$. In the Wi-Fi mode, the data size of RFID readers is very small. The IEEE 802.11 standard does not allow to transmit data of size less than 100 bytes. Again, the tag ID without MAC header is approximately 2 slots. If we allow the sytems to wait for 10 tag IDs of size 20 slots then it will be $20 * 5 = 100$ bytes in in the Wi-Fi scale. Thus, in the proposed approach, we aggregate tag IDs upto 100 bytes to transmit as a single frame. Reader data size with 802.11 MAC and PHY header is 37 $WiFitimeslot$.

Sleeping Probability of Tags

Table 3.1: Calculation of Sleeping values for RFID networks

Average Sleeping time in minutes	Average Sleeping time in Time Slots	Corresponding Sleeping Probability (P_{sleep})
1 minute	187500 slots	.999994667
5 minutes	937500 slots	.999998933
7 minutes	1312500 slots	.999999238
10 minutes	1875000 slots	.999999466
15 minutes	2812500 slots	.999999644

Tags go to sleep mode to save energy (e.g., battery power) after the CFP period of PCF and remain in sleep mode according to the value of sleeping probability, which is calculated by using the formula, $\bar{V} = 1/1 - P_{sleep}$

$$\bar{V} = 36000/.00032 = 1/1 - P_{sleep} or, P_{sleep} = .999999911 \tag{3.4}$$

In the proposed simulation model, the tag goes to sleep mode after sending one packet with the P_{sleep} is equat to (0.999999911). Most of the time tags are in sleep state and check beacon message after they wakeup. If the beacon is not available tags go to sleep mode again. The value of average sleep time value is equal to $1/P_{sleep}$.

Table 3.1 illustrates the average sleeping time in minutes and in RFID slots and also their corresponding sleeping probability values.

The parameters and their corresponding values that we use in the simulation simulator are listed in Tables 3.2 and 3.3.

Table 3.2: WLAN Parameters

Parameters	Value
RTS	14 Slots
CTS	13 Slots
ACK	13 Slots
DIFS	2.5 Slots
SIFS	0.5 Slots
PIFS	1.5 Slots
POLL	14 Slots
POLL-ACK	14 Slots
CF-END	14 Slots
DATA WiFi nornal station	500 Bytes or 100 slots
DATA reader/station	100 Bytes or 20 slots
Retry Count	7
Maximum Frame Response Time	161 Slots
Beacon	10 (Slots)
Contention Window value of normal nodes	CWminAC[0] = 32,CWmax[0]=124
Contention Window value of reader/station	CWminAC[3]=7, CWmaxAC[3]=15
AIFSN[0]	7
AIFSN[3]	2
Transmission opportunity value(TXOP)	0
Maximum No. of Normal Stations	40
Maximum No. of reader/stations	3
Maximum Slot Time	20 microseconds
Data transmission rate	2Mbps
WiFi superframe size	122.28ms or 6144 WiFitimeSlots
Beacon Interval (BI)	100 TU
aSlot	5 Bytes

Table 3.3: RFID Networks Parameters

Parameters	**Value**
DATA/ID RFID tag	4 RFID time slots or 38 bytes
ACK	2 Slots
Beacon	2Slots
Data Transmission Rate	250 Kbps
Superframe duration (SD)	15.36(ms)
RFID super frame or BI	491.52ms 0r 1536 RFIDtimeSlots
SO	0
BO	5
TAG	450
Contention window	2
Retry Count	3
Maximum Slot Time	320 microSeconds
P_{sleep}	0.999999911
aSlot	10 Bytes

Chapter 4

Simulator Design

4.1 Simulator Model

Simulator is a way of validation and performance evaluation of a model. We use the Artifex simulation tool to validate our proposed scheme and measure the performance. Artifex is built using object oriented Petri net simulation engine [11] that provides graphical user interface to build a simulator model using different combination of objects, elements and classes. In Artifex, the common elements are places, transitions and links as shown in Figure 4.2. The rectangles, circles and arrows represent transitions, places and links, respectively. Places hold tokens and are connected with one or more transitions. In transitions, action codes are written, which are actually the processing unit of the model. Tokens are transmitted from a transition to another according to the user controlled code of transition actions. Links are connectors that connect places with transitions.

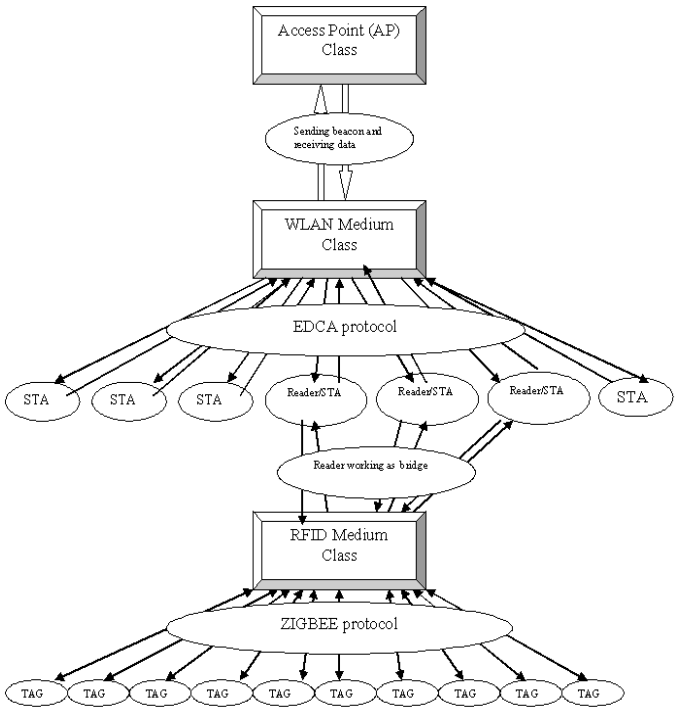


Figure 4.1: Graphical representation of our simulator

Places hold information in the form of tokens. Tokens are structured data. Objects are connected to each other through interfaces, which are a set of input and output places. To transfer information, the input place of one object is connected to the output place of another object. Using Artifex, a complex simulator can be designed by splitting a page into multiple pages and connecting them through the interface. Artifex is suitable for discrete event systems and user can build a non-ambiguous model of a system. Figure 4.1 illustrates the graphical representation of simulator design of the proposed scheme.

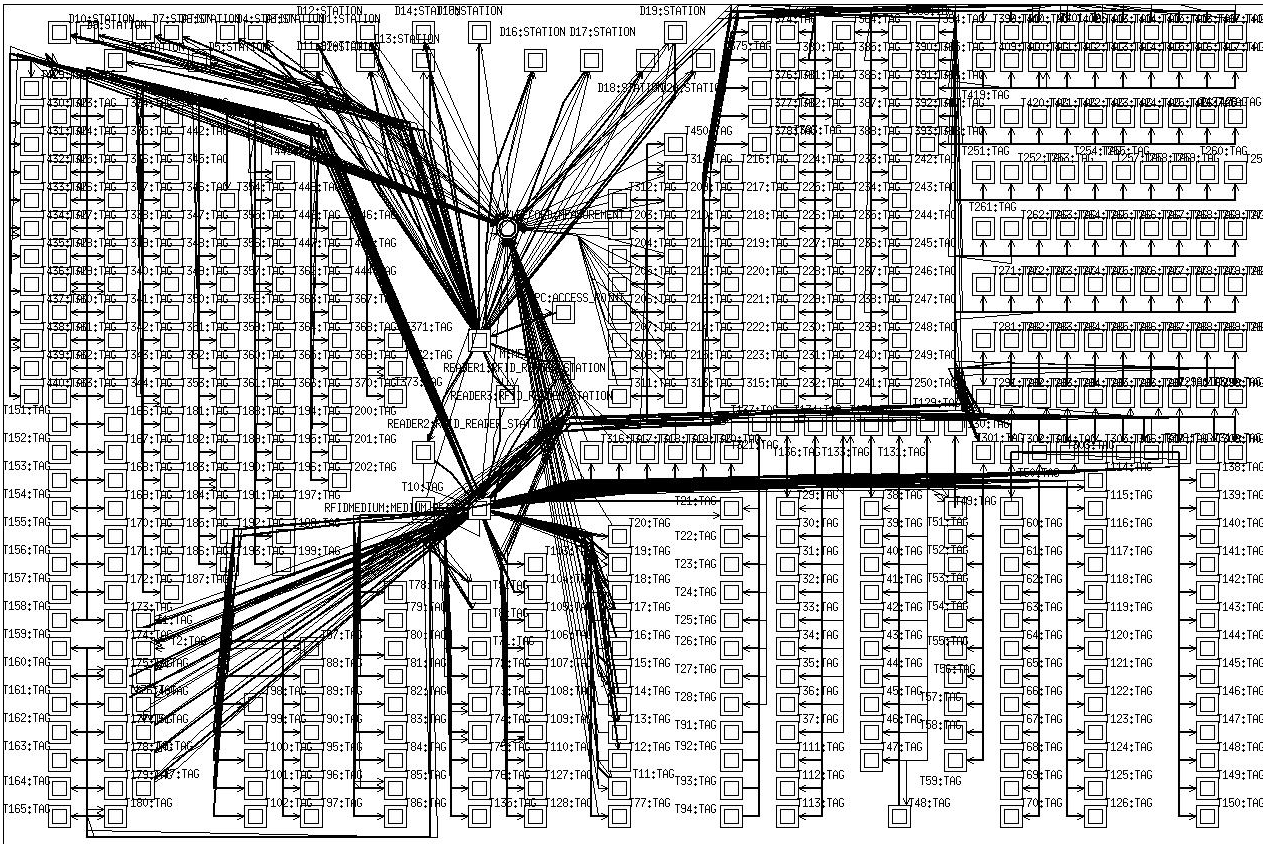


Figure 4.2: Top level page of the simulator

4.1.1 The Top Level

The top level page of the proposed simulator integrates RFID with the WLAN networks (Figure 4.2. In IEEE 802.11 WLAN networks, 40 stations (D1, D2 and so on) are connected with the medium to send uplink data to access point (AP). Stations, wifi_medium and APs are connected to each other through interfaces and also to the RECORD. When an event occurs, data go to the MEASUREMENT page through RECORD input place(Figure 4.3) to measure the value of different performance metrics. In the RFID side, tags(T1,T2 and so on) are connected with rfidmedium to send their ids to the defined readers (R1 or

R2 or R3). Readers are also connected with wifimedium and AP to send the tags ids to AP in WLAN mode. Two networks are integrated with each other through reader. In the WLAN mode, these readers work as special stations along with other normal stations. In the proposed model, we only consider uplink communications, where data are only sent from stations/readers to AP.

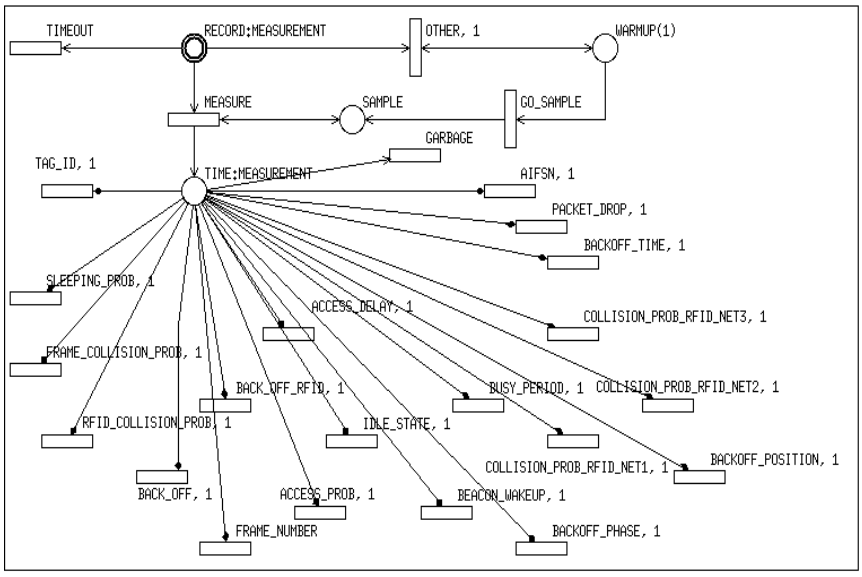


Figure 4.3: Measurement page of Top level

4.1.2 Access Point

The Access Point (AP) consists of three pages: MAIN_PAGE, CSMA_CA_ALGORITHM, and DOWNLINK_QUEUE page. AP contains two input places (i) RECEIVE_DATA:PACKET, and (ii) GET:BACKOFF and two output places (i) SEND_OUT:PACKET, and (ii) SEND:BEACON. Figures 4.4 illustrate AP class. The PACKET, and BACKOFF are two different data types or tokens that are sent to and received from the MEDIUM class. An AP receives uplink data and stores them in the DOWNLINK_QUEUES class. For each station in the

DOWNLINK_QUEUE page, there are buffers to store data. These data are sent later to the application server. In the proposed simulation model, a single AP covers both the RFID and WLAN networks. In the contention free period (CFP) of point coordination function (PCF), an AP can poll one reader at one time. AP sends beacon frames and then sends Poll frames to the appropriate reader (R_1 or R_2 or R_3). After polling the readers send Poll ACK frame to the AP. The reader sends the beacon frame to notify the neighboring tags about its availability. Tags send their IDs to the AP through the reader. AP sends beacon to the stations and receives CTS and data. After receiving RTS from a station AP waits for the SIFS period of time (0.5 slots) and generates CTS frame and sends to that station. When a station receive CTS it sends data to AP through medium. AP sends beacon frames after beacon interval of 100 Time Unit (TU), which is the total superframe time of PCF and DCF. To convert time unit, Artifex uses real and virtual time. In our simulation model, we consider the virtual time. In the first cycle of the simulator, the first beacon is sent and reader R_1 is polled. Readers R_2 and R_3 are polled in the 2nd and 3rd cycle. Since we have only three RFID networks, only WLAN networks work in the fourth cycle. The same process repeats afterwards.

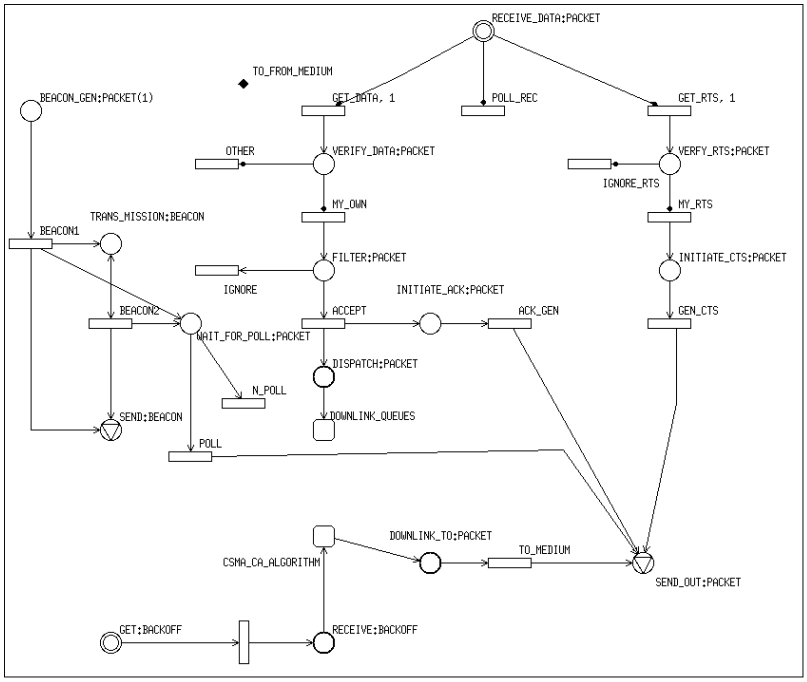


Figure 4.4: Main Page of Access Point (AP)

4.1.3 WLAN Medium Class

Medium receives PACKET, and BEACON from the stations and sends BACKOFF and DATA to AP. Medium receives frames from stations and AP through the input places, RECEIVE:PACKET and LISTEN:BEACON . It sends the frames to stations and AP through the SEND_TO_DEVICE, SEND_TO_AP and SEND_DCF:BACKOFF output places. MEDIUM synchronizes the time period of RFID and WLAN. After receiving the BEACON frame from AP, the medium starts a clock that indicates the start of the RFID networks. Receiving the CF_END frame from the RFID_MEDIUM indicates the end of the RFID duration.

After receiving the CF_END (i.e., finish of *CFPmaximum* duration) the DCF period starts, as shown in the transition GO_TO_DCF_PERIOD of Figure 4.5. At each timeslot the clock sends a token to the stations in the form of BACKOFF token (SEND_DCF:BACKOFF output place). Collision occurs if more than one token arrives in the MEDIUM. However, collision is only considered for RTS frames. The medium is considered to be busy when any transmission is sensed in the MAC layer. If non collided RTS can pass through the medium, the medium is kept busy until the end of current transmission. This status is defined in the RTS frame as a Network Allocation Vector(NAV). Other nodes set their NAV value accordingly and cannot access the medium during this time. Medium becomes IDLE again when ACK is received by the stations for the current transmission. In case of collision, the medium is kept busy for the duration of $packet_{size} + t_{ack} + ACK_{size}$ before passing the packets to the place, DESTROY:PACKET. Once the packet is destroyed the medium becomes free again.

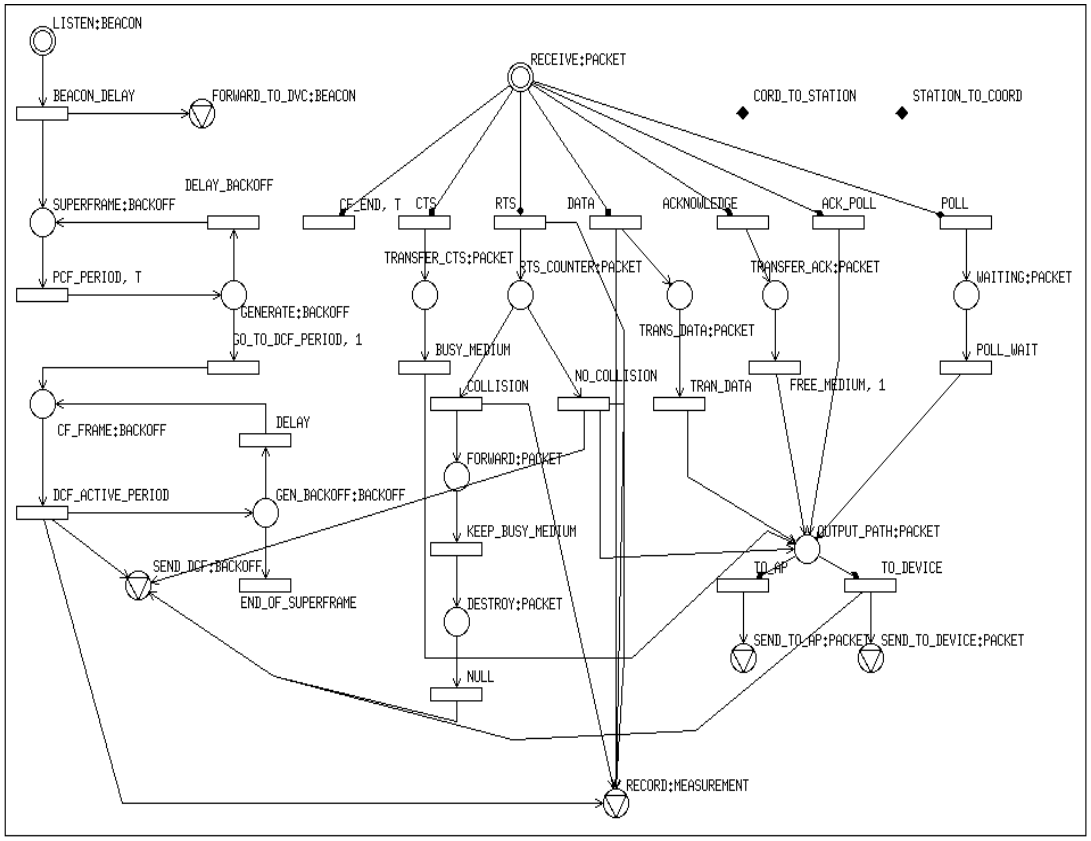


Figure 4.5: MEDIUM class of WiFi networks

4.1.4 Station Class

Station class contains three pages: MAIN_PAGE, CSMA_CA_ALGORITHM, and SOURCE_POISSON page. The SOURCE_POISSON page is responsible for generating the packets according to Poisson Distribution method. The inter arrival time between two packet (WAIT transition) is maintained by an exponential distribution. Firstly, the participating station‘s ID is checked through the transition CHECK_DEVICE that is illustrated in Figure 4.6. The SOURCE_POSSION page maintains a finite buffer size of 1023 bytes. If the buffer becomes full but more packets are still arriving the extra packets are passed to the DISCARD

transition.

The CSMA_CA algorithm is implemented in the CSMA_CA_ALGORITHM page. If there is a ready packet to transmit in the SOURCE_POISSON page then the station initializes the value of AIFS and contention window (CW) according to the access category (AC) of the stations. We consider the highest AC for reader/station and the lowest AC for normal Wi-Fi stations. After sensing the medium for AIFS period a random number is generated. The BACKOFF value is sensed through the SENSE_DCF:BACKOFF place and the random number is decremented by one in every free medium backoff slot. The predicate of the transition READY_TO checks if there is any packet in the queue. If the random number becomes zero and there are ready packets in the queue then the packets are directly transmitted to the medium after zeroth backoff through UPLINK_TO place connected to the MAIN_PAGE. If there is no packet in the queue, i.e., the predicate of transition AC2 becomes true, (as illustrated in Figure 4.8) then the packet needs to wait until the another packet is ready to send. Before sending the packet the station keeps a copy of the packet in case of failure due to collision. Collision is detected by the lack of receiving CTS within $(RTS + CTS + DATA + ACK + 3 * SIFS)$ slots. The packet can be retransmitted 7 times. After this number of attempts that packet is dropped and information is sent to the MEASUREMENT page through the RECORD:MEASUREMENT output place.

The MAIN_PAGE receives PACKET and BACKOFF through the WELCOME:PACKET and RECEIVE_DCF:BACKOFF input places and sends packet to the medium and MEASUREMENT page through the SEND_OUT:PACKET and RECORD:MEASUREMENT output places as is shown in Figure 4.7. Ready to transmit packets (RTS and data) are sent through the SEND_OUT:PACKET output place, and CTS and ACK are received through

the WELCOME:PACKET input place. Upon the successful transmission of the current packet, that is confirmed by the receiving of ACK packet, the process continues (PROCESS_NEXT) if packets still exist in the queue. In the proposed simulation model, readers also work as special stations following the same working mechanism mentioned above.

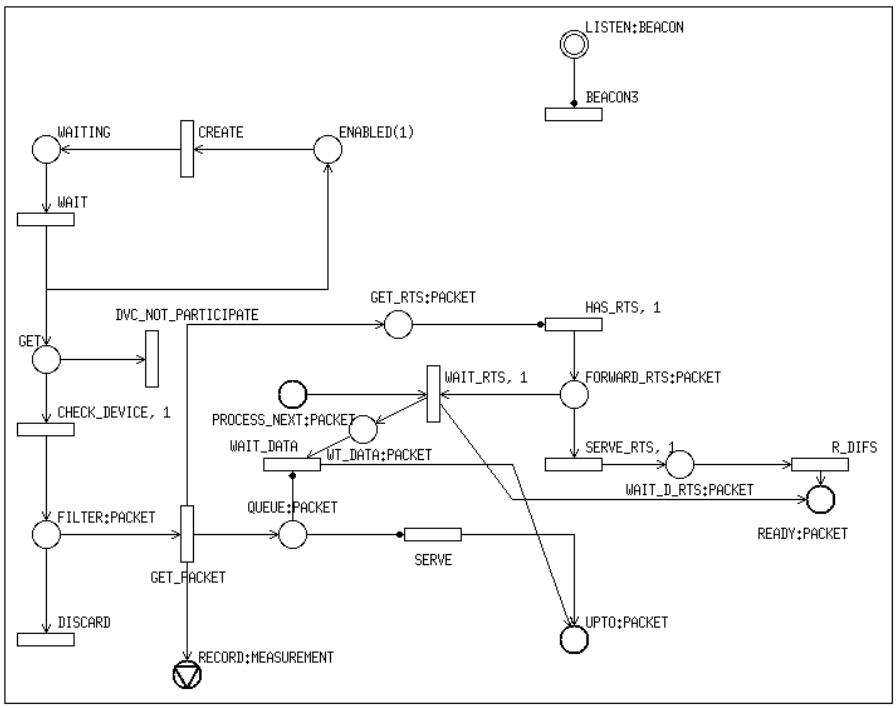


Figure 4.6: packet generating page of WiFi Station Class

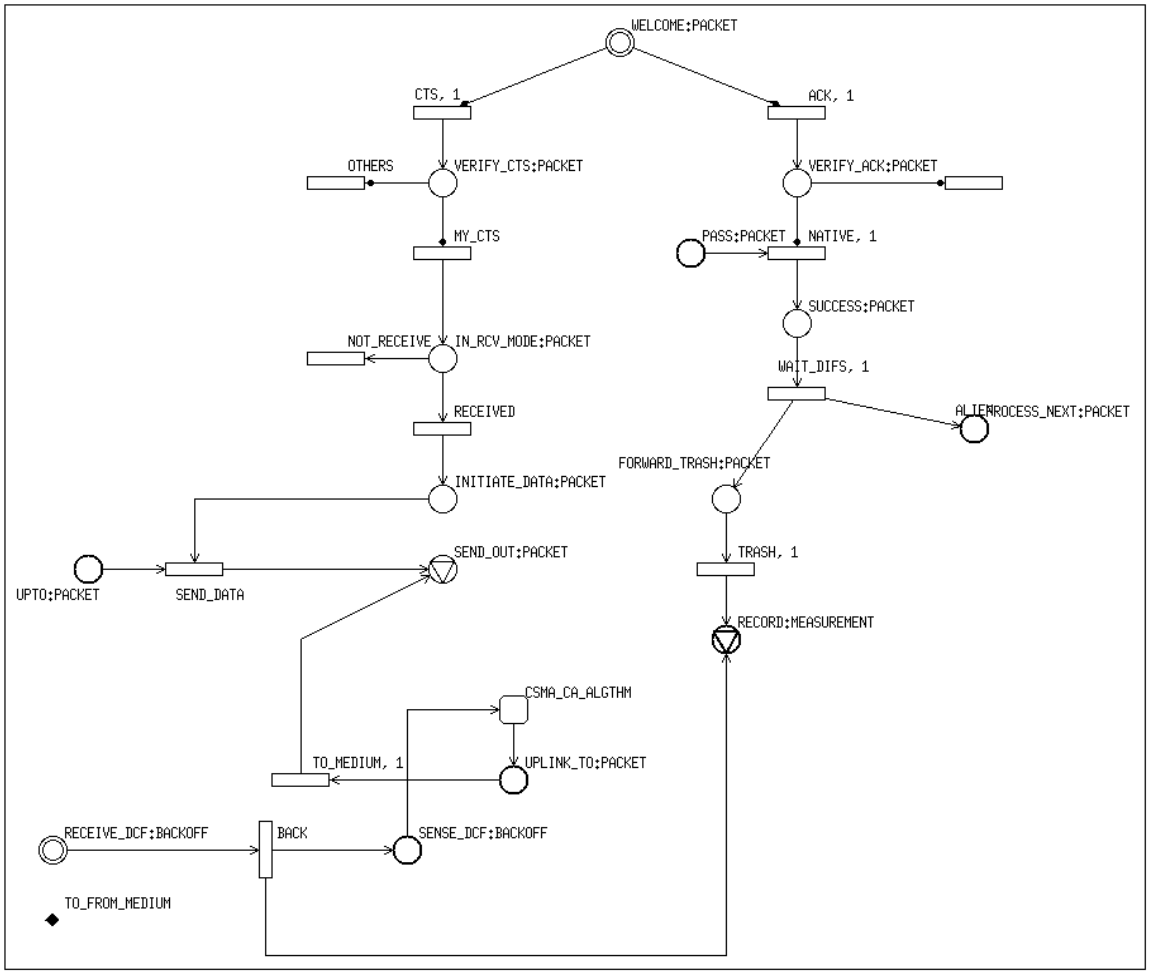


Figure 4.7: main page of Station Class

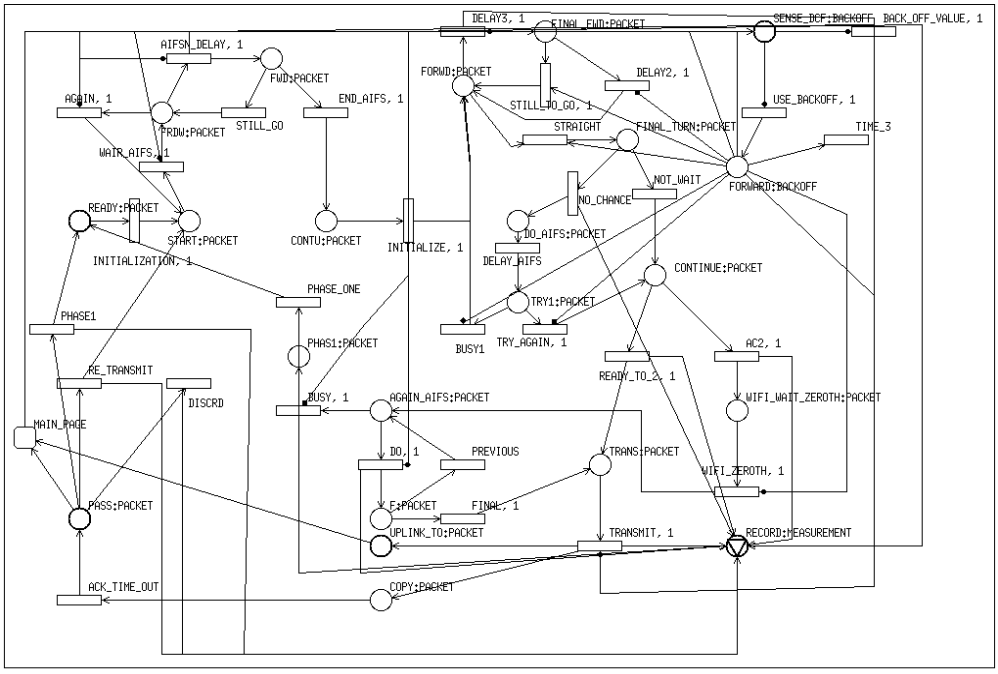


Figure 4.8: CSMA-CA Page of Station Class

4.1.5 Tag

In the RFID level, we consider three RFID networks. Each RFID network consists of maximum 200 tags and one reader. At a time one reader and tags in the vicinity of the reader can send their IDs to the AP. Once the reader is polled by an AP, the reader sends a beacon control request frame to its neighboring tags through the LISTEN:BEACON input place. As the response of this request tags send their IDs through the SEND_OUT_RF:PACKET output place. The tag class contains three pages: MAIN_PAGE, CSMA_CA_ALGORITHM, and SOURCE_POISSON page. The SOURCE_POISSON page works similar to the SOURCE_POISSON page of station class. The only difference is that tags receive the active reader information through the LISTEN:R_BEACON input place and the availability of the tags are checked

accordingly.

The IEEE 802.15.4 CSMA/CA protocol is used as a medium access mechanism to send the IDs to the medium. Figure 4.10 shows the CSMA_CA page of the networks. Whenever the tags wakeup from the sleep mode they receive the information regarding the availability of active readers through BEACON (MAIN_PAGE). Then, the tag initializes (INITIALIZE) the value of three parameters: Retry Count(NB), CW, and backoff exponent(BE) and generates a random number. The random number is decremented by one after receiving the backoff through the place FORWARD:BACKOFF. In this standard, transmission occurs at the beginning of the boundary. Once the random number reaches to zero this algorithm checks if the current superframe has enough time (or active period) to transmit the frame through the (WAIT_ACTIVE_PERIOD) transition and receive its subsequent ACK. If not, the token or data packet needs to wait in the WAIT_INACTIVE_PERIOD transition for the next superframe. After completing two Clear Channel Assessment (CCA) if the medium is still IDLE data packet is passed to the MAIN_PAGE to send to RFID_MEDIUM. Before sending the packet the CSMA/CA protocol used in this page keeps a copy of the token to be retransmitted in case of collision. On the presence of the subsequent readers, tags send IDs to the reader and wait for the ACK that ensures the successful transmission.

The MAIN_PAGE receives acknowledgement (ACK) through the RECEIVE_ACK:PACKET input place. This page also has two output places: SEND_OUT_RF:PACKET, and RECORD:MEASUREMENT. Each tag sleeps (GO_TO_SLEEP) according to the sleeping probability (0.999999911). The sleeping time of two tags is randomized exponentially. Thus, the probability that two tags wake at the same time is very less. When tags wakeup from the sleep mode tokens are passed to the WAIT_FOR_BEACON transition (Figure 4.9) to check and wait for the

subsequent active reader. After that tokens are passed to the SOURCE_POISSON page. After the successful transmission of the packet (tag IDs) the tag goes to sleep mode again and the process continues. In the event of successful transmission of tag ID or when tag wake up data is passed to the measurement(RECORS:MEASUREMENT) page.

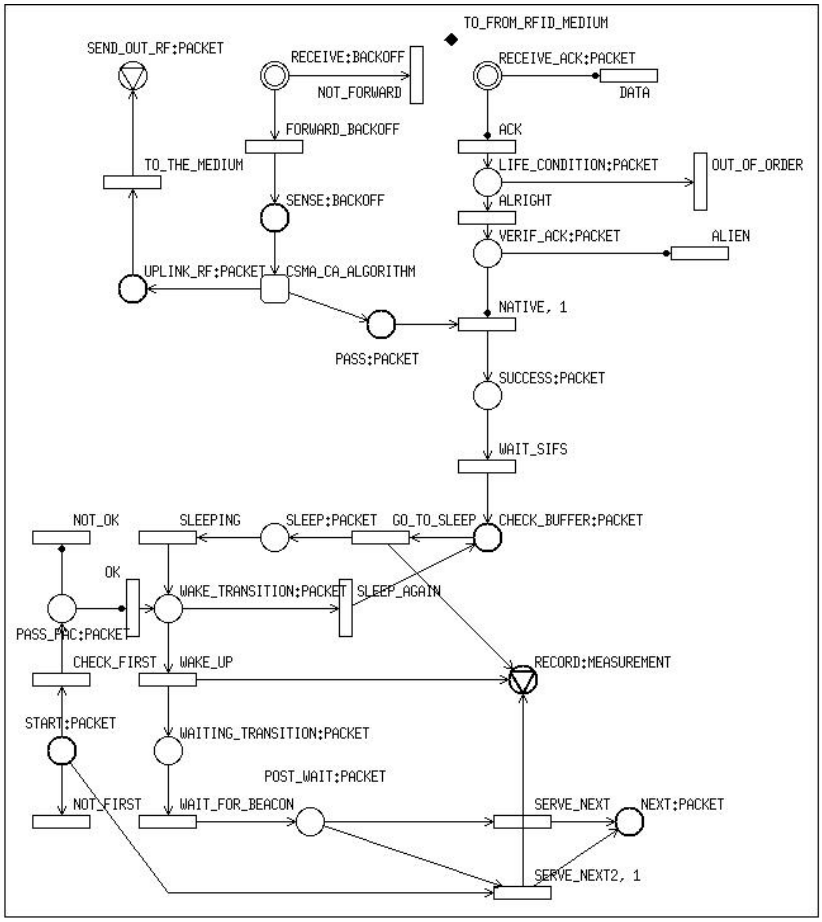


Figure 4.9: RFID Tag :Main page

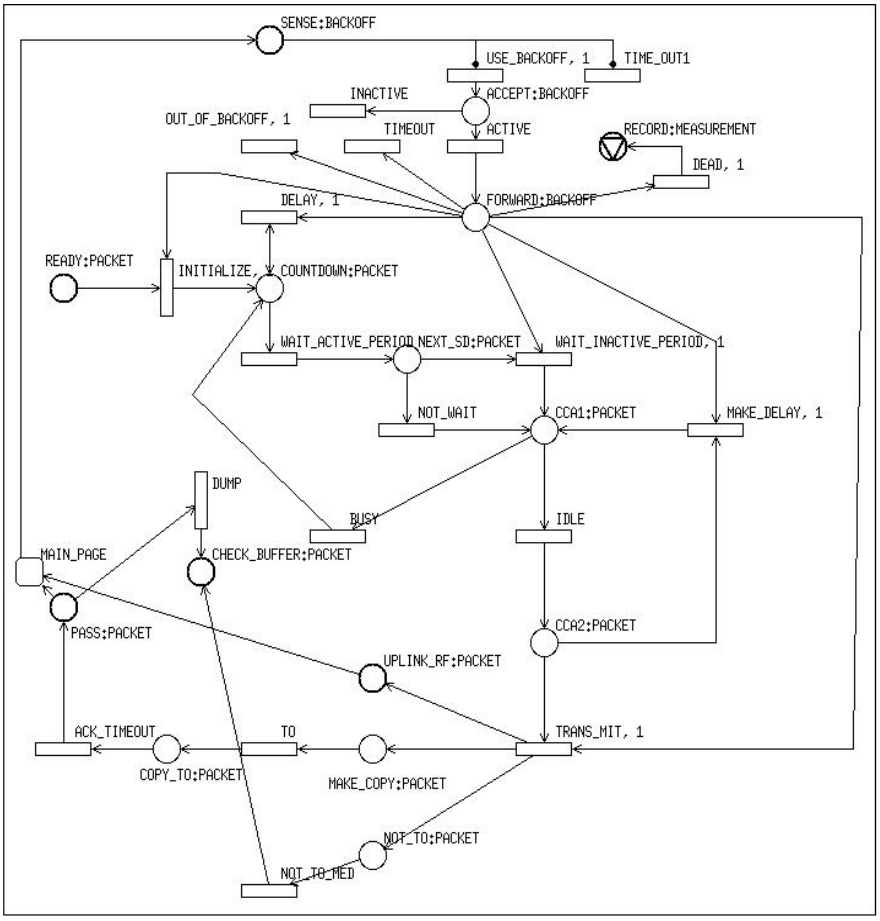


Figure 4.10: CSMA-CA page of TAG class

4.1.6 Medium_RFID

Medium page is responsible for generating backoff and transmitting packets (tag IDs) to the appropriate active reader. This page sends backoff to the tag class through the SEND:BACKOFF output place so that tags can check the medium status. After receiving BEACON through (REC_BEACON:BEACON) in each timeslot this page sends the medium status to the tag class.

The size of the active period (ACTIVE_PERIOD) of superframe is only 48 slots. After

this period, token is passed to the INACTIVE_PERIOD transition, which indicates the end of the superframe and a CF_END frame is transmitted to the WiFi-MEDIUM. Medium receives tag IDs through the RECEIVE:PACKET input place and sends the packets to the reader through (TRANSMIT:PACKET). When the medium receives a packet it becomes BUSY for other tags. Those tags also set their NAV value accordingly. If more one token arrive in the medium at the same time a collision is occurred. The collided tokens are passed to the COLLISION transition. Before destroying the token medium is kept busy for the duration of $(packet size + ACK + t_{ack})$. After that the medium declares itself as idle. Even if no collision occurs the medium is also kept busy for the duration of $(packet - size + ACK)$. The medium becomes idle again once it receives ACK for the current transmission (Figure 4.11).

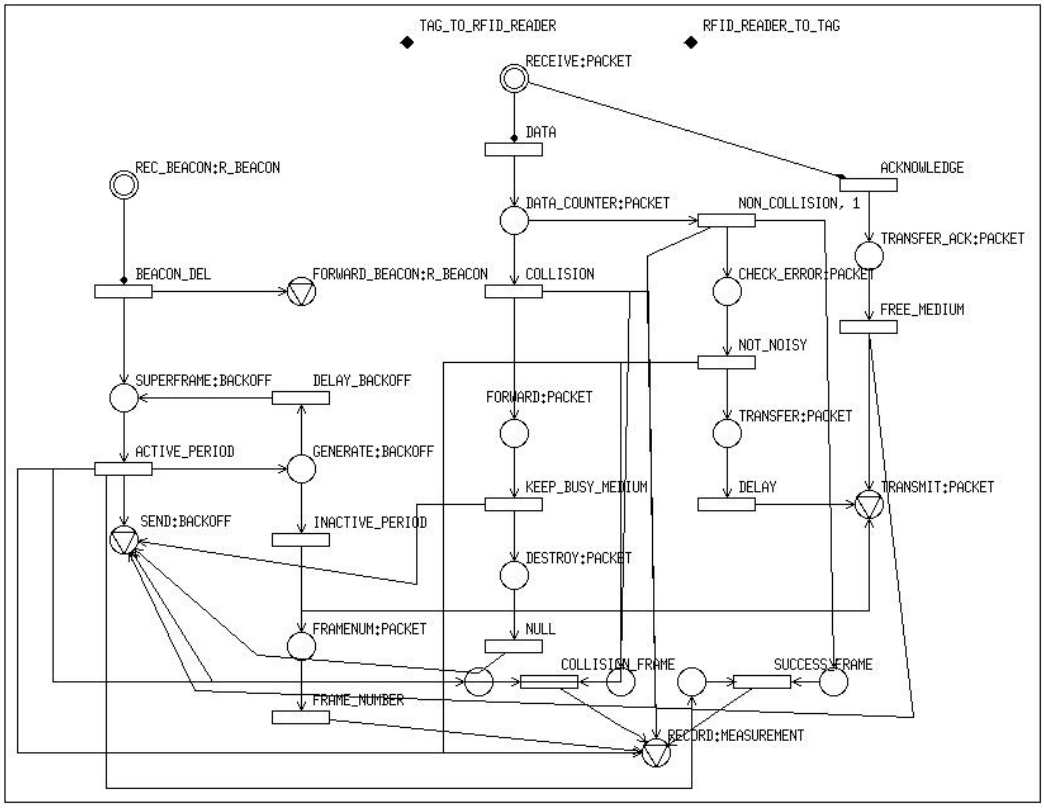


Figure 4.11: Medium class of RFID

4.1.7 RFID _ Reader _ Station

The RFID reader works as a bridge for both RFID and Wi-Fi WLAN networks. It works as a reader for the RFID network and a special station for the WLAN networks. The working mechanism of reader in the WLAN mode is same as the normal stations. It contains three pages: MAIN_PAGE, CSMA_CA_ALGORITHM, and SOURCE_POISSON page. When it works as a reader, firstly, it is polled by AP through the (MAIN_PAGE-WELCOME:PACKET) input placce. Then, it sends beacon frame to its subsequent networks through SEND_OUT_R:R_BEACON to notify its presence. It also sends POLL_ACK

frame through the SEND_OUT:PACKET output place to AP (Figure 4.12). As the response to this request, tags send their IDs to the reader using (REC_RFID_DATA) and store data into the buffer of SOURCE_POISSON page using GET_PACKET (Figure 4.13). This is done for the transmissions to AP later in the WLAN period. RFID readers work as the QoS stations for the IEEE 802.11e WLAN networks and send the collected tag IDs to AP. The working mechanism of CSMA_CA page and MAIN_PAGE is same as the CSMA_CA_ALGORITHM page and MAIN_PAGE of station class. Thus, they send RTS, wait to receive CTS, send the stored tag ids, and again wait for the ACK.

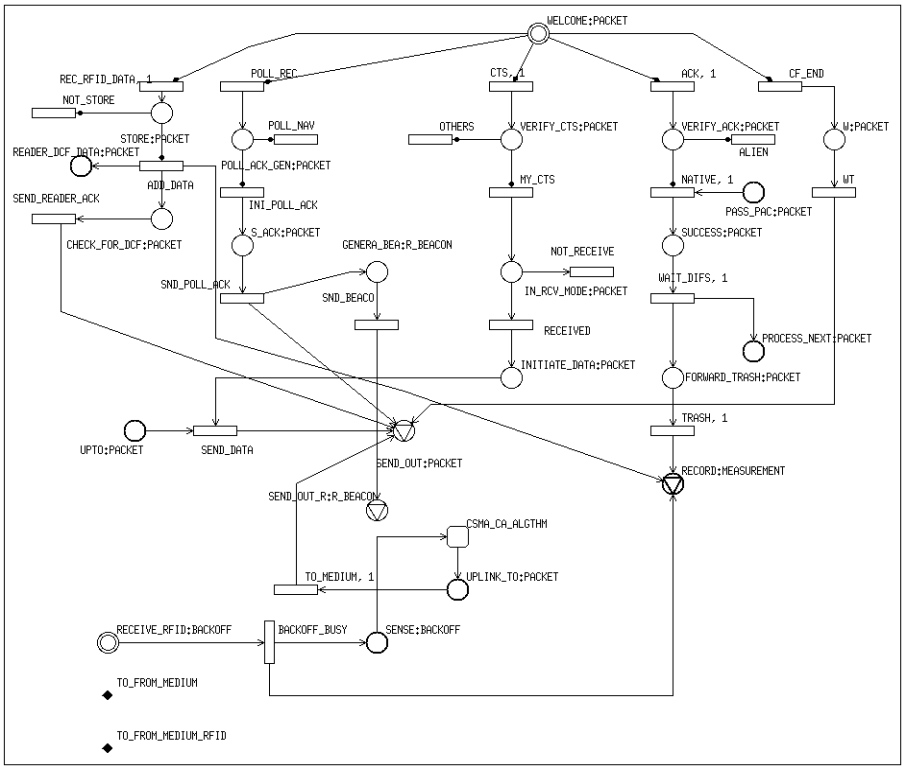


Figure 4.12: RFID Reader station class :Main page

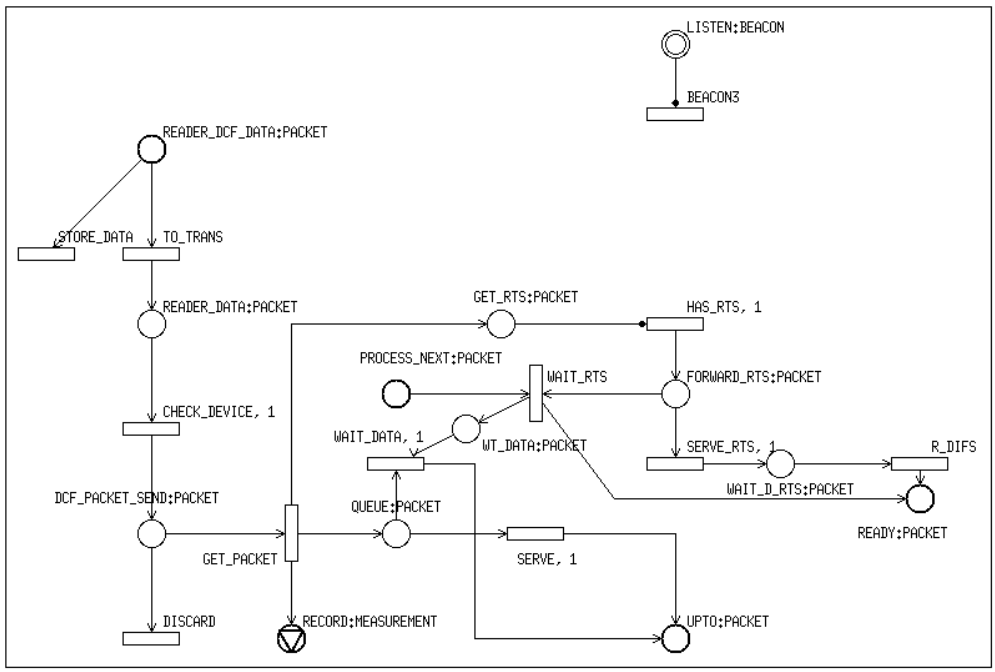


Figure 4.13: RFID Reader packet generating page

Chapter 5

Performance Evaluation

A simulation model is designed for the proposed approach that solves the coexistence and integration problems of IEEE 802.11 Wireless LAN (WLAN) with Radio Frequency Identification (RFID) technologies. This approach locates and identifies the RFID tags in the physical spaces with the co-located Wi-Fi WLAN using IEEE 802.11 Wi-Fi compatible existing hardware. In this chapter, we present the simulation results and performance evaluation.

5.1 Performance Evaluation of RFID

5.1.1 Design Consideration

In the simulation model for RFID network, we assume that an infrastructure network is operating in the saturation mode for single hop communication using IEEE 802.15.4 or Zigbee standard. We assume that three RFID networks exist in this model, each having one reader and 200 active tags working in the frequency band of 2.4 GHz microwave sub-

band or ISM band with transmission rate of 250 kbps. We consider that each tag always has a packet to transmit when wake-up from the sleeping mode. Each tag sleeps most of the time since it has a sleeping probability (0.999999911). As a result, their wakeup time is randomized exponentially and the probability that more than one tags wakeup at the same time is very less. This way CSMA-CA protocol works better and reduces collision. After a successful transmission tags go to the sleep mode again and search for the active reader when they wakeup. If the active reader is not available tags wait until the beacon frame arrives that contains information about the active reader. Each RFID network has one reader and 200 active tags. Each RFID network works in such a way that no reader collects information of the tags of anothe networks or no tag responses with the requrest of other networks reader. In this model, we only consider the uplink queue that allows the transfer of packets from tags to access point (AP) but not the vice versa. We consider the transmission time and delay in number of slots, where a slot time is 320 microseconds for RFID network. The length of a tag ID is 4 RFID slots that includes the MAC header. The size of beacon and acknowledgement(ACK) frame is 2 RFID slots.The size of the active period of the superframe is 48 slots and SO,BO value is chosen as 0 and 5.Tags compete to win the medium following the IEEE 802.15.4 slotted CSMA/CA medium access mechanism.

5.1.2 Simulation Results

We measure the performance in terms of frame collision probability, average number of collision in each superframe, average waiting time of tags after wake up, average number of awaken tags in each superframe, average collision position in each superframe, and average successful transmission position in each superframe. Results are generated as 2-D

plots using Maple mathematical software.

We measure the performance for two scenarios.

1. By changing the average sleeping time (1,5,7,10,and 15 minutes) for a fixed number of tags (80 tags in each network)

2. By changing the number of tags (20,40,60,100, and 150) for a fixed average sleeping time (1 minute)

Now, we define the operational metrics that are used to measure the performance of the proposed approach.

Frame Collision Probability

The probability of unsuccessful packets in the network is called collision probability. Collision probability is calculated as the ratio of the the total number of collided tags to the total number of tags that are transmitted.

Average number of Collisions in each superframe

The ratio of calculating total unsuccessful frames in a duration of a frame cycle is define as the number of collisions in each superframe. Average number of Collisions in each superframe is calculated by measuring the total number of collisions over the total number of superframes.

Average Waiting time for Tags

Average waiting time for tags is the average of all tags waiting time, where tags waiting time is calculated as the time difference between the moment when a tag wakes-up and receives the subsequent beacon.

Average number of awaken tags in each superframe

The tag that is active means wakeup from sleeping mode is called awaken tag. Average number of awaken tags in each superframe is calculated by measuring the number of total awaken tags over the total number of superframes.

Average collision position

The slot number of a superframe in which collision happens is identified as collision position of that collided packet. Average collision position in each superframe is the ratio of the average of all positions when collision happens in the 48 slots superframes.

Average successful transmission position

The slot number of a superframe in which packet was successfully transmitted is identified as successful transmiossion position of that packet. In the 48 slots superframe, the average successful transmission position is calculated by measuring the total successful packets over the number of superframes.

Figure 5.1 illustrates the results for a variable sleeping time but for a fixed number of tags in each networks having 80 tags.

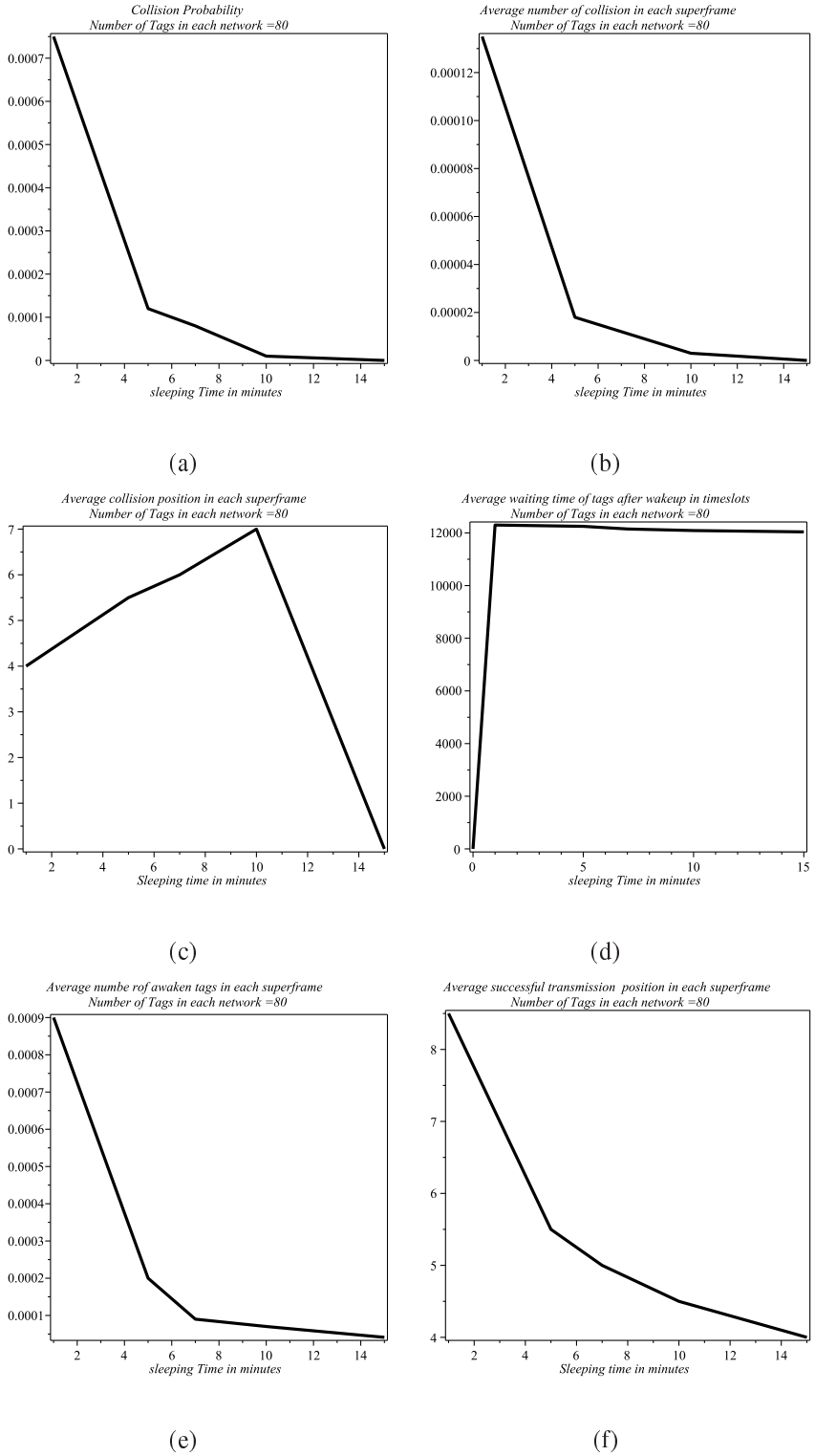


Figure 5.1: Performance measurement varying average sleeping time

In Figure 5.1(a), we find that increasing the average sleeping time from 1 to 15 minutes decreases the collision probability. This is because if the average sleeping time of tags is high, i.e., tags remain in sleep mode for a long period of time, then the probability that more than one tags wakeup at the same time is less. On the other hand, if the average sleeping time is low, this probability of waking up more than one tags at the same time will be high. A random number generator is used to generate tag's wakeup time. Hence, Figure 5.1(a) demonstrates that the collision probability for 1 minute sleeping time is much higher than that of the collision probability for sleeping time 15 minutes.The effect of decreasing the collision probability has relation with the number of collisions in the network. Hence, Figure 5.1(b) demonstrates that the average number of collisions of the network decreases when the sleeping time of tags increase. Figure 5.1(c) illustrates the average collision position in each superframe over sleeping time. We observe that the position of a collision is near the start of a superframe, where the collision position is at the slot number 4 for 1 minute sleeping time. The collision position is moving forward to the slot number 7 with increasing the sleeping time upto 10 minutes then decreases. We do not observe any collision for the sleeping time 15 minutes. Figure 5.1(d) demonstrates that the average tags waiting time after they wake up and receive the beacon do not change significantly when average sleeping time is increasing. When the sleeping time of tags is low (i.e., 1 minute) there is a high probability that several tags wakeup at the same time and wait for beacons. However, only one vicinity tags is allowed to receive the beacon. Thus, remaining tags wait for the next available beacons that increases the average tag waiting time. But this is not the case, when the sleeping time of tags is high. Hence, Figure 5.1(d) shows a slight decrease of the waiting time for increasing the sleeping time of tags.According

to the Figure 5.1(e), the number of awake tags decreases when the sleeping time of tags increases since it increases the wakeup interval.According to the Figure 5.1(f), the position of successful transmission moves towards the beginning position of the superframe as the number of collision decreases and vice versa. At the beginning, when the average sleeping time is 1 minute, the number of collision increases that decreases the number of successful transmissions (occurs at the timeslot 9 in superframe). Similarly, the position of successful transmission moves towards the starting position of the superframe for the increase average sleeping time (5,7,10 and 15 minutes), which is at the slot number 4. No collision is observed at all in this case.

In the IEEE 802.15.4 standard, transmission always takes place at the beginning of backoff slots. Hence, the position of frame a collision or a successful transmission occurs at the beginning of a superframe. We observe from Figure 5.1 that increasing the sleeping time has a positive impact on the overall networks performance as the collision probability deceases and the successful transmission position moves towards the starting position of the superframe.

Figure 5.2 illustrates the simulation results of the second scenario, a variable number of tags but for a fixed average sleeping time (1 minute).

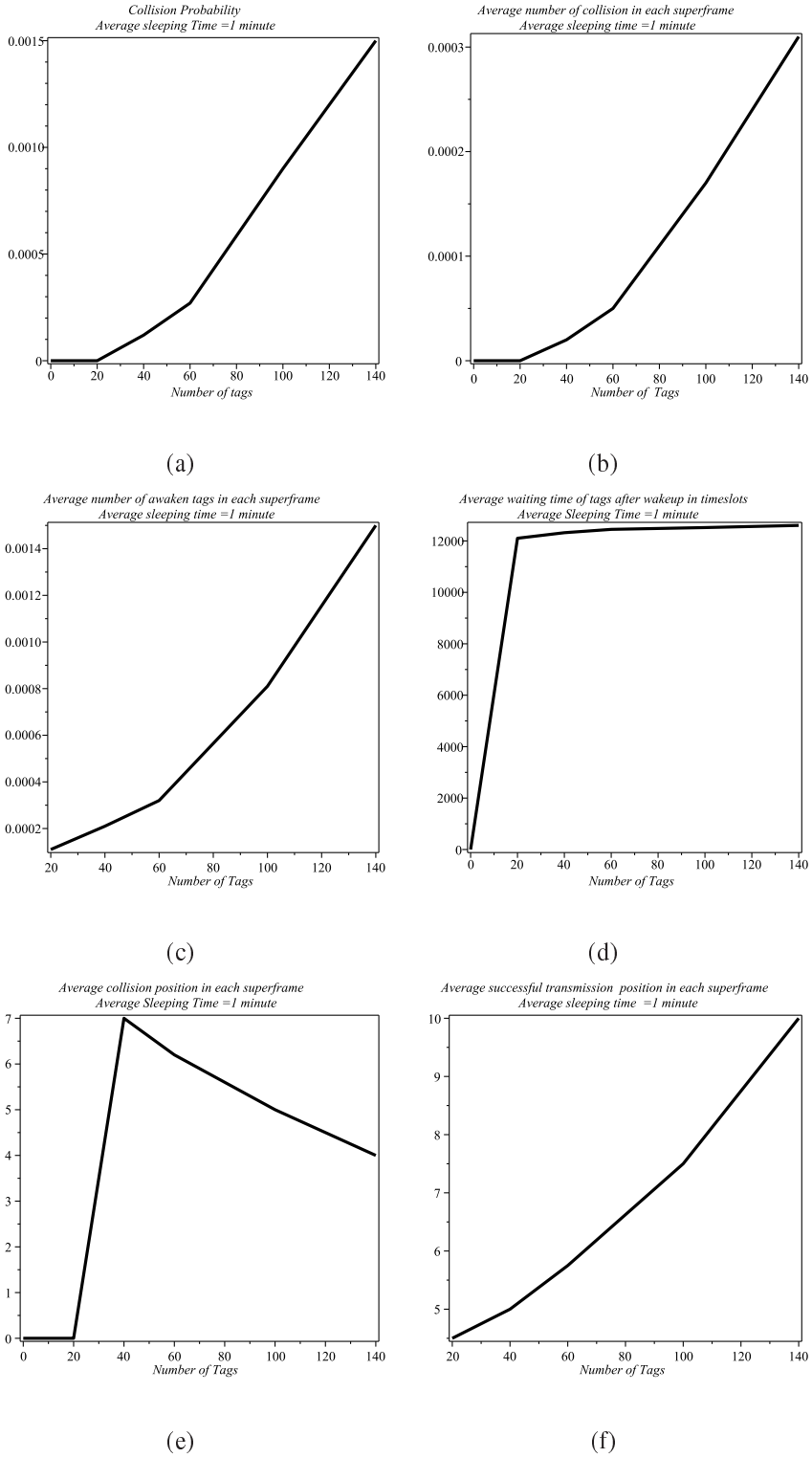


Figure 5.2: Performance measurement for variable Number of Tags

In Figures 5.2(a) and 5.2(b), we observe that increasing the number of tags has impact on the network performance. Collision probability and number of collisions increase for increasing the number of tags from 20 to 140.When the network traffic is high, the probability that more than one tags wakeup at the same time increases. This increases the number of collisions. On the other hand, when the network traffic is very low (number of tags is 20), the collision in the network decreases (Figure 5.2(a)).Again, if the number of tags with a fixed sleeping time increases, the number of tags that wakeup at the same time also increases. As a result, the number of collisions in each superframe increases (Figure 5.2(b)).Figure 5.2(c) illustrates the average number of awake tags in each superframe. The result slows that average number of awake tags increases if the number of tags in the network increase from 20 to 140 tags.Increasing the number of tags does not change much of the average tag waiting time as shown in Figure 5.2(d). However, when a large number of tags are awake most of them need to wait for the beacon as only for a subsequent reader the subordinate tags response. As a result, the waiting time of tags increases.According to Figure 5.2(e), the collision position moves towards the beginning of the superframe for increasing the number of tags. We observe that there is no collision when only 20 tags are present in the network. But for the increased traffic in the network (40 tags) the collision position moves forward of the superframe at the slot number 7. Similarly, the collision position moves towards the beginning position of the superframe when we further increase the tags number to 60,100 and 140 tags because of the increased collision probability. For the value of CW (=2) the collision position should be between 0 and 8 that is observed in the result.On the other hand, the successful transmission position moves forward of the superframe as is illustrated in Figure 5.2(f). When the number of collision in superframe

increases the number of successful transmissions decreases. As a result, the superframe position of successful transmission moves forward. We also observe that when the number of tags is 20, the collision probability(Figure 5.2(a)) is 0 and the position of successful transmission is very close to the beginning of the superframe (approximately at slot number 2). When the collision probability increases for the number of tags 140, the position of successful transmission moves to the slot number 10.

Figure 5.2 shows that if the number of tags in each network increases the collision probability increases. This is opposite to the result illustrated in Figure 5.1.

5.2 Performance Metrics and Simulation Results for EDCA

In the simulation model, we assume that an infrastructure network is operating in the saturation mode for single hop communication. We consider only two station classes: Wi-Fi normal/ordinary stations and reader/station class. For WiFi normal/ordinary nodes, we consider that packets are generated from the top level of the TCP in saturation mode. Poisson distribution is used to calculate the inter arrival rate between two packets with the assumption that $p\_device\_lambda = p\_arrival\_rate$. For reader/station, data arrival rate depends on the RFID networks, where 150 tags send their ID with the average sleeping time is equal to 1 minute.

We measure the performance in terms of throughput, access probability, average backoff time, average backoff phase, packet drop probability, AIFSN restart, collision probability, and probability of idle state. We define the following operational metrics.

Throughput

Throughput is defined as the ratio of the total amount of transmitted data (in slots) to the total number of back-off slots. It is calculated for data transmissions by all stations in the network and also for transmitting data by a specific station over the back-off period. Amount of data transmission in slots = number of transmitted data * 100. Where data size for the Wi-Fi node is assumed to be 100 slots without the header information. On the other side, the data size of reader/stations is only 100 bytes, which is assumed to be 20 slots without header information.

RTS collision probability

The probability of unsuccessful packets in the network is called collision probability. Collision probability is calculated by measuring the total number of collided RTS over total number of transmitted RTS packets.

Average backoff time

It is defined as the time a packet needs to wait before transmitting.

Access probability

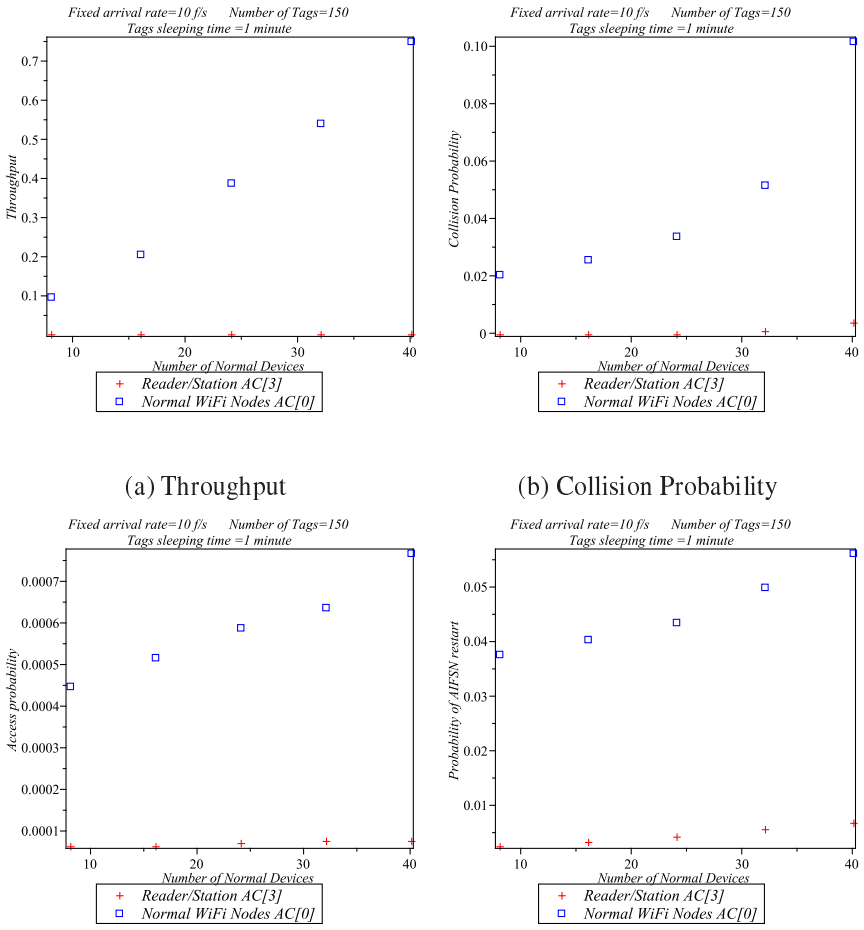
The probability of accessing the medium by a device in order to transmit a successful packet is denoted as access probability. It is calculated by measuring the total number of transmitted RTS over the number of free back-off slots.

We measure the performance of WLAN networks considering the following scenario.

1. Varying the number of normal Wi-Fi stations (8,16,24,32, and 40) but for a fixed data arrival rate (10 frames/sec) and fixed reader/station (3).

Normal Wi-Fi nodes have the lowest priority (AC[0]) and reader/stations have the highest priority (AC[3]) to access the medium. A reader receives tag‘s id from the tag and the number of receipt data varies based on the number of tags that are present in its vicinity.We measure the performance of reader/station for a fixed number of reader/stations (reader = 3). Readers receive data from a fixed number of tags (150) and fixed tag sleeping time. We aggregate the received tag‘s data upto 100 bytes (i.e., 10 IDs) so that the throughput of the overall network is maintained as the desired level. The plotted line with plus (+) represents reader/station and box (□) represents normal nodes.

Figure 5.3 and 5.4 demonstrates simulation results of WLAN networks for varying the number of normal stations but for a fixed data arrival rate and number of reader/stations (data from fixed tags=150 with fixed sleeping time = 1 minute)



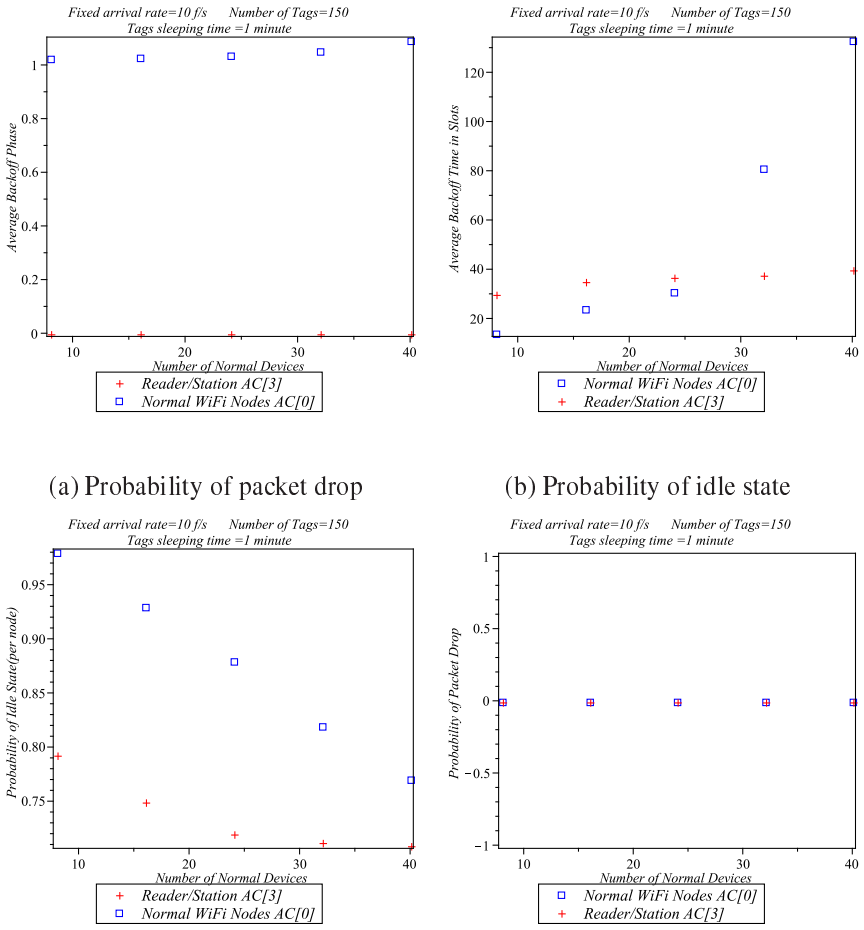
(a) Throughput (b) Collision Probability

(c) Access Probability (d) AIFS restart

Figure 5.3: Performance evaluation of WLAN varying number of normal stations

Figure 5.3(a) illustrates the throughput of the WLAN networks. When the number of normal stations increases from 8 to 40 the network traffic also increases. Hence, the throughput of AC[0] increases. On the other hand, the reader/station traffic load is almost same for the whole network as the number of tags and their transmitted IDs (data) are constant in the network and they are transmitted with high priority. We also aggregate the tag IDs that restuls the throughput for AC[3] is almost constant. Figure 5.3(b) illustrates

that the collision probability of the Wi-Fi normal nodes increases from 2% to 10% as the number of nodes increases.Number of collision for reader/stations is lower since they have the higher priority with the lower AIFSN and CW values. When the traffic load is smaller (i.e., the number of normal station 8,16, and 24) the collision probability of reader/station is almost zero. However, collision occurs for higher traffic load of normal stations, for instance, when the number of stations is 32, and 40. Figure 5.3(c) illustrates that the access probability for AC[0] increases as the number of nodes increases. Hence, the probability to access the medium decreases for increasing number of nodes. On the other hand, the access probability for AC[3] also slightly increases as the network traffic load increases. This shows that AC[0] nodes have small impact on traffic coming from AC[3] modes. In Figure 5.3(d) we observe that the AIFSN value for AC[3] increases for varying the number of normal nodes. That means, medium access is interrupted while accessing the medium due to the unavailability of the medium. There is a difference between the increase of AIFSN value for AC[0] and AC[3], which is about 4% difference on an average.



(a) Probability of packet drop

(b) Probability of idle state

(c) Average back-off phase

(d) Average back-off time

Figure 5.4: Performance evaluation of WLAN varying number of normal stations

Figures 5.4(a) and 5.4(b) demonstrate the average backoff phase and average backoff time in slots. We see from the Figure 5.4(a) that the average backoff phase of reader/station is zero or negligible. This is because all the transmitted packets are successful within the 1st backoff phase and average backoff time (slot) that increases slightly. On the other hand, the average backoff phase for normal stations increases (Figure 5.4(a)) and the backoff time also increases from 14 to 133 slots on an average (Figure 5.4(b)). Figure 5.4(c) illustrates

that the probability of being in idle state decreases as the traffic load increases from node 8 to 40. When only 8 normal stations with AC[0] and 3 reader/stations with AC[3] work most of the time the nodes remain idle as the traffic load increases. They become busy whenever require to transmit data.

Only 3 reader/stations are used for AC[3]. In this case, the total network load increases for increasing the number of normal nodes. Moreover, there is always a station that is ready to transmit. No packet drops are observed in Figure 5.4(d) since the network load is low having only two access category. Hence, the transmitted packet is successful within the 7th backoff phases that results the overall networks performance as is desired.

5.3 Discussion

From the results (Figure 5.1, 5.2 5.3 and 5.4), we observe that individual network performs at the desired level. We see that the collision probability for both networks is very low. In RFID network, the collision probability is only 0.15% with a high traffic load, and is .07% for a medium traffic load (number of tags = 80). On the other hand, in WLAN network, the collision probability is 10% and 0.39% for a high traffic load but for the lower priority and higher priority nodes, respectively. This result demonstrates that both networks are not in interference by each other and the ratio of successful transmission is high.

When two networks are integrated through the reader (works as a bridge), the throughput of the networks for lower priority nodes and higher priority nodes are in satisfactory level. The highest priority nodes are not affected by the lower priority nodes (observed in Figure 5.3). The QoS of the networks are also maintained. Thus, the proposed approach is efficient to eliminate the problems of interference and co-existence for RFID and WLAN

networks.

Chapter 6

Conclusion

In this thesis, we implemented a framework comprising of Radio Frequency Identification (RFID) and IEEE 802.11 WLAN technologies that eliminates the well-known coexistence and integration problems of these two widely used networks working in the same 2.45 GHz ISM frequency band. The IEEE 802.11 WLAN uses the Enhanced Distributed Channel Access (EDCA) protocol to improve the network quality of service (QoS). Both networks work in a time sharing manner using the medium access mechanisms of Point Coordination Function (PCF) and Distributed Coordination Function (DCF). In this framework, readers work as a special nodes and an interface between two networks to maintain the QoS.

We simulate and measure the performance of this framework using Artifex simulation tool for only uplink communication. In the WLAN networks, we vary the number of ordinary stations for a fixed data arrival rate and a fixed number of reader/stations. We measure the performance in terms of throughput, frame collision probability, packet drop probability, and access probability etc. In the RFID network part, we measure the performance in

terms of collision probability, frame collision position etc. The collision probability decreases, as is desired, for increasing the sleeping time of tags and increases for increasing the number of tags. Results also show that when readers work as the highest priority station and Wi-Fi nodes as lower priority, they maintain the network accuracy as the desired level. Simulation results also show that the highest priority nodes are not affected by the lower priority nodes. Thus, we achieve the objective of this thesis work.

Appendix A

Abbreviations

AC	Access Category
ACK	Acknowledgement
ACS	Anti-collision/select
AID	Association Identifier
AIFS	Arbitration Interframe Space
AP	Access Point
BE	Backoff Exponent
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	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear-To-Send
CW	Contention Window
DCF	Distributed Coordination Function
DIFS	Distributed Interframe Space
DSRC	Dedicated Short Range Communication
DSSS	Direct Sequence Spread Spectrum
DTIM	Delivery Traffic Indication Message
EDCA	Enhanced Distributed Channel Access
EM	Electromagnetic

EPC	Electronic Product Code
FFD	Full functional device
FHSS	Frequency Hopping Spread Spectrum
HF	High Frequency
HC	Hyprid Coordinator
HCF	Hybrid coordination function
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
ISM	Industrial, Scientific and Medical
LF	Low frequency
LLC	Logical Link Control
MAC	Medium Access Control
MLME	MAC Sublayer 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
PGF	Probability Generating Function
PHY	Physical Layer
PIFS	Point coordination function Interframe Space
QoS	Quality of Service
RBC	Random Backoff Countdown
RFD	Reduce functional device
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
TXOP	Transmission Oppertunity
UHF	Ultra High Frequency
UP	User Priority
WLAN	Wireless LAN
WPAN	Wireless Personal Area Network

Bibliography

[1] http://aimglobal.org/technologies/rfid/. Visited May 2011.

[2] http://ieee802.org/15/pub/tg4f.html. Visited June 2011.

[3] http://revolutionwifi.blogspot.com/. Visited July 2011.

[4] http://wi-fiplanet.com/tutorials/article.php/1548381/80211-medium-access-methods.html. Visited June 2011.

[5] IEEE 802.11. *IEEE Standard for Information Technology Telecommunications and information exchange between systems local and metropolitan area networks specific requirements - Part 11: Wireless LAN medium Access Control(MAC) and Physical Layer(PHY) Specifications*. IEEE, 2007.

[6] IEEE 802.15.4. *Standard for part IEEE 802.15.4: Wireless medium access control (MAC) and phusical layer (PHY) specifications for low rate wireless personal area networks (WPAN)IEEE Std 802.15.4*. IEEE, New York, 2003.

[7] Norman Abramson. The aloha system: another alternative for computer communications. In *Proceedings of the November 17-19, 1970, fall joint computer conference*, AFIPS '70 (Fall), pages 281–285, New York, NY, USA, 1970. ACM.

[8] A.A. Alahmadi and M.A. Madkour. Performance evaluation of the ieee 802.11e edca access method. In *Innovations in Information Technology, 2008. IIT 2008. International Conference on*, pages 490 –494, dec. 2008.

[9] G. Bagnato, G. Maselli, C. Petrioli, and C. Vicari. Performance analysis of anti-collision protocols for rfid systems. In *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th*, pages 1 – 5, april 2009.

[10] V. Chawla and Dong Sam Ha. An overview of passive rfid. *Communications Magazine, IEEE*, 45(9):11 – 17, september 2007.

[11] RSoft Design. *Artifex V.4.4.2*. RSoft Design Group,Inc., 2003.

[12] N. Golmie, D. Cypher, and O. Rebala. Performance evaluation of low rate wpans for medical applications. In *Military Communications Conference, 2004. MILCOM 2004. IEEE*, volume 2, pages 927 – 933, Nov 2004.

[13] I. Howitt and J.A. Gutierrez. Ieee 802.15.4 low rate - wireless personal area network coexistence issues. In *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, volume 3, pages 1481 – 1486, march 2003.

[14] Ming-Chuan Hsu and Yaw-Chung Chen. Enhanced pcf protocols for real-time multimedia services over 802.11 wireless networks. *Distributed Computing Systems Workshops, International Conference on*, 0:56, 2006.

[15] Hongwei Huo, Youzhi Xu, C.C. Bilen, and Hongke Zhang. Coexistence issues of 2.4ghz sensor networks with other rf devices at home. In *Sensor Technologies and*

Applications, 2009. SENSORCOMM '09. Third International Conference on, pages 200 – 205, june 2009.

[16] Gyung-Ho Hwang and Dong-Ho Cho. Performance analysis on coexistence of edca and legacy dcf stations in ieee 802.11 wireless lans. *Wireless Communications, IEEE Transactions on*, 5(12):3355–3359, December 2006.

[17] Jennic technology for a changing world. *Co-existence of IEEE 802.15.4 at 2.4 GHz Application Note*, first edition, February 2008.

[18] k. Ranjit, R. Srinivas, and I. Rajesh. Qos and interoperability issues of 802.11 and 801.11e. Technical report, KReSIT,Indian Institute of Technology Bombay, 2006.

[19] H. Khaleel, C. Pastrone, F. Penna, M.A. Spirito, and R. Garello. Impact of wi-fi traffic on the ieee 802.15.4 channels occupation in indoor environments. In *Electromagnetics in Advanced Applications, 2009. ICEAA '09. International Conference on*, pages 1042 –1045, sept. 2009.

[20] James F. Kurose and Keith Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edition, 2002.

[21] Su-Ryun Lee, Sung-Don Joo, and Chae-Woo Lee. An enhanced dynamic framed slotted aloha algorithm for rfid tag identification. In *Proceedings of the The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, pages 166–174, Washington, DC, USA, 2005. IEEE Computer Society.

[22] Cloran M. Simulation of ieee 802.11 pcf function in glomosim. Master's thesis, DUBLIN CITY UNIVERSITY, 2004.

[23] Jelena Misic and Vojislav Misic. *Wireless Personal Area Networks: Performance, Interconnection, and Security with IEEE 802.15.4*. Wiley Publishing, 2008.

[24] Saeed Rashwand and Jelena Misic. Stable operation of ieee 802.11e EDCA: Interaction between offered load and mac parameters. *Ad Hoc Networks*, In Press, Corrected Proof, 2010.

[25] D. Raychaudhuri and K. Joseph. Performance evaluation of slotted aloha with generalized retransmission backoff. *Communications, IEEE Transactions on*, 38(1):117 – 122, jan 1990.

[26] S. Shafi. Performance of a beacon enable ieee 802.15.4 complient network.a report presented to university of matitoba in partial fulfillment of the requirements for the degree of master in science. Master's thesis, University of Manitoba, 2005.

[27] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas. Co-existence of zigbee and wlan, a performance study. In *Wireless Telecommunications Symposium, 2006. WTS '06*, pages 1 –6, april 2006.

[28] A. Sikora and V. F. Groza. Coexistence of ieee802.15.4 with other systems in the 2.4 ghz-ism-band. 3:1786–1791, may 2005.

[29] S. Siwamogsatham. Improving csma for wlans via piggybacking and scheduled backoff mechanisms. In *Future Generation Communication and Networking (FGCN 2007)*, volume 1, pages 557 – 563, Dec 2007.

[30] Silverio Carlo Spinella, Antonino Giordano, Antonio Iera, and Antonella Molinaro. Indoor positioning techniques based on wlan/rfid technology integration.

[31] William Stallings. *Wireless Communications and Networks*. Prentice Hall Professional Technical Reference, 1st edition, 2001.

[32] Xiaoyong Su, Chi cheng Chu, B. S. Prabhu, and Rajit Gadh. On the creation of automatic identification and data capture infrastructure via rfid.

[33] Cisco Systems. *Voice over Wireless LAN 4.1 Design Guide*, 2010.

[34] G.M. Tamilselvan and A. Shanmugam. Probability of channel collision and per analysis of coexistence heterogeneous networks for various topologies. In *Control, Automation, Communication and Energy Conservation, 2009. INCACEC 2009. 2009 International Conference on*, pages 1 – 7, june 2009.

[35] Nitin Vaidya and Samir R. Das. Rfid-based networks: exploiting diversity and redundancy. *SIGMOBILE Mob. Comput. Commun. Rev.*, 12:2–14, January 2008.

[36] Harald Vogt. Efficient object identification with passive rfid tags. In *Proceedings of the First International Conference on Pervasive Computing*, Pervasive '02, pages 98–113, London, UK, 2002. Springer-Verlag.

[37] H. Wu and Y. Zeng. Efficient framed slotted aloha protocol for rfid tag anticollision. *Automation Science and Engineering, IEEE Transactions on*, PP(99):1, 2011.

[38] Guang Yang and Yu Yu. Zigbee networks performance under wlan 802.11b/g interference. In *Wireless Pervasive Computing, 2009. ISWPC 2009. 4th International Symposium on*, pages 1 – 4, feb. 2009.

[39] Lei Zhang and Zhi Wang. Integration of rfid into wireless sensor networks: Architectures, opportunities and challenging problems. In *Grid and Cooperative Computing Workshops, 2006. GCCW '06. Fifth International Conference on*, pages 463 – 469, oct 2006.

[40] S. Zoltan, A. John, and T. Pradeep. Radio frequency identification transponder. a report presented to ryerson university in partial fulfillment of the requirements for the degree of b.eng. Master's thesis, Ryerson University, 2008.