UNIVERSITY OF TURKISH AERONAUTICAL ASSOCIATION

INSTITUTE OF SCIENCES AND TECHNOLOGY

DEVELOPMENT OF AN ANTI-COLLISION PROTOCOL FOR RFID BASED STUDENTS' ATTENDANCE SYSTEM: A Combination of DFSA with Predefined BFSA

MASTER THESIS

Ghassan Ali Hameed HAMEED

Department of Electrical and Electronics Engineering

DECEMBER 2016

UNIVERSITY OF TURKISH AERONAUTICAL ASSOCIATION

INSTITUTE OF SCIENCES AND TECHNOLOGY

DEVELOPMENT OF AN ANTI-COLLISION PROTOCOL FOR RFID BASED STUDENTS' ATTENDANCE SYSTEM: A Combination of DFSA with Predefined BFSA

MASTER THESIS

Ghassan Ali Hameed HAMEED

1406030019

Department of Electrical and Electronics Engineering

Thesis Supervisor: Asst. Prof. Dr. Hassan SHARABATY

December 2016

Ghassan Ali Hameed, having student number 1406030019 and enrolled in the Master Program at the Institute of Science and Technology at the University of Turkish Aeronautical Association, after meeting all of the required conditions contained in the related regulations, has successfully accomplished, in front of the jury, the presentation of the thesis prepared with the title of: "DEVELOPMENT OF AN ANTI-COLLISION PROTOCOL FOR RFID BASED STUDENTS' ATTENDANCE SYSTEM: A Combination of DFSA with Predefined BFSA"

Thesis Supervisor: Asst. Prof. Dr. Hassan SHARABATY
University of Turkish Aeronautical Association

Jury Members: Asst. Prof. Dr. Özgür KELEKÇİ
University of Turkish Aeronautical Association

Asst. Prof. Dr. Tayfun Küçükyılmaz
TED University

Thesis Defense Date: 01. 12. 2016

UNIVERSITY OF TURKISH AERONAUTICAL ASSOCIATION

INSTITUTE OF SCIENCES AND TECHNOLOGY

I hereby declare that all information in this study I presented as my Master's Thesis, called: Development of anti-collision protocol for RFID based students' attendance system, has been presented in accordance with the academic rules and ethical conduct. I also declare and certify with my honor that I have fully cited and referenced all the sources I made use of in this present study.

Ghassan Ali Hameed HAMEED

01.12.2016

ACKNOWLEDGEMENTS

Firstly, I would like to thank my God, that helped and supported me in each day of writing and execution this thesis. Special thanks for my (father, and mother), and my family, that is because of the prays and support of them, I had reached my aim. Special thanks and best regards to the University of Turkish Aeronautical Association and its academic stuff for their corporation. Special thanks and best regards for my supervisor Dr. Hassan SHARABATY for his corporation and his support to me in the whole time of my master study until I reached to this stage.

DECEMBER, 2016 **Ghassan Ali Hameed HAMEED**

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ID	: Identity
RFID	: Radio Frequency Identification [29]
LF	: Low Frequency [34]
HF	: High frequency [34]
UHF	: Utlra High Frequency [34]
CF	: Carrier Frequency [37]
ASK	: Amplitude Shift Keying [44]
RC	: Resistance Capacitor [60]
D.C	: Direct Current [60]
GSM	: Global System for Mobile communications
PHP	: Hypertext Processor
LCD	: Liquid-crystal display
USB	: Universal Serial Bus
TDMA	: Time division Multiple Access
BT	: Binary Tree[60]
BS	: Binary Search [60]
QT	: Query Tree [60]
PA	: Pure ALOHA [60]
SA	: Slotted ALOHA [60]
FSA	: Framed Slotted ALOHA [60]
BFSA	: Basic Framed Slotted ALOHA [60]
DFSA	: Dynamic Framed Slotted ALOHA [60]

ABSTRACT

DEVELOPMENT OF AN ANTI-COLLISION PROTOCOL FOR RFID BASED STUDENTS’ ATTENDANCE SYSTEM: A Combination of DFSA with Predefined BFSA

HAMEED, Ghassan Ali
Master Thesis, Department of Electrical and Electronics Engineering
Thesis Supervisor: Asst. Prof. Dr. Hassan SHARABATY
December–2016, 79 pages

Recently a lot of researchers and scientists gave a huge interest to RFID technology. The importance of RFID systems come from its ability to communicate remotely with others parts in spite of barriers, obstacles, walls or even the water. Besides, it offers a high speed of processing for all operations performed by these systems. Main parts of RFID system are tags and reader. RFID Reader and tags can communicate in different distances depending on the frequency of operation. However, some problems affect its performance especially ‘‘tags collisions’’. Collision is occurring between tags because of their competition in the interrogation zone of the reader, this makes reader cannot detect collided tag ID’s successfully, and affects the accuracy of the identification process. When RFID system used as students’ attendance system, this problem can affect the time of authentication and then on the lecture time. This thesis proposes an anti-collision protocol to reduce RFID tags collision; we will combine the dynamic framed slotted aloha (DFSA) with the predefined basic framed slotted aloha (BFSA) to accelerate the identification process of the RFID based students’ attendance system. Simulation results, obtained by Matlab, show how proposed protocol enhances the time and throughput of the authentication, also the reduction in collided slots as compared with DFSA, BFSA with and without muting.

Key words: DFSA, BFSA, muting, RFID tags, attendance system, collision.

ÖZET

ÖĞRENCİ KATILIM SİSTEMİ BAZLI RFID İÇİN ÇATIŞMA ÖNLEYİCİ PROTOKOLÜN GELİŞTİRİLMESİ: DFSA'nın önceden tanımlanmış BFSA ile kombinasyonu

HAMEED, Ghassan Ali
Yüksek Lisans Tezi, Elektrik-Elektronik Mühendisliği Bölümü
Tez Danışmanı, Doçent Doktor Hassan SHARABATY
Aralık –2016, 79 sayfa

Son dönemde, pek çok araştırmacı ve bilimadamı, RFID teknolojisine büyük ilgi gösterdi. RFID sisteminin önemi, bariyerler, engeller, duvarlar, hatta su altına rağmen uzaktan iletişim sağlama yeteneğine dayalıdır. Öte yandan, bu sistemlerle işletilen tüm operasyonlar için yüksek hızda işleme özelliği sağlar. RFID sistemin ana parçaları etiketler ve okuyucudur. RFID Okuyucu ve etiketler, operasyonun frekansına bağlı olarak değişik mesafelerde iletişim sağlar. Ne var ki bazı problemler, özellikle de "etiket çatışması" performansını etkilemektedir. Çatışma, okuyucunun sorgulama bölgesinde etiketler arasında oluşan rekabetten kaynaklanmaktadır, bu durumda okuyucu çatışan etiket kimliklerini başarıyla belirleyememekte olup bu durum, tanımlama sürecinin doğruluğunu etkilemektedir. RFID sistemi, öğrenci katılım sisteminde kullanıldığı zaman, bu problem, kimlik doğrulama zamanını ve akabinde ders zamanını etkilemektedir. Bu tez, RFID etiket çatışmasını azaltmak için bir çatışma karşıtı protokol önermektedir; dinamik çerçeveli dilimli aloha (DFSA) ile önceden tanımlanmış temel çerçeveli dilimli alohayı (BFSA), RFID bazlı öğrenci katılım sisteminin tanımlama işlemini hızlandırmak amacıyla birleştireceğiz. Matlab tarafından elde edilen simülasyon sonuçları, önerilen protokolün kimlşk doğrulama zamanını ve iş hacmini nasıl yükselttiğini ve ayrıca DFSA, BFSA ile karşılaştırıldığında, durdurma olsun ya da olmasın çatışan yuvalarda azalma olduğunu göstermektedir.

Anahtar sözcükler: DFSA, BFSA, durdurma, RFID etiketleri, katılım sistemi, çatışma.

CHAPTER 1

TYPES OF CURRENT COMMONLY USED ATTENDANCE SYSTEMS AND THEIR LIMITATIONS

1.1. Introduction

In this chapter there is an exploration for a number of an attendance systems which are can be used in universities, institutes, and schools. There are two parts for each attendance system. Firstly, there is a brief explanation supported by a diagram for clarification its work in order to illustrate the processes inside the system. Secondly, there will be the properties of each attendance system. The attendance systems will be in four sections, which are starting by Barcode attendance system and ending by Iris recognition based attendance system.

1.2. Types of current commonly used attendance systems

1.2.1. Barcode based attendance system

The Barcode identification system is composed from two main parts: barcode scanner and barcode card as shown in Figure 1. Barcode identification is a reading mechanism of the information, this information is existing on the surface of solid card, the card may be plastic, paper, or metal. The barcode card contains this information as a series of bars and spaces in between. The bars and spaces are with different widths depending on the information encoded on the Barcode card in case of one-dimension Barcode. In the case of two dimensions Barcode, the data are represented by using dots and spaces in order to increase the data size of the Barcode card. The scanner (reader) device can read this information by applying a directed light onto the card, then the reflected light from the card will contains high and low regions, this variation will be decoded into zeros and ones. The information on the Barcode card may represent a data of a product, commodity price, or may be include an (ID) number as in case of the attendance or security systems which are used in factories, universities, schools [1]. Barcode based student attendance system is employing the Barcode identification system to record the students' attendance. Additional hardware and software are used with Barcode identification system: microcontroller, computer to use them in the controlling and database processing. Barcode scanner device acts as the reader whereby the student's ID card (that contains the Barcode number) is scanned. There are two main processes in the student attendance system: registration process and identification (recognition) process. In the registration process, the student must scan his ID card by the barcode scanner for the purpose of saving his information inside the database. In the identification process the registered students pass their IDs in front of the reader device to read (record) their attendances. After scanning (reading) process, the student's ID will be compared with the ID saved in the database, if there is match the attendance will be successful, otherwise the attendance will fail.

Figure.1. Barcode system: scanning device (reader) and the barcode card.

Thus, the lecturer can detect all the late comers and absent student that will be view on the system. When the student scans his ID by the reader device, all relevant information (time, lecture name, student name) will appear in the LCD or in the computer of the lecture. Number of modifications had been added onto the Barcode based students' attendance system such as sending a message to the parents by using a GSM model or by email through the internet to tell them that their son is within the school or institute [2]. The block diagram of the barcode based attendance system as shown in Figure 2.

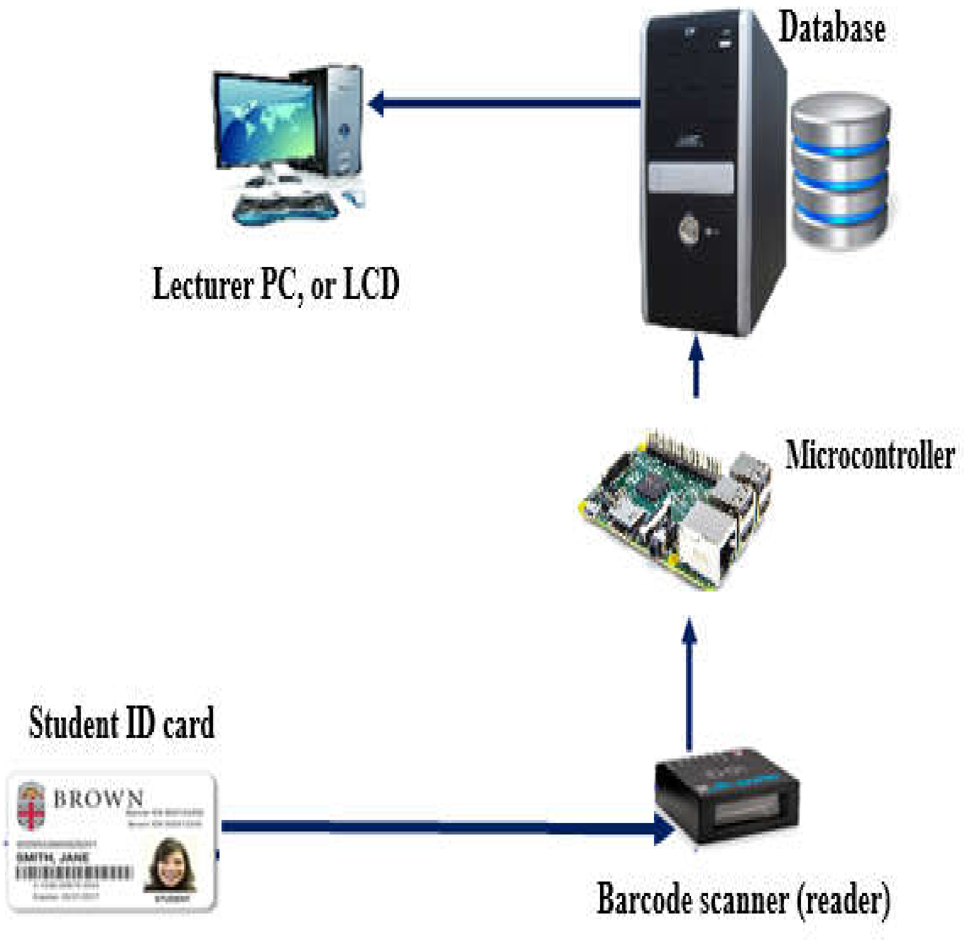


Figure.2. Block diagram of barcode based attendance system.

1.2.1.1. Limitations of barcode based attendance system

The Barcode system is less expensive than any attendance system, such as RFID system, face recognition system, finger print system or even iris recognition system, but this in the typical state in which there are no damage or an update in information of the ID card.

1. Security. The security of Barcode based system is very low or almost non-existent, because it is easy to duplicate the barcode based identification ID card, which in the case of attendance system will affect negatively on the safety of the institute, university, or school.
2. Reliability. The information in barcode can be damage more easily because of any type of envelopes that will be cover the card in order to protect the printed data will prevent the scanning process even it was transparent, if the barcode scratched or stained with grease or even the dust. In addition to the reading in the sunlight is impossible.
3. Data capacity. The data on the barcode can be range from (8-15) characters in the case of one-dimensional code, while the two-dimensional code can be up to (2000) characters. This capacity is very low and cannot be more than few bytes, in order to increase it the barcode tag must be bigger [1].
4. Read/write. Barcode does not support the reading/writing property as in RFID based-systems, any information after printing the code on the card cannot be added or removed. At this situation, the Barcode ID card can be used one time only, so if there is any error in the information printed onto the Barcode ID card will cost extra money, the administration will have to make a new one [3,4].
5. Speed. Each Barcode ID card requires from one to several seconds to read it successfully.
6. Multiple IDs reading. The Barcode scanner cannot read more than one ID card at the same time, that required from all users to be in a queue.

7. Distance. The maximum distance in which the ID card can be read successfully is several centimeters, while in some types successful reading requires a physical contact.

8. Movement support. The ID card must be exactly stable in a direct line of sight of Barcode scanner device because any movement during the reading process will fail the identification [5].

1.2.2. Face recognition based attendance system

The human face had recently taken a great interest from the scientists and researchers who specialized in various fields: communication, security, digital signal processing. The automatic identification systems which depend on face recognition technology had been finding many application areas that can be used in, the examples of these applications are: human-computer interfaces, security control systems, and model-based video coding. Face recognition based systems have been advancing, especially when the Eigenface had been proposed [6]. Face recognition based system can operate in two modes: face verification (authentication), and face identification (recognition). In face verification mode, the matching process is between one query face image with one saved face image in the data base (comparison of one to one), and it is implemented in E-passport. While the face identification mode performs the comparison process between one query face image with several faces saved in the database, and this mode can be found in attendance systems [7]. The similarity alone is not enough in some identification systems which implement face recognition, since the face must equal or exceed the threshold or confidence level in order to be successfully identified. The factors which mainly affect the performance of face recognition based system are: facial wear, illumination, facial pose, age span, expression, hair, and motion. The acquired face image can be taken as two dimensional or three dimensional, depending on the security level of the face recognition based system. Face recognition system is based on extracting the coordinates of the face features like: width of mouth, width of eyes, pupil, and compares the results with the measurements stored in the database computer [8].

1.2.2.1. Stages of operation of face recognition based attendance system

The face recognition attendance system works by using face recognition algorithm. When the student enters the lecture room his face image will be captured by the camera mounted in the room wall at the entrance. Then the face region is extracted and passed to pre-processed stage for further processing. All these stages are combined in the face recognition attendance algorithmically in order to success the identification process. The stages of work of the faces recognition attendance system will be as below:

a. Image capturing stage

In this stage there is a camera mounted at the distance from the entrance of each class room to capture the frontal images of all students which registered in the class.

b. Face detection stage

In the face detection stage, the system performs the segmentation (separation) the face region from the surrounding background, and this can be done by finding the face boundaries (forehead, left side, right side, and chin). A lot of face detection approaches had been proposed, some of them depend on the colour skin and the others depend on the RGB colour space [8].

c. Pre-processing stage

After the detection process, the face is extracted and subjected to processing. These sub-processes are necessary to enhance the image quality, and when the detected face image has the following un wanted features. The pre-processing stages involves the following numbers of processes:

- Illumination normalization. It used when the surrounding area of the captured face image has different illumination levels [9].

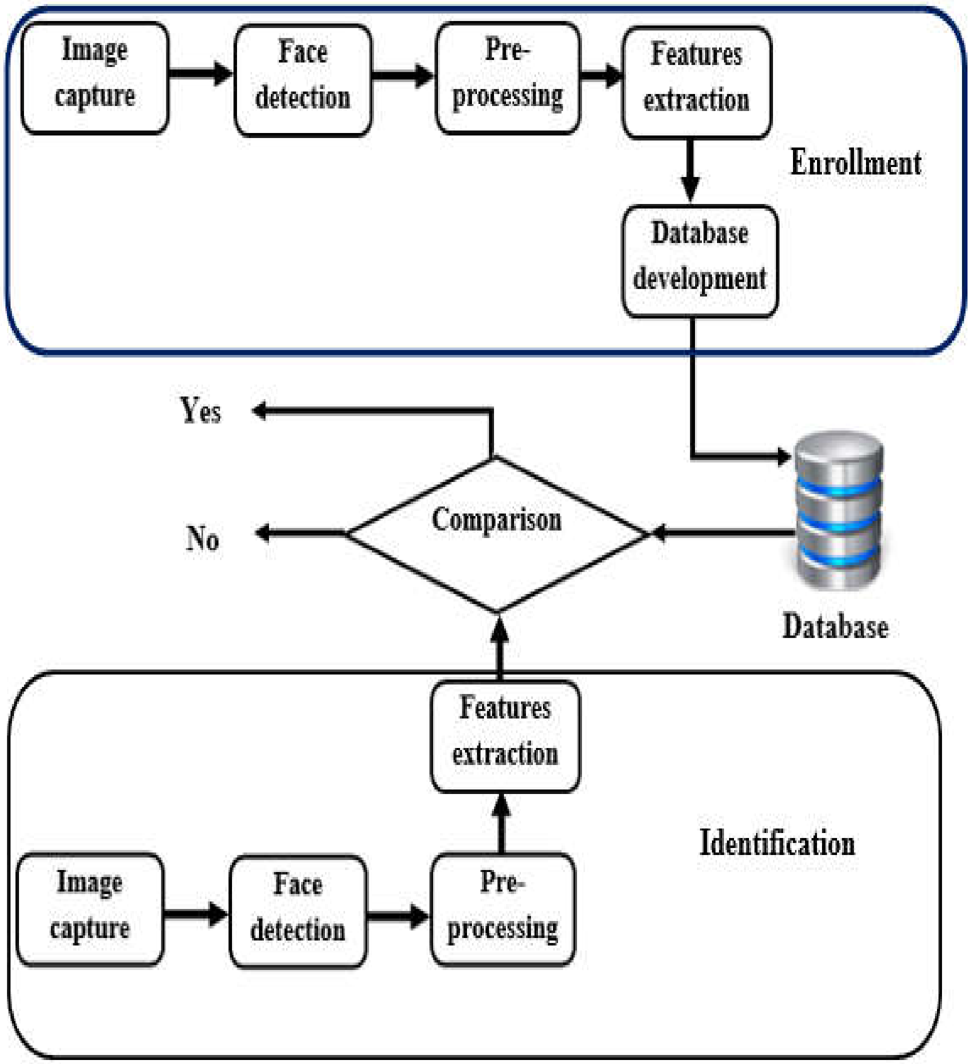


Figure.3. Processes stages inside face recognition attendance system.

- Histogram equalization. It usually used when the contrast of the captured face image is very low.

- Image re-sizing using bi-cubic interpolation method. It is used to reduce the mathematical complexity in the system, especially in the case of captured face image has high resolution and big size.
- Low pass filtering. It is used when the captured face image contains a blurry effect [10].

d. Feature extraction

The face recognition system its performance mainly depends on the feature extracting. The process of feature extracting can be achieved by using some techniques in between holistic technique. The face recognition based identification system can be considered robust and reliable whenever there are many distinctive facial features are extracted during the recognition processes. The features that can be recognized in face recognition based identification system are: inter pupil distance, distance between the eyes, face dimensions, eyes dimensions, the length of the nose, and the length of the lips, distance from the lips to the chin, and else [8].

d. Database development stage

After extracting the facial features of the users, all the information will be converted to digital data and then be saved into the database storage device for the purpose of enrollment. The system will consider all the stored data as a template that can be compared again with the face data of any user want be identified. Figure 3 shows the block diagram of all processes inside the face recognition system [8].

1.2.2.2. Limitations of face recognition based attendance system

The giant role of biometric based identification systems in access control cannot be denied, that the face recognition system includes to them. The cheating in any authentication system that bases on the face recognition system is almost difficult. Despite the wide separation of face recognition systems in serval fields such as: military, government, education, and business, but face recognition attendance system has some limitations which still affect its wide spread and these limitations are:

1. Speed. The speed of the face recognition attendance system depends on the devices used, algorithms for recognition and detecting features, the need of these properties is because any movement of the face will cause disturbance in recognition. In addition, it requires from all users to be in a queue [7, 12].

2. Twins faces. At this situation, the faces of twins are very hard to be recognized because the variation in facial expressions is very small and difficult to be revealed [8].

3. Changes due to age. One of the big disadvantages of face recognition attendance system is the age effect, because it depends on the main feature dimensions of the human face which it is hard to stay unchangeable with advancing in age [11].

4. Illumination and pose. The recognition features of the same face can significantly change by the variation of illumination and pose which play an important role in the identification process, this situation imposes special conditions on the face recognition attendance system to work properly. In addition, the solution of these problems is more expensive [12].

5. Unreadable face. Some students have defects which are congenital or by accidents, such as oblique nose, and the other may have unclear face features, because some certain surgeries, or injured as a result of incidents. This will make the face scanning process cannot be done [13].

6. The cost. one of the greatest disadvantage is the high cost of face recognition based attendance system. The reason behind this, it is needing to different devices which have a high range with respect to the cost [14].

7. Distance. the distinct advantage is contactless process, because it can capture the image of face with a separation distance between the device and the user, while in other hand the finger print based system in which user must touch the device to take his or her attendance [14].

1.2.3. Iris recognition based attendance system

The iris is an internal region inside the eye, its location is in front the eye lens and behind the cornea. The attendance system based on eye iris has a unique characteristic that is giving some new ideas to authentication process. The iris based system is the most accurate authentication system, because it implements the recognition methods which depends on the features of the eye pupil which their similarity between the humans is impossible [15]. These distinctive features contain information at multiple scales so that the signal processing technique that depends on wavelet is used to extract the iris features. The place of human iris is inside the eye, so it is protected by a different types of layers, and it has a very complicated structures that will remain unchangeable throughout the life of person [16].

1.2.3.1. Stages of operation of iris recognition based attendance system

The iris recognition attendance system works by using iris recognition algorithms. These algorithms are applied in a number of stages of work in order to complete the identification, as shown below.

a. Iris image acquisition stage. A two dimensional images of the eye are captured by using of a monochrome CCD camera that is implementing near infrared (NIR) for the purpose of getting iris region. The reason behind this, is the reflection of human iris mostly high at the (NIR) band. Some iris situations require additional illumination so that an external NIR light that will be co-located with the system in order to reveal the iris texture. There are two types of iris acquisition systems depending on the user cooperation degrees that are required. The first type of the system requires from the user an intensive cooperation. The system asking the all users to adjust their heads posing for the system in purpose of acquire an iris image. In this type of system, the process of image acquisition must be repeated until the iris image is qualified. Because of the size of human eye iris is very small, the iris camera has a lens with high magnification. The second system has the ability of controlling the orientation and/ or the zooming and focus setting of the camera for acquiring a satisfactory iris images, so the cooperation requirement of the user is less than from the first system that make it more compatible from the first system.

b. Localization of iris boundary stage (segmentation). This process is summarized on finding the iris region which consists from a color zone surrounded by a white color area named as (sclera) forming outside and black color zone that is the pupil from the inside. This can be done by finding inner and outer boundaries of the eye iris. The accuracy of this stage should be high, because the success of the system significantly depends on it. Number of steps are implemented in this process. These steps start by eye image converting into greyscale image. After that extraction of binary image from result of first step and this is depending on the threshold value used. There is ability that the binary image contains some noise, this image can be considered as the pupil region. Removing of the noise and extraction of the only image is done by using structural image processing such as dilation and erosion. The next step is filling holes to fill all light spots reflected which caused by illumination. The reason of this operation is to pupil region appears clearly. After that operation of canny edge detection for finding iris and pupil edge in separate forms. The last step is the Hough transformation on the resulting images from canny edge process for providing the necessary information such as iris' center and radius and pupil area to be used in normalization process, to obtain complete circular shape of pupil.

c. Normalization stage. It represents a process of mapping the annular texture in the rectilinear iris image to a doubly polar format without dimension. This can be done by using the pupillary and limbic boundaries that are existing in the iris. Thus it can be considered that the main goal of normalization is to alleviate the effects of the size variation of the eye pupil upon the result of iris recognition, and because of this it is adopted in most of the iris recognition methods.

d. Resize of iris region. It is the second step of the normalization stage; it will be performed by making all iris images uniform in the recognition system in order to be in fixed size. The main reason behind this step is that difference in iris images captured for one person as well as for different people. Because of some factors such as illumination variation, eye rotation in eye socket and tilting the user head, camera orientation and vibration, position of the eye with respect to camera, instability of the distance between eye and the camera.

e. Encoding and matching. It is the most important process in which the extracted features be converted into binary codes (0, 1). The encoding algorithms are using wavelet filters to analyze and examining the iris. The quadrature two dimensional (2D) Gabor wavelets are commonly used to extract the information of the iris texture. After building these data, the authentication for any person must pass all these previous five stages as well as the data base saving then the result will be compared with the data base of person eye iris.

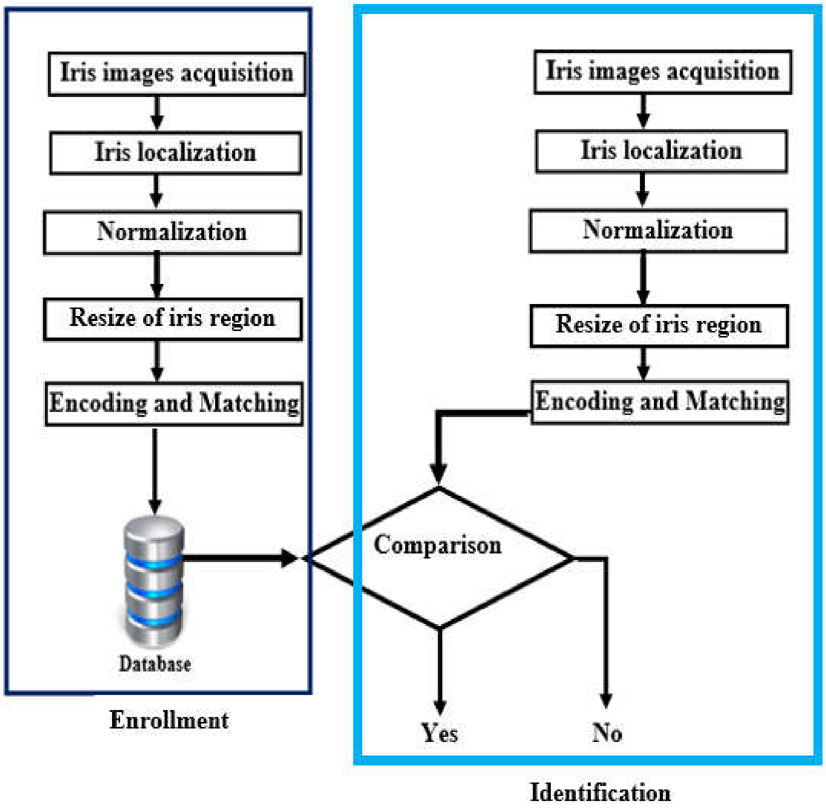


Figure.4. Block diagram for the operation stages of an iris recognition based attendance system.

If there is matching between the new iris image of the user and the data base, then there will be authentication, if not the user must update his data, or that person is not authorized to enter [12, 17]. All stages for the iris recognition attendance system are as shown in Figure 4.

1.2.3.2. Limitation of iris recognition based attendance system

Undoubtedly the most important feature of iris recognition attendance system its stability, since the iris of the eye for all humans be completely formed will all attributes from age of ten months and all these attributes will remain unchangeable until death or accidents. Security. In addition, the possibility of that two persons have the same iris features and details are nonexistent, also the irises of one person are different. But the following limitations still affect its work.

1. The cost. one of the greatest disadvantage is the high cost of iris recognition based attendance system same as face recognition system but its cost is higher because it is needing instruments have accuracy more than those used in face detection system.
2. Unreadable iris. Some students have defects in the eye either because accidents or from birth, and this will make iris detection impossible.
3. Distance. The iris recognition based attendance system is contactless and this is the main important property, but the distance is small and depending on the resolution of the camera used.
4. Stolen texture features. One of the biggest disadvantage of biometric based identification systems which the iris recognition belongs to them is hacking the biometric features. That situation forces the administration extra procedures for encoding, on the contrary, the Barcode and RFID based identification system can easily deal with this problem by replacing the card [18].
5. Delay. Iris recognition attendance system be accompanied with delay because it consists of more than one stage, and each stage is composed from a

number of algorithms. In addition, it requires from all users to be in a queue (one by one) to take the attendance [19, 20].

1.2.4. Fingerprint recognition based attendance system

Because of the increasing in the robberies, fraud, cheating and scams, it becomes a huge necessary to reliable access control mechanisms. With the rapid growth of the digital electronics, most of the countries become directed to the contactless technologies starting from telephones and ending with verification systems. Fingerprint comes from the most reliable and trusted systems, which include attendance authentication and security verification systems. This is because of the robust construction and use, in addition to ease of installation and non-complex running. There are a lot of facilities and foundation which used and they are still widely using fingerprint recognition as an authentication system, among them financial banks, military locations, headquarters for granting passport and universities for academic stuff attendance. The main components of fingerprint recognition system are fingerprint scanner portable of fixed at the entrance and database that is represented by a computer [21]. Recently, number of modifications and developments have been introduced into it either by hardware or software. With regard to software some smart phones became have fingerprint scanner application and for the hardware some fingerprint systems became work wirelessly and other can connect with (GSM) network [22]. Generally, all the fingers of the hands of humans have an exclusive and distinctive properties. These properties are represented by the arrangement of furrows and ridges in the surface of the finger. The identity verification depends on the characteristics of these furrows and ridges. The use of fingerprint as biometric verification system made an urgent need for understanding number of features of the fingerprint patterns [23].

These unique patterns are ridges and minutia as follows;

a. Ridges, they are consisting of lines and spaces called valleys or furrows.

b. Minutia, it represents the whole shape that is containing the ridges. There are some characteristics details of minutia which vary from fingerprint to another. Such as ends of the ridge, bifurcations, dotted or short ridge.

1.2.4.1. Stages of operation of fingerprint recognition based attendance system

The operation of fingerprint based attendance system mainly comprised from five stages as follows:

1. Fingerprint image acquisition. This operation can be done by using one of the following methods such as optical, radio frequency, capacitive, thermal, and ultrasound [24]. The most common method of image acquisition is the optical one, in this method multiple raw images for each finger in the two hands should be taken whenever the finger touches sensor device. These images are representing various wavelengths of the illumination. Each image contains very little information about the fingerprint [21].
2. Image processing for extraction features, in this stage number of sub-operations will be included such as normalization and segmentation, orientation estimation, ridge filtering and smoothing, thinning, binarization. Normalization purpose is for calibrating the intensity of pixilated image of fingerprint. Meaning that the fingerprint image will be divided into a number of blocks, the grey scale variance must be computed for every block in the fingerprint image. The processing on each block depends on the computed value of the variance. With respect to the objective of field orientation of the fingerprint image, which is to define the ridges' local orientations after fingerprint image normalization. The filtering goal is separating background from foreground areas. The objective of binarization operation is comparing all pixels in the filtered image to a saved threshold and after that makes a changes either to a pure black pure white. The purpose of thinning is

reducing the binary values of the fingerprint image into a lines which near from their center lines and the result is a pixelated single line. The fingerprint image resolution will be taken into account when these operations are running [25].

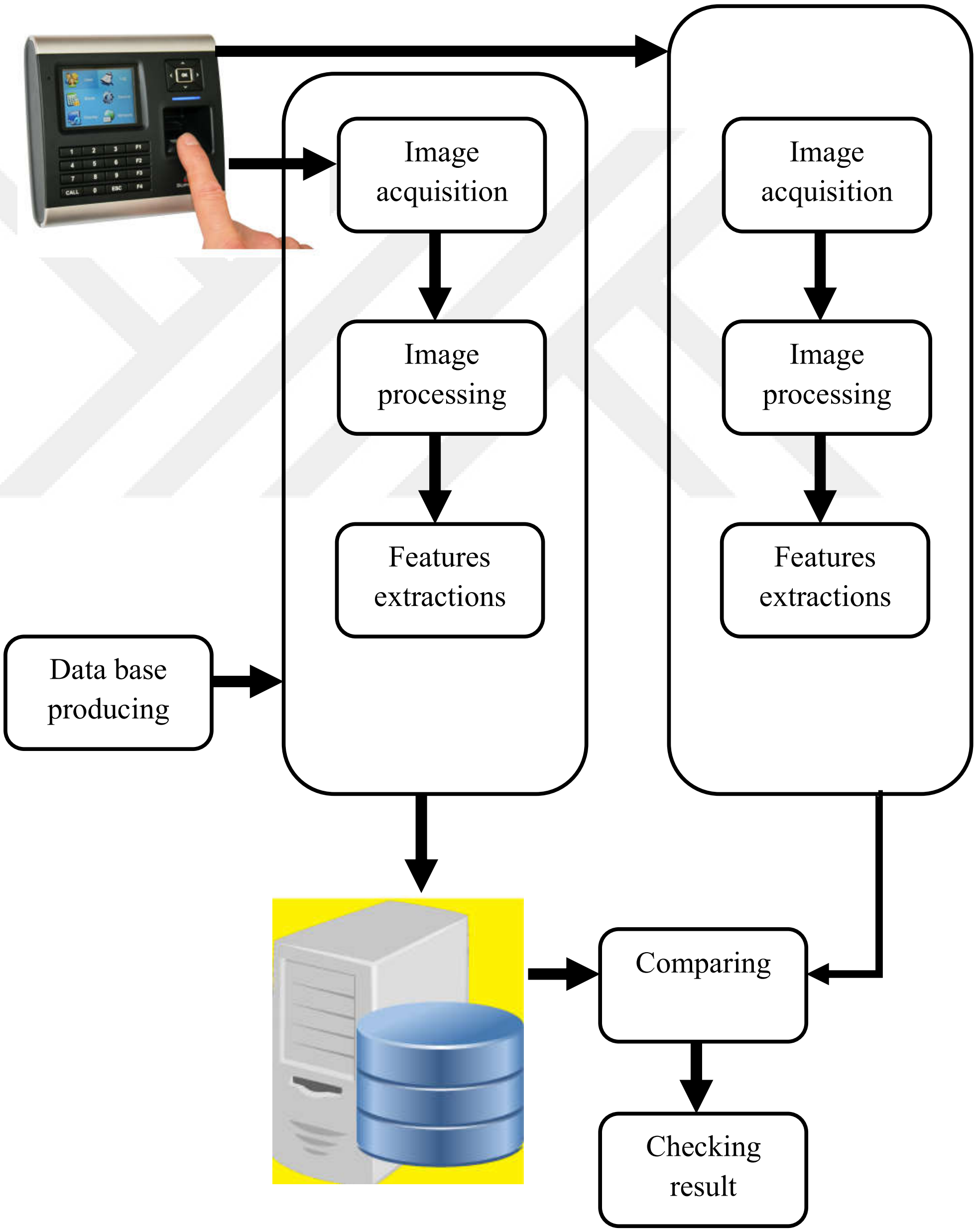


Figure.5. Block diagram of fingerprint recognition system, database producing, checking process.

3. Extraction of finger print features, after the fingerprint image passes the processing stages, the features will be ready to use. These features contain the characteristics of minutiae that must be saved in order to be an identity template for each user in the system in order for the comparison with the new fingerprint image of the same person when he want to take his attendance [21, 26].

The block diagram of the fingerprint based attendance system that involves all main recognition operation will be as shown in Figure 5. Firstly, each user must scan his finger print by the reader, then the captured image is passed to three a processing operations mentioned above and the result will be saved as data base for the user. At each new attendance registration for the user must scan his finger and then be subjected to a checking process by comparison with the information stored within data base.

1.1.4.2. Limitations of fingerprint recognition based attendance system

1. Speed. Fingerprint based attendance system is slow with respect to RFID based attendance system, since it requires from each user registered in the system put his fingerprint on the scan device for reading its information and in this case some problems occur such as the orientation is not precise, or movement of the finger. These problem will extend scan time of each user and a result overall attendance time will be increased [27].
2. Movement support. The fingerprint recognition process does not allow the user to move his fingerprint when the scan is running, because it will fail same as in face recognition and iris and barcode based attendance systems. Meaning successful scan requires contact between user’s fingerprint and the reader.
3. Distance. There is no distance support in the fingerprint based attendance system. The reason is the system requires from the user touches the scan device in order to take his attendance. As a result, all user should be in a queue one by one. In

huge number of users, there is a jostling resulting in overstock leading to disturbance the attendance process.

4. Fingerprint defects. One of the biggest known problem of fingerprint recognition system. It happens because of some skin diseases and infections, or because some accidents, leading to that the scan device cannot distinguish the minutiae correctly [28].

5. Security, the system is effectively secure because there is no possibility of similarity between two different users' fingerprints.

6. Skin diseases. The biggest dangerous drawback occurs when the finger skin is infected by some disease. This situation effects in within two branches, first when there is normal disease (not contagious) but has influences on the fingerprint skin, in this case the fingerprint scan will be effected and the result is inaccurate data. This will make the user re run the scan process in order to get clear fingerprint scan, then there will be delay in the attendance system as shown in Figure 6. The second branch of skin diseases influences is when they contagious, this case will cause risk on the system user and delay in the authentication time.

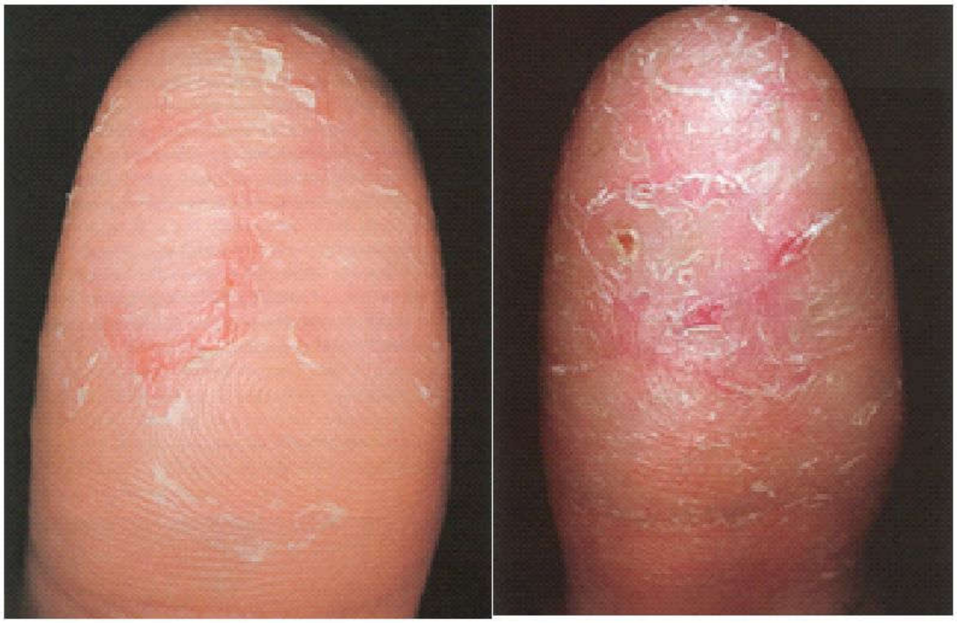


Figure.6. Skin disease affection on fingerprint scan.

7. Some severe conditions. System performance decreases in case of the user has dry finger print (scanning process) especially at low temperature degrees. Some companies were able somewhat overcome this problem by putting a silicon layer on the reader window but they discovered its solidity is less under ponderous use [29].

1.3. Conclusion

Number of attendance systems had been explored briefly in this chapter with their pros and cons. Some of these systems have a good reputation with respect to the security and confidence level such as fingerprint and iris recognition systems, but they are suffering from some crucial obstacles. Finger print system is secure but we cannot guarantee that all users don't have a defected fingerprints due to an accident or diseases, and a line of sight does not enough because it requires finger touch. Also, we cannot deny the security of the iris recognition, but some eye diseases affect the iris recognition accuracy, in some times prevent the recognition. In addition, some users which have myopia or hyperopia are obligated to wear glasses or lenses, which also affect the iris recognition, also the high cost of the system. Face recognition system has also the same handicap of fingerprint and iris recognition systems with regard to the users' defects, and requires a line of sight, and the twins' faces detection is more difficult. Barcode system works just in very small distance of the order of few centimeters and requires a line of sight between the tag and the reader device. In addition, data is easy to damage, in this case an extra cost will must be paid to make new ID cards, as well as it does not supports read and write property, that it means any information written onto it are permanently unchangeable after printing. On the top of that, all the systems mentioned previously they require all users to be in a queue one by one for the succession of authentication, and any movement during scanning will fail the reading process. In addition, all the mentioned systems are requiring a whole time duty watching, this is because the errors can happen at any time during work, leading to an extra delay in the identification process.

In fact, RFID based attendance system could overcome all obstacles that can hinder the speed of operation of the attendance systems mentioned in this chapter, and this is due to the high speed of data transmission, and its security, more details will be in the next chapter.

CHAPTER 2

RFID BASED ATTENDANCE SYSTEM AND ITS MAIN COMPONENTS

2.1. Introduction

In this chapter, the explanation of RFID system is existent, that include firstly a background of the RFID, after that the classification of RFID system with respect to the operation frequency. Then, the RFID system parts which include the reader and tag with its types are explained, which are followed by the RFID system operation in near and far field. Also, number of RFID based students' based attendance system which had been proposed by some researchers in order to replace the traditional students' based attendance system will be mentioned. The section before the last contains the properties of the RFID based attendance system, and the last section contains the conclusion.

2.2. RFID background

In fact, RFID is not contemporary technology. The same principle of current RFID technology was implemented in the second war in (1942) by the British armies. But the way of implementation was different. Since they used the radio frequencies based systems to identify their own crafts from the enemy crafts and this system was known as (IFF) that means ''identify: Friend or Foe''. As well as it used in the sixty decade especially in (1960) in the access control systems which were somewhat similar to the RFID systems in our present time. After this era, in (1970) a numerous claims were existed to introduce the RFID technology in the tracking, particularly for nuclear materials [29]. Number of scientists invited the transponder in the tracked object and the reader such as those in the facilities' entrances. The reader antenna in entrance will sense the incoming vehicle and cars, so if it senses the signal correctly, then it will awaken the vehicle transponder. Then the responded transponder will send data back to the reader which represents the (ID) of the car or vehicle. Another type of tracking was invited by Los Alamos in the agriculturally fields for tracking the cows. The idea for that is to know whether the cow took the medicines or vaccines regularly in the exact time [30]. Even libraries took their share of the use of this system, since they used it for controlling and managing the books' borrowing. By attaching on each book an RFID tag contains all information such as number of borrowings, name of users and time of each borrowing [31]. Also supply chain management has used RFID system to perform all operation of computation and inventory. Shops which used this system provides tags to all their properties and products and reader to read information in the attached tags on it [32]. After that the qualitative change occurred in the use of the RFID technology when it was used for the first time in the attendance systems instead of the traditional systems such as paper sheets, or when they were the most appropriate alternative to the Barcode or magnetic tape based attendance systems. This step opened prospects for innovators and researchers in the fields of developing and enhancing electronic microcontrollers and integrated circuits [33].

2.3. Classification of RFID system

RFID systems are considered as radio systems because they operate using radiation of the electromagnetic waves. Same other radio frequency systems, there are some limitations on its operation field because that some of frequency ranges are used by other systems such as police, industry, security, agriculture, medicine, aviation, and other fields of services. Depending on the information above, RFID systems can be classified as (LF, HF, UHF, Microwave) as in Table 1 according to [34]. The table shows frequency bands boundaries, related coupling type between the RFID reader and tag, and the data rate level.

Table .1. RFID's frequency operation bands.

Frequency band	Frequency range	Coupling	Data rate
LF	125-135 kHz	Inductive	Low
HF	13.56 MHz	Inductive	High
UHF	868-928MHz	Backscatter	Medium
Microwave	2.45-5.8 GHz	Backscatter	Medium

2.4. Main components of RFID system

2.4.1. RFID tag

The first component of RFID system is the tag, main operations inside is storing, transmitting and receiving data using radio frequency waves. Tag is a small electronic circuit attached to the object or thing which must be identified. Tags come in different shapes and sizes depending on the purpose of work and the frequency of operation [34]. The main components of RFID tag are;

1. Antenna; the function of the antenna is tuning between the RFID tag and reader for transmitting and receiving electromagnetic waves signals. The antenna has the electrical conductivity characteristics which allow to electromagnetic waves to propagate between RFID tag and the reader through it. Antenna size determines the distance between the tag and the reader which make the tag activated. The shapes of antenna which used in most of times are rectangular, spiral, planner, and others depending on the operation frequency.
2. Substrate; dielectric material constructed from mixed of chemical substances. The purpose of substrate to give the desired protection to the antenna and the electronic microchip of the RFID tag against weather conditions and external influences.
3. Electronic integrated circuit; main components of tag are the microchip and the transponder. The microchip contains a memory which is responsible for storing

and releasing data. These data represent the tag identifier number which is called tag's (ID). The microchip can support the read/ write property or read only property, this mean the reader can only read data from the tag or can read and write data on tag respectively depending on the field of application and the characteristics of the reader and tag. In addition to the memory the microchip has a microprocessor that performs all computing and processing operation inside the tags as well as controlling the on/ off state of the tag. Figure 7 shows the construction of passive (LF, HF) RFID tag, as can be seen from the figure the electronic integrate circuit which contains microprocessor, substrate, and the antenna and how the (ID) of the tag can be generated when the tag is activated by the reader.

The RFID tag can be readable from a distance depending on the type of the tag and the frequency used.

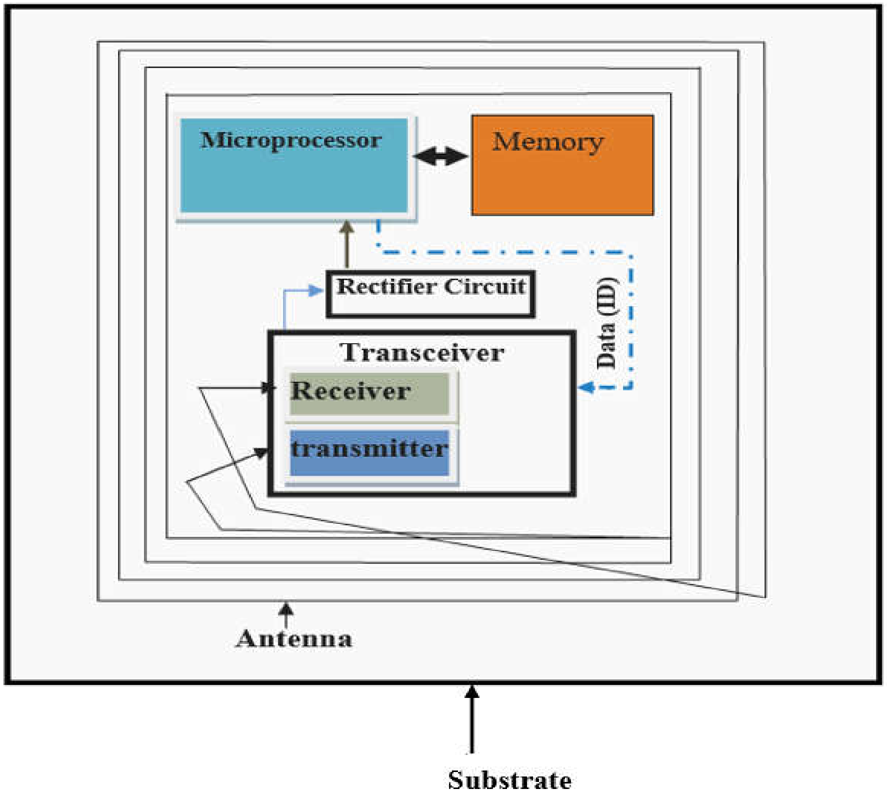


Figure.7. The construction of passive (LF, HF) RFID tag.

This distance ranges from few centimeters up to several hundreds of meters. The reading of the tag by the reader device does not required align of sight (LOS) and contact. Programming the identifier number code (ID) inside the tag can be done using electronic product code (EPG) which is formed as a universal identifier that provides a unique identification process for each object anywhere in the world need to be identified. Sometimes the identification code ID contains the unique serial number of tag or it contains some relevant information such as stocking number, production information as date or expire, and may contain batching number. The exclusivity of tags' performance makes its tracking for moving objects has a significant interest from all companies and facilities [35]. RFID tags in most of time have small size ranges between one square inch to several inches and each size has its complexity and price. The RFID tags exists in different features depending on its electrical operation characteristics, this mean they may be active, passive or semi passive. Active tag can operate without needing the help of the reader with regard to the electric power. Because it contains a small battery inside the electronic circuit of the tag. This battery makes the tag has its independency from the RFID system especially from the reader. Active tags can contact with the RFID reader from a long distances depending on the strength of the electrical power stored inside the battery and the frequency of operation. The life of the active tags is restricted by the life of the battery. The battery of the active tags must be recharged or replaced whenever it exhausted. A lot of application which need the implementation of the RFID does not favor the use of the active tag due to the big size as compared by the semi active or passive tags, or due to the expensive price. For the speech on the semi passive tags, they also contain a small battery for storing electrical power. But the operation does not rely only on the stored energy of the battery only, because other part comes from the radio frequency wave of the reader. By this reason the life of the semi passive tags is longer than that of active tag and the size is less. Depending on the power source third type of the RFID tags is passive which are the most favored and widely used compared with other two types the reason is they does not contain a battery and have unlimited life time. Passive tags are cheaper lighter and smaller than active and semi passive tags, and do not require a period maintenance, but the distance of operation is less and depends on the RFID reader used [36]. Practically, the passive tags return the incident (RF) signal back to the reader device as a response signal. The information represented by the tag (ID) is transmitted after modulation by using the same carrier frequency (CF) of the incident reader signal, and this is done by microchip of the tag. Figure 9 shows the three types of tags mentioned above. Another classification of the RFID tags depends on the frequency of operation [37] as follows:

a. Low frequency tags (LF)

RFID tags which operate in low frequency band (125-135 kHz) have some significant features as follows:

1. Tags that operate in low frequency band (LF) are not influenced by the metallic environment, therefore they can be used in identification and tracking system for vehicles, cars, metallic instruments and others.
2. The reading distance can be range from few centimeters to a meter and this depends on the geometry and the length of the antenna.
3. They do not affect by the water environment and vital tissues, so that they used for tracking animals.
4. They have high prices compared by a high frequency (HF) tags and this is due to the long antenna used in the tag’s circuit.
5. They use a frequency band (125-135 kHz) without any restrictions in all world countries.

b. High frequency tags (HF)

These tags operate in the frequency value of (13.56 MHz) and have properties as the follows:

1. The practical scope of their work is confined to the water and vital tissues and cannot operate in the metallic environment.
2. The thickness of the tag is very small approximately (0.1mm) and manufactured with variable size of antenna.
3. The reading distance is practically ranges around (100 cm).

4. From financial aspect, the price of (HF) tags cheaper than (LF) tags.
5. Their signals cannot interfere with electrical signals coming from induction of electrical devices such as motors, transformers and others.
6. The reader has the ability to read more than one RFID tag at the same time.
7. In the all world the frequency of their operation does not have any limitation.

c. Ultra-high frequency (UHF) and Microwave tags

These tags have significant properties.

1. The reader has opportunity to read large number of tags at simultaneously.
2. Because of the high frequency of operation, the optimum reading distance can be achieved even by using very small antenna.
3. Due to the high frequency used, the (UHF) and Microwave tags can be implemented for identifying high speed objects.
4. Their ability to work in the metallic and liquid environment decreases.

2.4.2. RFID reader

RFID reader is the device capable of reading and retrieving information stored inside the RFID tags. The RFID reader consists of antenna, filters, modulator, demodulator, coupler and a microprocessor. Additional equipment may be used with the RFID reader like (RS 232, RS 485, etc.) to enable the data streaming from the RFID reader to another controlling device to perform necessary processing operations as shown in Figure 8. The RFID reader sends a pulse of radio waves to the tags and listens for its response. The tag detects this pulse and sends back a response which contains the tag (ID) number and possibly other information [38]. In the case of passive RFID tags, the transmitted (RF) signal provides the required electrical power to these tags to modulate their (ID) and transmit it back to the reader whenever they passed the reader's interrogation zone. Because of this the final result signal is suffering from two attenuations. The connection between the reader and the tag is established by the reader antenna. There are some types of reader antennas which differ by the shape and length according to the frequency of operation. The RFID reader can be classified based on the design and technology used (read or read-write) or based on the fixation of the device [39]. The read only RFID reader only reads data from the tags and redirects these data to the microcontroller to perform any required processing.

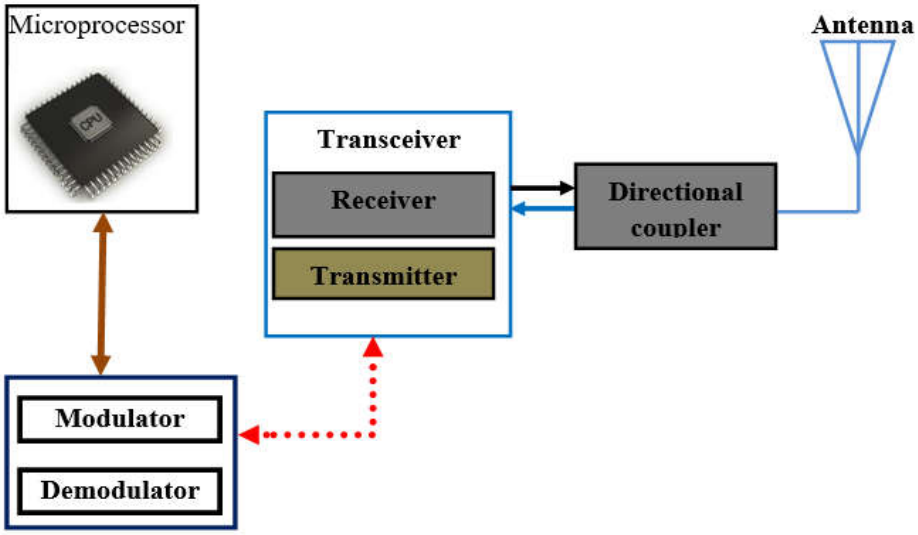


Figure.8. Block diagram of the RFID reader.

The read/write reader reads data from the tags and has the ability to write data onto the tags whenever requested to do so. With respect to the fixation there are two types stationary readers and mobile readers. Stationary readers have fixed location and they are used for identification processes in education institutes, schools [40]. Most of time their locations are in the entrance of the buildings or lecture halls and are passive devices, means that they do not have battery storage. Mobile readers they can perform the identification process of RFID tag within its moving like portable barcode reader device. Because of this they are active devices means that they have their own battery storage. They have a lot of applications like inventory in shopping markets [41], RFID based libraries [31].

2.5. Operation of RFID system in near field and far field region

As was shown in the previous section which talked about the RFID reader, its main parts are the antenna and electronic circuit. Frequency of operation is the main effective factor in the composition of RFID systems' infrastructure represented by the length of the antennas and their geometrical shape in addition to the electronic design of the RFID tag and the reader [42]. The length and geometry of the reader's antenna determine the maximum interrogation zone's distance that if tag passed within can be activated successfully. So that there are two interrogation zone of the RFID reader, first one is near the reader's antenna and the second extends beyond the first one is far field region as shown in Figure 9 which will be explained later.

2.5.1. Near field region

The first interrogation zone of the RFID system is the near field region, which is a few centimeters far from the reader antenna as shown in Figure 9. Communicating between the reader and tags in near field region needs the frequency of operation be under (100 MHz) as in [43]. Operation principle of the near field region absolutely depends on the faraday's law in the magnetic induction. The antenna coil of the reader in this case behaves as primary coil of the transformer and the antenna coil of the tag behaves as the secondary coil. The RFID reader generates an alternating magnetic field in its vicinity by passing a high an alternate current through the antenna coil. When the RFID tag enters the circumference of this region an induced voltage will be across its antenna coil terminals. Then the induced voltage be subjected to rectification and filtering process by using diode and an RC circuit to get a smooth (D.C) voltage (V_T) that used to turn on the tag chip as shown in Figure 10. After the tag chip be turned on it be ready to transmit the tag (ID), data transmission of the (ID) between the RFID tag and the reader depend on the load modulation technique. Expression of this mechanism will be as follows;

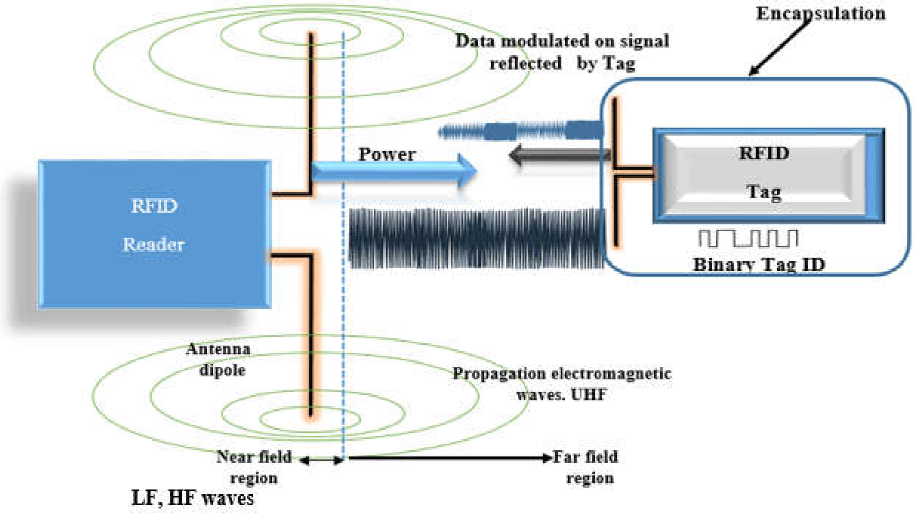


Figure.9. Near field and far field regions.

magnetic field established by the reader will draw current and voltage from it. The reader can measure this additional power consumption remotely as a voltage turbulence that can be sensed at the internal resonant circuit of the reader. Investment of this phenomenon status came by discovering a type of amplitude modulation named load modulation. That needs an additional impedance (Z_L) be applied across the resonant circuit of the tag named load impedance, when (Z_L) increases the current (I_L) across the antenna's coil terminals of the tag decreases leading the current (I_R) in the antenna coil of the reader decreases thus its voltage (V_R) will be at low level. When (Z_L) decreases (I_L) will increases meaning drawing more current (I_R) from the reader that results as a high voltage drop (V_R) on its antenna's coil terminals. It is possible to controlling the value of $(Z_{L)}$ using the electronic circuit of the tag chip to send the digits of the binary tag ID. When the state of the digit is high the value of the (Z_L) is at high value and when the state of the digit is low (Z_L) at low value. The resultant of this variations is variable voltage (V_R) across reader antenna terminals which can be filtered using baseband filter to pick and demodulate the correct signal and removing the unwanted noisy ones. After the demodulation stage, the received signal pass to logical circuit to decide if the tag (ID) belong to the registered IDs list or not as shown in Figure 10. In near field region the communication is restricted by the high frequency values according to the equation (1) as follows;

$$d = \frac{c}{2\pi F} \tag{1}$$

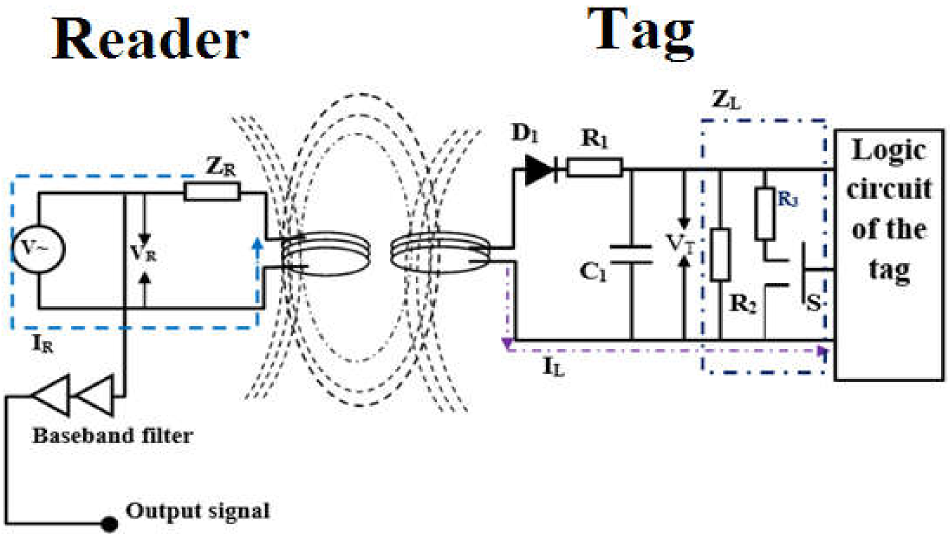


Figure.10. Mechanism of the load modulation.

Where (d) is distance between tag and reader, (c) is the light speed, and (F) is frequency of operation. From the equation above it can be seen that the distance between the reader and tag is proportional to the inverse of (F). So that when there is a necessary to use a high frequency in high speed systems the distance is diminishing. Situation like that push the scientists to invite another modulation type named ‘‘backscattering modulation’’ which will be expressed next.

2.5.2. Far field region

In the identification systems based on the RFID when it requires the distance between the reader and the tag to be longer than (1 m) are considered long range systems. This specification requires from the reader and tag to operate at (UHF) frequencies like (865-915MHz) or even in some times (2.45-5.8 GHz). When the frequency of operation is above (100 MHz) RFID systems operate in the far field region as in Figure 9. Antenna constructed to operate in (LF, HF) unqualified to receive these frequencies because they have very short wavelengths, which is requiring antenna much smaller dimensions and higher efficiency. Backscattering modulation is used by the tag to send its (ID) to the reader when be activated. This type of communication depends on the electromagnetic waves, because the magnetic field strength very little or virtually non-existent beyond the boundary of near field region. According to the nature of an electromagnetic wave when faces any object in its path has half its wavelength it will be reflected back to the source. In the case of RFID systems, the amount of reflected electromagnetic waves from the tag toward the reader are controlled by the cross sectional area of the tag and antenna properties as length and impedance [44]. Figure 11 shows the diagram of typical RFID tag operates in backscattering modulation. Reader transmits power (P_1), RFID tag will receive some portion of the power of transmitted signal as (P_{12}) using dipoles antenna.

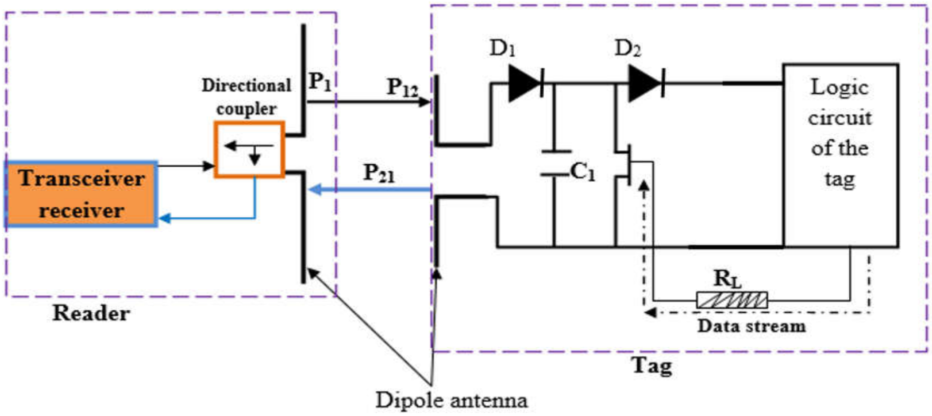


Figure.11. Backscattering operation in the RFID tag at far field region.

The voltage of this power is rectified by using the diodes (D_1) and (D_2) to turn on the tag electronic chip. The other portion of the incoming power (P_1) will be reflected back to the reader using dipoles antenna as (P_{21}). The nature of the reflected power will be affected by the characteristics of the tag's antenna (reflection cross section). Changing the characteristics of the reflected power (P_{21}) be via load resistance (RL) parallel connected with the dipole antenna. This connection is controlled by data stream of the tag (ID) by logical circuit of the electronic chip.

2.6. Some RFID based students' attendance systems and their main components

As mentioned before, the RFID technology can be invested in several various areas, most of which have been briefly stated previously, and the RFID based attendance system in between. This paragraph will be talk about the RFID based (students) attendance system, main components, and possible additions onto it to enhance the performance. Same as other attendance systems in previous sections, RFID came to replace the traditional based attendance systems represented by the paper sheet and calling class names which take a few minutes and are mainly borne by teachers. In this situation, it consumes the teacher time, also does not have any flexibility in generating reports or statistics. Speaking about the RFID as an alternative to traditional attendance system for students, recently a lot of researchers and scientists give a huge interest to that technology. The importance of RFID systems come from its ability to communicate remotely with others parts in spite of barriers, obstacles, walls or even the water. Beside it offers a high speed of processing for all operations performed by these systems and the integration with biometric based systems [45].

Other RFID based students' attendance systems have been merged with ''Global Systems for Mobile communication'' by adding a (GSM) module. This procedure allows to send a message to the parents in order to reassure the student

[46]. The RFID system components are connected to the computer by using (RS 232) hardware to enable any statistics required by the administrator (attendance time, leaving time, number of absences for each student) where the codification of reports be daily, weekly, monthly, or at the end of each semester according to the policy of the university or the institute. The additional monitoring process in that project was performed by the (GSM) module represented by connecting (SIM 300) modem through (RS 232) hardware to the computer. In conjunction with the census operations of the system can send messages to parents to inform them about their student status. Microsoft visual basic was the software of the system to communicate with all its parts.

Other RFID based students' attendance system was integrated with website through the internet service to provide the flexibility of delivering the attendance data since all data be uploaded onto the internet server of the university or institute [47]. The system composed from three main parts which are the RFID reader module, Data reporter module, and web server module. Operation of the RFID components same, tag contains student ID whenever be passed onto the reader, reader take information and delivers it to the processing units. Processing units starts by Data Reporter module which is responsible on bringing all log on data of ID's from the reader every (30) minutes periodically. Then it is passing information into the online server which in turn will register data into the database. Web server module will transfer all information related to the attendance to the internet page of the university or institute according to the instructions. The data inside the online sever is managed by MySQL database management system which represents an open source data base. The personal page of each student is connected directly into the MySQL database. Students' internet pages are designed by using the Hypertext Processor (PHP)scripting language that is suitable with majority of web browsers. The main purpose of automatic access control system based on RFID technology is providing the authorization to legal student or people to take their attendance register and input to the building with official form, in the same time prevent un authorized people from entry. According to such function author in [48] had been designing the RFID based student attendance system with automatic door controlling unit. Its main components are the software and the hardware, software of the system based on the Visual Basic.net for interfacing between the RFID reader and the database. The hardware equipment consists of RFID tag type (UME4100) and reader type SEED (125 kHz), the ATMEL AT89S52 microcontroller for controlling the operation of the reader, computer for database storing, the door unit mainly represented by the motor, the power supply unit, the universal serial bus (USB), USB to serial converter, the (RS232) interface, the universal asynchronous receiver transmitter (UART) and the serial data transmission. The hardware components were designed so that the motor can interface with the database, the graphical user interface (GUI) is responsible for taking information from the reader. The RFID tags were passive meaning that maximum reading distance approximately about (7 cm) because it depends on the rectified voltage coming from the induction field around the RFID reader as in [43]. With respect to the additional property of the designed system represented by the motor control unit. In which RFID reader transmits the (ID) signal of the tag to the microcontroller through the (RS 232) serially, and the microcontroller in turn receives signal and sends it to database to perform necessary processing operation. Then according to the processing results inside database it directs the motor control unit for opening or closing the door for the student.

In [49] proposed a combination between RFID and biometric system represented by face recognition to be attendance system in the university. He used passive RFID tag type (IPC80) that uses (ASK) modulation to transmit ID data to the reader. The reader was installed at entrance door of each lecture hall, operating at frequency was (125 kHz) and maximum reading range was (4 inch). For the face recognition system, he used a web camera type (C500) with (1.3 MP) sensor and video resolution of (1280x1024) pixels. The RFID reader and face recognition camera were connected to a microcontroller type (AT89C52) because its high flexibility in integration with other hardware, ease of programing and does not consume high electric power. It has a flash memory of (8 Kbytes) and internal ram of (256 bytes), eight interrupt sources. Additional equipment was provided to make the designed system more robust such as door lock to prevent any illegal people from entering, and alarm for warning if any un authorized person enters illegally. This attendance system is comprising from two phases; registration phase and authorization phase. In the registration phase, user must stand in front of the camera for taking ten images which be processed to be in his data base together with the ID of the RFID tag. The recognition phase comes after the registration phase when the user represented by the student or any one of the academic staff want to enter the desired place, firstly must pass the ID card (contains the RFID tag) onto the reader then stand in front the camera. If the ID number and the face image are coinciding with the saved user data, the name will be shown on the LCD display as successful attendance else if there is no match alarm will be on as a signal to announce the authority that there is illegal person exists.

In [50] the author proposes student attendance system based on RFID and finger print recognition. The students or teacher must have the RFID identity tag ID and finger print identity ID in order to get permission of attendance record. The system aims to replace manual attendance management represented by the paper sheet or names calling into automatic management attendance system by helping some software such as Microsoft Visual studio2012, Microsoft SQL Server 2012 and C # language in order to run the overall operations inside the proposed system. Two authorized persons can access to the system's contents, the administrator (manager) or user (student or teacher) with specified domain for each one. The eligibility of administrator is summarized in his ability to add, delete, save and update any registration information of any student or teacher. The eligibility of user can give him only access to personal information and attendance registration by the help of administrator. Each user must pass his RFID ID onto the reader and then scan the finger print ID in order to enroll his name in the database of the system. After that the recognition stage, when the user (student or teacher) want to enter the class or institute officially again must pass the RFID ID onto the reader and make a finger print ID scan. Whenever these two ID's are combatable with the user saved

ID's the attendance will be successfully recorded, another case when there is no match the attendance will be rejected. The components of the system were (CR10MRFID) reader for communication with the RFID tag. The operation frequency was (13.56 MHz), means that the system operates at (UHF) band, the maximum separation distance for which tag can transmit ID to reader was (3 m). The RFID tag that used in the system was passive tag, means there is no internal battery storage inside it. With respect to the finger print recognition equipment, he used (ZK 4500) fingerprint reader. All the previous components are connected through USB cable to the database computer to perform any necessary processing and to perform the required function.

The proposed system in [51] was different in some way, since he used a combination between the RFID technology and heart beats detecting for taking the attendance of students in the university or the educational institute. In the RFID based student attendance system, the successful attendance be done when the student tag ID matches the ID saved in the database of the system. When the student has more than one RFID tag, he can take two attendances for him and his friend. The proposed system came to solve this problem by using an RFID watch and reader instead of RFID tag and reader. Each student enrolled in the system must wear the RFID watch around his wrist when he intends to take the attendance. The RFID watch can work in two cases as follows;

1. Normal operation (student wears one RFID watch), depending on the main feature of this watch which is heart beats sensing, the watch will be activated when it is worn around the student wrist. Activation of the RFID watch will enable the RF transmitter to send the ID to the RFID reader. According to the database processing unit the received ID from the reader will be compared with the stored ID, if there is match the attendance will be successful, if the there is no match the attendance will be rejected.
2. Extreme operation (student wears two RFID watches) when trying to take attendance for two names. In this case the RFID reader will give a warning signal that referring to un normal attendance situation, which askes the student to rescan

his RFID ID. By this procedure the proposes system will decrease the cheating cases in the students' attendance.

2.7. Properties of RFID based attendance system

In electronics field or any industry field when some technology takes attention and interest of people researchers off Corse there are a lot of reasons. This is what happened in the case of RFID system since in the recent years it had captured the concern. But we all know that any technology or system come with some features and characteristics some good and others are needing to harness the scientific efforts in order to solve their technical challenges, so the properties of RFID based attendance system will be as follows:

1. Each RFID reader has a controllable reading zone for each tag within the boundaries of this zone, which is provided by a (100%) read rate [52].
2. The orientation or the RFID tag does not affect the transmission of the tag (ID), so that the user or student (in the case of educational institutes) is not obliged to put his (ID) card in a particular direction and in the line of sight as well as in barcode, fingerprint, iris or face recognition systems.
3. The effect of the environment in which the RFID reader and tag are communicating is very small or almost imperceptible [53], this will give the RFID based attendance system a wonderful characteristic such as it can operate in hot and high humidity weather without any performance crippling, this property does not exist in the iris, barcode, face or fingerprint recognition systems.
4. The reading speed of the RFID system exceeds the iris, barcode, face or fingerprint recognition systems by (100) times because the reading time is mere milliseconds while in the aforementioned system takes from one to several seconds.
5. The RFID reader can read multiple tags at the same time if it is provided by collision free property, so when the attendance system be based on the RFID

technology enables ability to take attendance of more than one user (student) without necessary to stand in a queue and wasting time.

6. The RFID reader can receive the tag ID from a distance and even there are some obstacles like wall, metal, human body or else [54]. So, in the case of (UHF) RFID based system the user can register his attendance even he is outside the reader's room by some meters.

7. The information amount that the RFID tag can accommodate are much more than the iris, barcode, face or fingerprint recognition systems since it can carry about (2 kilobytes). Which is enough to represent serial number of the student ID and any related information.

8. The RFID tag has the property of read only or read and write, means that in some RFID based systems if some users left the institute the authority can replace their ID's by another new coming (ID) without needing to buy extra RFID tags [55].

9. The information in the RFID tag is more secure than information in barcode against the environmental conditions, because information in barcode are easy to damage when scratched or be covered by a grease layer [56, 44].

10. RFID system has one problem represented by the collision, the collision problem is divided into two parts. First one is reader to reader collision problem which happens between two or more readers are operating close to each other [57]. Second part of the collision is the tags collision occurs when there is more than one tag communicate with the RFID reader simultaneously [58]. The phenomenon of collision took a great interest from scientists and researchers to solve it in order to enhance the system performance as will be shown in next sections.

2.8. Conclusion

Now days, the identification of things is prevailing and widespread issue, due to the scientific and technological development in various fields of daily life; education, banks, libraries, supermarkets, factories, surveillance systems, access control. These fields became more difficult to be controllable skillfully and completely in traditional systems, so that number of alternatives had been proposed, in between the Radio Frequency Identification (RFID). As an example for the use in the educational field, RFID system had presented the desired activity with respect to speed, control and time management when it used to be a students’ attendance system, but still some problems affect their operations such as collision as mentioned above, that will be explored with more details in the next chapter.

CHAPTER 3

COLLISION PROBLEM IN THE RFID BASED ATTENDANCE SYSTEMS AND ITS SOLUTIONS

3.1. Introduction

In the RFID based attendance system, the colliding tags are degrading the efficiency of the identification process. Due to the importance of RFID technology, number of studies had taken it upon themselves to solve this problem. Firstly, the collision problems in the RFID students' based attendance is explored in this chapter: the RFID tags' collision, and RFID readers' collision are explored and supported by figures, to be clearly understood. In the second paragraph, the tags anti-collision protocols will be explained, that include two types of protocols: tree protocols (binary and query), and aloha protocols with an examples for the operation manners and properties for each one of them. In the last there will be the conclusion of this chapter.

3.2. Collision problem in RFID based attendance system

RFID based system had been widely diffused in various fields of our daily lives very quickly, such as security, production, inventory and so on, this is because the businesslike and practical developments which had been conducted on it especially in the last few decades. RFID based system had been gaining same popularity and spread as well as any RFID based systems, but still there are some snags are standing in its way. Among the most important snags in the way of RFID system is collision problem. If we solve the collision problem, the performance of RFID system when used as students' attendance system will be better than barcode, face recognition, or any of the system mentioned above in chapter 1. The collision problem in RFID system is divided into two gadgetries: readers' collision problem and tags' collision problem. Readers' collision problem occurs when there is more than one RFID reader operate in close, the interrogation signal of one reader will disturb the interrogation signal between another reader and its own tag [57]. For example, when reader 1 is communicating with tag 1, the signal coming from reader 2 will interfere with the signal coming from reader 1 when they arrive at tag 1 simultaneously, so that tag 1 cannot recognize activation signal of reader 1 correctly as shown in Figure 12. In RFID tags collision phenomenon, the situation is different because it happens when there is more than one tag in the interrogation zone of the reader response simultaneously to their reader. In that case the RFID reader can not recognize any of them correctly [58].

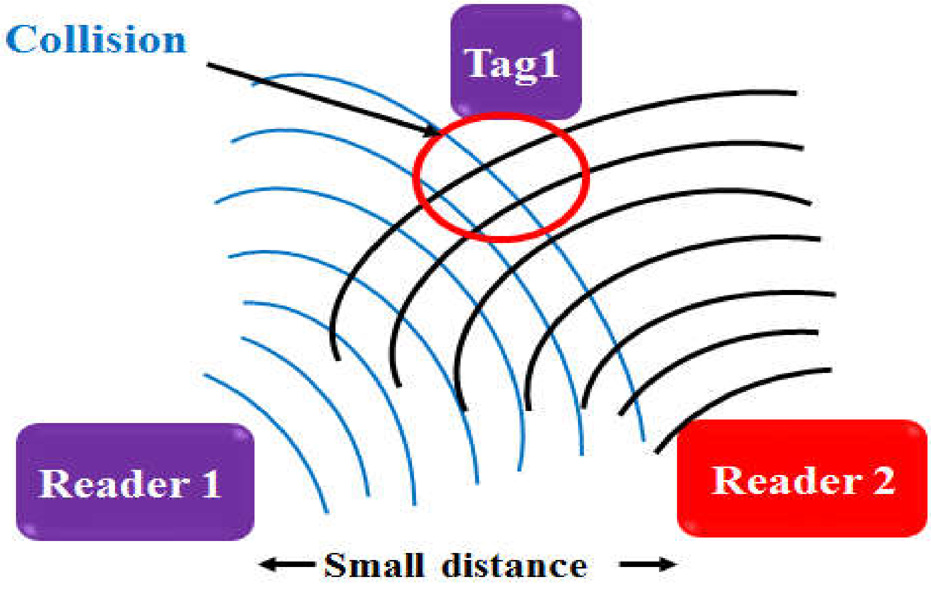


Figure.12. Readers' collision, when there is more than one reader operate in close.

Assuming that there are a five number of tags responding simultaneously to their reader, these tags are (T_1, T_2, T_3, T_4, T_5). After they be activated, the response signal (S_1, S_2, S_3, S_4, S_5) will arrive the reader at the same time, and because of the nature of radio frequency these signals will disturb each other, then the reader cannot recognize any of them correctly as shown in Figure 13. Any one of collision problems of RFID system their effect will be a negative impact the performance of RFID based system whether in terms of speed or accuracy.

Since the subject of this thesis is talking about finding a solution for RFID tags' collision in RFID based students' attendance system, the talk on RFID readers' collision will be limited only the information mentioned above. The next sections will be firstly talk about the related works of RFID tags anti-collision protocol which proposed previously, and then will be the expression of the proposed protocol as a solution to be used in RFID based students' attendance system in the next chapter.

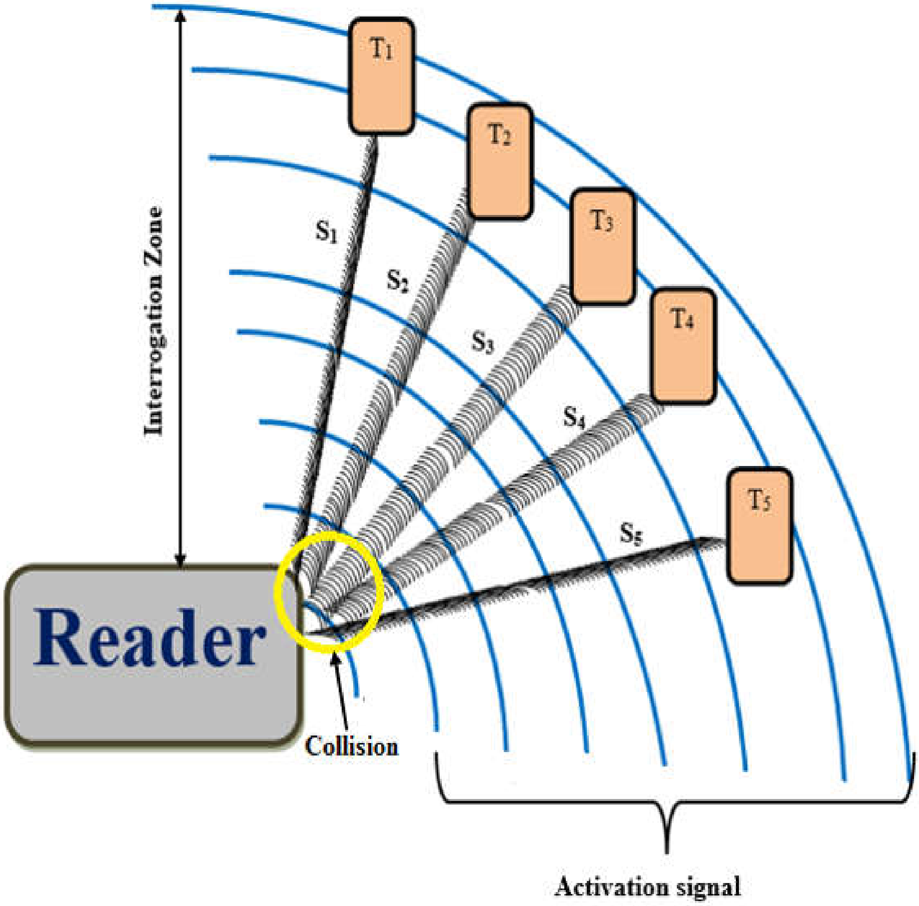


Figure.13. Expression of RFID tags collision problem.

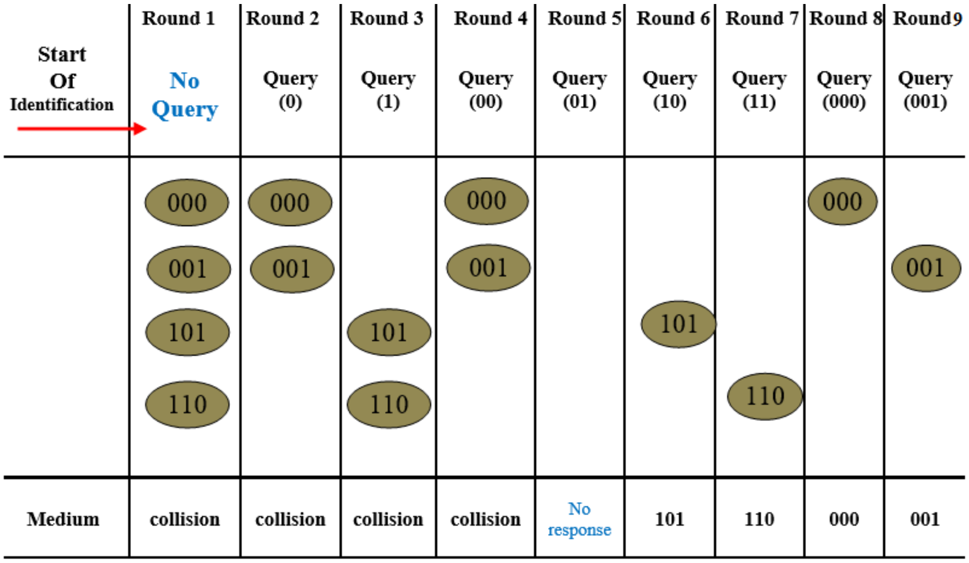
3.3. RFID tags' anti-collision protocols

In the RFID based attendance system, the reader communicates with tags using radio frequency signal through the air as an interface medium. When more than one tag and/ or reader transmits its ID or any data simultaneously in the same data channel, collision will occur and identification process will fail which result in time waste. At this time, the anti-collision protocol became an important part in the (UHF, LF) RFID systems, because of that there are two types of anti-collision protocols: first type for readers and second type for tags. The main objective of tags' anti-collision protocols is reducing the collision by scheduling the ID's transmission for all tags in the interrogation zone of the RFID reader so that each tag will have the same opportunity as its neighbors. In addition, the anti-collision protocol must be capable of detecting the collision occurrence powerfully [58]. Tags' anti-collision protocols are divided into two categories, tree based protocols and ALOHA based protocols and each of them are belonging to Time Division Multiple Access (TDMA).

The tree anti-collision protocol is divided into three types: Query Tree protocol (QT), Binary Tree protocol (BT), and Binary Search protocol (BS).

3.3.1. Query tree protocol

In Query Tree protocol (QT) the identification process is composed from a number of query reading rounds. The RFID reader in each reading round transmits a command directed to the tags called a Query Command (QC). The Query Command (QC) contains a variable coefficient which is named prefix. The prefix is including a combination of binary digits (0,1). Each one these combinations will be exactly similar to one tag (ID) in the interrogation zone of the reader. The role of tags will come after that, each tag around the reader receives query command and then compares its (ID) with the prefix digits. If the prefix matches the tag (ID) then the tag will transmit its (ID), if does not match the tag will wait until another query cycle be transmitted by the reader to send the (ID). At each query around the reader divides the tags into two groups until reaching a group that contains one tag, then this tag responds successfully. The identification a round according to the responded tags may be (Idle, collided, or successful). If the reader does not sense any response will change the prefix and transmit, or the identification process will be end after specific time according to the nature of the installed software of the identification system as shown in Figure 14 [60]. There are four RFID tags with IDs (000, 001, 101, 110) which want to be identified. At first round, they transmit their ID’s without any query, so the collision will occur. In the second round, the reader sends a query with a prefix (0), so two tags responded (000, 001) and collision occurred. The reader in the third round sends a query with a prefix (1), so two tags responded (101, 110) and collision occurred. In the fourth round, the reader inserted additional zero into the query of the second round to be (00), at this stage two tags again responded (000, 001). The query of fifth round was (01), and no response was existing, so this round is (Idle).



	Round 1	Round 2	Round 3	Round 4	Round 5	Round 6	Round 7	Round 8	Round9
Start Of Identification	No Query	Query (0)	Query (1)	Query (00)	Query (01)	Query (10)	Query (11)	Query (000)	Query (001)
	000	000		000				000	
	001	001		001					001
	101		101			101			
	110		110				110		
Medium	collision	collision	collision	collision	No response	101	110	000	001

Figure.14. The procedure of Query Tree protocol (QT) in identification process.

In the sixth round reader inserted query of (10), so only tag (101) responded successfully. Tag (110) responded in seventh round because the prefix of query (11). The eighth and ninth rounds contain (000) and (001) query prefix respectively, and tag (000) and (001) successfully.

3.3.2. Binary tree protocol

The second type is Binary Tree protocol (BT) in which the RFID reader performs a process of splitting the collided tags into a several different sets depending on the randomly generated number in the collided tags. Since each tag has a binary digit generator to produce a pseudo random number in order to decide in which group it will stay and decimal counter with zero initial value. When the identification process starts, the RFID reader transmits a REQUEST code to all tags as a notification of the reading process. Then, each tag will generate a random binary digit (0 or 1). After that, all the tags will add the generated values to their counters, and according to the counter value the tags will be split into two sets, first one is containing (0) and the second is containing (1). All tags which belong to the set of (0) will send their (IDs) directly to the reader and wait response message, and the tags of set (1) will wait. Then the reader performs identification process and send a response message to the two sets (0 and 1). Depending on the response message the tags will increase, decrease, or produce random binary digit (0 or 1) as will be expressed in Figure 15 [59]. The figure contains four tags: Tag A, Tag B, Tag C, and Tag D which they want to transmit their ID’s. The tags will generate a random number and add it to the counter, counter value of Tag A, Tag B, and Tag D equal to zero so they transmit their ID’s in the current reading slot 1. The Tag C will wait another reading slot because its counter value equal to one. In the reading slot 1 as shown there is a collision, Tag A, Tag B, and Tag D again will generate a random binary digit and add it to the counter value. With respect to Tag C, it will increase the counter by one and waits another reading slot. In the reading slot 2 only Tag A and Tag B transmit their ID, Tag C and Tag D will wait another reading slot. According to the message response of reading slot 2 there is a collision, so Tag A and Tag B will generate a random binary digit and add it to the counter. Tag A only will transmit in the reading slot 3, Tag B will wait because its counter value equal to one. Tag C and Tag D will increase their counters by one and wait. The response message of reading slot 3 states that Tag A successfully identified. At this time, Tag B, Tag C, and Tag D will decrease their counter by one and any of them has a value of zero will transmit its ID in reading slot 4. The response message of slot 4 indicates that Tag B successfully read, and Tag C and Tag D must decrease their counters by one, so only Tag D will transmit in the slot 5, finally, only Tag C transmits its ID in the slot 6.

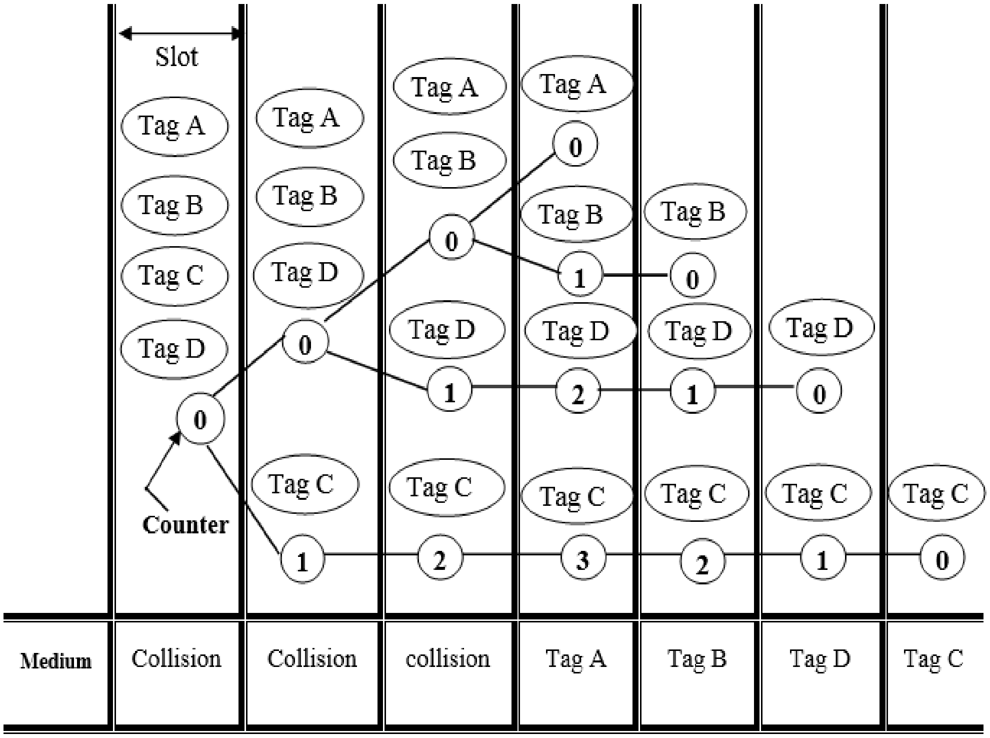
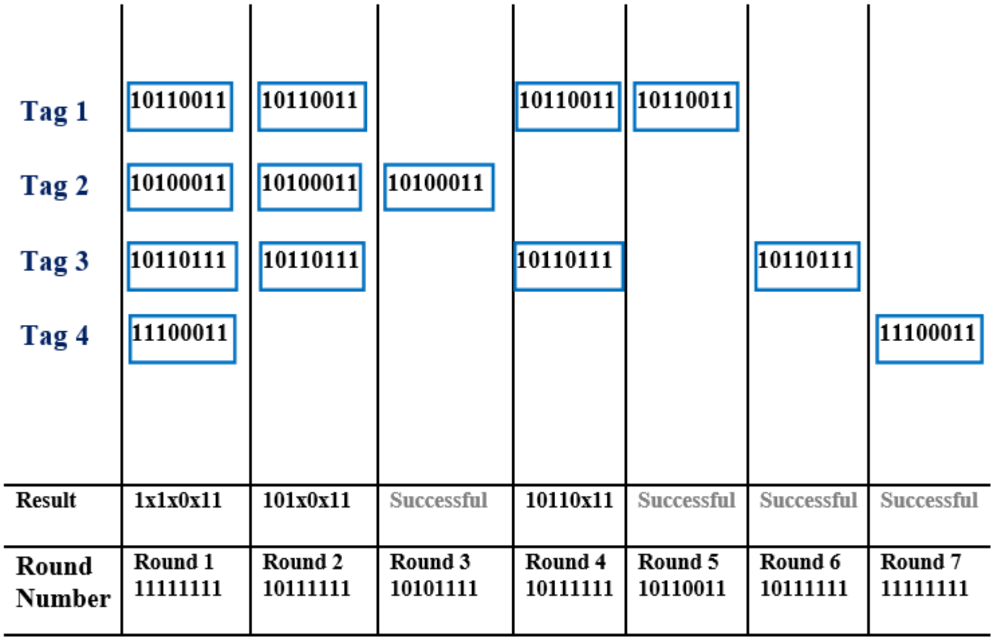


Figure.15. The procedure of identification process in binary tree protocol (BT).

3.3.3. Binary search protocol

The third type of tree protocols is Binary Search protocol (BS), in which the RFID reader decomposes the large group of tags into subsets until reaches to one tag and reads it successfully then put it into muting state. The muting state means that the successfully read tag will be inactive and cannot respond to any reading Request later. Unlike the Query Tree protocol (QT) and Binary Tree protocol (BT), since the reader uses several binary digits' number in each reading round to inform the tags in the interrogation zone to send their ID's. The tags perform a comparison between the transmitted number by the reader and their ID's, if their ID's are equal or less than that number they will send their (IDs), if not they will wait another reading round's Request [62]. Figure 16 shows an example of four RFID tags which want to be identified by the reader using BS anti-collision protocol, and these tags are: tag 1, tag 2, tag 3, and tag 4 with serial numbers (10110011, 10100011, 10110111, 11100011) respectively. The first round begins by sending a reading Request of a number of (11111111), the four tags compared that number with their ID's, then all tags sent their ID's because the result of comparison revealed that the transmitted number is bigger than the ID's. The result of the first reading round was (1x1x0x11), means the collision occurred in the positions marked by (x). At the second round, the reader changed the numbers in the positions that contain (x) from (1) to (0) starting from second position in the left at which the collision had occurred. Then, the reader transmitted (10111111), in this case tag 1, tag2, and tag 3 had responded according to the comparison result. The reader detected a collision at the bits of the positions marked by (x) as (101x0x11). In third round the reader changed (4th) digit from the left by zero, then transmitted the number (10101111), at this time, tag 2 only transmitted its ID, and the reading result was successful transmission. After reading tag 2, the reader will mute it and starts reading round 4 by sending the number (10111111), in that time only tag 1 and tag 3 transmit their ID's, and the collision had occurred at the (2nd) position's bit as (10110x11). The reader in the fifth round had changed the digit of the position marked by (x) in (10110x11) to zero and transmitted the number (100110011), tag 1 had compared that number and transmitted its (ID), then the reader read it successfully and put it into muting. In the sixth round, the reader transmitted (10111111) and only tag 3 responded, so there is no collision, so the tag 3 after reading will go into muting. The number (1111111) was transmitted in reading round 7, and tag 4 only sent its ID so there is no collision, and after reading process tag 4 will go into muting. In spite the guarantee of deterministic identification process, the tree based anti-collision protocols are suffering from a number of impediments in between their implementation costs extra overheads since they require additional big memory inside the RFID tag, that is make its size much larger than the normal size. Also, they require a complicated hardware design with respect to the reader [52]. Moreover, they consume long identification time and have low selection efficiency especially when there is a large number of tags in the interrogation zone of the reader, and when the distribution of tags' ID's around the reader is irregular and scattered [62]. These reasons forced the electronics scientists and experts to go to another anti-collision protocol named ALOHA protocol that will be explained in next paragraph.



Tag 1	10110011	10110011		10110011	10110011		
Tag 2	10100011	10100011	10100011				
Tag 3	10110111	10110111		10110111		10110111	
Tag 4	11100011						11100011
Result	1x1x0x11	101x0x11	Successful	10110x11	Successful	Successful	Successful
Round Number	Round 1 11111111	Round 2 10111111	Round 3 10101111	Round 4 10111111	Round 5 10110011	Round 6 10111111	Round 7 11111111

Figure.16. Identification process for four tags by using the Binary Search protocol (BS).

3.3.4. ALOHA protocol

The second category of RFID tags anti-collision protocols is ALOHA, which as mentioned earlier it belongs to Time Division Multiple Access (TDMA). This protocol is classified as a probabilistic protocol, means that it reduces the probability of collision but not prevents it. Unlike the tree anti-collision protocols, this protocol deals with tags' collision problem in a different way by making each tag in the interrogation zone of the reader randomly transmits its (ID) [63, 65, 66-70]. There are several types of ALOHA protocol, and each type has its features and properties of work with respect to the others, but all the types share a common feature that they use the following commands:

- REQUEST command contains information about frame size and duration of each slot in the frame and it is directed from reader to tags.
- RESPONSE command directed from each tag to the reader contains number of selected slot of every tag around the reader.
- SELECT command directed from reader to tags to inform which tags were read successfully, and which tags should try again transmitting their (IDs).

3.3.4.1. Pure ALOHA

When the anti-collision protocol Pure ALOHA (PA) is implemented in the identification process of the RFID system, all tags in the interrogation zone around the reader device whenever they receive the reading Request command, they send their ID's randomly selected time by using the Response command and wait for a specific time in order to know if they are successfully read. If the reader received the tag ID successfully without any collision, then it sends a message to that tags as an acknowledgement for the succession of the identification, and this can be done by sending the Selected command. The identification process of tags ends when there are no responses. Any tag failed to read successfully during the identification process, it must retransmit its ID again in the continuous time line [63]. However, the pure ALOHA protocol had could minimize the collision problem between the tags, but the probability of successful transmissions in each identification process still small (18%), this is because the partial collision that makes the ID data packet of each tag takes double its duration time to be successfully read. To increase the performance of the pure ALOHA with respect to time and collision avoiding, scientists and experts had directed toward the modification of pure ALOHA by dividing the time into small pieces which are so-called slots [64]. Figure 17 shows an example of three tags are communicating with reader by using Pure ALOHA (PA) anti-collision protocol.

Tag 1 sent its ID at randomly selected time, in the first transmission there is a complete collision because exactly at the same time Tag 3 sent (ID_3), so that the (ID_1) have to be retransmitted again.

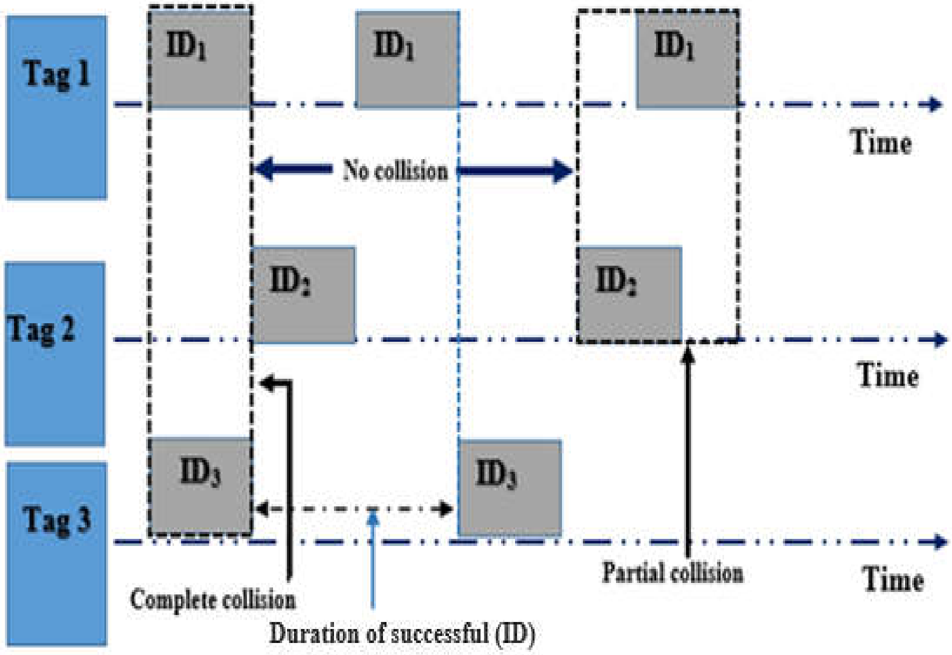


Figure.17. Pure ALOHA (PA): partial and complete collision and duration of successful (ID).

Tag 1 retransmitted its ID and because there is no other (ID) shares its time line, the transmission is successful, and the reader had identified Tag 1. In the second transmission of (ID_1) the empty time interval is twice (ID_1). Tag 2 from the first transmission successfully identified by the reader due to the same reason of (ID_1) succession, but in the second transmission (ID_2) had made a partial collision with (ID_1) because the small time interference. With respect to Tag 3, the first transmission of (ID_3) was failed due to complete collision with (ID_1), but in the second transmission it succeeded.

3.3.4.2. Slotted ALOHA

The Slotted ALOHA (SA) anti-collision protocol is the modified prototype of the Pure ALOHA (PA). In which the reader divides the time into small discrete pieces which are so-called a slots, and each slot must exactly equal the data packet of the tag's ID. In each identification process the reader firstly sends a command to the tags to inform them about the time of each slot and the specific time of the identification (how many slots available). All tags in the interrogation zone of the reader when receive the command of the identification process must so synchronize their IDs' transmission that each ID occupies one slot only [65]. The reader can identify three types of slots:

- Idle slot. This slot does not contain any ID.
- Successful slot. This slot contains only one ID.
- Collided slot. This slot can contain two ID's or more.

Time division of the identification process into slots prevents the occurrence of partial collision, so that the probability of successful transmission in each identification process had rose to (36%). Each ID to be successfully identified by the reader takes only same its time.

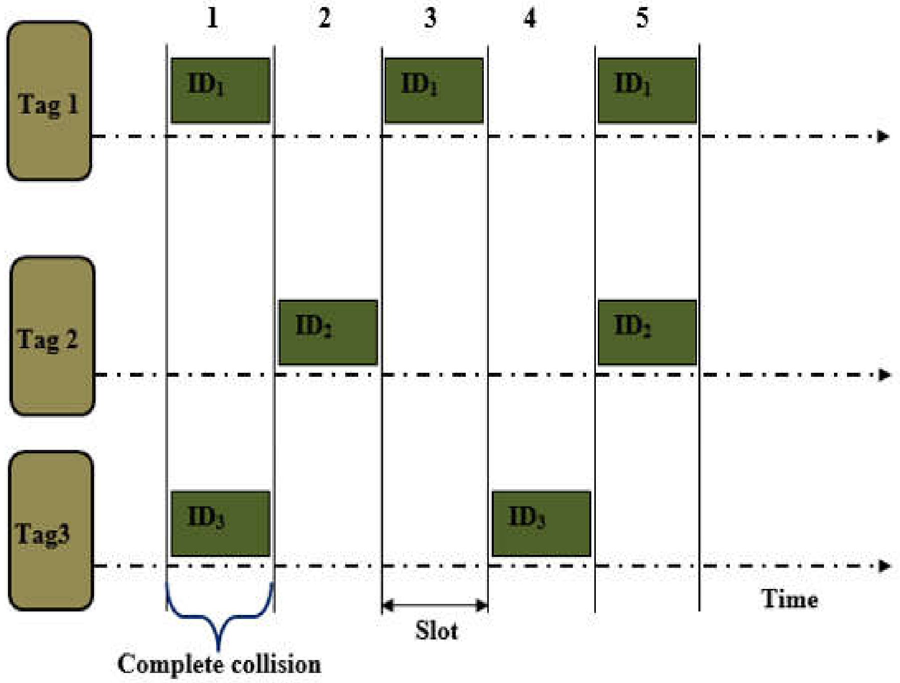


Figure.18. Slotted ALOHA (SA): complete collision and duration of slot (ID).

The tag that failed to read successfully during the identification process, it must retransmit its ID again in randomly selected slot [52].

The elucidation of the implementation of Slotted ALOHA in the RFID system is as shown in Figure 18. Three tags are communicating with reader by using Slotted ALOHA (SU) anti-collision protocol, and the identification time is five slots. Tag 1 sent its (ID) randomly in the first slot, there is a complete collision in the first transmission of Tag 1 because exactly at the same slot Tag 3 sent (ID_3), so that the (ID_1) have to be retransmitted again. Tag 1 retransmitted its (ID) in the third slot and because there is no other (ID), the transmission is successful, and the reader had identified Tag 1. Tag 2 from the first transmission successfully identified by the reader due to the same reason of Tag 1 succession, but in the second transmission (ID_2) had made a complete collision with (ID_1) at the fifth slot. With respect to Tag

3, the first transmission of (ID$_3$) was failed due to complete collision with (ID$_1$), but in the second transmission at the fourth slot it succeeded.

Despite the betterment in the successful transmission probability (36%) by eliminating the partial collision occurrence, but the collision percentage still noticeable, this is because any tag continuo transmitting its ID even if it read successfully by the reader, and this will affect other unidentified tags. This situation is existing in pure ALOHA and slotted ALOHA as can be seen in Figure 17 and Figure 18, so that another features had been implemented on the PA, SA, and on the others types of slotted ALOHA protocols [52]. These features are as follows:

- Muting. In this feature the reader reads any tag in the interrogation zone successful, it sends a command to make it inactive, in order to prevent it from affecting another unread tags in its vicinity. This feature can be applied on PA and SA.
- Early end. In this feature the reader closes any idle slot after a specific time. This feature can be applied only on SA.

3.3.4.3. Framed Slotted ALOHA

The RFID systems that had adopted pure ALOHA and slotted ALOHA are suffering from a time consumption because the tags can transmit their ID’s once at each identification process, and this makes the reader in sometimes repeats the process even there is only one unidentified tag. The Amendment of slotted ALOHA had been coming by dividing the identification process into a number of frames, and each frame is composed from a number of slots [66-68, 70]. Two types of Framed Slotted ALOHA (FSA) are existing, that will be shown in the following sections.

3.3.4.4. Basic framed slotted ALOHA

In Basic Framed Slotted ALOHA (BFSA) the frame size is constant in each reading cycle of the identification process. In each identification process, the reader sends a Request command to the tags as a notation of the beginning of the reading cycle, and information about the size of the frame and slot. The frame size in the framed slotted ALOHA protocol must be {16, 32, 64, 128, 256}, because of the restrictions imposed to the RFID systems [66]. This condition creates a great challenge that is the optimality of frame size. Optimality of frame size means that how the number of slots in the frame during each reading cycle of the identification process can be equal or relatively close from the number of tags in the interrogation zone of the RFID reader. The tags around the reader when receive the Request command, they transmit their ID's in randomly selected slot by using the Response command. There are four types of the BFSA as the following:

1. BFSA with muting.
2. BFSA without muting.
3. BFSA with muting and early end.
4. BFSA with early end.

Figure 19 shows an example of implementation of BFSA with muting in RFID system. There are six tags around one RFID reader. The identification process is composed from two reading cycle with sixteen slots frame size. In the first reading cycle (T1, T2) were collided because they chose the same slot (1), the other tags (T3, T4, T5, T6) were successfully read. At the same time, it can be seen that there are a number of idle slot (2, 3, 4, 6, 7, 9, 11, 12, 13, 14, 16). The successfully read tags in the first reading cycle (T3, T4, T5, T6) will go into muting mode. In the second reading cycle, tags (T1, T2) transmitted successfully and went into muting.

When the RFID tags transmit their (IDs) in each reading cycle, each slot can accept three possible cases: idle, successful, and collided. Bin Zhen [68] had been gave the mathematical expression for the probability of that j tags from all tags (k) around the reader are answering in one timeslot in order to find each number of the three cases as follows:

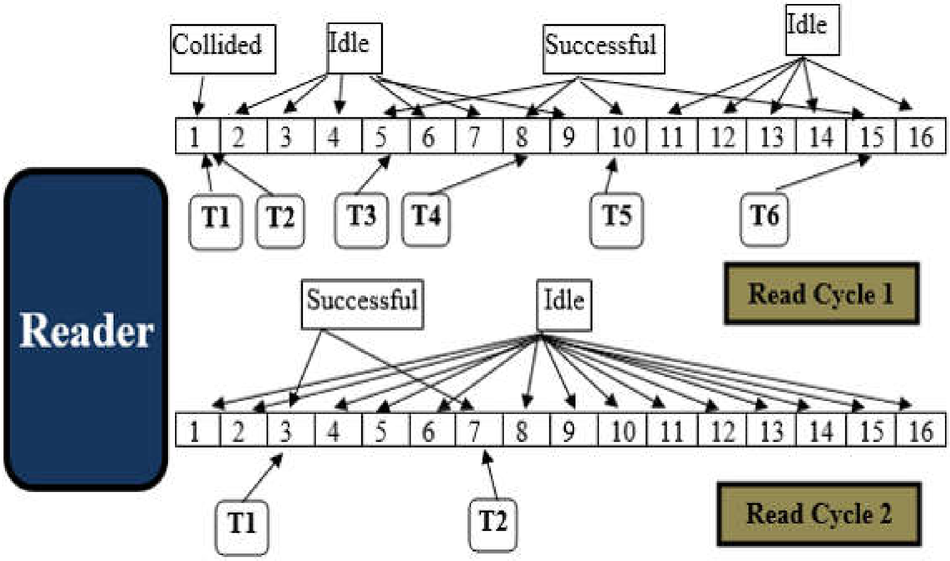


Figure.19. BFSA with muting anti-collision protocol.

Where (L) is the size of frame, and (i) is representing the number of reading cycle in which the tags are responding to the reader.

From equation (1), the probability of having an idle, successful, and collided slots in one frame of the read cycle (i^{th}) will be given by $p_0(i), p_1(i)\ and\ p_k(i)$ respectively:

$$p_0(i) = \left(1 - \frac{1}{L}\right)^k \quad (2)$$

$$p_1(i) = \frac{k}{L}\left(1 - \frac{1}{L}\right)^{k-1} \quad (3)$$

$$p_k(i) = 1 - p_0(i) - p_1(i) \quad (4)$$

Let use ($E_0^{k,L}$), ($E_1^{k,L}$), and ($E_c^{k,L}$) to denote the numbers of idle, successful and collision slots in the frame, according to equation (1) the mathematical expectations of ($E_0^{k,L}$), ($E_1^{k,L}$), and ($E_c^{k,L}$) can be calculated with:

$$E_0^{k,L} = L\left(1-\frac{1}{L}\right)^{k} \tag{5}$$

$$E_1^{k,L} = k\left(1-\frac{1}{L}\right)^{k-1} \tag{6}$$

$$E_c^{k,L} - L - E_1^{k,L} - E_0^{k,L} \tag{7}$$

Since there are (L) slots in each read cycle, we can calculate the probability of having an unread tag after (R) read cycles as [68]:

$$p_{miss}(i) = \prod_{i=1}^{R}\left(1-\frac{L\,p_1(i)}{k}\right) = 1-\alpha \tag{8}$$

Where (R) represents the number of required read cycles to identify a set of tags with a confidence level (α). Because the number of tags (k) and the frame size (L) are the same for all read cycles, $p_1(i)$ remains constant, and we can write the last equation as:

$$p_{miss}(i) = \left(1-\frac{L\,p_1}{k}\right)^{R} = 1-\alpha \tag{9}$$

Solving equation (9) for R:

$$R \geq \left[\frac{\log(1-\alpha)}{\log(1-L\,p_1)}\right] \tag{10}$$

In the ALOHA protocol that has standard specifications when its frame size is (256) slots, the relationship between the mathematical expectations of ($E_0^{k,L}$), ($E_1^{k,L}$), ($E_c^{k,L}$) and the number of answered tags in the frame according to [69] is shown in Figure 20. In this figure, we can see that "when the tags' population increases, the number of collision slots continues increasing and the number of idle slots keeps decreasing, while the number of successful slots, after reaching a maximum value, remains decreasing". The term throughput is usually used to assess effective use of the data channel in collision resolution protocols. For collision resolution of the RFID tags, the throughput of a protocol is defined as ratio between the numbers of identified tags divided by the number of the consumed slots to identify these tags:

$$\theta_{k,L} = \frac{S_1^{k,L}}{L} = \frac{k\left(1-\frac{1}{L}\right)^{k-1}}{L} \qquad (11)$$

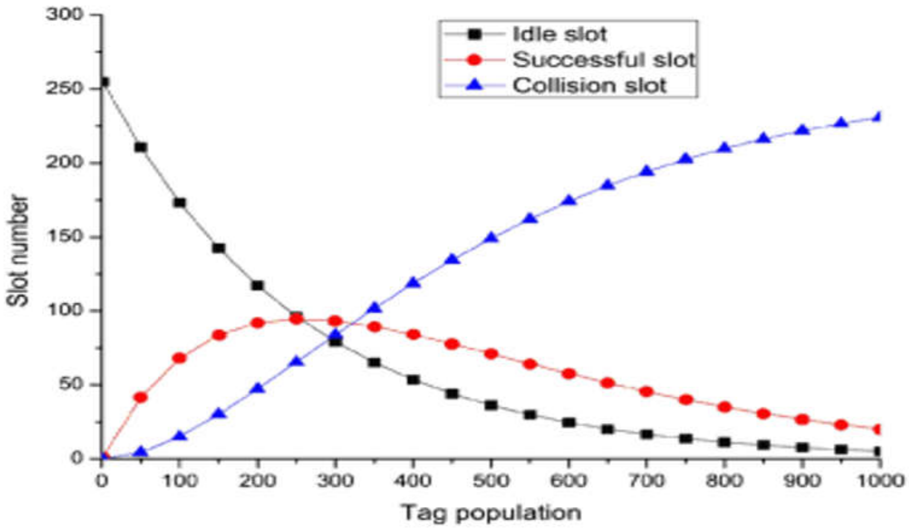


Figure.20. The mathematical expectation of Idle, Collided, and successful slots when the frame size is (256).

The maximum throughput from equation (11) is occurred when the frame size (L) is equal to the number of tags (k) in the RFID reader interrogation zone. The time of each slot in every reading process can be found by:

$$T = \frac{ID_{bits}}{Dr} \qquad (12)$$

Where (ID_{bits}) is the size of tag (ID)'s bits, and (Dr) is the data rate between the reader and the tag and its unit is (bit/sec).

3.3.4.5. Dynamic framed slotted ALOHA

All mathematical equations and features in BFSA stay the same in DFSA, just one difference that is a reader dynamically adjusts the frame size of next read cycle according to results in current read cycle of identification process. Thus, it is important to estimate the number of tags accurately [70]. In the Figure 21 there are twenty tags are communicating with the RFID reader by using Dynamic Framed Slotted ALOHA (DFSA) with muting.

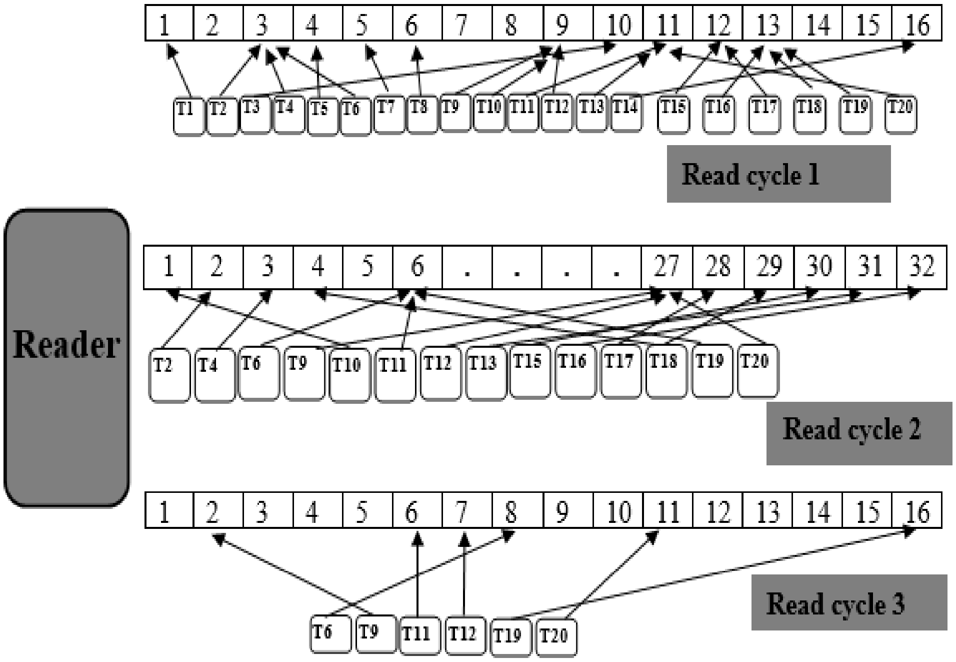


Figure.21. DFSA with muting anti-collision protocol.

There are six tags (T1, T3, T5, T7, T8, T14) were successfully ready by the RFID reader in the first reading cycle, so that they will not respond in the second reading cycle. There are fourteen tags transmitting their ID's in the second reading cycle. Eight tags went into muting mode, and the others (T6, T9, T11, T12, T19, T20) will try in the third reading cycle, and after they read successfully, they will go into muting. Also the frame size in each next reading cycle changes automatically depending on the previous reading cycle result. In DFSA in order to decide the next optimal frame size, the number of unread tags, which is called the collided or backlogged, has to be estimate1d carefully at each frame. In order to estimate the number of the unread tags, Schoute proposed a backlog estimation technique for

DFSA using Poisson distribution [70]. Bin Zhen [67] developed the last technique calculating the remaining backlogged tags:

$$N(i+1) = S + 2.39 * K \qquad (13)$$

Where (K) and (S) represent the number of collided and successful slots in the current frame respectively, and $N(i+1)$ represents the remaining backlogged tags. In [68] chebyshev's inequality estimation method, in this method the procedure to estimate backlog is presented by minimizing the difference between the observed value, including number of idle slots(I), successful slots, collided slots(S), collided slots(K), and the expected values of them ($E_0^{k,L}$), ($E_1^{k,L}$), ($E_c^{k,L}$). The reader need to resolve the equation below:

$$N(i+1) = min \left| \begin{pmatrix} E_0^{k,L} \\ E_1^{k,L} \\ E_c^{k,L} \end{pmatrix} - \begin{pmatrix} I \\ S \\ K \end{pmatrix} \right| \qquad (14)$$

Despite the good enhancement with respect to total slots, time consumption and throughput which have been gained if we apply DFSA or BFSA into RFID based attendance system but still there is wasting in time and low throughput due to the tag collisions phenomenon occurred when students are congregating around the reader register their attendance. Because of those reasons we proposed an anti-collision protocol that will be explained in next section to improve the parameters mentioned above.

3.4. Conclusion

Tags anti-collision protocols are divided into two categories: ALOHA based protocol and Tree protocol. Each one of these anti-collision protocols has its advantages and disadvantages, but the ALOHA anti-collision protocol has advantages more than those of Tree protocol, due to its simplicity and flexibility in programing, and low cost. At this point, the proposed work is depending on the ALOHA protocol as will be introduced in next chapter.

CHAPTER 4

PROPOSED PROTOCOL, RESULTS AND CONCLUSION

4.1. Introduction

The students' attendance in every educational institute of the world plays a significant role in assessment of the education level for student. Number of educational foundations had invested the modern technological development to control the students' attendance through use of the identification systems, RFID system was in between, but the tags' collision problem still affects its identification time. ALOHA and Tree based anti-collision protocols were proposed to overcome the tags' collision. With respect to ALOHA, the studies are continuing to decrease identification time, one of these studies is the proposed work in this chapter.

4.2. Proposed protocol

In order to increase the performance of BFSA, our proposed "predefined BFSA" protocol use multiple frames whose size are equal to the closer multiple of 16 slots instead of using one frame with size equal to the nearest power of 2 (i.e. 16, 32, 64, 128 or 256) as BFSA propose. Table 1 shows how this developed BFSA protocol can overcome the redundancy or shortage of slots when there are an irregular number of tags i.e. not a multiple power of two. For example, in case of a group of 48 tags, we can use combination of two frames whose sizes are 32 & 16 slots instead of using one frame with 64 slots. The condition to make this procedure in BFSA is by making each tag knows at what frame and slot number can send its ID. Figure 22 illustrates the information of Table 1, there are 48 tags want to send their IDs by using predefined BFSA protocol. Tags are divided into two groups: from 1 to 32 will send their IDs in the first frame (F1), while tags from 33 to 48 will send their IDs in the second frame (F2). In addition to the save of slots, IDs require on send in order to be identified by the reader.

Table .2. Slots required for first run “Predefined BFSA”.

Tags’ number	Frame size in **BFSA** (Nearest power of 2)	Required frames in predefined BFSA	Total number of slots in predefined BFSA	Saved slots’ number in predefined BFSA
10	16	**16**	16	**0**
20	32	**32**	32	**0**
30	32	**32**	32	**0**
40	64	**32+16**	48	**16**
50	64	**64**	64	**0**
60	64	**64**	64	**0**
70	128	**64+16**	80	**48**
80	128	**64+16**	80	**48**
90	128	**64+32**	96	**32**
100	128	**64+32+16**	112	**16**
150	256	**128+32**	160	**96**
200	256	**128+64+16**	208	**52**

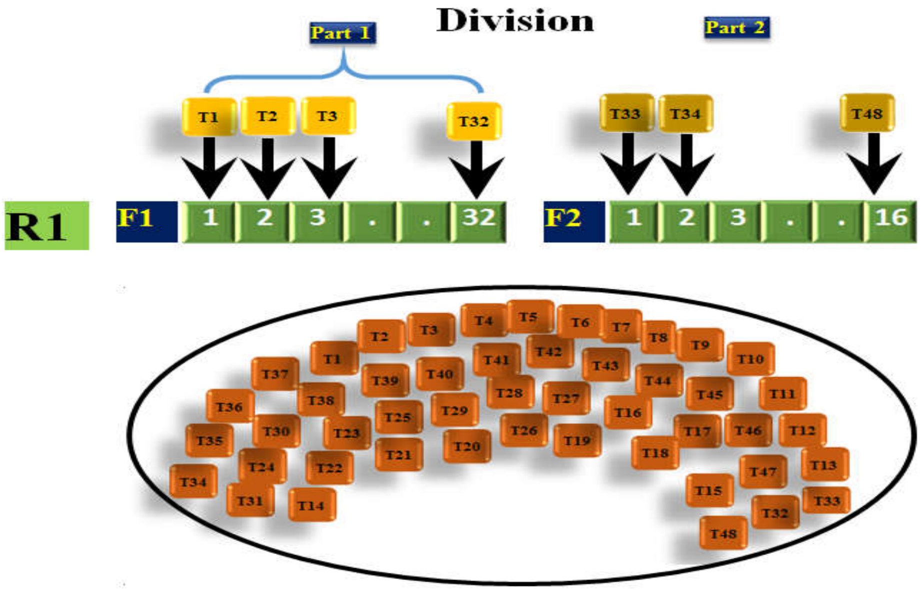

Division
Part 1
Part 2
T1
T2
T3
T32
T33
T34
T48
R1
F1
1
2
3
.
.
32
F2
1
2
3
.
.
16
T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12 T13 T14 T15 T16 T17 T18 T19 T20 T21 T22 T23 T24 T25 T26 T27 T28 T29 T30 T31 T32 T33 T34 T35 T36 T37 T38 T39 T40 T41 T42 T43 T44 T45 T46 T47 T48

Figure.22. An example of identification by Predefined **BFSA** for 48 tags.

Also, in some times using one frame is more suitable for saving time such as in case of 50,60, and other number of tags. In next paragraph, we will explain the implementation of predefined BFSA into the proposed tag and reader's model.

4.2.1. Tag's specifications

The proposed model of tag supports two types of identification runs' commands; first run "predefined BFSA", second run "DFSA". According to these identification runs, **tag** will send its **ID orderly** to a predefined slot and frame number, if it received the **first** run REQUEST command, and if it did not receive the SELECT command of the first run (not identified), it will send it **randomly** to a selected slot and frame number in the second run REQUEST command that operates by DFSA.

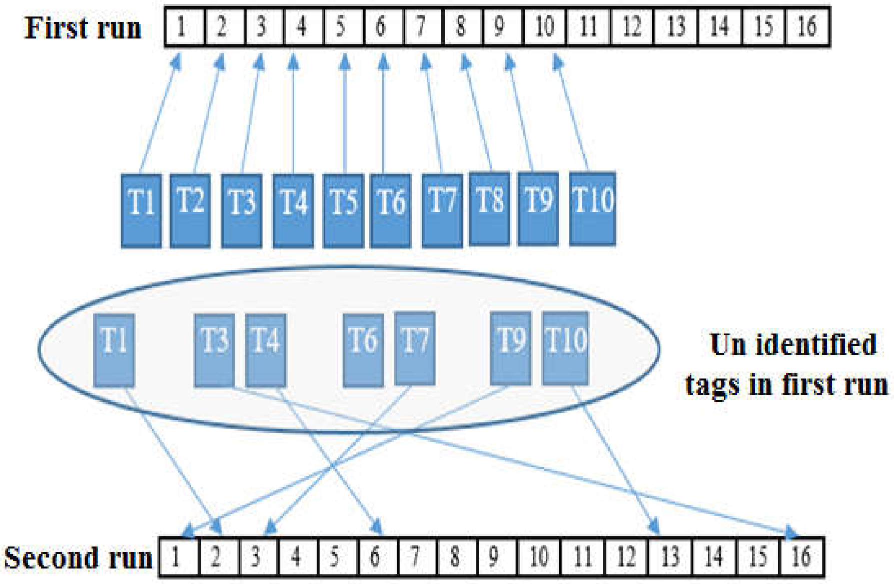


Figure.23. Tags operation in first run and second run of the proposed protocol.

The illustration of these tag properties are shown in Figure 23. In this figure, we can see a sample of ten tags are sending their IDs, as a response to the first mode REQUEST command, but due to the competition or because the miss of first mode REQUEST command, just three of them (T_2, T_5, T_8) were successfully read in the first run, and therefore they went into muting run. Using the second run (DFSA), the other tags (T_1, T_3, T_4, T_6, T_7, T_9 and T_{10}) retransmit their IDs randomly to the selected slot and frame until receiving the acknowledgement from the reader, where they will turn into muting run.

4.2.2. Reader's specifications

As the names and numbers of all students, enrolled in each class, are already known in the attendance system, so reader previously know all tags' IDs numbers that will compete in reading interrogation zone around the reader at each day.

As described in tag's model, reader operates also in two runs; each of them has its reading REQUEST command and SELECT command with a predefined start and end time.

In the first run, using the REQUEST command, reader will scan all registered tags in the database without repeating this identification process. Hence, in the first run, the number of slots is approximately equal to the number of tags registered in the system, and all activated tags, in this run, have their predefined frame and slot number. However, the frame size, which depends on the slots' number, will be equal to a closer multiple of 16 slots as explained before in predefined BFSA.

When finishing the first run, reader will compute the number of unread tags to initiate the frame size for the DFSA by using:

$$T_{m2} = T_{total} - T_{m1} \tag{15}$$

Where T_{m2} represents number of tags that should be identified in second run, T_{total} is the total number of registered tags in the system and T_{m1} is the number of recognized tags in the first run.

In traditional DFSA the identification process should start with frame size of 16 slots, and then it will be changed according to the reading result of each reading cycle. In the second run of our proposed protocol, the situation is different by two points; firstly, the DFSA in the second run is not obligated to start identification process with frame size of 16 slots, and secondly there is no need to waste time by consuming number reading cycles to reach optimal frame size that covers the number of unread tags in first run, because the appropriate size of frame for DFSA will be generated from the beginning of the second run. And this will give advantage of the proposed protocol, because it saves time in the first run and in the second run. In addition, the collision averages will be decreased in first run and second run. Reader will use equation (13) to estimate the unread tags in each read cycle of DFSA in the second identification run. The total slots consumed by each group of tags:

$$S_M = S_{M1} + S_{M2} \tag{16}$$

Where S_M represents the total slots' number consumed during the identification process, S_{M1} number of slots consumed by the first run and S_{M2} is number of slots consumed by the second run. The main idea behind the proposed protocol is reducing the effort on the RFID system used as attendance system, with respect to time and energy and the collisions of tags. Since the interrogation zone of the reader and first run time are limited, at each day there will be a competition from all the students to scan their IDs in the first run, so it is impossible to assume all tags receive the commands of reading REQUEST or SELECT in first run correctly, normally, at any time some of tags be unread in first run. This meaning in a lot of times, there will be two run of operation of the protocol.

The flow chart shown in Figure 24 summarize the identification process, when the system is turn on, reader will start reading ID's tags using first run. After time of first run end, reader will check number of read IDs' tags if they equal to the number of the students' registered IDs' tags in the system then will end reading process without transition to the second run. If there are number of tags still unread in first run, reader will compute initial frame size for DFSA to start second run of reading.

Second identification run will end in two cases if there are no responses for specific time or it reaches end time as expressed by the flow chart.

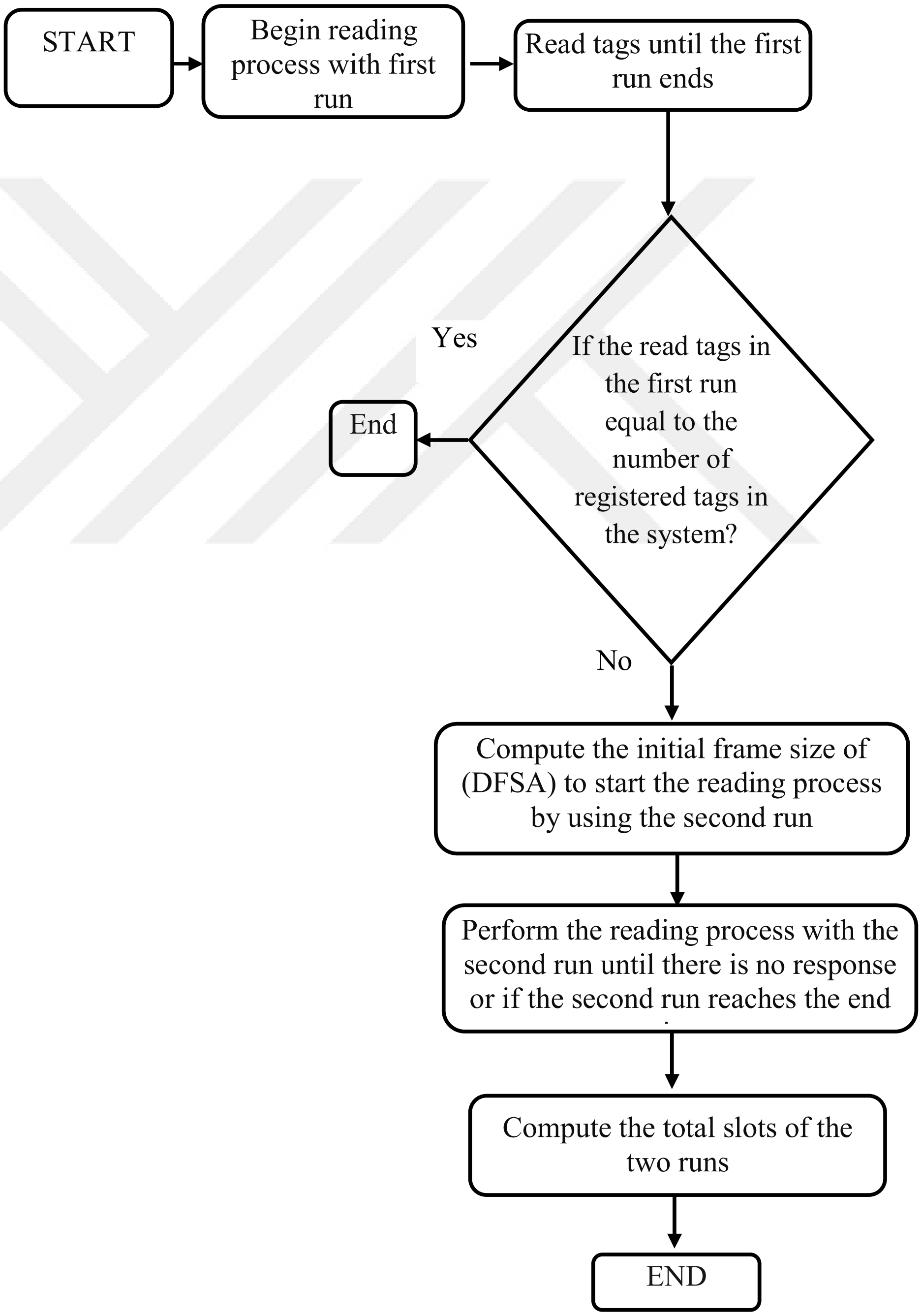

START
Begin reading process with first run
Read tags until the first run ends
If the read tags in the first run equal to the number of registered tags in the system?
Yes
End
No
Compute the initial frame size of (DFSA) to start the reading process by using the second run
Perform the reading process with the second run until there is no response or if the second run reaches the end
Compute the total slots of the two runs
END

Figure.24. The flow chart of the proposed protocol.

4.3. Simulation information

For the purpose of comparison between the proposed protocol and BFSA with and without muting, and DFSA with muting, the number of tags groups will be as following. Tags from (10 to100) by a step of (10 tags), and from (100 to 200) tags by a step (50) tags.

Table .3. Time data for slot and commands in simulation.

Variable	**value**
Confidence level	0.99
Data rate (Dr)	5000,000 (bit/sec)
Duration of single slot (T)	0.00016 (sec)
REQUEST command size (reader→tag)	88 bits
SELECT command size (reader→tag)	72 bits
RESPONSE command size (tag→ reader)	80 bits
REQUEST command time sec	0.000176 (sec)
SELECT command time	0.000144 (sec)
RESPONSE command time	0.00016 (sec)

Regarding to the characteristics of data rate between reader and tags, REQUEST, SELECT, RESPONSE packets, the assurance level, and duration of slot, the simulation depended on the parameters adopted by Prodanoff and Kang as shown in Table 3 [71]. In the simulation, I had applied two cases of operation of the proposed protocol. In first case, I applied first run only, and then I computed the consumption of slots, time and resultant throughput. In the second case, I applied the two runs and the number of tags which were read in the first run using predefined BFSA in each identification process for all tags groups was randomly taken for (1000) identification process, and the average were that (50%) from each group read in first run (predefined basic framed slotted ALOHA), and the rest (50%) remained to be read in second run DFSA. Time in (sec) consumed by each group of tags will be computed according equation (17).

$$t_{consumed} = t_{slots} + t_{com} \qquad (17)$$

Where ($t_{consumed}$) is total time, (t_{slots}) is time of slots and (t_{com}) is summation of commands time in all read cycles required to identify each group of tags.

4.4. Results

The results of simulation are containing the average total slots consumed by each protocol, time in (msec) for each group of tags and the throughput which represents the number of tags that must be identified to the number of consumed slots, in addition to the average of collided slots in each protocol. It can be seen from the simulation results how the total slots consumed by the proposed protocol is lower than from DFSA and BFSA with and without muting. The difference in plots in low number of tags is not clear for example in a group of 10 tags, and when we reach 20 tags the difference is small but noticeable and increases each time the tags increase. The difference reaches its maximum when approaching to a group of 200 tags, with respect to slot consumption in the first run only as compared with DFSA is 70%, while by using the two identification runs the difference is 26%, as shown in Figure 25. Same thing with same style happens to the time consumption plot because consumption low number of slots will decrease the authentication time as shown in Figure 26. The throughput plot shows how the proposed protocol has higher level even at low number of tags in the two cases of simulation, and whenever the tags' number increases throughput increases and achieves higher level of 100% at 80 tags in first identification run, and the difference between it and

DFSA's throughput in most of time is 70%. Also by using the two identification runs, the difference is 20% as compared to DFSA, as shown in Figure 27. As returning to the collision problem in the RFID tags, the average number of the collided slots in each identification process is lower than those of the other three protocol (DFSA, BFSA with and without muting), by using the first run only or using the two runs as shown in Figure 28. Two important things in the Figure 28: first one is that the average collided slots in the DFSA is higher than the BFSA with muting, this is due to the fact that the frame size of the DFSA is not equal the number of tags around the reader from the beginning of the identification process, but it is modified from size to size until it reaches the optimal size to satisfy the desired purposes of consuming low number of slots, the second one is that the average number of the collided slots in proposed protocol by using first run only is zeros for every number of tags, and the reason is predefined BFSA.

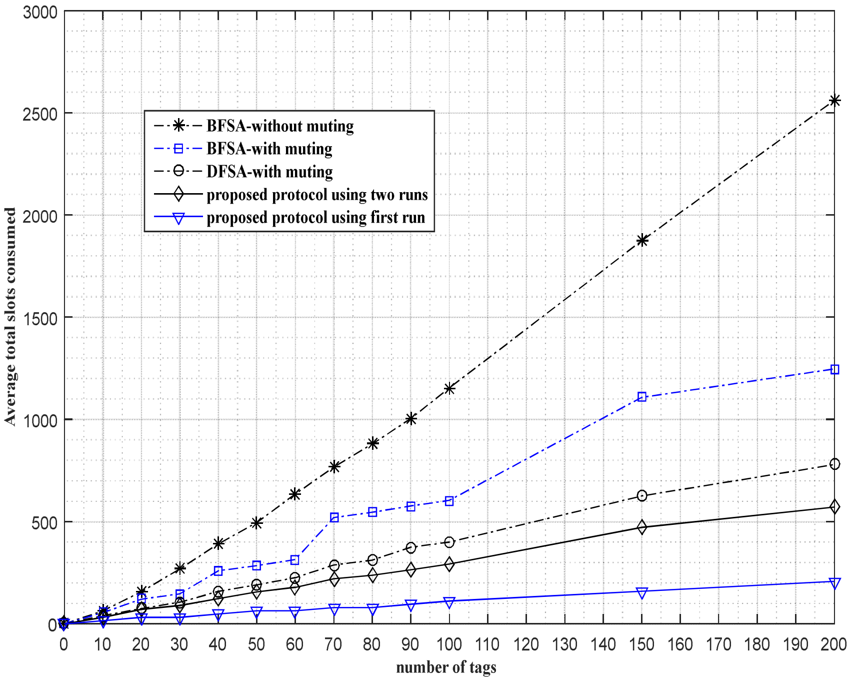


Figure.25. Slots consumption: proposed protocol with first run and by two runs, and DFSA, BFSA with muting, BFSA without muting.

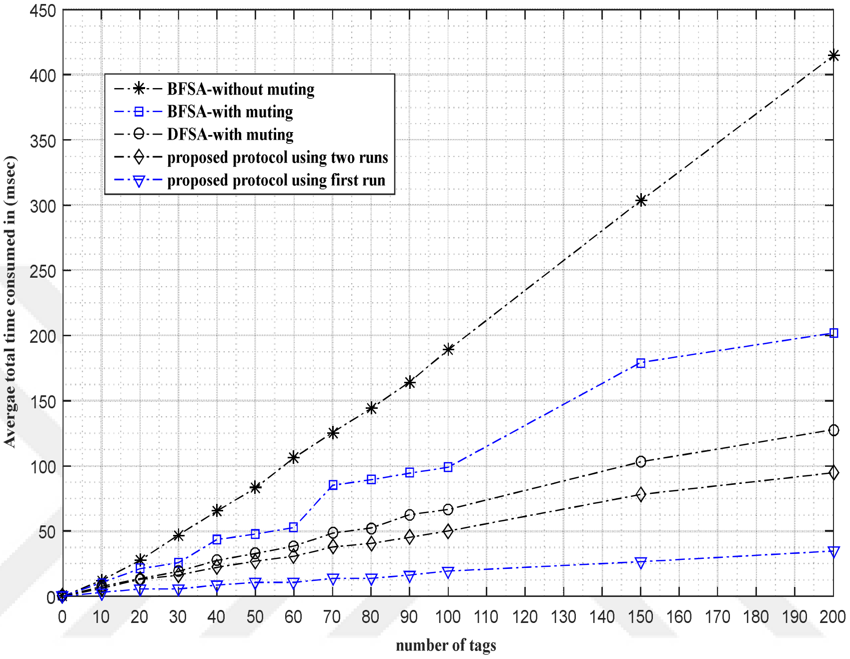


Figure.26. Time consumption: proposed protocol with first run and by two runs, and DFSA, BFSA with muting, BFSA without muting.

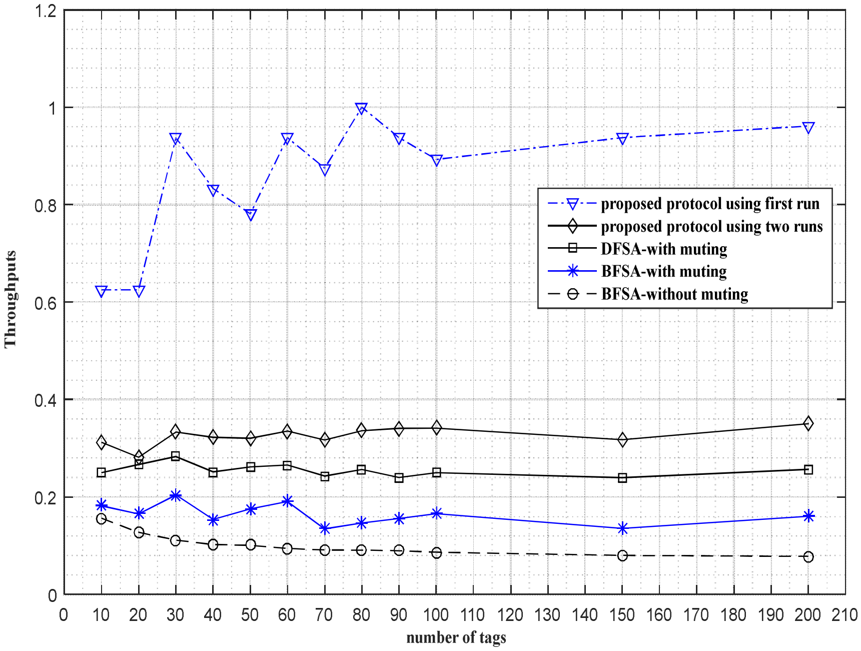


Figure.27. Throughputs: proposed protocol with first run and by two runs, and DFSA, BFSA with muting, BFSA without muting.

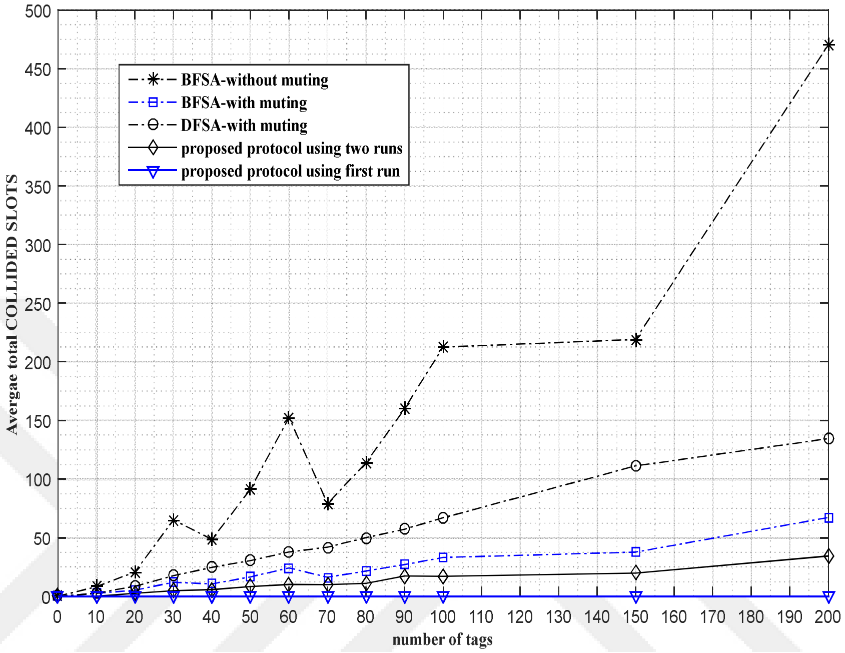


Figure.28. Average number of collided slots: proposed protocol with first run and by two runs, and DFSA, BFSA with muting, BFSA without muting.

4.5. Conclusion

RFID based system had been widely diffused in various fields of our daily lives very quickly, such as security, production, inventory and so on, this is because the businesslike and practical developments which had been conducted on it especially in the last few decades. RFID based system had been gaining same popularity and spread as well as any RFID based systems, but still there are some snags are standing in its way especially tags' collision. For a large number of students in the university that problem will waste of time, and the cause of the RFID tags' collisions is due to overcrowding around reader device. In this thesis, I had developed a new protocol, and when I had applied the proposed protocol, a good enhancement in the slots consumption had appeared. From the results of simulation, it is clear that the number of consumed slots taken by the proposed protocol lower than other protocols (BFSA, DFSA) in two cases. The first case was that all tags be read in first run only, the second case by using two runs together in which I found after taking the average of 1000 identification process that 50% of students' IDs' cards were unidentified in first run. The proposed protocol will save time, and energy even though the RFID reader operates in the first run or it uses the two run, and this is approved by the results of test. Regarding to the throughput, proposed protocol had reached to 100% in first run only, that is higher than DFSA's throughput by 70%, while in two runs together reaches to 35.03%, that is higher than DFSA's throughput by 20%. In addition, the collision of tags had been decreased to lower level as was shown in the results. Also, the proposed protocol can be applied to any company or foundation that depends RFID as an attendance system. If we will make modification on Predefined BFSA, the protocol can be used also in super markets or any inventory places.

4.6. Future works

The proposed protocol indeed had decreases the time and slots consumption, but it needs a modification with respect to Predefined BFSA, since in some cases in the first run, the arriving tags are few may be lower than 20% of total number of tags, and despite of that, the first run continue until its end time. the modification of the proposed protocol can be as the following:

1. I suggest use the Predefined DFSA (changes its Frame according the existence responding Tags).
2. Predefined BFSA with a time segmentation into a 16 slots frame size can be used for any number of tags, in order to overcome the redundancy in slots in first run.
3. As we had seen time consumption difference of the proposed protocol and other protocol increases whenever the number of tags increases, so we can generalize its work to be used in companies or any general foundations and facilities.

REFERENCES

[1]. Sabri E., Gupta A., Beitler M., “Purchase Order Management Best Practices: Process, Technology, and Change Management”, United States of America: J. Ross Publishing. 2006.

[2]. Sudha K., Shinde S., Thomas T., Abdugani A., “Barcode based Student Attendance System”, International Journal of Computer Applications (0975 – 8887); 119: 1-4.

[3]. Roberti M., “Bar-Code Technology is not Cheaper Than RFID”, RFID JOURNAL 2009: 1-2.

[4]. Chen C H., “Handbook of Pattern Recognition and Computer Vision”, 5th ed. Massachusetts, Dartmouth, USA: World Scientific. 2015.

[5]. Kato H., Tan K., Chai D., “Barcodes for Mobile Devices”, United Kingdom: Cambridge University Press. 2010.

[6]. Adrian. R. S., Maulahikmah G., “Implementation of Face Recognition Algorithm for Biometrics Based Time Attendance System”, ICT for Smart Society (ICISS), 2014 International Conference; 24-25 Sept. 2014; IEEE. pp 149 – 154.

[7]. Zhang D., Jain A., “Advances in Biometrics”, United Kingdom, London: Springer Science & Business Media. 2006.

[8]. Li Stan, Jain A., “Handbook of Face Recognition”, 2nd ed. United Kingdom, London: Springer Science & Business Media. 2011.

[9]. Anila S., Dr. Devarajan N., “Preprocessing Technique for Face Recognition Applications under Varying Illumination Conditions”, Global Journal of Computer Science and Technology Graphics & Vision 2012; 12: 13-18.

[10]. Dharavath K., Talukdar F., Laskar R., “Improving Face Recognition Rate with Image Preprocessing”, Indian Journal of Science and Technology August 2014; 7: 1170-1175.

[11]. Jafri R., Arabnia H., “A Survey of Face Recognition Techniques”, Journal of Information Processing Systems June 2009; 5: 41-68.

[12]. Jain A., Ross A., Nandakumar K., “Introduction to Biometrics”, New York, United States of America: Springer Science & Business Media, 2011.

[13]. Uludag U., Pankanti S., Prabhakar S., Jain A., “Biometric cryptosystems: issues and challenges”, In Proceedings of the IEEE 18 May 2004; 92: 948 – 960.

[14]. Xiao Q., “Biometrics—Technology, Application, Challenge, and Computational Intelligence Solutions”, IEEE Computational Intelligence Magazine 07 May 2007; 2: 5-25.

[15]. Bhagat P., Prof. Shilwant D., Prof. Kharde S., Andure A., Prof. Shirsath A., “Iris based attendance system”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) August 2015; 4: 3329-3332.

[16]. Dobeˇs M., Machala L., Tichavsk´y P., Posp´ıˇsil J., “Human eye iris recognition using the mutual information”, International Journal for Light and Electron Optics 2004; 115: 399–405.

[17]. Burge M., Bowyer K., “Handbook of Iris Recognition”, London, United Kingdom: Springer, 2016.

[18]. Singla S., Sethi P., “Challenges at different stages of an iris based biometric system”, Songklanakarin Journal of Science and Technology Mar. - Apr. 2012; 34: 189-194.

[19]. Gupta S., Doshi V., Jain A., Iyer S., “Iris Recognition System using Biometric Template Matching Technology”, International Journal of Computer Applications (0975 – 8887) 2010; 2: 1-4.

[20]. Das P., Bhattacharyya D., Bandyopadhyay S., Kim T., “Person Identification through Iris Recognition”, International Journal of Security and its Applications January 2009; 2: 129-148.

[21]. Maltoni D., Maio D., Jain A., Prabhakar., “Handbook of Fingerprint Recognition”, 2nd ed. London, United Kingdom: Springer Science & Business Media, 2009.

[22]. Saavedra B., Reillo R., Gomez R., Jimenez J., “Small fingerprint scanners used in mobile devices: the impact on biometric performance”, IET Biometrics IEEE 2016; 5: 28-36.

[23]. Darlow L., Akhoury S., Connan J., “Internal fingerprint acquisition from optical coherence tomography fingertip scans”, In: Digital Information, Networking, and Wireless Communications (DINWC), 2015 Third International Conference; 3-5 Feb. 2015; Moscow, Russia: IEEE. pp. 188 – 191.

[24]. Verma P., Bahendwar Y., Sahu A., Dubey M., "Feature Extraction Algorithm of Fingerprint Recognition", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) October 2012; 2: 292-297.

[25]. Shreef S., Sharabaty H., "Biometric Fingerprint Identification System (review)", Turk Hava Kurumu universitesi, Term Project Report, April 2016.

[26]. Hrechak A., Mchugh J., "Automated Fingerprint Recognition Using Structural Matching", Elsevier 1990; 23: 893-904.

[27]. Farooq F, Bolle R, Jea T-Y, Ratha N., "Anonymous and Revocable Fingerprint Recognition", In: 2007 IEEE Conference on Computer Vision and Pattern Recognition; 17-22 June 2007; Minneapolis, MN, USA: IEEE. pp. 1-7.

[28]. Stewart R., Estevao M., Adler A., "Fingerprint recognition performance in rugged outdoors and cold weather conditions", In: Biometrics: Theory, Applications, and Systems, 2009. BTAS '09. IEEE 3rd International Conference; 28-30 Sept. 2009; Washington, DC, USA: IEEE. pp.1-6.

[29]. Rieback M., Crispo B., Tanenbaun A., "The evolution of RFID security", IEEE Pervasive Computing 2006; 5: 62-69.

[30]. Voulodimos A., Patrikakis C., Sideridis A., Ntafis V., Xylouri E., "A complete farm management system based on animal identification using RFID technology", Elsevier March 2010; 70: 380-388.

[31]. Grover P., Ahuja A., "Radio Frequency Identification Based Library Management System", International Journal of Advanced Computer Science and Applications July 2010; 1: 41-45.

[32]. Tang C., "Robust strategies for mitigating supply chain disruptions", International Journal of Logistics: Research and Applications March 2006; 1: 33-45.

[33]. Ahmed F., Abbas S., Singh J., Mishra N., "Students Attendance Monitoring System Based on RFID and GSM Network", Journal of Emerging Technologies and Innovative Research (JETIR) April 2015; 2: 1230-1235.

[34]. Bartneck N., Klaas V., Schoenherr H., “Optimizing processes with RFID”, Erlangen, Germany: John Wiley & Sons, 2009.

[35]. Lehpamer H., “RFID Design Principles”, 2nd ed. USA: Artech house, 2012.

[36]. Kumar S., “Wireless Communications Fundamental & Advanced Concepts”, Denmark: River Publishers, 2015.

[37]. Hunt V., Puglia A., Puglia M., “RFID-A Guide to Radio Frequency Identification”, New Jersey, USA: John Wiley & Sons LTD, 2007.

[38]. M Stephen., Sarma S., Williams J., “RFID Technology and Applications”, 1st ed. United Kingdom: Cambridge University Press, 2008.

[39]. Karmakar N C., “Handbook of Smart Antennas for RFID Systems”, Singapore: John Wiley & Sons, 21 July 2010.

[40]. Shukla S., Shah S., Save P., “RFID Based Attendance Management System”, International Journal of Electrical and Computer Engineering (IJECE) December 2013; 6: 784-790.

[41]. Wang B., Zhuang Y., Li X., “Compact Dual Ports Handheld RFID Reader Antenna with High Isolation”, International Journal of RF and Microwave Computer-Aided Engineering 2014; 25: 548-555.

[42]. Kaur M., Sandhu M., Mohan N., “RFID Technology Principles, Advantages, Limitations & Its Applications”, International Journal of Computer and Electrical Engineering February 2011; 3: 151-157.

[43]. Coskun V., Ok K., Ozdennizci B., “Near Field Communication (NFC): From Theory to Practice”, 1st ed. United Kingdom. John Wiley& Sons Ltd. 2012.

[44]. Finkenzeller K., “RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification”, 2nd ed. United Kingdom: John Wiley & Sons, 21 July 2003.

[45]. Matta V., Moberg C., “The Development of a Research Agenda for Rfid Adoption and Effectiveness in Supply Chains”, Issues in Information Systems 2006; 7: 246-251.

[46]. Singhal Z., Gujral R., “Anytime Anywhere- Remote Monitoring of Attendance System based on RFID using GSM Network”, International Journal of Computer Applications February 2012; 39: 37-41.

[47]. Kassim M., Mazlan H., Zaini N., Salleh M., “Web-based Student Attendance System using RFID Technology”, In: Control and System Graduate Research Colloquium (ICSGRC), 2012 IEEE; 16-17 July 2012; Shah Alam, Selangor, Malaysia: IEEE. Pp. 213 – 218.

[48]. Nwaji O., Onyebuchi N., “Automatic Door Unit Radio Frequency Identification (RFID) Based Attendance System”, International Journal of Science & Emerging Technologies IJSET June 2013; 5: 200-211.

[49]. Farooq U., ul Hasan., Amar M., Hanif A., Asad M., “RFID Based Security and Access Control System”, IACSIT International Journal of Engineering and Technology August 2014; 6: 309-314.

[50]. Thein M., Tun C., Students’ “Attendance Management System Based On RFID and Fingerprint Reader”, International Journal of Scientific & Technology Research July 2015; 5: 30-38.

[51]. Dhanush V., Gnanendra D., Hegde G., “Unique Attendance Tracker Using Heart Beat Detector Based On RF Technology”, International Journal of Combined Research & Development (IJCRD) April 2015; 4: 550-553.

[52]. Stojmenovic I., Simplot-Ryl D., Bolic M., “RFID Systems: Research Trends and Challenges”, 1st ed. West Sussex, United Kingdom: John Wiley & Sons, 2010.

[53]. Nikitin P., Rao K., “Antennas and Propagation in UHF RFID Systems”, In: 2008 IEEE International Conference on RFID; 16-17 April 2008; Las Vegas, NV; IEEE. pp. 277 – 288.

[54]. Golding P., Tennant V., “Evaluation of a Radio Frequency Identification (RFID) Library System: Preliminary Results”, International Journal of Multimedia and Ubiquitous Engineering January 2008; 3: 1-18.

[55]. Wright S., Steventon A., “Intelligent Spaces: The Application of Pervasive ICT”, United States of America (EB): springer, 30 May 2010.

[56]. Karmakar N., “Advanced RFID Systems, Security, and Applications”, United States of America: IGI Global, 2012.

[57]. Zheng F., Kaiser T., “Digital Signal Processing for RFID”, United Kingdom: John Wiley & Sons Ltd, 2016.

[58]. Hsu C., Chen S., Yu C., Park J., “Alleviating reader collision problem in mobile RFID networks”, Springer 17 April 2009; 13: 489–497.

[59]. Law C., Lee K., Yeung Siu K., “Efficient Memoryless Protocol for Tag Identification”, In Proceedings of the 4th international workshop on Discrete algorithms and methods for mobile computing and communications; August 2000; New York, NY, USA; ACM. pp. 75-84.

[60]. Hussain A., Ivanovic M., Electronics, “Communications and Networks IV”, London, UK: Taylor & Francis Group, 2015.

[61]. Shi X., Wei F., Huang Q., Wang L., Shi X., “Novel Binary Search Algorithm of Backtracking for Rfid Tag Anti-Collision”, Progress in Electromagnetics Research B (PIER B) 2008; 9: 97-104.

[62]. Bhochhibhoya R., “Mobile Tag Reading in a Multi-reader RFID Environment”, Pokhara, Nepal; ProQuest LLC, July 2005. Bachelor of Engineering in Information Technology Pokhara University.

[63]. Abramson N., “The ALOHA System: Another Alternative for Computer Communications”, In: The AFIPS Joint Computer Conferences; 1970; Houston, Texas, USA. pp. 281-285.

[64]. Lopez P., Julio C., Li T., “Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID”, United States of America: IGI Global, 2013.

[65]. Metcalfe B., “Steady-state Analysis of a Slotted and Controlled Aloha System with Blocking”, ACM SIGCOMM Computer Communication Review 1975; 5: 24–31.

[66]. Vogt H., “Efficient object identification with passive RFID tags”, In: Proceeding of Pervasive Computing conference 2002; Berlin, Germany. pp. 98–113.

[67]. Zhen B., Kobayashi M., Shimizu M., “Framed ALOHA for multiple RFID objects identification”, IEICE Transactions on Communications 2005; E88-B (3): 991–999.

[68]. Klair D K., Wu Chin K., Raad R., “On the Suitability of Framed Slotted Aloha based RFID Anti-collision Protocols for Use in RFID-Enhanced WSNs”, Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference; 13-16 Aug 2007; Honolulu, USA: IEEE. pp. 583-590.

[69]. Luo Z. “Innovations in Logistics and Supply Chain Management Technologies for Dynamic Economies disseminates supply chain”, USA: IGI Global, 2012. pp.71-74.

[70]. Schoute F C., “Dynamic frame length ALOHA”, IEEE Transactions on Communications. IEEE April 1983; 31: 565–568.

[71]. Prodanoff Z., Kang S., “RFID Model for Simulation Framed Slotted ALOHA Based Anti-Collision Protocol for Muti-Tag Identification”, Current Trends and Challenges in RFID: InTech, 20 July 2011. pp. 280-304.