Negar Khast

Overview of Radio Frequency Identification

Security Issues and Suggesting a Solution

Helsinki Metropolia University of Applied Sciences

Bachelor Degree

Information Technology

Radio Frequency Identification(RFID)

13.02.2017

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Negar Khast Radio Frequency Identification(RFID) 35 12 February 2017
Degree	Bachelor's Degree
Degree Programme	Information Technology
Specialisation option	Telecommunications
Instructor(s)	Anssi Ikonen, Lecturer
Keywords	

Contents

1 Introduction

This thesis studies the architecture of a RFID system and security issues concerning this technology. The goal of the thesis provides a better understanding of this technology and to suggest a solution for its privacy and security problems using a strong symmetric authentication in order to further the development and usage of RFID systems in the near future.

Nowadays, there is a necessity of automatic identification of elements and collecting their related data without the need for human intervention to enter information in many industrial, scientific and social services fields. In response to this need, several technologies have been designed and implemented.

A set of technologies that are used to identify objects, people and animals is called Automatic Identification or Auto ID for short. The goal of most of automatic identification systems is to increase efficiency, reduce errors, entering information and free up staff time to do more important tasks such as better customer service. RFID is one of these technologies that has been implemented in order to make the identification process faster and easier.

Essentially, any system that is able to read and recognize people or objects' information is called an Identification System. In general, automatic identification and data storage is a method in which software or hardware equipment is able to read and recognize data without the help of a person.

Barcodes, two-dimensional codes, finger printing systems, identification systems using radio frequency, identification systems using the cornea of the eye and sound are some examples. One of the most recent topics considered by scientists is Radio Frequency Identification (RFID).

2 Radio Frequency Identification

2.1 History of RFID

The history of recognition via radio waves technology goes back to Faraday's discovery that light and radio waves are both forms of energy in 1864. In 1946 Leon Theremin invented a tool for the government of the Soviet Union that was able to transfer the radio waves caused by any events in the form of sound to the desired location. These sound waves would translate reflection of radio waves into an understandable language by mobilizing the diaphragm that was connected to a vibrator device. This tool is considered as the first RFID-based device, but some of the sources believe that RFID technology was common among the experts since 1920 and has been completed in 1960s.

Another technology that was very similar to RFID is named IFF (Identification Friend or Foe). IFF was invented in Great Britain in 1939 and was used as an efficient tool in World War II in order to make it easier to identify German aircrafts as enemy aircrafts(Figure1). [1]

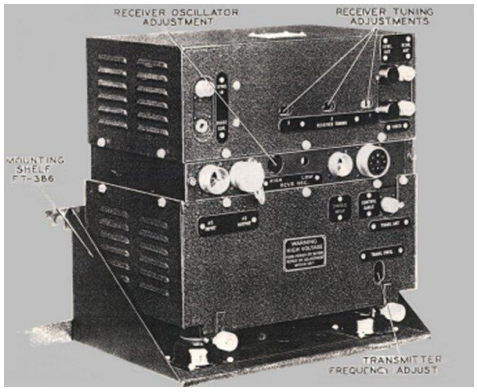

Figure 1. IFF used in WWII. [2]

An American researcher, Harry Stockman, also published an article in 1948 with the title "Communication by Means of Reflected Power" which shows Stockman's vision about RFID before its invention. In recent years, development of this technology sparked a revolution in identification systems. [1]

2.2 Overview of RFID

RFID stands for Radio Frequency Identification and it is the concept of identification through radio frequency. It is a method of transmitting data via radio waves in magnetic fields wirelessly and without contact. This technology is used for automatic identification of, for example, goods, objects, and people. RFID offers an important platform for identification of objects, data collection and management of goods. The platform consists

of a set of data carrier technologies and products that help to exchange data between the carrier and an information management system via a radio frequency link. [3;4]

For example, by using RFID technology it will be possible to exit the shops without having to stand in long lines or even without having to show your purchased items to the cashier. Because the tag on the product is RFID instead of barcode and by sending radio signals to the computers at exit doors, it transmits all its information such as price, weight, and number of items.

These tags consist of a chip and an antenna. The chip releases the information through the antenna, and sensors that are around, receive this information. One of the advantages of this technology is reducing theft, and it is easier to keep track of the number of goods in stock without the help of the human forces. However, it is an expensive technology. [4]

Generally, RFID or identification system by using radio frequency, is a wireless identification system that is able to exchange data by establishing information between a tag that is connected to an object and a reader. RFID systems benefit from electronic and electromagnetic signals for reading and writing data without contact. Tags are identification devices that are attached to the goods which we want to track, and readers detect the presence of the tags in the environment and read the information stored in them. Since this system works based on changes in magnetic waves and radio frequencies, to strengthen environmental signals, sometimes an antenna is also used. [4]

2.3 Principle of RFID Operation

Tag or transponder device, contains an electronic circuit that is attached to an object which needs to have an identification code. When the tag is placed near or within the reader area, the magnetic field generated by the reader activates the tag. Then, the tags continuously send data through the radio pulse. Finally, data received by the reader will be processed by related software such as ERP (Enterprise Resource Planning) and SCMS (Supply Chain Management Systems) (Figure2).

Figure 2. RFID operation. [5]

In general, the RFID system consists of an antenna to scan information, a receiver with a decoder to interpret the information and a transmitter where the information is programmed. The antenna sends radio signals in a short range. Radio emissions establish a communication platform with the sender (RFID tag) and send energy to the tag in order to communicate. This type of RFID tags that do not require any power source can be used for several years. Antenna can be connected directly to the system shell although there are separate antennas. It is also possible to design an antenna into any required shape. For example, it might be installed in a door by which individuals or goods in transit can be identified. [4;6]

When a tag or RFID card passes through working range of an antenna, it detects the activation signal sent by an antenna. This signal activates RFID internal ICs and as a result, the information on tag will be sent to reader.

2.4 Benefits of Using RFID

Both readers and tags can be in different sizes and shapes. Some of the benefits of using RFID technology include:

- Tags can be hidden or embedded in most materials.
- Due to the fact that tags are available in different sizes and shapes, users can choose one of them according to their needs.
- To read the code, tag does not have to be placed under direct vision of the reader.
- Due to the nature of tags (no need for direct contact), there will not be any wear or tear.

- Possibility to manipulate the stored serial codes in the tags will not exist.

Due to the small size of tags and their freedom to move, organizations and institutions that are interested in using this technology, have a high flexibility in this case.

2.5 RFID Applications

RFID technology is used in many office buildings to control the movement of staff in legal and illegal departments. Some applications of RFID technology include:

- Security applications
- Warehousing and stocking goods
- Livestock management
- Controlling entry and exit of vehicles
- Books and libraries management
- Medical and experimental analysis
- Access control
- Controlling the number of rounds. For example, number of rounds a runner should run will be automatically recorded.
- Vehicle identification

A large number of sellers use this technology in order to take care of their products against theft. Some of government agencies also use this technology for monitoring and controlling offenders. [6]

2.5.1 Security Applications

In addition to the specific RFID tags for product tracking and security applications, identification cards and other types of RFID transponders can also be produced. The reader will read the data in identification cards that contain RFID tags as soon as people pass a specific gate. RFID tags embedded in the security bags are considered to be an alternative method to control access to critical information or access to a specific area. [4]

2.5.2 Warehousing and Tracking Goods

When using this technology in commodities and stock control, computers, manage and record data received by readers from tags so that production manager can use this information to always keep the warehouse stock under control. Reader antennas are placed within the warehouse doors to read the data from goods, boxes and pallets

containing tags. RFID price may not be low enough to use RFID tags for variety of products and services, but tags can be used to control small items by attaching tags on boxes that contain them.

2.5.3 Livestock Management

Perhaps it could be said that one of the oldest applications of RFID technology in tracking and control, have been controlling the movement of livestock especially dairy cows. Nowadays, as a quite common process, animals are equipped with this technology by injectable capsules or tags that are attached to their ears. The tags are used to identify lost pets and to sort and taking care of livestock medical records. In recent years this technology has been widely applied in agriculture and medicine. Information about livestock, food and medicine can be very useful in times of crisis for the health of human society.

2.5.4 Controlling Entry and Exit of Vehicles

Another common application of RFID technology is controlling vehicles in places that security of vehicles which enter or exit seems crucial. This system is possible by placing a tag on the vehicle and entering all its information in this device memory. Before the vehicle reaches the entrance or exit, it passes through a place that have an antenna to receive the information from a tag which is attached to vehicle. Reader review the information on tag from antenna and if the information on tag shows that vehicle has permission to exit or enter, gates open. If there is no tag or if the information on the tag indicates vehicle is not allowed to enter or exit, security guards inspect that vehicle. [4]

2.5.5 Books and Library Management

Sticking a tag on a book and placing series of antenna and reader in the library, has the following benefits:

- Prevention of theft of available books
- The implementation of automated return system and even withdrawal of books from the library
- Track and control the correct arrangement of books on their respective shelves

This application of RFID technology is widely used in large libraries. [7]

2.5.6 Medical and Experimental Analysis

RFID technology has very wide applications in medical subject. This interesting technology begins since the entrance of patient in a well-equipped hospital by a bracelet that all information about the patient is placed in that. Record or storing patient information such as name and address, date of admission and hospitalization and type of disease, name of doctor and type of surgery plays a vital role in reducing errors and irreparable damages. Escaping or stealing a patient and switching new-borns seems almost impossible with this technology. Also in drug storage areas, by attaching a tag on drugs, expiration date and the amount that has been used can be easily learned. [7]

2.6 RFID Systems

RFID system can include tag, technology to read the information stored on tags, stimulus servers, software and hardware. The main objective of setting up an RFID system is to receive information of a moving object. This information can be about a person's identity, his location or all of information related to a particular product such as price, colour, production date and expiration date. If an individual or company is planning to install RFID tags on small objects, this can cost them a substantial amount of money. These tiny tags which have a memory chip embedded in them, make a special electronic codes for each object so that the system can easily identify them. A device is located on RFID antennas which is able to change the received information to zero and one code (binary code) and when it is time to read them, convert it to an understandable information. RFID systems can be divided into two general categories; closed systems and open systems. [8]

In RFID closed systems, after attaching a tag on desired product, it goes into the hands of customers and returns again. This type of tag is relatively permanent and have a potential to be in harsh working conditions. Closed system is used where products do not leave the company or organization and they move in a loop, such as CPG cylinders, movie rental and library books. On the other hand, in RFID open systems tracking object is not returnable; thus the tag information will be lost after a while. This type of system is used in postal parcels, fabrics, food and different type of store products. [9]

3 RFID Frequency Spectrum

3.1 Read Range

An important consideration in RFID technology is their operating frequency. Like television that can operate in UHF (Ultra High Frequency) and VHF (Very High Frequency) bands, RFID systems can also use different bands for their communication. Choosing a frequency affects different characteristics of an RFID system that in the following outlines some of them will be discussed.

The first point in choosing RFID tags is to find a balance between the size of a tag and its reading distance. The proper read distance is the same as actual distance between an object that has an RFID tag attached to it and is going to be tracked, and the tag reader. For example, in the RFID application for loading and transportation activities, it is necessary that each truck can be tracked easily within the specified range which is usually a long distance. While in a shop or in any other places that a large number of tags are located next to each other in a small space, long range for reader will cause interference and general list making or selecting a special sample will be difficult. Therefore, when facilities are within walking distance from each other, shorter read range will respond better.

At a low frequency band, read range of passive tags due to poor antenna gain is not more than a meter. At low frequencies, the length of the electromagnetic wave is very high. In some cases, it is up to several kilometres longer than the dimensions of the antenna embedded in RFID tags. Antenna gain is directly related to the size of the antenna with an appropriate wavelength. Therefore, antenna gain at these frequencies is very low. At higher frequencies, the read range usually will increase, especially in cases where active tag is used. Due to the fact that high frequency bands can cause different issues relating to human health, a considerable number of radio regulation agencies such as FCC, apply more restrictions regarding power of microwave and UHF systems. This will cause the read range of high frequency systems in passive tags change to three to nine meters. [4;8]

3.2 Interference from Other Radio Systems

RFID systems are susceptible to interference from other radio systems. RFID systems that operate in LF band are at risk of this damage. LF frequencies cannot tolerate loss due to long distance or very slow wakening in short distances (compared to systems with higher frequency). This means that radio signals of other communication systems that work within the same LF frequency, will have a high field strength in antenna of a RFID reader that can cause interference. At the other side of spectrum, microwave systems

are less potential to interference because the loss is much greater for low frequencies in the microwave band.

3.3 Liquids and Metals

The RFID system performance is affected by damp or watery surfaces. HF signals has better permeability in water and other liquids compare to microwave and UHF signals. UHF shorter wavelengths has more potential to be absorbed in water. This is the reason that HF tags are often used for labelling liquids materials. In such cases, UHF tags can also be used; however, its effective read range will markedly reduce.

Metallic environments have an influence on all of RFID frequencies. Radio frequency signals are not able to pass metals and in some cases that metal material is placed close to reader or tag antenna, behaviour and characteristics of system will face major changes.

One of the common effects of metals on HF and UHF frequencies is changes in the inductance of the antenna, the consequence of which would be reduction of read range. Another effect of metals on both frequencies is absorbing RF energy by metals. Although both types of frequency are not able to penetrate through a metal object, absorption in HF and UHF tags behave quite differently. In HF tags, there is a poor read range, while in UHF tags, read range can be increased in case of an air gap between the metal surface and the UHF tag. In cases where metal material is part of an object that is going to be labelled by an RFID tag, it is better to use metal as an antenna (for example, implementing an air gap between the metal surface and tags). If it was not possible to do that, recap methods should be used.

3.4 Data Rate

In RFID systems that operate in LF band, data rates are as low as a few kilobits per second. Based on the frequency used in the RFID system, data rate can be as high as a couple of megabytes per second which is similar to what has been achieved at microwave frequencies. [4]

3.5 Antenna Size and Type

According to the high wavelength of low-frequency radio signals, antenna of LF and HF systems should be larger than antenna of UHF and microwave systems so that they are

able to receive signals with same quality. This topic is in contrast with the aim of creating RFID tags that are small and inexpensive. This has led many system designers to stop using antenna gain in favour of price control and accept to use HF and LF systems in small areas. LF and HF tags are usually bigger than UHF and microwave tags.

Note that the operation frequency imposes the type of antenna used in a radio system. LF and HF systems use induction and inductive coupling antennas that are usually ring type antennas. In UHF and microwave frequencies, coupling capacitor is used and antennas are dipole. [9]

3.6 RFID Tag Size and Price

Table 1 shows that early RFID systems generally used LF band (due to ease of manufacture). This type of system has its own problems such as the large size of the antenna that could increase their price.

Table 1. RFID systems characteristics in different frequencies.

Frequency band	**LF**	**HF**	**UHF**	**Microwave**
Read range	Less than 62cm	Less than 1m	Between 3m-9m	Several meters
Tag energy source	Generally passive tags	Generally passive tags	Generally active	Generally active
Tag price	Expensive	Less than LF	Has Potential for cheap production	Has Potential for cheap production
Common applications	Tracking livestock	Library	Cargo tracking	Electronic tool collection
Data rate	Slow	Medium	Fast	Very fast
Performance in the vicinity of liquids and metals	Very good	Good	Bad	Worse
Passive tag size	Very large	Large	Small	Smaller

Nowadays using HF band is very common. According to recent advances in technology to make chips, the price of UHF tags is competitive with HF tags. RFID microwave tags are similar to UHF tags; the difference is that they can be smaller and produced at a lower cost.

4 RFID System Components

4.1 Overview of RFID Systems Components

RFID systems use wireless data exchange technology for unique identification of objects, people and animals. The ability of these systems is based on the usage of the following elements(Figure3):

- Tag: that is also known as Transponder, including a semi-conductor chip, an antenna and in some cases a battery.
- Reader: includes an antenna, a RF electronic module and a control module.
- Controller: which is also called Host, it is often a personal computer or a workstation on which databases and application controls have been implemented

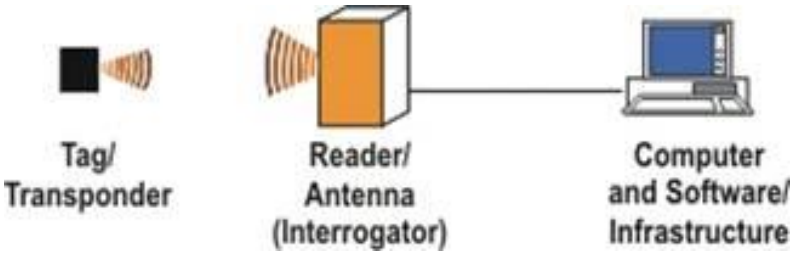

Figure 3. RFID components. [3]

Exchange of information between a tag and a reader is through radio waves. When an object containing a RFID tag enters the reader zone, the reader informs the tag of sending the stored data by sending a signal. Tags are capable of storing various information about an object such as serial number or configuration instructions. After receiving the data stored in the tag, the reader sends the related information to the controller, through a standard interface such as an Ethernet LAN interface or the internet. Then, the controller can use the provided information in various fields. For example, it can use this information to update an existing product in the database or divert an object on a conveyor belt system. [7]

An RFID system may contain numerous readers within a warehouse building or assembly lines. All the readers can be connected to a controller and create a network with each other. A reader can communicate with several tags at the same time. RFID tags can be attached to anything from an infant to a box at the store.

4.2 RFID Tags

Tag is an identification device which is attached to an object, product or a person that needs to be tracked. Each tag consists of two main parts, a chip to maintain and provide memory and an antenna to transmit information. In order to identify a person or an object in RFID systems, a tag needs to be attached to them. In the first step, tag substrate is made of PVC, RET or paper or similar type of material. Then an antenna from a conductive material (to establish radio communication with readers) is placed on top of that and a semiconductor chip will be welded to antenna. Finally, it will be covered with a protective layer(Figure4).

Depending on the type of application, location and needed read range, tag size and price will differ. Therefore, these tags have been designed in various types due to their field of usage. Tags can be classified based on their characteristics such as energy source, frequency range, operation and internal memory.

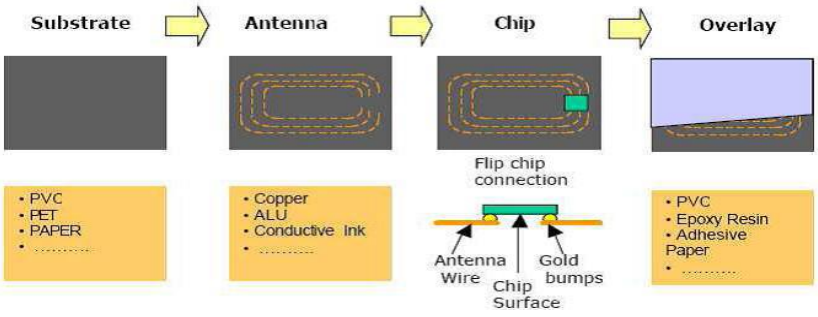

Figure 4. Main components of a RFID tag. [10]

The primary task of a tag is to store data and send it to a reader. In the simplest case, a tag contains an electronic chip and an antenna which are placed in a package together. Chip in a RFID tag uses a read-only or write / read memory in order to store and retrieve data and sometimes to change it. In some tags a battery might be used (the difference between passive and active tags). [7]

4.2.1 Classification Based on Size and Shape

RFID tags can have different sizes and shapes. There are tags with plastic base from PVC material which usually have a hole in centre of them and they are durable and can be used many times. Tags which are similar to credit cards and they are normally called contactless smart cards. Some other tags called smart tags, are made like layers of paper on labels. In addition, there are also tags which work well in environments with a possibility of erosion (like water or liquid). Such tags are placed in cylinders. For public objects such as clothes, watches and bracelets small tags are placed in them. [7]

4.2.2 Classification Based on Energy Source

RFID tags can be divided into passive, active, semi-passive and semi-active group based on their energy source. Passive tags provide their required power and energy from readers by series of transmission methods. Needed energy for active tags is provided by an internal battery and in order to be able to communicate, it has a processor, a memory and a sensor. Tags which are classified as semi-passive, can benefit from transmitted energy by readers in addition to their internal battery. Semi-active tags, in addition to using their internal battery, are able to detect other types of tags and communicate with them without reader.

4.2.3 Classification of Tags Based on Radio Frequency

Generally, radio frequencies are divided into four categories:

- LF (Low Frequency, 30-300 KHz)
- HF (High Frequency) or RF (Radio Frequency, 3-30 MHz)
- UHF (Ultra High Frequency, 300 MHz – 3GHz)
- Microwave > 3GHz

However, in RFID systems, operating frequency range of system should not have interference with other radio equipment. For this purpose, at any level of frequency only a range of frequency is used. Table 2 compares the RFID tags based on their radio frequency. [9,32]

Table 2. Comparison of RFID tags based on the energy source.

Tag type	**Disadvantages**	**Advantages**

Passive	Short read range (about 4m), low performance in vicinity of liquids and metals, usually has read-only memory	Low price, small size, long lasting, wide application range, high flexibility
Semi-passive	High price, shorter life, bigger size, because of battery usage is not widely used	Read range between 4 to 50m, ability to connect to sensors and transfer information, bigger memory, better for identifying large objects
Semi-active	High price, shorter life, bigger size, because of battery usage is not widely used	Read range between 4 to 50m, ability to connect to sensors and transfer information, bigger memory, better for identifying large objects
Active	High price, shorter life, bigger size, because of battery usage is not widely used	High read range (more than 1000m), ability to connect to sensors and transfer information, bigger memory

a) LF frequency range which is used in RFID systems, is between 125 to 134 KHz. In this range, the reader's speed of reading information is low, read range is short (about 3 meters) and it is mostly used for tracking livestock and access control.

b) HF or RF frequency range in RFID systems is between 13.553 to 13.567 MHz and reader reads the tag information with an average speed. This frequency range also has a short read range (about 1 meter) and it is generally used for applications like library management and smart cards.

c) UHF frequency range in RFID systems varies based on each country's standards (Figure 5). For example, in the USA, the reader's reading speed is high and read range is about 3 meters for 900-950 MHz and 90 meters for 433 MHz This is used for applications such as tracking pallets, and trucks.

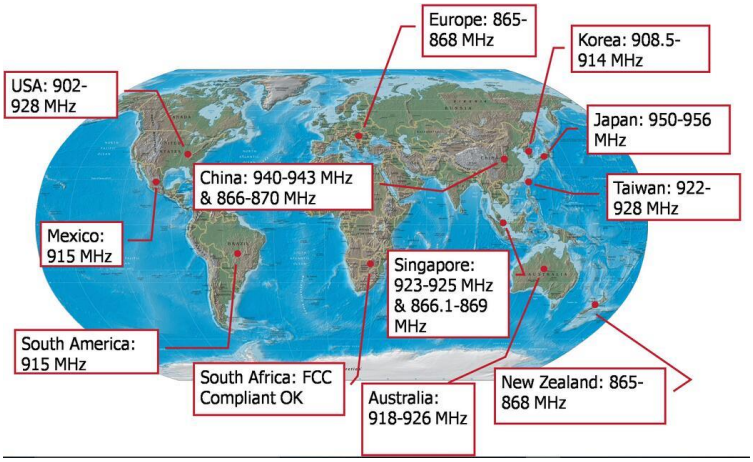

Figure 5. UHF frequency band in different countries. [11]

d) RFID systems use the microwave frequency ranges of 2.48 GHz and 5.6 GHz. In this range, the reader is able to read tag information very fast and the read range is over 100 meters. Some of the RFID applications which use this frequency range are supply chain management and mine industries. Frequency ranges indicate that tags range, influence on material, required energy and data transmission rate. [4;8;11]

4.2.4 Smart Tags versus Read-only Tags

One of the main differences between tags used in RFID systems is the type of memory used in them. Two types of read-only memory (RO) and read / write (RW) are used in RFID tags.

Read-only memory is a type of memory that information can only be read from it and there is not a possibility to change the information on it. Tags that have this type of memory can only be programmed once (by a manufacturer) like bar codes. This tags usually have a small amount of data stored in them, information like serial number or section number is permanently programmed on them and they can be easily integrated by barcode systems.

Tags with RW memory which are also known as smart tags have a high flexibility. In these tags a large amount of information can be stored. They use type of memory that is capable of addressing so that contents of each memory location can be easily changed with appropriate addressing. The information contained in RW tags can be erased and re-write multiple times.

According to this important feature, this type of tags can be considered as portable databases that carry important information (unlike the situation in which data is centrally stored on the controller). Due to reduced production costs of this type of tag and their wide application in recent years, using RFID technology continues growing at high speed. In addition to two mentioned memories, other kinds of memory are used in RFID tags. Write-once-read-many memory is similar to read-only memory that small amount of information can be stored in it but it cannot be changed. Some of RFID tags depending on the application, may use two types of RO and RW memory at the same time but each memory has its own place.

4.2.5 Active Tags versus Passive Tags

Frequent long years of research led scientists to produce three different types of RFID tags that are known as passive, semi-passive and active tags. Passive RFID tags have no internal source of power. Very little electrical power that enters these tags, moves the antenna in order to receive radio frequencies and from this process it produces the required power for CMOS so that internal ICs will be able to demonstrate appropriate reactions.

Unlike passive RFID tags, active tags can provide their own required power by using internal sources and thereby they can always keep the ICs that are related to receiving radio waves active. Active tags are generally safer and more reliable than the passive type and they encounter errors less. As a result of the force that these devices produce, they can more easily adjust themselves with disorders such as bad weather, fluctuations in radio waves or long distances to receive these waves. Many active tags that are produced today, can easily receive these waves from hundreds of meters. Batteries that are implanted within these devices last up to ten years. Some of RFID active tags have sensors with which they can detect temperature, humidity, light intensity and the possible impact of applied pressure on object even from long distances.

Active tags have a battery installed on their motherboard. When an active tag needs to send its stored data to reader, it uses this source to send the data (like the battery in mobile phones). Due to this, active tags are able to communicate with the less powerful readers and can also send information to a higher range. In addition, these tags generally

have more storage memory. Compared to passive tags, active tags are larger and more complex. This has caused their production value to be high.

Passive tags do not have power supply on their board and they get their power to send data from transmitted signal by readers. This is the reason for smaller tag sizes and reduction in production costs. Moreover, passive tags, compare to active tags cover smaller range.

Due to the fact that passive tags get their required power to send data, from their reader, this type of readers should have suitable power. Passive tags have much less memory than active tags. Some of these tags may have a built-in battery on their motherboard which does not have an effect on sending radio signals and it is only used to activate the electronic circuits on the board.

For example, a food manufacturer may install RFID tags equipped with thermal sensors on cargo platforms in order to control the products temperature during the transportation. After an increase in temperature of a product to a specific level, characteristics of that will be automatically recorded on tag by sensors. Then, at the time of distribution or sale of goods, this stored information in the tag will be used to verify the shipping and storing process. This type of sensors may need a battery on their motherboard so that they can perform their tasks during transportation or storage. [6]

4.2.6 Tag Sizes and Shapes

RFID tags can be offered in different sizes and shapes. Given the fact that the chip and the antenna used in RFID tags are tiny, RFID tags can be used in any shape and size (like small plastic balls that are connected to animal ears). The size and shape of a RFID tag depends on the type of application. Some tags should be structured in a way that some factors such as high temperature, humidity and chemicals will not have an effect on their performance. Others must be constructed in such a way that they are inexpensive and consumption, such as smart tags.

A rule of thumb is that the larger the tag (consequently antenna will be bigger), the bigger the read range. In many applications, because there is plenty of space to attach a tag on the object that is going to be tracked, tag size does not matter. But in the small valuable objects such as electronic equipment, tag size can be considered as vital criteria.

In many electronic equipment, the most of surface is used by ventilation holes and connector insertion. Placing tags on ventilation holes of device, causes heat increase and possible failure of device. During the recent years, RFID technology, have been released tags with small and smaller sizes.

After determining the read range and size of tag, the most important point in designing solutions is the electromagnetic field in which RFID system will be install and work in. Every substance has its own specific electromagnetic properties that affect the operating frequency. A standard dipole tag that is attached on an object, will be affected by the conductivity properties of the material. This is the reason that such tags do not work on the metal or liquid. Using the tags that operate efficiently on any type of material, plays an important role in designing a RFID system. [9,29]

4.3 RFID Readers

RFID reader can be considered as a small computer which is composed of three essential parts:

- An antenna
- A RF electronic module that is responsible for communicating with RFID tags
- An electronic control module that is responsible for communicating with controller

A RFID reader acts as a bridge between the RFID tag and controller and it has the following tasks:

- Reading the contents of RFID tag
- Writing data on tag (in smart tags)
- Relay or release data for controller and vice versa
- Supply energy for tag (passive tags)

In addition to above operations, more complex RFID readers are able to do deal with concussion and ensure communication with several tags, approve tags to prevent possible misuse and unauthorized access to system and ensure the integrity of data by encryption. [9,43; 4]

4.3.1 Encryption and Decryption

Data encryption is a security process that should be implemented to prevent external invasion to system. In order to protect the integrity of transmitted data and prevent interception and eavesdropping, encryption is used. Reader is responsible for encryption and decryption.

4.3.2 Reader Location and Size

In RFID systems, it is not necessary for tags to be placed in reader devices sight (unlike barcode systems). The most important advantage of the above characteristics is that designers can decide where to place the reader according to their needs. Some readers can be permanently attached to doors, others can be hung from the ceiling and smaller handheld readers make it possible for users to read the information by standing in a distance (for places that is not possible to install the readers permanently). In most cases, this type of handheld readers can be connected to computer wirelessly.

Sometimes to cover an environment, several antennas are used at the same time so that if an antenna was not able to read a tag correctly or if there is a large amount of tags, each antenna read couple of tags or double the read distance so each antenna covers half the gate width.

4.4 Antenna

Antenna makes it possible for readers and tags to communicate with each other in RFID tracking system. This device is responsible for sending and receiving radio frequency in a defined frequency for system. Antenna should be placed in a suitable location and correct direction. Angle and location of installing antennas (polarization) in addition to number of required antennas in order to cover the desired space, will be determined by advanced mathematical and telecommunication relations by experts.

These devices are produced in different types and sizes which work in different frequency bands. Also, according to terms of use of HF and UHF waves, different types of antenna are needed. It is worth noting that choosing a suitable antenna and determining the number of required antenna, capacity, location and angle of coverage is very important. It is obvious that if it is not installed properly and precisely, desired coverage and performance cannot be achieved.
Generally, antenna is a device that is used to transmit or receive electromagnetic waves. Both tag and reader contain antenna which makes it possible for them to communicate with each other and is an essential component in RFID systems. [9]

4.4.1 Dipole Antenna

Dipole antenna is one the most common and simplest types of antenna. This model consists of two symmetrically placed conductive elements that each act as a pole. It is designed in a way that it is capable of providing optimal power for transmitting radio waves between tag and reader. In other words, its length is simply half the wavelength of used communication wave. This half of the wavelength is actually based on technical calculations to benefit more from received wave and provide enough energy in response to reader. [9]

4.4.2 Monopole Antenna

Monopole antenna is type of dipole antenna that instead of both parts in dipole antenna half the antenna is replaced and it includes a surface with electrical conductivity to reflect radio waves. If this part is large enough it will act as a dipole antenna. A familiar example of such antennas is whip-like antennas that are also used in other cases beside RFID and installed vertically on the surface. [9]

4.4.3 Linearly Polarized Antenna

Electromagnetic waves contain electrical and magnetic components which are perpendicular to each other and are released in the direction of radiation.

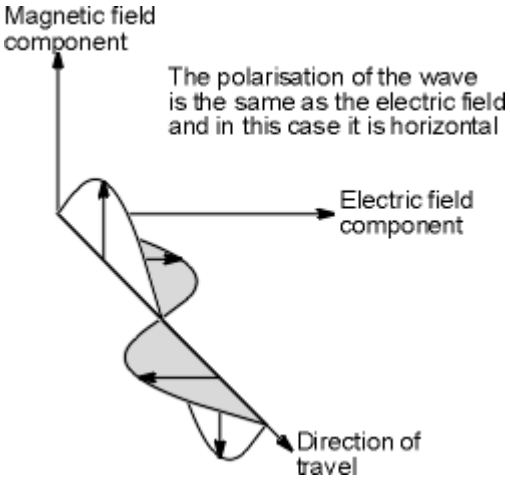

Figure 6. Linearly polarized antenna. [12]

In this type of antenna, type of polarization will be determined by electrical field parallel to transmitted radio wave (Figure6). For example, if this direction is horizontal, then that wave have a horizontal polarization and if the direction is vertical it will have a vertical polarization. [12]

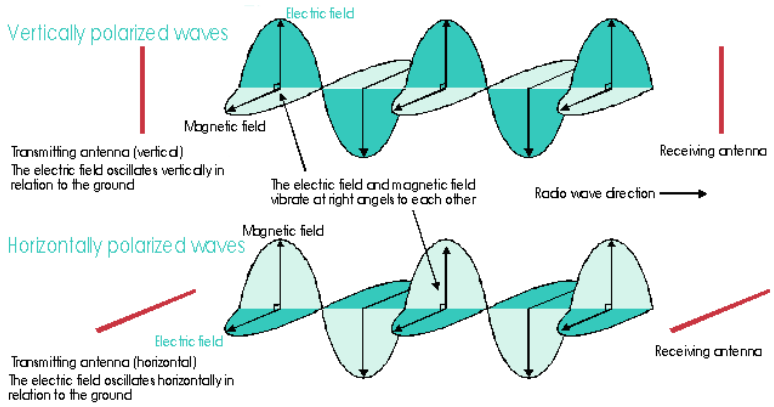

Figure 7. Vertical and horizontal polarized antenna. [13]

Horizontal or vertical polarization in general, is called linear polarization. Such a way of radiation causes wave range to increase because it is moving in just one surface not multiple surfaces (Figure7). This type of antenna is also sensitive to angle of tags and if the tag is parallel to antenna, reading will be maximum. Using this antenna is recommended when passing boxes on a conveyor belt at a fixed angle (meaning that tag always has the same angle toward the reader).

4.4.4 Circularly Polarized Antenna

If an electric field has a rotational motion with respect to time, then desired wave has a circular polarization. Type of antenna which is able to transmit this kind of waves, is called rotating antenna (Figure8). If this rotation is clockwise, then polarization is clockwise otherwise it is called counter clockwise polarization. In fact, this polarization has its both vertical and horizontal components, therefore it is able to transfer energy and read tags in any direction that is in front of reader. However, because it is sending radio waves in two directions, read range is half of the read range in linearly polarized antennas.

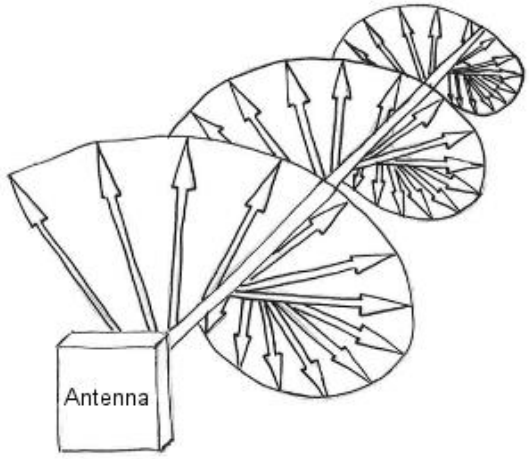

Figure 8. Circularly polarized antenna. [14]

Rotating antenna is used in applications that tag direction is not accurately specified. This type of antenna also responds well to recurrent and multi-path waves and has fewer errors in reading tags.

4.4.5 Omni-directional Antenna

Such antennas, spread wave power uniformly in all directions. Only this type of antenna is capable of acting as an ideal antenna by being able to send in three dimensions and cover a spherical volume around them. [9,47]

4.5 RFID Controller

RFID controllers act as the mastermind of an RFID system. This device is used to connect a network to readers and process the information. In each network, controller is often a personal computer or a workstation on which database or software system has been implemented. The controller is able to perform different actions based on received information and based on type of RFID system. Some of them are listed below:

- Maintaining and updating information about goods stock and automatically informing supplies unit (when number of available products become less than a specific amount)
- Tracking the transportation of objects in a system, and even change their path (such as conveyors in an industrial program)
- Determine the identity and granting permissions
- Updating user account

4.6 Middleware

Codes that have been read by reader will be sent to a computer. In the meantime, to make connection between these codes and database at the comprehensive tracking system, a software is needed. This software has the ability to connect data on the tags and system database. The software will be written separately for each operating system and cannot be offered as a general software package (Figure9). So according to system needs, monitored information and database, required software will be designed for each company. [9,53]

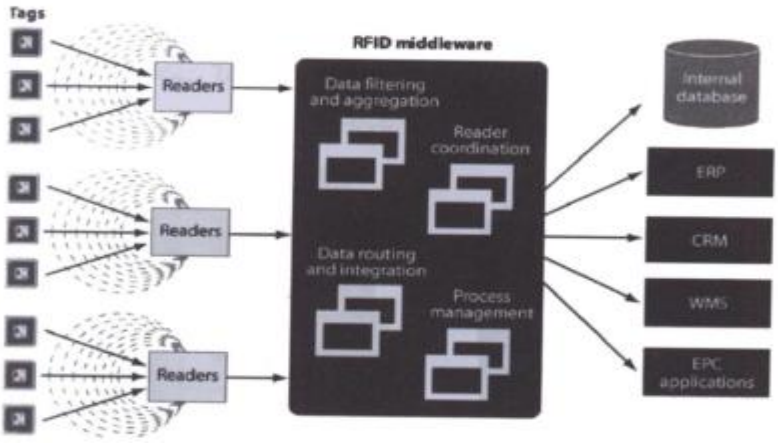

Figure 9. Performance of RFID middleware. [15]

5 RFID Security

5.1 Overview of RFID Security

To understand this topic better, factors which can cause a RFID system to crash should be evaluated. This factors can target the entire system until the whole system breaks down or they can attack the most minor component in order to disable a part of system. In order to study the security issues, the process of communication between tag and reader will be divided in to three layers. First layer which handles the information defined by user, such as information about the item which has been tagged, is called Application Layer. Second layer which determines the communication between tag and reader, is the Communication Layer. Physical layer is the final layer in which specifies principles like data coding and modulation for the communication. [16]

Professionals who deal with IT security, should not only focus on maintaining data in the database and they must develop security in the whole system. In the event that an

organization has a proper architecture in e-commerce, with an attack to its database or other parts of organization, inflict damage would be minimal. On the other hand, physical assets are more important than electronic data.

5.2 Intrusion Factors

When studying intrusion to RFID systems, many factors have to be considered. Some of these factors attack RFID system to steal an object or prevent the sale of a product in a store or series of chain stores. Invasion element of RFID system varies from a warehouse to a chain of warehouses and those who do this have various purposes, such as accessing physical assets or databases. It is possible to do this by manipulating tags and middleware. Attacks and intrusions to the RFID system can be divided as follows:

5.2.1 Radio Frequency Manipulation

One way to attack the RFID system is to manipulate radio frequency in order to stop the reader from reading the tag information. Since many metals block radio frequency, wrapping aluminium foil around items or using a metal wallet blinds the system. This attack can be placed at the physical layer.

5.2.2 Embedded Attack

Embedded attack is done by system commands at the location where data naturally is entered (like injecting a SQL command to the database). It is more common on websites. This type of attack usually takes place in the database and will not have a physical state. This attack can be classified at the application layer and the database. [17]

5.2.3 Relay Attack

Relay attack is an attack to entire RFID system and its goal is to use reader, tag and even database computing resources. In this attack, valid RFID signal invades a system by an invalid tag and its data will be recorded. These data will then be transmitted to a reader. Because the data appears to be valid, system accepts them. For example, if someone is familiar with the naming standard in an organization and creates a tag which is similar to original tag, can infiltrate the organization. [17]

5.2.4 Torrential Attack

Disruption in service attacks that also known as torrential attacks are formed when a signal flows with over capacity data. For someone who intent to steal several products, it is easier to use tag data manipulation methods and depending on characteristics of each tag, price, technical number and any other information in that can be changed. By changing the price of a product, a hustler can achieve a special discount. By changing the information of tag anyone is able to purchase the goods that are limited. When a commodity that its tag has been manipulated is sold automatically, no one notices any change and only warehouse stock has been flawed.

5.2.5 Middleware Attacks

Middleware attacks take place at any point between reader and backend data. Usually the weakest point of this route is local area network. Attacking data when it is transferring over the network to the database or attacking reader software are middleware attacks. Since the database is behind the line and the farthest point from both physical distance and receiving information point of view, possibility of attacking this section is much less but sometimes they have been attacked. [17]

5.3 Security Threats

Another factor that must be considered in RFID security, is threats to the system. Classification of security threats is still an important discussion and it is one of the challenges for security. It is worth noting that, researchers consider threats and attacks as two separate channels in this field.

5.3.1 Physical Layer Threat

Physical layer threats are including eavesdropping, blocking and copying. Mostly they exceed the electromagnetic characteristics (RF signal) in physical layer, such as frequency and carrier clock cycle.

Because RFID system is a wireless system, RF signals between the tags and readers can be intercepted. The attacker enters a range of radio frequencies and host or recipient must process the signals. In eavesdropping attack, invader uses an antenna with the same frequency to record signals between tag and a reader. If an attacker knows the encryption coding, taken signal have communication concept and this information can be used in other attacks against system like fraud attacks, spying attacks and distribution and tracking attacks.

Blocking happens by noise signals that periodically emits RF signals and can block and damage any reader system operation to prevent radio waves from arriving to attached tags on objects. Blocking can be tragic and dangerous in some cases, for example, when trying to read medical data from chips in the hospital.

RFID tags especially cheap tags, are simple devices, so a high level attacker can conquer a tag manually with reverse engineering. In the copying process, they may analyse automatic communication of carrier clock cycle signal and even coding method. In copying method, checking the structure of tag ID is not needed. This task is accomplished by reverse engineering. Since the tags are always transmitting information, copying the tag is only identifying the transmitted signal and it is not necessary to know the signal type or signal coding. Copying is a stronger threat than fraud and spying attack. [8]

5.3.2 Connection Layer Threats

Connection layer threats is collision attack. In this method, reader chooses a special tag for communication and attacks it. Interfere of other radio devices may prevent reader to detect tags. Clash of tags occurs when several tags respond to reader at the same time and therefore, other tags stay unknown for reader. Collision attack is a type of DoS. In other words, reader can be confused by sending a large amount of information to tags. [17]

5.3.3 Application Layer Threats

Application layer threats includes fraud and spying, distribution, tracking, asynchronous and viruses. They mainly attack application program characteristics such as tag ID number, database related operations and privacy. Fraud attack is an activity whereby the tag is considered as a valid tag and by that, products and services information will be collected with another ID. In this type of attack, attacker may read and record tag ID by using a programmed reader. When the ID is sent again, tag appears as a valid tag. This will help the attacker to deceive password reader, contactless payment systems and building access control stations.

Apart from all RFID attacks discussed previously, tracking is threat that directly targets the privacy. RFID reader can record tag ID in strategic locations and then combine with

other features. The major disadvantage emerges when tags be tracked involuntarily which is contrary to privacy.

Asynchronous attack is an endless attack of line and tag, it means it destroys the communication and connection between tag and database and makes tag useless. There are always two concepts of writing and reading for reader. Writing means insert tag ID. This attack disrupts operation of writing the ID and this happens when the connection between tag and database is interrupted. This type of attack is commonly used in wireless networks. [17]

6 Identify and Analyse Attacks

6.1 Physical Layer Attacks

Physical layer in RFID communications, has been formed from physical interfaces and used radio signals as well as RFID devices. The attacker, in this layer, uses the RFID wireless communications nature. This layer from physical security point of view is weak and it is not flexible against physical changes and it includes attacks which deactivate RFID tags permanently or temporarily and also re-send attacks.

6.1.1 Permanent Disablement of Tags

Disabling RFID tags permanently, includes all risks and possible threats which are able to generally or partially damage or destroy a RFID tag. Physical destruction or removing a RFID tag is one of the possible ways to cause a permanent damage to a tag. Moreover, criteria for protecting confidentiality like kill command, can be exploited for this purpose. Since RFID tags have a poor physical security, a tag that is not well placed can be easily removed and then be attached to another object (just like switching price tags). Therefore, objects can be easily lost and integrity of data on the system will be compromised. Because RFID systems cannot properly relate id tags with objects. This is not only a real threat, but can also be done easily, because it does not require special technical skills. So here a fundamental security problem arises. Fortunately, such attacks cannot be done on a wide scale.

RFID malicious that is interested to create a nuisance for people or disadjust an activity, can easily destroy tags with poor physical security by applying pressure (on electric charges) and contacting chemicals or even by disconnecting any visible antenna. After

damaging RFID tag which was attached to a product, a thief can remove it from automatic payment portal and this action will not be saved.

RFID tags are exposed to damaging effects of environmental condition such as very high or very low temperature or even attrition due to storing in rough places. Moreover, active tags are not usable when their battery is removed or discharged. There are some cases in which passive tags are not applicable because they receive their operating power from a reader, therefore a battery does not limit their lifetime.

RFID tags are extremely sensitive to static electricity. RFID tag electronic circuits can be damaged in a moment by electrostatic discharge caused by conveyor belts or high-energy waves. Not only RFID tags can be unusable by accidental discharge but they can also be damaged by intentional improper usage of privacy protection devices like RFID Zapper. This device is able to disable RFID passive tags permanently, by creating a strong electromagnetic field by a coil. Each RFID tag that is placed in this field receives a powerful energy shock which causes this tag to become permanently unusable.

Auto-ID centre and Electronic Product Code (EPC) global have created a KILL command which can permanently disable RFID tag. According to this method, each tag has a unique password that is defined by the tag manufacturer and using this command can disable tags permanently. In passive tags, KILL command can partially or completely erase any data stored on the device. Although this feature is used in order to maintain confidentiality, but it is clear that it can be exploited by attackers to sabotage communications in RFID.

6.1.2 Temporary Disablement of Tags

It is a possible to temporarily disable RFID tags. A faraday coverage such as aluminium bags can be used to protect electromagnetic waves and prevent the theft of products. Environmental conditions such as a tag covered in ice can also cause temporary and unintentional failure of RFID tags. In addition, radio waves interference may also temporarily disable tags.

Considering the fact that RFID networks often operate in noisy and inherent unstable environment, interference and collisions from any source of radio interference like e-noise generators and storing switching power supplies is possible. Metallic compounds,

water or ferric hydroxide particles can disrupt or block radio signals and cause radio frequency interference. This interference prevents efficient accurate communication.

One of RFID features is that it constantly listens to all radio frequencies in its frequency range and an attacker could use this feature for destructive purposes. So it is possible that the attacker by creating a signal at the same frequency range and in order to stop the communication between tags and reader, causes an intentional electromagnetic interference.

6.1.3 Removing and Destroying RFID Reader

Although small size of RFID tags causes their high vulnerability by physical threats, RFID readers can also be dismantled and destroyed. RFID readers can be stolen in an unprotected environment. A RFID tag reader which contains critical information such as required encrypted credits for accessing certain tags, can be the target of malicious threats. Negative effects of a stolen RFID reader are significant, because manipulating it causes attackers to have access to not only RFID tags but also to the backup system which can lead to manipulation of future data. This method was a critical concern during the design of European passport standard because only authorized tag readers had to be able to have access to the biometric passport data. In addition to this, by damaging RFID readers they will be unusable.

6.1.4 Relay Attacks

In a relay attack, attacker's tool is secretly placed between authorized tag and reader. This tool can eavesdrop and change the radio signals between verified tags and reader. As a result, by this tool a transient connection from tag or reader will be retransmit to tag or reader. In this case, authorized tag and reader think that they are in a direct contact with each other. To design this type of attack, even in a complex case, separate tools should be used so that one of them is for communicating with reader and the other ones to communicate with tags. [17]

Relay attacks can be divided in two types: "mafia fraud attack" and "terrorist attack". Mafia fraud attack was first introduced by Desmedt and colleagues and consists of an unauthorized section entity which resends the information between two legal sections [18]. Terrorist attack is the developed type of mafia fraud attack including cooperating with authorized tag with retransmitting unauthorized third sector to convince the reader

that an incorrect but legal tag is near that. This tag does not share any of its confidential information with retransmission of unauthorized section.

The biggest concern is the fact that relay attacks can be successful even at great distances. For example, a relay attack on a RFID card can be used to pay fees. A German graduate student, by providing a relay attack on Dutch transport ticket modified the vulnerability of Dutch public transportation. This student only implemented the “ghost and leech” attack which has been described by Kfir and Wool and created a lot of concern for Dutch public transportation system [19].

6.2 Defence against Physical Layer Attacks

For RFID systems protection against low-level attacks (such as temporary or permanent deactivation of tags), usual common actions should be applied. This type of operations can be such as enhancing physical security by guards, fences, walls, door locks and cameras. Therefore, intentional or unintentional damages by using aluminium bags can be prevented.

By applying policies separating tags from objects should be stopped. Issues such as physical protection or using more powerful ways (such as glue or strong mechanical bond) can prevent easy detachment of tags. One solution is to embedding tags in the device so that they are invisible and inaccessible. When RFID active tags are removed, a warning function can be activated. This function can be simplified by using sensors which protect tags. If additional studies to ensure tagged product specifications will be applied and related tag ID will be saved in the backup section, the success rate of tag switching can be significantly reduced.

Intentional or unintentional radio interferences can be restricted by using matte paint walls for radio frequencies. Moreover, by efficient password management, unauthorized use of KILL command can be avoided. For example, in KILL command for Class-1 Gen-2 EPC, tags need a 32-bit password. In addition, using a main password for a large number of tags, is a policy that prevents the impact of a single password that can have on a system.

In order to prevent relay attacks, possible methods are RFID communication encryption or adding a second form of authentication such as password, a PIN or biometric information. However, these methods eliminate the ease and advantages of RFID

communications. The important criteria that can be used to defend RFID system against relay attacks is the distance between tag and reader. The shortest distance makes relay attack very difficult for the attacker without being defended. A variety of techniques that can be used to measure the distance between tag and reader, can be radio signal round-trip time delay or signal strength.

One of the ideal ways is limited to the distance protocol which has been presented by Hancke et al [20]. and it is based on ultra-wide band (UWB) pulse communications. Hancke not only failed to offer practical and useful solutions based on his proven results and assess, but recently it has been shown that their protocol is vulnerable to terrorist attacks.

Raid et al. proposed far more useful distance limited protocol which has been provided based on a XOR function used in a challenge- response mechanism and has led to many breaches in the channel and as a result allows the reader to detect the presence of the genuine tag [21]. They also performed empirical analysis on their proposed protocol, to discover relay attacks in ISO 1443 contactless smart cards in a simulated environment. However, these results are primary and actual detection speeds was not achieved. The problem with this method is the fact that it reduces the operating range of used smart cards.

6.3 Multi-layer Attacks

Most of the attacks that target the RFID communications, are not limited to a single layer and this kind of classification contains those attacks which affect several layers including physical layer, network- transmission, application and strategic. In certain modes, this layer contains covert channels attack, denial of service, traffic analysis, cryptographic attacks, side-channel attack and relay attack.

6.3.1 Covert Channels

Attackers may use RFID tags to create illegal communication channels and transfer information. They can also use unused memory storage of several RFID tags in order to secretly transfer data by an unrecognizable method. For example, a set of RFID tags that have been embedded in human body due to natural purpose of identifying a person, is able to secretly report private information related to medical data or social activities. [17]

6.3.2 Denial of Service Attacks

RFID tags normal performance may be intentionally stopped by blocking access to them. Intentional blocking of access resulting in RFID tags service denial, may be created by the perpetrators of attack which uses RFID protector or blocker tags. Both of these methods, are used to secure and protect RFID communications against privacy threats, but attackers use them in order to perform service denial attack.

Another way for service denial is unauthorized use of lock commands. These commands include multiple RFID standards and are used in order to prevent unauthorized writing on RFID tags memory. According to the applicable standard, lock command is used by a pre-defined password and can have permanent or temporary effects.

Moreover, since RFID middleware has been contained networking devices, the attacker is able to use the limited system resources and cause service denial in RFID middleware. For example, sending a sequence of packets to middleware with the size of network bandwidth and processing capacity, causes middleware to be filled and thereby it prevents the access to legitimate users. [8]

6.3.3 Traffic Analysis

RFID communications are also exposed to traffic analysis attacks. An eavesdropper is able to read messages and extract data from a communication pattern. Even if RFID communication is protected by encryption and authentication techniques, it is vulnerable to traffic analysis attacks. The large number of eavesdropped messages in a traffic analysis attack can have a great impact on RFID systems.

6.3.4 Cryptographic Attacks

When vital information is stored on RFID tags, encryption techniques are used in order to maintain integrity and secure confidential information. However, to break used encryption algorithms, cryptographic attacks is used and confidential information will be revealed or manipulated. For example, a Dutch security company called rescure, has shown that keys used in Dutch passports can be easily discovered [22]. This is done by using a standard PC which runs a severe attack for two hours. In addition, Raboud University of Nijmegen researchers perform an attack against MIFARE card Crypto-1

algorithm in March 2008, by using exclusive algorithm method [23]. This type of card is also used in Dutch public transportation protocols.

Researchers also did reverse engineering on the security mechanism used in classic MIFARE contactless smart cards. They described vulnerability of security mechanisms and provided two attacks [24]. The first attack allows retrieving of MIFARE reader secret key form. Experimental results have shown that secret key can be obtained in 2 to 14 minutes. They showed that the secret key in second attack can be retrieved in a tenth of a second without any pre-calculation by using typical hardware. Thus, by using a little time to retrieve secret key, attacker not only is able to decrypt communications effects, but also can copy cards and return valid cards to their previous state.

6.3.5 Side-channel Attacks

Side channel attacks, use normal implementation of a cryptographic algorithm and also uses information which includes scheduling, energy consumption or even electromagnetic fields. The effective use of side-channel attacks, needs deep knowledge of internal system that runs encryption algorithms.

Timing attacks is done by using fluctuations in target calculation speed analysis, while simple power analysis (SPA) attacks extract information based on changes in energy consumption. Differential power analysis (DPA) attacks are certain type of SPA attacks that operate based on produced electromagnetic changes (for example, in the communication between RFID tag and reader). More precisely, when a RFID tag is performing a cryptographic operation, the changes in the electromagnetic field can be used to reveal encrypted secret keys.

6.3.6 Replay Attacks

In replay attacks, attacker copies valid responses of RFID communications and in another time sends them to one or several parts in order to impersonate. Copied messages usually are gathered through eavesdropping or by groups created by attackers. An example of this type of attack is unauthorized access to limited access areas; in a way that after reader confirmed the access to valid tag in a limited area in order to send radio signal, attacker resends this signal.

Although relay and replay attacks are quite relevant to each other, but the main difference between them is that in replay attacks, there is usually a delay between copying authorized responses and repeating them. [8]

6.4 Defence against Multi-Layer Attacks

Covert channel attack is a challenging threat which is hard to detect and defend against. A possible mechanism to fight this type of attack is to consider reducing access to memory resources on RFID tags, such as clean up unused memory every few seconds or randomizing code and data location.

Denial of service attacks (DOS) and traffic analysis are various types of vigorous security threats in the whole networks (such as wireless networks). Although theoretically it is possible to confront these kinds of attacks, RFID tags limited resources, make it hard to defend them and it still needs a lot of research.

Cryptographic attacks can be resolved by using strong encryption algorithms such as open encryption standards and using a key with the required length. In this way, damages like revealing MIFARE smart cards security flaws can be avoided.

By restricting the propagation of electromagnetic waves, the system can be protected against side-channel attacks or more precisely differential power analysis attacks. However, this action reduces operation range. Increasing complexity of RFID chip internal circuit, is another approach of fighting side-channel attacks or in general, manipulation attacks. It makes it more difficult for attacker to understand and analyse internal systems and operations. Because of RFID tags small physical dimensions and also cost factors, increasing complexity of chips is limited. Currently, there are some RFID tags which cannot be manipulated, like PlusID, and according to the Federal Information Processing Standard (FIPS) they belong to security level 3 (tamper-resistant).

In order to defend against replay attacks, there are some simple countermeasures such as using time stamps, one-time passwords, challenge- response cryptographic, by using increasing sequential numbers, synchronizing clocks. By taking into account the vulnerability of challenge- response protocols that are at risk because of inherent limitations of RFID tags, mentioned methods are less efficient. For example, challenge-response mechanisms based on synchronizing clock, cannot be used in RFID passive

tags, because this type of tags does not have battery and therefore they are not able to use clock.
Another method is to use radio frequency shielding in readers in order to limit radio signals navigation and also prevent the appearance of ghost in ghost-and-leech model. There is also another method based on the distance between requester and owner of information. In RFID systems signal to noise ratio of reader signal and also the approximate distance between reader and tag can be determined. This information can be used to discriminate between authorized and authorized tags and readers and to reduce replay attacks.

7 Secure RFID system

7.1 Security protocol

To design a RFID system with an enhanced security, it should be mentioned that the used cryptographic algorithms strength is not the only factor that affects the security level. Whether an attacker succeeds to interfere with the system or not, also depends on the used protocols. Protocols need to be secure even if cryptographic algorithms are strong. The protocol which will be described in this chapter, uses the Advanced Encryption Standard (AES) [25] as the cryptographic primitive for authenticating a RFID tag to a reader. Limited and low computing power of tags in RFID systems should be considered regarding the used protocols. Moreover, besides accessible bandwidths for transmitting data, compatibility to standards such as EPC [26] or ISO/IEC 18000 [27] should be examined.

This protocol is formed based on the unilateral authentication using random numbers. Special consideration is required when integrating the challenge response authentication protocol into the ISO/IE 18000 standard. Custom commands can be defined, in addition to compulsory commands that all tags need to implement. The two command which are integrated for authentication, send a challenge to the tag and wait for the encrypted value. Even though the fundamental functionality stays unchanged, these commands expand the existing standard. Because of the low power limitations, RFID tag’s internal clock frequency should be divided from 13.56 MHz to 100 kHz. The used standard requires that a reply should take place 320 µs after the request has been sent. If the tag is not able to send a response during that specified time, it must remain silent. However, encrypting a challenge by AES algorithm cannot be done during this 32 clock cycles at 100 kHz frequency.

This problem can be solved by modifying the protocol. The challenges sent to tags and its responses are interleaved together. Typically, in a reader environment there are many RFID tags that needs to be authenticated. The RFID reader transmits a challenge to a tag (T1), after all of the tags IDs have been retrieved by using the anti-collision sequence and the inventory request. T1 begins to encrypt the challenge instantly without sending a response. While waiting for T1 to respond, the reader sends more challenges to other tags (T2, T3). T2 and T3 also start encrypting after receiving their challenges. When T1 completed the encryption of challenge, it waits for the appeal to send the encrypted value (R1) to reader. After sending all three challenges, reader sends a request in order to collect the response from T1. The R1 value will be confirmed after encrypting the challenge and comparing its result with the collected value. The other two challenges will be verified using the same method. The reader then start to authenticate all other existing tags in the same way.

By applying high level models of RFID communication channel, this security protocol was assessed. This challenge-response protocol has the benefit of each tag having minimum 18ms for encrypting the challenge. With this security protocol up to 50 RFID tags are able to be authenticated each second. In case that number of tags in a reader range is low, instead of sending interleaved demands, reader is able to decide to make at least 18 ms breaks.

7.2 Secure RFID tag

Architecture of a RFID tag with enhanced security contains an AES module, a digital controller, analog frontend and EEPROM. Strong cryptographic authentication in a RFID tag with high level security is calculated by an AES module which is formed for low die size limitations and low power requirements. The digital controller is a finite state machine which is responsible for executing the commands in the protocol, handling communication with the reader, implementing the anti-collision mechanism, and it also grants read and write permission to the AES module and EEPROM. The power supply of a RFID tag which is transferred from the reader to RFID tag is handled by the analog frontend. The analog frontend is also responsible for the clock recovery from the transmitted frequency and the modulation and demodulation of data. Tag data such as cryptographic key and unique ID is stored by the EEPROM. These tag-specific data should be retained in case of power loss.

Contactless identifications should be able to perform within a few meters range and as a result of that, the environmental conditions have an important role besides the low cost perspective. Therefore, the signal strength for modulation and demodulation and accessible power supply for RFID tag are the restricting factors. For the digital controller and AES module, the amount of available power consumption is 20 µA. By estimating 5 µA of the current consumption for the digital controller, the remaining 15 µA amount will be for the AES module which should not be more than a chip area of 5000 gates. Moreover, about 50 tags per second are authenticated and as mentioned earlier this leads to a 18ms available time gap for encryption of a 128-bit block of data.

8 Conclusions

In this thesis security issues of an RFID system have been studied and a high security RFID system which allows strong cryptographic authentications has been presented. By proposing a symmetric challenge-response authentication protocol in this model, everyday usage of RFID technology and new security challenging applications will be easier. For the safer future of the RFID technology and pushing the applications further, other authentication methods such as asymmetric techniques should also be examined. As mentioned earlier, Radio Frequency Identification is a growing technology worldwide and new applications of it, is defined and applied per day for different processes. However, in order to implement RFID in a process, before purchasing and installing the equipment, besides learning basic required knowledge, all possible economic and technical aspects in this area should be analysed for optimal use of this technology. In the meantime, system environmental conditions and required information and equipment which can be effective in increasing costs and reducing the desirability of system are very important factors. In this regard, complete use of available resources and especially receiving and reviewing technical and costs proposals from qualified suppliers, is necessary for choosing appropriate system components and making a final decision. Due to high costs and economic evaluation results of implementation and deployment of this system, this technology is not yet fully developed as it is supposed to be. But due to its rapid development during recent years and predictable decrease in its implementation costs, it is anticipated that this technology will be widely used in the near future.

Due to the daily advancement of RFID systems, their security is a very important subject. In this thesis some of the possible structures that could attack and affect these systems have been described. Also according to the place of attack, system effects and

countermeasures, more coherent view of the threats and methods to confront them can be found. Finally, it is noted that for a proper defence against RFID systems attacks, more should be done especially on other layers of the systems.

References

1 Landt J. The history of RFID [online]; November/ October 2005.
URL: http://www.sepaco-tech.com/modules/Manager/Articles/the%20history%20of%20rfid.pdf. Accessed 31 October 2016.

2 2 Colin MacKinnon. A typical ground based IFF Transponder, a BC-800, with the receiver at the top and the transmitter below. [online].
URL: http://www.qsl.net/vk2dym/radio/iff.htm. Accessed 2 February 2017.

3 Radio Frequency Identification (RFID) 101 [online].
URL: http://www.aimglobal.org/?page=rfid_basics. Accessed 11 April 2016.

4 Mobin Mohsen zadeh. *RFID technology [online]*.
URL: http://www.aiaciran.org/cache/fck_files/file/magazine/fild/91136-11fi.pdf. Accessed 20.03.2016.

5 IEEE GlobalSpec. Advanced Infrstructure [online].
URL:http://www.globalspec.com/learnmore/data_acquisition_signal_conditioning/data_input_devices/rfid_readers. Accessed19 April 2016.

6 What is RFID Technology | How RFID Works | RFID Applications [online]. Electronics Hub; 2015.
URL: http://www.electronicshub.org/rfid-technology-and-its-applications/. Accessed 28 November 2016.

7 Teymouri A. Benefits and limitations of using RFID [online]. Elme Farda; 2012.
URL: http://www.elmefarda.com/rfid-%DA%86%DB%8C%D8%B3%D8%AA-%D8%9F/.Accessed 17 September 2016.

8 Jechlitschek C. A survey paper on radio frequency identification trends [online]; 2013.
URL: https://www.cse.wustl.edu/~jain/cse574-06/ftp/rfid.pdf. Accessed 27 May 2016.

9 Gholampour M. Radio Frequency Identification; 2013.

10 Kumar P. Construction of RFID Tag [online]; 2011.
URL: http://tech-lightenment.blogspot.fi/2011/11/rfid-technology.html. Accessed 17 May 2016.

11 Shenzhen RICH RFID Tag Co, Ltd. UHF Frequency in different countries and regions [online].
URL: http://www.passive-rfid-tags.com/52/UHF-Frequency.html. Accessed 5 August 2016.

12 Poole I. Antenna polarisation or polarization [online].
URL: http://www.radio-electronics.com/info/antennas/basics/polarisation-polarization.php. Accessed 8 August 2016.

13 Horizontally polarized waves and vertically polarized waves [online]. URL: http://www.cdt21.com/resources/guide3.asp. Accessed 8 August 2016.

14 Armstrong S. Circular Polarization (right-hand) [online]; 2013. URL: http://blog.atlasrfidstore.com/circular-polarization-vs-linear-polarization. Accessed 8 August 2016.

15 shun Chen r. The system architecture of the RFID middleware [online]; 2015. URL: https://www.researchgate.net/publication/262331762_An_RFID-based_manufacture_process_control_and_supply_chain_management_in_the_semiconductor_industry. Accessed 12 September 2016.

16 Queisser M. Cataloging RFID Privacy and Security [online]; 2006. URL: https://www.researchgate.net/figure/228537718_fig1_Figure-1-Layers-of-an-RFID-System. Accessed 20 December 2016.

17 Samadi Gharajeh M. Investigate the Attacks on the Physical Layer and Multi-Layer Attacks on RFID and Offer Solutions for Dealing with Them [online]; 2011. URL:https://www.researchgate.net/publication/259221741_Investigate_the_Attacks_on_the_Physical_Layer_and_Multi-layer_Attacks_on_RFID_and_Offer_Solutions_for_Dealing_with_Them. Accessed 11 February 2017.

18 Y. Desmedt. Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them. In SecuriCom '88, SEDEP Paris, France, 1988.

19 Kfir, Z. and Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smart card. appears in: Security a nd Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference On page(s): 47 – 58. 05-09 Sept. 2005

20 Gerhard P. Ha ncke, Markus G. Kuhn. University of Cambridge, Computer Laboratory.15 JJ Thomson Avenue, Cambridge CB30FD, UKAn RFID Distance Bounding Protocol. (2005). In Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm'05) (pp. 67-73). IEEE Computer Society.

21 Reid, J., Gonzalez Nieto J.M., Tang, T., Senadji, B. (2007). Detecting relay attacks with timing-based protocols. ASIACCS '07 Proceedings of the 2nd ACM symposium on Information, computer and communications security ACM New York, NY, USA ©2007.

22 Riscure. Privacy issue in electronic passport[online]; 2006. URL: http://www.riscure.com/contact/privacy-issue-in-electronic-passport.html. Accessed 24 February 2016.

23 Raboud University Nijmegen. Dismantling contactless smart cards[online]; 2008. URL: http://www2.ru.nl/media/pressrelease.pdf. Accessed 24 February 2016.

24 Garcia, F.D., de Koning Gans, G., Muijrers, R., van Rossum P., Verdult, R., Wichers Schreur, R., Jacobs, B. (2008). Dismantling MIFARE classic. Institute for Computing and Information Sciences, Radboud University Nijmegen, The Netherlands.

25 National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard[online]; November 2001.
URL: http://www.itl.nist.gov/fipspubs/. Accessed 25 February 2016.

26 EPCglobal. 13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification [online].
URL: http://www.epcglobalinc.org/. Accessed 25 February 2016.

27 International Organization for Standardization. ISO/IEC 18000-3. Information Technology AIDC Techniques — RFID for Item Management; March 2003.

28 Introduction to the RFID [online].
URL: http://www.centrenational-rfid.com/introduction-to-the-rfid-article-15-gb-ruid-202.html. Accessed 25.03.2016.

29 Journal, R. *RFID (radio frequency identification) technology news & features[online]*;2002.
URL: http://www.rfidjournal.com. Accessed: 26 March 2016.

30 Bhuptani, M. and Moradpour, S. *RFID field guide: Deploying radio frequency identification systems*; 2008. United States: Prentice Hall PTR.

31 Modiri, N. and Shir afkan, M. *Radio Frequency Identification Systems Engineering*;2010. Mehregan Ghalam.

32 Modiri, N. and Fazeli Nia, H.R. *Radio-Frequency Identification technology infrastructure requirements*;2010. Ganj-e-Nafis.

33 Ahson, S.A. and Ilyas, M. *RFID handbook: Applications, technology, security, and privacy*;2008. Boca Raton: CRC Press.

34 Dobkin, D.M. *The RF in RFID: Passive UHF RFID in practice*;2007. Amsterdam: Newnes (an imprint of Butterworth-Heinemann Ltd).

35 Jannati, H. and Ardeshir-Larijani, E. 'Detecting relay attacks on RFID communication systems using quantum bits', Quantum Information Processing;2016.