Chapter 2

Radio Frequency Identification Technology Overview

2.1. Introduction

Identity plays a crucial role in writing a success story of the Internet of Things (IoT). Some of the traditional approaches to collect the identity are machine readable characters, MICR (magnetic ink character recognition), bar-codes, smart cards, magnetic strips, face and retina scans (especially for human beings), etc. Some of these are contact type, where the object storing the identity information has to make physical contact with the reader, and others are of proximity type. Most of the proximity-based techniques require a clear line-of-sight path for successful identification. This could be a major issue in several applications. For example, if the objective is to identify the objects stored on a palette, it is almost prohibitive to take each of the boxes out of the palette, show them to the reader, and store them back on the palette. In such a situation, it would be desirable to have a system that could collect the identity of each of the boxes without the need for a clear line-of-sight. Another interesting application could be that of identifying perishable items that are stored in a freezer compartment. Ideally we would like to know the expiry date of each

Chapter written by Ayyangar Ranganath HARISH.

The Internet of Things: Connecting Objects to the Web Edited by Hakima Chaouchi

of the items without even opening the freezer compartment. A barcode-like technique, which requires a clear line of sight to obtain the identity, would hardly be of any use in a scenario like this, unless the items are stacked so that every barcode is visible to the reader. The radio frequency identification (RFID) system is able to overcome most of these difficulties to an extent.

The RFID system consists of a tag (also known as a transponder) attached to the object being identified. The tag usually consists of an integrated circuit and an antenna. Another important module in the system is a reader. The reader queries the tag using radio frequency (RF) waves, and gets the identity of the tag via the RF waves. The RFID systems operate in various frequency bands. Some of the most popular frequencies are:

– 125 kHz to 134.2 kHz (LF: low frequency);

– 13.56 MHz (HF: high frequency);

– 860 to 915 MHz (UHF: ultra-high frequency); and

– 2.45 GHz to 5.8 GHz (microwave frequency).

The RFID systems operating in the LF band were the first to be deployed in the market for high-volume short-range industrial applications and car immobilizer devices. These systems are attractive in systems where the data rates are not very high. The HF RFID systems are capable of handling much higher data rates compared to the LF system, and the tag antenna is much smaller. HF systems have longer read range compared to the LF systems. The UHF RFID system has a much longer read range and much higher data rate compared to the LF and HF systems. However, the UHF system does not work very well in the presence of metallic objects, water and the human body, compared to the LF system.

2.2. Principle of RFID

Consider a coil made of copper wire through which alternating current is flowing. The coil offers impedance to the source and a voltage develops across its terminals. It is possible to increase the

voltage by connecting a capacitor in parallel with the coil. Let us call this the "primary" coil. Now we bring in another coil, called the "secondary" coil, close to the first. Due to electromagnetic induction, voltage appears across the terminals of the secondary coil. The amplitude of the voltage depends on the size, shape, location and orientation of the secondary coil. If we connect a resistor (also known as a load) across the terminals of the secondary coil, current flows through it. The strength of the current flowing through the secondary coil depends on the load. The interesting phenomenon is that the current flowing in the secondary coil induces a voltage back into the primary coil, which is proportional to its strength. The induced voltage, also known as back emf (electromotive force), can easily be sensed by using suitable electronics. Therefore, by observing the voltage on the primary, it is possible to estimate what is connected to the secondary coil [FIN 03, PAR 05].

A circuit schematic of the arrangement is shown in Figure 2.1. The two coils and the coupling between them have been modeled as a transformer. The coupling coefficient is used to determine how tightly the two coils are coupled to each other. A larger value suggests tighter coupling, i.e. the two coils are close to each other. The system is excited by a sinusoidal source. Capacitors are connected across both primary and secondary coils, forming a parallel resonant circuit. A load resistance is also connected in parallel with the secondary coil.

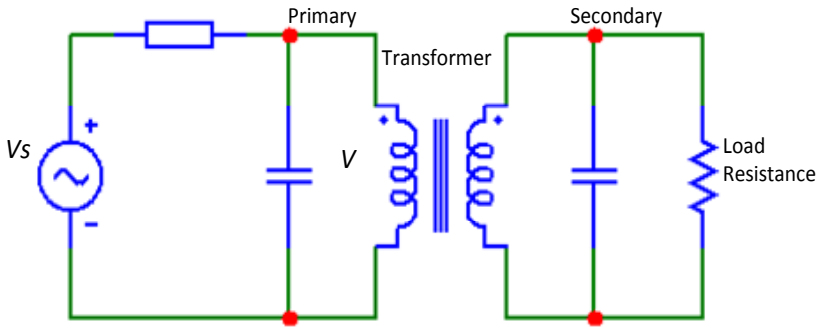

Figure 2.1. *Circuit schematic of two coils electromagnetically interacting with each other*

The voltage V, developed at the terminals of the primary coil, *versus* the frequency of the excitation is plotted in Figure 2.2. As the frequency of the source increases, the voltage also increases, reaches a maximum, and then decreases. The frequency corresponding to the maximum voltage is known as the resonant frequency. Now, if the load resistance is changed, the voltage at the primary corresponding to the resonant frequency drops sharply (see Figure 2.3).

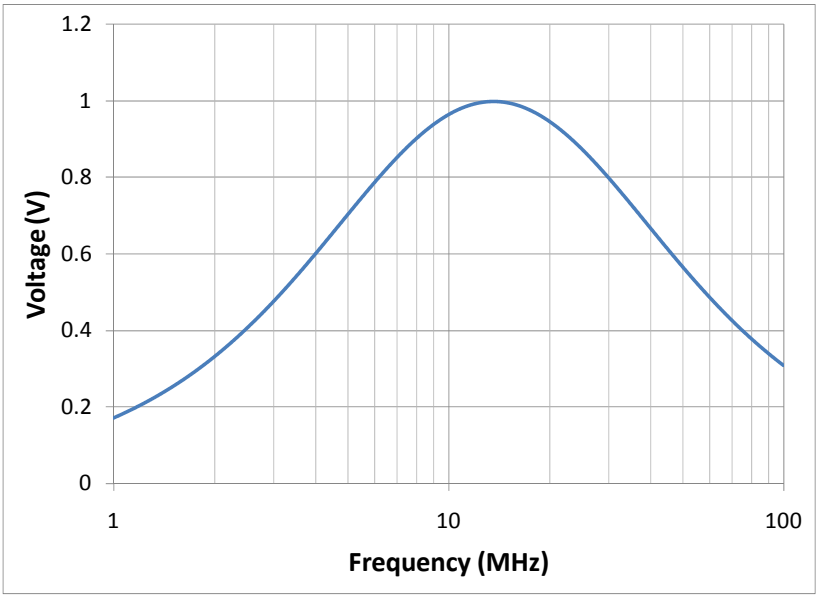

Figure 2.2. *Voltage across the primary coil as a function of frequency*

From this, we can conclude that it is possible to change (or modulate) the voltage at the primary by changing the load connected to the secondary. This is known as "load modulation". It is important to remember that the primary and secondary coils are not physically in contact with each other, but interact via electromagnetic coupling.

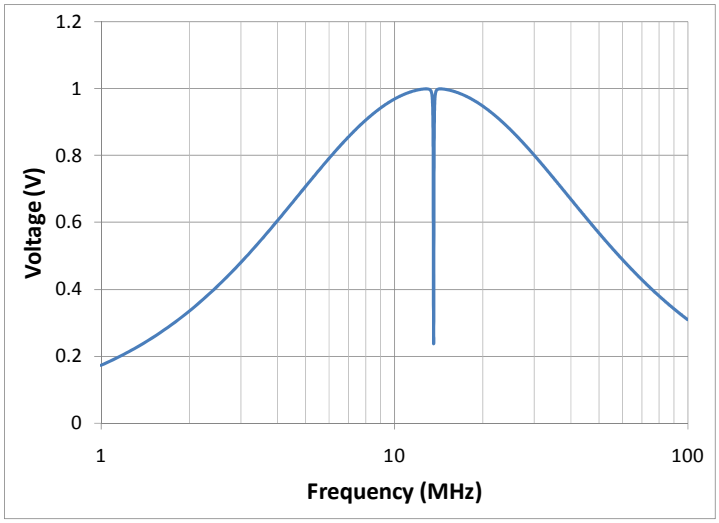

Figure 2.3. *Voltage across the primary coil as a function of frequency for a different value of load resistance*

The primary coil can be thought of as the reader of the RFID system, and the secondary coil as the transponder or tag. The tag can convey any message back to the reader using RF signals, by simply changing the load connected to its terminals. This could be achieved by switching in a load to represent a logical state 1 and taking off the load to represent a logical state 0. Using load modulation, a tag is able to communicate with the reader and transfer its identity without actually using a transmitter. The identity information is stored in a memory chip located on the tag. A processor (also known as the state machine) reads this information and modulates the load by operating a switch. Two more ingredients are required to operate the entire system: power and clock. It is quite straight forward to have a battery on the tag supplying the power and an oscillator that generates the clock signal. This would make the tag bulky and expensive. In a class of tags, called batteryless tags, the energy to operate the tag is supplied by the reader itself. A diode in the tag is used to rectify the RF energy and convert it into direct current, which is used to power the electronics in the tag. It is not difficult to provide the clock from the reader itself. With the exception of the antenna coil, all other

components are included in the integrated circuit located on the tag (see Figure 2.4).

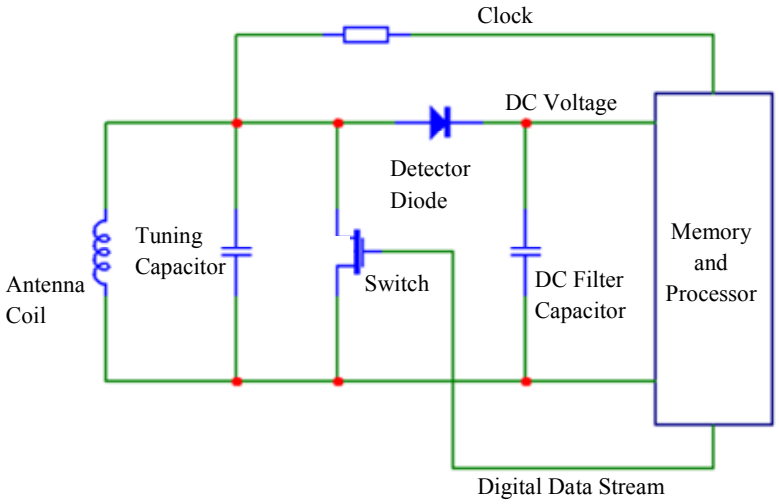

Figure. 2.4. *Schematic of an RFID tag*

Load modulation is the principle used to establish communication between the reader and the tag operating in the LF and HF bands. RFID tags operating in the UHF and microwave bands use a backscattering method to communicate with the reader. In the UHF band, the signals from the reader are radiated out by an antenna and the tags are placed far away (also known as the far-field region) from the antenna.

If D is the largest dimension of the antenna operating at a wavelength λ, the distance beyond $2D^2/\lambda$ is known as the far-field region of the antenna. When the electromagnetic energy falls on the antenna attached to the tag, it backscatters a portion of the energy. The amount of backscattered energy depends on the load connected to the tag antenna. Therefore, by modulating the load according to the data, it is possible to change the strength of the backscattered signal from the antenna. The backscattered signal is sensed by the reader and is able to extract the information carried by it.

2.3. Components of an RFID system

So far we have been discussing the issue of establishing communication between a tag and a reader. Reader and tag constitute two important components of an RFID system. The reader gets the identity information stored in the tag. An RFID system, in general, can have several readers and tags. A reader will be able to "see" several tags, and systematically read the identity of each of the tags. The reader is capable of storing information into a tag as well as altering the state of the tag. The information collected by the reader is not really useful unless it is available to a network server. Therefore, two more components also enter into the system: a server and a network.

2.3.1. *Reader*

A functional block schematic of an RFID reader is shown in Figure 2.5. The RF carrier is modulated according to the information to be transmitted to the tag. The modulated carrier is amplified and radiated out of the antenna. The reader also receives the electromagnetic waves backscattered by the tag, amplifies the received signals, and demodulates to extract the information.

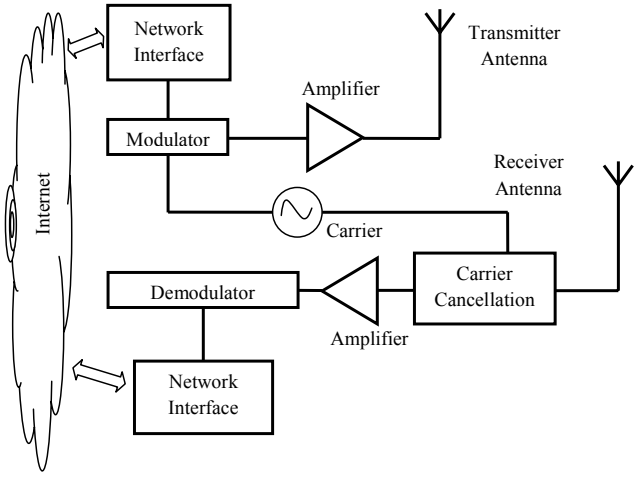

Figure 2.5. *Block schematic of an RFID reader*

An important component of the reader is the antenna. Antennas are generally the largest and the most visible component of an RFID system. The size of the antenna depends on the operating frequency. The size of the reader antennas are usually of the order of wavelength. For example, the size of the reader antenna in an UHF system (operating frequency of 865 MHz) is about 200 to 300 mm (see Figure 2.6). The reader antenna of an HF system can be as large as a meter in size.

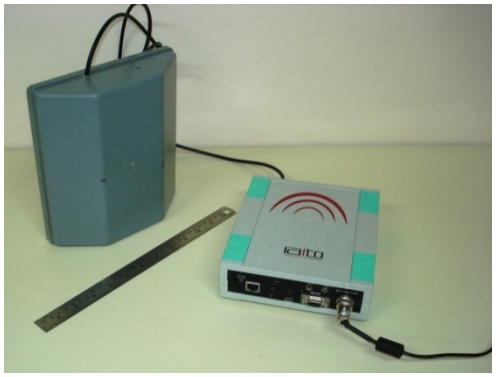

Figure 2.6. *Photograph of an UHF RFID reader with its antenna (Image courtesy of Iaito Infotech Pvt. Ltd., IIT Kanpur, India)*

An UHF RFID reader can be designed to operate with a single antenna or two antennas. Systems that use two antennas are known as "bistatic". One antenna is used to transmit the RF signals, and the other antenna is used to receive the signal backscattered by the tag (see Figure 2.5). The two antennas are placed physically far apart to provide sufficient isolation between the transmitter and the receiver. This is necessary to ensure that the transmitter signal does not saturate or overload the receiver.

There are other ways of providing isolation between the transmitter and the receiver. One of the techniques is to use two antennas with orthogonal linear polarizations (for example horizontal for transmitting and vertical for receiving), and use a tag that has a circularly polarized antenna. Such a solution is much more complex and expensive compared to the earlier solution.

It is also possible to design a reader with a single antenna. Such a system is known as "monostatic". In this design, a single antenna transmits and receives the RF signals. Directional couplers and circulators are used to separate, transmit and receive signals. The front end of a monostatic system with an isolator is shown in Figure 2.7. The isolator has three ports. The transmitter is connected to port 1, the antenna to port 2, and the receiver to port 3. Signals from the transmitter flow from port 1 to port 2 and nothing goes into port 3. Similarly, the backscattered signal received by the antenna enters the circulator at port 2 and continues to flow out of port 3. This way, the circulator is able to isolate, transmit and receive signals.

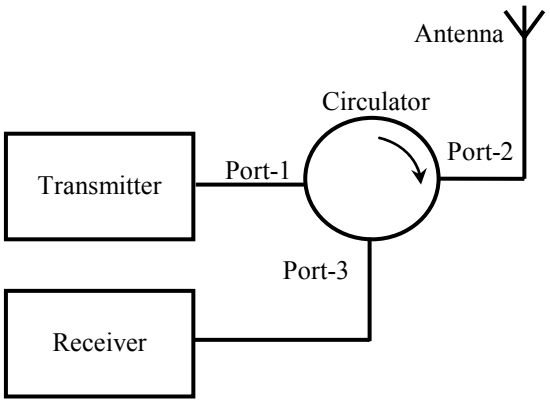

Figure 2.7. *RF front end of a monostatic RFID reader*

Several modulation schemes have been proposed to overlay the information onto the carrier. The most popular scheme is amplitude shift keying. In this scheme, the amplitude of the carrier is changed between two levels, say A0 and A1, where A0 represents one of the logical states and A1 represents the other logical state. The modulation index is a parameter that denotes the change in the amplitude level between the two states. For example, a modulation index of zero represents no change in the level, while a modulation index of one indicates that the amplitude of one of the signals, say, A0 is equal to zero. Using a larger modulation index introduces a larger difference between the two levels, and hence makes the system more

immune to noise. However, if one of the levels is close to zero, there is very little energy that is being transferred to the tag during this period. This poses some challenges to the design and operation of the tag itself. Therefore, a reasonably high value of modulation index is used for RFID application, especially if the tag has no power source of its own and is energized by the reader.

2.3.2. *RFID tag*

An RFID tag in its basic form could be made of a simple inductor in parallel with a capacitor. This could be easily designed to operate in the HF band. The inductance and the capacitance are chosen such that they form a resonance circuit that resonates at 13.56 MHz. When this tag is brought close to the reader antenna, the tag induces back emf into the reader antenna, which can be sensed by the reader. This way, the reader knows the presence or absence of the tag. This is called a "1-bit" tag, and is used in electronic article surveillance to protect goods in shops. One of the major problems with this system is false triggering. Any article that has similar resonance characteristics as that of a tag, e.g. a bundle of electrical cable, can potentially trigger the system and generate a false alarm. However, simplicity and cost has made this system very popular.

It is possible to reduce the false alarm rate by incorporating a diode in the tag. A diode is a non-linear element and hence is capable of generating harmonic frequencies. Consider a capacitance diode connected to an antenna. When this tag is exposed to a RF carrier at 2.45 GHz, the diode generates a second harmonic at 4.9 GHz. This signal can easily be picked up by a receiver that is tuned to 4.9 GHz. Instead of sending a pure carrier, it is possible to modulate its amplitude or frequency. The harmonic generated by the tag also contains the same modulation, and hence can be used to distinguish the signal generated by the tag and any interference. This reduces the possibility of false alarms. This, again, is a 1-bit tag and has limited applications.

It is possible to make the tag a little more sophisticated and store more information. This is achieved by attaching an integrated circuit

(IC) to the terminals of an antenna. An UHF tag with its antenna and the IC is shown in Figure 2.8. The antenna geometry is chosen so that the terminal impedance of the antenna is equal to the complex conjugate of the IC terminal impedance. This way, maximum RF power is delivered to the IC. The IC consists of a detector stage that rectifies the incoming RF signal, and the capacitor acts like a filter removing the ripple from it. The rectified and filtered signal is used to power up the electronics, which respond to the query sent by the reader by generating a bit stream. This is used to modulate the load connected in shunt with the antenna and hence change the backscattered signal from the antenna.

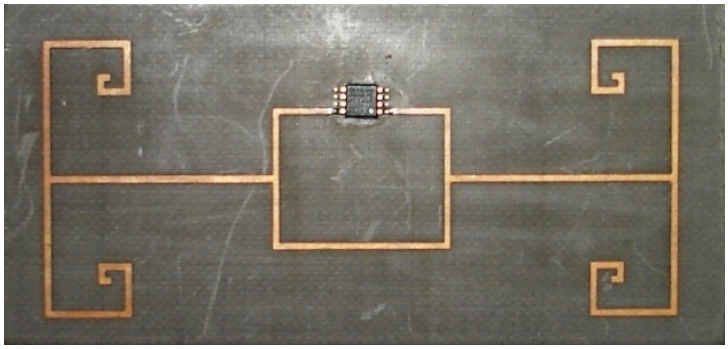

Figure 2.8. *Photograph of an UHF RFID tag showing the antenna and the integrated circuit*

2.3.3. *RFID middleware*

A typical RFID system can have several readers and tags (operating in different frequency bands and using various protocols), and several applications accessing these tags via the readers. It is important to provide a seamless connectivity between the RFID hardware and the application by insulating the applications from the RFID hardware. In systems with large amounts of raw RFID data being generated at the reader end, it is necessary to perform some kind of pre-processing of data before the information is passed on to the application. Such tasks are performed by a software subsystem known as a middleware.

General middleware architecture is comprised of three components (see Figure 2.9):

– device interface;

– core processing interface;

– application interface.

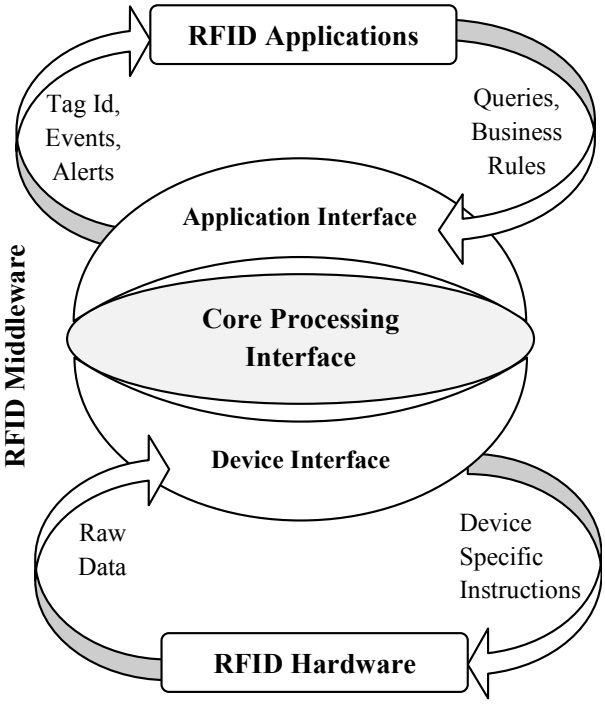

Figure 2.9. *RFID middleware architecture*

2.3.3.1. *Device interface*

The device interface provides the necessary functionality to establish a connection between the core processing interface and the RFID hardware. This forms one of the peripheral components of the middleware and is also known as edgeware. This interface enables RFID systems to discover, manage and control readers and tags. In a

large deployment of an RFID system consisting of several hardware devices of different makes and kinds, discovering and configuring them could be a tedious task. Physical distance could also add another dimension to the problem.

The device interface enables the communication between core processing and the RFID hardware by serving as a buffer between them and shielding one from the other. In this way, the differences between readers become invisible to the functions and the applications of core processing interface. Device interface is also responsible for directing data to the correct reader. If a new hardware is added to the existing system, all that needs to be done is to modify the device interface so that the system is able to recognize and communicate with the new hardware.

2.3.3.2. *Core processing interface*

The decision-making component of the middleware is the core processing interface. The core processing interface gets the raw RFID data from the RFID hardware. The core processing interface manages and manipulates the large amount of raw RFID data before passing them on to the application interface. The processing is also sometimes referred to as filtering. It includes removal of partial, erroneous, duplicate or redundant data. Usually the application has enough control over the way the core processing interface filters the raw data. The filtering process reduces the amount of data flowing into the application interface.

Information flow also takes place in reverse order, i.e. from application to RFID hardware. The core processing unit converts the business rules coming from the application into corresponding device instructions and then passes them on to the device interface, which then passes these instructions to the appropriate devices.

2.3.3.3. *Application interface*

The last component of the middleware is the application interface. The application interface forms a boundary between the core processing interface and enterprise applications (such as warehouse management, enterprise resource planning and supply chain

management, etc.). It is also a form of edgeware that is responsible for delivering RFID data to and from enterprise applications.

The communication between the application interface and the core processing interface takes place using a uniform format. However, the application interface interacts with different kinds of applications, and hence uses formats compatible with each of the applications. Therefore, one of the important tasks of the application interface is to convert the data from application-specific format into a common format that is used by the core processing interface. The advantage of this design is that, if a new application needs to be integrated into the existing RFID system, it is sufficient to modify the application interface.

The basic architecture of several published middleware solutions is more or less similar. In every middleware solution, the names of the component are different but the functionality provided by them is almost the same.

2.4. Issues

An RFID system has a high reliability when operating under controlled conditions. For example, consider a reader trying to read a tag, when both the tag and the reader antennas are placed in free space. As long as the tag is within a specific distance of the reader antenna, the reader will be able to read the tag. In a practical scenario, the tag is attached to an object whose electrical properties are different to that of free space. This generally degrades the performance of the tag (in exceptional circumstances it can enhance the performance). Further, there could be several tags trying to communicate with the reader and several readers trying to read several tags at the same time. This results in a collision of data being transferred between the readers and tags. Algorithms to avoid collisions have been proposed and successfully used to solve some of these issues.

Consider a tag trying to communicate with the reader using either load modulation or backscattering when several other tags are present in its neighborhood. It is not possible for the neighboring tags to

detect the communication taking place between the tag and the reader. Therefore, the schemes used in a standard communication system for multi-access cannot be used here. Anti-collision schemes, very specific to the RFID system, have been proposed and are very effective in enabling several tags to communicate with the reader.

Binary search algorithm is one of the most popular anti-collision schemes used in the RFID system. This algorithm relies on the fact that the reader is capable of detecting a collision when multiple tags respond simultaneously. This is possible when using Manchester coding to transmit the data [FIN 03]. Let us suppose that there are several tags in the vicinity of the reader, and each of the tags has a unique serial number. If the reader issues a command asking the tags to respond back with their serial numbers, all the tags receiving this command will respond back with their respective serial numbers, causing collision. Now the reader issues a request command with a parameter, asking the tags whose serial number is less than or equal to the parameter to respond. Thus the reader is able to select a group of tags that would respond to the command. If there is no collision, the reader gets the serial number of the only tag in the sub-group, and selects the tag by issuing the select command with its serial number as the parameter. The reader can perform read and write operations on the selected tag. If there is a collision, the reader issues another request command by lowering the value of the parameter, thereby targeting a smaller group of tags to respond.

If there are multiple readers operating in the same space, they avoid collision with each other by a procedure known as listen-before-talk. In this scheme, a reader always listens to the air space for any transmissions from other readers before transmitting.

Propagation of electromagnetic waves is influenced by the environment. Therefore, the amount of energy reaching the tag antenna depends on the interaction of the waves and the environment in which the reader and the tag are placed. For example, a tag placed in front of a large electric conductor is equivalent to a current (that is established on the tag) and its image radiating into free space. If the total field due to the tag current and its image is zero at the reader antenna, the tag cannot be read. Due to the interaction of the

environment with the electromagnetic fields radiated by the reader, there could be null field regions. Placing a tag in such regions will not excite the tag, and hence it cannot be read.

The behavior of a tag stuck on a dielectric sheet, such as a wooden board or a glass sheet, depends on the permittivity of the material, thickness of the material and the location of the tag itself. For example, it is not quite intuitive to predict the performance of the tag as the thickness of the material increases, permittivity changes or if the tag is placed such that the slab itself blocks the line of sight path.

Consider a tag attached to a wooden board and placed at a distance of about a meter from the reader antennas (see Figure 2.10). The transmission power of the reader is increased in steps of 0.1 dB and an attempt is made to read the tag. The lowest transmission power at which a tag is read, which is known as the "threshold power", is recorded. Threshold power is the smallest transmission power required to detect (read) the tag with all other parameters held constant. It is also possible to measure the threshold power for writing data into a tag. Usually while writing into a tag, the tag is placed in a controlled environment, which is less challenging. Therefore, the threshold power for writing a tag is usually not very important.

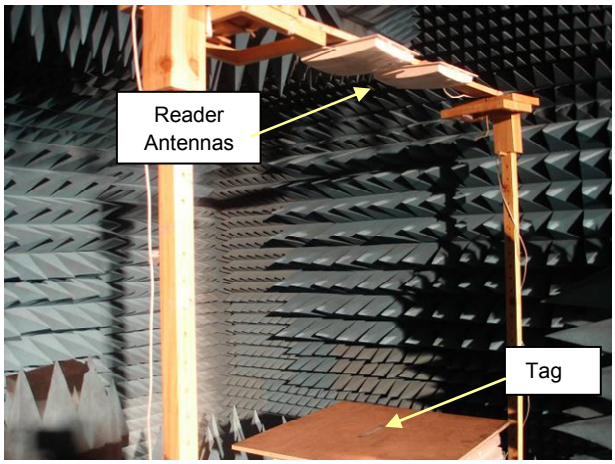

Figure 2.10. *Photograph of the measurement setup placed inside an RF anechoic chamber*

Threshold power can be used to compare the performance of a tag placed in different environments. Higher threshold power indicates degradation in the system performance. Another parameter that could also be used for this is the "read range". Read range is the longest possible distance at which a tag can be read with all other parameters held constant. Lower threshold power corresponds to a longer read range.

Consider a tag placed above a wooden board, as shown in Figure 2.10. The reader antennas are placed at a height of about 1 m from the surface of the board. The measurements are carried out inside a shielded RF anechoic chamber so that the interference from external signals and reflection from structural members are minimized. Measured threshold power as a function of board thickness (d) is shown in Figure 2.11. The wooden boards used in this study are 17 mm thick. Zero thickness indicates that the measurement is carried out without any board. As the board thickness increases, the threshold power increases, and reaches a maximum when d = 51 mm, indicating degradation in the performance of the tag. Further increase in the thickness results in improvement in the tag performance.

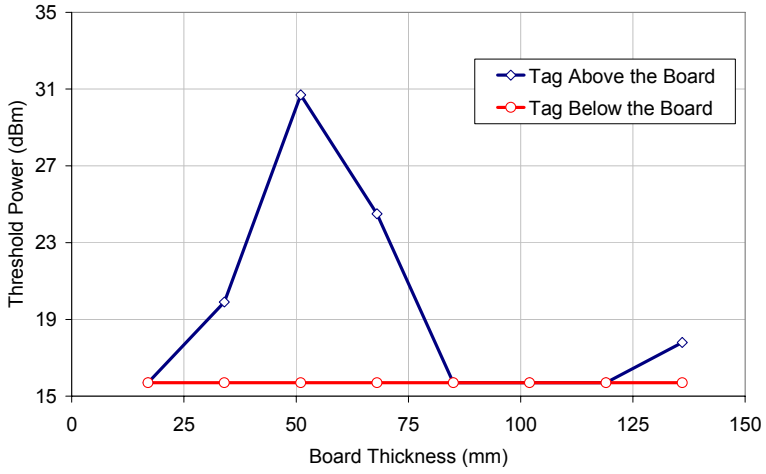

Figure 2.11. *Threshold power for the tag placed on wooden board (distance between reader antenna and tag: 119 cm)*

A similar experiment has been conducted with the tag placed below the board. In this configuration, the tag is detected with the transmission power set to 15.7 dBm, the lowest transmission power that the reader can be set to. This is indicated by the flat line in Figure 2.11. When the tag is placed below the board, the wooden board blocks the line of sight between the reader and the tag. In spite of a blocked line of sight path, the tag has increased performance.

Privacy of data stored in the tag becomes an issue when these are associated with people. For example, in the retail sector, it is possible to link the product (via the data stored in the tag attached to it) and the person buying it (through his or her credit card number). If a tag can be associated with a person (via a tag stuck on the shirt that the person is wearing), the RFID system using a collection of stationary readers could be used to track the person's movement [GAR 06].

Security of information stored on the tag also plays a crucial role in several applications. Issues such as tampering with the data stored in the tag, altering the association between the tag and the product, collecting security-related data stored on the tags, etc. have prompted designers to implement encryption techniques to secure the information on the tag itself.

2.5. Bibliography

[FIN 03] FINKENZELLER K., *RFID Handbook*, 2nd edition, John Wiley and Sons, 2003.

[GAR 06] GARFINKEL S., ROSENBERG B. (eds), *RFID Applications, Security and Privacy*, Addison-Wesley, 2006.

[PAR 05] PARET D., *RFID and Contactless Smart Card Applications*, John Wiley & Sons, 2005.