

Chapter 2

Characteristics and Limitations of Conventional RFIDs

2.1 Introduction

Although RFID technology has been proven to be sufficiently adequate for some applications, such as toll collection and anti-theft systems, there are numerous other applications that cannot benefit from this technology due to some of the limitations of the conventional RFID technologies. With the widespread interest and usage of RFIDs, the vulnerabilities of current RFID systems are becoming apparent. These limitations are directly related to the environment that the tags and readers communicate. This environment consists of both the wireless channel and the physical object that the tags are attached to. Various objects and systems in the wireless channel can cause a range of signal degradation such as attenuation, multipath fading, and interference to the RF signal carrying the tag information. Since the reliability of an RFID system is directly dependent on the robustness of the tag-reader RF link, the signaling scheme becomes a fundamental area of study for characterization and further performance improvement of such systems.

To date, most of the commercial RFID systems use narrowband signaling (continuous sinusoidal waveforms) for their tag-reader RF link, therefore they face the same difficulties that any narrowband wireless communications system may encounter. In this chapter we start with a general overview of the issues associated with narrowband signaling in RFID systems. Then we provide a comprehensive performance analysis of some of the commercial UHF RFID systems to characterize their performance and report on their capabilities and limitations for various applications.

The chapter ends with a brief discussion on ultra-wideband technology and how it can address many of the challenges associated with existing RFID systems. This discussion sets the ground for Chaps. 3, 4, 5, and 6 that offer an extensive discussion on use of UWB technology in RFIDs with detailed overview of implementation aspects of UWB pulses, discussion on UWB antennas for RFID tags and readers, and overview of special applications that could benefit from UWB RFIDs.

2.2 Physics of Narrowband Signaling

RFID systems that use narrowband signaling for tag-reader communications face certain technical challenges related to the physical properties and propagation characteristics of narrowband RF signals. Figure 2.1 represents a narrowband signal in time and frequency domain.

As shown in Fig. 2.1, a narrowband signal uses a specific carrier frequency and has well-defined signal energy in a very narrow frequency band [1]. The nature of continuous waveforms (CW) and their high power spectral density in a very narrow frequency band, limits the suitability of narrowband signals in many RFID applications. These limitations include susceptibility to detection and tampering, poor performance around metallic objects, signal blockage, privacy issues, inadequate range of passive tags, high power consumption of active tags, and limitations to world-wide operations. The above-mentioned limitations and challenges are discussed in great detail in the following subsections.

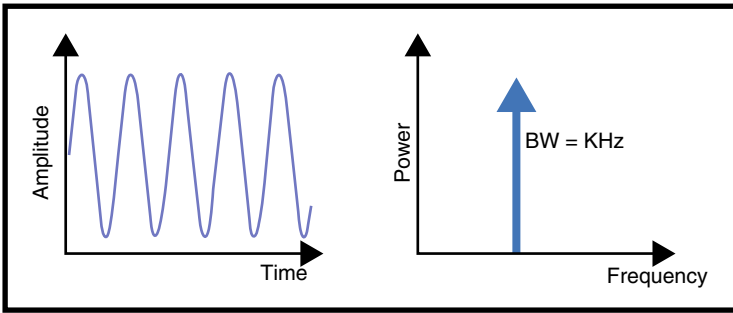


Fig. 2.1 A narrowband signal in time domain (*left*) and frequency domain (*right*)

2.2.1 Performance Limitations Around Metallic Surfaces

One of the major challenges that RFID systems with narrowband signaling face is the poor performance around EM reflective objects and materials. This is due to multipath phenomenon caused by reflection of continuous RF waveforms from metallic surfaces that can destructively add and degrade the received signal. Figure 2.2 represents multipath phenomenon in narrowband signaling.

Although multipath effects can also degrade the performance of active tags, their effect on passive tags can be more dramatic. Since passive RFID tags have to extract power from their reader's transmitted signal, if the energy transfer is not efficient due to antenna impedance mismatch near conductors, such as a metal surface, the tag will not power up and will fail to operate. Because antenna efficiency is a function of frequency, the lack of frequency diversity can result in significant performance degradation of tags that are attached to metal surfaces. Figure 2.3

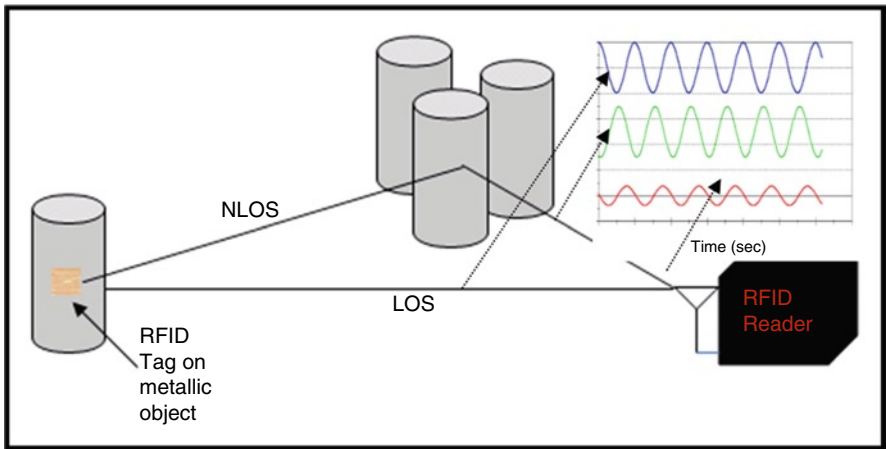


Fig. 2.2 Representation of multipath phenomenon in a wireless link on narrowband signals

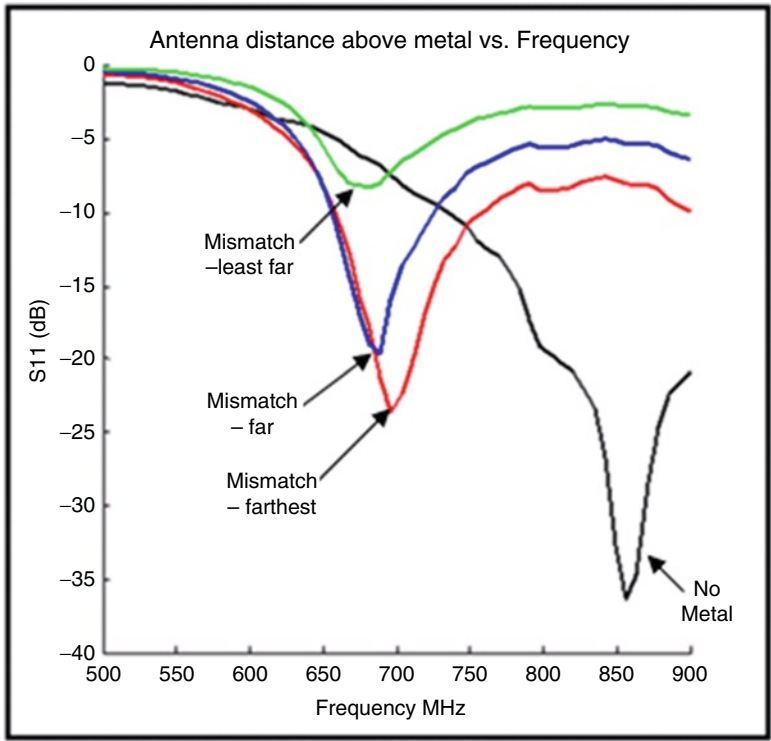


Fig. 2.3 Simulated response of a typical UHF tag over a metallic surface at various distances and as a function of frequency. There is a large impedance mismatch as the tag gets closer to the metallic object

shows the simulation results of reflection coefficient (S_{11}) versus frequency for a typical UHF passive tag at various distances from a metallic object.

As shown in the above simulation, the passive tag's antenna becomes de-tuned in the presence of a metallic object. The shift in resonance frequency from the tag's operating frequency (for example, 850 MHz) and hence the impedance mismatch between the tag and reader frequencies causes the tag to receive less energy from its reader. This will cause severe deterioration of the read range and therefore undermines the performance of the passive tag. Figure 2.4 shows the simulated radiation pattern of a UHF tag antenna in free space and on a metallic object.

As shown in Fig. 2.4, the performance response (radiation efficiency) of a UHF tag antenna severely degrades when it is located in the close vicinity of a metallic surface [2]. Benchmarking of UHF passive tags in the presence of conductive materials is presented in Sect. 2.3.

In theory HF passive tags (operating at 13.56 MHz) generally performs better, compared to UHF tags, around metallic surfaces due to their lower frequency and better penetration properties. However, these tags have shown serious limitations in read range when they are in contact or in close vicinity of a metallic surface. Figure 2.5 represents the read range performance of a commercial passive HF tag versus its distance from a metallic object.

As shown in Fig. 2.5, the read range of the HF passive RFID tag is noticeably reduced as the tag gets closer to the metallic object to a point that there is no read capability when the tag is placed directly on the metal. Since HF tags use inductive coupling to communicate with their reader, the “tag-on-metal” challenge for such tags can be explained by the Eddy current induced from metallic surface that is hit by the magnetic field generated between the tag and its reader. This induced Eddy current generates a magnetic field that is in opposite orientation of the original magnetic field between the tag and its reader (Lenz's law). Figure 2.6 illustrates the change in magnetic lines due to Eddy currents when tag is placed on a metallic object.

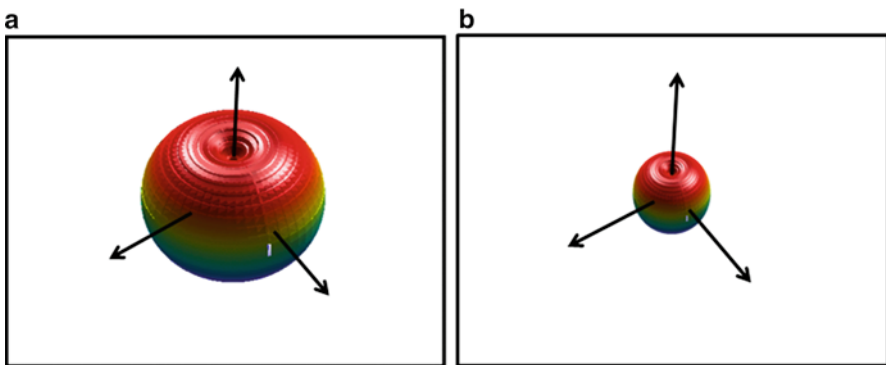


Fig. 2.4 Simulated radiation pattern of a UHF tag antenna in (a) free space and (b) on a metallic object

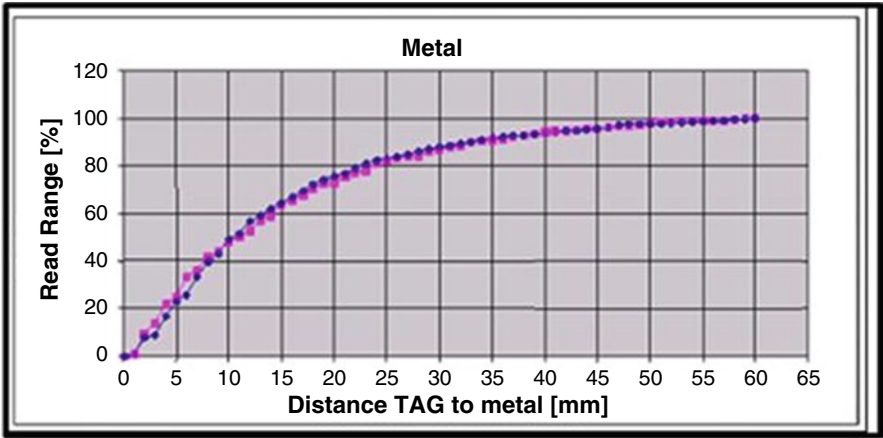


Fig. 2.5 Effect of metallic objects on tag-it transponders (Courtesy of texas instruments, reprinted with permission [3])

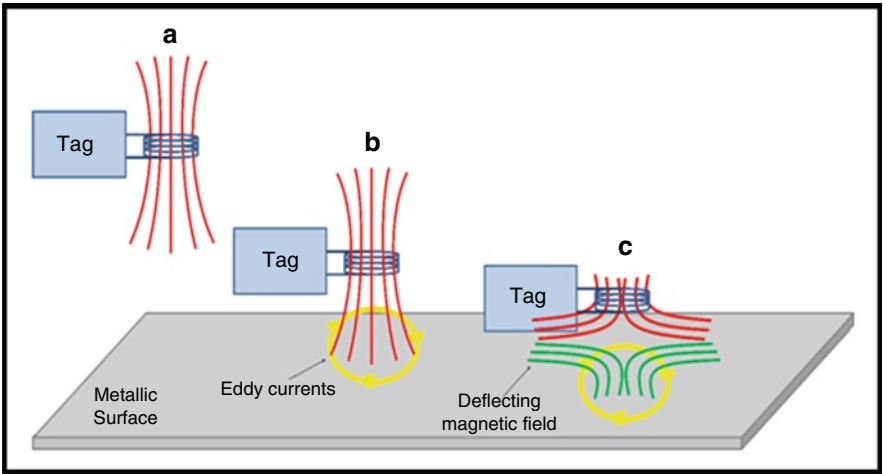


Fig. 2.6 Illustration of the change in magnetic lines as the tag gets closer to a metallic surface (a) tag in air, (b) tag near metal (c) tag on metal

The interference between the two magnetic fields results in magnetic deflection; causing poor performance of HF tags around metallic surfaces since the tag’s coil will not receive enough magnetic flux to power up.

The fact that RFID tags perform poorly in the presence of metallic objects can be used in shielding/coupling attacks by adversaries. In shielding attacks the tag-reader communications is disrupted by wrapping the tagged item in a piece of aluminum foil, where in coupling attacks the tagged item is placed near a ferrous material that can detune the tag frequency to stop the communications with its reader.

2.2.2 Signal Detection and Jamming

Signal jamming and tampering is another serious concern in many RFID applications for monitoring assets of high value. Since the narrowband signals, used in some conventional RFID systems, have well defined RF energy in narrow frequency bands (as shown previously in Fig. 2.1) they are extremely vulnerable to intercept and detection. Therefore such signals can cause all kinds of security and privacy concerns such as sniffing/eavesdropping, cloning, tracking, and hindering or blocking service. The following section explains some of the common threats to narrowband RFID systems at physical layer level because of their highly detectable signal.

Sniffing/Eavesdropping Attacks

Eavesdropping is considered as passive attack where unauthorized RFID readers can capture the transmission between a tag and its reader from a long distance without the holder's knowledge [4]. There is a misconception that RFID systems that use magnetic coupling are relatively secure due to their short read range. For this situation, since the eavesdropper does not need to power up the tag, it can read tag information from a longer distance. In addition, high gain antennas or a set of antenna arrays can be used to detect tags at more extended ranges leading to violation of privacy. Some of these concerns include: accessing personal data from RFID enabled passports for identity theft, or obtaining account information from RFID enabled credit cards [4] (Fig. 2.7).

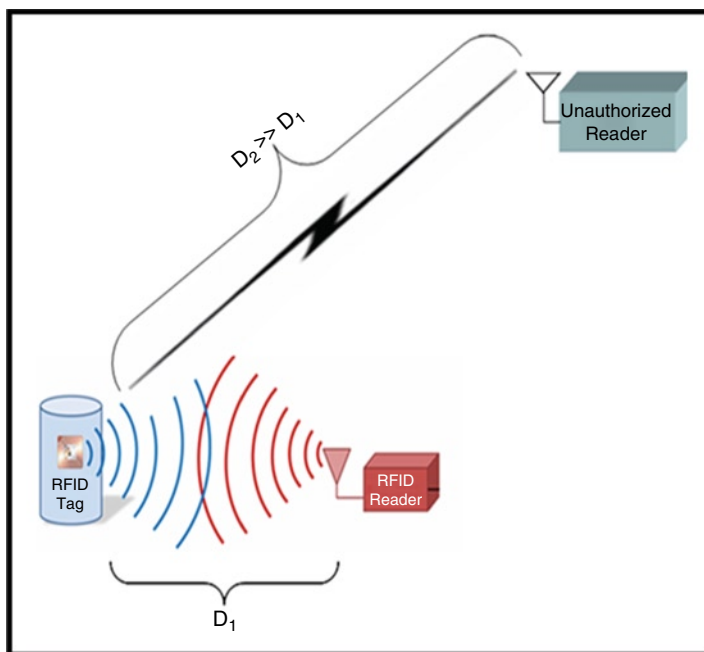


Fig. 2.7 Example of eavesdropping/sniffing attack where a sensitive unauthorized reader detects the tag information from a much longer distance (D_2) than its intended reader (D_1)

Spoofing/Cloning and Replay Attacks

Once the RFID signal is detected, tag information can be copied to an unauthorized blank tag by adversaries, called cloning [5, 6]. The cloned tag sends the same electromagnetic signal to the reader; this fake transmission fools the monitoring system thinking that a high value item is still in its place.

As shown in Fig. 2.8, first a sensitive unauthorized reader detects the tag information from a long distance (step 1); then the detected tag information is copied to a cloned tag (step 2); finally, the cloned tag replaces the stolen item and constantly sends its information about its presence to the authorized reader (step 3). This vulnerability could allow illegal access to all kinds of valuable and sensitive items/information that are secured by RFID monitoring. An example of spoofing attack would be the illegal modification of a passport-tag.

Relay Attacks

This type of attack is just like a man in the middle scenario, where one or multiple unauthorized readers can be placed between a tag and its reader to detect and change or counterfeit the transmitted signal between the tag and its legitimate reader [7]. This type of attack will fool the reader for similar scenarios that were described in the case of spoofing and cloning.

As shown in Fig. 2.9, the difference between the relay attack and spoofing attack (Fig. 2.8) is the information stored in the unauthorized tag. In spoofing attacks,

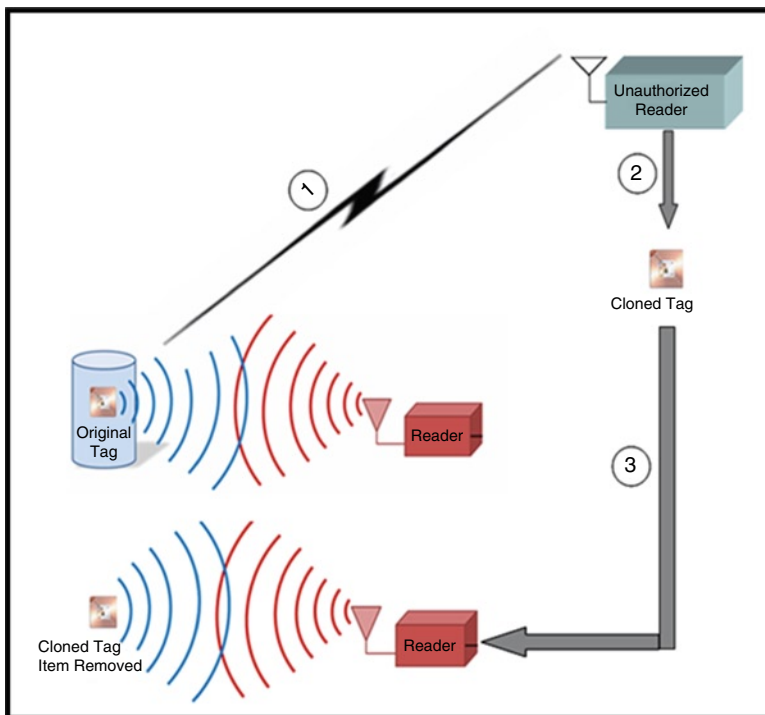


Fig. 2.8 Representation of spoofing attack in RFID systems

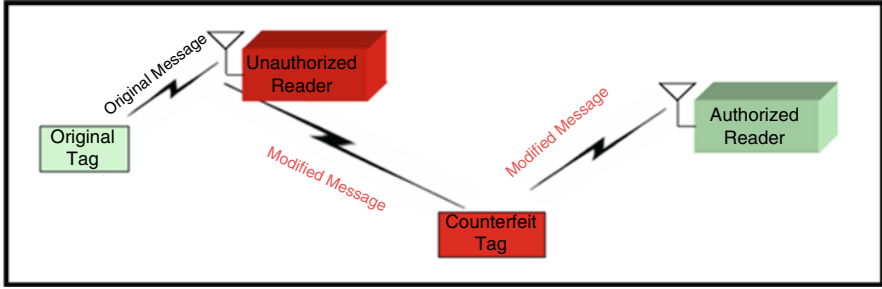


Fig. 2.9 Example of the relay attack, the original tag data is modified by the unauthorized reader and the counterfeit tag, before it gets to its authorized reader

the unauthorized tag has the exact same information as the original tag (cloned version), while in the relay attacks the unauthorized tag sends a different message to fool the authorized reader (Fig. 2.9).

Tracking Attacks

Unauthorized trackers can trace a tag transmission to the specific tagged item. Tracking attacks can help the hacker to locate and replace the tag for malicious activities or monitor the movement of assets and people for criminal reasons. This would be a serious concern in scenarios such as tagging of military assets that can be located and detected by adversaries.

Denial of Service (Jamming or Blocking)

Once the RFID transmission signal is detected, hackers can use interferers at the same operational frequency to jam the original signals and hinder the service to authorized users. Denial of service is an unavoidable problem in narrowband RFIDs since the tag/reader signal is very easily detectable (refer to Fig. 2.1).

Another form of denial of service is blocking the tag from receiving the reader powering signal in passive tags or blocking the transmission signals in the active tags by wrapping them in a metallic foil (refer to Figs. 2.2–2.6). The effects of metal on RFID tags were extensively discussed in Sect. 2.2.1, and is discussed further in the next section.

Denial of service attacks can help shoplifters to disrupt the service while stealing a product.

2.2.3 Signal Fading and Blockage

Fading, shadowing, and signal blockage is commonly found in narrowband communication systems. Walls, machinery, and foliage, can result in loss of signal in narrowband RFID systems making them unreliable for real-time monitoring

applications. Furthermore, for unauthorized access to an RFID tagged item, the item can be placed in a metallic container or simply wrapped in an aluminum foil. The metallic enclosure creates a Faraday cage shield so the RFID tag becomes unreadable. This phenomenon can be shown by calculating the skin depth of the metallic shield enclosing the tag. Skin depth is a representation for penetration depth of electromagnetic signals within a conductor, given by (2.1).

$$\delta_s = \sqrt{\frac{2}{\omega \cdot \mu \cdot \sigma}} \quad (2.1)$$

where: δ_s is skin depth (m), ω is the angular frequency (rad/s) equal to $2\pi \cdot f(\text{Hz})$, μ is the permeability (H/m), and σ is the conductivity (mho/m). Based on the values of conductivity and permeability from [7], the skin depth for aluminum in 900 MHz (UHF) RFID tags is around 2.5 μm . Since a thin aluminum foil has about 200 μm thickness, the depth of penetration of 2.5 μm makes aluminum foils opaque to narrowband signals at UHF frequencies.

Using the skin depth equation above, we can see that HF and LF tags have higher skin depth and therefore, better chance of penetrating through metal. For example, a typical LF tag with frequency of 132 KHz, will have a skin depth of 206 μm that can barely pass the aluminum foil obstruction. It's important to mention that penetration through other materials including various metals depends on their conductivity and permittivity and can be calculated from (2.1) using available data for μ and σ of various materials in [8].

2.2.4 High Power Used by Active Tags

As explained in the previous chapter, active RFID tags are fully powered transponders that require an internal energy source to power up their on-board electronics such as RF transceivers, microcontrollers or processors, memories, and other sensors integrated with them. This class of tags typically consumes a large amount of power for achieving data transmission to long ranges with high data rates. Most of the power used by an active tag is used by the transceiver and microcontroller/microprocessor blocks. The transceiver circuitry in active tags consumes a large amount of energy in standby mode in order to receive every incoming signal. Although the state-of-the-art energy storage systems such as 1 cm^2 lithium battery can supply several years of continuous power supply at 10 μW , the standby power of the transceiver circuit in most active tags exceeds 10 μW . Hence, the several years of power provided by the battery will last only months or days for typical active tags (depending on the level of information they provide and the number of times they transmit in a day).

It's also important to emphasize that the transceiver circuitry in narrowband active tags are complex with many components that adds to the size, and power

consumption of the tag. These components are specific to narrowband tags since tag-reader communications uses a specific carrier frequency, therefore, mixers and local oscillators are needed to translate the carrier frequency to baseband and the need for carrier recovery stage at the receiver end.

The high power consumption in narrowband active tags leads to the following disadvantages in their usage:

- Large tag size
- High cost of production
- Low reliability due to limited operational lifetime
- Long term and expensive periodic maintenance for changing tag batteries

Each of the above parameters plays an important role in the effectiveness of active tags for various applications. As a general rule, although active tags are designed for longer ranges, long-range communication can soon drain the power in the tag, and thus make monitoring quite unreliable.

2.2.5 Limited Range for Passive Tags

Since passive tags do not have an internal source of power and collect energy from their reader signaling, their communications range is very limited. In the passive tag category, the UHF and microwave tags have longer read ranges than the LF and HF tags. This is due to the fact that the operation of microwave and UHF tags is based on the far field communications, because the distance between the tag and reader antenna is typically longer than one wavelength in such frequencies (33 cm for UHF, and 12 cm for microwave tags) (Fig. 2.10).

In far field communications, the power in the transmitted signal decays in proportion to the square of distance from the antenna, where in near field communications (LF and HF tags) the signal power decays as the cube of the distance from antenna as shown in (2.2) and (2.3) respectively [9].

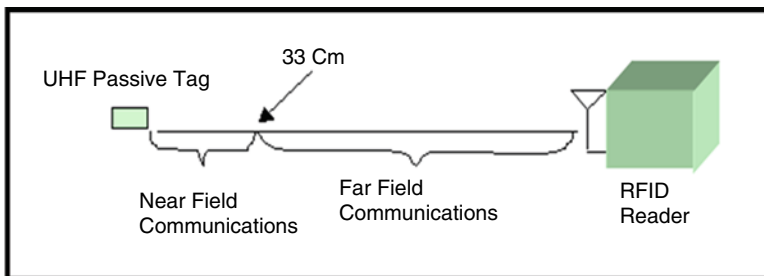


Fig. 2.10 Illustration of near field, and far field propagation modes for UHF passive tags. The near field-far field boundary (33 cm) is defined by one wavelength of the tag's operating frequency

Table 2.1 Forward link (reader-to-tag) budget analysis of a typical passive UHF tag at 915 MHz operating frequency

Reader transmit power	30 dBm
Aperture and path loss (3 m)	−41 dB
Reader transmit antenna gain	6 dBi
Tag antenna gain	2 dBi
Received power at tag	−3 dBm
Required power to activate the tag	−10 dBm
Link margin	+7 dB

$$P_{tag} \propto \frac{1}{d^2} \quad (2.2)$$

$$P_{tag} \propto \frac{1}{d^3} \quad (2.3)$$

where P_{tag} depicts the power received at the tag from its reader, and d is the distance between the tag and its reader.

Although UHF tags have longer communication range compared to lower frequency passive tags, their read range is still not acceptable for many applications. Link budget analysis of the forward link (reader-to-tag) for a typical UHF tag in Table 2.1 shows that under regulatory restrictions at a 3 m distance, the forward link margin is marginal (about 7 dB). This theoretical margin is based on the assumption that tag-reader communications occur in free space. In many practical scenarios, the 7 dB margin can easily be reduced to an even lower number, often by many factors, in real environments. The environmental factors affecting the tag performance include the presence of interferers, conductive and absorptive materials such as metal and liquids respectively, diffraction, and shadowing effects. The decrease in forward link margin demands even shorter distances between UHF passive tags and readers for reliable communications.

The calculations in Table 2.1 is based on the following operating parameters:

- Reader transmit power at 1 W (maximum FCC limit)
- Free space path loss at 3 m per (2.4)

$$P_r = P_{tx} \frac{A_e}{4\pi d^2} \quad (2.4)$$

where P_r is the received power at the tag, P_{tx} is the transmitted power from the reader, A_e is the effective aperture equal to $\frac{\lambda^2}{4\pi}$, and d is the distance between the tag and its reader.

- Reader antenna is assumed to be isotropic with 6 dBi gain.
- Tag antenna is assumed to be isotropic with 2 dBi gain.
- Power required by the tag is 100μ Watt limited by silicon process. Typically, CMOS process can reduce the power requirement of the tag.

Although forward link (reader-to-tag) in UHF passive tags is limited to short ranges (< 3 m), the reverse link (tag-to-reader) is only limited to the reader sensitivity.

Table 2.2 Reverse link (tag-to-reader) budget analysis of a typical passive UHF tag at 915 MHz operating frequency

Tag incident power	−3 dBm
Aperture and path loss (3 m)	−41 dB
Tag antenna gain	2 dBi
Reader receive antenna gain	6 dBi
Tag modulation loss	−6 dB
Received power at reader	−42 dBm
Reader sensitivity	−100 dBm
Link margin	+58 dB

Sensitive readers can pick up signals as low as −90 to −110 dBm, so the reverse link margin could be very large as shown in Table 2.2.

The numbers in Table 2.2 is based on the following operating parameters:

- Tag incident power of −3 dBm (from Table 2.1)
- Symmetric path loss for forward and reverse links
- Tag modulation loss of −6 dB defined by (2.5):

$$K = \alpha |\rho_1 - \rho_2|^2 \quad (2.5)$$

where K represents the tag modulation loss, α modulation coefficient, ρ_1 and ρ_2 are tag reflection coefficients.

As shown in Table 2.2, the reverse link has a very large margin (58 dB), hence the UHF reader is capable of reading a passive tag from much longer distance compared to the distance it can power up the tag. So the limitation in range for UHF passive tags is really related to their forward link. If UHF tags can be powered up more efficiently, sensitive readers can pick up tag's backscattered signals from very far distances (Km range, with a reader sensitivity of −100 dBm). This can cause a vulnerability in detecting tags by unauthorized readers from long distances (refer to Fig. 2.7).

2.2.6 Limitations to Worldwide Operation

Operation of the currently available RFID systems is limited to the specific narrowband frequencies used by the readers and transponders. Since the UHF tags operate in unlicensed ISM band, EPCglobal (worldwide RFID governing body) has rules for regulating the use of such frequencies around the world. Table 2.3, shows the UHF frequency allocations assigned by EPCglobal for various regions of the world [10, 11].

As shown in the Table 2.3, some frequencies are not available in different parts of the world, so there is no global solution for narrowband RFIDs and the tags operating frequency needs to be modified based on the specific region that they will be operating at.

Table 2.3 UHF operating frequency regulatory specifications for various countries

Country	Frequency band
America	902–928 MHz
Australia	918–926 MHz
Argentina	902–928 MHz
Brazil	902–928 MHz
China	No allocations yet
Hong Kong	920–925 MHz
India	865–867 MHz
Japan	950–956 MHz (Experimental purposes only)
Korea	910–914 MHz
Peru	902–928 MHz
Singapore	923–925 MHz

2.3 Performance Benchmark of UHF Passive Tags

The discussions in Sect. 2.2 revealed some theoretical limitations for the conventional tags that operate based on narrowband signaling. However, their true capabilities and limitations need to be evaluated in real world scenarios for a better understanding of their practicality in various applications. In this section we present a comprehensive performance benchmark of Commercial-Off-the-Shelf (COTS) RF tags to determine how they perform in the presence of conductive and dielectric materials such as metals and water, respectively. The benchmark presented in this section only covers the performance of some of the conventional UHF passive tags due to their popularity in many applications, and the fact that their performance depends heavily with respect to their environment. The benchmarks presented in sections 2.3.1 and 2.3.2 are excerpts from a report based on a previous research taken in University of Kansas for RFID Alliance Lab.¹ Although our main interest in this section is to show performance benchmarks of UHF tags with respect to metals and liquids, more interesting benchmarking information with respect to other important parameters such as orientation sensitivity, read in isolation and population, and variance of tags consistency is available in the report from University of Kansas [12, 13].

2.3.1 Read Performance near Metal and Water

As discussed earlier, the presence of a material near tags changes the characteristics of the tags antenna. The materials that are common and pose greater challenges to tag

¹Courtesy of Karthik Ramakrishnan from University of Kansas [12]. Portions reprinted with permission from “Performance Benchmarks for Passive UHF RFID Tags” Master’s Thesis by Karthik Ramakrishnan, University of Kansas, 2003.

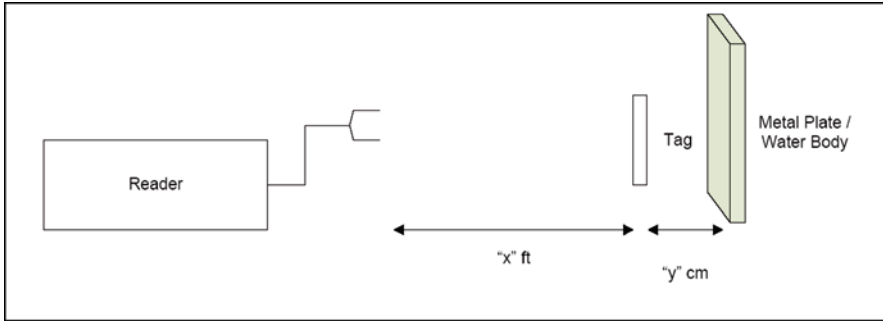


Fig. 2.11 Test setup for performance in front of materials

performance are metal and water. Water and metal affect tag performance in a number of ways. They provide multi-path and create fading zones. In fact, metals can be used to boost the performance of tags. The presence of high-dielectric material in the near field of the tag causes detuning of the antenna, so the antenna would resonate at a lower frequency. The presence of material changes the impedance bandwidth of the antenna and reduces the power transfer efficiency. The benchmarks in this section are aimed at studying the effects of tag performance near these materials.

2.3.1.1 Test Procedure

In this experiment the setup shown in Fig. 2.11 was used to evaluate the performance of UHF passive tags in the presence of conductive or absorptive materials.

The median tag from each tag model should be oriented at their best possible orientation in front of a metal plate whose size is comparable to wavelength. If the testing is done in front of water, a water body whose size is again comparable to wavelength should be used. The attenuation at which the tag becomes unreadable should be measured at various separations from the metal/water. Small separations between the tag and the material are the most interesting and most useful regions where the benchmark should be measured (as the tags are generally stuck on the materials). The attenuation is increased slowly until the tag becomes unreadable. This attenuation value should be measured for different separation between tag and material. The following test parameters should be considered for this benchmark:

- Separation range
- Separation step size
- Number of attempts done by the reader
- Attenuation step size – increments in attenuation
- Best orientation of the tag
- Separation between the reader and tag

Since the metric is an attenuation value at a particular separation, it is recommended that at least a few hundred read attempts are to be performed before assuming that the response rate has gone down to 0%. For statistical accuracy, the

Table 2.4 Parameters for read performance in front of metal/water

Test parameter	Parameter value
Environment	Free-air
Reader model	Class 0 – Matrics AR 400 Class 1 – Alien 9780
Reader software version	Class 0 – 03.01.09 Class 1 – 3.7.3
Antenna type	Bi-static and circular polarized
Number of antennas	1
Protocol of the tag	EPC Class 0/EPC Class 1
Multi-protocol reader settings	Scans only Class 0/Class 1 depending on protocol of the tag
Cables to connect antenna and reader	Factory default
Maximum power	32.5 dB
Application	Custom software on reader
Separation between tag and reader	34 in.
Separation range from materials	Metal – 0–2 cm Water – 0.55–2.55 cm
Separation step size	0.24 cm
Number of attempts	100
Attenuation step size	0.1 dB
Best orientation of the tag	(0,0)

number of attempts should be higher. The testing should be done in non-noisy environments, ideally, anechoic chamber is preferred.

2.3.1.2 Experiment

We placed the tag in front of the reader antenna at a distance of 3 ft as shown in Fig. 2.11. The tag and the material were separated in free-air. The material for the experiment was a large flat piece of steel ($\approx 2\lambda \times 5\lambda$) in front of metal while it was a 10-gallon aquarium filled with water and in front of the water. The separation was varied from 0 to 2 cm in steps of 2.5 mm from the material. It should be noted that the thickness of the glass plate (0.55 cm) has to be taken into account when the experiment is done in front of an aquarium. The attenuation at which the tag became unreadable for each separation was noted. Table 2.4 lists the parameters that were used for both the experiments in front of metal and water. Different readers were used for reading Class 0 and Class 1 tags.

2.3.1.3 Results and Lessons Learned

Tags in Front of Metal

Figure 2.12 shows the comparison of performance for four Class 0 tags in front of metal.

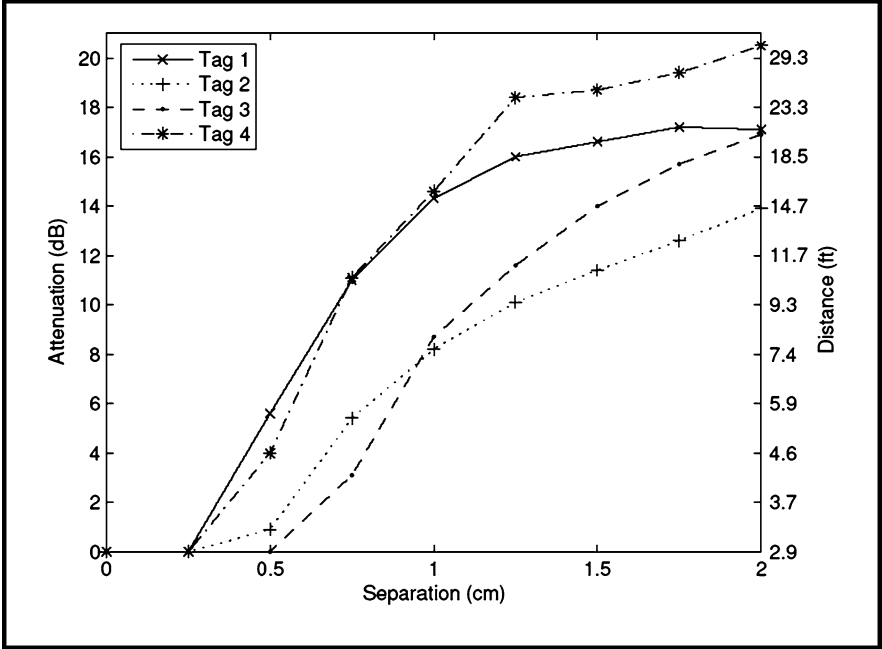


Fig. 2.12 Tag performance in front of metal

As seen in Fig. 2.12, Tag 1 and Tag 4 have better performance than the other two tags starting from a separation of 5 mm. It should be noted that Tag 1 design is supposed to work better in reflective environments and as can be seen from the experiments it turns out to be the best in front of metal when compared to the Class 0 tags. The performance of Tag 4, a dual dipole design is comparable to Tag 1. Even in our free-air experiments, Tag 4 was a fundamentally better tag compared to other tags.

It can be seen that, all the tested tags were unreadable at a separation of 2.5 mm from metal. Some of the tags had a good performance at a separation of even 5 mm from metal.

Tags in Front of Water

Figure 2.13 shows a selection of Class 1 tags that we had tested in front of water.

As can be seen in Fig. 2.12, Tag 4 is the best performing in front of water at a distance of 0.8 mm. However, it should be noted that the same tag is not the best performer in free air. Tag 3 is a better performer in free air but is highly detuned when it comes in front of water. Tag 2 is the worst among the compared Class 1 tags. This showed that some of the tags were tuned to work in front of water but it should be noted that none of the tested tags worked at a separation of 0.55 mm from water (when the tags were directly on the container).

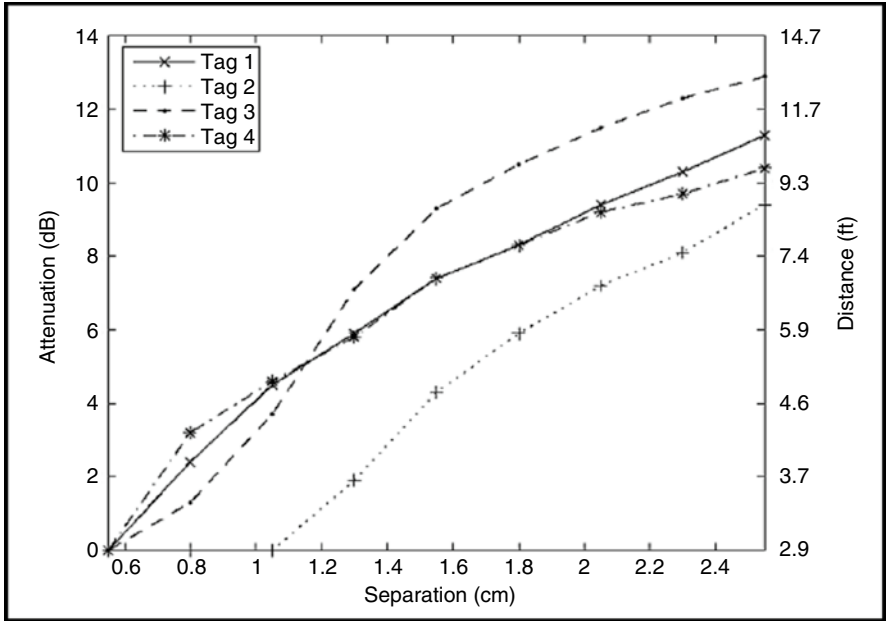


Fig. 2.13 Class 1 tag performance in front of water

2.3.2 Frequency Dependent Performance

As seen in the previous section, presence of materials near tags affects the frequency response of the tags. The objective of this benchmark is to determine the changes in the frequency response of tags near materials.

2.3.2.1 Test Procedure

The same test procedure described in Sect. 2.3.1 should be used for this benchmark. The tag should be read at a fixed frequency and then the frequency is varied. The attenuation at which tag is unreadable is measured across all the frequencies of interest. The following test parameters should be considered for the benchmarks:

- Separation range
- Separation step size
- Number of attempts done by the reader
- Attenuation step size – increments in attenuation
- Fixed frequencies of interest
- Separation between the reader and tag
- Best orientation of the tag

Table 2.5 Parameters for frequency response in front of materials

Test parameter	Parameter value
Environment	Free-air
Reader model	Thingmagic Mercury 4
Reader software version	2.4.22
Antenna type	Bi-static and circular polarized
Number of antennas	1
Protocol of the tag	EPC Class 0/EPC Class 1
Multi-protocol reader settings	Scans only Class 0/Class 1 depending on protocol of the tag
Cables to connect antenna and reader	Factory default
Maximum power	32.5 dB
Application	Custom software on reader
Separation between tag and reader	34 in.
Separation range from materials	Metal – 0–2 cm Water – 0.55–2.55 cm
Separation step size	0.25 cm
Number of attempts	1,000
Attenuation step size	0.1 dB
Best orientation of the tag	(0,0)

The higher the number of frequencies under consideration, higher would be the resolution of the frequency response.

2.3.2.2 Experiment

The experiment parameters for the frequency response in the presence of metal and water are summarized in Table 2.5.

The experiment described in Sect. 2.3.1 was repeated when the reader was programmed to do the reads in a single, fixed frequency and then the frequency was varied. The parameters used for this experiment are listed in Table 2.5.

2.3.2.3 Results and Lessons Learned

Tags in Front of Metal

It was seen in Sect. 2.2.6 that the ISM band in UHF frequencies varies between different countries. The ISM band frequencies in various countries are 860–868 MHz in Europe, 902–928 MHz in USA, and 950–956 MHz in Japan. Most of the antennas that are used for tags are resonant antennas and it is widely known that the presence of high dielectric like water near antennas changes their resonant frequency. Thus, if a tag is to be read globally, they should perform well across all these frequencies.

In this benchmark, the experiment was performed at 902 MHz, 915 MHz, 928 MHz, and 955 MHz. We measured the attenuation at which the response rate

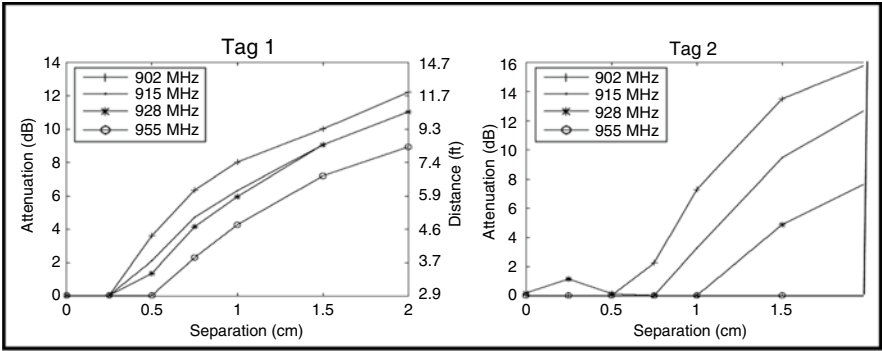


Fig. 2.14 Comparison of tags in front of metal based on operating frequency

goes down to 0% across different frequencies. Figure 2.14 shows the frequency dependent performance of two different tags in front of metal.

It should be noted that Tags 1 and 2 are readable at all the frequencies in free-air. In front of metal, Tag 1 performs better at lower frequencies and degrades a little bit as the frequency is increased. This is typical performance of most of the tags near metal. However, as can be seen with Tag 2 there are drastic changes in performance with increase in frequency. At 2 cm separation, Tag 2 performs better than Tag 1 at 902 MHz but as can be seen, Tag 2 is unreadable at 955 MHz near metal. This means that if a metal product with Tag 2 on it is shipped from USA to Japan, it would be readable and would work when it is shipped but would be completely unreadable in Japan.

Tags in Front of Water

A similar observation was made with the above tags when they are in front of water. However, we observed one more interesting behavior of the frequency response in front of water.

The Fig. 2.14 shows two tags that have a similar behavior but different performance levels. In this Figure, the performance of the tags at different separation from water container is shown. It can be clearly seen that both the tags have good performance at 955 MHz at a separation of 2.55 mm. As the separation is decreased, the performance degrades rapidly at 955 MHz compared to moderate decrease at other frequencies. This is a common behavior that we have observed for all the tags when the tags are in front of water. The performance rapidly decreases at higher frequencies whereas there is comparatively gradual decrease in performance at lower frequencies (Fig. 2.15).

Another observation about performance is that at small separations, Tag 1 still has some link margin at which the tag is still readable. Thus, it is quite evident that Tag 1 is better in terms of performance than Tag 2.

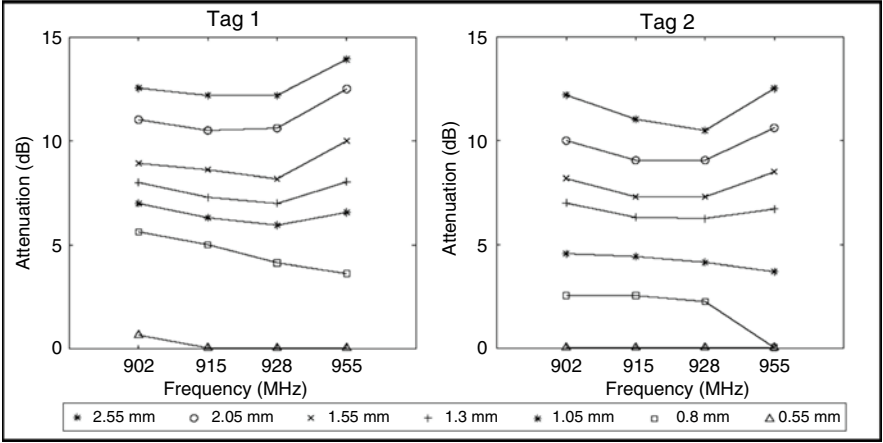


Fig. 2.15 Comparison of tags in front of water based on operating frequency

Frequency dependent analysis gives insight into the detuning effects of the antennas, permits a way to analyze better antenna designs for specific materials, and provides a performance criterion through which a globally visible tag can be developed.

2.4 Overview of Ultra-Wideband Technology

Many of the difficulties in tag-reader communications associated with narrowband signaling discussed earlier in this chapter can be addressed through the use of ultra-wideband (UWB) technology in new generations of RFID systems. In UWB signaling scheme, extremely narrow RF pulses are used to communicate between transmitters and receivers. The duration of UWB pulses are typically few hundred picoseconds to a few nanoseconds. These narrow pulses naturally generate very wide bandwidth in the range of few GHz in frequency domain as shown in Fig. 2.16.

Referring to Fig. 2.16, as the frequency spectra of the UWB pulses are spread out over many GHz of bandwidth with a power spectral density in the noise floor, trans-

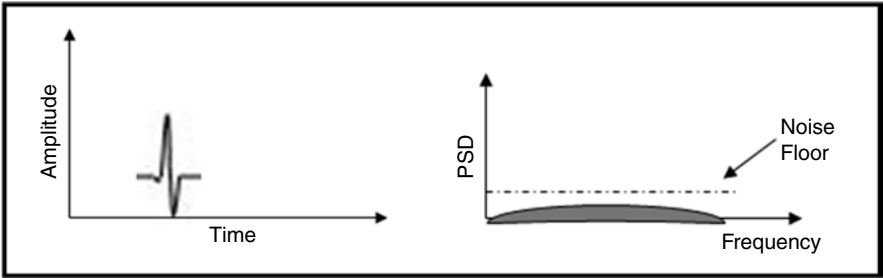


Fig. 2.16 A typical UWB pulse (left) in time domain (right) in frequency domain

mitted pulses are not only very difficult to detect when transmitted with a certain time-space coding, but are effectively invisible to unauthorized readers. In addition the extremely wide spectrum of UWB pulses generates large channel capacity and a robust link with respect to multi-path and diffraction in harsh RF propagation environments such as cluttered and reflective environments. Figure 2.17 shows a comparison of frequency spectrum of narrowband and UWB signals in a multipath channel, where signal fading is visible in narrowband signals and UWB spectrum keeps a steady signature.

Another advantage of UWB systems is their simpler transceiver circuitry due to carrierless transmissions. Therefore, UWB systems can be developed with smaller form factor and lower cost compared to narrowband systems.

It's important to note that despite the many advantages that come with the nature of UWB signaling in communications systems, they face serious technical challenges. These challenges include: synchronization between the transmitter and receiver for narrow RF pulses, difficulty in sampling such short duration pulses, and lack of similarity between the transmitted and received pulses. Figure 2.18 shows an example of transmitted and received UWB pulses in a multipath channel that makes the detection difficult using conventional pulse detectors or classical matched filters (CMF).

Ultra-wideband conceptually is not a new technology as it was first demonstrated by Guglielmo Marconi in 1901 for transmitting the Morse code sequences across the Atlantic Ocean using spark gap radio transmitters [1]. This technology was heavily used in military radars back in late 1960s and gained its momentum after FCC's approval of the commercial applications of ultra-wideband in early 2002. FCC's approval of 7,500 MHz unlicensed frequency band for ultra-wideband systems allowed two different approaches to UWB signaling, single band and multi-band. Single-band UWB approach is the traditional UWB where very short duration pulses (impulse radio) are transmitted where it occupies the entire spectrum with minimum bandwidth of 500 MHz and fractional bandwidth of larger than 20%. This is similar to time and frequency representations of a UWB signal shown earlier in Fig. 2.16. However, in another approach, referred to as the multi-band approach, multiple overlapping smaller bands with bandwidths greater than 500 MHz have been used to construct the UWB signaling; an example of a multi-band UWB spectrum is shown in the following Fig. 2.19.

As shown in the Fig. 2.19, multiband UWB approach has similarities to narrowband frequency hopping techniques. Although the two schools of thought are often skeptical of the other approach to UWB technology development, both approaches are technically viable and have their unique advantages and challenges. The supporters of the single-band approach believe that the high complexity of the multi-band systems due to complex Fast Fourier Transforms (FFT) makes multi-band system more complex. While advocates of multi-band approach believe that their technique is easier to synchronize compared to very narrow radio impulses used at single-band approach.

Ultra-wideband technology is well discussed in various books and publications therefore; we won't go into the details of UWB technology in this book. However, we will focus our attention to the use of UWB signaling in RFID systems in the following chapters. The details of advantages of UWB signaling in RFID systems is

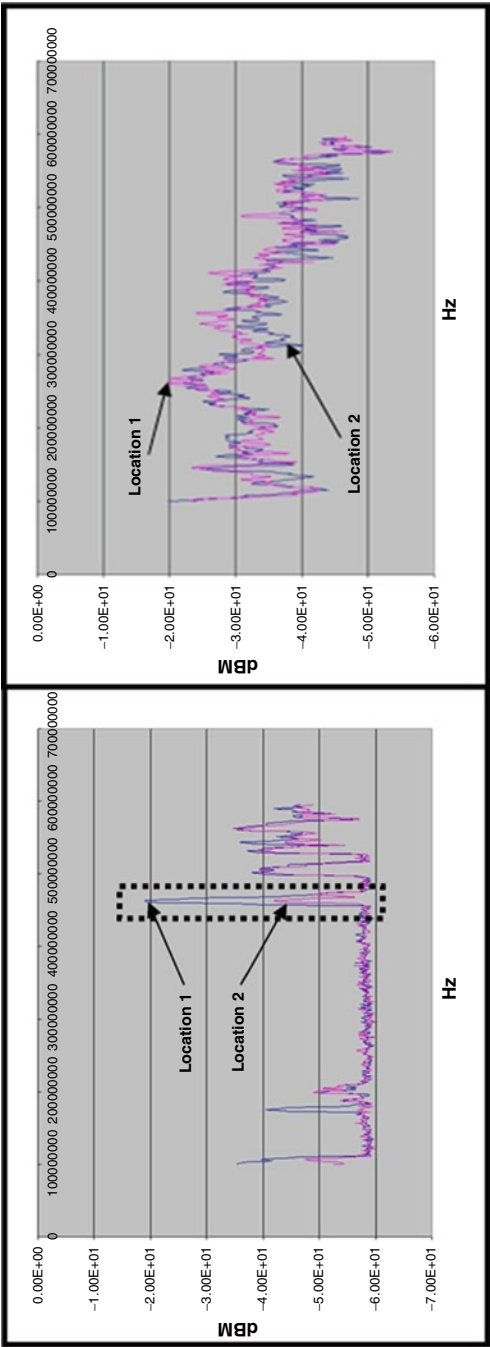


Fig. 2.17 Multipath effect on *(left)* narrowband signals, and *(right)* UWB signals. Please note that the vertical axis is not to the same scale for both graphs. This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract, DE-AC52-07NA27344-LLNL-PRES-401143

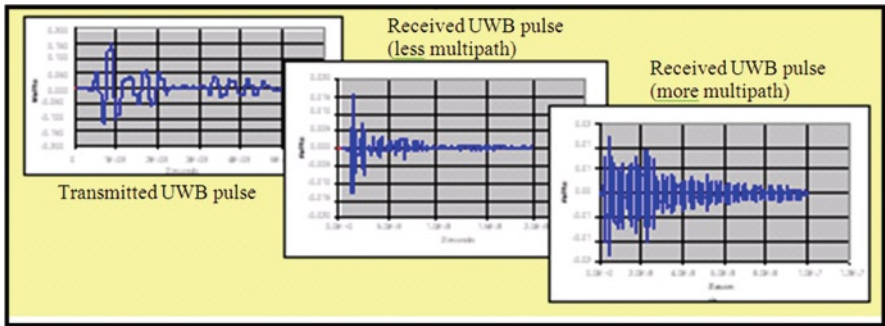


Fig. 2.18 Example of multipath effect on UWB signals. Pulses can get stretched heavily depending on the amount of multipath in the wireless channel²

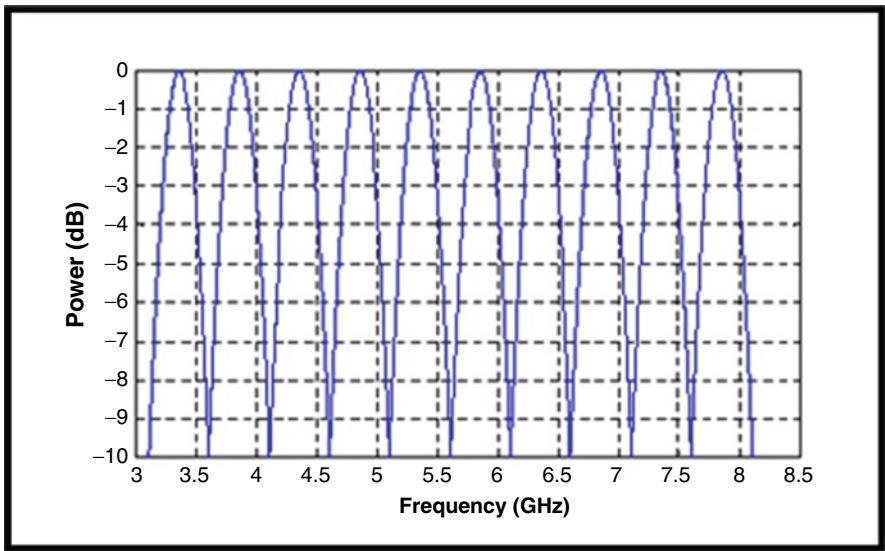


Fig. 2.19 Representation of UWB signaling in multi-band approach

discussed in Chap. 3, followed by implementation aspects of UWB signals in RFIDs in Chap. 4. A comprehensive discussion on UWB antennas for RFID systems is covered in Chap. 5 and applications of UWB RFID systems are discussed in Chap. 6.

For more detailed information on UWB technology, we encourage the reader to study some of the references listed in this chapter’s bibliography section.

²This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract, DE-AC52-07NA27344-LLNL-PRES-401143

2.5 Summary

Although narrowband RFIDs have reached a considerable level of maturity where they can be useful for many applications, the limitations posed by utilizing narrowband signaling for tag-reader communications limits their widespread adoption in some practical environments. In this chapter we covered the fundamental physical limitations that are caused by narrowband signaling scheme in tag-reader communications. The limitations that were discussed this chapter included: (1) security and privacy of tags due to various types of attacks including spoofing, cloning, and denial of service; (2) performance degradation in the presence of metals; (3) limited lifetime of active tags; (4) short range for passive tags; (5) and limitations to world-wide operations.

Also, in this chapter, to complete our discussions on limitations of narrowband signaling in conventional RFID systems, we presented results of a detailed report on benchmarking of some commercial narrowband UHF systems.

Finally, we ended the chapter with a brief overview of ultra-wideband technology to set the ground for later chapters for discussing more advanced topics such as advantages of UWB signaling for RFID systems, as well as UWB implementation aspects, and UWB antennas for RFIDs.

References

1. "Ultra-Wideband Communications – Fundamentals and Applications", F. Nekoogar, Prentice Hall PTR, Aug. 2005. ISBN: 0131463268.
2. M. Eunni, "A Novel Planar Microstrip Antenna Design for UHF RFID", Master's Thesis defense, 2006.
3. <http://focus.ti.com/lit/an/scba018/scba018.pdf>.
4. http://www.nytimes.com/packages/pdf/business/20061023_CARD/techreport.pdf.
5. <http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grunwald.pdf>.
6. DN-Systems: BBC Reports on Cloning of the new e-passport. In: <http://www.dnsystems.de/press/document.2007-01-04.2112016470>.
7. M. Hlavac, T. Rosa, "A Note on the Relay Attacks on e-passports? The Case of Czech e-passports". In <http://eprint.iacr.org/2007/244.pdf>.
8. <http://encyclopedia2.thefreedictionary.com/Skin+depth+effect>.
9. R. Pappu, "The Physics of RFID", In: <http://ocw.cupide.org/NR/rdonlyres/Engineering-Systems-Division/ESD-290Spring-2005/5FE9474C-3365-463A-B1F5-6E9B252356DA/0/lect6.pdf>.
10. D. Yee, "RFID – moving beyond compliance...", RFID Summit Singapore (2004).
11. D. Brown, "RFID Implementation", ISBN-13: 978-0072263244.
12. K. Ramakrishnan "Performance Benchmarks for Passive UHF RFID Tags" Master's Thesis, University of Kansas, 2003.
13. D. Deavours, "UHF EPC Tag Performance Evaluation" a production of RFID Alliance Lab, May 2005.

Bibliography

- J.D. Taylor, Ed. *Introduction to Ultra-wideband Radar Systems*, (Boca Raton, FL. CRC Press, 1995).
- Avoine, G., Oechslin, P.: RFID Traceability: A Multilayer Problem. In: Patrick, A., Yung, M. (eds.). In: Proc. of the Ninth Int'l Conf. on Financial Cryptography and Data Security (FC'05), Lecture Notes in Computer Science, Vol. 3570. (2005) 125–140.
- Center, A.I.: 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specifications. In: Draft, www.epcglobalinc.org/standards/specs/900MHzClass0RFIDTagSpecification.pdf. <http://it.toolbox.com/blogs/adventuresinsecurity/securing-rfid-tags-9329>.
- Bolotnyy, L., Robins, G.: Physically Unclonable Function-Based Security and Privacy in RFID Systems. In: Proc. of PerCom'07. New York, USA (2007) 211–220.
- “Performance Benchmarks for Passive UHF RFID Tags” Master’s Thesis by Karthik Ramakrishnan, University of Kansas, 2003.
- Juels, A.: Strengthening EPC Tags Against Cloning. In: Proc. of ACM Workshop on Wireless Security (WiSe'05). ACM Press (2005) 67–76.
- Burton, G.J., Ohlke, G.P., (May 2000), Exploitation of millimeter waves for through-wall surveillance during military operations in urban terrain, Land Force Technical Staff Programme, Royal Military College of Canada, Kingston, Ontario.
- CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology. In: Interim Draft, <http://www.cdt.org/privacy/20060501rfid-best-practices.php>, (2006).
- Dimitriou, T.: A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks. In: Proc. of IEEE Conf. on Security and Privacy for Emerging Areas in Communication Networks, (2005).
- Envelope: Products. In: <http://www.emvelope.com/products>. (2008).
- EPCGlobal: Guidelines on EPC for Consumer Products. In: <http://www.epcglobalinc.org/public/ppscguide>, (2005).
- EPCGlobal: Class-1 generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz. In: *EPC Radio-Frequency Identity Protocols*, Vol. 1.1.0, (2005).
- Fedhofer, M., Dominikus, S., Wölkerstorfer, J.: Strong Authentication for RFID Systems Using the AES Algorithm. In: Proc. of Cryptographic Hardware and Embedded Systems (CHES'04), Vol. 3156. *Lecture Notes in Computer Science*. (2004) 357–370.
- Fishkin, K., Roy, S., Jiang, B.: Some Methods for Privacy in RFID Communication. In: Proc. of the 1st European Workshop on Security (2004) 42–53.
- Friedl, S.: SQL Injection attacks by example. In: <http://www.unixwiz.net/techtips/sqlinjection.html>, (2007).
- Garfinkel, S., Juels, A., Pappu, R.: RFID Privacy: An Overview of Problems and Proposed Solutions. In: *IEEE Security & Privacy*, Vol. 3. (2005) 34–43.
- Hancke, G., Kuhn, M.: An RFID Distance Bounding Protocol. In: Proc. of the 1st Int'l Conf. on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005) (2005) 67–73.
- ICAO. ICAO Document 9303. In: <http://mrtd.icao.int/content/view/33/202>, (2006).
- Inoue, S., Yasuura, H.: RFID Privacy Using User-Controllable Uniqueness. In: Proc. of RFID Privacy Workshop. MIT, Massachusetts, USA (2003).
- Juels, A.: Minimalist Cryptography for Low-cost RFID Tags. In: Proc. of the 4th Conf. on Security in Communication Networks (SCN'04), Vol. 3352. *Lecture Notes in Computer Science*. Springer-Verlag (2004) 149–164.

Ultra-Wideband Radio Frequency Identification Systems

Nekoogar, F.; Dowla, F.

2012, XVI, 160 p., Hardcover

ISBN: 978-1-4419-9700-5