Chapter 2
Background

The establishment of RFID based localization requires a deep understanding on the component, operation principle, and propagation of RF signals. It is necessary to introduce the background information about RFID systems before stepping towards the RFID based localization. In addition, we will introduce the related localization approaches in the literature in this chapter.

2.1 Radio Frequency Identification

2.1.1 RFID History and Practice

The RFID technology was derived by the usage of Radar for object detection. With the increasing demand of detecting airplanes beyond visual range, radar techniques were rapidly developed in 1930s. With the backscattered microwave, the radar operator was able to alert when the aircraft moved at hundreds of kilometers per hour. However, one of critical tasks of radar based detection was not well solved at that time, distinguishing the side to which the aircraft was belonging.

The first solution was found by the German air force in a simple way. Some fighters from the German air force suddenly performed some maneuvers, for example a roll, before the air combat. Sometimes, a squadron of fighters did this behavior without any reasons. Later, this behavior was intercepted as a very naïve but effective Identification of Friend or Foe (IFF) solution. By rolling together, the Luftwaffe pilots could change the backscattered signals to the radar, such that the "modulated" signals shown on the reader screen appeared a specific pattern. In this way, the German radar operators could identify them as the friendly targets. This story is a typical case to show how passive RFID systems work via backscattered radio waves.

Considering the basic goal, the information modulated into the maneuver based behavior is too limited for identification. First, the maneuver can be performed either by friendly or foe targets, lacking of effective protection on the modulated

J. Han et al., *Device-Free Object Tracking Using Passive Tags,* SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-12646-3_2

information. Second, the contained information by this behavior is also limited, for example, only 1 bit in a roll. But such an idea inspired the development of passive backscattering communication, which is the basis of RFID technology. The most distinct feature of passive backscattering is that the object is not with any transmitter. The object scatters back the radio signal transmitted from the radar station for identification.

After World War II, the RFID technique was not developed rapidly, due the highly expensive and large sized transponder. Later, with the development of very large scale integrated circuit (VLIC), people were able to produce extremely cheap and small chips as well as circuit components, resulting a rapid progress in the RFID manufacture. Using RFID tags to achieve more automatic and intelligent identification finds an increasingly requirements from many applications, such as the asset management, logistics, supply chain, access control, etc.

An RFID system comprises of three parts, the reader, tag, and backend server. The reader is used for read/write tags, determining the operating frequency and range. For most RFID systems, the tag is a media that stores certain information about the user or the object it attaches. The identity is the most commonly used information stored in the tag. Therefore, the identification, in which the reader retrieves the ID from a tag, is the most essential functionality of RFID systems.

Generally speaking, the major functionalities of the reader include:

- The reader communicates with the backend application via some standard interfaces. The backend application actively operates the reader for communicating with the tag, and exchanges with the reader with three major types of information: the information of tags (e.g., ID), identifier of the reader, and necessary information about the operation.
- The reader tackles the collision among tags, and identify each tag within its interrogation range. To this end, people develops the anti-collision algorithms for RFID systems.
- The reader can detect the error in the reading/writing tag procedures. Due to the ambient interference to the wireless communication between the reader and tag, the error detection and correction are very important for RFID systems to achieve reliable identification.

Normally, the backend server and the reader are jointly termed as "*reader*". Without loss of generality, we also term the combination of reader and backend applications as reader in the following. We show an example of RFID systems in Fig. 2.1.

2.1.2 Active and Passive RFID Tags

Three major types of RFID tags are currently available in the market. There are active, semi active (or semi passive), passive tags.

Active tags generate the high-frequency RF signals using the power from their own batteries. The battery also provide power to tags for their internal operations,

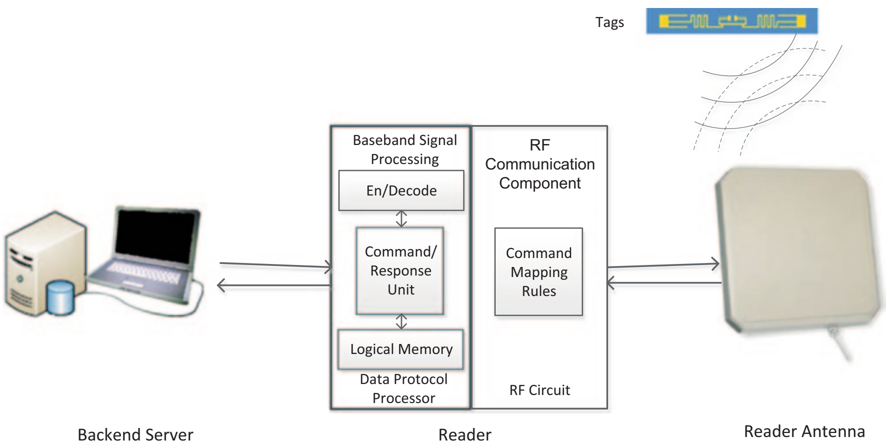

Fig. 2.1 An example of RFID Infrastructure

such as the modulation and computation. The normal operating range of active tags is often tens of meters, sometimes above 100 m. Due to limited capacity of battery, the lifetime of active tags is not long. It is non-trivial to replace the battery after deploying a active RFID system. The large size and high manufacture cost are other two issues for active RFID systems.

Passive tags are not with battery on board. They can only backscatter the RF signals sent from readers. Meanwhile, the passive tag harvests the energy from those signals for modulating its data to the backscattered signals. The interrogation range of passive tags is generally much shorter than that of active tags, e.g. ranging from only several centimeters to a few meters. On the other hand, passive tags are generally cheaper and smaller than their active counterparts, which is its major advantage for large-scale implementation.

Semi active (or semi passive) tags are a combination of active and passive RFID transponders. They use their own power for the modulation while adopting the backscattering data transmission pattern similar to passive tags.

The tag has two functional components, the antenna and chip. Figure. 2.1 shows a passive tag. The tiny rectangle in the center is its chip, while the other metal parts are its antenna. The chip is in charge of decoding/demodulating the command from the RF signal sent by the reader and encoding/modulating the response or data to the returned RF signal. As aforementioned, the active tag will actively generate the RF signal, while the passive tag will backscatter the RF signal sent from the reader. There are also two major types of antennas used by current RFID systems, coil and dipole antenna, for the inductive coupling and electromagnetic radiation systems, respectively. When the antenna is connected with the chip, it would introduce high capacitance and impedance. For achieving a good power matching, the total resistance should be equal to the maximum load resistance of antenna. On the other hand, the antenna is usually designed as a twisted shape to minimize its size Fig. 2.2.

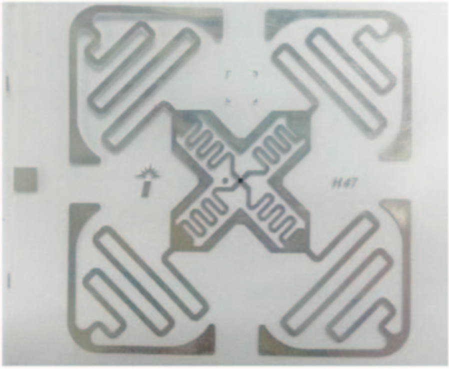

Fig. 2.2 An example of an RFID tag used at Wal-Mart. (Source: Wal-Mart)

2.1.3 Frequency and Operating Range

The most important factor in passive RFID systems is the operating frequency of the reader. Although the frequency used by existing RFID systems is widely distributed, say from 135 kHz to 5.8 GHz, the available frequency spectrum for a certain type of RFID devices is limited, e.g. 860~960 MHz for UHF passive tags. There are four typical frequency ranges used in practice: 135 KHz, 13.56 MHz, UHF (433 MHz, for active tags, 860–960 MHz for passive tags), 2.45 GHz, and 5.8 GHz.

The operating patterns between the reader and tags are separated into two groups. The RFID systems that use the frequency below 30 MHz are belonging to the inductive coupling, while those that use the frequency above 30 MHz are using electromagnetic radiation. The frequency selection is generally determined by consideration of RF wave's penetration and absorption. For example, the low-frequency RFID systems are usually used for the better penetration capability. For the higher-frequency RFID systems, the operating range is larger and the sensitivity is better than the lower-frequency one. In this paper, we focus on the passive UHF RFID systems working on the 860–960 MHz spectrum, where the bottleneck of operating range is the transmission power of the reader.

2.1.4 Inductive and Radiative Coupling

Generally, the RFID systems mainly use two ways for communication, inductive computing and radiative coupling.

The inductive computing is usually adopted by the lower frequency RFID systems, such as the LF and HF RFID tags. The inductively coupled transponder uses a large-area coil or conductor loop as its antenna. The reader also has its coil for the communication. The reader actively generates an electromagnetic field using its coil. If the wavelength of the operating frequency of the reader is much larger than the distance between the transponder and reader, the electromagnetic field can be treated as a magnetic alternating field, which penetrates the area around the coil. For

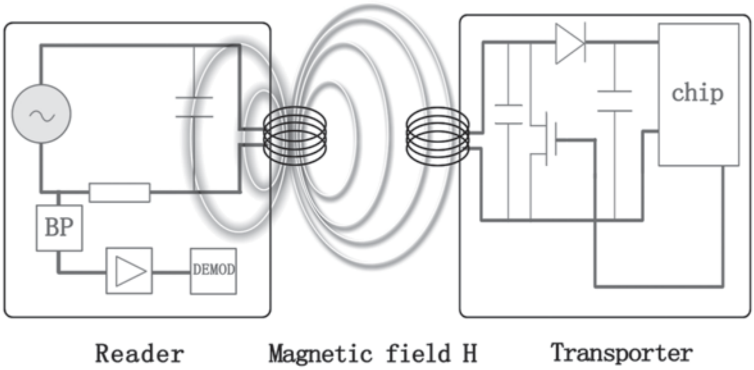

Fig. 2.3 An example of inductive coupling systems

the part that penetrates the coil of the transponder, it induces a voltage on the transponder's antenna. In addition, the inductive coupling is actually a transformer-type coupling, which the induced voltage is rectified and used as a power supply. Since the RF signal sent from the reader is not a stable and continuous power supply, a capacitor serves as an energy bank in the transponder. The transponder then requires certain time periods to charge the capacitor for accumulating sufficient energy for operation. In practice, the tag usually switches between two states, standby and power-saving modes in the charging procedure for achieving an efficient charging (Fig. 2.3).

Besides the charging cycle, the inductive coupling is also used for data transmission. The transponder activates an on-chip oscillator, resulting in a weak magnetic alternating field. Similarly, the generated magnetic alternating field also penetrates the reader coil, inducing a weak voltage on the reader coil. The modulation can be achieved by changing the on/off state of the impendence connected to the coil such that the induced voltage shows corresponding high/low state. In this way, the data can be transmitted between the transponder and reader.

Radiative coupling, also known as the electromagnetic backscatter coupling, support a long-range communication. The antenna of radiative coupling transponders is comparable in size to the wavelength of their operating frequencies, including the UHF frequencies of 868 MHz (Europe) and 915 MHz (USA), or the microwave frequencies 2.5 and 5.8 GHz. In the radiative coupling, the reader antenna radiates continuous electromagnetic waves (CW in short). According to the free space path loss principle, the CW power fades in a relationship to the square of the distance traveled. A portion of the wave interacting the transponder antenna induced a coupled current, which can be used as the power supply. Another portion of the original CW is scattered to different directions, in which a small portion of CW will be backscattered to the reader. In this procedure, the reader can modulate the data it transfers via amplitude shift keying(ASK), frequency shift keying(FSK), or phase shift keying(PSK). For the cost concern and simplicity of demodulation, the majority of passive RFID systems use ASK modulation. On the other hand, the IC circuit of transponder can change its impendence in time with the data to be transmitted, and hence vary the relationship between the impendence of transponder Z_T and the impendence of transponder antenna Z_A. In this way, the transponder modulates its data to the backscattered CW.

Corresponding to the inductive coupling and radiative coupling, there are two types of communication ranges between the reader and tag, near-field and far-field. According to [1], the boundary between the two fields is $R=2D^2/\lambda$, where D is the size of antenna and λ is the wavelength of antenna. In the near-field communication, the interaction between the reader's and tags' antennas is based on inductive coupling [2]. Far-field communication operates based on radiative coupling.

2.1.5 Dipoles Antenna and T-Match Structure

Most passive tags use a half-wave dipole antenna. In our system, Twins uses commercial passive tags modeled as Impinj E-41b in Fig. 2.4 The length of antenna is usually half of the wavelength $\lambda/2$, i.e. 16 cm (with the operation frequency 915 MHz). The antenna is bent to form a *meandered dipole* for further reducing its size. However, meandered dipole introduces mismatching impendence between the antenna and the IC circuit in the tag, which might result in a small power transfer coefficient and inefficient energy absorption. Manufactures then adapt a short antenna to connect the capacitive IC load, forming a T-match structure, as shown in Fig. 2.5. In this structure, the impedance is balanced between the longer meandered dipole (with the length of L) and shorter dipole (with the length of a). The IC of the tag connects to the meandered diploe via two wings of the short dipole Fig. 2.6.

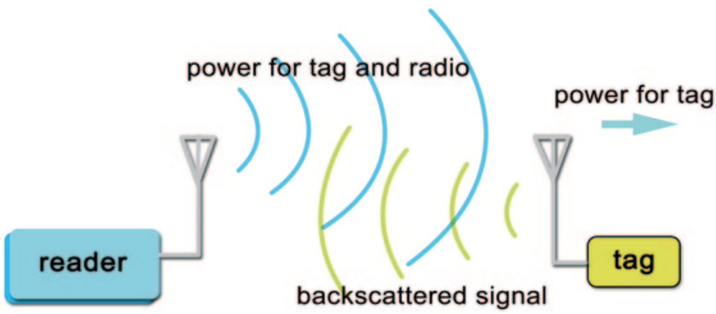

Fig. 2.4 An example of radiative/backscatter coupling systems

Fig. 2.5 Half-wave dipole antenna of passive tags

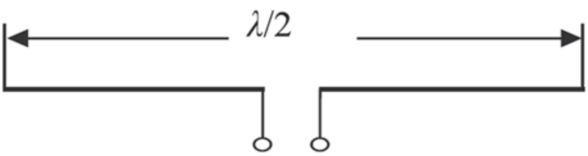

Fig. 2.6 Real tag model and T-match structure

2.2 Localization and Location Based Service

Location based services (LBSs) have been a part of our life. In the literature of indoor localization, many techniques have been proposed in the recent decades. Generally, they fall into two categories: model-based and fingerprinting-based.

2.2.1 Model-Based Indoor Localization

Model-based indoor localization approaches use geometrical models to figure out locations. In those methods, locations are calculated instead of retrieving from known reference data.

RSSI-based ranging algorithms calculate distances among nodes based on the Log-Distance Path Loss (LDPL) model according to the measured RSS values. These approaches decrease the localization accuracy due to the irregular signal propagation, especially in indoor environment. Lim et al. [3] use WiFi sniffers deployed at a known locations to measure the RSS from APs, and then use the LDPL model to build RSS map. Madigan et al. [4] use a Bayesian hierarchical model without the need of locations of the training points. However, they are still required to have prior knowledge about the AP locations. To avoid the use of AP localizations, EZ [5] builds the physical constraints of wireless signal propagation based on the LDPL model and uses the genetic algorithms to solve the positioning problems. RSSI is susceptible to multipath propagation, which results in large errors inside. Wu et al. [6] proposes to extract the dominant cluster of paths from CIR to reduce the ranging error from RSSI. They implemented a prototype, namely FILA, on OFDM based WiFi with off-the-shelf NICs, and leveraged the channel state information (CSI) to alleviate multipath effect at the receiver. Centaur [7] combines RSSI and acoustic ranging.

Other than the RSS related model, the geometric models are also exploited to characterize the relationship of signal between transmitters and receivers. PinPoint [8]and the work proposed by Werb et al. [9]use the time delay in signal propagation to estimate the distance between wireless nodes. GST [10] uses the difference in time of arrival (ToA) of the RF signal from multiple transmitters at known positions. Similarly, PAL [11] uses ToA between the UWB signals to a plurality of receivers to determine the position. Cricket [12] and AHLoS [13] utilize propagation delays between RF and ultrasound signals to estimate the location of wireless devices. These solutions usually require tight synchronization of time and equipment extra ranging hardware, which limits their applicability.

Angle-of-arrival (AoA) based techniques make use of multiple antennas to estimate the angle at which the signal is received, and their geometric relationship to locate the wireless transmitter. Even with access to the information of the raw signal using 8 antennas [14], they can be derailed in rich multipath indoor environments where the direct signal path is often blocked. To solve this problem, some techniques based AoA require 6–7 sophisticated antenna systems [15], not possible in low resolution WiFi hardware products. Recently the Array-Track system [16] achieves a very precise localization using the AoA calculated from a rectangular array of 16 antennas. Arraytrack uses spatial and temporal smoothing, and time-based AoA grouping to suppress the effect of multipath on the location estimation. Although these techniques will certainly improve the accuracy of localization, Arraytrack stops to identify the actual angle of the direct path, particularly within the constraints of linear antenna arrays offered by the hardware WiFi products. SpinLoc [17] and Borealis [18] require the user to do a complete a 360°± turn.

2.2.2 *Fingerprinting-Based Indoor Localization*

Fingerprinting based solutions are established upon a general paradigm that, for each state instance $p \in P$, there is a unique corresponded "fingerprint" vector $v_p \in V$.

When this v_p is detected again at another time, we know the system is currently at state instance p. When this paradigm is specialized in the localization problem, this is fingerprint-based localization.

In outdoor environments, most wireless signals are propagated in Line-of-Sight (LoS) mode. It provides well suitable environment for model-based localization, i.e. precise timing or ranging.

However, in indoor environments, the multipath propagation has the major effect. The received signal at the endpoint is the sum of a larger number of reflected signals. It is difficult to separate these reflections, and hence hard to adopt model-based system.

Fingerprint-based schemes shortcut this difficulty by directly focusing on the signal distribution at specific positions.

Although it requires nontrivial human labor to site survey the signal map, its environmental-robustness still demonstrates its strong practicability to both research and industry communities.

In the early development stage of fingerprint based localization, there are few assistant techniques to improve the accuracy. With the rapid spreading of smart phone, more hybrid solutions appear.

a. ***Fingerprint Types***

Among various approaches, RADAR [19] is the most famous and influential Wi-Fi fingerprint based localization system. It models the localization as a min-distance problem. In the deployment phase, the indoor environment is sampled by 2×2 m grid. For each grid, the RSS values from multiple APs are collected as the fingerprint for this grid. In the localization phase, the candidate position is the one which has the smallest "vector distance" to the fingerprint.

Since the human body may block the signal, the fingerprint shows large variance for different directions at the same spot. RADAR handles this problem by requiring sampling each position in 4 directions to alleviate this problem. The RADAR gains great success. It could achieve an average accuracy within 2 m, and most of fingerprint-based localization could be seen as variants of RADAR.

Horus [20] is widely accepted to be the most accurate Wi-Fi based fingerprint localization system. Its high accuracy relies on additionally deployed Wi-Fi sniffer devices. The additional Wi-Fi sniffers help create find-grained local RSS propagation model, which significantly improves the fingerprint accuracy. In experimental environment, the accuracy could be within 1 m.

In wireless signal domain, FM radio signal may be a promising medium for location fingerprint. The work proposed in [21] shows a FM radio signal based indoor localization system. The main protocol follows the RADAR scheme. The evaluations show that the FM radio RSS has much higher location distinction ability. The authors in [22] proposed an automatic FM fingerprint system by interpolating the RSS distribution map according to known indoor floor plan and pre-defined propagation model.

Wireless signal is not all about RSS. Channel State Information (CSI) or Channel Frequency Response (CFR) is another aspect of the signal. It is more find-grained PHY layer information than RSS. It reveals the amplitude and phase of wideband subcarriers. The works proposed in [23] and [24] proposed channel impulse response fingerprint based indoor localization. PinLoc [17] presents the first CSI-based indoor localization in rich multipath environment. These methods can generally achieve sub-meter fingerprint accuracy. However, since the channel response change very quick along spatial displacement, the fingerprints should be densely sampled.

Magnetic field also could be a type of fingerprint. [25] demonstrates a geomagnetism deviation based indoor localization system. The system is based on a discovery that the massive use of steel frame in modern construction alters the geomagnetism direction within the building. By recording the geomagnetism deviation for each spot, the geomagnetism could be used as the fingerprint. To measure the geomagnetism deviation, the authors built a rotational magnetometer. The evaluation shows strong de-correlation between spots.

Sound spectrum could be a natural fingerprint for indoor rooms. [26] proposed a room-level localization solely base on acoustic spectrum fingerprint. The advantage of acoustic fingerprint is that it does not require deploying infrastructures and it avoid the impact from the device variance problem commonly seen in Wi-Fi fingerprint solutions.

Besides the wireless signal, the ambient environment contains rich information to distinguish location. SurroundSense [27] is such a system. It traits the ambient sound spectrum, background color, and the like, as the "ambient fingerprint" to distinguish those spatial-nearby yet contextually-distant positions. A demonstrative example could be determine whether the user is at a bar or cafe, which are nearby according to GPS signal. Unloc [28] develops the idea of SurroundSense. It unified these ambient fingerprints as “Organic Landmarks” including sound spectrum, luminance, magnetic deviation, Wi-Fi landmarks, etc.

The localization for passive RFID tags is also an important problem. PinIt [29] proposed a RFID passive tag localization solution by densely deploying reference tags. PinIt uses synthetic aperture radar (SAR) technique to acquire the multipath profile for each reference tag. When the test tag is near a reference tag, their multipath profiles will be similar. By finding the reference tag which has the smallest difference, the position of test tag is determined.

b. *Crowdsourcing*

Crowdsourcing is a popular strategy trend that a difficult task is transformed and decomposed to many small and easy tasks. Each participant solves an easy task. All their efforts are then grouped together to have the difficult one finished. For fingerprint based indoor localization, the most difficult part is the tedious site survey procedure. If we could crowdsourcing this task, the fingerprint-based localization would become easy.

LiFS [30] proposed a system which employs the crowdsourcing idea. The major insight behind LiFS is that the adjacent fingerprint graph is highly similar to the floor plan routing graph. LiFS proposed an algorithm to automatically match these two graphs. In this way, it could eliminate the specific site survey task. Users only need to install and open an App in their smartphone. When people are moving in the environment, the App will collect the RSS values along the walking and send them to the localization server. When adequate amount of data is collected, the fingerprint map is generated.

SENIL [31] proposed a passive crowdsensing based system to automatically generate the radiomap. It uses graph matching algorithm to match the fingerprint map and floor plan. SENIL is deployed in the AP end. When there is communication traffic, the client is simultaneously contributing to the fingerprint collection task. Therefore, it does not require the client to install specific App, which significantly improves the crowdsourcing contribution rate.

c. *Hybrid Solutions*

The work proposed in [32] is a hybrid indoor localization system combining the Wi-Fi fingerprint and acoustic ranging. The acoustic ranging accuracy is much higher than Wi-Fi fingerprint. By combining both the coarse-grained Wi-Fi fingerprint localization and short range accurate acoustic ranging into one single optimization framework, it did push the limit of Wi-Fi localization accuracy.

Zee [33] is a combination of RADAR and inertial navigation based indoor localization. It proposed a hybrid localization framework, which supports various indoor localization schemes to work with inertial navigation. Since the position transition in indoor environments is restricted by the indoor structure, Zee proposed a Neuron-Network based user position interference scheme, which can correct the error accumulation of inertial navigation.

http://www.springer.com/978-3-319-12645-6

Device-Free Object Tracking Using Passive Tags
Han, J.; Xi, W.; Zhao, K.; Jiang, Z.
2014, VI, 62 p. 33 illus., Softcover
ISBN: 978-3-319-12645-6