BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF RADIO ELECTRONICS
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV RADIOELEKTRONIKY

SPATIAL IDENTIFICATION METHODS AND SYSTEMS FOR RFID TAGS

METODY A SYSTÉMY PROSTOROVÉ IDENTIFIKACE RFID ETIKET

SHORT VERSION OF PHD THESIS
TEZE DISERTAČNÍ PRÁCE

AUTHOR Ing. ALEŠ POVALAČ
AUTOR PRÁCE
SUPERVISOR doc. Ing. JIŘÍ ŠEBESTA, Ph.D.
VEDOUCÍ PRÁCE

BRNO 2012

KEYWORDS

RFID, RTLS, radiofrequency identification, channel modeling, ranging, distance measurement, phase-of-arrival, angle-of-arrival, spatial identification, localization, MIMO, SIMO, SDR, USRP, ISO 18000-6C

KLÍČOVÁ SLOVA

RFID, RTLS, radiofrekvenční identifikace, modelování kanálu, ranging, měření vzdálenosti, phase-of-arrival, angle-of-arrival, prostorová identifikace, lokalizace, MIMO, SIMO, SDR, USRP, ISO 18000-6C

DISERTAČNÍ PRÁCE JE ULOŽENA:

Ústav radioelektroniky
Fakulta elektrotechniky a komunikačních technologií
Vysoké učení technické v Brně
Purkyňova 118
612 00 Brno

© Aleš Povalač, 2012

CONTENTS

1 Introduction **3**

2 State of the Art **4**

2.1 Tag Distance and Angle Estimation 4
  2.1.1 Ranging-based Methods 4
  2.1.2 Direction-based Methods 6
2.2 Aims of Dissertation 6

3 Channel Modeling and Ranging Theory **7**

3.1 Overview of RFID Channel Models 7
3.2 Antenna Placement 9
3.3 Phase-based Ranging Principles 10
  3.3.1 Multi-carrier Wideband Ranging 11
3.4 Direction of Arrival Principles 11
3.5 Channel Models and Simulations 12
  3.5.1 RFID Channel Emulator 12

4 Testing Systems for RFID Ranging **14**

4.1 Requirements for UHF RFID Operation 15
4.2 Ettus USRP N200 Platform 16
  4.2.1 Hardware and Host Driver Modifications 17
  4.2.2 Wrapper Library 18
  4.2.3 MATLAB Interface for Testing System 18

5 Positioning Methods and Experiments **20**

5.1 Backscatter CTF Measurement 20
5.2 Phase-based Ranging Evaluation 21
  5.2.1 Narrowband PDoA with Frequency Hopping 21
  5.2.2 FFT-based Wideband Range Estimation 22
5.3 Localization Based on Range and Angle 23
  5.3.1 Multipoint Bistatic Ranging 24
  5.3.2 Bistatic Ranging with Direction Estimation 24

6 Conclusions **25**

References **27**

1 INTRODUCTION

In recent years, radio-frequency identification (RFID) technology has moved into mainstream applications. RFID uses a radio communication to identify a physical object. Although the technology has existed for more than a half century [1], its massive expansion has been started by the possibility to manufacture very inexpensive transponders – the integrated circuits in RFID tags. Nowadays, we can find RFID implemented in areas such as retail chains, warehouses, manufacturing, logistics, etc. The RFID technology enables far identification, unlike traditional bar codes. However, it allows much more.

A typical low-cost RFID tag is a passive device, which is powered by the energy of electromagnetic field transmitted by an interrogator (reader). The uplink transmission from the tag uses a principle called backscattering, when the tag alters its antenna reflection coefficient s_{11}. This reflected signal is separated in the reader from the coherent continuous-wave (CW) transmitted signal and demodulated. There are several standardized frequency bands for RFID operation, which differ in reading range, communication speed, or the possibilities of reading tags near metals and liquids. This thesis focuses on RFID systems in the ultra-high frequency (UHF) band, i.e. at center frequencies of 868 MHz in Europe and 915 MHz in the USA.

Basic wireless operation for an RFID tag is the reading of its identification number. Modern tags feature a rewritable memory and allow also its overwriting, locking or even permanent shutdown of the tag (called killing). Typical communication range in the UHF band is a few meters. The exchange between an interrogator and a tag is described by several mutually incompatible standards, such as iP-X EM4444, EPCglobal Class-1 Generation-2, or ISO 18000-6A and ISO 18000-6B.

Nowadays, signal processing methods and RFID tag identification technologies are solved and widely used in the industry. There are several challenges regarding the reading speed, its reliability, and particular tag localization, that allows precise definition of the reading area [2].

The communication range is pertinent to the concept of RFID transmission. It strongly depends on tag orientation, obstacles, environmental attenuation, and other local circumstances. Typical reading range of 2 m (using 0.5 W as typical RF power) can drop to a tenth, as well as increase several times [1]. This variability of range is currently one of the key issues in RFID technology. Precise definition of the reading area is necessary in a lot of applications, e.g. in a typical setup of parallel RFID gates in a warehouse.

Unfortunately, the industrial environment produces a really challenging RFID channel from the point of multipath propagation. This effect is desirable for tag reading, as it allows the communication between tag and reader even if there is no direct line of sight (LOS). On the other hand, a considerable fading margin is needed to ensure detection of all RFID tags within the read volume while undesired reads of tags outside the read zone are hard to avoid. Furthermore, multipath propagation seriously damages the ranging information, which can be otherwise extracted from the LOS signal in quite a simple way.

This thesis is trying to provide another point of view to the UHF RFID localization. Most of the scenarios described later are based on simple models with light and highly deterministic propagation, e.g. open space, large rooms, etc. It is oriented more practically, with an emphasis on prototyping, particular examples, and real measurements on developed ranging equipment. The UHF RFID system as a whole is also a combination of very challenging technology from the engineering point of view. It combines the knowledge from channel modeling, propagation, RF design, antenna design, signal processing, programming, networking, and many others. The know-how obtained from design and development of RFID systems is also described in the next chapters.

2 STATE OF THE ART

This chapter provides a comprehensive introduction to the principles of RFID localization. Most of the techniques are based on the fusion from several information sources, such as range, direction-of-arrival, and propagation characteristics [2].

Long range positioning and localization is a common topic, widely discussed also in the areas of radar systems and wireless networks [3]. On the contrary, short range distance and angle estimation is very specific to RFID backscattering principles and the research in this area started in recent years.

2.1 TAG DISTANCE AND ANGLE ESTIMATION

The majority of RFID localization techniques is based on two types of measurement: the range between the reader antenna and the tag, and the direction to the tag with respect to orientation of the reader antenna [2]. The accuracy of these measurements is fundamental for a reliable 2D/3D positioning.

2.1.1 Ranging-based Methods

The most common method of distance estimation is based on the received signal strength (RSS) of the RFID signals. This measurement is implemented in most commercial RFID readers but has many drawbacks [4].

The signal power at a reader with a round-trip loss strongly depends on the environment where the RFID system is deployed. It can be expressed as:

$$P_{RX} = P_{TX} \cdot \eta \cdot G_{tag}^2 G_{reader}^2 \cdot \left(\frac{\lambda}{4\pi d}\right)^{2n}, \tag{2.1}$$

where P_{TX} is the power transmitted by the reader, η is the power transfer efficiency of the tag, G_{tag} and G_{reader} are the antenna gain of the tag and the reader, respectively, λ is the wavelength, d is the range between the tag and the reader, and n

is the path loss exponent. The typical value of η is -5 dB and it depends among others on the power received by the tag. The path loss exponent n is defined by the environment and varies between 1.6 for indoor line-of-sight and 6.0 for outdoor propagation.

As a result, the range estimation based on RSS is very inaccurate in general case. For reasonable precision, it is necessary to characterize the environment, compensate the η coefficient of the tag, and specify its antenna orientation with G_{tag} correction.

The second type of distance estimation is based on time-based technique:

$$\widehat{d} = c \cdot \frac{\mathrm{ToF}}{2}, \tag{2.2}$$

where ToF is the round-trip propagation time of flight. This measurement only utilizes reader clock and thus does not require clock synchronization between the reader and the passive tag [2]. On the other hand, measurement of one-way time of arrival (ToA) for active RFID tags requires that the reader and the tag have precisely synchronized clocks, which may be impractical.

The application of ToF/ToA techniques in conventional narrowband RFID systems is difficult because of the poor time resolution limited by the frequency bandwidth. Nevertheless, these techniques could be promising in ultra-wideband (UWB) RFID systems, where a sufficient signal bandwidth is available [5].

The third approach to distance estimation employs phase-of-arrival (PoA) measurement. Two transmitted continuous-wave (CW) signals on different frequencies propagate over the same path, but their phase delays are proportional to their respective carrier frequencies. This concept is similar to the principle of the dual-frequency radar systems for range estimation [6]. Phase-based techniques of RFID ranging allow coherent signal processing, and they achieve better performance than traditional RSS approach [2]. On the other hand, simple PoA measurement fights with phase wrapping. The distance estimation is based on the phase difference observed at the two frequencies:

$$\widehat{d} = \frac{c \cdot \Delta\phi}{4\pi(f_2 - f_1)} + \frac{cm}{2(f_2 - f_1)}, \tag{2.3}$$

where $\Delta\phi$ is the measured phase difference ($0 \leq \Delta\phi < 2\pi$), and m is an unknown integer. The second term in (2.3) denotes the range ambiguity due to phase wrapping. The maximum unambiguous range is:

$$d_{\max} = \frac{c}{2(f_2 - f_1)}. \tag{2.4}$$

Larger frequency separation is more resistant to noise [7] but yields to a smaller value of $d_{\max}$. Note that as long as the tag is stationary, the measurement does not require simultaneously transmitted CW signals. Multiple successive measurements can be performed instead.

The biggest drawback of simple PoA measurements based on (2.3) is that only the group delay can be measured. Because of the multipath propagation, the distance estimation based on an average of several group delays typically leads to high standard deviations compared to UWB methods. This issue is explained in detail in Section 3.3.

Another method to phase wrapping elimination uses continuous-time frequency change realized by a linear FM chirp signal [8]. This time domain (TD-PDoA) measurement also allows the estimation of tag velocity vector [9], as it gives the Doppler shift information.

2.1.2 Direction-based Methods

Direction-of-arrival (DoA) estimation methods are typically based on directional antennas, phased arrays, and smart antennas [2]. The transmitted energy is directed to a small angular sector. When an RFID tag enters such area, the reader can sense it and thus determine its DoA.

Another approach to estimating the tag direction is based on the phase difference from multiple reader RX antennas. With this spatial domain phase difference of arrival (SD-PDoA) method [9, 10], the tag bearing θ can be approximated as:

$$\theta \approx \arcsin\left(\frac{c}{2\pi f}\cdot\frac{\Delta\phi}{a}\right), \tag{2.5}$$

where $\Delta\phi$ is the measured phase difference, a is the spacing between the two receiving antennas, and f is the operating frequency. Phase offset between the RX antennas can be calibrated out, thus the TX antenna can be located anywhere.

2.2 AIMS OF DISSERTATION

The main goal of this PhD thesis is to evaluate and improve the current UHF RFID ranging and localization methods. Spatial identification of RFID tags is an extremely evolving topic, as can be also seen from the list of references – most of them are not older than five years.

The main aims of the thesis correspond to the content of next chapters and can be stated as follows:

- **Channel Modeling:** Several simple models are proposed and implemented in MATLAB. These models cover the cases from the simplest ideal free space to a combined deterministic/stochastic model for a real room. Each model is analyzed for two different antenna placements.
- **Ranging Theory:** Study of current ranging techniques, analysis of phase-based methods in time, frequency and spatial domain. Introduces wideband

technique with a large number of measurement subcarriers and a single-input multiple-output SIMO system (i.e. one transmitter and multiple receivers).

- **Testing Systems for RFID Ranging:** Description of the design and development of prototype readers for RFID localization experiments. Includes a discussion of current regulatory requirements, RFID protocols, and antenna switching matrix for pseudo-SIMO operation.
- **Positioning Methods and Experiments:** The results obtained by proposed ranging methods, discussion of localization reliability in deterministic environments.

3 CHANNEL MODELING AND RANGING THEORY

This chapter introduces the theory of channel modeling. It explains basic parameters for channel characterization from both narrowband and wideband point of view. More details are given about ranging and direction finding. Finally, several positioning scenarios are analyzed with developed channel models. Note that all the described models use backscatter (degenerate, pinhole) channel [11], i.e. combined signal propagation from the transmitter (TX) to the tag and from the tag to the receiver (RX).

3.1 OVERVIEW OF RFID CHANNEL MODELS

The wireless channel with multipath propagation can be characterized using its channel impulse response (CIR), the response of the tapped delay line channel model to the Dirac pulse. The general CIR is a time-variant function, which also depends on environment, RX/TX position, polarization, etc. For known positions $\vec{p}_{TX}, \vec{p}_{RX}$ of RX and TX, respectively, it is possible to simplify the CIR to $h(\vec{p}_{TX}, \vec{p}_{RX}, \tau)$, where τ is the propagation delay [12]. The CIR itself is a complex-valued function, it is therefore better to plot its squared magnitude, i.e. power delay profile (PDP) [13]:

$$S(\vec{p}_{TX}, \vec{p}_{RX}, \tau) = |h(\vec{p}_{TX}, \vec{p}_{RX}, \tau)|^2. \tag{3.1}$$

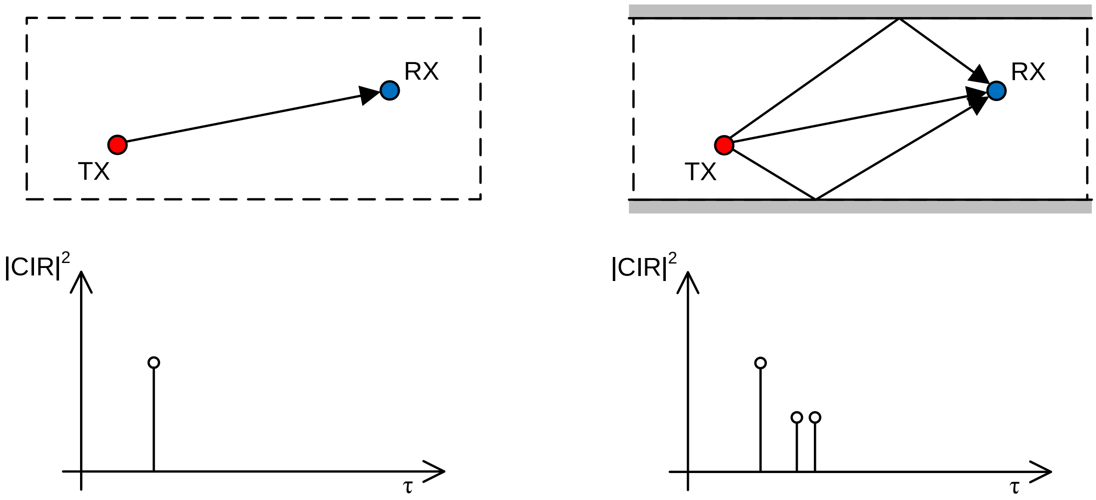
The physical representation of the PDP with only one path is shown in Fig. 3.1(a). This unobstructed direct path is called line-of-sight (LOS) component. In a multipath propagation, several other paths are added, called non-line-of-sight (NLOS) components, e.g. Fig. 3.1(b).

The following channel parameters can be defined using the PDP (see Fig. 3.1(c)) according to [13]:

- **Mean delay**, τ_0: the average delay weighted by power defined as:

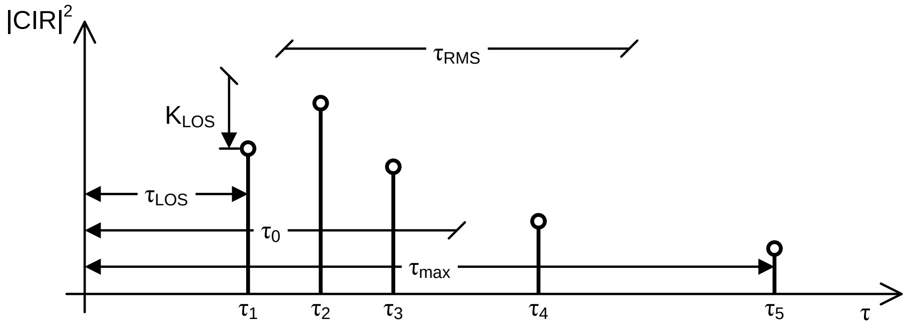
$$\tau_0 = \frac{1}{P_T} \sum_{i=1}^{n} P_i \tau_i, \quad \text{where} \quad P_T = \sum_{i=1}^{n} P_i. \tag{3.2}$$

- **LOS delay**, τ_{LOS}: the delay corresponding to direct LOS path.



(a) PDP of LOS only

(b) PDP of LOS and two reflections



(c) Channel parameters in PDP

Fig. 3.1: Physical representation of power delay profile

- **Maximum excess delay**, $\tau_{\max}$: the last significant delay.
- **RMS delay spread**, τ_{RMS}: the spread of the taps, considering both relative powers and delays of the taps, defined as:

$$\tau_{RMS} = \sqrt{\frac{1}{P_T}\sum_{i=1}^{n} P_i \tau_i^2 - \tau_0^2}. \tag{3.3}$$

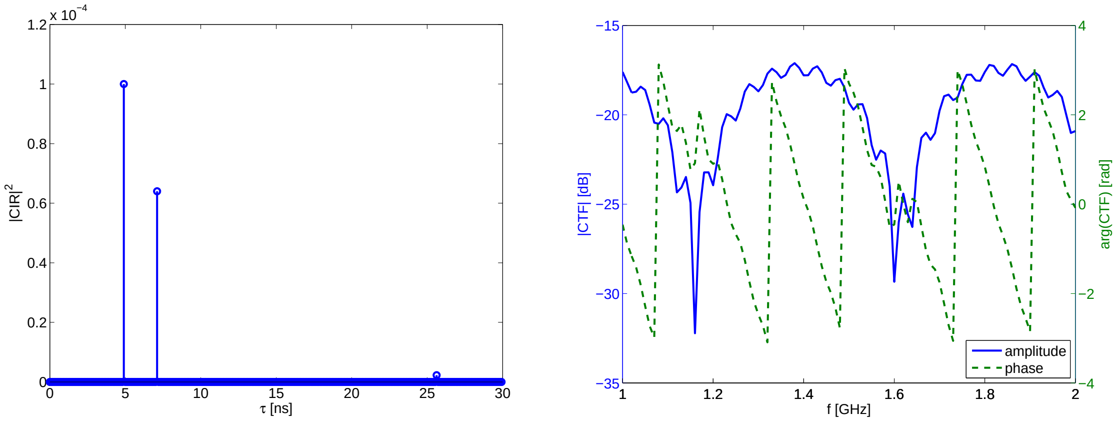
- **Ricean K-factor**, K_{LOS}: the power ratio between the direct (LOS) path and scattered (NLOS) multipath components.

The LOS delay τ_{LOS} is the most important parameter for ranging, as it directly defines the distance between RX and TX. Unfortunately, to isolate this component from the others in a strong multipath environment with large τ_{RMS}, it is necessary to use large measurement bandwidth, i.e. an ultra-wideband (UWB) system [14]. The spatial resolution of UWB is in an ideal case given by:

$$d_{res} = \frac{c}{2B}, \tag{3.4}$$

where c is the speed of light and B the signal bandwidth. The direct LOS path does not have to be the strongest path in a severe multipath environment ($K_{LOS} < 0$ dB).

Another channel characterization approach is based on channel transfer function (CTF), which is the inverse Fourier transform of the CIR. The CTF provides the complex channel gain of a given frequency and therefore can be measured in a relatively simple way. An example of the CTF corresponding to the CIR with three components is shown in Fig. 3.2.



(a) Example CIR with three paths

(b) Corresponding CTF

Fig. 3.2: Relationship between CIR and CTF

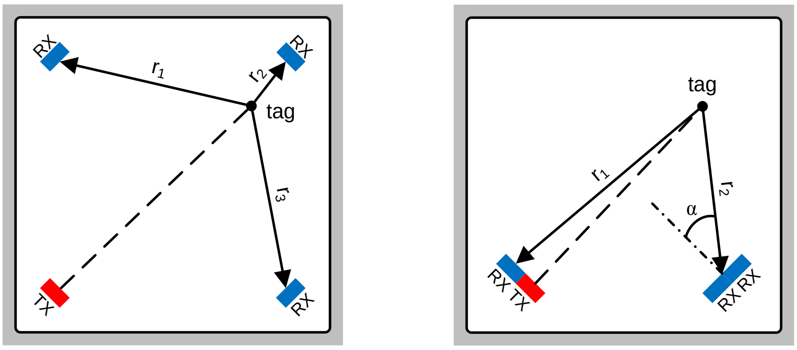
3.2 ANTENNA PLACEMENT

Several positioning sites are considered in the following sections. All of them are simplified cases of a real situation, as there are no major obstacles in the measurement area. The simulations include an anechoic chamber (idealized direct LOS propagation with no multipath), open space (direct path and one ray reflected by the floor), ideal room (direct path and multiple rays reflected from all the walls), and common room (modeled as the ideal room with stochastic propagation components). An area with square-shaped ground plan has been selected.

According to the defined hardware constraints, it is possible to place up to four antennas. The placement needs to consider antenna directional characteristics, maximum reading distance, self-interference between RX and TX path in reader, and most of all the desired methods of tag localization.

The first setup is shown in Fig. 3.3(a). The antennas are placed in each corner of the area. One of the antennas is TX, while the three others are RX, enabling range ellipses measurement. This scenario does not allow direction estimation, however it provides more independent ranging points.

Another setup in Fig. 3.3(b) can be used for both distance and direction measurement. It consists of two pairs of antennas. The first pair is placed in lower-left corner, serves for TX and RX, and it can be used for ranging. If the antennas in the pair are close enough ($d \ll \lambda$), it is considered to be a monostatic system, thus



(a) Distance only (b) Distance and direction

Fig. 3.3: Antenna placement scenarios for positioning

simplifying the ranging problem from ellipses to circles. The second pair is placed in lower-right corner and provides two RX antennas. Together with the TX antenna, it allows to do another independent ranging. Moreover, the two antennas act as an array, and therefore they are able to provide direction-of-arrival (DoA) information. In order to work in such configuration, the measured tag must be placed in the far field region of such antenna system.

3.3 PHASE-BASED RANGING PRINCIPLES

Phase difference of arrival in frequency domain (FD-PDoA) method is based on a set of measurements at discrete frequencies. It is independent on signal strength variations and allows reliable ranging [9] in non-multipath environment, e.g. in an anechoic chamber. The RFID tag must be stationary during the measurement. Range estimation using linearly spaced measurement frequencies is:

$$d = \frac{c}{4\pi \cdot \Delta f} \cdot \overline{\Delta\phi} - l_{corr}, \tag{3.5}$$

where $\overline{\Delta\phi}$ is an average of phase change between consequent frequencies. The estimation d includes the real distance between a reader antenna and a tag, signal propagation delay in RFID front end and antenna cable, and tag backscatter phase offset. The last two components are nearly constant and can be subtracted or calibrated out from the result, leaving the real range estimation itself.

These factors are incorporated in l_{corr} correction distance. The measured correction can be obtained as an average of differences between measured and real distances. It includes the propagation delay on antenna cable, phase delay caused by the tag reflection (typical value ca. 1 m according to [15]), and various delays of the front end.

Described method is not reliable for complex multipath environments [12]. Even if there is a large number of measurement points covering wide bandwidth, it is still a narrowband measurement – each phase pair gives an independent range estimation, which is averaged later. As a result, only the mean delay τ_0 can be estimated in a multipath environment with large RMS delay spread τ_{RMS}. This value is therefore always higher than τ_{LOS}.

3.3.1 Multi-carrier Wideband Ranging

Instead of common frequency hopping method, a multi-carrier transmission can be used. Such configuration provides an estimation of CTF on multiple frequencies at the same time. Typically, one high power signal for tag powering is transmitted, accompanied by several lower-level signals for measurement purposes.

Tag under test modulates all the carriers with backscattering, as shown in Fig. 3.4. The frequency offset between carriers Δf needs to be carefully selected, as the main tag response at BLF offset must not collide with higher-order harmonics of BLF produced by neighbor carrier.

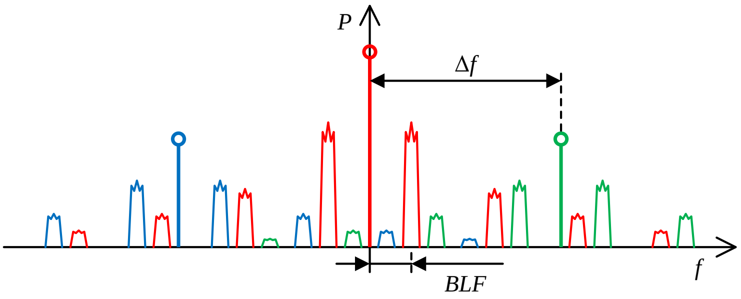


Fig. 3.4: Multi-carrier measurement, high power signal and two subcarriers

The CTF phase can be processed for each samples pair independently, which provides the same type of range estimation as the methods described earlier. On the other hand, if the measurement bandwidth is large enough, it is possible to calculate the CIR using a Fourier transform. Distance estimation based on CIR would not be seriously affected by multipath propagation.

Another approach to a true wideband measurement is based on the combination of narrowband estimates. As long as the reference frequency is phase coherent, it is possible to retune the PLL synthesizer and perform independent CTF estimates for each frequency. These estimates can be joined over an arbitrary bandwidth, which makes it possible to perform even UWB measurements, as long as the channel parameters do not change during the measurement process.

3.4 DIRECTION OF ARRIVAL PRINCIPLES

The implementation of SD-PDoA direction finding with two receiving antennas is based on measured phase difference of the backscattered signal between these two antennas [9, 16]. Fig. 3.5 illustrates the basic principle.

The phase difference $\Delta\phi$ is calculated from the absolute phase values ϕ_1, ϕ_2 of received signals. If the tag is placed in far field of the antenna array ($l > 2D^2/\lambda$, where D is the largest dimension), it is possible to express the bearing (direction to tag under test) with (2.5).

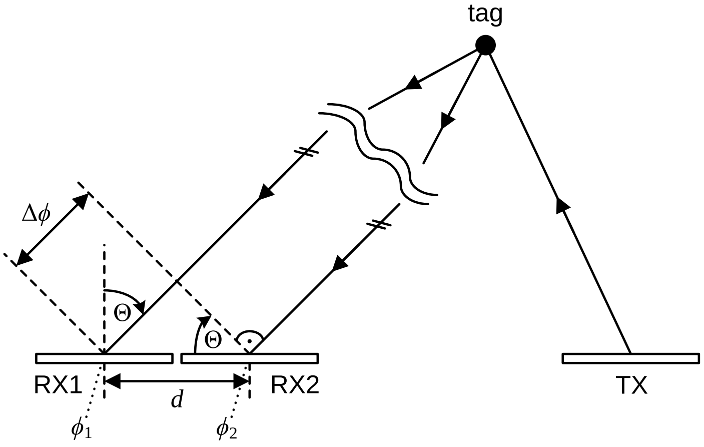


Fig. 3.5: Direction of arrival finding with SD-PDoA method

The arccos$(\cdot)$ argument must be in the range of -1 to $+1$. Considering the 2π phase periodicity, a single solution is given only for the distance $d < \lambda/2$ between antennas, two solutions for $\lambda/2 < d < \lambda$, and multiple solutions for $d > \lambda$ [10].

Much like the ranging methods, even direction finding suffers from multipath propagation. The angle power spectrum (APS) can be perceived as an angular equivalent of power delay profile [11]. Measurements performed at single frequency thus provide only the estimation of mean angle of arrival. However, multipath propagation may cause high RMS angle spread in the APS.

3.5 CHANNEL MODELS AND SIMULATIONS

A new RFID channel simulator has been created as a support tool for this thesis. The simulation level is basic compared to PARIS Simulation Framework [12], but the system is very intuitive and quick to set up. It provides combined deterministic/stochastic wideband modeling with high-order ray folding. Moreover, it is devoted to RFID backscatter channels, so it assumes the degenerate pinhole behavior.

3.5.1 RFID Channel Emulator

The RFID Channel Emulator (RCHE) is a set of several MATLAB functions that allows computation of the complex CTF for two basic sweeps: over frequency with fixed 3D position, and over 2D position with fixed height and frequency.

The propagation is always simulated on a pinhole channel, i.e. the signal goes from the TX antenna, it is backscattered (received and transmitted) by the tag under test, and received by the RX antenna. The power level of received signal is checked both on the tag (tag power-on threshold requirement) and on the RX antenna (minimum detectable signal with respect to self-blocking CW).

Each simulation is configured by a definition file. Several examples can be found in full version of the thesis. The definitions include:

- TX power in watts,

- complex tag reflection coefficient,
- complex obstacle reflection (ray folding) coefficient,
- TX and RX antenna positions in 3D space together with antenna bearing (vertical angle is assumed zero),
- room dimensions,
- number of stochastic component sources and the standard deviation of its distribution,
- list of basic (first order) reflections,
- the order of ray folding.

The deterministic simulation can include multiple signal reflections. Every signal path is computed (two complex CTFs for TX–tag and tag–RX) and added together. The stochastic components are modeled using a defined number of isotropic signal sources. Each of these sources has a random position outside the room dimensions and a random power, which is Rayleigh distributed.

Both simulators start with filling the list of possible reflections. This list can include two types of information: a reflector plane definition, and an isotropic source definition. Both ray folding and stochastic generator add new lines into this list. As a result, the list includes all considered reflection planes and stochastic sources.

RCHE with Frequency Sweep

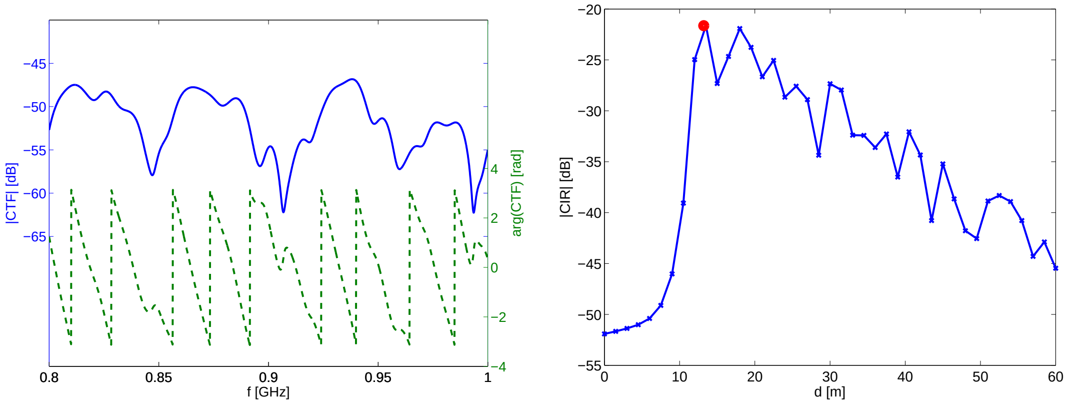
The simulation with frequency sweep requires a defined tag position in 3D space. Frequency sweep is defined by the frequency range and step size. Two complex CTFs are computed, the first one for TX–tag and the second one for tag–RX. Received complex signal at the RX antenna is a product of TX power, CTF between TX–tag, tag reflection coefficient, and CTF between tag–RX. Both the CTFs already include directional antenna gains.

As the last step, the absolute value of CIR is computed using direct Fourier transform. Fig. 3.6 shows the example of simulated CTF and CIR, together with a highlighted point at real TX–tag–RX distance. Two additional numerical results are provided: the range estimation based on group delay averagingand the FFT range estimation based on the first component in the CIR.

RCHE with 2D Position Sweep

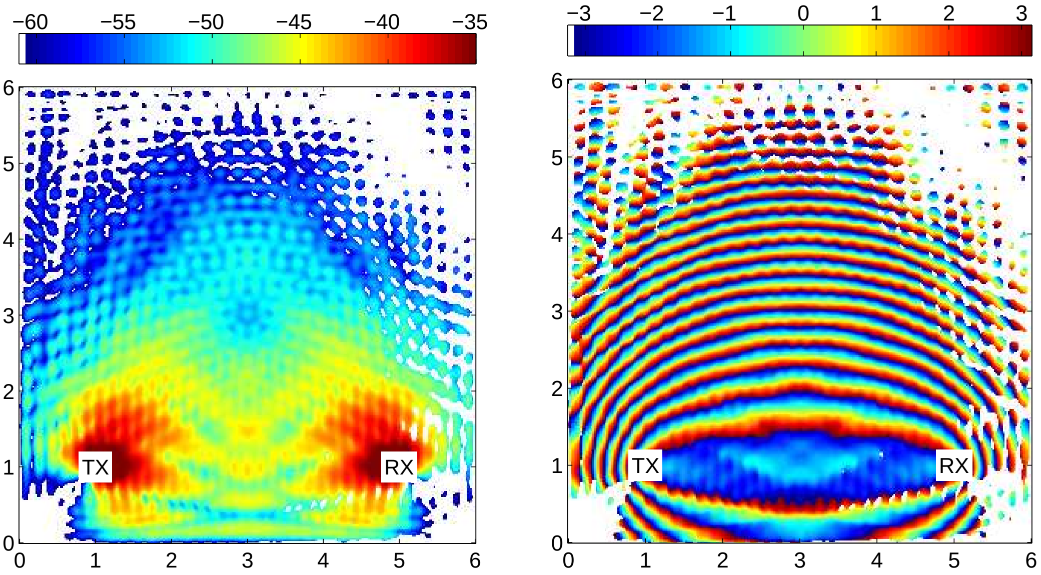
This type of simulation performs 2D tag position sweep in X-Y plane. Both antennas are stationary and the tag under test is moved over a 2D mesh. Its height is constant, as well as the measurement frequency. Two CTFs are computed (TX–tag and tag–RX). Much like in previous simulation, the received complex signal at the RX antenna is a product of TX power, CTF between TX–tag, tag reflection coefficient, and CTF between tag–RX.

Examples of amplitude and phase of the simulated signals are shown in Fig. 3.7. White color in the images shows the regions, where the power level was under the



(a) Channel transfer function (b) Channel impulse response

Fig. 3.6: Example of RCHE with frequency sweep



(a) Amplitude of tag signal [dBm] (b) Phase of received tag signal [rad]

Fig. 3.7: Example of RCHE with 2D position sweep

threshold – either under the minimum tag power-on threshold or under the minimum detectable signal.

4 TESTING SYSTEMS FOR RFID RANGING

This chapter summarizes the techniques and principles of software defined radio in UHF band together with the specialties of RFID communication. The main part is devoted to the description of two laboratory RFID reader systems: experimental interrogator EXIN-1 and its successor, RFID measurement equipment based on Ettus USRP N200 platform. An antenna switching matrix has been developed for the latter one, enabling an emulation of single-input multiple-output (SIMO) system.

4.1 REQUIREMENTS FOR UHF RFID OPERATION

The RFID communication has its specialties, which make the usage of standard SDR test equipment very disputable. One of the biggest issues is caused by a transmit carrier leakage into receive path – the RFID reader transmits high power continuous wave (CW) signal and receives tag backscatter response on the same frequency simultaneously. Therefore, the receiver must be able to operate with specified sensitivity even in the presence of such large blocking signal. Moreover, the phase and amplitude noise of the signal leaked into RX may be very high.

An RFID reader can be classified as monostatic (one antenna for both TX and RX) or bistatic (two independent antennas). A monostatic reader typically uses a circulator for the separation of RX and TX paths. The parameters of this circulator together with return loss s_{11} of the antenna determine the level of carrier leakage. Although the circulator isolation is typ. 25 dB, it is usually limited by the antenna return loss – typical value of common patch antennas is only -15 dB. Bistatic readers provide isolation over 30 dB but require two antennas [17].

Carrier Leakage

Transmitted CW signal is converted into large DC offsets in the receiver, which can be subtracted or filtered out using either analog or digital way. Analog filtering is typically provided by an AC coupling of the baseband signal using a capacitor. This approach is used in EXIN-1 design, together with quick charge of the capacitors to common mode voltage after the end of command transmission. Digital subtraction is simpler and provides better results. On the other hand, it requires high input range of the AD converter, which deteriorates the minimum detectable signal level. This method is used on USRP-based measurement system.

Carrier leakage can be actively cancelled using destructive signal interference. The principle is based on subtraction of the transmitted signal from the received signal, see Fig. 4.1. The signal is coupled from power amplifier and adjusted by a vector modulator in both amplitude and phase. The adjusted signal needs to have the same amplitude and the opposite phase (shifted by 180°) as the leaked signal in receive path [18]. The carrier suppression of 30 to 45 dB is achievable using this active cancellation [19].

Local Oscillator Signals

Typical SDR equipment capable of full-duplex operation (e.g. Ettus USRP radios) has two independent frequency synthesizers. Such synthesizer is based on a phase-locked loop (PLL) with a reference frequency input. This reference is common for all SDR subsystems including both synthesizers.

For an RFID operation, the same frequency needs to be set for both RX and TX paths. The synthesized LO signals are coherent because they are both locked to the same reference frequency. On the other hand, the phase noise of these two

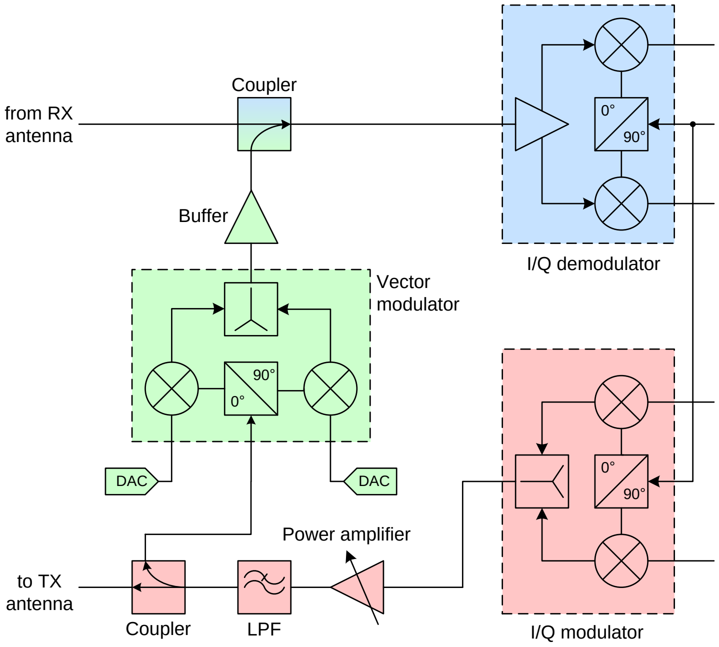


Fig. 4.1: Carrier cancellation by destructive interference (subtraction)

synthesized LO signals is not correlated. As a result, the overall performance is degraded.

It is therefore necessary to use a single LO source for both RX and TX paths. This can be accomplished by PLL synthesizers with two frequency outputs, as described in Section 4.2.1.

4.2 ETTUS USRP N200 PLATFORM

Although the EXIN-1 reader served well in the beginning of the experiments, it had several limitations, which were hard to overcome. Most of all, only the front end has been developed, and the design of FPGA signal processing is a complex task, which may form a complete PhD thesis [20]. Therefore, it was decided to create a complete experimental system based on an off-the-shelf SDR product.

The universal software radio peripheral (USRP) platform forms a family of SDR products developed and manufactured by Ettus Research. Each SDR consists of a motherboard (USRP) for baseband processing and RF daughterboards, which provide conversion to the desired frequency band. According to the requirement of dull-duplex operation at 800 – 1000 MHz frequency band, the networked series USRP N200 with WBX daughterboard has been selected.

The host code for the controlling PC is called USRP hardware driver (UHD). It is a library written in C++, which provides functions for the communication with a USRP. The onboard FPGA provides another digital down- and up-conversion, decimation and interpolation filters, soft RISC processor for command processing, and data streaming via Ethernet. Sample rates between ca. 200 kSPS and 25 MSPS are supported for both RX and TX with 16-bit complex I/Q samples.

4.2.1 Hardware and Host Driver Modifications

As described in Section 4.1, several extensions and modifications of such standard SDR system had to be done. First of all, the required RF power transmitted by an RFID reader is several watts, while the maximum output power provided by WBX is only about 15 dBm. Fortunately, the WBX daughterboard provides a grand-daughterboard (GDB) expansion slot.

The designed RFID GDB provides RF power up to 2 W (33 dBm) together with its precise measurement using a directional coupler and a power detector. This value is required for channel measurements performed in Chapter 5, because the power level strongly depends on frequency and TX antenna matching. The overall block diagram of WBX daughterboard with RFID GDB is shown in Fig. 4.2.

The WBX board itself required a modification of LO sources for mixers. The frequency synthesizes are independent, both locked to the same clock reference. If they are tuned to the same frequency, the produced LOs are coherent, but their phase noise is uncorrelated. As a result, there is an excessive level of noise in the received signal, and because of the output frequency division, there is also an unpredictable phase shift of $n \cdot \pi/2$ between RX and TX.

To overcome this issue, the same LO must be used for both RX and TX mixing. The RX synthesizer has been selected as the master LO source. Its auxiliary output is wired directly to the balun in TX mixer LO input (red connection in Fig. 4.2). Moreover, the currently unused TX synthesizer needs to be disabled at all, otherwise it produces unwanted signals, which also gets coupled into RX path.

The UHD driver has been updated in order to support the RFID GDB. An unique identification code is stored in GDB EEPROM memory. According to this ID, the RFID GDB is identified by the UHD, and an appropriate GDB driver is loaded. It

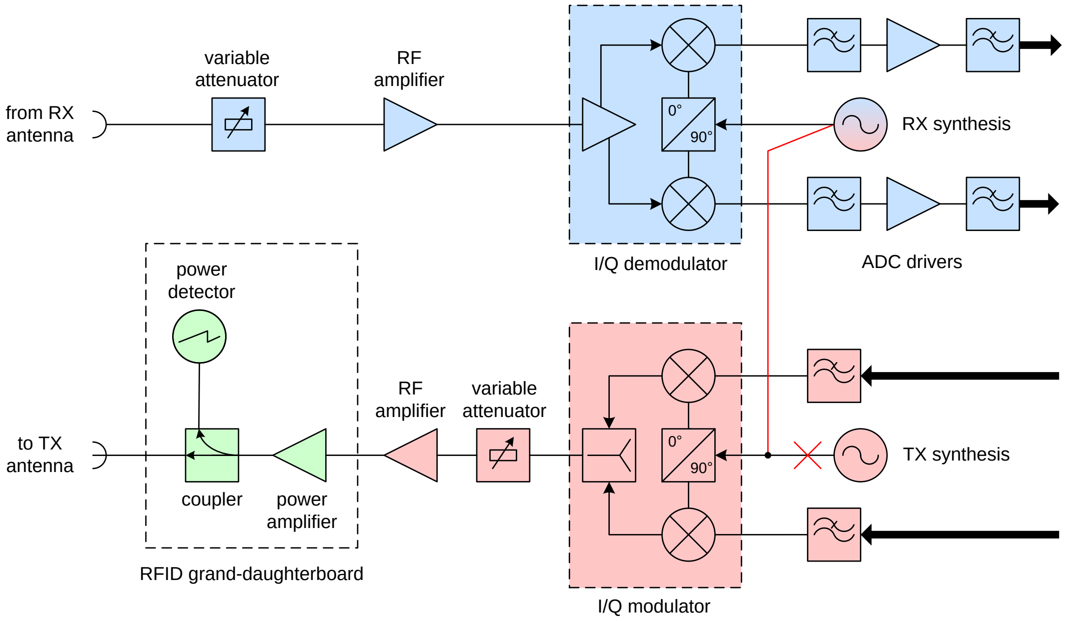


Fig. 4.2: Modified WBX daughterboard + RFID GDB block diagram

ensures correct switching of the PA during the transmission bursts, allows output power level measurement in a precisely defined time, and changes the behavior of WBX synthesizers – the TX synthesizer is disabled and the auxiliary output of the RX synthesizer is enabled. It also registers all necessary parameters of the RFID GDB, such as frequency range and available antenna connectors.

4.2.2 Wrapper Library

The purpose of the wrapper dynamic-link library (DLL) is to provide an interface between the C++ based UHD drivers and the high-level implementation in MATLAB. The driver library covers three main functions.

The signal generator module is responsible for the generation of basic Gen2 protocol signals [21]. It provides 90% ASK and PR-ASK modulations. Tari values of 25 µs, 12.5 µs and 6.25 µs are supported. The actual Tari value error depends on TX resampling capabilities of USRP. Each transmit burst consists of 0.2 ms silence, signal ramp-up, 1.5 ms of CW, optional **Select** command, **Query** command, CW signal of adjustable length, signal ramp-down, and several silent samples. The receiving window is defined over the CW part of the signal following the **Query** command.

The transceiver subsystem module is responsible for data transmission from and to the USRP. It implements the UHD call for frequency tuning, calls for adjusting TX power and RX gain, and disables slow DC offset correction in FPGA. The main part is devoted to the transmission of the burst and the reception of the tag reply. All operations are precisely synchronized. Modulation is scheduled typ. 10 – 20 ms after the beginning of the frame, power detector measurement takes place 1 ms after transmission start, reception is scheduled according to the receive signal window. Once the burst transmission is finished, this function checks all results for errors, computes the real power levels in dBm from the sampled ADC value, and returns the captured I/Q data.

The main code module exports the DLL functions for MATLAB. Callings of DLL functions are logged into the log file, which can be analyzed for debugging purposes.

4.2.3 MATLAB Interface for Testing System

The top-level measurement control takes place in MATLAB environment. In order to test the system, a simple example has been created.

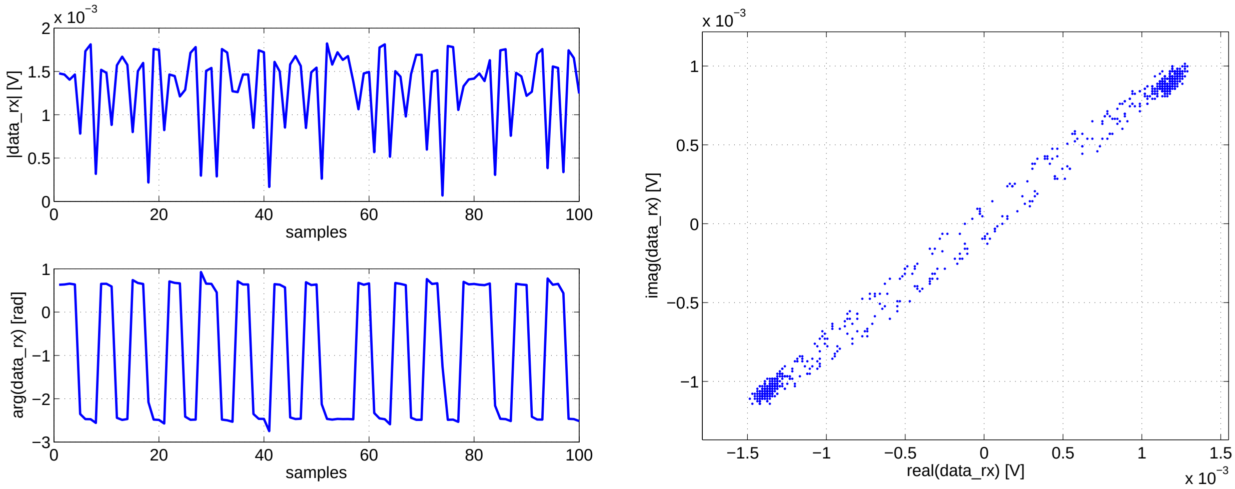
The example code initializes the measurement (lines 1–6), sets up the output power, working frequency (8–10), and transmits one burst (12–13), which consists of **Select** and **Query** commands with defined parameters. Backscattered response is received (12–13), processed (15–17), and plotted (19–26) both as an amplitude/phase and as a scatterplot, see Fig. 4.3. Measured output power is printed out (28–29) and the system is released (31–32).

Signal processing (15–17) starts with a conversion between ADC value and real input voltage level (16). Only the beginning of the returned samples is used. Line (17) provides subtraction of mean signal value. The mean values are computed independently for both I and Q channels. This subtraction provides the digital cancellation of CW carrier leaked into RX input, as described in Section 4.1.

```
1  %% load USRP wrapper
2  load_usrp('192.168.10.2');
3
4  %% prepare reader commands: Select tags with EPC beginning 3005FB63, Query ...
       at Tari 12.5us, backscatter link 320kHz Miller-4, enable TRext
5  select = hex2dec([ '30'; '05'; 'fb'; '63' ])';
6  BLF = prepare_burst(nTARI_12_5, 2.5, 2.13333, false, nDR_64_3, nMILLER_4, ...
       true, 8*length(select), select);
7
8  %% set gain 10dB, output power ca. 23dBm -0dB; set frequency 867MHz
9  voltage_step = set_power(10., 23., 0);
10 set_freq(867e6);
11
12 %% transmit Select+Query, receive tag response; RX sample rate 2MSPS
13 [data_rx_int16, meas_power] = trx_burst(2e6);
14
15 %% use first 40% of received data (preamble+beginning of RN16), subtract ...
       mean value (carrier leakage)
16 data_rx_all = double(data_rx_int16(1:round(end*0.4))) .* voltage_step;
17 data_rx = data_rx_all - mean(data_rx_all);
18
19 %% plot amplitude and phase of received data
20 figure(1); selection = 200:300;
21 subplot(211), plot(abs(data_rx(selection)));
22 subplot(212), plot(angle(data_rx(selection)));
23
24 %% plot constellation I/Q diagram of received data
25 figure(2);
26 plot(real(data_rx), imag(data_rx), '.'), axis equal;
27
28 %% display backscatter link frequency and measured RF power
29 disp(BLF), disp(meas_power);
30
31 %% release USRP
32 unload_usrp();
```

The measurement interface allows free setting of Gen2 protocol parameters, as well as completely user-defined TX signal. Input I/Q signal from RX is simultaneously sampled during the CW part of TX burst and provided in its source form to MATLAB as an array. The proposed system is universal, however, it is not possible to **Ack** the RN16 because of the strict timing constraints – the turnaround time is typically over 50 ms, which is over T_2 timeout in Gen2 protocol. Support for **Ack** and **ReqRN** transmissions would have to be added to onboard FPGA.

Measurement system is fully coherent and allows extraction of both phase and amplitude from the received signal. It is suitable for RFID channel experiments, as it operates with backscattered responses. Moreover, the real output power is



(a) Amplitude and phase (b) Constellation diagram

Fig. 4.3: Example outputs from backscattered response

measured during every transmission burst, which enables additional amplitude correction. The developed system is also useful for antenna measurements and tag performance testing, as described in [22].

5 POSITIONING METHODS AND EXPERIMENTS

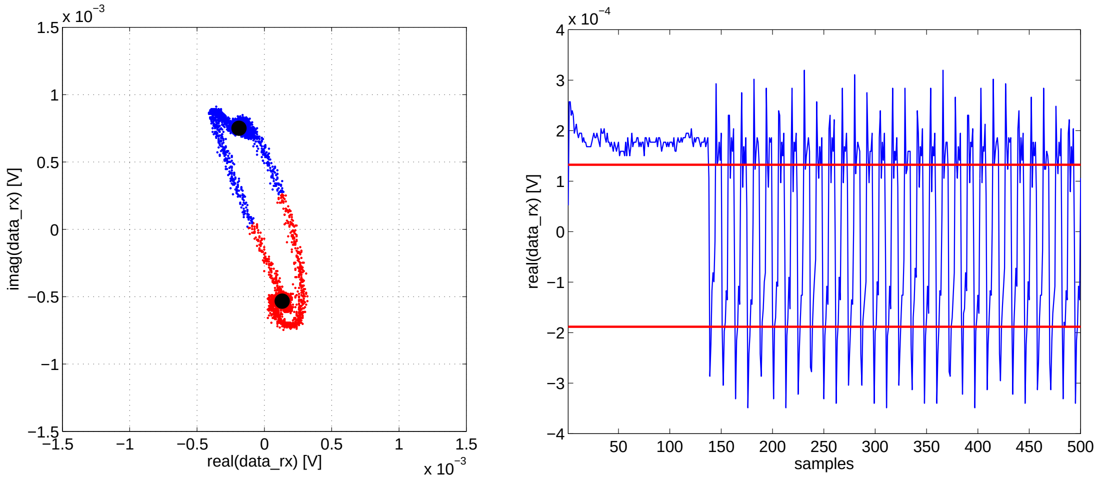
This chapter summarizes the results obtained with positioning experiments. Both the FD-PDoA ranging and the SD-PDoA direction estimation methods are extended with advanced signal phase measurement, based on the cluster detection algorithm. The last part describes a combination of ranging and direction finding in order to perform a 2D localization.

5.1 BACKSCATTER CTF MEASUREMENT

All the positioning methods except the simplest RSS-based estimation are based on the evaluation of received signal phase, i.e. on coherent signal processing. In other words, the complex CTF at one or more frequencies is being measured. The accuracy of phase extraction is vital for all the following methods.

The method of phase measurement, which has been used for positioning in the following sections, is based on k-medians clustering in constellation diagram for a known $k = 2$. Received signal has always two complex states. The k-medians clustering provides detection of cluster indices corresponding to both tag transmission states. Moreover, it is possible to eliminate the π phase ambiguity by definition of the initial conditions.

Fig. 5.1 shows scatter plot and in-phase signal for a tag with NXP G2XM chip. Although the transition between tag states in Fig. 5.1(a) is nonlinear in this case [23], the cluster indices are correctly identified including the initial condition (positive in-phase value in Fig. 5.1(b) – red part).



(a) Scatter plot with clusters (b) Received in-phase signal (NXP G2XM)

Fig. 5.1: Constellation cluster detection

5.2 PHASE-BASED RANGING EVALUATION

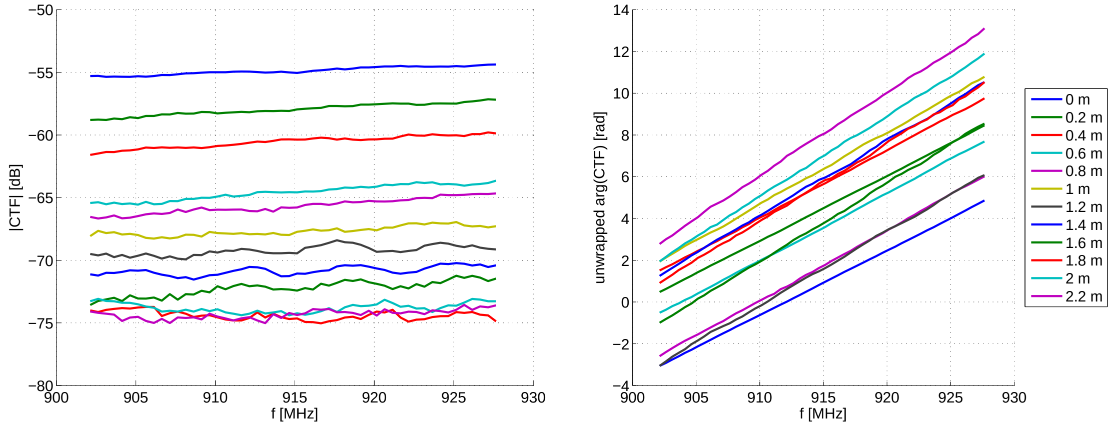
Distance estimation has been tested on the roof of DREL building. Tag responses have been automatically captured with MATLAB script at frequencies from 800 MHz to 1000 MHz with 250 kHz step. Measurements have been performed with a monostatic variant of the system described in Section 4.2, which has been connected via circulator to the Poynting PATCH-A0025 antenna. Tag responses have been captured on all 800 applicable frequencies, manually varying the distance between antenna and tag from zero to 2.2 m with 0.2 m step. The tag was placed on a simple nonconductive hung. Measurements have been done using tag with Impinj Monza chip, which comply with Gen2 protocol [21].

Fig. 5.2 shows the CTF of RFID backscatter channel for various distances. For the lucidity, the frequency range has been limited to the US RFID band (902 MHz – 928 MHz) and the phase has been unwrapped. It can be noticed, that absolute CTF value declines with range while the slope of CTF phase (i.e. $\mathrm{d}\phi(f)/\mathrm{d}f$) rises.

5.2.1 Narrowband PDoA with Frequency Hopping

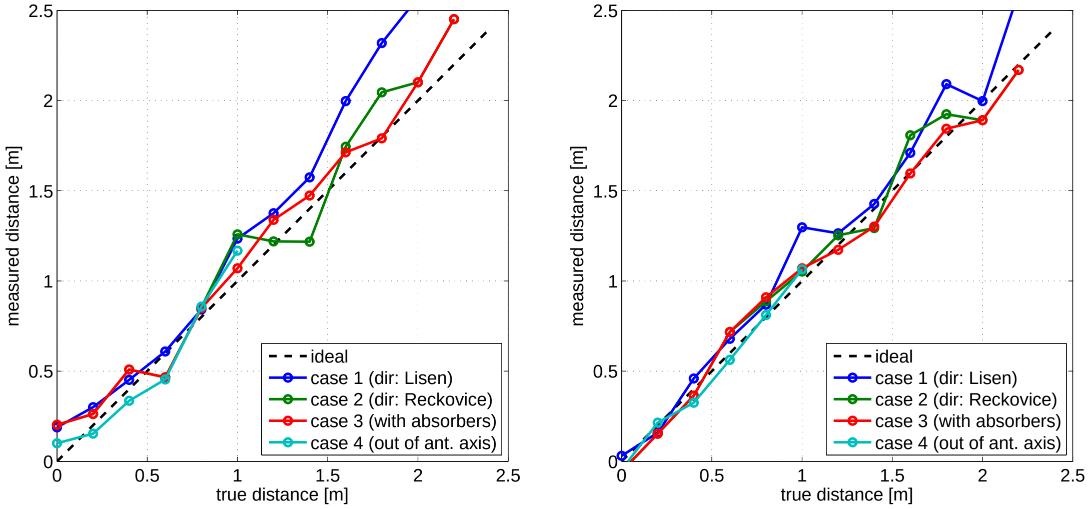
The distance estimation is calculated from the phase difference average using (3.5). Results include the propagation through antenna cable, delays caused by RF part of the front end, and phase offset of the tag backscatter.

Fig. 5.3(a) shows the results of range estimation for the US RFID channel plan with altering distance between the antenna and the tag. Four trials have been taken. In order to suppress floor reflection, broadband pyramidal absorbers has been added in the third measurement. The fourth case was performed with the tag 45° out of antenna axis. The mean absolute errors of the range estimation were $[232, 147, 110, 97]$ mm. Ranging inaccuracy is caused by several factors, such as variation of l_{corr} over frequency and temperature, and light multipath environment.



(a) Channel attenuation (b) Phase of received signal

Fig. 5.2: Measured channel attenuation and phase of received signal



(a) US RFID channels only ($B = 26$ MHz) (b) Wideband average ($B = 200$ MHz)

Fig. 5.3: Narrowband FD-PDoA distance estimation results

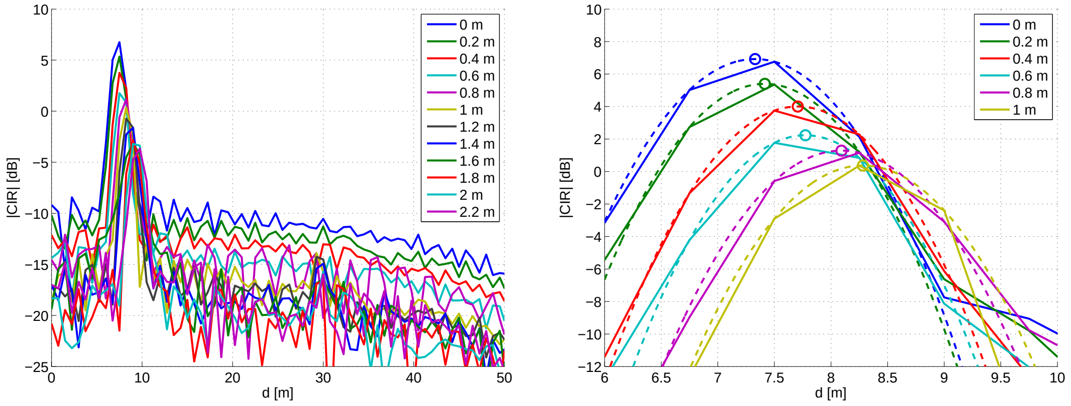
Another ranging on the same principle has been performed for the complete 200 MHz bandwidth with several omitted frequencies (mainly strong GSM signals). The distance estimations are shown in Fig. 5.3(b), the computed mean absolute errors were $[123, 85, 62, 41]$ mm.

The difference between performed trials is not significant. Additional absorbers (case 3) improved the estimation slightly. The estimation is not dependent on tag bearing with respect to antenna, as can be seen from case 4. However, the antenna gain is directional and declines out of the axis, so the range is limited by tag turn-on power threshold.

5.2.2 FFT-based Wideband Range Estimation

Cluster indices detection method allows the CTF measurement in arbitrary bandwidth. If the chosen bandwith is large enough, it is possible to provide the range estimation based on computed CIR. The same measured signal as in the last section has been used for the evaluation of this method. According to (3.4), the monostatic distance resolution for $B = 200$ MHz is 0.75 m.

The CTF is multiplied by a window function, e.g. by Hamming window. The result is then processed by Fourier transform (implemented as FFT) and resulting CIR plotted. CIRs for altering distance in case 3 is shown in Fig. 5.4(a). The range bias of $l_{corr} = 7.25$ m has not been subtracted in this plot.



(a) Amplitude of CIR (b) CIR peaks with parabolic interpolation

Fig. 5.4: CIR range estimation from measured CTF for case 3, $B = 200$ MHz

Because of the limited bandwidth, the estimates would be averaged into multiplies of 0.75 m. This inaccuracy can be compensated by better methods of CIR peak search. An example is given in Fig. 5.4(b). The CIR peak is found and a parabola is fitted into this peak and its two neighbors [24]. Finally, the new peak position of parabolic interpolation is used as the range estimation.

Using the parabolic CIR interpolation method, the range estimations in Fig. 5.5 have been obtained. The computed mean absolute errors for all four cases were $[122, 155, 73, 191]$ mm. Although these values are worse than the estimates from phase averaging, the CIR-based method should be very robust to multipath propagation.

An optimal solution may be based on a combination of both methods. The wideband CTF can be filtered in frequency domain, which would suppress the long paths ($d > 20$ m) and noise. Such filtered signal can be passed to FD-PDoA range estimator. This approach would provide accurate results with some particular immunity to long indirect propagation paths. However, it is still necessary to use large bandwidth and FFT estimation technique for severe multipath environments.

5.3 LOCALIZATION BASED ON RANGE AND ANGLE

This section provides the positioning results according to the antenna placement scenarios proposed in Section 3.2. Scenario A provides six range estimations, while scenario B allows to estimate two bearings and three independent ranges.

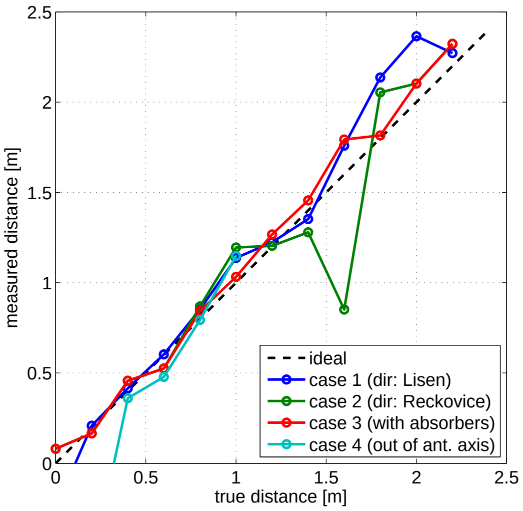


Fig. 5.5: Wideband CIR distance estimation results

All the measurements have been taken on DREL building roof with antennas and tags at height $h = 0.9$ m. Four Poynting PATCH-A0025 antennas have been connected to the measurement system via the switching matrix. The RFID tags with Impinj Monza chip have been used. Ranging has been performed over $B = 26$ MHz bandwidth according to the US RFID channel plan.

5.3.1 Multipoint Bistatic Ranging

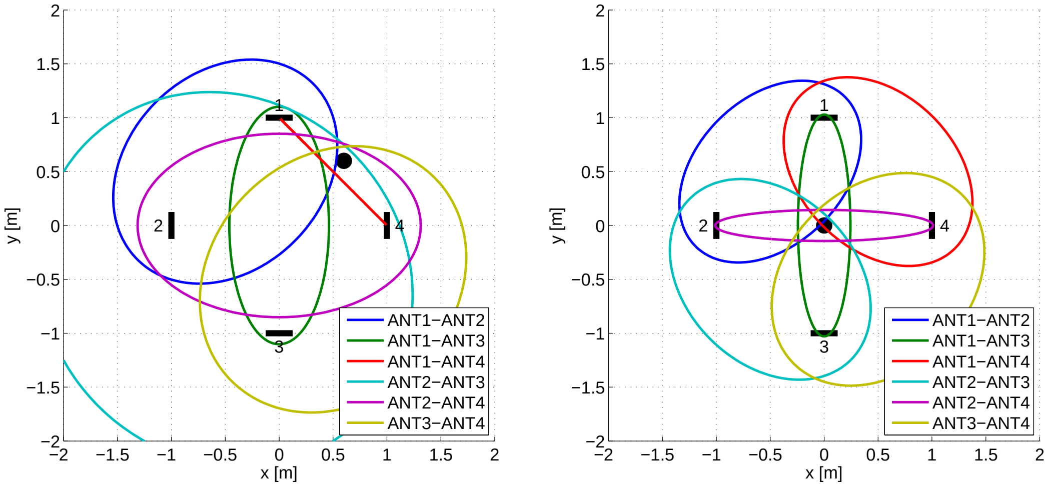
Scenario A allows to estimate a set of bistatic ranges. An area of 1.4×1.4 m with diagonal antenna distance of 2 m has been selected due to limited communication range with passive RFID tags. The scenario provides six bistatic ranges, i.e. the distances from TX antenna via tag under test to RX antenna. Due to the large distance between the antennas, it is not possible to provide tag direction estimation.

Unlike monostatic ranging described in Section 5.2, the signal propagation in bistatic configuration is not back and forth, and the positioning circle transforms to an ellipse. For a system with one TX and two RX antennas, the tag can be localized in the intersection of two ellipses. Finding the intersections is a common geometrical problem. However, more complex methods need to be used for multiple bistatic range estimations, such as target tracking based on probability hypothesis density [25].

The positioning results for two selected tag positions are shown in Fig. 5.6. Each ellipse is defined by its foci corresponding to the positions of TX and RX antennas and the major radius resulting from the measured distance.

5.3.2 Bistatic Ranging with Direction Estimation

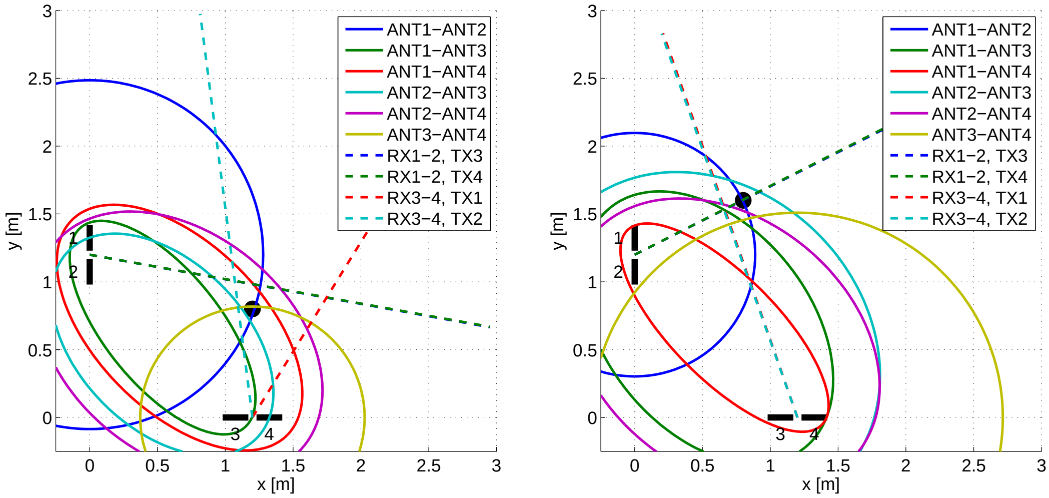
Scenario B provides both range and angle estimations. Distance of 1.7 m between antenna array centers has been selected. The scenario provides two tag direction estimations (one from each antenna array) and up to six bistatic ranges.



(a) Tag placed at $x = 0.6$ m, $y = 0.6$ m (b) Tag placed at $x = 0$ m, $y = 0$ m

Fig. 5.6: Multipoint bistatic range ellipses, scenario A

Unlike the previous case, four of these ranges are highly correlated due to small distance between antennas for bearing measurement. As a result, two independent semi-monostatic ranges and four correlated bistatic ranges are available in addition to directional information. Fig. 5.7 shows the final localization results for two defined tag positions.



(a) Tag placed at $x = 1.2$ m, $y = 0.8$ m (b) Tag placed at $x = 0.8$ m, $y = 1.6$ m

Fig. 5.7: Multipoint bistatic ranging with direction estimation, scenario B

6 CONCLUSIONS

This doctoral thesis started with an introduction to RFID systems operation in the UHF band. Chapter 2 described the state of the art in the field of RFID localization. Short range positioning is a very broad area and a quickly evolving topic in the worldwide scientific community. Both distance and angle estimation methods were described, with an emphasis to coherent phase-based procedures.

Chapter 3 described the RFID channel modeling and the pinhole channel simulator developed in MATLAB. The simulation results for two proposed positioning scenarios and several channel complexity levels are attached in the appendix. The channel simulator and involved theory has been published in [26, in review process]. Furthermore, the chapter explained details of phase difference of arrival (PDoA) ranging. Time domain PDoA (with LFM chirp) simulation results have been published in [8].

Chapter 4 introduced software defined radio (SDR) concept and its adaptation to UHF RFID systems. The requirements on SDR architecture, published in [18], led to the design of two measurement systems. The experimental interrogator EXIN-1 (published in [27]) was a complete custom modular design created on purpose of ranging experiments. It served for several frequency domain PDoA ranging measurements in anechoic chamber, published in [28]. However, the baseband signal was processed on a computer sampling card, which had low performance and was very slow.

The second measurement system design was based on commercial Ettus USRP platform with custom RFID extension (described in [22]). All the experimental results presented in this thesis were obtained with this system. Moreover, in order to support multiple inputs/outputs, the antenna switching matrix was developed, which enabled the pseudo-SIMO operation and thus data fusion from multiple signal sources.

Final part of this thesis in Chapter 5 was focused on positioning experiments. Several approaches to pinhole CTF measurement were described. The evaluation of narrowband PDoA with frequency hopping and wideband FFT-based range estimation was performed, as well as phase-based direction of arrival estimation with system calibration. Finally, the proposed antenna placement scenarios were validated by positioning experiments.

The experimental results show accurate distance estimation for simple environments without strong multipath propagation. All the described methods have been based on phase extraction from the cluster indices in tag constellation diagram, which provides better results compared to RSS-based phase evaluation. Moreover, the described measurement method enables slow wideband measurements for stationary targets and consequential FFT-based CIR estimation. Parabolic CIR interpolation has been used to further improve wideband distance estimation. This approach is suitable even for environments with stronger multipath propagation, assuming large measurement bandwidth.

Accuracy of direction-based method is lower in comparison to ranging approach. Direction finding also requires on-site calibration with a tag placed at a reference position. The lower accuracy of this method was probably caused by improper antennas, which were too large to form a precise antenna array. Multipoint bistatic ranging with optional direction estimation enables the tag localization in 2D space. Generaly, the monostatic and semi-monostatic (with RX/TX antenna distance much lower than tag distance) ranging provides better results in comparison to bistatic ranging.

The contribution of this thesis can be summarized according to the dissertation aims defined in Section 2.2 as follows:

- **Channel Modeling and Ranging Theory:** Proposal of two multistatic antenna placement scenarios for localization. Development of RFID Channel Emulator (RCHE) and analysis of several models for pinhole RFID channel using simulated CTF and CIR characteristics.
- **Testing Systems for RFID Ranging:** Definition of the requirements on SDR systems for UHF RFID operation. Design of measurement prototypes according to these demands.
- **Positioning Methods and Experiments:** Phase of arrival detection based on cluster indices detection from tag constellation diagram. Wideband CTF estimation from a set of narrowband measurements. Parabolic interpolation applied to CIR for range resolution enhancement. Evaluation of multipoint bistatic ranging with optional direction estimation.

REFERENCES

[1] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in practice*. Burlington, MA (USA): Newnes, 2007.

[2] Y. Zhang, X. Li, and M. G. Amin, *RFID systems: Research trends and challenges*, ch. Principles and techniques of RFID positioning, pp. 389–415. Chichester: John Wiley & Sons, 2010.

[3] A. H. Sayed, A. Tarighat, and N. Khajehnouri, "Network based wireless location: challenges faced in developing techniques for accurate wireless location information," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 24–40, 2005.

[4] K. Chawla, G. Robins, and L. Zhang, "Object localization using RFID," in *Proceedings of the IEEE International Symposium on Wireless Pervasive Computing, ISWPC 2010*, pp. 301–306, 2010.

[5] D. Arnitz, U. Muehlmann, and K. Witrisal, "UWB ranging in passive UHF RFID: proof of concept," *IET Electronics Letters*, vol. 46, pp. 1401–1402, September 2010.

[6] Y. Zhang, M. Amin, and F. Ahmad, "Time-frequency analysis for the localization of multiple moving targets using dual-frequency radars," *IEEE Signal Processing Letters*, vol. 15, pp. 777–780, 2008.

[7] X. Li, Y. Zhang, and M. G. Amin, "Multifrequency-based range estimation of RFID tags," in *Proceedings of the IEEE International Conference on RFID 2009*, pp. 147–154, April 2009.

[8] A. Povalač and J. Šebesta, "Phase of arrival ranging method for UHF RFID tags using instantaneous frequency measurement," in *ICECom 2010, Conference Proceedings (CD-ROM)*, pp. 1–4, September 2010.

[9] P. V. Nikitin, R. Martinez, S. Ramamurthy, H. Leland, G. Spiess, and K. V. S. Rao, "Phase based spatial identification of UHF RFID tags," in *Proceedings of the IEEE International Conference on RFID 2010*, pp. 102–109, April 2010.

[10] C. Angerer, R. Langwieser, and M. Rupp, "Direction of arrival estimation by phased arrays in RFID," in *Proceedings of the International EURASIP Workshop on RFID Technology*, pp. 1–5, September 2010.

[11] A. Paulraj, R. Nabar, and D. Gore, *Introduction to Space-Time Wireless Communications*. Cambridge: Cambridge University Press, 2003.

[12] D. Arnitz, *Tag Localization in Passive UHF RFID*. PhD thesis, Graz University of Technology, Austria, 2011. Available: `<http://www.spsc.tugraz.at/sites/default/files/phdthesis-arnitz_online.pdf>` [cit. 2012-01-24].

[13] S. R. Saunders and A. A. Zavala, *Antennas and Propagation for Wireless Communication Systems*. Chichester: John Wiley & Sons, 2nd ed., 2007.

[14] G. Li, D. Arnitz, R. Ebelt, U. Muehlmann, K. Witrisal, and M. Vossiek, "Bandwidth dependence of CW ranging to UHF RFID tags in severe multipath environments," in *Proceedings of the IEEE International Conference on RFID 2011*, pp. 19–25, April 2011.

[15] V. Viikari, P. Pursula, and K. Jaakkola, "Ranging of UHF RFID tag using stepped frequency read out," *IEEE Sensors Journal*, vol. 10, no. 9, pp. 1535–1539, 2010.

[16] S. Azzouzi, M. Cremer, U. Dettmar, R. Kronberger, and T. Knie, "New measurement results for the localization of UHF RFID transponders using an angle of arrival (AoA) approach," in *Proceedings of the IEEE International Conference on RFID 2011*, pp. 91–97, April 2011.

[17] P. V. Nikitin and K. V. S. Rao, "Antennas and propagation in UHF RFID systems," in *Proceedings of the IEEE International Conference on RFID 2008*, pp. 277–288, April 2008.

[18] A. Povalač, J. Šebesta, and M. Dušek, "Software defined radio requirements for UHF RFID systems," in *7th MC Meeting and Workshop of the COST IC0803*, pp. 1–12, September 2011.

[19] R. Langwieser, G. Lasser, C. Angerer, M. Rupp, and A. L. Scholtz, "A modular UHF reader frontend for a flexible RFID testbed," in *Proceedings of the International EURASIP Workshop on RFID Technology*, pp. 1–12, 2008.

[20] C. Angerer, *Design and Exploration of Radio Frequency Identification Systems by Rapid Prototyping*. PhD thesis, Vienna University of Technology, Austria, 2010. Available: `<http://publik.tuwien.ac.at/files/PubDat_187386.pdf>` [cit. 2012-01-24].

[21] EPCglobal Inc., *Class-1 Generation-2 UHF RFID protocol for communications at 860 MHz – 960 MHz*, 2008. Version 1.2.0.

[22] M. Dušek, V. Derbek, A. Povalač, J. Šebesta, and R. Maršálek, "Hardware and software stack for an SDR-based RFID test platform," in *4th International EURASIP Workshop on RFID Technology 2012*, 2012. Accepted for publication.

[23] D. Arnitz, K. Witrisal, and U. Muehlmann, "Multifrequency continuous-wave radar approach to ranging in passive UHF RFID," *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, pp. 1398–1405, May 2009.

[24] J. O. Smith, III and X. Serra, "PARSHL: An analysis/synthesis program for non-harmonic sounds based on a sinusoidal representation," in *Proceedings of the International Computer Music Conference*, 1987. Available: `<https://ccrma.stanford.edu/~jos/parshl/parshl.pdf>` [cit. 2012-08-12].

[25] M. Tobias and A. D. Lanterman, "Multitarget tracking using multiple bistatic range measurements with probability hypothesis densities," in *Signal Processing, Sensor Fusion, and Target Recognition XIII. SPIE Proceedings Vol. 5429*, pp. 296–305, 2004.

[26] A. Povalač, K. Witrisal, and J. Šebesta, "Degenerate RFID channel modeling for positioning applications," *Radioengineering*, 2012. Submitted, in review process.

[27] A. Povalač and J. Šebesta, "Experimental front end for UHF RFID reader," *Elektrorevue Journal for Electrical Engineering*, vol. 2, pp. 55–59, April 2011.

[28] A. Povalač and J. Šebesta, "Phase difference of arrival distance estimation for RFID tags in frequency domain," in *IEEE International Conference on RFID-Technology and Applications 2011*, pp. 180–185, September 2011.

CURRICULUM VITAE

Personal

Name	**Ing. Aleš Povalač**
Born	July 28, 1985 in Třebíč
Address	Srbská 1850/49, 612 00 Brno, Czech Republic
Contact	alpov@alpov.net

Education

2009 – 2012	Doctor of Philosophy (PhD) Brno University of Technology (Department of Radio Electronics) Thesis: Spatial Identification Methods and Systems for RFID Tags
2007 – 2009	Master's degree (MSc) – inženýr (Ing.) Brno University of Technology (Department of Radio Electronics) Thesis: Control Microprocessor Unit with Frequency Synthesizer for SW Radiostation
2004 – 2007	Bachelor's degree (BSc) – bakalář (Bc.) Brno University of Technology (Department of Radio Electronics) Thesis: Remote Control of Measurement Devices in SRD Band

Internships

1/2012	Signal Processing and Speech Communication Laboratory Graz University of Technology, Graz (Austria)

Courses

6/2011	Training School on RF/Microwave System Design for Sensor and Localization Applications CTTC, Barcelona (Spain)
7/2011	International Summer School on Radar/SAR Fraunhofer FHR, Bonn (Germany)

Additional

Languages	Czech – mother tongue English – proficient user (C1) German – basic user (A1)

ABSTRACT

The doctoral thesis is focused on methods and systems for ranging and localization of RFID tags operating in the UHF band. It begins with a description of the state of the art in the field of RFID positioning with short extension to the area of modeling and prototyping of such systems. After a brief specification of dissertation objectives, the thesis overviews the theory of degenerate channel modeling for RFID communication. Details are given about phase-based ranging and direction of arrival finding methods. Several antenna placement scenarios are proposed for localization purposes. The degenerate channel models are simulated in MATLAB.

A significant part of the thesis is devoted to software defined radio (SDR) concept and its adaptation for UHF RFID operation, as it has its specialties which make the usage of standard SDR test equipment very disputable. Transmit carrier leakage into receiver path and requirements on local oscillator signals for mixing are discussed. The development of three experimental prototypes is also presented there: experimental interrogator EXIN-1, measurement system based on Ettus USRP platform, and antenna switching matrix for an emulation of SIMO system.

The final part is focused on testing and evaluation of described positioning techniques based on complex backscatter channel transfer function measurement. Both narrowband/wideband ranging and direction of arrival methods are validated. Finally, both proposed antenna placement scenarios are evaluated with real-world measurements.

ABSTRAKT

Disertační práce je zaměřena na metody a systémy pro měření vzdálenosti a lokalizaci RFID tagů pracujících v pásmu UHF. Úvod je věnován popisu současného stavu vědeckého poznání v oblasti RFID prostorové identifikace a stručnému shrnutí problematiky modelování a návrhu prototypů těchto systémů. Po specifikaci cílů disertace pokračuje práce popisem teorie modelování degenerovaného kanálu pro RFID komunikaci. Detailně jsou rozebrány metody měření vzdálenosti a odhadu směru příchodu signálu založené na zpracování fázové informace. Pro účely lokalizace je navrženo několik scénářů rozmístění antén. Modely degenerovaného kanálu jsou simulovány v systému MATLAB.

Významná část této práce je věnována konceptu softwarově definovaného rádia (SDR) a specifikům jeho adaptace na UHF RFID, která využití běžných SDR systémů značně omezují. Diskutována je zejména problematika průniku nosné vysílače do přijímací cesty a požadavky na signál lokálního oscilátoru používaný pro směšování. Prezentovány jsou tři vyvinuté prototypy: experimentální dotazovač EXIN-1, měřicí systém založený na platformě Ettus USRP a anténní přepínací matice pro emulaci SIMO systému.

Závěrečná část je zaměřena na testování a zhodnocení popisovaných lokalizačních technik, založených na měření komplexní přenosové funkce RFID kanálu. Popisuje úzkopásmové/širokopásmové měření vzdálenosti a metody odhadu směru signálu. Oba navržené scénáře rozmístění antén jsou v závěru ověřeny lokalizačním měřením v reálných podmínkách.