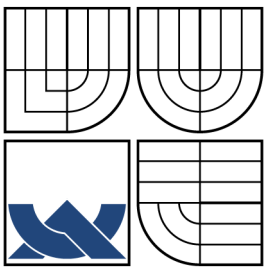
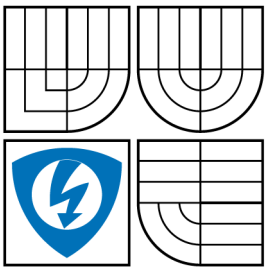


BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ



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

DOCTORAL THESIS
DISERTAČNÍ PRÁCE

AUTHOR
AUTOR PRÁCE
Ing. ALEŠ POVALAČ

SUPERVISOR
VEDOUCÍ PRÁCE
doc. Ing. JIŘÍ ŠEBESTA, Ph.D.

BRNO 2012

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.

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

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.

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

PROHLÁŠENÍ

Prohlašuji, že svou disertační práci na téma *Metody a systémy prostorové identifikace RFID etiket* jsem vypracoval samostatně pod vedením školitele a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené disertační práce dále prohlašuji, že v souvislosti s vytvořením této disertační práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....
podpis autora

Bibliografická citace

POVALAČ, A. *Metody a systémy prostorové identifikace RFID etiket.* Disertační práce. Brno: FEKT VUT v Brně, 2012. 82 stran.

ACKNOWLEDGMENT

First of all, I would like to express my gratitude to my advisor Jirka Šebesta. You helped me a lot – both as a mentor and as a great friend. Your visits to our office accompanied with extensive verbal motivation (*makéj*) became truly legendary over the years.

This thesis would not exist without Michal Zamazal, who provided me the opportunity to get in touch with real-world RFID problems in the first year of my studies. I would also like to thank Klaus Witrisal for his help during my stay at his institute in Austria. It has been a great month and a valuable experience.

I am obliged to many of my colleagues and friends at DREL, who supported me during the past years, especially Jiťa, Mufan, Ráďa, Marťas and Vojta. You made it possible to finish this thesis.

Last but not least, I am truly thankful to my parents for their support and encouragement throughout my studies and my whole life.

Aleš Povalač is a holder of Brno Ph.D. Talent Scholarship Funded by Brno City Municipality

The research was performed in laboratories supported by the SIX project; the registration number CZ.1.05/2.1.00/03.0072, the operational program Research and Development for Innovation.

CONTENTS

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 [13], 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 [14]. 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 [15].

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 [13]. 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.

One of the thesis objectives should have been focused to analysis of multipath propagation. In 2011, an extensive PhD thesis about this subject has been published [16], which invalidated this original goal. The main result of this work is outright: "*Is it possible to accurately determine the position of passive UHF RFID tags in typical applications and within the boundary conditions of passive UHF RFID systems? No, it is not. Not within the limits of UHF RFID.*" [16, p. 155]. Several ways has been proposed to overcome the given limitations, mostly based on wideband and ultrawideband measurements.

The referenced PhD thesis has been limited by several requirements given by the funding company. Most of the research has been done on the scenario of RFID portals in a warehouse, i.e. in a strong multipath environment. It has been necessary to use passive tags, maintain compatibility to ISO 18000-6C [17], and perform ranging during less than 1 ms detection time. It has been also focused mostly to ranging and doesn't give enough credit to direction-based methods.

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 [15, 18].

Long range positioning and localization is a common topic, widely discussed also in the areas of radar systems and wireless networks [19]. 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.

Last section of this chapter describes UHF RFID prototyping systems and addresses several issues related to RFID, such as large self-blocker signal.

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 [15]. 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 [20, 21].

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 [15, 22]. 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 [23].

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 [24]. Phase-based techniques of RFID ranging allow coherent signal processing, and they achieve better performance than traditional RSS approach [15, 25]. On the other hand, simple PoA measurement fights with phase wrapping [26]. 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 [27] 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 [1], [22, 28]. This time domain (TD-

PDoA) measurement also allows the estimation of tag velocity vector [29], 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 [15, 30, 31]. 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 [29, 32], 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 Positioning Techniques for RFID

Using the known range and/or direction-of-arrival information from several sources, a tag can be localized in 2D or 3D space. The trilateration method determines tag position using the range information, while the triangulation method using its DoA angle [33].

To unambiguously localize a tag in an n-dimensional space using trilateration, range information from at least $n + 1$ reference points is required. In some special cases, n reference points are sufficient, as the ambiguity can be resolved by an area-of-interest specification [15].

Fig. 2.1 depicts a tag positioning problem in a 2D space with three independent RFID readers in reference points $\vec{p}_1(0, 0)$, $\vec{p}_2(x_2, y_2)$, and $\vec{p}_3(x_3, y_3)$. The range estimations are r_1, r_2, and r_3, respectively. Unknown location of the tag $\vec{p}_m(x_m, y_m)$ can be solved from the system of three equations:

$$\begin{aligned} r_1^2 &= x_m^2 + y_m^2 \\ r_2^2 &= (x_2 - x_m)^2 + (y_2 - y_m)^2 \\ r_3^2 &= (x_3 - x_m)^2 + (y_3 - y_m)^2. \end{aligned} \tag{2.6}$$

One way to solve this over-determined nonlinear system is described in [19]. The

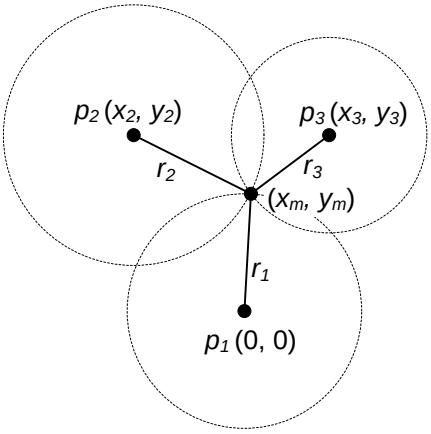


Fig. 2.1: Trilateration positioning

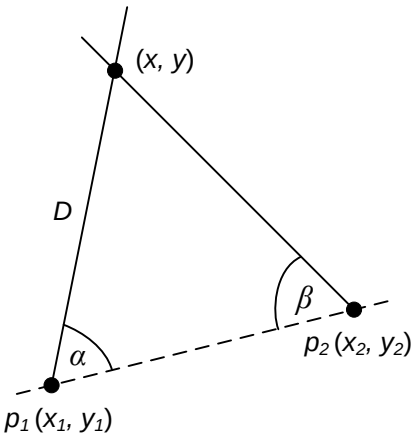


Fig. 2.2: Triangulation positioning

least-squares solution can be written in matrix form as:

$$\begin{bmatrix} x_2 & y_2 \\ x_3 & y_3 \end{bmatrix} \begin{bmatrix} x_m \\ y_m \end{bmatrix} = \frac{1}{2} \begin{bmatrix} K_2^2 - r_2^2 + r_1^2 \\ K_3^2 - r_3^2 + r_1^2 \end{bmatrix}, \quad \text{where} \quad K_i^2 = x_i^2 + y_i^2. \tag{2.7}$$

With more than three range estimations available, the trilateration transforms into a multilateration. It can be verified that an extension of (2.7) is still valid:

$$\mathbf{Hx} = \mathbf{b}, \quad \text{where} \quad \mathbf{H} = \begin{bmatrix} x_2 & y_2 \\ x_3 & y_3 \\ x_4 & y_4 \\ \vdots & \vdots \end{bmatrix}, \quad \mathbf{b} = \frac{1}{2} \begin{bmatrix} K_2^2 - r_2^2 + r_1^2 \\ K_3^2 - r_3^2 + r_1^2 \\ K_4^2 - r_4^2 + r_1^2 \\ \vdots \end{bmatrix}. \tag{2.8}$$

In this case, the least-squares solution of (2.8) is given by [19]:

$$\hat{\mathbf{x}} = \left(\mathbf{H^T H}\right)^{-1} \mathbf{H^T b}. \tag{2.9}$$

The triangulation of a tag is shown in Fig. 2.2. Its location is determined by measuring the DoA of the received signal from two or more known reference points. In this example, the DoAs are measured at $\vec{p}_1(x_1, y_1)$ and $\vec{p}_2(x_2, y_2)$ as angles α and β with respect to the line determined by the two reference points. The intersection of the two rays determines the coordinate of the tag:

$$\begin{aligned} x &= x_1 + D\cos(\alpha + \gamma) \\ y &= y_1 + D\sin(\alpha + \gamma), \end{aligned} \tag{2.10}$$

where $D = \frac{\sin\beta}{\sin(\alpha+\beta)}\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ is the distance from the unknown tag to $\vec{p}_1$ and $\gamma = \arctan\frac{y_1 - y_2}{x_1 - x_2}$. For an over-determined solution with more than two reference points, the problem can be solved with matrix expression similar to (2.9) according to [15].

Multiple measurement points can be obtained by the synthetic aperture radar (SAR) and holographic localization methods [34]. The SAR is based on a moving antenna with known trajectory, which produces additional data for multiangulation method. The holographic method features a spatial optimal filter.

Another concept of RFID localization uses radio map matching methods, also known as the scene analysis. This matching consists of two distinctive steps. Firstly, the radio scene information (fingerprints) are collected to form a radio map. Secondly, unknown tags are localized by matching the measured data with the fingerprints in the radio map. Two major fingerprinting-based matching methods are the k-nearest-neighbor (kNN) and the probabilistic methods, based on Bayesian rule. The best known application of the kNN method in RFID positioning is called LANDMARC [35].

The simplest approach to RFID localization is called proximity. It is based on a limited read range of an RFID reader. While this system requires dense deployment of reader antennas, it is very easy to implement [36, 37]. It can also be used in a "reverse" localization scenario with non-stationary RFID reader and multiple reference tags in known positions [38].

2.3 UHF RFID Simulators

In order to test the performance of current ranging methods and to simplify the development and testing of its derivatives, it is necessary to use an RFID channel simulation tool. Most of the currently used systems are targeted to an analysis of narrowband state-of-the-art RFID setups, without the consideration of pinhole behavior of the channel [39, 40, 41]. Moreover, it is especially important for ranging simulations to include multi-ray propagation with ray folding, otherwise the results are inaccurate.

As a consequence, the simulators specialized on channel simulation for ranging are being developed. The most advanced open-source system is the PARIS Simulation Framework, described in [42] and [16, p. 69]. It is a complex MATLAB-based time-domain system-level simulator, which features tag behavioral models and hybrid ray-tracing/stochastic RF propagation channel models. The framework is also very demanding on computational power.

On the other hand, there are several simple simulators based on deterministic channel, which are easy to understand and use, such as [29]. These systems typically ignore high-order reflections (i.e. all reflections except the first one) and provide only a limited number of rays.

2.4 Prototyping and Testing of RFID Systems

Many manufacturers provide off-the-shelf products such as RFID readers for end users. A common problem of their use in research and development is the embed-

ding of these systems, as they do not provide access to advanced configuration and internal signals required for non-standard operations.

The RFID communication has its difficulties, which make it problematical to use generic software defined radio (SDR) test equipment, especially in a monostatic system. The biggest challenge inherent to all UHF RFID systems is the fight with large self-blocker signal – the reader receives the tag response on the same frequency where it transmits an unmodulated CW signal for tag powering.

Two general approaches are used. The first one is based on carrier cancellation [43]. Part of the transmitted signal is altered using a vector modulator in order to have the same amplitude and the opposite phase with respect to the received signal. When mixed together using a directional coupler, most of the blocking signal can be cancelled out. This carrier cancellation is necessary for multiple-IF receivers to allow optimal signal reception [44].

A PhD thesis about RFID rapid prototyping based on this concept [45] has been published in 2010. The described system allows DoA estimation with two antennas, as well as reading and decoding of collision between two tag responses.

The second approach is based on a direct conversion to in-phase and quadrature baseband channels [46]. In this scenario, the transmitted CW signal is converted into large DC offsets, which can be subtracted or filtered out using either analog or digital way. The requirements on the down-converting I/Q demodulator are very demanding in such application, but they can be fulfilled by modern ICs. Both systems described in Chapter 4 are based on this approach. It is very important to use the same local oscillator (LO) frequency source for both modulator and demodulator [2], otherwise the overall performance will be degraded by uncorrelated phase noise of these synthesized LOs.

2.5 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.

As can be seen from the list, a significant part of the PhD thesis is focused to practical implementation, measurements, experiments and evaluation. These parts will not be achievable without appropriate equipment. Although the details about the selected platform (Ettus Research USRP N200 software defined radio with custom RFID extension) are described in Chapter 4, several features given by the system also limit the available methods. Most important constraints selected for the localization system design are:

- software defined radio: operating frequency 700–1100 MHz, output power up to 33 dBm, RX/TX bandwidth up to 25 MHz (full 16-bit samples) or 50 MHz (limited 8-bit samples), Gigabit Ethernet interface
- antenna switching matrix: electromechanical, 2 inputs (RX/TX), 4 outputs (ANT1–ANT4)
- passive RFID tags only, ISO 18000-6C protocol, stationary during the measurement, positioning time up to 10 seconds
- operation only in controlled environments – open space, labs, offices, etc.

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, as briefly introduced in Section 2.1. Finally, several positioning scenarios are analyzed with developed channel models. Note that all the described models use backscatter (degenerate, pinhole) channel [47, 48], 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 [16]. The CIR itself is a complex-valued function, it is therefore better to plot its squared magnitude, i.e. power delay profile (PDP) [49]:

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

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).

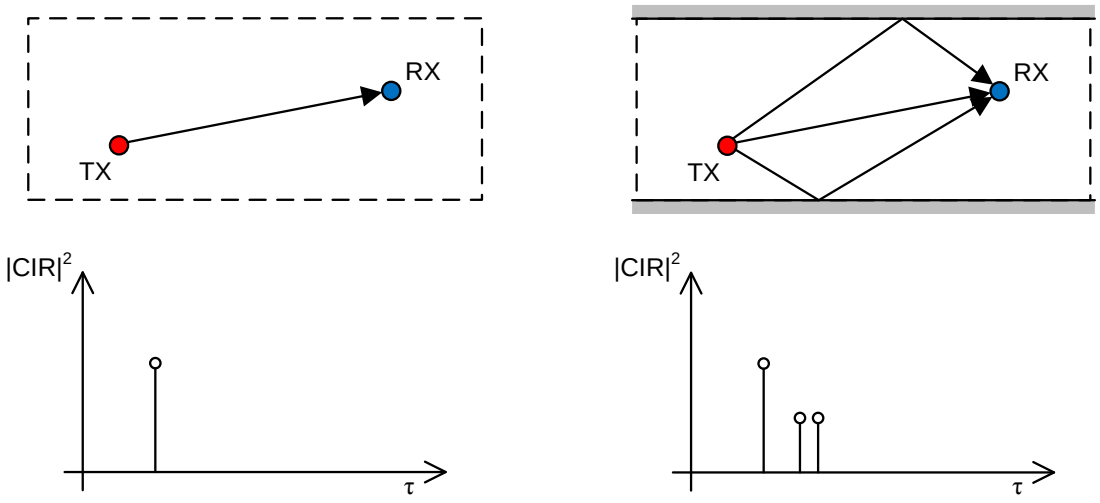
The following channel parameters can be defined using the PDP (see Fig. 3.1(c)) according to [49, 50]:

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

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

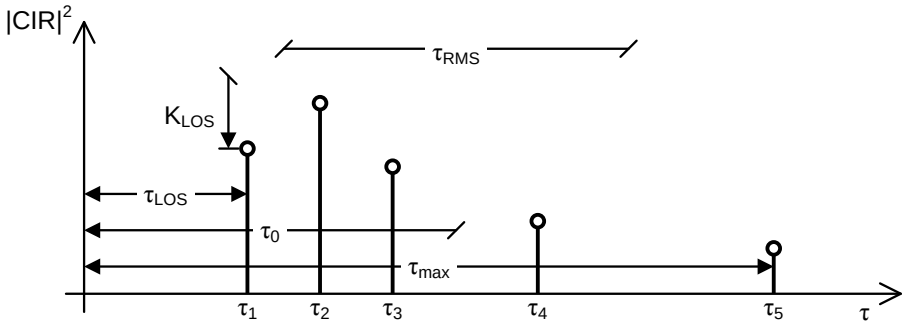
- **LOS delay**, τ_{LOS}: the delay corresponding to direct LOS path.
- **Maximum excess delay**, $\tau_{\max}$: the last significant delay.
- **RMS delay spread**, τ_{RMS}: the spread of the taps, considering both relative powers and delays of the taps, defined as:

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



(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

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

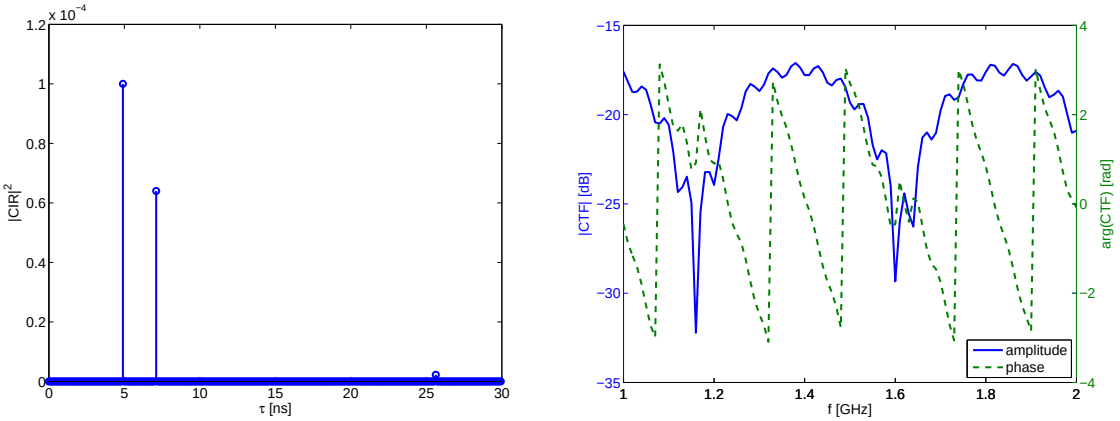
The LOS delay τ_{LOS} is the most important parameter for ranging, as it directly defines the distance between RX and TX. Unfortunately, to isolate this component from the others in a strong multipath environment with large τ_{RMS}, it is necessary to use large measurement bandwidth, i.e. an ultra-wideband (UWB) system [51]. 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 [52]. 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

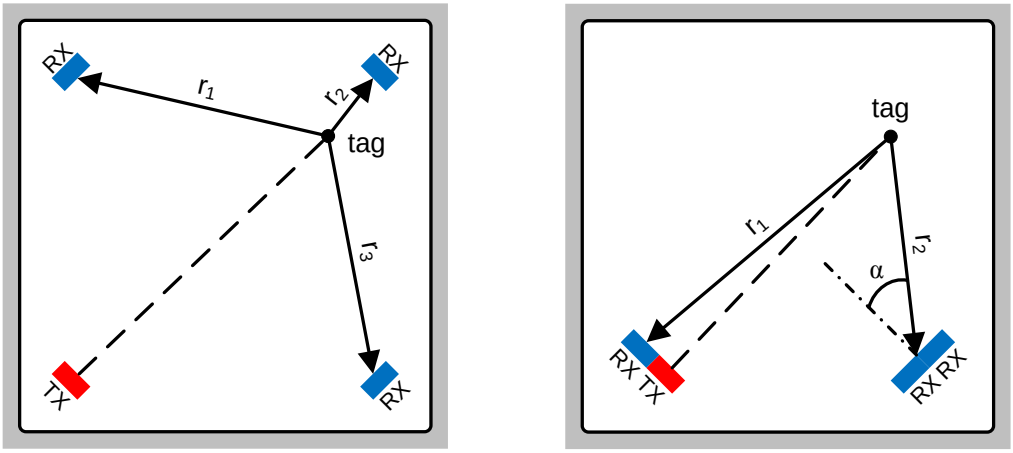
There are two additional parameters limiting the ranging accuracy. The coherence distance is the maximum distance over which an antenna can be moved before the correlation between previous and new CIR drops below a given limit. Similarly, the coherence bandwidth is the maximum frequency shift of the signal before the correlation between previous and new CTR drops below a given limit. The measurement system bandwidth can be defined using this parameter: for wideband system, the bandwidth used for ranging is larger than the coherence bandwidth. On the contrary, for narrowband system, the utilized bandwidth is smaller.

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 hardware constraints listed in Section 2.5, 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



(a) Distance only

(b) Distance and direction

Fig. 3.3: Antenna placement scenarios for positioning

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 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-based ranging methods are able to provide high accuracy of range estimation because of their robustness to the variation of signal strength. Phase measurement in both time and frequency domain described below has been explored and published in [1, 3].

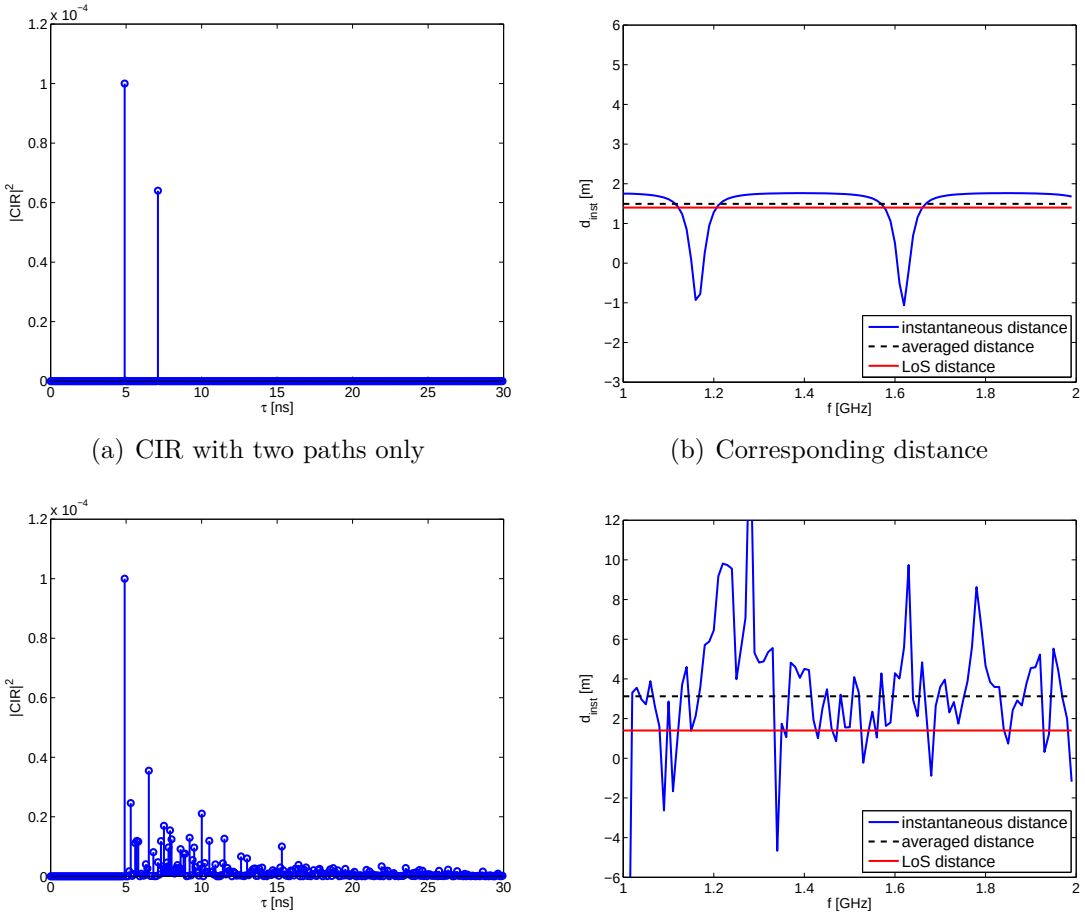
The range estimation is sensitive to the phase corruption caused by multipath propagation because all these methods are based on narrowband measurements. As a consequence, the estimation is given by an average of several group delays, which are the derivatives of the phase with respect to frequency.

The problem is depicted in Fig. 3.4. An “instantaneous distance” with respect to measurement frequency has been computed based on the CIR after phase un-

wrapping according to:

$$d_{inst} = -\frac{\Delta\phi}{\Delta f} \cdot \frac{c}{2\pi}, \tag{3.5}$$

where $\Delta\phi$ is the phase difference between the CTF samples spaced by Δf, and c is the speed of light.



(a) CIR with two paths only

(b) Corresponding distance

(c) CIR with stochastic NLOS part

(d) Corresponding distance

Fig. 3.4: Relationship between CIR and instantaneous range

For a simple deterministic channel with only two paths, as shown in Fig. 3.4(a), the averaging over large bandwidth works reliably – the difference between true LOS distance and the estimation is only a few percent. The estimation is always positively biased (higher than LOS) because all the NLOS paths arising from multipath propagation are longer than LOS. For a narrowband measurement, e.g. near 1.15 GHz in Fig. 3.4(b), the result may be completely wrong and leads to negative distances.

If we consider a CIR with large stochastic NLOS part, e.g. Fig. 3.4(c), the range estimation gets significantly biased even using a large averaging bandwidth – the

range in Fig. 3.4(d) is about two times higher than the true LOS distance. The results from narrowband measurements in such multipath scenarios are therefore purely random.

3.3.1 Narrowband PDoA with LFM Chirp

This chapter introduces a method based on the evaluation of received signal phase change during a linear frequency modulation (LFM) chirp. The phase of signal arrival is converted to the instantaneous frequency of a FMCW beat. Range estimation is afterwards calculated from the averaged instantaneous frequency. A chirp signal can be expressed as:

$$s_{TX}(t) = \sin\left(2\pi \int_0^t (f_0 + \mu t')\, dt'\right) = \sin\left(2\pi f_0 t + \mu\pi t^2\right), \tag{3.6}$$

where f_0 is the frequency at time $t = 0$, and μ is the chirp rate, defined as a frequency change B over time T, i.e. $\mu = B/T$. Two chirp signals with 90° phase difference, $s_I(t)$ and $s_Q(t)$, are necessary for baseband mixing.

One of these signals, e.g. $s_I(t)$, is transmitted by the reader and propagates through an environment. It is reflected by numerous targets, as well as by the selected RFID tag. The backscattered tag signal needs to be distinguished from other targets. This is done using tag modulation:

$$s_m(t) = \cos\left(2\pi f_m t\right), \tag{3.7}$$

where f_m is the backscatter modulating frequency. As a result, the desired signal received by the reader consists among others of the AM modulated signal shifted by a propagation time τ:

$$s_{RX}(t) = s_I(t - \tau) \cdot s_m(t). \tag{3.8}$$

Other multi-path propagations are neglected for this simplified scenario. The received signal is mixed into the baseband by multiplication in both I and Q channels, and unwanted frequency conversion products are filtered out using a band-pass filter tuned around the tag frequency f_m. Afterwards, the signals are demodulated by a coherent demodulator or a simple envelope detector, and the phase $\phi(t)$ of received signal is computed.

At this time, we can measure the phase of arrival (PoA) over the frequency range defined by the bandwidth B. As the measurement takes place in a continuous chirp, there is no ambiguity typical for phase difference of arrival (PDoA) methods [27]. The signal phase as a change in time can be expressed using the instantaneous frequency:

$$f_i(t) = \frac{1}{2\pi}\frac{\mathrm{d}}{\mathrm{d}t}\phi(t), \tag{3.9}$$

which corresponds to the beat frequency of conventional FMCW radars. This frequency depends on chirp rate and signal round trip time:

$$f_b(t) = \mu \cdot \frac{2d}{c}. \tag{3.10}$$

The result from the equality of (3.9) and (3.10) determines the range estimate:

$$d = \frac{c}{2} \cdot \frac{\overline{f_i(t)}}{\mu} = \frac{c \cdot T}{4\pi \cdot B} \cdot \overline{\frac{\Delta}{\Delta t}\phi(t)}. \tag{3.11}$$

The instantaneous frequency is computed for every sample and averaged. As can be seen from (3.11), the range estimation depends only on chirp rate and averaged instantaneous frequency.

This ranging method is very effective for simulations, but its practical realization is rather complicated as it requires high system bandwidth, and its performance is low because of described narrowband processing. It is therefore more common to use the frequency hopping, as described in the next section.

3.3.2 Narrowband PDoA with Frequency Hopping

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 [29] 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:

$$d = \frac{c}{4\pi \cdot \Delta f} \cdot \overline{\Delta\phi} - l_{corr}, \tag{3.12}$$

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 [53]), and various delays of the front end.

Described method is not reliable for complex multipath environments [16, 54]. 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}, as discussed in Section 3.3.

3.3.3 Multi-carrier Wideband Ranging

Instead of frequency hopping, 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. 3.5. 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.

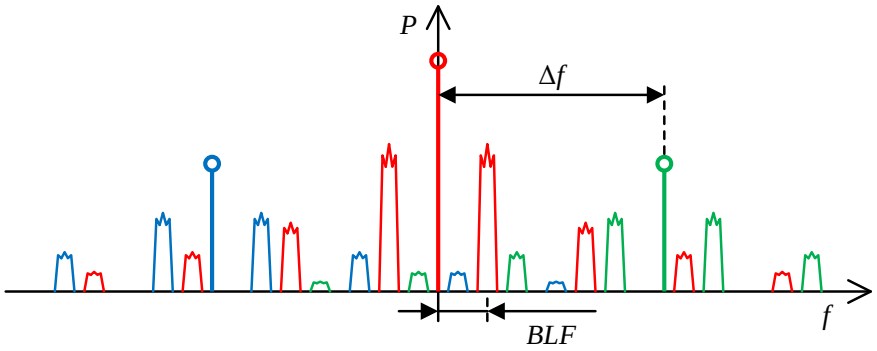


Fig. 3.5: Multi-carrier measurement, high power signal and two subcarriers

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 [29, 55, 56]. Fig. 3.6 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). Direction estimation for antenna arrays with more than two elements can be solved by MUSIC algorithm [31, 58].

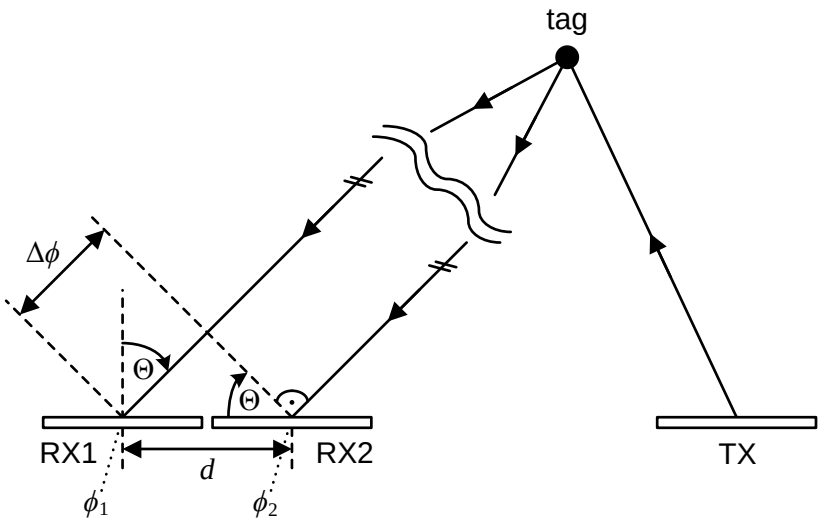


Fig. 3.6: Direction of arrival finding with SD-PDoA method

The arccos(·) 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 $d > \lambda$ [32].

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 [47]. 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 (see Section 2.3), 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 block structure of RCHE source files is shown in Fig. 3.7.

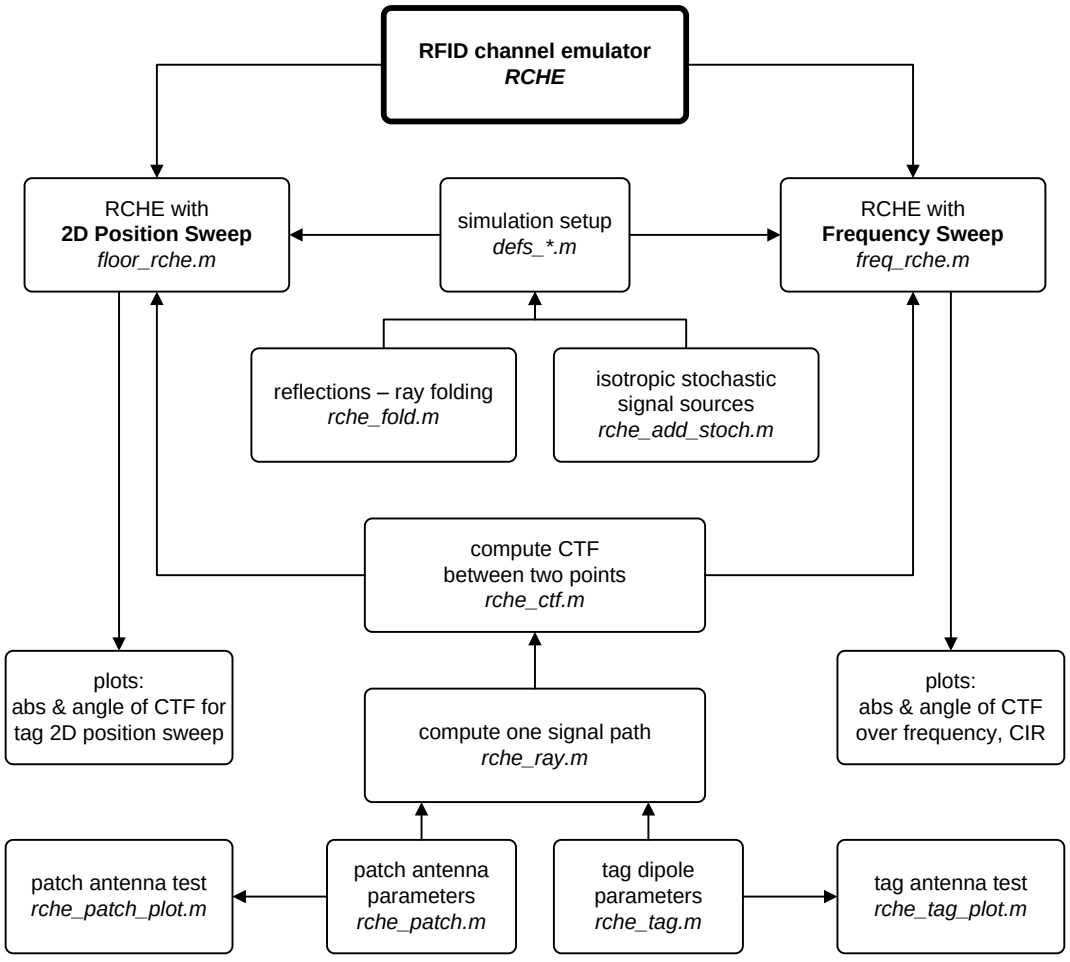


Fig. 3.7: Structure of RCHE source files

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 Appendix A. 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.

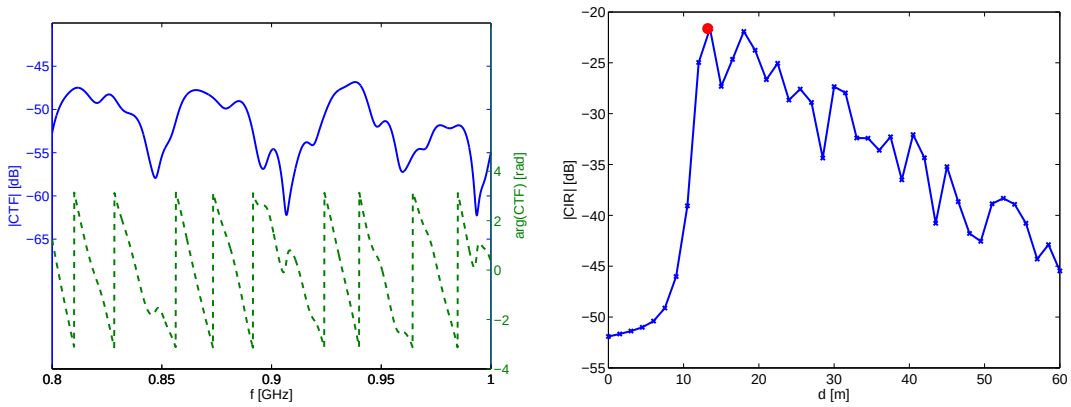
The deterministic simulation can include multiple signal reflections. Every signal path is computed (two complex CTFs for TX–tag and tag–RX) and added together. The stochastic components are modeled using a defined number of isotropic signal sources. Each of these sources has a random position outside 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. 3.8 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 averaging (see Section 3.3), and the FFT range estimation based on the first component in the CIR (as described in Section 3.1).



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

Fig. 3.8: Example of RCHE with frequency sweep

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.

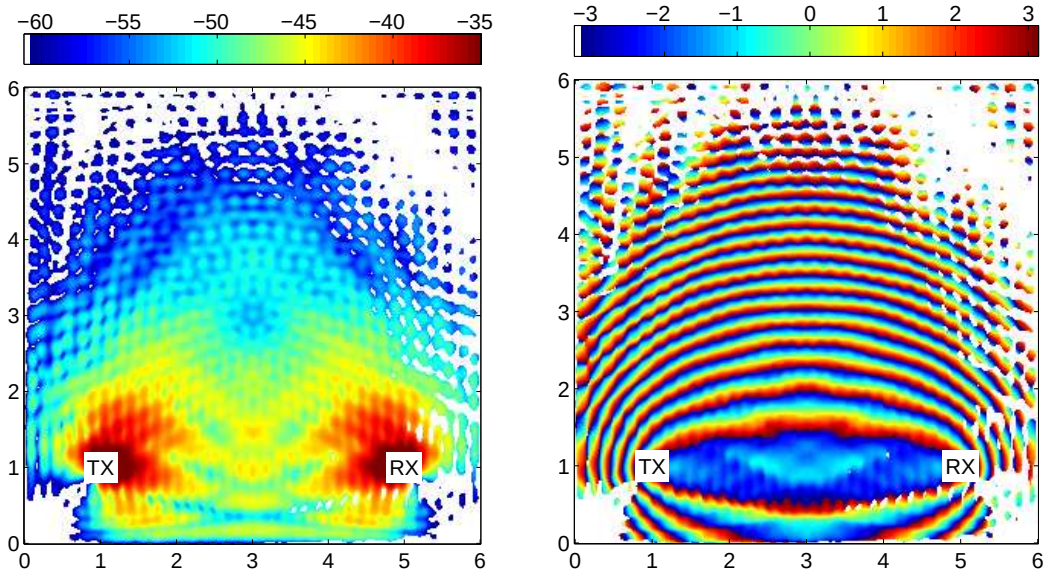
Examples of amplitude and phase of the simulated signals are shown in Fig. 3.9. White color in the images shows the regions, where the power level was under the threshold – either under the minimum tag power-on threshold or under the minimum detectable signal.

3.5.2 Channel Models

The simulations have been processed for several levels of complexity. All of them are simplified cases of a real situation without large obstacles in the measurement area. The results are attached in Appendix A. Frequency has been swept from 800 to 1000 MHz with tag placed at $\vec{p}_{tag} = [3, 4, 0.95]$, 2D tag position has been altered over the whole area at 0.95 m height, simulated at 915 MHz. Every model type has been computed for both antenna placements, as described in Section 3.2.

Free Space Deterministic Environment

Free space provides an idealized direct LOS propagation with no multipath. The anechoic RF chamber can be considered as an example of such environment, despite of some limitations on its parameters (typical RF chamber has a reflection coefficient of about -20 dB, as measured in DREL chamber with ECCOSORB VHY-12-NRL pyramidal hybrid absorbers [59]).



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

Fig. 3.9: Example of RCHE with 2D position sweep

The results are shown in Appendix A.1. Simulation is based on LOS propagation only, resulting in a Gaussian degenerate channel. Noise is not considered. Both amplitude and phase of received signal are ideally distributed. There is a strong peak in the CIR, representing the range estimation. Moreover, this channel is practically frequency independent even in a wide band scope.

Ground Reflection (Two-ray Deterministic Model)

Two-ray deterministic model adds a ground (floor) reflection into previous setup with direct ray. Such model can be used to estimate the ranging performance in places like a building roof, large open spaces, etc. Two- and three-ray models are good for RSS calculation, but still not accurate enough for ranging [16, p. 42].

The results shown in Appendix A.2 are very similar to the first scenario. There is a small distortion in the amplitude of received signal, the phase is not affected. Strong range peak in the CIR is clearly visible.

Ideal Room (Multi-ray Deterministic Model)

Multi-ray model consists of a large number of deterministic rays added to the direct path. The rays are created by the reflection from all the walls, floor and ceiling. Only the first and the second order reflections are considered. Such model approximates an ideal room.

Simulation results are shown in Appendix A.3. It can be seen that the amplitude distribution is strongly affected, especially near the reflecting walls. On the other

hand, the phase distribution in short range is still very clear. Range peak in the CIR is clearly visible.

Combined Deterministic/Stochastic Model

Combined model adds stochastic components into previous multi-ray simulation. It is an example of an actual room with small obstacles. Stochastic components are modeled using 40 signal sources with a random position outside the room and a Rayleigh distributed power. The number of sources has been selected according to the central limit theorem.

The simulations based on combined model can be found in Appendix A.4. Both amplitude and phase of received signal are affected by multipath. The tag power-on threshold causes random behavior at longer distances. Range peak in the CIR can be found only if the measurement bandwidth is wide enough.

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. Common RFID communication protocols are described, covering both reader-talks-first and tag-talks-first approaches.

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 Introduction to Software Defined Radio

Software defined radio (SDR) is a modern concept, which uses direct digital signal processing for both reception and transmission [60]. Hardware of such transceiver consists of input RF filters, optional down-/up-conversion, and fast AD/DA converters. The entire signal processing, such as baseband filtering, demodulation, and signal level measurement, is done by software.

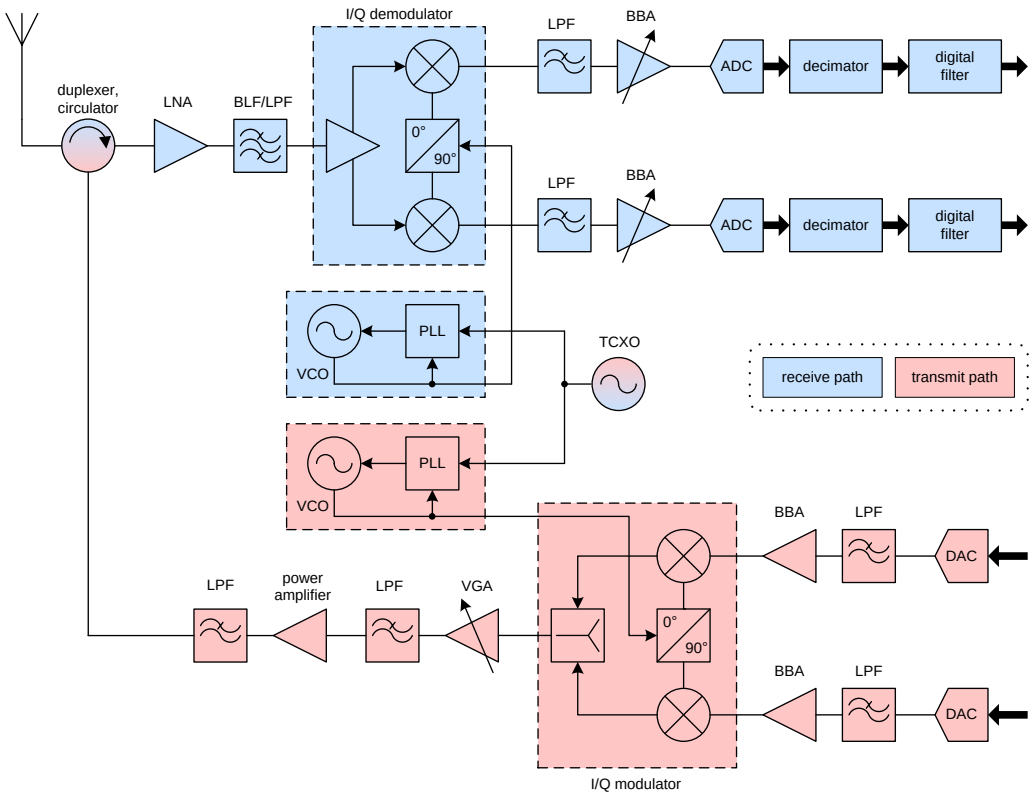


Fig. 4.1: I/Q transceiver architecture for software defined radio

Most of the state-of-the-art AD converters does not provide sufficient speed and resolution for direct sampling on the desired RF frequency. It is possible to overcome this issue with undersampling (also known as band-pass sampling, super-Nyquist sampling [60]) with high quality analog RF band-pass filters, but the widely used principle uses down-/up-conversion to complex baseband signal, as shown in Fig. 4.1. This concept is also used in both systems described later.

The RF signal from the RX antenna is wired to an optional low noise amplifier (LNA), followed by band-pass or low-pass filter (BPF, LPF) and an I/Q demodulator. This demodulator down-converts the RF signal to the zero-frequency IF, i.e. to baseband I and Q channels. Down-conversion is realized by mixing the RF signal with in-phase and quadrature local oscillator (LO) signals, typically produced by a PLL synthesizer. Baseband signals are filtered by LPF, amplified, and connected to high-speed AD converters.

Similar concept is used for transmission. Baseband signals from high-speed DA converters are filtered by LPF, amplified, and connected to an I/Q modulator, which realizes the up-conversion. The RF signal is amplified, filtered, and wired to a power amplifier with another LPF. Its output is connected to the TX antenna.

Digitized baseband signals are typically processed by an FPGA, which provides another frequency conversion and decimation/interpolation to desired lower signal bandwidths.

4.2 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 [61] is only −15 dB. Bistatic readers provide isolation over 30 dB but require two antennas [48].

4.2.1 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 [2]. The principle is based on subtraction of the transmitted signal from the received signal, see Fig. 4.2. 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. The carrier suppression of 30 to 45 dB is achievable using this active cancellation [43].

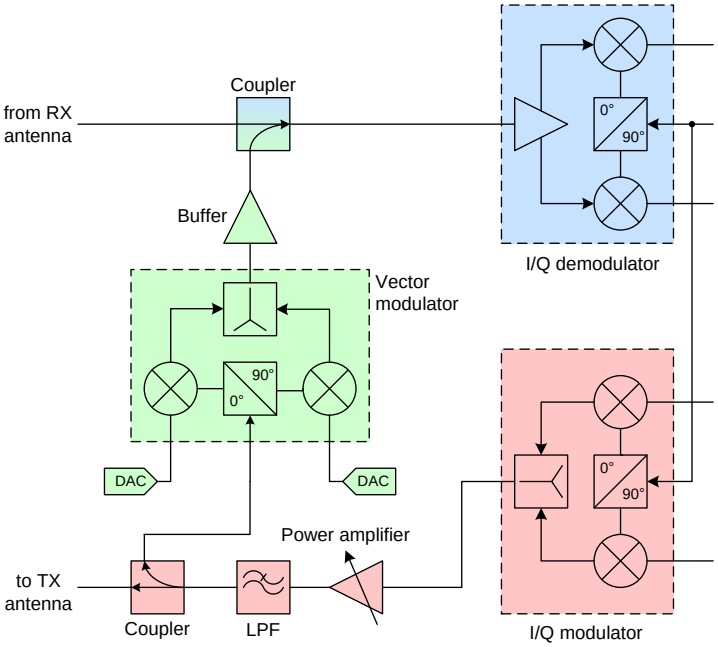


Fig. 4.2: Carrier cancellation by destructive interference (subtraction)

4.2.2 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

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 4.5.1.

4.3 RFID Communication Protocols

A communication protocol is an agreement on conventions about how to send the messages. It must specify the medium and its access methods, the message format, and the content of messages. The RFID protocols for systems operating in the UHF band can be divided into three groups according to medium access methods: reader talks first (RTF), tag talks first (TTF), and tag talks only (TTO).

The general UHF RFID band is 860 – 960 MHz. Depending on the national regulation authority, only a small part of this band is actually released for RFID systems operation. The band allocation is not coordinated world-wide. European band features four high-power channels at 865 – 868 MHz (ETSI EN 302 208 [62]), while the frequency range 902 – 928 MHz is being used in the USA (FCC part 15.247 [63]). The bandwidth is therefore 3 MHz in the EU and 26 MHz in the USA.

The two most common protocols have been standardized in ISO 18000-6:2010 [64] as parts C and D. Part C is an RTF protocol specification known as EPC Class-1 Generation-2 UHF RFID standard [17], or simply Gen2. The recent TOTAL (tag only talks after listening) specified in part D extends the iP-X TTO protocol, which has been used by IPICO and EM Microelectronics (EM4122 tags [65] and their successors).

4.3.1 EPC Class-1 Generation-2 UHF RFID

The Gen2 is robust and flexible RTF standard with Aloha-based adaptive collision resolution [17, 13]. It features variable data rates and modulations for spectral control of reader and tag transmissions, several memory banks including user memory, memory locking, variable-length commands, and link cover coding for basic security.

Traditional approach to an inventory round (see Fig. 4.3) consists of **Select** command, followed by **Query** with specified slot count (Q value) and **QueryRep** repeated for every remaining slot. If a tag replies in any slot, the reader receives its RN16 and replies with **Ack** (this is a time-critical operation, the **Ack** must be send during short T_2 time [17]). After the tag backscatters its EPC, a **ReqRN** command may be issued by the reader. In this case, the tag transits to Open state and additional commands can be sent.

Readers typically use amplitude shift keying (ASK) modulation. Tags backscatter the response by changing their antenna reflection coefficient. The signal observed at reader therefore depends on the distance and multipath propagation, which is

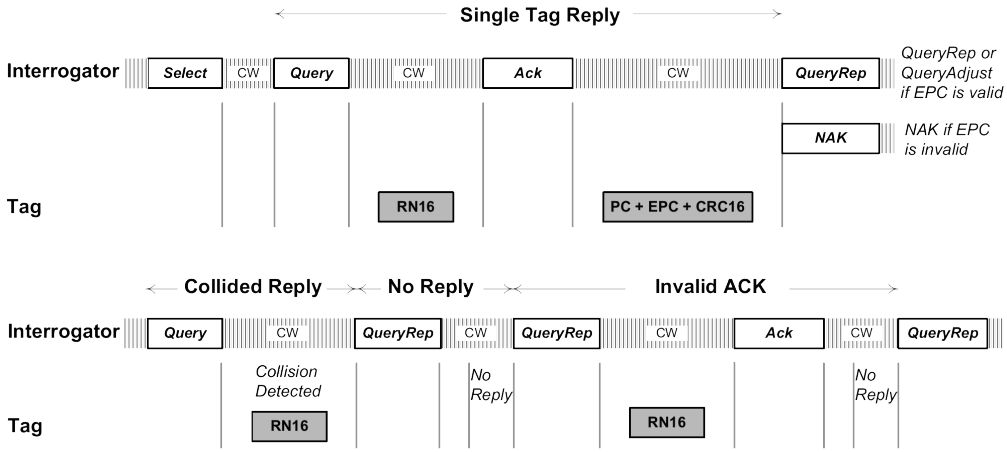


Fig. 4.3: Gen2 interrogation process [17]

unpredictable. Therefore, all tag codes are based on frequency shift keying (FSK) modulations, i.e. the demodulation is performed according to the number of changes in tag state during a given time interval.

For the laboratory experiments, it is typically sufficient to capture the response of one RFID tag only. Single **Query** command (with Q = 0) can be transmitted and the RN16 response received. The tag internal protocol processing times out and the **Query** may be repeated without any other commands as many times as necessary. This approach is used in both developed systems. As a result, the overall processing speed is not critical. It is also possible to pick one tag from a larger group using the **Select** command transmitted before the **Query**.

4.3.2 Tag Only Talks After Listening (TOTAL)

Collision arbitration in the TOTAL protocol is based on TTO approach; the IDs backscattered by tag are separated by pseudorandom delays, e.g. Fig. 4.4. The implementation on the RFID reader side is therefore very simple – it just transmits CW signal and receives the tag responses. Tag collisions are filtered according to the CRC checksum of the backscattered ID.

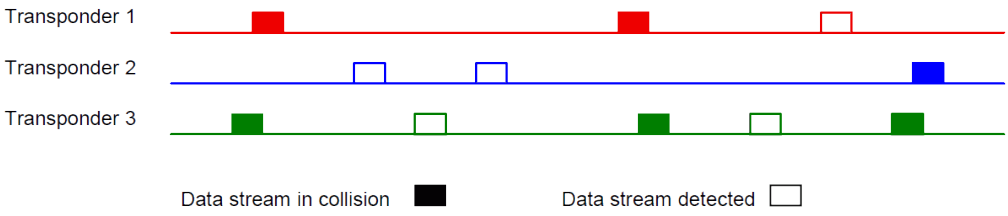


Fig. 4.4: Typical TOTAL tag transmissions [64]

4.4 Experimental Interrogator EXIN-1

First ranging experiments were performed on a modified commercial reader RFI21.1 manufactured by Metra Blansko [66]. The experience from these tests leads to development of the RF front end especially for UHF RFID applications. This reader has been completely designed from scratch using modern integrated circuits and discrete components.

Basic block diagram of the developed system is shown in Fig. 4.5. It consists of four main blocks: front end unit, power amplifier unit, circulator, and AD and DA converters followed by a signal processing unit.

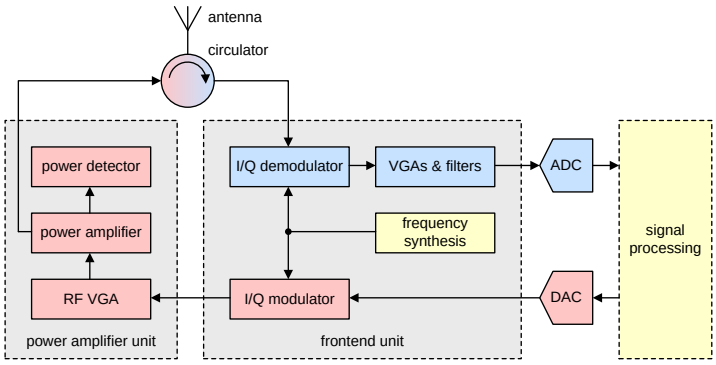


Fig. 4.5: Experimental UHF RFID front end block diagram

The front end should be capable of operation in the frequency range of 860 – 960 MHz, which covers both the EU and the US bands for UHF RFID standards. Output power should be adjustable in the range from 10 dBm to 33 dBm. The design is modular, i.e. any of the blocks can be removed or replaced by new version without the need to replace other blocks. Operation in both bistatic and monostatic (using the circulator unit) modes is supported.

The digital signal of AD and DA converters is prepared for connection to FPGA signal preprocessing board. For simplified operation, it is also possible to bypass DA converter and connect the modulator input directly to the outputs of a microcontroller. Basic RFID reader commands can be generated very simply this way.

4.4.1 Front End and PA Layout

The Analog Devices ADF9010 front end [67] comprises the frequency synthesis, TX quadrature modulator, external RX quadrature demodulator, and RX baseband filters with programmable gain and cutoff frequency. Conversion between RF signals in 900 MHz band and baseband I/Q signals is direct without any immediate frequencies. This concept ensures high linearity and low noise signal path [46].

The carrier leakage into the RX causes a self blocker signal, which is inherent for all RFID reader systems. In this configuration, the self blocker is converted into DC

offset at I/Q channels and can be filtered out. This is not possible with multiple-IF receiver [43], where the carrier cancellation is necessary to allow optimal signal reception.

Common Blocks

Clock distribution and PLL synthesis are common for both RX and TX paths. A temperature compensated crystal oscillator (TCXO) working at 40 MHz is used as the main clock source. Using one clock only distributed all over the testbed ensures the coherence of all system clocks.

The synthesizer is integrated into main front end IC. It is an integer-N PLL with LC-VCO, working at 3.6 GHz band (four times the LO frequency) [67]. Typical phase noise of the synthesizer is −120 dBc/Hz at 100 kHz offset with −70 dBc SFDR at 250 kHz offset [68].

Transmit Path

The transmit path, shown in Fig. 4.6, begins with a differential I/Q upconverter and a driver amplifier, fully integrated into ADF9010 IC. The output level of the driver is up to 8 dBm with 20 MHz baseband bandwidth. The modulated signal is amplified in RF variable gain amplifier (VGA). It consists of two digitally programmable attenuators and a fixed-gain amplifier. The gain range of the VGA is −49 dB to +11 dB at 900 MHz. This block acts as a driver for the power amplifier stage, which uses PA1162 linear hybrid module.

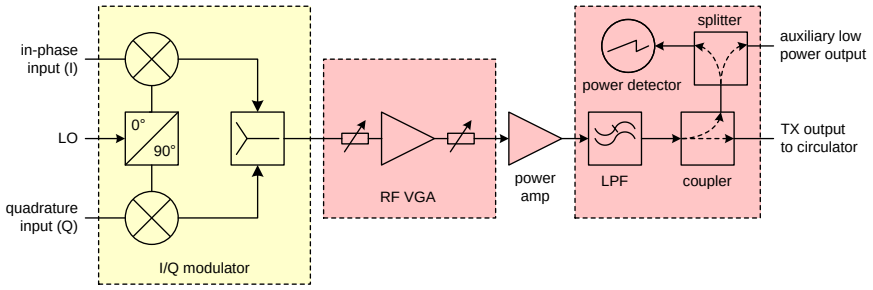


Fig. 4.6: Transmit path block diagram

The unwanted high-order harmonics are later filtered out using a low-pass filter and the signal is led to a directional coupler, followed by a splitter. These weakly coupled signals are used for power measurement and as an auxiliary output from the PA module, e.g. for carrier cancellation unit.

The baseband signal for the upconverter is usually generated by a high-speed DA converter. For testing purposes, it is possible to use a simple 1 bit conversion (digital output) from a microcontroller. This signal would not meet regulatory requirements because of missing shaping, but it is sufficient for experimental measurements.

Receive Path

Fig. 4.7 shows the block diagram of RX path. The first component is a PIN diode, connected as a RF power limiter. This protection is very important on an experimental prototype, as a large TX signal connected accidentally to RX input may damage the demodulator.

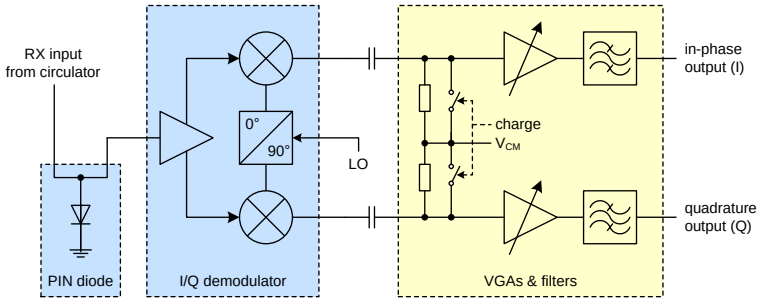
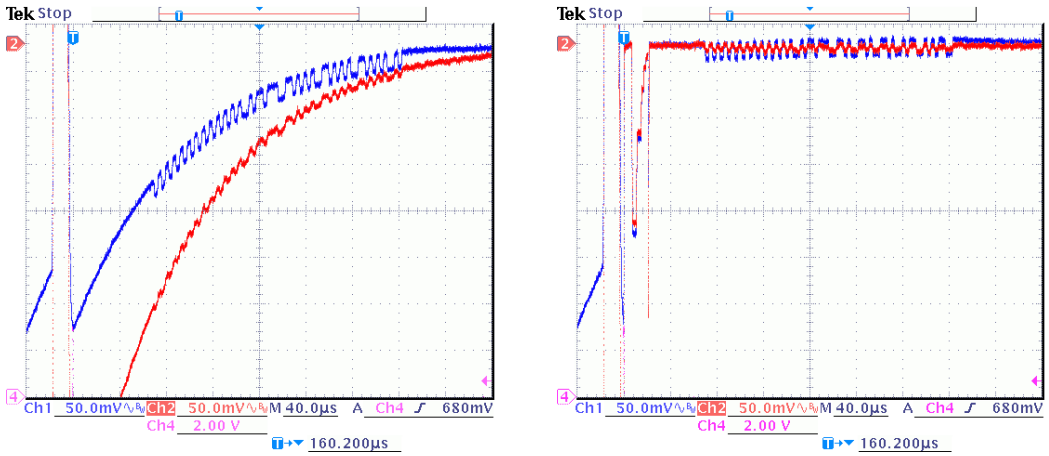


Fig. 4.7: Receive path block diagram

The I/Q mixer used for quadrature demodulation must be able to handle high self blocker signal leaked from TX section. Selected ADL5382 demodulator achieves input IP3 of 33 dBm, making it suitable for this purpose.

The self blocker signal is mixed with local oscillator (LO) signal from the synthesizer, which is coherent. Therefore, it produces large non-zero DC offsets at both I and Q outputs of the mixer. These DC offsets can be filtered out using a simple AC coupling by a capacitor. The disadvantage of this solution is that after a TX to RX transition the coupling capacitors are not charged to proper common mode voltage level and they start the charge up too slowly, as can be seen in Fig. 4.8(a).



(a) RN16 superimposed on unboosted TX-to-RX transition

(b) TX-to-RX transition, followed by AC coupling boost charge and RN16

Fig. 4.8: The effect of AC coupling boost charge after TX-to-RX transition

The ADF9010 IC includes a boost mode to quickly charge the coupling capacitors to the desired common voltage level (see Fig. 4.8(b)). This boost is started manually after every TX to RX transition. The baseband RX functions include continuous time low-pass filters with programmable cut-off frequency and a VGA with programmable gain from 0 to 24 dB in 3 dB steps [67]. Amplified and filtered baseband signal is usually connected to a high-speed AD converter and processed by an FPGA.

4.4.2 EPC Gen2 Testing

The presented front end has been tested as a prototype. Basic measurements have been done with UPM ShortDipole tags. These tags are compatible with EPC Class 1 Generation 2 UHF RFID protocol [17].

Fig. 4.9 shows a basic Gen2 inventory round. The tag population to participate in the round is selected at first, followed by the **Query** command. The tag responses with random number **RN16**, which should be acknowledged by the reader. After correct acknowledgement, the tag backscatters its EPC and changes its inventoried flag. Another tag may respond to succeeding **QueryRep**s in the inventory round.

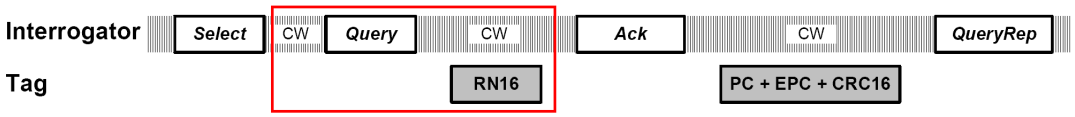


Fig. 4.9: EPC Gen2 interrogation process with Query command [17]

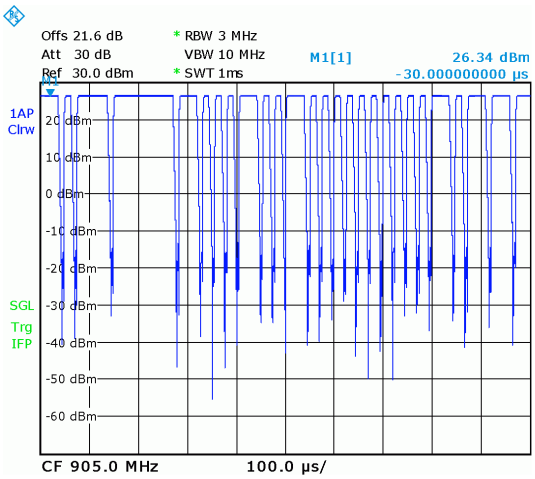
For the testing of developed front end, it is sufficient to measure the response of one RFID tag only. Therefore it is necessary to transmit single **Query** command only and observe the **RN16** response (highlighted in Fig. 4.9). The tag internal protocol processing times out (T_2 parameter in [17]), and the consequent **Query** (see Tab. 4.1) may be repeated as long as needed.

The baseband signal for upconverter has been generated by an AVR microcontroller using 1 bit DA conversion. Fig. 4.10(a) shows the transmitted RF signal with amplitude keying.

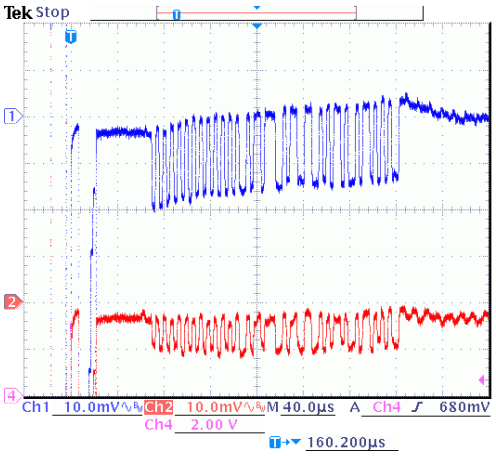
Received **RN16** response from the tag has been captured (see Fig. 4.10(b)) during the test with $f = 905$ MHz, $P_{OUT} = 27$ dBm, $G_{VGA} = 12$ dB, $BW_{VGA} = 1$ MHz, and an RFID tag in the distance of 0.5 m from Poynting PATCH-A0025 antenna.

Tab. 4.1: Query command structure with parameters description

Data	Parameter	Description
preamble	Tari = 25 µs	Tari length
	RTcal = 75 µs	R→T calibration
	TRcal = 133 µs	T→R calibration
1000	**Query**	Command ID
1	DR = 64/3	BLF: 160 kHz (with TRcal)
00	M = 1	FM0 coding
1	TRext = 1	Use pilot tone
00	Sel = All	Don't test SL flag
00	Session = S0	S0 powers-on in A target
0	Target = A	Query A tags
0000	Q = 1	One slot in the round only
01011	CRC-5	CRC-5 over the Query



(a) Query command captured from RF signal on a spectrum analyzer in time domain (with zero frequency span)



(b) I and Q signals of amplified and filtered RN16

Fig. 4.10: Transmitted request (Query command) and received response (RN16)

4.5 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 [45]. 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 as an initial development point. Tab. 4.2 overviews the parameters of this system.

Fig. 4.11 shows the block diagram of USRP N200 motherboard, based on Xilinx Spartan 3A-DSP FPGA. The motherboard includes AD and DA converters, Ethernet PHY for Gigabit LAN, and reference clock distribution subsystem locked to a TCXO. Both the FPGA code and the host drivers code are available as open-source under the GPL license.

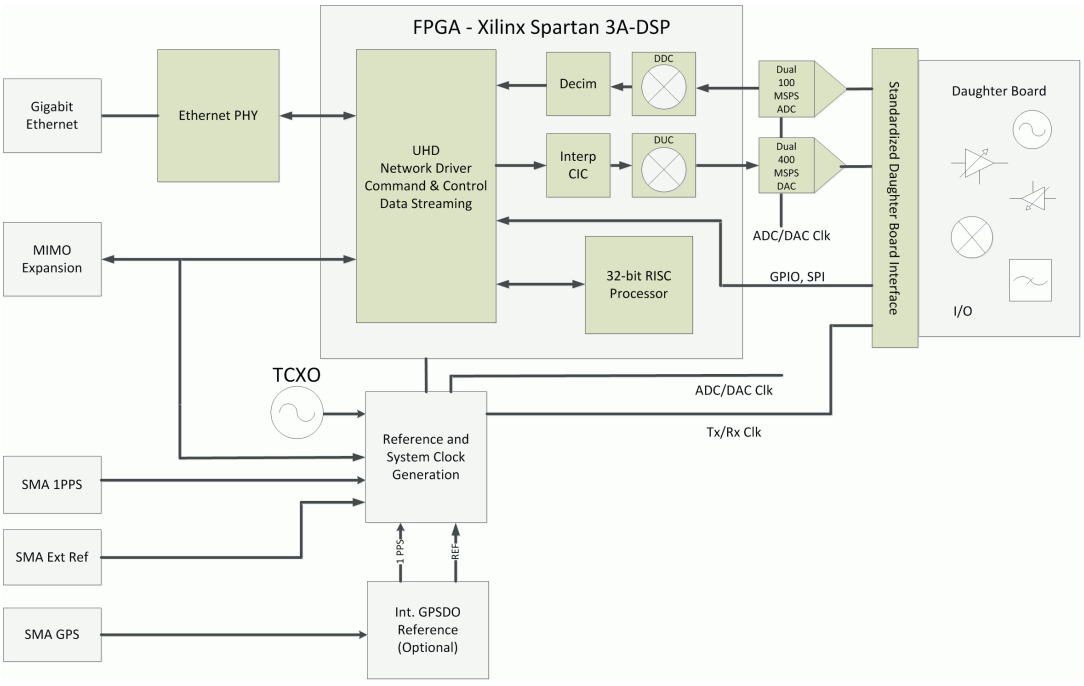


Fig. 4.11: Ettus USRP N200/N210 Networked Series SDR block diagram [69]

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,

Tab. 4.2: Ettus USRP N200 specifications

Parameter	**Typ.**	**Unit**
ADC/DAC sample rate	100/400	MSPS
ADC/DAC resolution	14/16	bits
ADC/DAC wideband SFDR	88/80	dBc
Sample rate to/from host	25	MSPS
Frequency accuracy	2.5	ppm
SSB/LO suppression	35/50	dBc
Phase noise @ 10 kHz	−80	dBc/Hz
Phase noise @ 100 kHz	−100	dBc/Hz
Output power	15	dBm
Input IP3	0	dBm
RX noise figure	5	dB

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.

4.5.1 Hardware and Host Driver Modifications

As described in Section 4.2, 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. 4.12.

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. 4.12). Moreover, the currently unused TX synthesizer needs to be disabled at all, otherwise it produces unwanted signals, which also gets coupled into RX path. Photos of the complete USRP-based measurement system with modified WBX board and the RFID GDB can be found in Appendix B.

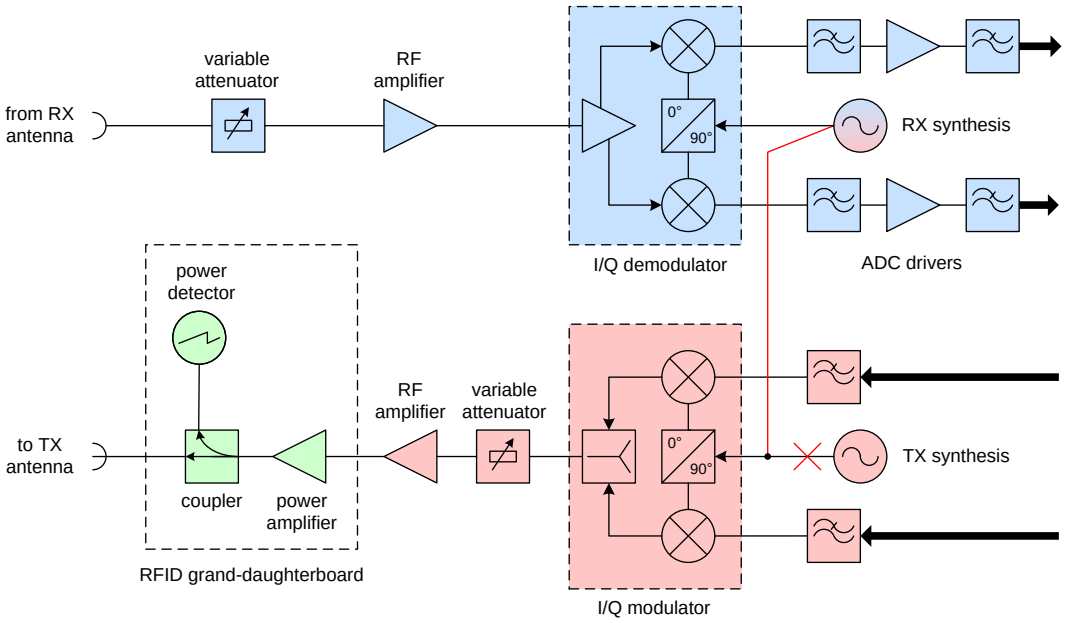


Fig. 4.12: Modified WBX daughterboard + RFID GDB block diagram

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 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.

4.5.2 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 [17]. 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.

4.5.3 MATLAB Interface for Testing System

The top-level measurement control takes place in MATLAB environment. Tab. 4.3 summarizes the available DLL calls imported to MATLAB. 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. 4.13. Computed backscatter link frequency (BLF) and measured output power are 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 4.2.1.

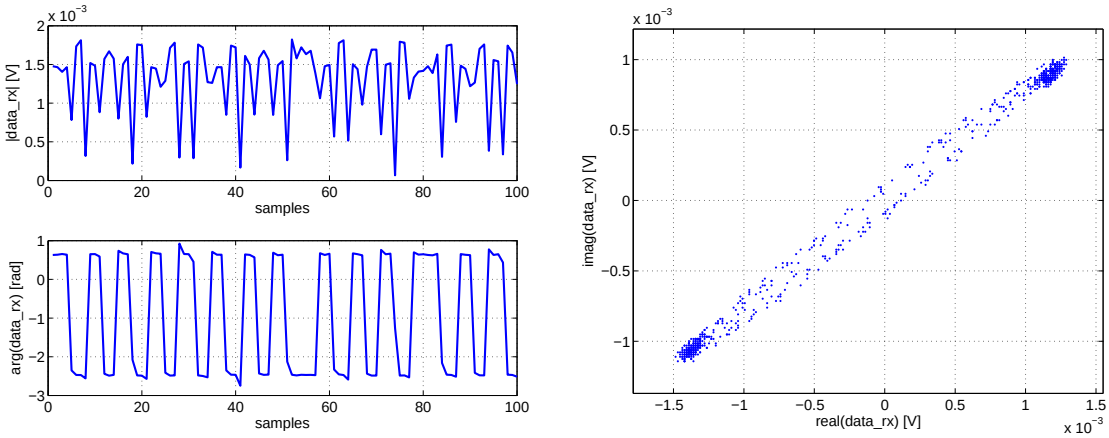
```
1  %% load USRP wrapper
2  load_usrp('192.168.10.2');
3
4  %% prepare reader commands: Select tags with EPC beginning ...
       3005FB63, Query at Tari 12.5us, backscatter link 320kHz ...
       Miller-4, enable TRext
5  select = hex2dec([ '30'; '05'; 'fb'; '63' ])';
6  BLF = prepare_burst(nTARI_12_5, 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
```

Tab. 4.3: MATLAB interface to USRP-based measurement system

Function	Description
`load_usrp()`	Initialize USRP at given IP address.
`unload_usrp()`	Release USRP.
`get_last_error()`	Return last error message and clears it.
`prepare_burst()`	Prepare TX burst with defined parameters. Returns BLF of tag computed from the given parameters.
`load_user_signal()`	Load user-defined signal for transmission.
`save_user_signal()`	Copy the transmission signal to user variable.
`set_freq()`	Set synthesizer frequency in [Hz].
`set_power()`	Set RX gain (0 to 31.5 dB), coarse TX power on main attenuator (14 to 39 dBm, compression and nonlinearity occur at power levels over 32 dBm), and fine TX power on transmitted I/Q data. Returned voltage step is the voltage of one ADC step, i.e. the real input voltage can be obtained by multiplying this value by I/Q sample value.
`trx_burst()`	Transmit the burst and receive tag response. The burst is internally repeated up to 10 times if any communication error occurs, e.g. because of high PC load. Tag data are stored info buffer, the measured power is in [dBm]. Call returns indexes of predicted signal begin and end.
`uart_write()`	Send a null-terminated string to internal UART at J311 (used for communication with the antenna switching matrix).

```
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 described 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



(a) Amplitude and phase

(b) Constellation diagram

Fig. 4.13: Example outputs from backscattered response

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 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 [4].

4.6 Antenna System

Several commercially available reader antennas have been tested. Most of the antenna types were very narrowband, with standing wave ratio (SWR) under 1.5 limit just in a few megahertz band.

Finally, the PATCH-A0025 circular polarization antenna made by Poynting [61] has been selected. This antenna achieves good SWR in the complete 800 – 1000 MHz band, which has been confirmed by measurement (Fig. 4.14). However, its gain is frequency dependent and thus requires calibration if precise signal levels are required.

4.6.1 Switching Matrix

The antenna switching matrix provides an emulation of multi-antenna SIMO system. It allows routing of both RX and TX signals to four connected antennas. The wiring example in Fig. 4.15 shows RX connected to ANT2, TX to ANT3, and unused antennas (ANT1, ANT4) to 50 Ω dummy loads. Switching is performed with a set of RF relays (Omron G6Y), supervised by a microcontroller. Photo of the switching matrix is shown in Appendix B.

Fig. 4.14: Poynting PATCH-A0025 SWR measurement (two antennas)

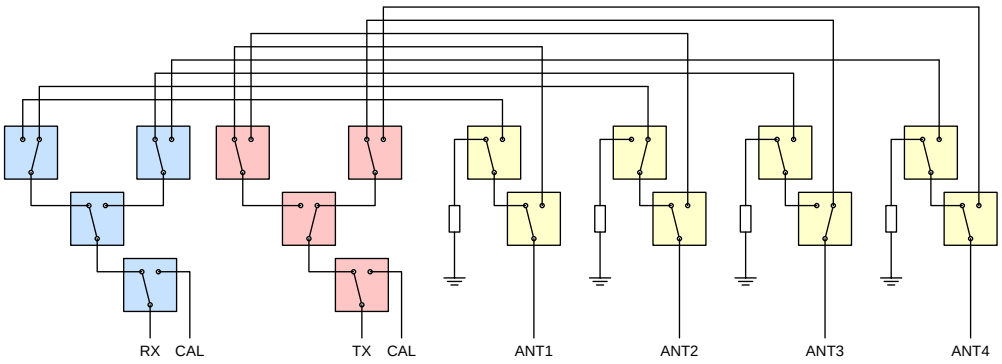


Fig. 4.15: Antenna switching matrix block diagram

Measured insertion loss of each branch is under 1 dB with excellent isolation over 60 dB. Relays allow the RF power of up to 10 W. The drawback of this design is switching time of several milliseconds and a limited endurance. However, guaranteed min. 10^6 operations are satisfactory for a laboratory equipment.

The switching matrix can be controlled manually using two onboard buttons or via an RS-232 compatible serial interface. This interface is also provided in the USRP and available as a MATLAB function.

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. These measurements have been performed according to the scenarios described in Section 3.2.

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.

In order to extract phase information, all the static scattering sources (TX–RX antenna coupling, reflections from obstacles, e.g. Fig. 5.1) need to be filtered out. This is possible because of the tag backscatter modulation. The stationary or slowly moving sources create large DC or low-frequency components in received signal. This behavior is shown in power spectrum estimation in Fig. 5.2(a). The DC component caused by static scatterers and TX leakage is several orders of magnitude stronger than the useful backscattered tag signal at $BLF = 160$ kHz.

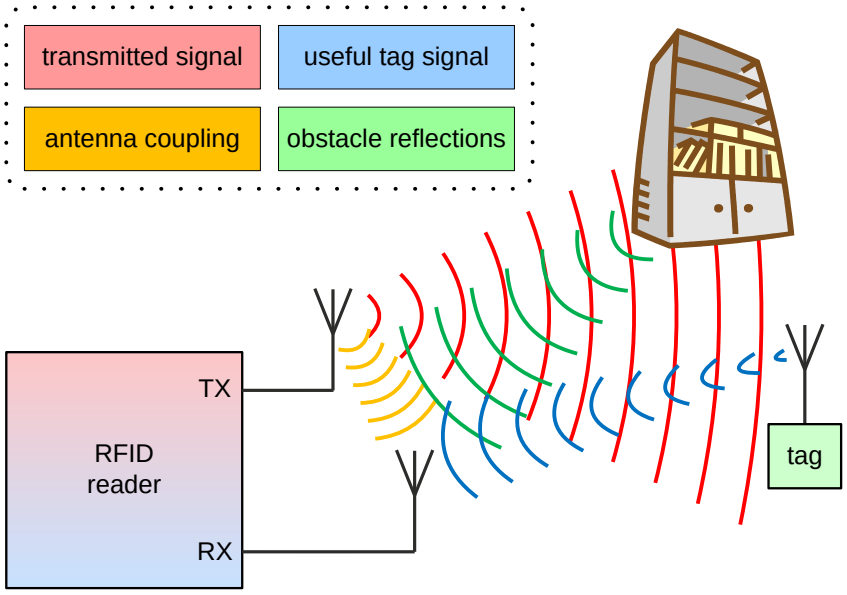
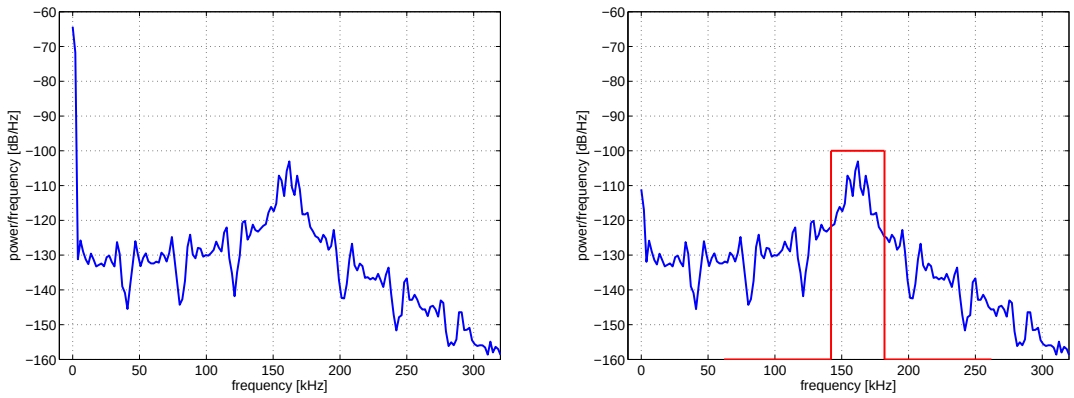


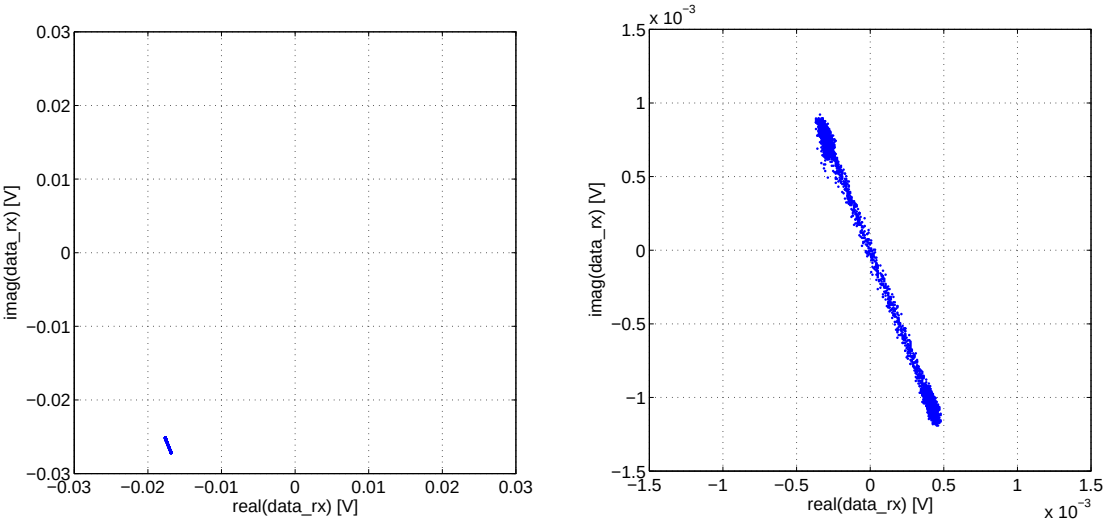
Fig. 5.1: Environment with multiple static scattering sources



(a) Original response (b) Subtracted DC component

Fig. 5.2: Power spectrum of backscattered responses (Impinj Monza)

The corresponding I/Q constellation diagram is shown in Fig. 5.3(a). For the further processing, the DC component needs to be subtracted. This is done by subtraction of complex I/Q signal mean value, as described in Section 4.5.3. As a result, the residual DC component drops below the BLF peak, see Fig. 5.2(b) and scatter plot in Fig. 5.3(b).



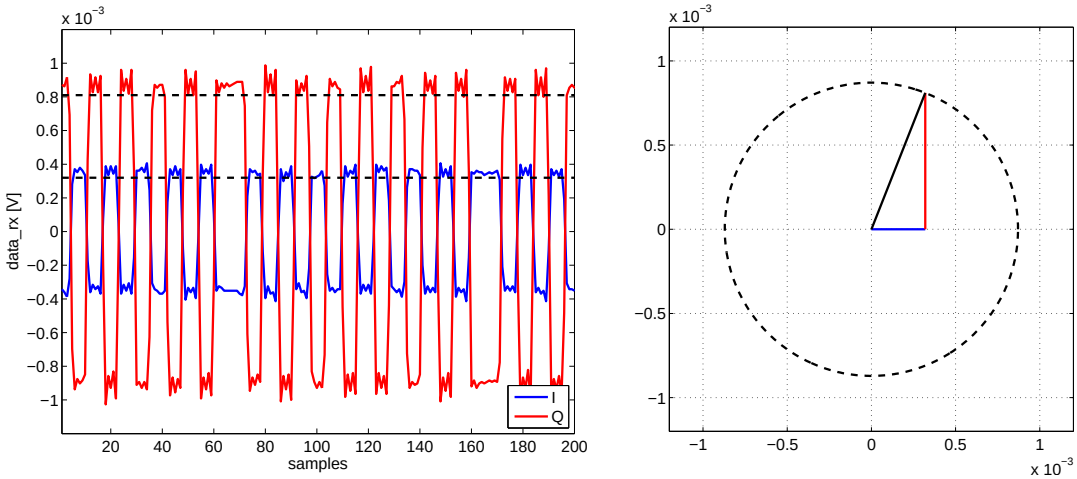
(a) Original response (b) Subtracted DC component

Fig. 5.3: Scatter plot of backscattered responses (Impinj Monza)

5.1.1 Signal Strength and Phase of Arrival

The RSS value is usually available on commercial RFID readers. It provides coarse information about received signal power level, typically inaccurate and without absolute reference. Fig. 5.4(a) shows a basic RSS estimation method. Samples from both

channels are digitally rectified (absolute value after DC subtraction) and averaged over tag response. As a result, two RSS values (always positive) are provided.



(a) Averaging absolute I/Q values (b) $\arctan(RSS_Q/RSS_I)$

Fig. 5.4: Signal strength and I/Q phase (Impinj Monza)

Simple phase estimation can be provided based on arctangent of these values, as shown in Fig. 5.4(b). However, this method suffers from a large drawback, which is the high phase ambiguity [70]. A common ambiguity value of 2π is deteriorated to $\pi/2$ because of the signal rectification process and an unknown initial conditions.

The estimation accuracy can be enhanced by band-pass filtering of the received signal. The BPF for passband near backscatter frequency (red line in Fig. 5.2(b)) allows suppression of wideband noise and interfering signal sources at nearby frequencies. For an exactly known BLF, it is also possible to use the Goertzel's algorithm [71], which provides an effective way to measure the power on a given frequency. This approach has been successfully tested in [3].

5.1.2 Phase Evaluation Based on Cluster Detection

The advanced 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.

Following listing shows basic clustering with build-in MATLAB function. In-phase and quadrature parts of the signal are separated (lines 3–5) and default state is calculated from averaged initial samples (7–8). Finally, the k-medians clustering for $k = 2$ clusters is performed (10–11), and the complex distance C between cluster indices is stored (14).

```
function C = rche_kmeans(data_rx)

% convert complex IQ signal to two cols
X(:,1) = real(data_rx);
X(:,2) = imag(data_rx);

% default starting location – idle state
Xs = mean(X(1:50,:));

% k–medians clustering
[idx,ctrs] = kmeans(X,2,'Distance','cityblock','Start',[Xs; –Xs]);

% compute complex cluster difference
C = (ctrs(2,1) + j*ctrs(2,2)) – (ctrs(1,1) + j*ctrs(1,2));
```

Returned C value carries the backscattered signal amplitude and phase at the given measurement frequency. Therefore, the CTF can be computed by a subtraction of transmitted power value. If the transmitted frequency is synthesized from a phase-coherent reference, it allows frequency sweeping and measurement of complex CTF for an arbitrary bandwidth.

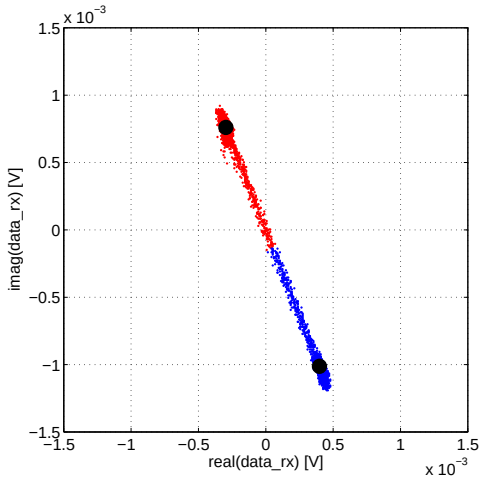
Following pictures show scatter plots and parts of in-phase signal for three cases. First measurement in Fig. 5.5(a) was taken with an Impinj Monza chip RFID tag. The constellation diagram is almost ideal, only slightly affected by noise. Also the received signal in Fig. 5.5(b) is clear, with the initial in-phase value at ca. $-3{\cdot}10^{-4}$ V, correctly identified as red part of scatter plot.

Second measurement was performed on a tag with NXP G2XM chip. Although the transition between tag states in Fig. 5.5(c) is nonlinear in this case [72], the cluster indices are correctly identified including the initial condition (positive in-phase value in Fig. 5.5(d) – red part).

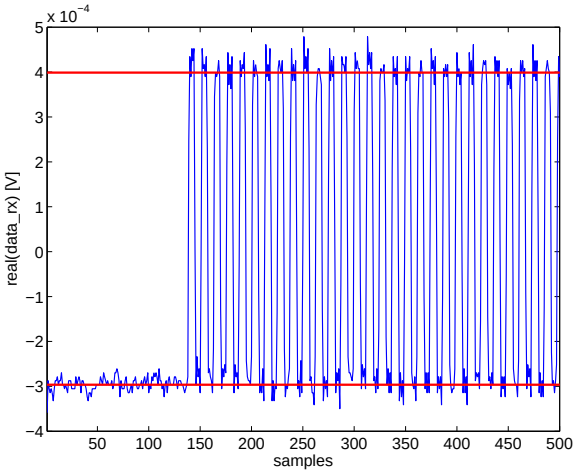
The last experiment was done with NXP G2XM chip again, but this time on a frequency occupied by a nearby GSM transmitter. However, the backscattered response was strong enough to enable clustering even in this case. The constellation diagram in Fig. 5.5(e) shows cluster indices of two tag states, combined with GMSK modulation of GSM symbols. Received signal in Fig. 5.5(f) is heavily disturbed.

5.2 Phase-based Ranging Evaluation

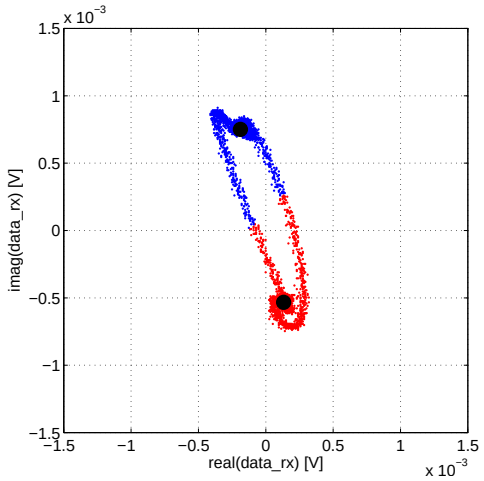
Distance estimation has been tested on the roof of DREL building. Tag responses have been automatically captured with MATLAB script at frequencies from 800 MHz to 1000 MHz with 250 kHz step. Measurements have been performed with a monostatic variant of the system described in Section 4.5, which has been 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 [17].



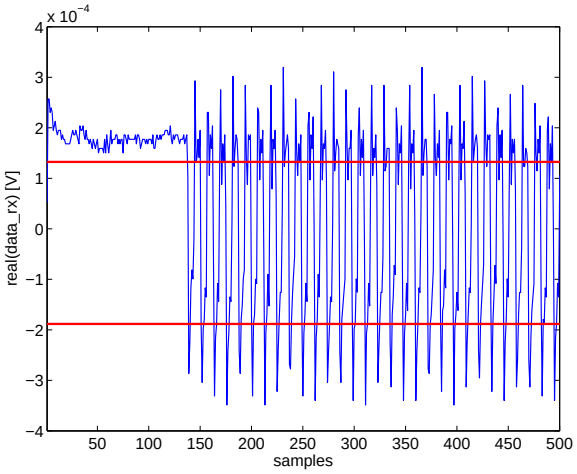
(a) Scatter plot with clusters



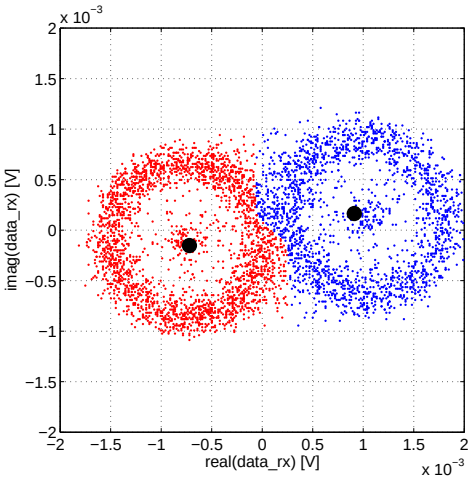
(b) Received in-phase signal (Impinj Monza)



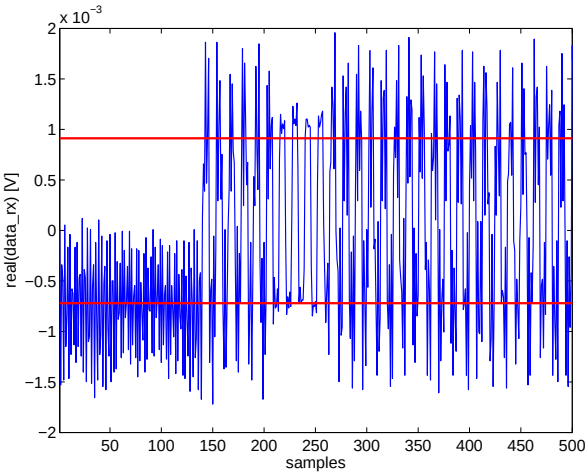
(c) Scatter plot with clusters



(d) Received in-phase signal (NXP G2XM)



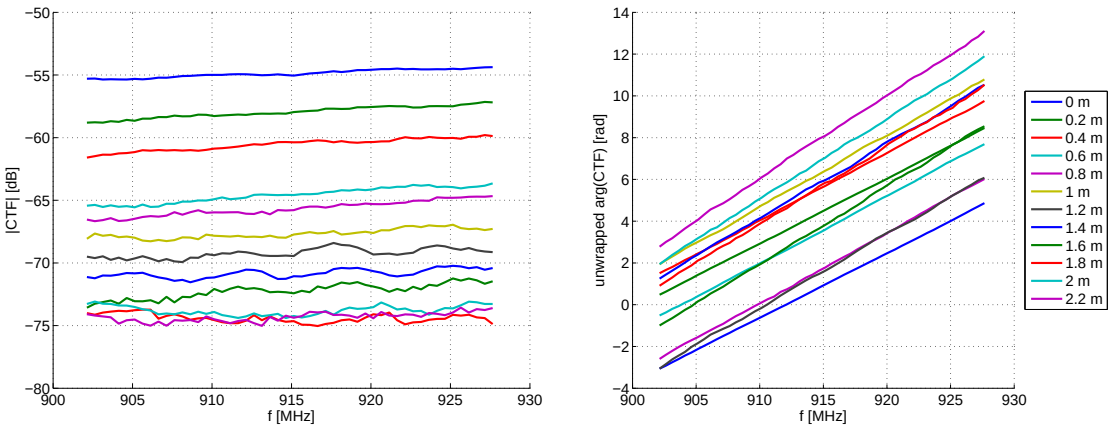
(e) Scatter plot with clusters



(f) Received in-phase signal (NXP G2XM) with GSM signal interference ($f = 944$ MHz)

Fig. 5.5: Constellation cluster detection for various tag signals

Fig. 5.6 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.



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

Fig. 5.6: Measured channel attenuation and phase of received signal

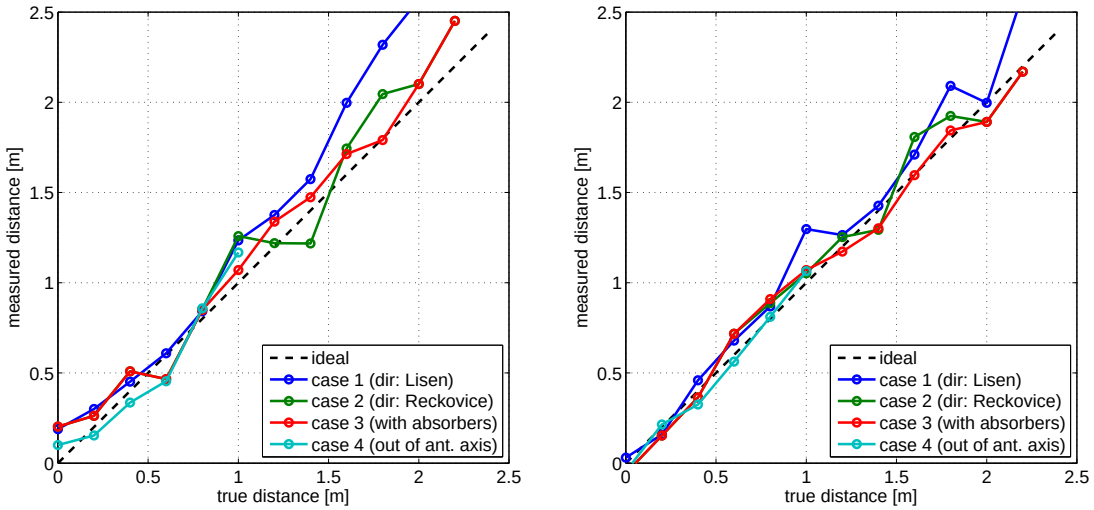
5.2.1 Narrowband PDoA with Frequency Hopping

The distance estimation is calculated from the phase difference average using (3.12). Results include the propagation through antenna cable, delays caused by RF part of the front end, and phase offset of the tag backscatter.

Fig. 5.7(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.

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. 5.7(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.



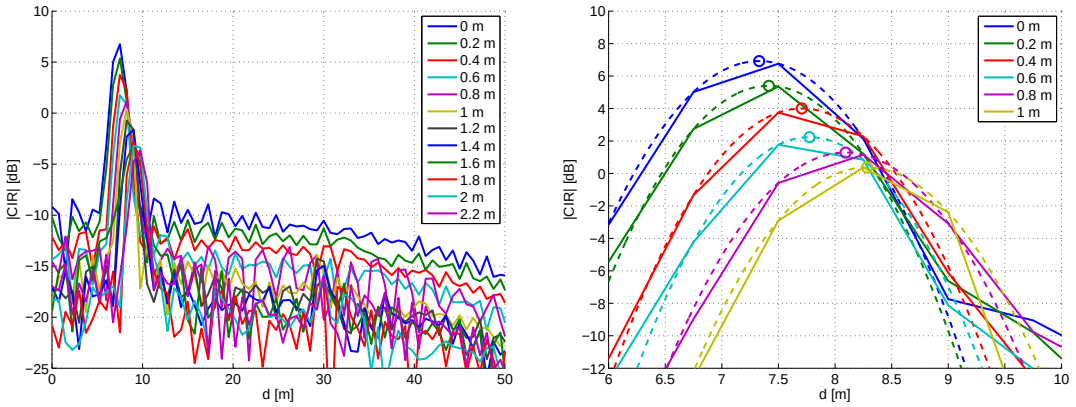
(a) US RFID channels only ($B = 26$ MHz) (b) Wideband average ($B = 200$ MHz)

Fig. 5.7: Narrowband FD-PDoA distance estimation results

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. 5.8(a). The range bias of $l_{corr} = 7.25$ m has not been subtracted in this plot.



(a) Amplitude of channel impulse response (b) CIR peaks with parabolic interpolation

Fig. 5.8: 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. 5.8(b). The CIR peak is found and a parabola is fitted into this peak and its two neighbors [73]. 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. 5.9 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.

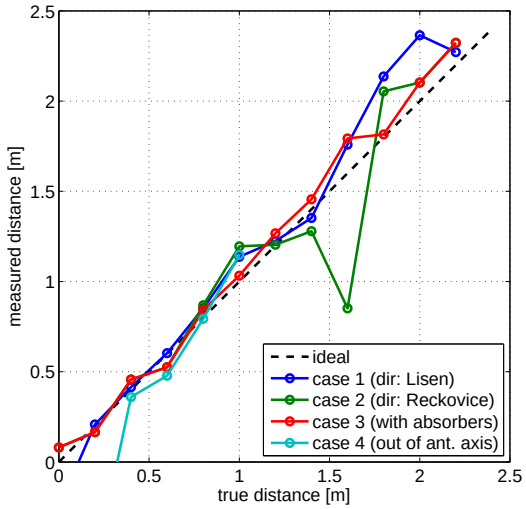


Fig. 5.9: Wideband CIR distance estimation results

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 Direction of Arrival Evaluation

Tag bearing estimation has been tested on a single frequency using a set of four antennas in a row connected to the measurement system via the switching matrix. Both the antennas and the tag under test have been placed in the same height above ground.

Each antenna pair can provide independent direction estimation. The experiment has been done with patch antennas outlying in $d = 0.25$ m distance. Therefore, due to 2π reciprocity of phase difference for $\lambda/2 < d < \lambda$, one solution only exists

for tag bearing $|\theta| < \arccos(c/2fd)$, i.e. $|\theta| < 48°$. Larger θ causes multiple direction solutions due to grating lobes in the beam pattern [32, 74].

With the antenna switching, the measured CTF values can be expressed in form of a matrix:

$$\mathbf{C} = \begin{bmatrix} 1 & c_{1,2} & c_{1,3} & c_{1,4} \\ c_{2,1} & 1 & c_{2,3} & c_{2,4} \\ c_{3,1} & c_{3,2} & 1 & c_{3,4} \\ c_{4,1} & c_{4,2} & c_{4,3} & 1 \end{bmatrix}, \tag{5.1}$$

where $c_{m,n}$ is the complex CTF between m-th RX antenna, the tag under test, and n-th TX antenna. Because of the distance limit, only the neighbor antenna pairs can be used for direction finding. However, each direction estimation on a given antenna pair can subsequently use the tag powered from two distinct sources.

5.3.1 Measurement System Calibration

The measurement requires precise align of phase at the antenna surface. Misaligned phase causes large bearing estimation errors.

Calibration process is based on FD-PDoA ranging averaged over large bandwidth, as described in Section 5.2. The same RFID tag has been placed to each antenna surface and ranged using a monostatic configuration, i.e. the measurement system has been connected via a circulator to TX port of the switching matrix. Therefore, the measured range included switching matrix phase imbalance, cable length variation, optional antenna connector adapter, and antenna phase offset itself. The calibration ranges are as follows:

$$l_{corr} = [l_1, l_2, l_3, l_4] = [7.0442, 7.0476, 7.0256, 6.9806] \text{ m}. \tag{5.2}$$

The difference of several centimeters is good enough for a range estimation but very large for a phase-based direction calculation. Using this distance values, a complex correction coefficient for each antenna pair in a bistatic configuration can be expressed as:

$$\mathbf{K} = \exp\left(-j \cdot \frac{2\pi f}{c} \cdot \begin{bmatrix} 2l_1 & l_1+l_2 & l_1+l_3 & l_1+l_4 \\ l_2+l_1 & 2l_2 & l_2+l_3 & l_2+l_4 \\ l_3+l_1 & l_3+l_2 & 2l_3 & l_3+l_4 \\ l_4+l_1 & l_4+l_2 & l_4+l_3 & 2l_4 \end{bmatrix}\right). \tag{5.3}$$

Due to the inaccuracy of range measurement, this coefficient provides coarse phase correction only. Fine tuning of phase differences needs to be based on reference calibration point. This approach is used later in Fig. 5.10.

5.3.2 Spatial Domain PDoA Measurement

Using the four antenna direction finding system, it is possible to obtain six bearing estimations θ_i based on (2.5), where the measured phase difference is:

$$\Delta\phi = \begin{bmatrix} \phi_{1,3} - \phi_{2,3} & \phi_{2,1} - \phi_{3,1} & \phi_{3,1} - \phi_{4,1} \\ \phi_{1,4} - \phi_{2,4} & \phi_{2,4} - \phi_{3,4} & \phi_{3,2} - \phi_{4,2} \end{bmatrix}, \tag{5.4}$$

where

$$\phi_{m,n} = \arg\left(\mathbf{C}(m,n) \cdot \mathbf{K}(m,n)\right). \tag{5.5}$$

Tag bearing estimation results for nine tag positions are shown in Fig. 5.10. Black point denotes the real tag position. Each subfigure shows six bearings, three of which are independent. Measurement system has been calibrated with reference tag placed at $x = 0$ m, $y = 1$ m.

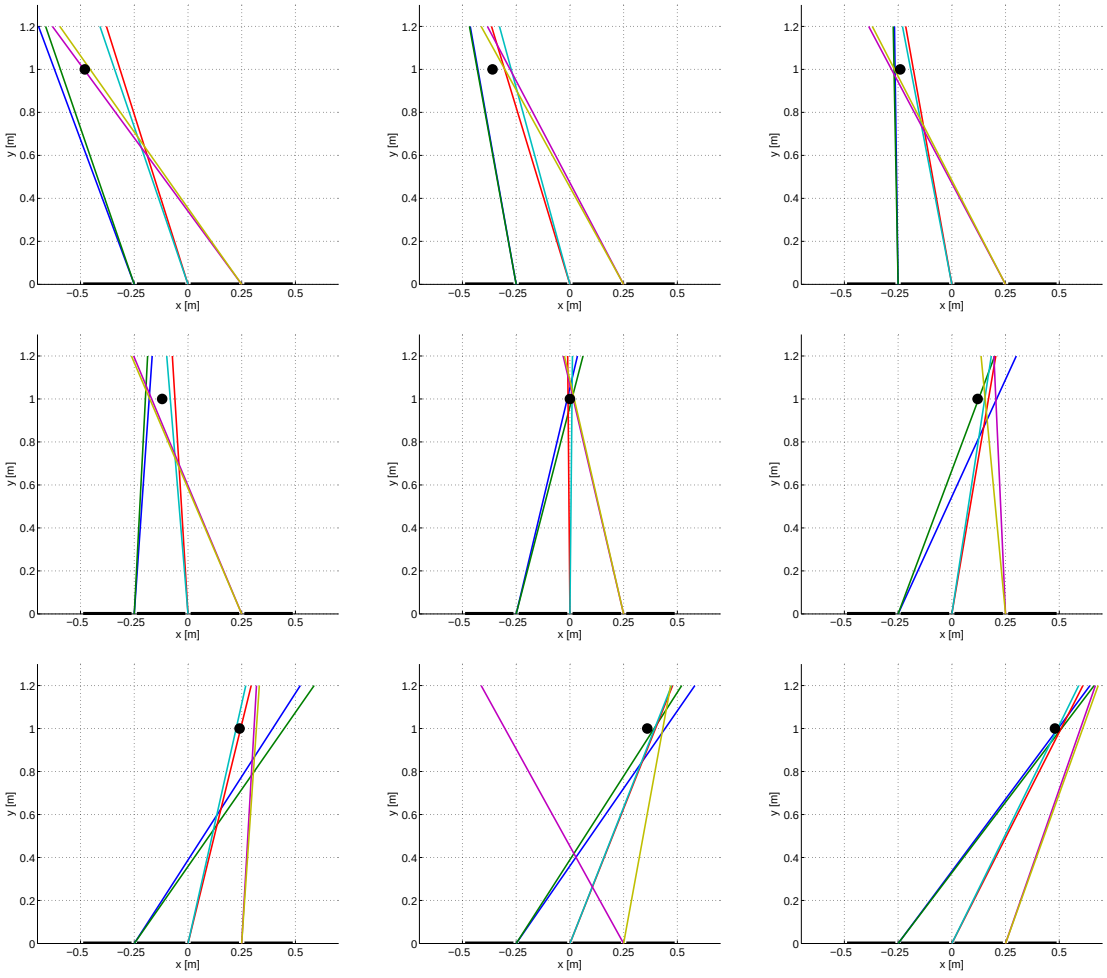


Fig. 5.10: Tag bearing estimation results

5.4 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.

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.

5.4.1 Multipoint Bistatic Ranging

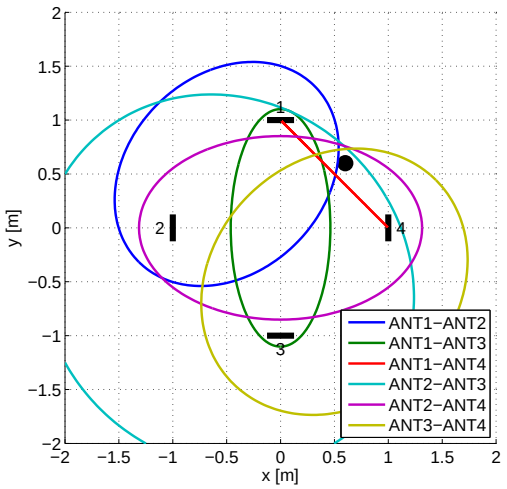
Scenario A allows to estimate a set of bistatic ranges. An area of 1.4×1.4 m with diagonal antenna distance of 2 m has been selected due to limited communication range with passive RFID tags. The scenario provides six bistatic ranges, i.e. the distances from TX antenna via tag under test to RX antenna. 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 [75]. However, more complex methods need to be used for multiple bistatic range estimations, such as target tracking based on probability hypothesis density [76].

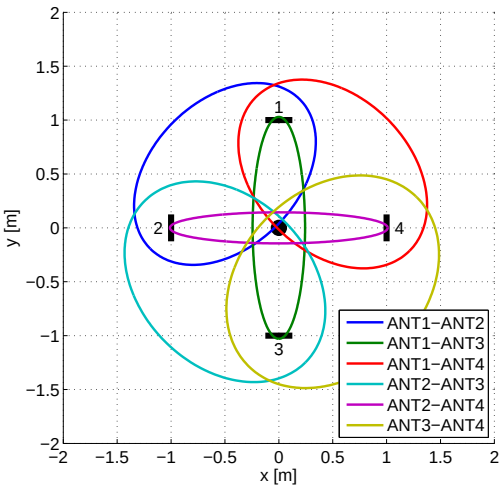
The positioning results for three selected tag positions are shown in Fig. 5.11. Each ellipse is defined by its foci corresponding to the positions of TX and RX antennas and the major radius resulting from the measured distance. For example, the blue ellipse in Fig. 5.11(a) with TX antenna at $\vec{p}_1(x_1, y_1)$, RX antenna at $\vec{p}_2(x_2, y_2)$, and bistatic range d is defined as:

$$\begin{aligned} a &= d/2 \\ b &= \sqrt{a^2 - \Big((x_2 - x_1)^2 + (y_2 - y_1)^2\Big)/2} \\ \alpha &= \arctan\left(\frac{y_2 - y_1}{x_2 - x_1}\right) \\ x_0 &= (x_1 + x_2)/2 \\ y_0 &= (y_1 + y_2)/2 \end{aligned} \tag{5.6}$$

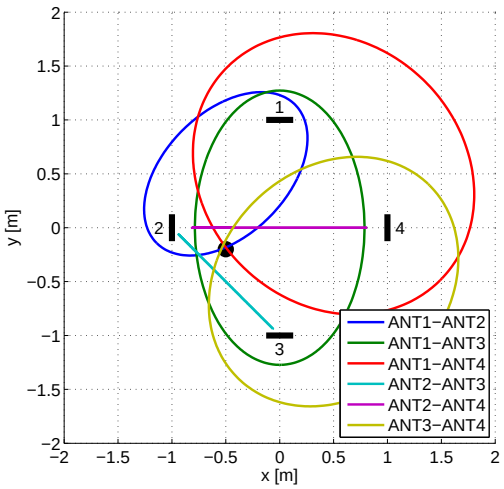
where a and b are the semimajor and semiminor axis lengths, α is the angle between the semimajor axis and the x-axis, and $\vec{p}_0(x_0, y_0)$ are the ellipse center coordinates.



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



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



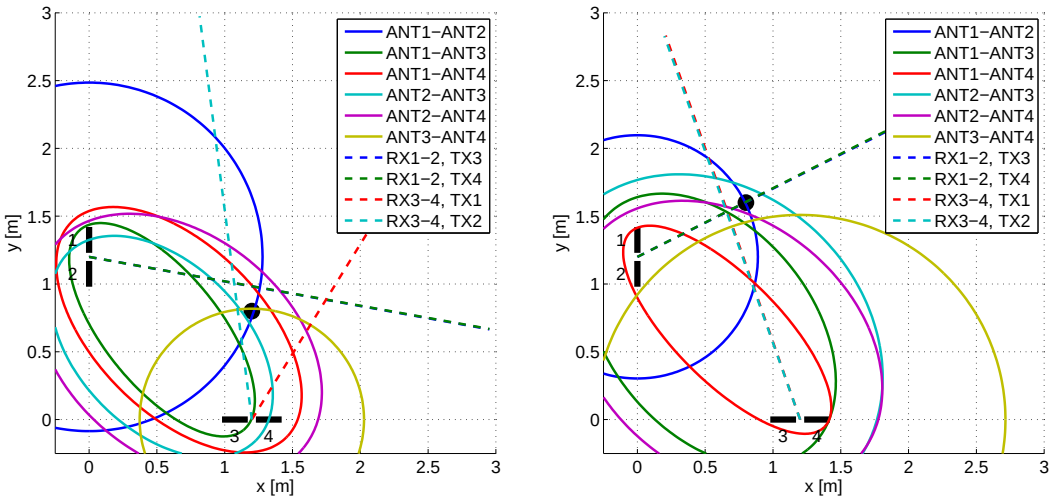
(c) Tag placed at $x = -0.5$ m, $y = -0.2$ m

Fig. 5.11: Multipoint bistatic range ellipses, scenario A

5.4.2 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.

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. 5.12 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. 5.12: 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. Parts of this overview have been published in [5, 6, 7].

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 [8, 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 [1].

Chapter 4 introduced software defined radio (SDR) concept and its adaptation to UHF RFID systems. The requirements on SDR architecture, published in [2], led to the design of two measurement systems. The experimental interrogator EXIN-1 (see Fig. B.1, published in [9, 10]) 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 [3, 11]. 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 (see Fig. B.2, described in [4]). 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 (see Fig. B.3), 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 2.5 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.

OWN PUBLICATIONS

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] A. Povalač, "Prostorová identifikace RFID etiket v pásmu UHF," in *Pokročilé metody, struktury a komponenty elektronické bezdrátové komunikace, GAČR 102/08/H027 v roce 2009*, pp. 80–83, November 2009.

[6] A. Povalač, M. Zamazal, and J. Šebesta, "Architectures for UHF RFID systems with tag ranging and localization," in *4th MC Meeting and Workshop of the COST IC0803*, pp. 1–3, February 2010.

[7] A. Povalač, "RFID ranging methods and positioning techniques," in *9th International Conference Vsacký Cáb 2011*, pp. 109–112, August 2011.

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

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

[10] A. Povalač, "Měření vzdálenosti UHF RFID tagů s využitím fáze přijatého signálu," in *Pokročilé metody, struktury a komponenty elektronické bezdrátové komunikace, GAČR 102/08/H027 v roce 2010*, pp. 82–85, November 2010.

[11] A. Povalač, "Využití FD-PDoA metody pro lokalizaci UHF RFID tagů v bezodrazové komoře," in *Pokročilé metody, struktury a komponenty elektronické bezdrátové komunikace, GAČR 102/08/H027 v roce 2011*, pp. 85–88, November 2011.

[12] A. Povalač, M. Zamazal, and J. Šebesta, "Firmware design for a multi protocol UHF RFID reader," in *Proceedings of the International Conference Radioelektronika 2010*, pp. 1–4, April 2010.

REFERENCES

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

[14] K. Finkenzeller, *RFID handbook: Fundamentals and applications*. Chichester: John Wiley & Sons, 2010.

[15] 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.

[16] 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].

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

[18] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, III, R. L. Moses, and N. S. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 22, pp. 54–69, July 2005.

[19] 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.

[20] 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.

[21] M. Alotaibi, K. S. Bialkowski, and A. Postula, "A signal strength based tag estimation technique for RFID systems," in *Proceedings of the IEEE International Conference on RFID-Technology and Applications, RFID-TA 2010*, pp. 251–256, 2010.

[22] Y. Huang, P. V. Brennan, and A. Seeds, "Active RFID location system based on time-difference measurement using a linear FM chirp tag signal," in *Proceedings of the IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2008*, pp. 1–5, September 2008.

[23] 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.

[24] 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.

[25] C. Hekimian-Williams, B. Grant, X. Liu, Z. Zhang, and P. Kumar, "Accurate localization of RFID tags using phase difference," in *Proceedings of the IEEE International Conference on RFID 2010*, pp. 89–96, April 2010.

[26] R. Mittra and U. Pujare, "Real time estimation of motion and range of RFID tags," in *Proceedings of the 5th European Conference on Antennas and Propagation 2011*, pp. 3804–3808, April 2011.

[27] 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.

[28] J. Heidrich, D. Brenk, J. Essel, G. Fischer, R. Weigel, and S. Schwarzer, "Local positioning with passive UHF RFID transponders," in *Proceedings of the IEEE MTT-S International Microwave Workshop on Wireless Sensing, Local Positioning, and RFID, IMWS 2009.*, pp. 1–4, September 2009.

[29] 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.

[30] A. Almaaitah, K. Ali, H. S. Hassanein, and M. Ibnkahla, "3D passive tag localization schemes for indoor RFID applications," in *Proceedings of the IEEE International Conference on Communications, ICC 2010*, pp. 1–5, May 2010.

[31] G. Hislop, D. Lekime, M. Drouguet, and C. Craeye, "A prototype 2D direction finding system with passive RFID tags," in *Proceedings of the Fourth European Conference on Antennas and Propagation, EuCAP 2010*, pp. 1–5, April 2010.

[32] 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.

[33] M. Bouet and A. L. Dos Santos, "RFID tags: Positioning principles and localization techniques," in *Proceedings of 1st IFIP Wireless Days, WD 2008*, pp. 1–5, November 2008.

[34] R. Miesen, R. Ebelt, F. Kirsch, T. Schafer, G. Li, H. Wang, and M. Vossiek, "Where is the tag?," *IEEE Microwave Magazine*, vol. 12, pp. S49–S63, December 2011.

[35] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "LANDMARC: Indoor location sensing using active RFID," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications, PerCom 2003*, pp. 407–415, 2003.

[36] T. Shiraishi, N. Komuro, H. Ueda, H. Kasai, and T. Tsuboi, "Indoor location estimation technique using UHF band RFID," in *Proceedings of the International Conference on Information Networking, ICOIN 2008*, pp. 1–5, 2008.

[37] T. Hori, T. Wda, Y. Ota, N. Uchitomi, K. Mutsuura, and H. Okada, "A multi-sensing-range method for position estimation of passive RFID tags," in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WIMOB 2008*, pp. 208–213, 2008.

[38] A. F. C. Errington, B. L. F. Daku, and A. F. Prugger, "Initial position estimation using RFID tags: A least-squares approach," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 2863–2869, 2010.

[39] V. Derbek, J. Preishuber-Pfluegl, C. Steger, and M. Pistauer, "Architecture for model-based UHF RFID system design verification," in *European Conference on Circuit Theory and Design (ECCTD05)*, vol. 2, pp. 181–184, September 2005.

[40] C. Floerkemeier and R. Pappu, "Evaluation of RFIDSim – a physical and logical layer RFID simulation engine," in *Proceedings of the IEEE International Conference on RFID 2008*, pp. 350–356, April 2008.

[41] A. G. Dimitriou, A. Bletsas, A. C. Polycarpou, and J. N. Sahalos, "Theoretical findings and measurements on planning a UHF RFID system inside a room," *Radioengineering*, vol. 20, pp. 387–397, June 2011.

[42] D. Arnitz, U. Muehlmann, T. Gigl, and K. Witrisal, "Wideband system-level simulator for passive UHF RFID," in *Proceedings of the IEEE International Conference on RFID 2009*, pp. 28–33, April 2009.

[43] 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.

[44] C. Angerer and R. Langwieser, "Flexible evaluation of RFID system parameters using rapid prototyping," in *Proceedings of the IEEE International Conference on RFID 2009*, pp. 42–47, April 2009.

[45] 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].

[46] M. Keaveney, J. Morrissey, P. Walsh, M. Tuthill, M. Chanca, I. Collins, and P. Hendriks, "A high performance RF front end for UHF RFID reader applications," in *IET Seminar on RF and Microwave IC Design*, pp. 1–7, 2008.

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

[48] 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.

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

[50] D. Arnitz, U. Muehlmann, and K. Witrisal, "Wideband characterization of backscatter channels," in *Proceedings of the 11th European Wireless Conference 2011 – Sustainable Wireless Technologies*, pp. 1–7, April 2011.

[51] 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.

[52] A. F. Molisch, *Wireless Communications*. Chichester: John Wiley & Sons, 2005.

[53] 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.

[54] T. Faseth, M. Winkler, H. Arthaber, and G. Magerl, "The influence of multipath propagation on phase-based narrowband positioning principles in UHF RFID," in *Proceedings of the IEEE-APS Topical Conference on Antennas and Propagation in Wireless Communications 2011*, pp. 1144–1147, September 2011.

[55] 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.

[56] S. Azzouzi, M. Cremer, U. Dettmar, T. Knie, and R. Kronberger, "Improved AoA based localization of UHF RFID tags using spatial diversity," in *Proceedings of the IEEE International Conference on RFID-Technology and Applications, RFID-TA 2011*, pp. 174–180, September 2011.

[57] R. Kronberger, T. Knie, R. Leonardi, U. Dettmar, M. Cremer, and S. Azzouzi, "UHF RFID localization system based on a phased array antenna," in *Proceedings of the IEEE International Symposium on Antennas and Propagation 2011*, pp. 525–528, July 2011.

[58] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, pp. 276–280, March 1986.

[59] Emerson & Cuming Anechoic Chambers NV, *ECCOSORB® VHY-NRL Pyramidal Hybrid Absorber (datasheet)*, 2010.

[60] P. B. Kenington, *RF and Baseband Techniques for Software Defined Radio*. Norwood, MA (USA): Artech House, 2005.

[61] Poynting Antennas Ltd., *PATCH-A0025: RFID Patch Antenna, 860 – 960 MHz, Circular Polarization (datasheet)*, 2005.

[62] *ETSI EN 302 208: Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W*, 2007.

[63] Federal Commonications Commission, *§ 15.247: Operation within the bands 902—928 MHz, 2400—2483.5 MHz, and 5725-–5850 MHz*, 2010.

[64] *ISO/IEC 18000-6:2010. Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz*, 2010.

[65] EM Microelectronic-Marin SA, *EM4122: Read-only UHF RFID IC (datasheet)*, 2005.

[66] METRA BLANSKO a.s., *RFI21.1: UHF RFID Compact Reader (datasheet)*, 2011. Available: `<http://www.metra.cz/files/rfid/rfi21.1/datasheet_RFI21_1_110204_en.pdf>` [cit. 2012-07-25].

[67] Analog Devices Inc., *ADF9010: 900 MHz ISM band analog RF front end (datasheet)*, 2008.

[68] Analog Devices Inc., *ADF9010-EVAL: Evaluation Board for ADF9010 RF Front End (datasheet)*, 2009. Available: `<http://www.analog.com/static/imported-files/eval_boards/EVAL-ADF9010.pdf>` [cit. 2011-02-15].

[69] Ettus Research, *USRP™ N200/N210 Networked Series (datasheet)*, 2012. Available: <https://www.ettus.com/product/details/UN200-KIT> [cit. 2012-07-25].

[70] S. Sarkka, V. Viikari, M. Huusko, and K. Jaakkola, "Phase-based UHF RFID tracking with non-linear Kalman filtering and smoothing," *IEEE Sensors Journal*, vol. PP, no. 99, pp. 1–7, 2011.

[71] A. V. Oppenheim, R. W. Schafer, and J. R. Buck, *Discrete time signal processing*, pp. 633–635. Upper Saddle River, NJ: Prentice Hall, 1999.

[72] 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.

[73] 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].

[74] C. A. Balanis, *Antenna Theory: Analysis and Design*. Chichester: John Wiley & Sons, 2nd ed., 1997.

[75] D. Eberly, "Intersection of ellipses." [Online], 2010. Available: <http://www.geometrictools.com/Documentation/IntersectionOfEllipses.pdf> [cit. 2011-04-10].

[76] 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.

LIST OF ABBREVIATIONS

AM	amplitude modulation
ANT	antenna
AoA	angle of arrival
APS	angle power spectrum
ASK	amplitude shift keying
BB	baseband
BLF	backscatter link frequency
BPF	band-pass filter
CIR	channel impulse response
CRC	cyclic redundancy check
CTF	channel transfer function
CW	continuous-wave
DLL	dynamic-link library
DoA	direction of arrival
DREL	Department of Radio Electronics
FD-PDoA	frequency domain phase difference of arrival
FFT	fast Fourier transform
FMCW	frequency modulated continuous wave
FPGA	field programmable gate array
FSK	frequency shift keying
GDB	grand-daughterboard
I/Q	in-phase/quadrature
IC	integrated circuit
IF	immediate frequency
IFFT	inverse fast Fourier transform
kNN	k-nearest-neighbor
LAN	local area network
LFM	linear frequency modulation
LNA	low noise amplifier
LO	local oscillator
LOS	line-of-sight
LPF	low-pass filter
NLOS	non-line-of-sight
PCB	printed circuit board
PDoA	phase difference of arrival
PDP	power delay profile
PLL	phase-locked loop
PoA	phase of arrival
RF	radio frequency
RFID	radio-frequency identification

RMS	root mean square
RSS	received signal strength
RTF	reader talks first
RX	receiver, receiving
SAR	synthetic aperture radar
SD-PDoA	spatial domain phase difference of arrival
SDR	software defined radio
SFDR	spurious-free dynamic range
SIMO	single-input multiple-output
SWR	standing wave ratio
TCXO	temperature compensated crystal oscillator
TD-PDoA	time domain phase difference of arrival
ToA	time of arrival
ToF	time of flight
TOTAL	tag only talks after listening
TTF	tag talks first
TTO	tag talks only
TX	transmitter, transmitting
UHD	USRP hardware driver
UHF	ultra-high frequency band
USRP	universal software radio peripheral
UWB	ultra-wideband
VCO	voltage controlled oscillator
VGA	variable gain amplifier

LIST OF FIGURES

LIST OF TABLES

A CHANNEL SIMULATION RESULTS

A.1 Free Space Model

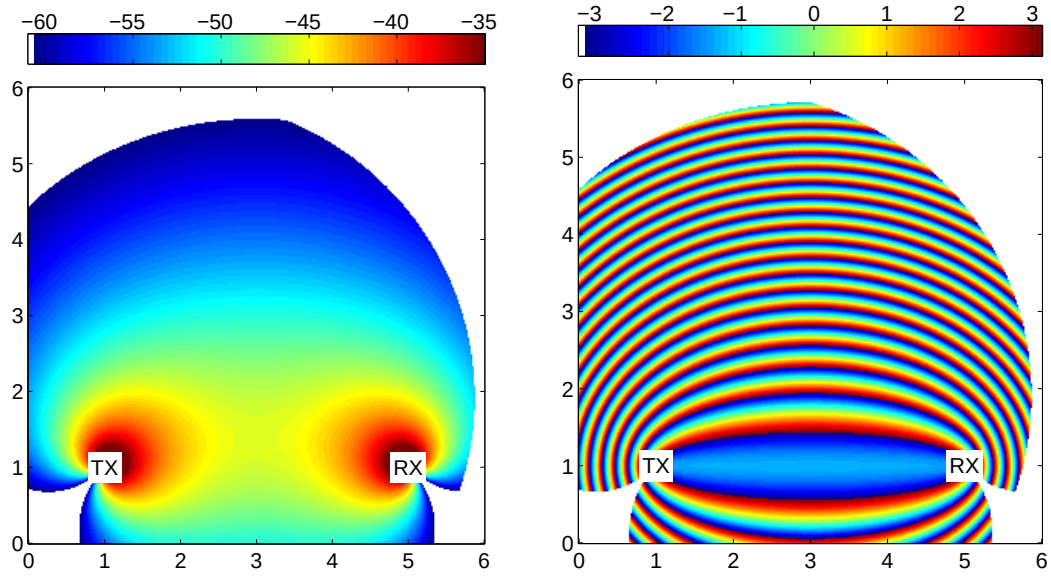
Free space provides an idealized direct LOS propagation with no multipath. The anechoic RF chamber can be considered as an example of such environment. Simulation is based on LOS propagation only, resulting in a Gaussian degenerate channel. Noise is not considered. Both amplitude and phase of received signal are ideally distributed. There is a strong peak in the CIR, representing the range estimation. Moreover, this channel is practically frequency independent even in a wide band scope.

A.1.1 Simulation Parameters

```
%% reader and tag parameters
P_TX = 0.5; % watt
tag_K = 0.1*exp(j*0);

%% RX and TX antennas as [x y z angle]
src = [1 1 1 45];
dst = [5 1 1 135]; % dst = [0.75 1.25 1 45];

%% room dimensions in X, Y and Z axis
h = [6 6 3];

%% number of stochastic components and its standard deviation
stoch_count = 0;
stoch_sigma = 0;

%% list of reflections as [shiftX shiftY shiftZ reflX reflY reflZ ...
   Gamma]
reflect = [];
```

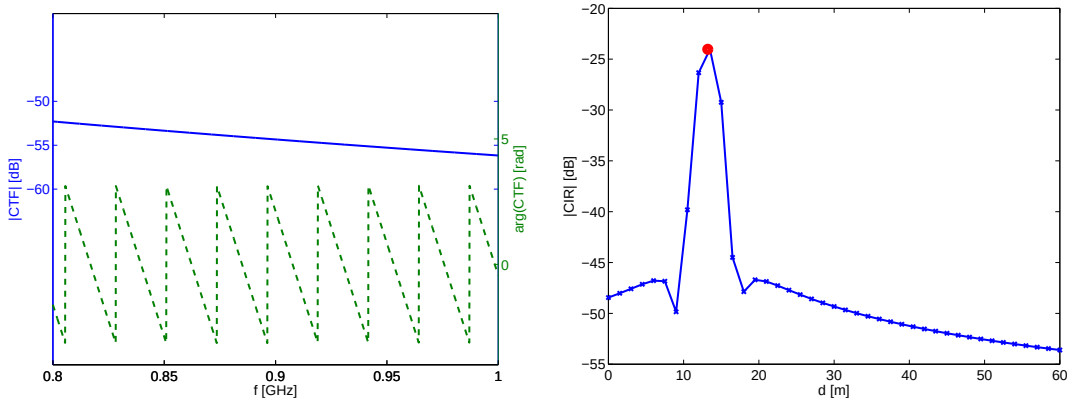
A.1.2 Simulation Results

```
%% dst = [5 1 1 135];
real_distance = 7.2118
measured_fft = 7.5000
measured_groupdelay = 7.2118

%% dst = [0.75 1.25 1 45];
real_distance = 7.1594
measured_fft = 7.5000
measured_groupdelay = 7.1594
```



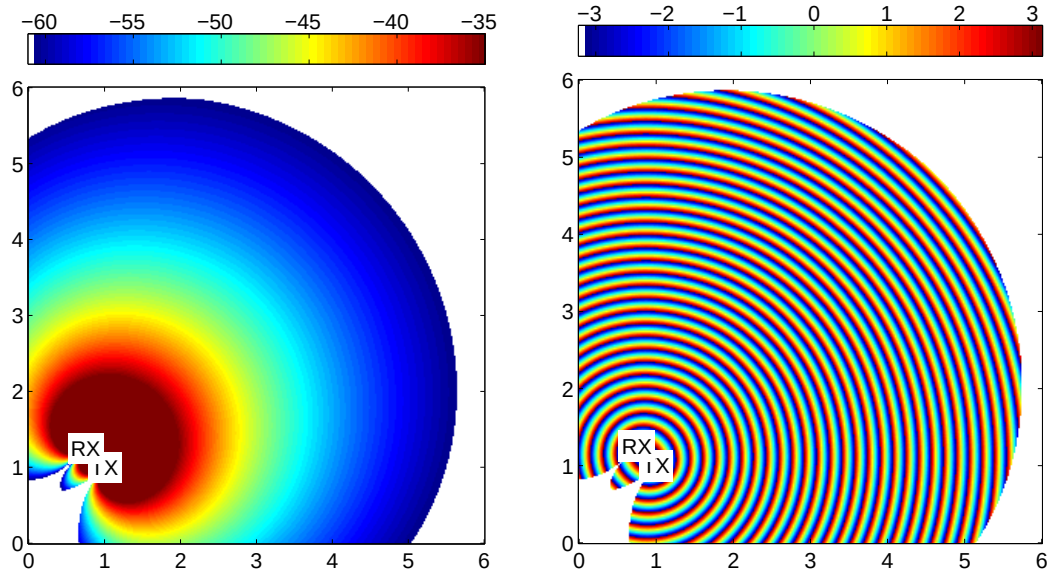
(a) Amplitude of received tag signal [dBm] (b) Phase of received tag signal [rad]

Fig. A.1: Free space model, scenario "Distance only".
Tag position $\vec{p}_{tag} = [x, y, 0.95]$ m is swept over x and y dimensions, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [5, 1, 1]$ m heading 135°, $P_{TX} = 0.5$ W, $f = 915$ MHz.



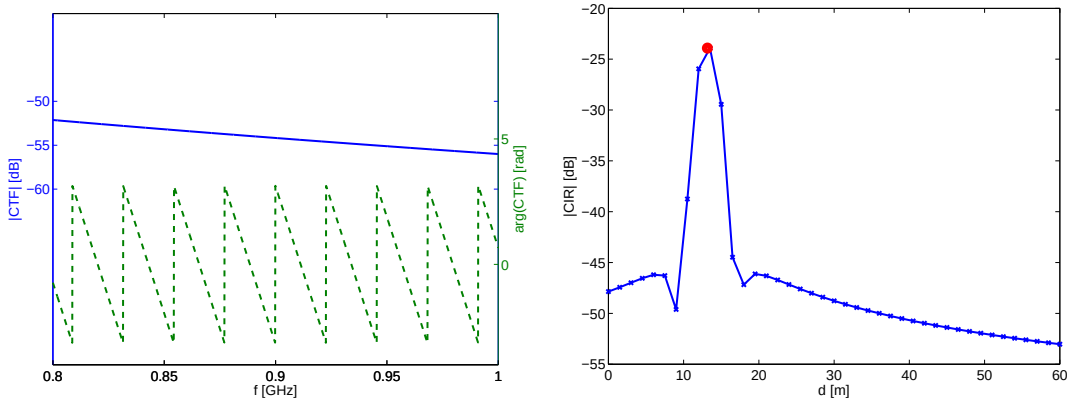
(a) Channel transfer function (b) Channel impulse response

Fig. A.2: Free space model, scenario "Distance only".
Frequency is swept from 800 to 1000 MHz, tag position $\vec{p}_{tag} = [3, 4, 0.95]$ m, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [5, 1, 1]$ m heading 135°, $P_{TX} = 0.5$ W.



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

Fig. A.3: Free space model, scenario "Distance and direction".
Tag position $\vec{p}_{tag} = [x, y, 0.95]$ m is swept over x and y dimensions, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [0.75, 1.25, 1]$ m heading 45°, $P_{TX} = 0.5$ W, $f = 915$ MHz.



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

Fig. A.4: Free space model, scenario "Distance and direction".
Frequency is swept from 800 to 1000 MHz, tag position $\vec{p}_{tag} = [3, 4, 0.95]$ m, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [0.75, 1.25, 1]$ m heading 45°, $P_{TX} = 0.5$ W.

A.2 Two-ray Deterministic Model

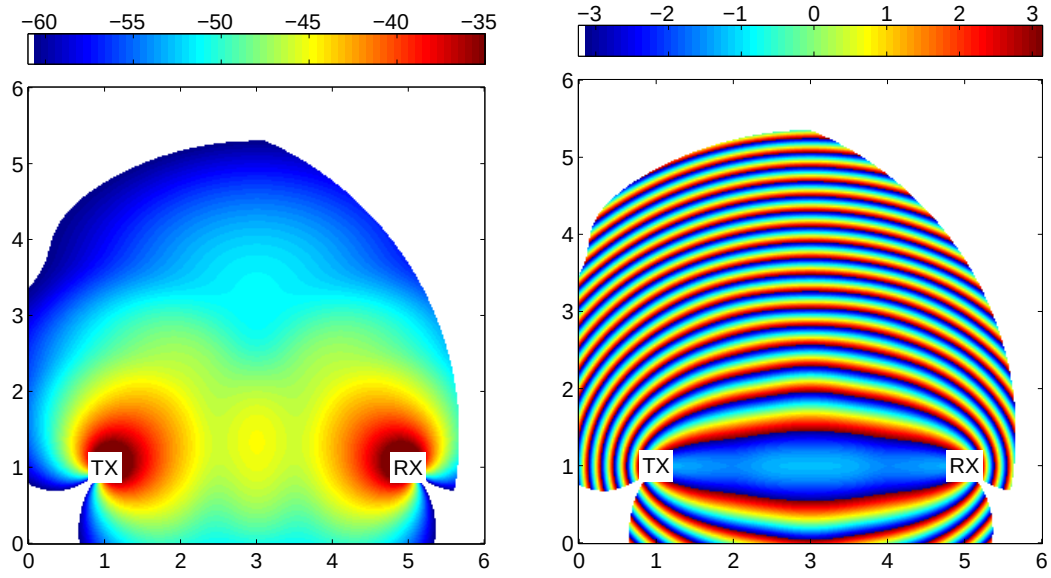
Two-ray deterministic model adds a ground (floor) reflection into previous setup with direct ray. Such model can be used to estimate the ranging performance in places like a building roof, large open spaces, etc. The results are very similar to the first scenario. There is a small distortion in the amplitude of received signal, the phase is not affected. Strong range peak in the CIR is clearly visible.

A.2.1 Simulation Parameters

```
%% reader and tag parameters
P_TX = 0.5; % watt
tag_K = 0.1*exp(j*0);
Gamma = -0.7;

%% RX and TX antennas as [x y z angle]
src = [1 1 1 45];
dst = [5 1 1 135]; % dst = [0.75 1.25 1 45];

%% room dimensions in X, Y and Z axis
h = [6 6 3];

%% number of stochastic components and its standard deviation
stoch_count = 0;
stoch_sigma = 0;

%% list of reflections as [shiftX shiftY shiftZ reflX reflY reflZ ...
   Gamma]
reflect = [
    0      0      0       1  1 -1  Gamma;  % floor reflection
];
```

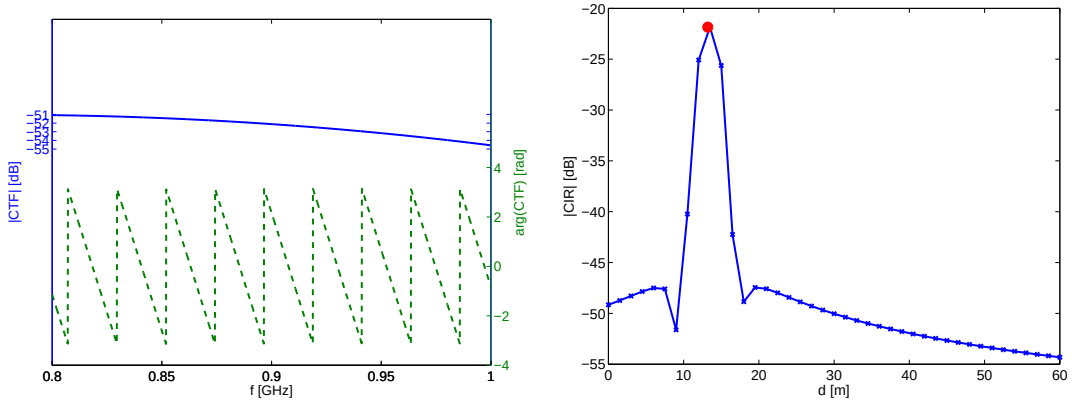
A.2.2 Simulation Results

```
%% dst = [5 1 1 135];
real_distance = 7.2118
measured_fft = 7.5000
measured_groupdelay = 7.4165

%% dst = [0.75 1.25 1 45];
real_distance = 7.1594
measured_fft = 7.5000
measured_groupdelay = 7.3640
```



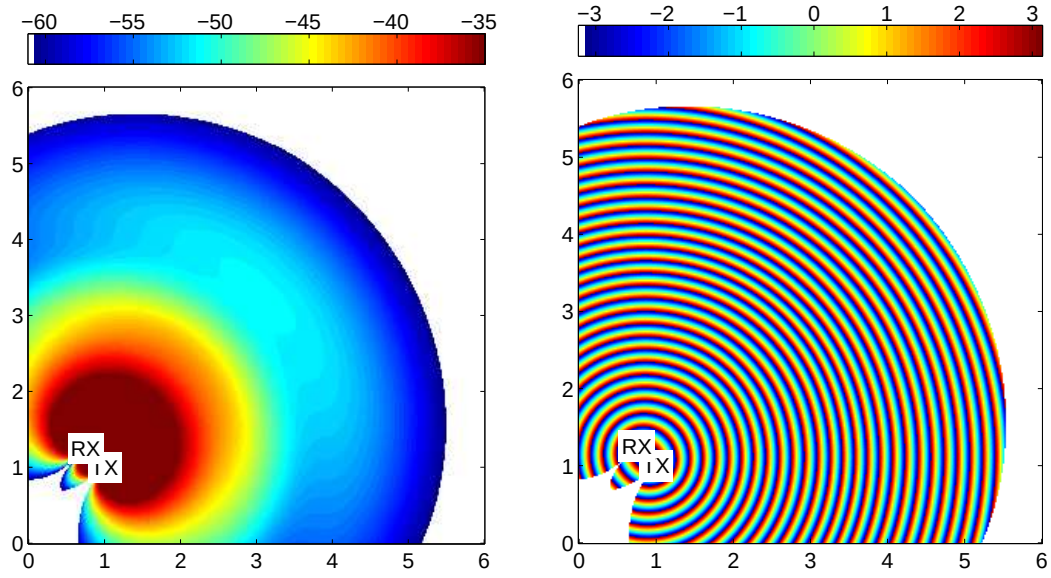
(a) Amplitude of received tag signal [dBm] (b) Phase of received tag signal [rad]

Fig. A.5: Two-ray deterministic model, scenario "Distance only".
Tag position $\vec{p}_{tag} = [x, y, 0.95]$ m is swept over x and y dimensions, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [5, 1, 1]$ m heading 135°, $P_{TX} = 0.5$ W, $f = 915$ MHz.



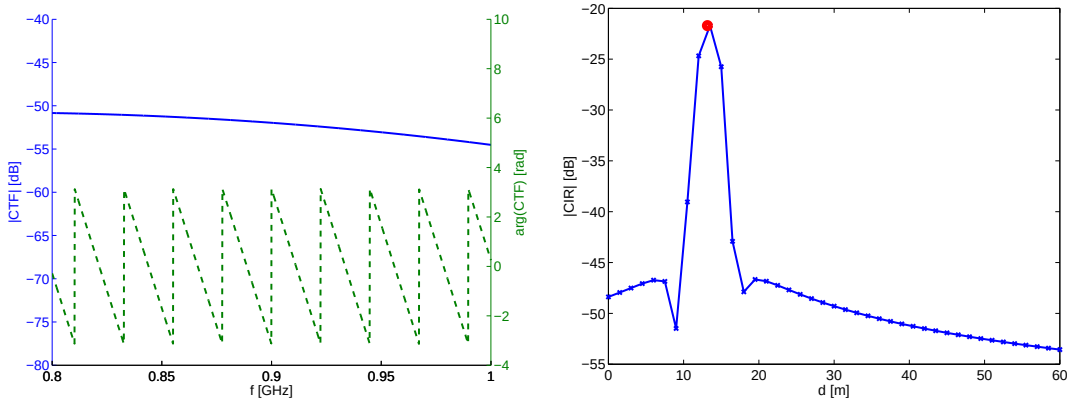
(a) Channel transfer function (b) Channel impulse response

Fig. A.6: Two-ray deterministic model, scenario "Distance only".
Frequency is swept from 800 to 1000 MHz, tag position $\vec{p}_{tag} = [3, 4, 0.95]$ m, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [5, 1, 1]$ m heading 135°, $P_{TX} = 0.5$ W.



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

Fig. A.7: Two-ray deterministic model, scenario "Distance and direction". Tag position $\vec{p}_{tag} = [x, y, 0.95]$ m is swept over x and y dimensions, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [0.75, 1.25, 1]$ m heading 45°, $P_{TX} = 0.5$ W, $f = 915$ MHz.



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

Fig. A.8: Two-ray deterministic model, scenario "Distance and direction". Frequency is swept from 800 to 1000 MHz, tag position $\vec{p}_{tag} = [3, 4, 0.95]$ m, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [0.75, 1.25, 1]$ m heading 45°, $P_{TX} = 0.5$ W.

A.3 Multi-ray Deterministic Model

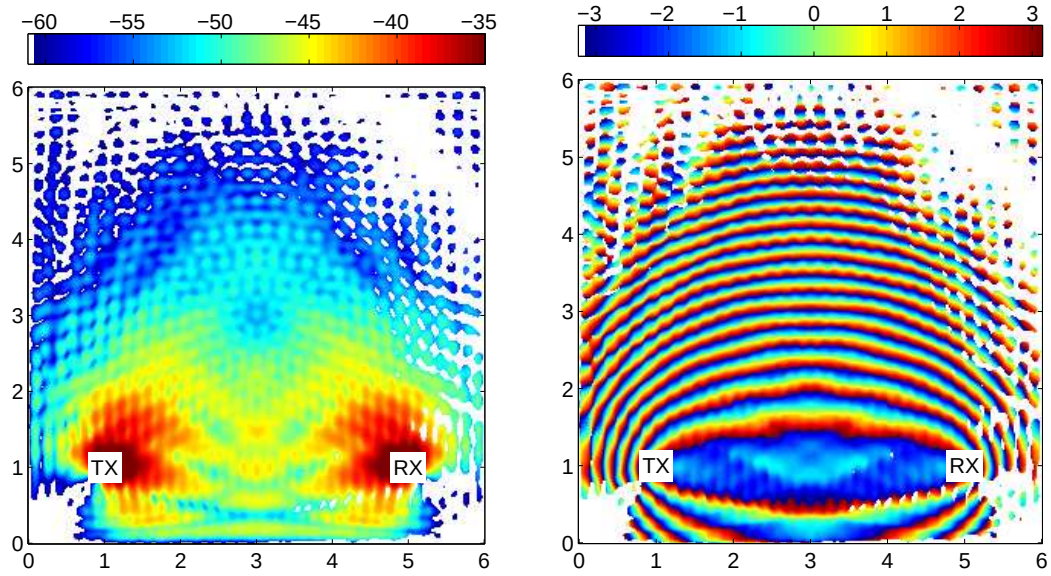
Multi-ray model consists of a large number of deterministic rays added to the direct path. The rays are created by the reflection from all the walls, floor and ceiling. Only the first and the second order reflections are considered. Such model approximates an ideal room. It can be seen that the amplitude distribution is strongly affected, especially near the reflecting walls. On the other hand, the phase distribution in short range is still very clear. Range peak in the CIR is clearly visible.

A.3.1 Simulation Parameters

```
%% reader and tag parameters
P_TX = 0.5; % watt
tag_K = 0.1*exp(j*0);
Gamma = -0.7;

%% RX and TX antennas as [x y z angle]
src = [1 1 1 45];
dst = [5 1 1 135]; % dst = [0.75 1.25 1 45];

%% room dimensions in X, Y and Z axis
h = [6 6 3];

%% number of stochastic components and its standard deviation
stoch_count = 0;
stoch_sigma = 0;

%% list of reflections as [shiftX shiftY shiftZ reflX reflY reflZ ...
   Gamma]
reflect = [
    0      0      0       1  1 -1  Gamma;  % floor reflection
    0      0      2*h(3)  1  1 -1  Gamma;  % ceiling reflection
    0      0      0       1 -1  1  Gamma;  % wall X-bottom reflection
    0      2*h(2) 0       1 -1  1  Gamma;  % wall X-top reflection
    0      0      0      -1  1  1  Gamma;  % wall Y-left reflection
    2*h(1) 0      0      -1  1  1  Gamma;  % wall Y-right reflection
];
```

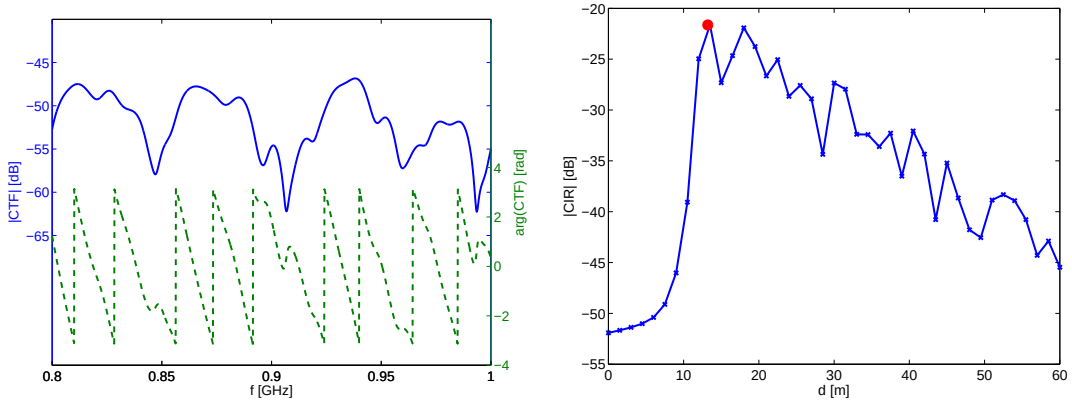
A.3.2 Simulation Results

```
%% dst = [5 1 1 135];
real_distance = 7.2118
measured_fft = 7.5000
measured_groupdelay = 7.7067

%% dst = [0.75 1.25 1 45];
real_distance = 7.1594
measured_fft = 7.5000
measured_groupdelay = 7.2166
```



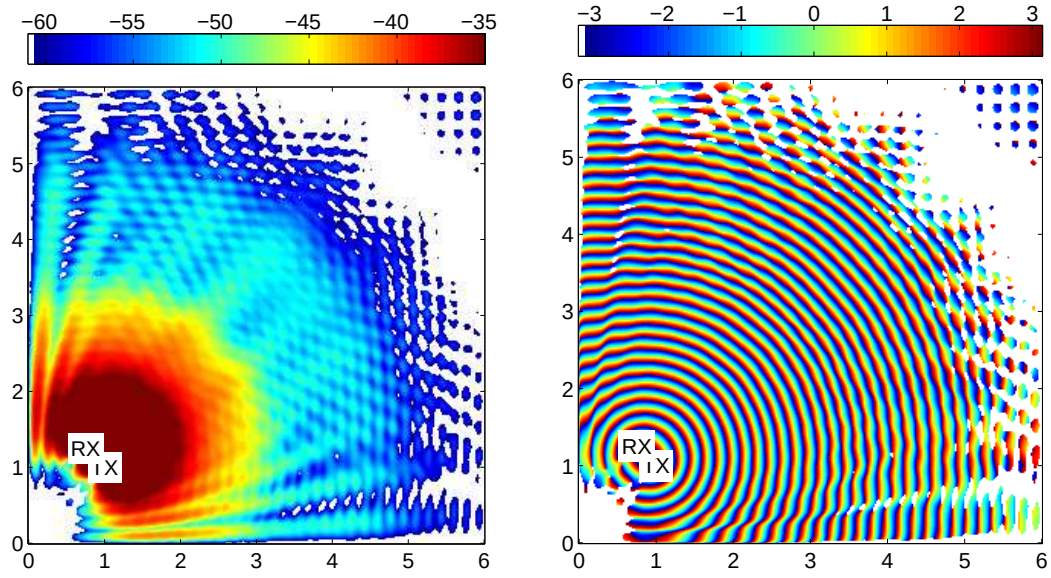
(a) Amplitude of received tag signal [dBm] (b) Phase of received tag signal [rad]

Fig. A.9: Multi-ray deterministic model, scenario "Distance only".
Tag position $\vec{p}_{tag} = [x, y, 0.95]$ m is swept over x and y dimensions, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [5, 1, 1]$ m heading 135°, $P_{TX} = 0.5$ W, $f = 915$ MHz.



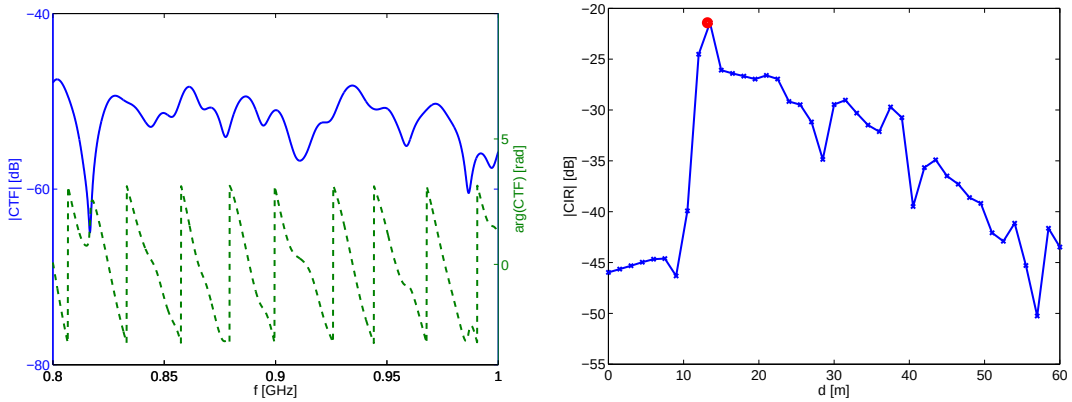
(a) Channel transfer function (b) Channel impulse response

Fig. A.10: Multi-ray deterministic model, scenario "Distance only".
Frequency is swept from 800 to 1000 MHz, tag position $\vec{p}_{tag} = [3, 4, 0.95]$ m, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [5, 1, 1]$ m heading 135°, $P_{TX} = 0.5$ W.



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

Fig. A.11: Multi-ray deterministic model, scenario "Distance and direction". Tag position $\vec{p}_{tag} = [x, y, 0.95]$ m is swept over x and y dimensions, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [0.75, 1.25, 1]$ m heading 45°, $P_{TX} = 0.5$ W, $f = 915$ MHz.



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

Fig. A.12: Multi-ray deterministic model, scenario "Distance and direction". Frequency is swept from 800 to 1000 MHz, tag position $\vec{p}_{tag} = [3, 4, 0.95]$ m, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [0.75, 1.25, 1]$ m heading 45°, $P_{TX} = 0.5$ W.

A.4 Combined Model

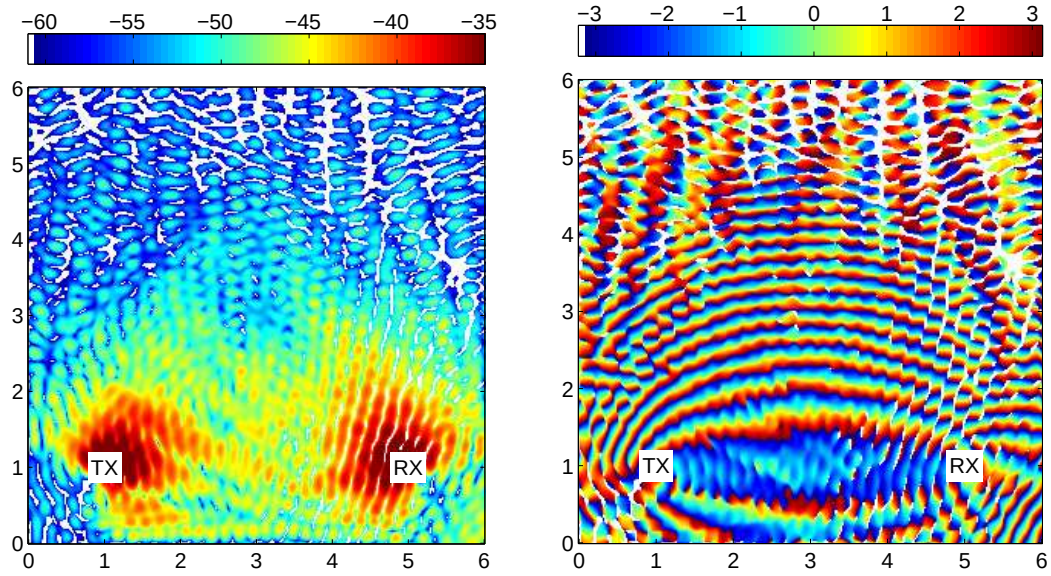
Combined model adds stochastic components into previous multi-ray simulation. It is an example of an actual room with small obstacles. Stochastic components are modeled using 40 signal sources with a random position outside the room and a Rayleigh distributed power. Both amplitude and phase of received signal are affected by multipath. The tag power-on threshold causes random behavior at longer distances. Range peak in the CIR can be found only if the measurement bandwidth is wide enough.

A.4.1 Simulation Parameters

```
%% reader and tag parameters
P_TX = 0.5; % watt
tag_K = 0.1*exp(j*0);
Gamma = -0.7;

%% RX and TX antennas as [x y z angle]
src = [1 1 1 45];
dst = [5 1 1 135]; % dst = [0.75 1.25 1 45];

%% room dimensions in X, Y and Z axis
h = [6 6 3];

%% number of stochastic components and its standard deviation
stoch_count = 40;
stoch_sigma = 1.5;

%% list of reflections as [shiftX shiftY shiftZ reflX reflY reflZ ...
   Gamma]
reflect = [
    0      0      0       1  1 -1  Gamma;  % floor reflection
    0      0      2*h(3)  1  1 -1  Gamma;  % ceiling reflection
    0      0      0       1 -1  1  Gamma;  % wall X-bottom reflection
    0      2*h(2) 0       1 -1  1  Gamma;  % wall X-top reflection
    0      0      0      -1  1  1  Gamma;  % wall Y-left reflection
    2*h(1) 0      0      -1  1  1  Gamma;  % wall Y-right reflection
];
```

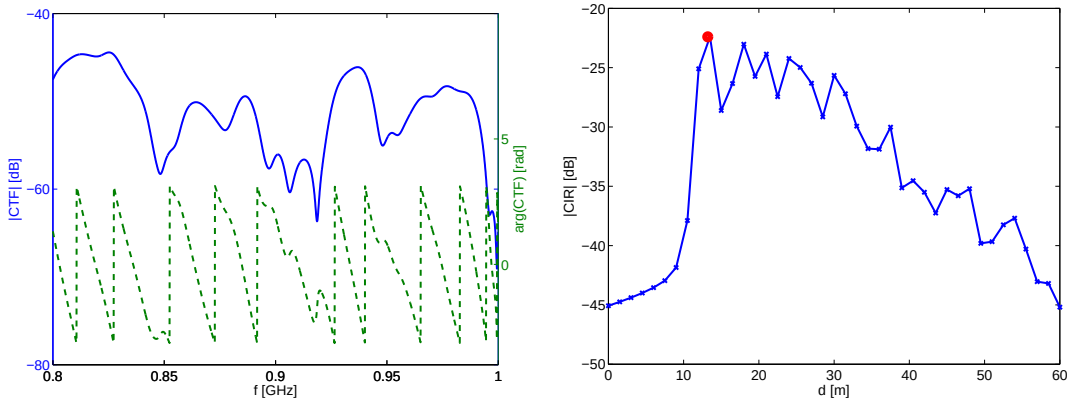
A.4.2 Simulation Results

```
%% dst = [5 1 1 135];
real_distance = 7.2118
measured_fft = 7.5000
measured_groupdelay = 10.3996

%% dst = [0.75 1.25 1 45];
real_distance = 7.1594
measured_fft = 7.5000
measured_groupdelay = 9.9052
```



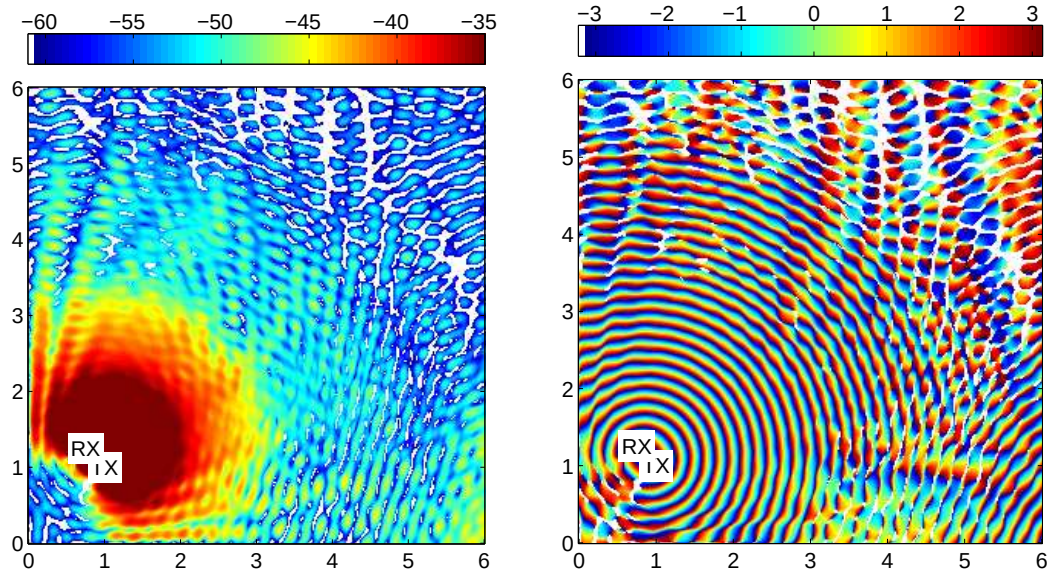
(a) Amplitude of received tag signal [dBm] (b) Phase of received tag signal [rad]

Fig. A.13: Combined model simulation, scenario "Distance only".
Tag position $\vec{p}_{tag} = [x, y, 0.95]$ m is swept over x and y dimensions, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [5, 1, 1]$ m heading 135°, $P_{TX} = 0.5$ W, $f = 915$ MHz.



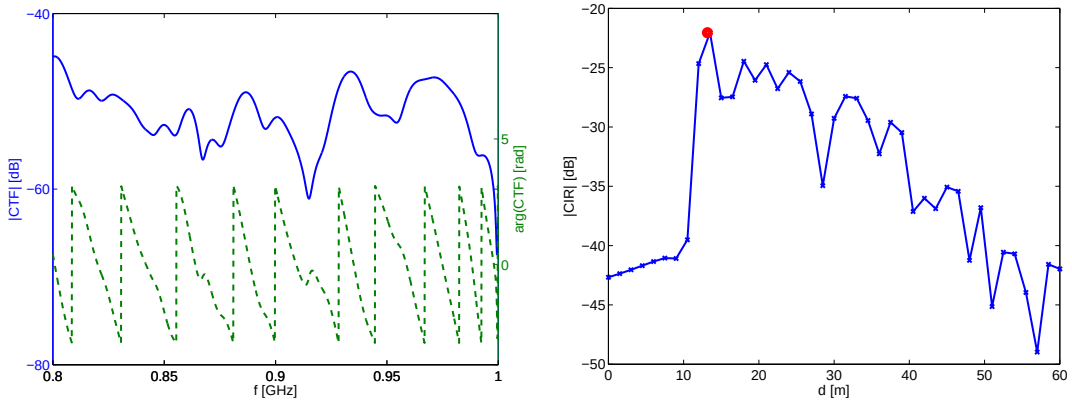
(a) Channel transfer function (b) Channel impulse response

Fig. A.14: Combined model simulation, scenario "Distance only".
Frequency is swept from 800 to 1000 MHz, tag position $\vec{p}_{tag} = [3, 4, 0.95]$ m, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [5, 1, 1]$ m heading 135°, $P_{TX} = 0.5$ W.



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

Fig. A.15: Combined model simulation, scenario "Distance and direction". Tag position $\vec{p}_{tag} = [x, y, 0.95]$ m is swept over x and y dimensions, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [0.75, 1.25, 1]$ m heading 45°, $P_{TX} = 0.5$ W, $f = 915$ MHz.



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

Fig. A.16: Combined model simulation, scenario "Distance and direction". Frequency is swept from 800 to 1000 MHz, tag position $\vec{p}_{tag} = [3, 4, 0.95]$ m, antennas at $\vec{p}_{TX} = [1, 1, 1]$ m heading 45°, $\vec{p}_{RX} = [0.75, 1.25, 1]$ m heading 45°, $P_{TX} = 0.5$ W.

B PHOTOS OF MEASUREMENT SYSTEMS

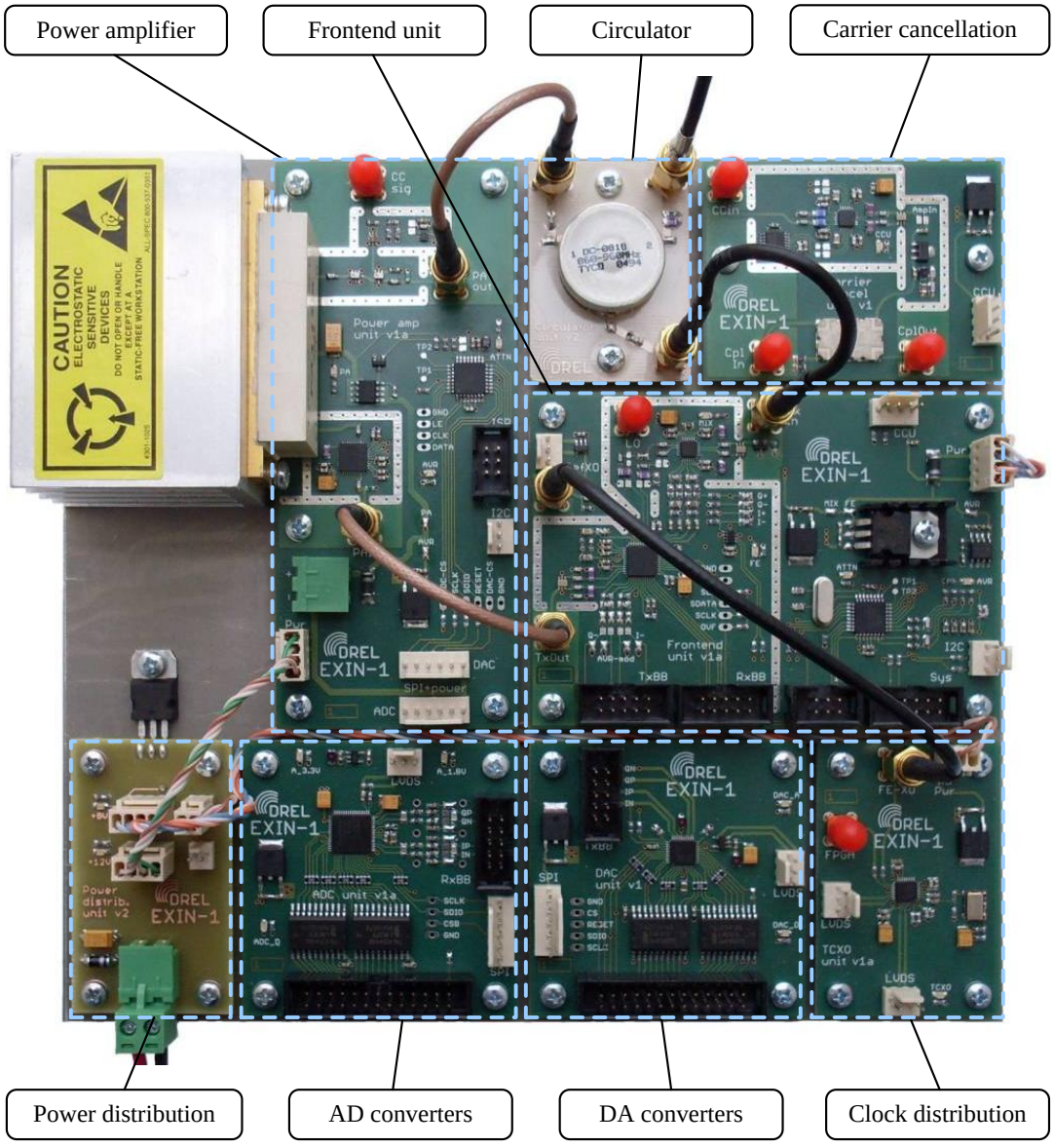


Fig. B.1: Testbed with the experimental UHF RFID front end

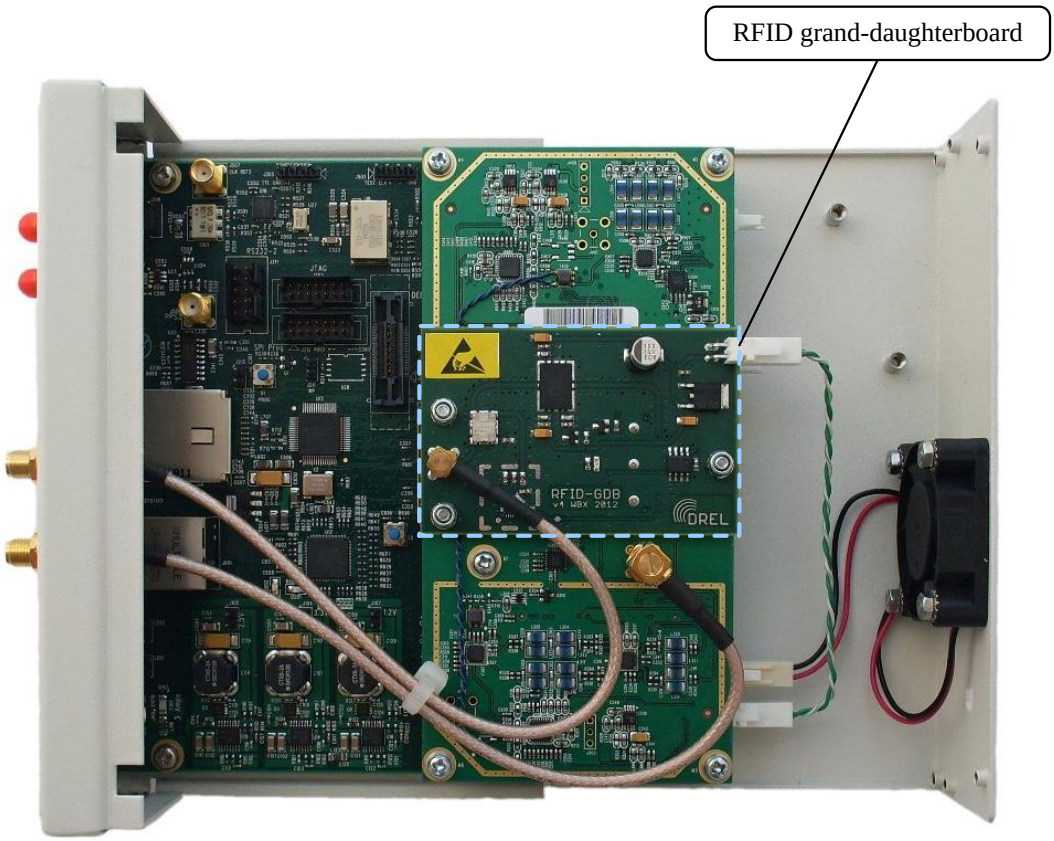


Fig. B.2: Measurement system based on Ettus USRP N200

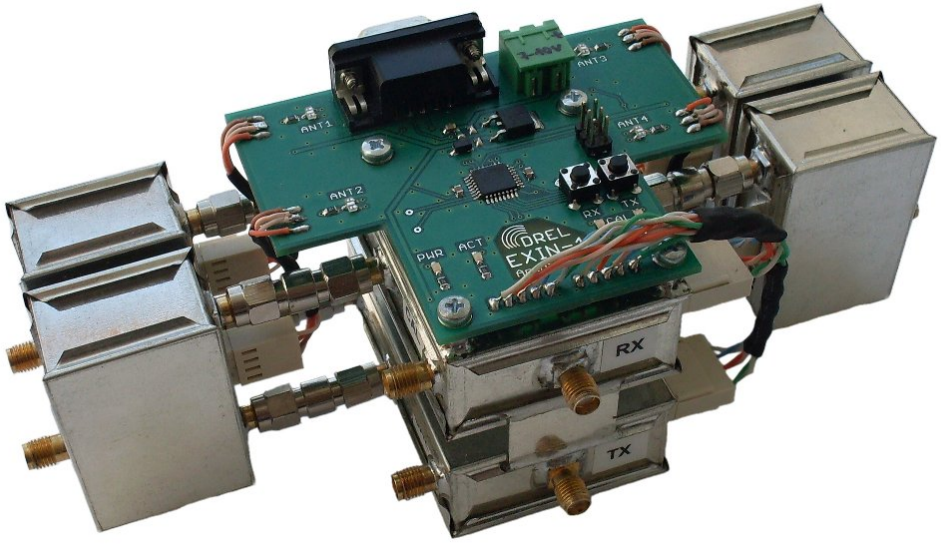


Fig. B.3: Antenna switching matrix

C 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)
Skills	Programming (Borland Delphi, Borland C++ Builder, MS Visual Studio, HTML, PHP, SQL – Firebird, Oracle), embedded systems programming in C (AVR, STM32, MCS51, HCS08), TCP/IP networking, Eagle PCB design, LaTeX typesetting, SVN versioning