Technical University of Crete, Greece

School of Electronic and Computer Engineering

SDR Readers for Gen2 RFID and Backscatter Sensor Networks

Nikolaos Kargas

Thesis Committee

Associate Professor Aggelos Bletsas (ECE)

Associate Professor George N. Karystinos (ECE)

Associate Professor Antonios Deligiannakis (ECE)

Chania, 2015

Abstract

Scatter radio has emerged as a key enabling technology for low-cost and large scale ubiquitous sensing. Radio frequency identification (RFID) tags/sensors utilize scatter radio technology to transfer sensed information to readers, typically employing Gen2, the industrial RFID protocol.

This work offers a complete software-defined radio Gen2 reader, based on GNU Radio and USRP2 commodity software defined radio (SDR) platform. In sharp contrast to prior art, a single radio front end card is used with coherent detection and optimal exploitation of the FM0 line coding memory. The reader can act as a research tool to experiment with state-of-the-art signal processing algorithms and RFID devices. The two tag collision problem is studied and problems that arise in a real world system, such as channel estimation and tag symbol synchronization are highlighted. Experimental measurements are conducted and it is shown that the reader can identify a commercial, passive UHF RFID tag up to 6 meters with acceptable reliability. In addition, it is shown that collision recovery algorithms can increase performance of the implemented reader.

Furthermore, an implementation of a SDR reader for a wireless backscatter sensor network (BSN) is presented. The developed reader implements noncoherent frequency shift keying (FSK) detection. The reader can decode multiple tags in real time and achieves communication ranges with semi-passive tags/sensors up to 130 meters.

Acknowledgements

First of all, I would like to thank my advisor Aggelos Bletsas, an excellent instructor and researcher, for his trust and guidance during this thesis. He has been a constant source of motivation.

I would also like to thank my thesis committee, professors Antonios Deligiannakis and George Karystinos who graciously agreed to serve on my committee.

Next, I would like to thank the members of the Telecommunications Laboratory for the valuable discussions and all the fun we had in the last two years.

Finally, I would like to thank my friends and family for their love, support and constant encouragement.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Scatter radio achieves communication by means of reflection. Although its principles date back in 1948 [1], it has recently been utilized in radio frequency identification (RFID) systems. RFID tags reflect a continuous carrier wave (CW) transmitted by a reader in order to modulate a constant bit sequence (ID). The reader receives the backscattered signal, identifying the tags by their unique ID. RFID technology is extensively used for supply chain monitoring and object tracking applications.

Recent advances in sensor technology have enabled the integration of low-cost sensors with RFID tags leading to the development of computational RFID (CRFID), i.e. battery-less sensors that backscatter sensed information, rather than a constant ID bit stream. The tags utilize Gen2, a communication protocol used in commercial RFID systems to transfer sensed information. Another prominent application of RFID technology is environmental monitoring. Work in [2] considers a wireless sensor network (WSN) based on a bistatic architecture with the deployment of semi-passive tags. Towards that direction, work in [3] develops noncoherent detectors for FSK and OOK modulations. In addition, coherent detection and channel coding for increased range bistatic architectures have been proposed in [4].

There has been a continuously growing interest on RFID and its applications. Commercial RFID readers are often used by researchers to study existing RFID protocols and new tag designs. However, these readers provide limited configuration and cannot be customized or enriched with new features. Considering the above, the development of flexible RFID reader platforms can further unlock the potential of RFID technology.

1.1 Thesis Contribution

The contribution of this thesis is summarized in the following bullets:

- Development a Gen2 RFID reader based on USRPN200 software defined radio (SDR) platform for ultra high frequency (UHF) RFID tags. The reader implements part of the commercial Gen2 protocol, performs coherent detection and exploits the FM0 line coding memory using already present preambles in Gen2.
- Study of two tag signal model and collision recovery algorithms that can be used in a real system. In addition, synchronization issues between two tags are also discussed.
- Development of a reader for backscatter sensor networks implementing detection algorithms presented in [3].
- Experimental evaluation of the developed readers with respect to reading rate and range.

1.2 Thesis Outline

In Chapter 2 we present all the background information needed for this thesis. We describe the bistatic signal model and give an overview of RFID systems and EPCglobal Class1 Gen2 Protocol. Furthermore, we discuss related work and highlight the differences between the developed Gen2 reader and existing implementations. In Chapter 3 we describe the SDR signal processing for single and two tag transmissions. In Chapter 4 we present the implementation details of the Gen2 reader and the reader for bistatic WSN. In Chapter 5 the performance of the implemented systems is evaluated. Finally, Chapter 6 acts as an epilogue for this thesis, presenting our conclusions.

Chapter 2

Background

2.1 RFID Systems

Radio-frequency identification (RFID) is a technology similar to barcodes that enables the identification of objects using radio waves [5]. An RFID system consists of RFID tags known as transponders, that are attached to objects and transfer information to a processing device called reader also known as interrogator. Typical applications of RFID include supply chain management, animal tracking, security (controlling access) and payment systems. However, RFID technology has been recently proposed for applications such as biomedical sensor applications and wireless sensor networks (WSNs).

Two possible configurations exist for an RFID system; monostatic and bistatic. In a monostatic configuration the reader both transmits and receives information to/from the tags. A monostatic system utilizes the same antenna for transmission and reception, typically with the help of a circulator. On the other hand, a bistatic system utilize two separate antennas for transmission and reception. The transmitter and receiver can also be dislocated offering advantages as increased coverage and lower cost [3].

Tags can be divided into three categories; passive, semi-passive and active tags. Communication between the reader and passive or semi-passive tags is achieved by means of reflection. More specifically, passive tags do not have independent source of electrical power. They use the received energy provided by the reader in order to power up and transmit information. A passive tag typically terminates its antenna between two loads; in that way, the incident carrier wave (CW) is reflected with altered amplitude and/or phase and tag information is modulated on the reflection coefficient changes. Semi-passive

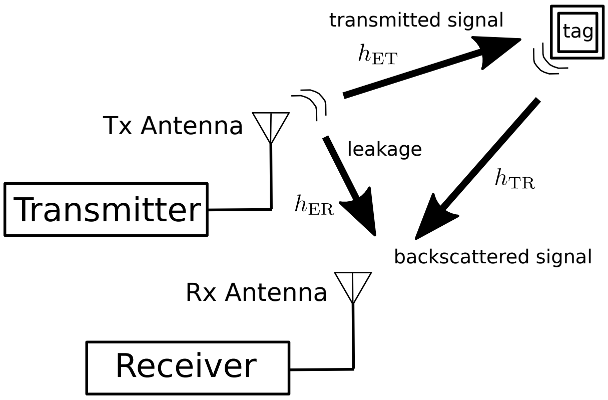


Figure 2.1: Communication between reader and tag in bistatic configuration.

tags, also known as battery-assisted passive tags, use a battery to power the tag circuitry but still use the same principle for the tag-to-reader (uplink) communication. On the other hand, active tags are similar to conventional bidirectional radio communications devices.

RFID systems can operate in various frequency bands; low frequency (LF), high frequency (HF) and ultra-high frequency (UHF). UHF bandwidth across the European Union is regulated by the European Telecommunications Standards Institute (ETSI), and ranges from 865 MHz to 868 MHz.

2.2 Bistatic System Model

As previously stated, two possible configurations exist for RFID systems. In this work a bistatic configuration is employed; the Gen2 reader uses two antennas, one for transmission and one for reception while in a backscatter sensor network the transmitter and receiver are dislocated. The bistatic configuration is shown in Fig. 2.1. In the following section we describe the communication between the reader and a single tag.

The reader transmits a constant CW illuminating the tag. The tag modulates the received CW by terminating its antenna between two loads, reflecting the incident CW with altered amplitude and/or phase. During this process, the transmitted CW also leaks into the reception path. Frequency non-selective (flat) fading is assumed for the three links depicted in in Fig. 2.1.

The baseband complex channel coefficients for the three links are given by

$$h_{\mathrm{ET}} = a_{\mathrm{ET}} e^{+j\phi_{\mathrm{ET}}} \tag{2.1}$$

$$h_{\mathrm{TR}} = a_{\mathrm{TR}} e^{+j\phi_{\mathrm{TR}}} \tag{2.2}$$

$$h_{\mathrm{ER}} = a_{\mathrm{ER}} e^{+j\phi_{\mathrm{ER}}} \tag{2.3}$$

where h_{ET} denotes the channel between emitter and tag, h_{TR} denotes the channel between tag and receiver and h_{ER} denotes the channel between emitter and receiver.

The baseband equivalent of the reader's transmitted CW is given by

$$c(t) = \sqrt{2P_c} e^{+j(2\pi\Delta f t + \Delta\phi)} \tag{2.4}$$

where P_c is the power of the CW at passband, Δf is the carrier frequency offset (CFO) between reader transmission and reception chain that may be caused by different oscillation signals for up and down-conversion and $\Delta\phi$ is a phase shift caused by the propagation delay between the transmission and the reception path. The transmitted CW is attenuated by a_{ER}, rotated by ϕ_{ER} and leaked into the reception path.

$$C_{\mathrm{dc}}(t) = a_{\mathrm{ER}} e^{+j\phi_{\mathrm{ER}}} c(t) = a_{\mathrm{ER}} \sqrt{2P_c} e^{+j(2\pi\Delta f t + \Delta\phi + \phi_{\mathrm{ER}})} \tag{2.5}$$

The tag is illuminated by the CW signal attenuated by a_{ET} and rotated by ϕ_{ET}. The reflected baseband tag signal is given by [3]

$$a(t) = s\left((A_s - \Gamma_0) + (\Gamma_0 - \Gamma_1)x(t)\right) a_{\mathrm{ET}} e^{+j\phi_{\mathrm{ET}}} \sqrt{2P_c} e^{+j(2\pi\Delta f t + \Delta\phi)} \tag{2.6}$$

where $x(t) \in \{0, 1\}$ corresponds to the modulation waveform of the tag, A_s is the tag antenna structural mode [6], Γ_0, Γ_1 are the antenna load's reflection coefficients and s is a parameter depending on the tag scattering efficiency.

Thus, the received baseband signal at the SDR reader is given by the superposition of the transmitted CW and the backscattered tag signal attenuated by a_{TR} and rotated by ϕ_{TR}.

$$y(t) = (L_{\mathrm{dc}} + s\left((A_s - \Gamma_0) + (\Gamma_0 - \Gamma_1)x(t)\right) a_{\mathrm{ET}} e^{+j\phi_{\mathrm{ET}}} a_{\mathrm{TR}} e^{+j\phi_{\mathrm{TR}}} \sqrt{2P_c} e^{+j\Delta\phi}) e^{+j2\pi\Delta f t} + n(t) \tag{2.7}$$

For simplified notation we set

$$m_0 \triangleq a_{\mathrm{ET}} a_{\mathrm{TR}} s |A_s - \Gamma_0| \sqrt{2P_c} \tag{2.8}$$

$$m_1 \triangleq a_{\mathrm{ET}} a_{\mathrm{TR}} s |\Gamma_1 - \Gamma_0| \sqrt{2P_c} \tag{2.9}$$

$$\phi_0 \triangleq \phi_{\mathrm{ET}} + \phi_{\mathrm{TR}} + \Delta\phi + \underline{/A_s - \Gamma_0} \tag{2.10}$$

$$\phi_1 \triangleq \phi_{\mathrm{ET}} + \phi_{\mathrm{TR}} + \Delta\phi + \underline{/\Gamma_0 - \Gamma_1} \tag{2.11}$$

Using the above notation, the received signal can be written as

$$y(t) = (L_{\mathrm{dc}} + m_0 e^{+j\phi_0} + m_1 e^{+j\phi_1} x(t)) e^{+j2\pi\Delta f t} + n(t) \tag{2.12}$$

where L_{dc} is the the component leaked in the reception path, $m_0 e^{+j\phi_0}$ is an unmodulated component which depends on the tag antenna structural mode A_s, reflection coefficient Γ_0 and channel coefficients $h_{\mathrm{ET}}, h_{\mathrm{TR}}$, the tag scattering efficiency s and the carrier transmitting power $\sqrt{2P_c}$. $n(t)$ is a baseband complex Gaussian random process which stands for the thermal noise at receiver. The power spectral density of the baseband complex Gaussian process $n(t)$ is given by

$$S_{nn}(F) = \begin{cases} \frac{N_0}{2}, & |F| \leq W \\ 0, & \text{otherwise,} \end{cases} \tag{2.13}$$

Carrier frequency offset (CFO) Δf can be directly estimated using the Fast Fourier transform (FFT) and periodogram-based techniques. The received signal is sampled with sampling period T_s. After CFO estimation and compensation, the received digitized signal is given by

$$y[k] \triangleq y(kTs) = A_{\mathrm{dc}} + hx[k] + n[k] \tag{2.14}$$

where $A_{\mathrm{dc}} \triangleq L_{\mathrm{dc}} + m_0 e^{+j\phi_0}$, $h \triangleq m_1 e^{+j\phi_1}$, $n[k] = n(kT_s) \sim \mathcal{CN}(0, 2\sigma_n^2)$.

2.3 EPCglobal Class 1 Generation 2 Protocol

EPCglobal Class 1 Generation 2 Protocol specification (EPC Gen2) defines the communication parameters (physical and media access control (MAC) layer) for an RFID system of readers and passive tags, operating in the 860 MHz - 960 MHz UHF range. The most recent update, Gen2v2, was published in April 2015 [7].

The EPC Gen2 standard utilizes a framed slotted Aloha (FSA) based protocol; a reader defines the number of slots and initiates the start of a frame. The communication between the reader and tags is half-duplex meaning that a tag does not receive reader messages while backscattering. Tags that participate in a frame choose randomly a specific slot of a frame to transmit. In case of a collision, the collided tags choose a new slot from the next frame. A new frame is initiated by a reader command called Query. The interval between two subsequent Query commands is called inventory round. The details of the operation procedure are discussed in the next sections.

2.3.1 Physical Layer

The EPC Gen2 physical layer describes how information is transmitted between the reader and the tags. A CW needs to be transmitted continuously regardless of whether it is the reader or the tag that is communicating. The tags harvest energy from this signal in order to operate. In addition, the modulation needs to be simple in order for a low power and low cost tag to decode it. Various configurations of the reader-to-tag (downlink) and tag-to-reader (uplink) communication are offered.

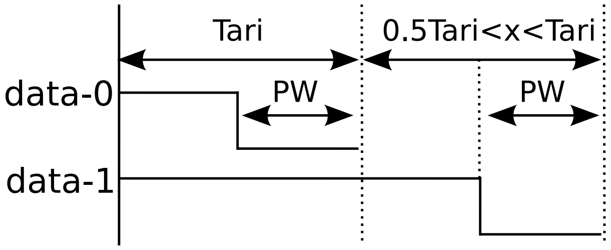


Figure 2.2: PIE encoding for downlink communication.

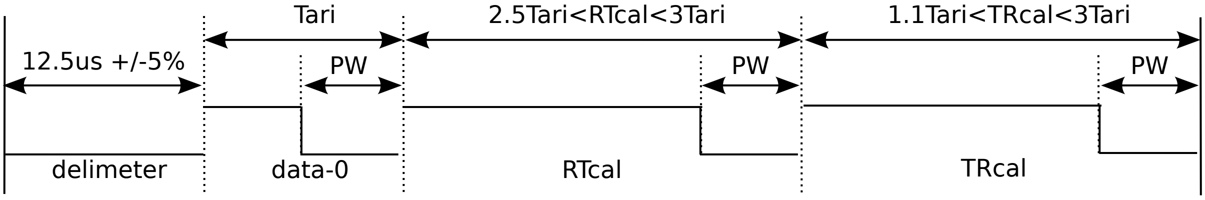


Figure 2.3: Preamble for downlink communication.

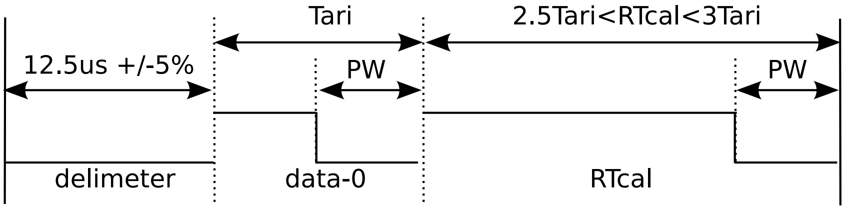


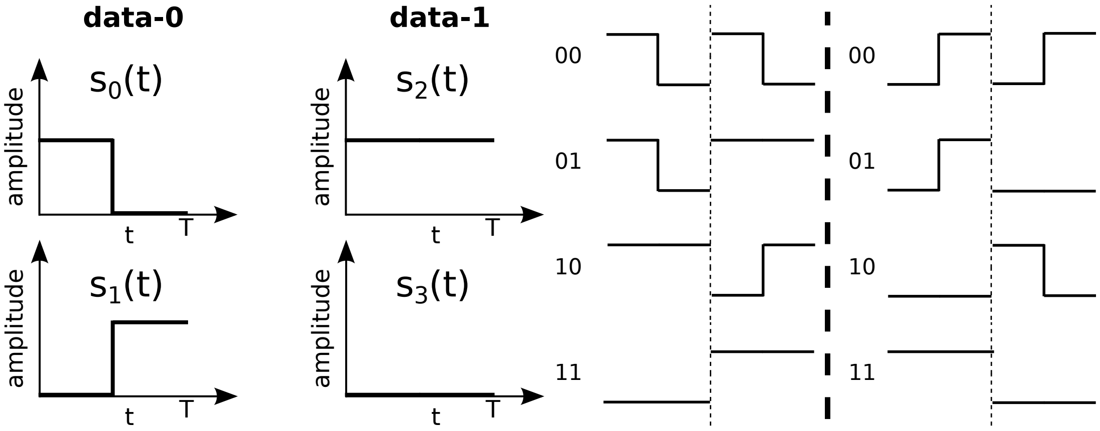
Figure 2.4: Frame-Sync for downlink communication.

2.3.1.1 Downlink Communication

The reader uses amplitude shift keying (ASK) with pulse-interval encoding (PIE) to communicate with the tags. The transmitted signals corresponding to data-0 and data-1 are shown in Fig. 2.2. Tari is the reference time interval for the downlink communication, and defines the duration of a data-0. RF pulsewidth (PW) is the duration of the attenuated carrier. Tari values are in the range of 6.25us to 25us. PW can be set between $\mathrm{MAX}(0.265\mathrm{Tari}, 2)$ and 0.525Tari. Depending on data-1 and data-0 durations, downlink rates range from 27 kbps to 128 kbps.

A reader starts the downlink communication with either a Preamble or a Frame-Sync which are shown in Figs. 2.3,2.4. A Preamble precedes a Query command. All other reader commands begin with a Frame-Sync. A Preamble consists of a start delimiter, a data-0 symbol, a reader-to-tag calibration signal (RTcal), and a tag-to-reader calibration (TRcal) signal. A Frame-Sync is similar to the Preamble but shorter as it does not include TRcal.

- **RTcal** A reader sets RTcal equal to the length of a data-0 symbol, plus the length of a data-1 symbol ($\mathrm{RTcal} = \text{ data-0}_{\mathrm{length}} + \text{ data-1}_{\mathrm{length}}$). The tags measure the RTcal length and compute a pivot which has half the duration of RTcal. A tag then interprets symbols longer than pivot as data-1s and shorter than pivot as data-0s.



(a) FM0 symbols.

(b) FM0 sequences.

Figure 2.5: FM0 encoding.

Symbols longer than 4 RTcals are interpreted by the tag as invalid. In order to change RTcal, a reader should first transmit a CW for a minimum of 8 RTcal.

- **TRcal**

  A reader specifies a tag's backscatter link frequency (BLF) using the TRcal and divide ratio (DR) in the Preamble and payload of a Query command respectively. The tags measure the length of TRcal, compute BLF, and adjust their data rate to be equal to BLF in case of FM0 encoding or BLF/M in case of Miller-M $M \in \{2, 4, 8\}$ encoding. BLF is in the range of 40 kHz and 640 kHz.

$$\text{BLF} = \frac{\text{DR}}{\text{TRcal}} \tag{2.15}$$

$$1.1\text{RTcal} \leq \text{TRcal} \leq 3\text{RTcal} \tag{2.16}$$

2.3.1.2 Uplink Communication

A tag communicates with the reader, modulating its information by switching its antenna load between two states. A tag uses fixed modulation format, data encoding and data rate for the duration of an inventory round. Tags select the modulation format, while readers select encoding and data rate. Tags may use ASK or PSK modulation and use either FM0 or Miller encoding.

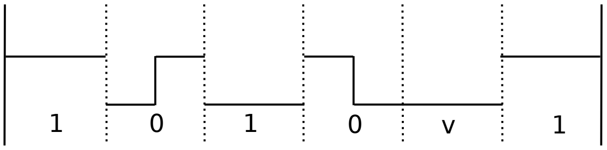


Figure 2.6: Tag Preamble for uplink communication.

In FM0 encoding amplitude level changes at every symbol boundary, while a data-0 has also an amplitude change in the middle of the symbol. The four FM0 pulses are shown in Fig. 2.5(a). Data-0 is transmitted either with a $s_0(t)$ pulse or a $s_1(t)$ pulse, depending on the data bit that was previously transmitted. The same applies for data-1. It is either transmitted with a $s_2(t)$ pulse or a $s_3(t)$ pulse. FM0 encoding always "ends" with a dummy data-1 bit. All possible sequences that can be created with FM0 encoding are shown in Fig. 2.5(b). Each tag response begins with the Preamble shown in Fig. 2.6. The "v" indicates an FM0 violation; an amplitude change should have occurred.

2.3.2 Tag-Identification Layer

A reader can interact with the tags using three operations; Select, Inventory and Access. During each of the above operations tags may change state as shown in Fig. 2.7. A detailed description of each operation is given below.

2.3.2.1 Select

The operation of selecting a particular tag population (subset) for inventory and access. A Select command may be applied successively to select a particular tag population. This operation is similar to that of selecting records from a database. Tags provide four sessions (S0, S1, S2 and S3). For each session the tags maintain an inventoried flag which defines their state in the corresponding session. The inventory flag can take the values A or B. In addition to the inventoried flag, tags also maintain a SL flag. The Select command can assert or deassert the SL flag and alter the value of the inventoried flag. Tags do not respond to Select commands. By issuing multiple identical select commands a reader can choose all tags matching the selection criteria even though downlink communication may suffer from short duration RF fades.

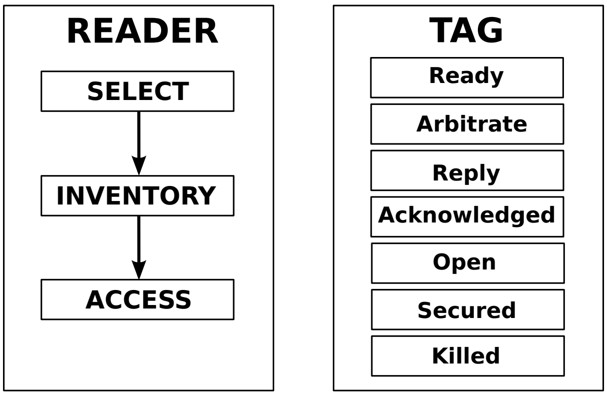


Figure 2.7: Reader and tag states.

2.3.2.2 Inventory

The operation of identifying tags. A new inventory round is initiated by transmitting a Query command. A Query provides the necessary information for the downlink and uplink communication parameters. Only tags that their session inventoried flag and SL flag matches the Query command, participate in the inventory round. During the inventory operation a reader can issue one of the following commands: Query, QueryAdjust, QueryRep, ACK, and NAK.

- **Query**

  A Query defines the SL and inventoried flag of the tags that will participate in the inventory round. It also contains a slot counter $Q \in [0, 15]$ in order to set the number of slots $N = 2^Q$. After a Query, tags that have slot counter equal to zero, transmit a message (RN16) to the reader. A Query also defines the backscatter link frequency (BLF) of the tags as well as the encoding. A Query is shown in Table 2.1. Query includes the following fields:

	Command	DR	M	TRext	Sel	Session	Target	Q	CRC-5
# of bits	4	1	2	1	2	2	1	4	5
description	1000	0 : DR = 8 1 : DR = 64/3	00 : M = 1 01 : M = 2 10 : M = 4 11 : M = 8	0:No pilot tone 1:Use pilot tone	00:All 01:All 10:∼SL 11:SL	00:S0 01:S1 10:S2 11:S3	0:A 1:B	$0 - 15$	

Table 2.1: Query command.

	Command	Session	UpDn
# of bits	4	2	3
description	1001	00:S0 01:S1 10:S2 11:S3	110 : $Q = Q + 1$ 000: No change to Q 011 : $Q = Q - 1$

Table 2.2: QueryAdjust command.

- **Command code(4)**: Query code is 1000.
- **DR(1)**: Defines the BLF frequency (together with TRcal). BLF is in the range of 40kHz and 640kHz.
- **M(2)**: Defines the tag encoding that can be set to either FM0 or Miller.
- **TRext(1)**: Chooses whether the preamble is preceded by an optional pilot tone. Pilot tone consists of 12 consecutive data-0s.
- **Sel(2)**: Selects which tags will participate in the inventory round depending on the SL flag. To select all the tags the reader sets Sel = 00 or Sel = 01.
- **Session(2)**: Chooses the session of the inventory round. There are in total four possible sessions. Each session differs on the time maintaining the inventoried flag.
- **Target(1)**: Selects which tags will participate in the round depending on their inventoried flag.
- **Q(4)**: Defines the number of slots in the current round.
- **CRC(5)**: 5-bit checksum.

- **QueryAdjust** QueryAdjust is used to change the number of slots in the inventory round without changing other parameters. Q value can be incremented/decremented by one or stay unchanged. QueryAdjust is shown in Table 2.2. QueryAdjust includes the following fields:

  - **Command code(4)**: QueryAdjust code is 1001.

	Command	Session
# of bits	2	2
Description	00	00:S0 01:S1 10:S2 11:S3

Table 2.3: QueryRep command.

- **Session(2)**: Verifies the session number for the inventory round. If a tag receives a QueryAdjust whose session number differs from the session number of the Query that initiated the inventory round ignores the command.
- **UpDn(3)**: Determines whether the tags will adjust the number of slots. The possible values are shown in Table 2.2. If UpDn has a different value, the tags ignore the command.

- **QueryRep**

  QueryRep repeats the previous query and defines a new slot. Each tag decrements its slot counter q by one and if $q = 0$ after a QueryRep command, backscatters an RN16 to the reader. QueryRep is shown in Table 2.3. QueryRep includes the following fields:

  - **Command code(2)**: QueryRep command code is 00.
  - **Session(2)**: Verifies the session number for the inventory round. If a tag receives a QueryRep whose session number differs from the session number of the Query that initiated the inventory round ignores the command.

- **ACK**

  It is used as an acknowledgement in response to a tag message. An ACK contains the 16-bit random number (RN16) that have been previously transmitted by the tag. If the ACK is correct, the tag transmits a 135-bit response that contain its ID (EPC). ACK command is shown in Table 2.4. ACK includes two fields:

  - **Command code(2)**: ACK code is 01.

	Command	RN16
# of bits	2	16
Description	01	Echoed RN16 or handle.

Table 2.4: ACK command.

  - **RN(16)**: 16 random bits that have been transmitted by a tag.

- **NAK**

  Any Tag that receives a NAK shall return to the arbitrate state without changing its inventoried flag. That means that if a reader has failed to decode a tag response, a NAK can be sent. The reader will try to correctly decode the tag's message by issuing a QueryAdjust command. NAK is shown in Table 2.5. A NAK command includes only one field:

  - **Command code(8)**: NAK command code is 11000000.

	Command
# of bits	8
Description	11000000

Table 2.5: NAK command.

2.3.2.3 Access

The operation by which a reader transacts with individual tags. After a tag has been identified a reader can read from or write to it. The reader can access its memory using one of the following commands: Req_RN, Read, Write, Kill, Lock, Access, BlockWrite, BlockErase, BlockPermalock. Again, a handshake mechanism is required. A reader instructs the tag to send a new random number which is called Handle using a Req_RN command. The reader may then issue an ACK with Handle as a parameter.

2.3.2.4 Tag States

During the Inventory operation, a tag transitions between Ready, Arbitrate, Reply and Acknowledged state. A brief description of each state is given below

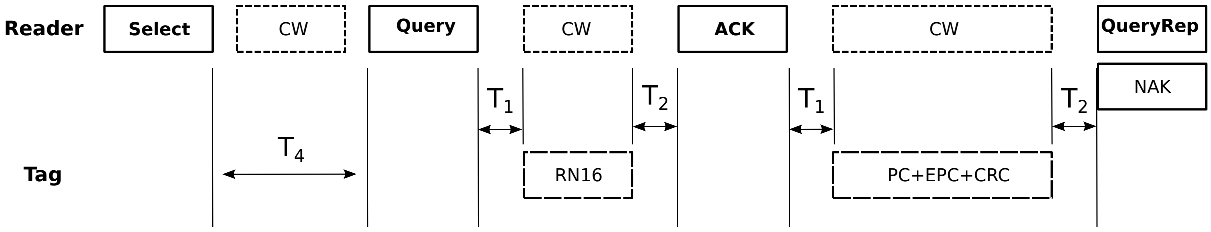


Figure 2.8: Successful communication between a reader and a tag.

- **Ready**: After being energized, the tags transition to Ready state. Ready state can be viewed as a "holding state" for energized Tags. The tags remain in the Ready state until they receive a Query command. Tags generate a random number q and transition to the Reply state if $q = 0$ or to the Arbitrate state if $q \neq 0$.

- **Arbitrate**: A tag in an Arbitrate state decrements its slot counter every time it receives a QueryRep command. When its slot number reaches zero, it transitions to the Reply state and backscatters a RN16.

- **Reply**: A tag backscatters a RN16, once it enters the Reply state.

- **Acknowledged**: If a tag in the Reply state receives a valid ACK, it transitions to the Acknowledged state, backscattering its PC, EPC, and CRC-16. If the tag receives an invalid ACK it returns to the Arbitrate state.

2.3.3 Inventorying Gen2 RFID Tags

In this section we offer a complete description of an inventory round. An inventory round is initiated by a reader which emits a CW causing the Tags to power up and transition to Ready. A tag can then transition either to Arbitrate or Reply state. The reader sends a Query command making tags that their inventoried and SL flag matches the Query choose a q value in the interval $[0, Q-1]$.

Tags that have chosen the first slot i.e $q = 0$, enter the Reply state immediately while remaining tags transition to Arbitrate. Tags that are in the Reply state backscatter a random 16-bit number (RN16). The reader receives the backscattered signal and decodes the tag response. The reader then sends an ACK that includes the same 16-bit number. When the tag receives the ACK, it compares it with the transmitted RN16. If the RN16

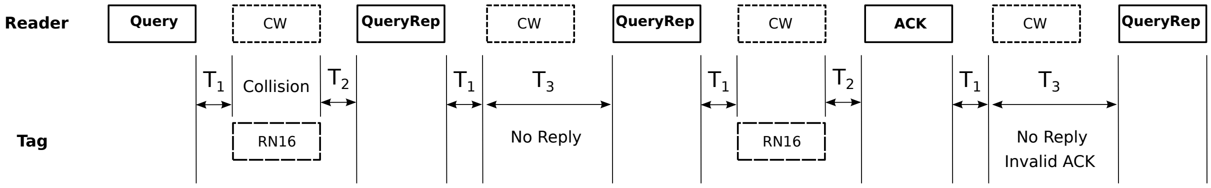


Figure 2.9: Unsuccessful communication between a reader and three tags.

was correctly decoded, the tag transitions to the Acknowledged state and backscatters a 135-bit response containing PC, EPC (ID) and a 16-bit CRC. This procedure is shown in Fig.2.8. A reader can resend the ACK and request again the tag's ID. The reader sends a QueryRep in order to identify another tag, repeating the above procedure. If no tag replies or if there is a collision and the reader is not able to resolve it, it can send another QueryRep without sending an ACK. If a reader fails to decode a RN16, the tag transitions to the Arbitrate state. Finally, a reader may decode a RN16 correctly but fail to decode the EPC. If the tag receives a NAK command it will transition to arbitrate. Otherwise, it will change its inventoried flag and transition to Ready. These scenarios are shown in Fig. 2.9

Finally, a reader can also alter the number of slots in the current inventory round using a QueryAdjust command. QueryAdjust signals the start of a new slot. QueryAdjust repeats the previous Query and causes every tag that is in the Arbitrate state to choose a new random number and pick a new slot.

2.3.3.1 Timing Constraints

Reader and tag communication must comply to specific timing requirements which are shown in Table 2.6. These parameters do play an important role and were taken into account in the implementation of the SDR reader. More specifically, T_{pri} denotes the symbol period of tag messages. T_1 represents the time from a reader transmission to a tag response as measured from the last rising edge of the reader to the first rising edge of the Tag response. T_2 is the reader response time required if a tag is to decode the reader signal. T_2 is measured from the end of the last bit of the tag response to the first falling edge of the reader transmission. T_3 is the time that a reader has to wait, after T_1, before it issues another command. Finally T_4 is the minimum time between reader commands.

Table 2.6: Timing parameters

Parameter	Minimum	Nominal	Maximum
T_1	$\mathrm{MAX}(\mathrm{RT_{cal}}, 10\mathrm{T_{pri}})\times$ $(1 - \lvert FT\rvert) - 2\mathrm{us}$	$\mathrm{MAX}(\mathrm{RT_{cal}}, 10\mathrm{T_{pri}})$	$\mathrm{MAX}(\mathrm{RT_{cal}}, 10\mathrm{T_{pri}})\times$ $(1 + \lvert FT\rvert) + 2\mathrm{us}$
T_2	$3.0\mathrm{T_{pri}}$		$20.0\mathrm{T_{pri}}$
T_3	$0.0\mathrm{T_{pri}}$		
T_4	$2.0\mathrm{RT_{cal}}$		

2.4 Related Work

The first implementation of a UHF Gen2 RFID reader based on the USRP software defined radio (SDR) platform was presented in [8]. The authors mainly focus on how to overcome limitations due to the hardware used. The presented system is based on the USRP1 which introduces latency issues due to the USB interface. EPC Gen2 protocol has strict timing requirements that were met by reducing the block size to the minimum allowed by the linux kernel. In addition, careful processing of the received samples (samples that corresponding to reader commands are blocked and ignored) further reduced the latency. The reader was evaluated and compared with a commercial Impinj reader. For their experiments, they used 40kHz Miller-2 encoding. It was shown that the reader could inventory commercial tags up to 6 meters, which approximates the range of a commercial reader with comparable transmit power. The code was released as an open source software and is available online [9]. However it is not compatible with the latest versions of GNU Radio and UHD as it was developed with GNU Radio v3.2.

A monitor device that could decode messages between a reader and tags i.e. sniffer was also presented in [10]. The developed platform is able to capture reader transmissions and uses the USRP2 SDR for real-time processing. The authors presented results that show it has high accuracy up to 3 meters and was used to study commercial RFID readers. The code is also available online [9].

An extension to the available SDR reader is presented in [11]. The authors use an HF multiplexer for the USRP1 SDR connected to four transmit and receive antennas and studied the read rate and range of the modified reader.

In [12], the authors modify the original Buettner's code and build a testing platform for evaluating the performance of commercial RFID tags. The platform enables the measurement of tag sensitivity and differential RCS. In [13] De Donno et al. develop a listener device that can be used in conjunction with the Buettner's reader and evaluate the impact of different clock recovery algorithms. Three clock recovery algorithms were compared; Mueller and Muller algorithm, zero-crossing and polyphase filter bank. Their work focused on the uplink communication channel. They conducted measurements using Miller-8 encoding in order to test the reading range of commercial RFID tags as well as how their performance is affected in various indoor scenarios. The code was released as open source software but it is not available online.

In [14], a complete SDR based UHF RFID system is presented. It consists of the basic reader ported to a newer version of GNU Radio (v3.6) and a SDR based tag. Two USRP1 were used with four antennas; two for transmit and two for receive. A cryptography protocol was also implemented and tested.

In [15], Zheng et al. ported the original reader presented in [8] to GNU Radio v3.6 and released it online [16]. The reader can only be used to inventory Wireless Identification and Sensing Platform (WISP) tags and not commercial Gen2 UHF RFID tags. A USRP2 is used with a RFX900 daughterboard.

In [17], Bothe et al. ported the original reader to the latest version of GNU Radio (v3.7) as for the time writing this thesis. The authors make two main contributions. They present the first SDR based UHF Gen2 RFID reader, that works with the latest release version of GNU Radio and extend it so that it can be run with offline data as input; without the need of a USRP. They compare two clock recovery algorithms and conduct experiments using Miller-8 encoding. The code is not available online.

Finally there are several works that focus on FPGA based signal processing. Authors in [18] present an UHF RFID reader implementation based on USRPN200. Their implementation in contrast to the previous presented works, supports the whole range of EPC backscatter-link frequencies (BLF) however, they focus only on Miller-M encoding and present a sub-optimal detection algorithm. Angerer in [19] also presents a custom FPGA implementation of a reader discussing synchronization and detection algorithms and targeting FM0 encoding. Table 2.7 summarizes the differences of the readers described.

	[8]	[12]	[14]	[15]	[17]	[18]	This work
Reader	x		x	x	x	x	x
Open source	x	x		x			x
Commercial tags	x	x			x	x	x
USRP1	x	x	x				
USRP2				x	x	x	x
GNU Radio version	obsolete	obsolete	obsolete	v3.6	v3.7		v3.7
FM0		x	x	x	x		x
Miller	x	x	x	x	x		
Coherent detection							x
Memory							x

Table 2.7: Related Work.

Chapter 3

SDR Signal Processing

3.1 Gen2 UHF RFID Reader Processing

According to the EPCglobal standard for UHF RFID [7], each tag encodes its information using either FM0 or Miller-M ($M \in \{2, 4, 8\}$) line coding. In FM0 encoding which has been described in Section 2.3.1.2, level transitions always occur on the bit boundaries. In addition a transition occurs in the middle of bit "0". Thus, there is memory-based modulation, resulting to four possible waveforms per bit, as shown in Fig. 3.1, where bit boundaries are separated by dashed lines.

Work in [20, 21] have shown that after shifted examination of the transmitted waveform by $T/2$ before the beginning of the bit, where T is the bit (symbol) period, only two possible pulse shapes can be generated (instead of four), shown in Fig. 3.1 marked with rectangles. In order to detect a transmitted bit, the reader has to differentially decode 2 received symbols (using $2T$ signal observation instead of just T), realizing a gain of 3dB compared to maximum-likelihood symbol-by-symbol detection.

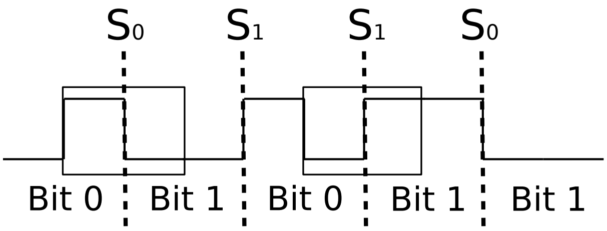


Figure 3.1: FM0 line coding signal.

The Gen2 reader of this work is based on a single transceiver card, with a common oscillation signal for both transmission and reception radio frequency (RF) chain. Thus, $\Delta f = 0$. Assuming that the reader can perfectly estimate one of the two tag states and remove it from the received waveform (zero-offset FM0), the received digitized signal from Eq. (2.14) is expressed as:

$$y[k] = y(kTs) = hx[k] + n[k] \tag{3.1}$$

$$x[k] = \sum_{n=0}^{N} S_{d(n)}[k - nL - \tau] \tag{3.2}$$

where $n[k] = n(kT_s) \sim \mathcal{CN}(0, 2\sigma_n^2)$, $d(n) \in \{0, 1\}$ denotes the transmitted bit, T denotes the nominal bit duration, τ is the delay before tag starts transmitting its information, $L \triangleq \frac{T}{T_s}$ the oversampling factor and $S_{d(n)}$ can be selected between the following waveforms:

$$S_0[k] = \begin{cases} 1, & \text{if } 0 \leq k < \frac{L}{2} \\ 0, & \text{if } \frac{L}{2} \leq k < L \end{cases} \tag{3.3}$$

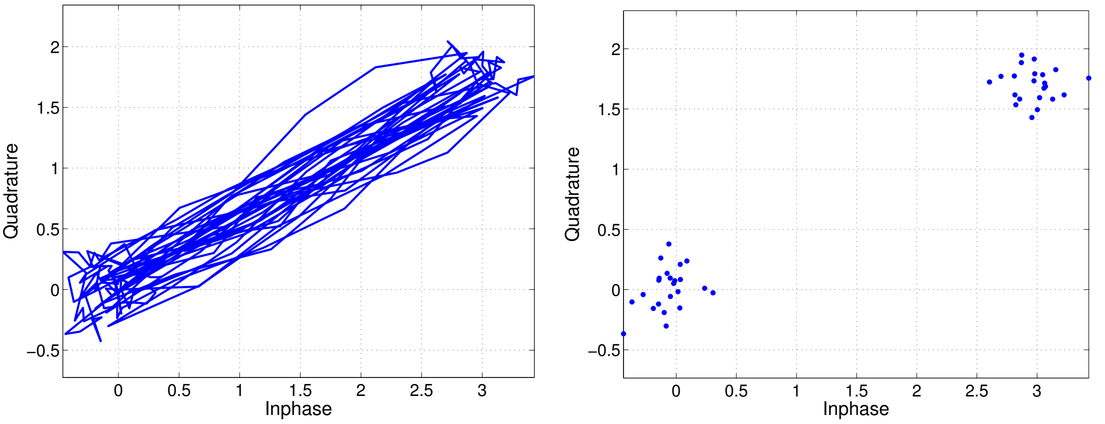
$$S_1[k] = \begin{cases} 0, & \text{if } 0 \leq k < \frac{L}{2} \\ 1, & \text{if } \frac{L}{2} \leq k < L \end{cases} \tag{3.4}$$

The above waveforms are the only possible signals when one observes the zero-offset FM0 signal for a duration of one bit (i.e., T), starting $T/2$ before the start of a bit (up to the middle of the bit), or starting at the middle of the bit (up to $T/2$ after the end of the bit). Detection of those two waveforms, spanning signal duration of $2T$, offers the detection of one of the four possible waveforms for each bit and fully exploits memory induced in FM0. The received signal is thus filtered using a square pulse $\Pi[k]$ of length $L/2$.

$$y_f[n] = \sum_{k=-\infty}^{\infty} y[k]\Pi\left[n-k\right] \tag{3.5}$$

Consequently, the received signal after matched filtering and synchronization (for a half symbol period) can be written as:

$$y = \sum_{k=0}^{\frac{L}{2}-1} y[k] = \sum_{k=0}^{\frac{L}{2}-1} \frac{L}{2} hx[k] + \sum_{k=0}^{\frac{L}{2}-1} n[k] = h'x + n', \tag{3.6}$$



(a) Received samples after matched filtering.

(b) Received samples after matched filtering and synchronization.

Figure 3.2: I/Q constellation diagram of a single tag transmission using simulated data.

where $x \in \{0, 1\}$ and $n' \sim \mathcal{CN}(0, L\sigma_n^2)$. Thus, each FM0 symbol observed with a $T/2$ shift can be written as a 2×1 complex vector:

$$\mathbf{y} \triangleq \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = h'\mathbf{x} + \mathbf{n}, \tag{3.7}$$

where $\mathbf{x} \in \{\mathbf{e}_0 \triangleq [1\ 0]^T, \mathbf{e}_1 \triangleq [0\ 1]^T\}$ and $\mathbf{n} \sim \mathcal{CN}(0, L\sigma_n^2\mathbf{I}_2) \equiv \mathcal{CN}(0, \sigma^2\mathbf{I}_2)$. Component y_0 or y_1 of the complex vector $\mathbf{y}$ will be referred to as half bit. The matched filter output as well as the FM0 half-bits are shown in Fig. 3.2 using simulated data. We have set SNR = 25db, $h' = 2.99 + 1.72j$. The tag signal-to-noise ratio (SNR) is defined as

$$\text{SNR} \triangleq \frac{|h'|^2}{\frac{L}{2}\mathbb{E}[|n[k]|^2]} = \frac{|h'|^2}{\sigma^2} = \frac{L|h|^2}{2\mathbb{E}[|n[k]|^2]}. \tag{3.8}$$

3.1.1 DC Offset and Channel Estimation

In a real time application, the DC offset component can be estimated during a Gen2-defined interval before the tag starts switching. This interval is known to the reader and is defined by [7] as T_1; its duration depends on the tag's data rate for FM0 encoding. Tag is absorbing energy with corresponding reflection coefficient close to zero; thus, the reflected signal corresponding to one of the two tag load states, can be estimated by averaging the received samples acquired in interval T_1. The received signal during T_1 is given by

$$y_{\mathrm{T}_1}[k] = A_{\mathrm{dc}} + n[k], \;\; k = 0, \dots, L_{\mathrm{T}_1} - 1 \tag{3.9}$$

where $L_{\mathrm{T}_1} = \frac{\mathrm{T}_1}{T_s}$ is the length of the interval T_1 in samples.

The ML estimate of $\widehat{A_{\mathrm{dc}}}$ is found by

$$\begin{aligned}
\widehat{A_{\mathrm{dc}}} &= \underset{A_{\mathrm{dc}}\in\mathbb{C}}{\operatorname{argmax}} f(\mathbf{y}|A_{\mathrm{dc}}) \\
&= \underset{A_{\mathrm{dc}}\in\mathbb{C}}{\operatorname{argmax}} \ln\left(\prod_{k=0}^{L_{\mathrm{T}_1}-1} \frac{1}{2\pi\sigma_n^2} e^{-\frac{|y[k]-A_{\mathrm{dc}}|^2}{2\sigma_n^2}}\right) \\
&= \underset{A_{\mathrm{dc}}\in\mathbb{C}}{\operatorname{argmin}} \sum_{k=0}^{L_{\mathrm{T}_1}-1} |y[k] - A_{\mathrm{dc}}|^2 \\
&= \frac{1}{L_{\mathrm{T}_1}} \sum_{k=0}^{L_{\mathrm{T}_1}-1} y[k]
\end{aligned} \tag{3.10}$$

The estimated component which is equal to the sample mean of the received samples, is subtracted from each sample offering Eq. (3.1).

A Gen2 tag that uses FM0 line coding transmits a known (real) sequence (preamble) $\mathbf{s}_p$ before sending information bits shown in Fig 2.6. This sequence consists of twelve half bits. At first, frame synchronization is performed and the delay τ is estimated by correlating the received signal with the known preamble. Although the duration of T_1 is known to the reader, it is subject to small deviations that are tag-dependent. Thus, the reader can search for a suitable τ in a small interval i.e., $\{0, \dots, L-1\}$.

$$\hat{\tau} = \underset{\tau\in\{0,\dots,L-1\}}{\operatorname{argmax}} \left|\sum_{n=0}^{N_p-1} s_p[n] y[\tau + n]\right|, \tag{3.11}$$

where N_p is the number of samples in the preamble.

Assuming that we are perfectly synchronized, the ML estimate of the parameter h is given by

$$\begin{aligned}\hat{h} &= \underset{h\in\mathbb{C}}{\operatorname{argmax}} f(\mathbf{y}_p|h) \\ &= \underset{h\in\mathbb{C}}{\operatorname{argmax}} \ln\left(\prod_{k=\hat{\tau}}^{\hat{\tau}+N_p-1} \frac{1}{2\pi\sigma_n^2} e^{-\frac{|y[k]-hs_p[k]|^2}{2\sigma_n^2}}\right) \\ &= \underset{h\in\mathbb{C}}{\operatorname{argmin}} \sum_{k=\hat{\tau}}^{\hat{\tau}+N_p-1} |y[k]-hs_p[k-\hat{\tau}]|^2 \\ &= \frac{\sum_{k=\hat{\tau}}^{\hat{\tau}+N_p-1} y[k]s_p[k-\hat{\tau}]}{||\mathbf{s}_p||^2},\end{aligned} \tag{3.12}$$

where $||.||$ denotes the Euclidean norm.

3.1.2 Detection

With parameter h' estimated and known, the maximum likelihood detection rule for system of Eq. (3.7) becomes:

$$\begin{aligned} f(\mathbf{y}|h',\mathbf{e}_0) &\underset{S_1}{\overset{S_0}{\gtrless}} f(\mathbf{y}|h',\mathbf{e}_1) \\ \|\mathbf{y}-h'\mathbf{e}_0\|^2 &\underset{S_0}{\overset{S_1}{\gtrless}} \|\mathbf{y}-h'\mathbf{e}_1\|^2 \\ \Re(h'^*y_1) &\underset{S_0}{\overset{S_1}{\gtrless}} \Re(h'^*y_0) \\ \Re(h'^*(y_1-y_0)) &\underset{S_0}{\overset{S_1}{\gtrless}} 0 \end{aligned} \tag{3.13}$$

where $\Re(z)$ denotes the real part of complex z. The probability of error of the above minimum distance rule can be easily found as $\Pr(e)_T^{\text{coh}} = Q\left(|h'|/\sigma\right) = Q(\sqrt{\text{SNR}})$, with $Q(t) = (1/\sqrt{2\pi})\int_t^{+\infty} e^{-t^2/2}dt$ [22].

Alternatively, an energy based rule where estimation of h' is not needed Eq. (3.7) is given by

$$|y_1|^2 \underset{S_0}{\overset{S_1}{\gtrless}} |y_0|^2, \tag{3.14}$$

with probability of error $\Pr(e)_T^{\text{ncoh}} = (1/2)\ e^{-|h'|^2/(2\sigma^2)} = (1/2)\ e^{-\text{SNR}/2}$ [22].

Having detected $N+1$ FM0 symbols of duration T and time-shifted by $T/2$, based on Eq. (3.7), the final decision for the transmitted bits $\mathbf{b}$, considering signal duration of

$2T$ for each bit is computed as:

$$\hat{b}(n) = \hat{d}(n-1) \oplus \hat{d}(n), \quad n = 1, \ldots, N, \tag{3.15}$$

where $d(n) = 0$ when S_0 is detected and $d(n) = 1$, otherwise; operation $\oplus$ denotes modulo-2 addition (xor). The specific rule fully exploits memory of FM0 and results to erroneous bit detection when *exactly* one of the two (shifted) consecutive FM0 symbols is erroneously detected:

$$\Pr(e)_{2T} = 2\Pr(e)_T\left(1 - \Pr(e)_T\right). \tag{3.16}$$

Thus the BER of coherent and noncoherent memory assisted detection is

$$\Pr(e)^{\text{coh}}_{2T} = 2Q(\sqrt{\text{SNR}})(1 - Q(\sqrt{\text{SNR}})) \tag{3.17}$$

$$\Pr(e)^{\text{ncoh}}_{2T} = e^{-\text{SNR}/2}(1 - (1/2)\ e^{-\text{SNR}/2}) \tag{3.18}$$

The performance of the coherent symbol-by-symbol detection, that ignores the FM0 encoding properties, suffers a 3dB loss and is given by [19],[21].

$$\Pr(e)^{\text{coh}}_{\text{symbol}} = 2Q(\sqrt{1/2\ \text{SNR}})(1 - Q(\sqrt{1/2\ \text{SNR}})) \tag{3.19}$$

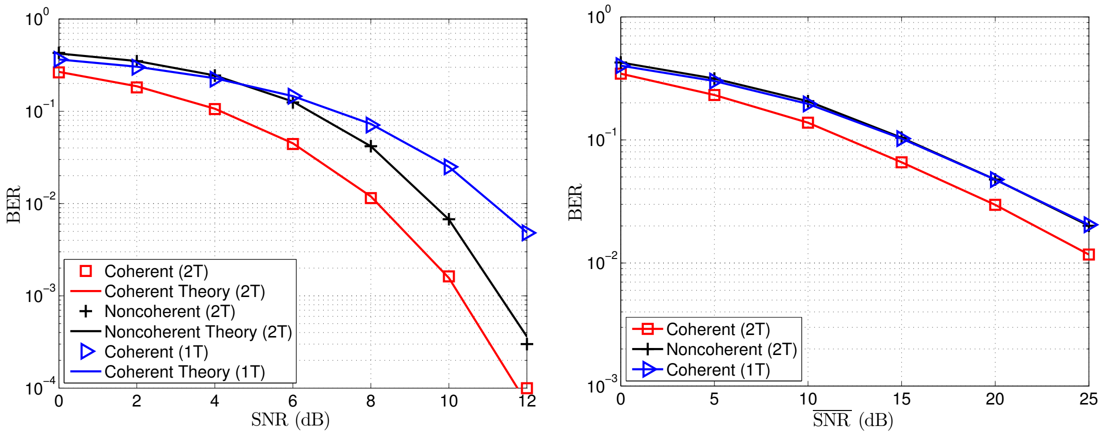
3.1.3 Performance

Fig. 3.3(a) shows the BER versus SNR for the three detection methods. The performace gain of the memory assisted detection is shown. Additionally, the advantage of coherent detection compared to noncoherent (broadly used in existing RFID systems) is also shown. It is remarked that coherent detection exploits already-offered preambles in Gen2 and thus, comes at no additional rate loss.

Fig. 3.3(b) shows the performance of the above detection methods with respect to the average received SNR. The avarage received SNR is defined as

$$\overline{\text{SNR}} = \mathbb{E}\{\text{SNR}\} = \frac{s^2|\Gamma_1 - \Gamma_0|^2 P_c}{4\sigma_n^2}\mathbb{E}[|a_{\text{ET}}|^2]\mathbb{E}[|a_{\text{TR}}|^2]L \tag{3.20}$$

In the simulation we have set $\mathbb{E}[|a_{\text{ET}}|^2] = \mathbb{E}[|a_{\text{TR}}|^2] = 1$.



(a) BER versus SNR

(b) BER versus $\overline{\text{SNR}}$.

Figure 3.3: Performance of detection methods.

3.2 Two Tag Model

In this section we study the communication between the reader and two tags. If two or more tags respond simultaneously, a collision occurs. In case of a two tag collision, the received digitized signal after DC offset estimation and removal is written as

$$y[k] \triangleq y(kT_s) = h_A x_A[k] + h_B x_B[k] + n[k] \tag{3.21}$$

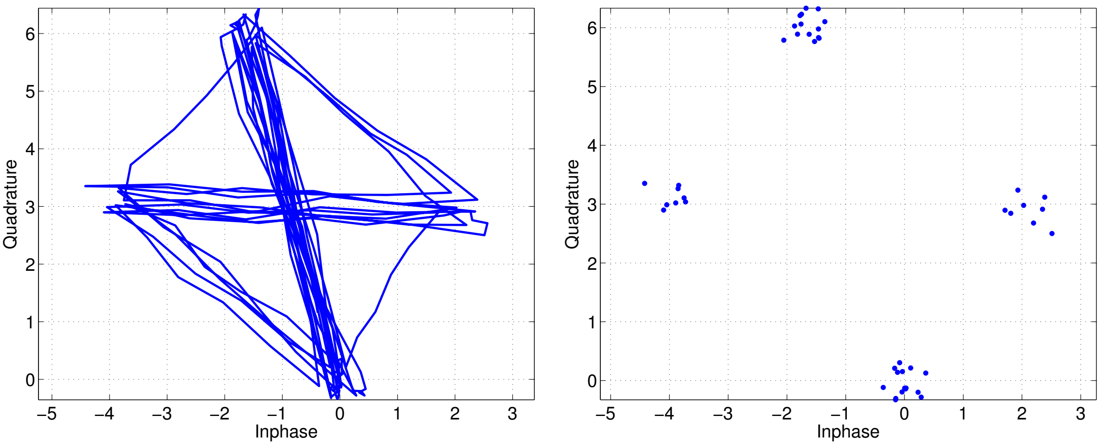
where

$$x_A[k] \triangleq \sum_{n=0}^{N} S^A_{d(n)}(kT_s - nL - \tau_A) \tag{3.22}$$

$$x_B[k] \triangleq \sum_{n=0}^{N} S^B_{d(n)}(kT_s - nL - \tau_B) \tag{3.23}$$

$S^A_{d(n)}$, $S^B_{d(n)}$ is the $n+1$th transmitted pulse for tag A and tag B respectively, $L = T/T_s$ is the oversampling factor denoting the number of samples of each transmitted pulse and $n[k] \triangleq n(kT_s) \sim \mathcal{CN}(0, 2\sigma_n^2)$.

Similar to the single tag case, there is no carrier frequency offset (CFO) as both signals are modulated using the same carrier wave and are jointly downconverted to baseband. According to the EPCglobal standard [7], symbol duration T can be adjusted between 1.5us and 25us with a maximum deviation of 24%. Thus the number of samples L may



(a) Received samples after matched filtering.

(b) Half bits after matched filtering and synchronization.

Figure 3.4: I/Q constellation diagram of two tag transmission using simulated data.

be different for the two colliding tags. Assuming that $\tau_A = 0, \tau_B = 0$ and nominal bit duration L i.e., synchronous transmission, each FM0 symbol observed with a $L/2$ shift can be written after synchronization and matched filtering as a 2×1 complex vector:

$$\mathbf{y} \triangleq \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = h'_A \mathbf{x}_A + h'_B \mathbf{x}_B + \mathbf{n}, \tag{3.24}$$

where $\mathbf{x}_A, \mathbf{x}_B \in \{\mathbf{e}_0 \triangleq [1\ 0]^T, \mathbf{e}_1 \triangleq [0\ 1]^T\}$ and $\mathbf{n} \sim \mathcal{CN}(0, L\sigma_n^2\mathbf{I}_2) \equiv \mathcal{CN}(0, \sigma^2\mathbf{I}_2)$. Equivalently,

$$\mathbf{y} = \mathbf{u} + \mathbf{n}, \tag{3.25}$$

where $\mathbf{u} \in \{\mathbf{u}_0 \triangleq [h'_A + h'_B\ 0]^T, \mathbf{u}_1 \triangleq [0\ h'_A + h'_B]^T, \mathbf{u}_2 \triangleq [h'_A\ h'_B]^T, \mathbf{u}_3 \triangleq [h'_B\ h'_A]^T\}$. We observe that in contrast to the single tag case, four symbols may exist in the received signal. Fig. 3.4(a) shows the received signal after matched filtering. Fig. 3.4(b) shows the received signal after synchronization and sampling. We have set SNR = 25db, $h_A = 0.43 + 0.58j$ and $h_B = -0.77 + 0.63j$. Four states can be observed in the I/Q constellation diagram.

The SNR is defined as

$$\text{SNR} = \frac{s^2|\Gamma_1 - \Gamma_0|^2 P_c}{4\sigma_n^2}\mathbb{E}[|a_{\text{ET}}^B|^2]\mathbb{E}[|a_{\text{TR}}^B|^2]L \tag{3.26}$$

3.2.1 Detection with Perfect Channel State Information

A reader can acknowledge only a single tag even if it is able to resolve a collision and detect the transmitted sequences of both tags. Thus, we study the performance of different detection methods for two cases: (a) when we are interested in decoding tag A, (b) when we are interested in decoding the strongest tag.

3.2.1.1 Ignore Weaker Tag

An intuitive solution to resolve the collision would be to ignore the weaker tag and detect only the strongest. Given that the receiver has estimates of h'_A or h'_B, it can perform single tag maximum likelihood (ML) detection ignoring the weaker tag. The ML rule for tag A is

$$\Re(h'_A(y_1 - y_0)) \underset{S_0}{\overset{S_1}{\gtrless}} 0 \tag{3.27}$$

3.2.1.2 Optimal ML Detection

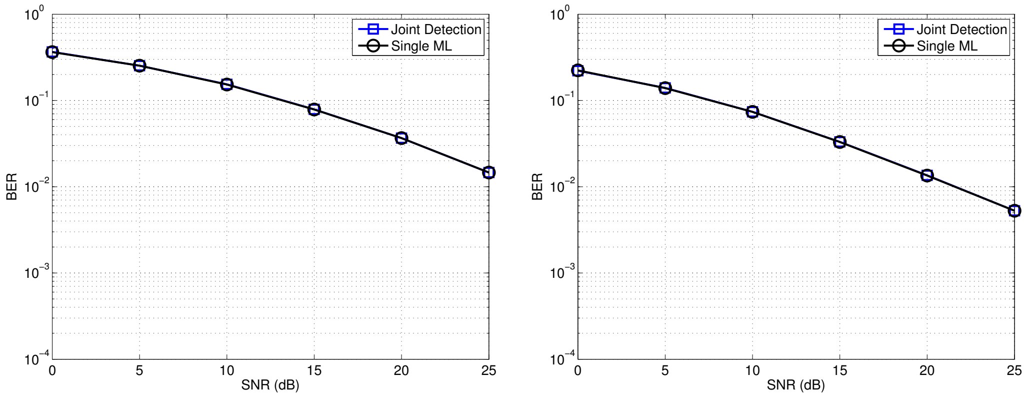
The optimal maximum a posteriori (MAP) detector minimizes the bit error rate (BER) for tag A. For equiprobable transmitted symbols the MAP detector reduces to the ML detector. The ML estimate of $\mathbf{x}_A$ is

$$\begin{aligned} \hat{\mathbf{x}}_A &= \underset{\mathbf{x}_A \in \{[1\ \ 0]^T, [0\ \ 1]^T\}}{\text{argmax}} \; f(\mathbf{y}|\mathbf{x}_A, h'_A, h'_B) && (3.28) \\ &= \underset{\mathbf{x}_A \in \{[1\ \ 0]^T, [0\ \ 1]^T\}}{\text{argmax}} \sum_{\mathbf{x}_B \in \{[1\ \ 0]^T, [0\ \ 1]^T\}} \frac{1}{2} \, f(\mathbf{y}|\mathbf{x}_A, \mathbf{x}_B, h'_A, h'_B) && (3.29) \end{aligned}$$

Thus the ML rule is written as

$$\begin{gathered} \exp\left\{-\frac{1}{\sigma^2}\left\|\mathbf{y} - \begin{bmatrix} h'_A + h'_B \\ 0 \end{bmatrix}\right\|^2\right\} + \exp\left\{-\frac{1}{\sigma^2}\left\|\mathbf{y} - \begin{bmatrix} h'_A \\ h'_B \end{bmatrix}\right\|^2\right\} \underset{S_1}{\overset{S_0}{\gtrless}} \\ \exp\left\{-\frac{1}{\sigma^2}\left\|\mathbf{y} - \begin{bmatrix} 0 \\ h'_A + h'_B \end{bmatrix}\right\|^2\right\} + \exp\left\{-\frac{1}{\sigma^2}\left\|\mathbf{y} - \begin{bmatrix} h'_B \\ h'_A \end{bmatrix}\right\|^2\right\} \end{gathered} \tag{3.30}$$

Notice that the optimal detector requires knowledge of noise variance.



(a) BER at tag A when $\mathbb{E}[|h'_A|^2] = \mathbb{E}[|h'_B|^2]$. (b) BER at tag A when $E\{|h'_A|^2\} = 4E\{|h'_B|^2\}$.

Figure 3.5: BER at tag A with perfect channel state information.

3.2.1.3 Joint ML Detection

The joint ML detection that minimizes BER of the two received signals is written as follows

$$\hat{\mathbf{x}}_A, \hat{\mathbf{x}}_B = \underset{\mathbf{x}_A, \mathbf{x}_B \in \{[1\ \ 0]^T, [0\ \ 1]^T\}}{\operatorname{argmax}} f(\mathbf{y}|\mathbf{x}_A, \mathbf{x}_B, h'_A, h'_B) \tag{3.31}$$

The ML rule can be equivalently expressed as a minimum distance rule

$$\hat{\mathbf{x}}_A, \hat{\mathbf{x}}_B = \underset{\mathbf{x}_A, \mathbf{x}_B \in \{[1\ \ 0]^T, [0\ \ 1]^T\}}{\operatorname{argmin}} \|\mathbf{y} - h'_A \mathbf{x}_A - h'_B \mathbf{x}_B\|^2 \tag{3.32}$$

This detector selects the constellation point $\mathbf{u}_i$, $i \in \{0, 1, 2, 3\}$ which is closer to the observation vector $\mathbf{y}$. The optimal ML detector and joint ML detector practically coincide [20].

3.2.2 Performance

We compute BER performance of the detection methods when we are interested only in decoding tag A. In Fig. 3.5(a) tag A and tag B have the same average power. In Fig.3.5(b) tag A is 6dB stronger than tag B. We assume that $h'_A = h^A_{\text{ET}} h^A_{\text{TR}}$, $h'_B = h^B_{\text{ET}} h^B_{\text{TR}}$ where h^A_{ET}, h^A_{TR}, h^B_{ET}, h^B_{TR} are independent channel coefficients and follow circularly symmetric complex Gaussian distribution.

In a real-world scenario we are interested in decoding one out of the two tags. Thus, we present the performance of the three algorithms when we have perfect knowledge of the channel coefficients h'_A, h'_B and decode the strongest of the two tags. Fig. 3.6 shows the performance of the three detection methods when we are interested in the strongest tag. We repeat the above experiments and compute the packet error rate (Fig. 3.7).

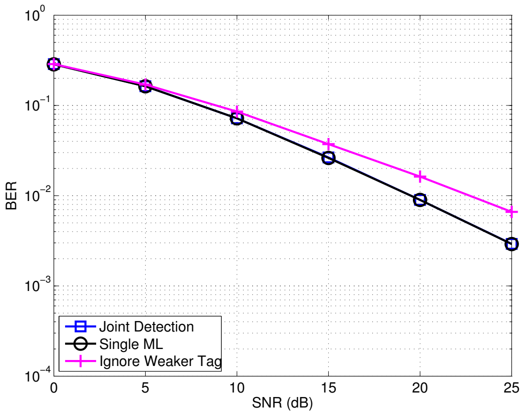
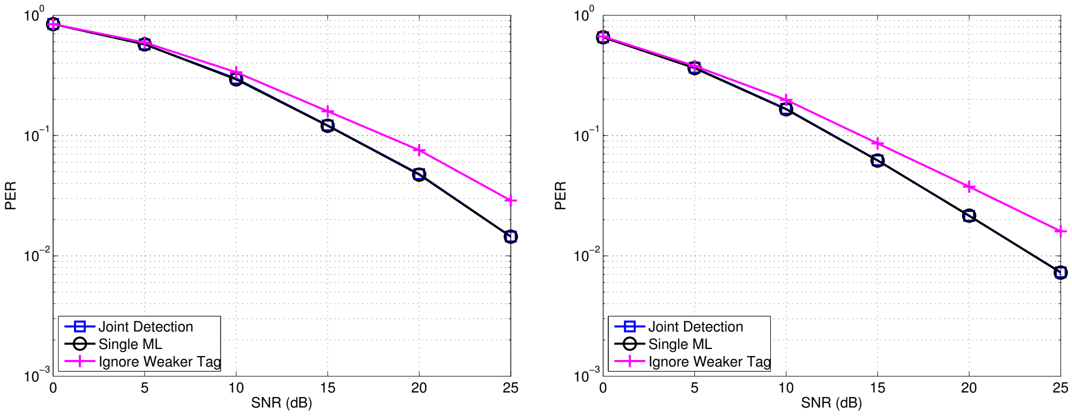


Figure 3.6: BER at strongest tag when $E\{|h'_A|^2\} = E\{|h'_B|^2\}$.



(a) PER when $E\{|h'_A|^2\} = E\{|h'_B|^2\}$.

(b) PER when $E\{|h'_A|^2\} = 4E\{|h'_B|^2\}$.

Figure 3.7: PER at strongest tag with perfect channel state information.

3.2.3 Detection with Partially Known Channel State Information

The above described detection methods cannot be directly applied in a real-world scenario because we do not have an estimate for the individual channel coefficients h'_A, h'_B. We discuss three possible methods for acquiring these channel estimates and then perform joint ML detection.

3.2.3.1 Channel Estimation with Projections

Let $\mathbf{y}_{1:N}$ be the received sequence of FM0 symbols that follow the preamble. We use a modified version of the method proposed in [23] for channel estimation where it was assumed that there are synchronization errors between the tags.

The algorithm is based on the observation that two states of the total four states are realized during the transmission of the preamble defining an one-dimensional subspace s_p (line). Projecting the received half bits onto the subspace orthogonal to s_p will give a non-zero value if the corresponding half bit is equal to h'_A or h'_B. The authors in [23] search for points that have the maximum signal strength in this orthogonal subspace. More specifically they process the received waveform after matched filtering y_f (Fig. 3.4(a)) and set

$$k_A = \underset{k \in \{0,1,2,\dots,NL\}}{\operatorname{argmax}} \ \Im\{y_f[k]e^{-j\underline{/h_A + h_B}}\} \tag{3.33}$$

$$k_B = \underset{k \in \{0,1,2,\dots,NL\}}{\operatorname{argmin}} \ \Im\{y_f[k]e^{-j\underline{/h_A + h_B}}\} \tag{3.34}$$

and use $y_f[k_A]$ and $y_f[k_B]$ as the channel estimates. It is explicitly underlined that the received signal cannot be jointly sampled using the nominal symbol duration L and thus process FM0 symbols.

However timing errors are not critical when tags operate using the minimum backscatter link frequency (BLF). We apply the proposed method in case of synchronous tag transmission. In addition taking into account the FM0 encoding, we can search for a symbol $\mathbf{y}$ that maximizes the following metric

$$k^* = \underset{k \in \{1,2,\dots,16\}}{\operatorname{argmax}} \ |\Im\{\mathbf{y}_k[0]e^{-j\underline{/h_A + h_B}}\} - \Im\{\mathbf{y}_k[1]e^{-j\underline{/h_A + h_B}}\}| \tag{3.35}$$

where $\Im\{\mathbf{y}_k[0]e^{-j}\underline{/h1 + h2}\}$,$\Im\{\mathbf{y}_k[1]e^{-j}\underline{/h1 + h2}\}$ are the projections of $\mathbf{y}_k[0]$ and $\mathbf{y}_k[1]$ onto $s_{p\perp}$. We then set $\hat{h}'_A = \mathbf{y}_{k^*}[0]$, $\hat{h}'_B = \mathbf{y}_{k^*}[1]$. It is insignificant if we exchange the estimates of the channel coefficients.

3.2.3.2 Channel Estimation with Enumeration

The above method was based on locating a symbol of the received signal and use it as an estimate for the two channel coefficients. Instead of searching for a symbol maximizing the projection, we find one that maximizes the conditional probability density function (pdf).

```
for each received symbol $\mathbf{y}_k$ do
  set $\hat{h}'_A = \mathbf{y}_k[0]$, $\hat{h}'_B = \mathbf{y}_k[1]$
  $\mathbf{x}^*_{A(1:N)}, \mathbf{x}^*_{B(1:N)} = \underset{\mathbf{x}_{A(1:N)}, \mathbf{x}_{B(1:N)}}{\text{argmax}} \ln[f(\mathbf{y}_{1:N}|\hat{h}'_A, \hat{h}'_B, \hat{h}', \mathbf{x}_{A(1:N)}, \mathbf{x}_{B(1:N)})]$
  $l = \ln[f(\mathbf{y}_{1:N}|\hat{h}'_A, \hat{h}'_B, \hat{h}', \mathbf{x}^*_{A(1:N)}, \mathbf{x}^*_{B(1:N)})]$
  if $l > best$ then
    $best = l, \mathbf{x}^b_{A(1:N)} = \mathbf{x}^*_{A(1:N)}, \mathbf{x}^b_{B(1:N)} = \mathbf{x}^*_{B(1:N)}$
  end if
end for
```

We have assumed that an estimate $\hat{h}'$ that corresponds to $h_A + h_B$ has been acquired using the preamble.

3.2.3.3 Channel Estimation with Clustering

Under the assumption of perfectly synchronized tags, four half bits $(h'_A + h'_B, h'_A, h'_B, 0)$ are observed after matched filtering. For example under hypothesis $\mathbf{u}_0$

$$\mathbf{y} = \begin{bmatrix} h'_A + h'_B + n_0 \\ n_1 \end{bmatrix} \tag{3.36}$$

where $\mathbf{n} \sim \mathcal{CN}(0, \sigma^2\mathbf{I}_2)$. We estimate $h'_A + h'_B$ using the known preamble and study each half bit independently. Given that both tags reflect i.e., $\mathbf{y}[0] = h'_A + h'_B + n_0$ we have that

$$x = |\mathbf{y}[0] - (h'_A + h'_B)|^2 = |n_0|^2 \sim \exp(\lambda), \lambda = \frac{1}{\sigma^2} \tag{3.37}$$

We want the probability of the event that x is larger than a threshold d to be smaller than ϵ.

$$P(x > d) = \epsilon \Leftrightarrow 1 - F_x(d) = \epsilon \tag{3.38}$$

The cumulative distribution function $F_x(d)$ is given by

$$F_x(d) = 1 - e^{-\frac{d}{\sigma^2}} \tag{3.39}$$

Using Equations 3.38,3.39 we can compute d as follows

$$\begin{aligned} P(x > d) &= \epsilon \\ 1 - (1 - e^{-\frac{d}{\sigma^2}}) &= \epsilon \\ e^{-\frac{d}{\sigma^2}} &= \epsilon \\ d &= \sigma^2 \ln \frac{1}{\epsilon} \end{aligned} \tag{3.40}$$

Given that both tags absorb i.e., $\mathbf{y}[0] = n_0$ we have that

$$y = |\mathbf{y}[0]|^2 = |n_0|^2 \sim \exp(\lambda), \lambda = \frac{1}{\sigma^2} \tag{3.41}$$

Thus, can exclude a half bit if $x < d$ or $y < d$ (it probably belongs to a $\mathbf{u}_0$ or $\mathbf{u}_1$ symbol). Remaining half bits will belong with high probability to either $\mathbf{u}_2$ or $\mathbf{u}_3$. We can then perform K-means clustering with $K = 2$ and set $\hat{h}'_A$, $\hat{h}'_B$ equal to the two cluster heads.

Instead of studying each half bit independently, we observe that under hypothesis $\mathbf{u}_0$

$$\mathbf{y}[0] - \mathbf{y}[1] \sim \mathcal{CN}(h'_A + h'_B, 2\sigma^2) \tag{3.42}$$

while under $\mathbf{u}_1$

$$\mathbf{y}[0] - \mathbf{y}[1] \sim \mathcal{CN}(-(h'_A + h'_B), 2\sigma^2) \tag{3.43}$$

Given that the transmitted symbol is $\mathbf{u}_0$

$$x = |(\mathbf{y}[0] - \mathbf{y}[1]) - (h'_A + h'_B)|^2 \sim \exp(\lambda), \lambda = \frac{1}{2\sigma^2} \tag{3.44}$$

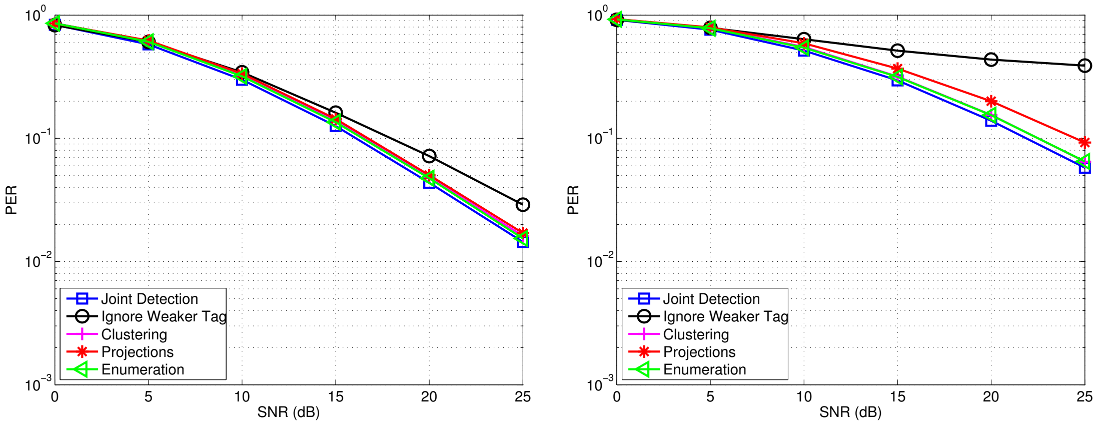
Given that the transmitted symbol is $\mathbf{u}_1$

$$y = |(\mathbf{y}[0] - \mathbf{y}[1]) + (h'_A + h'_B)|^2 \sim \exp(\lambda), \lambda = \frac{1}{2\sigma^2} \tag{3.45}$$

Working similarly, we can exclude a symbol $\mathbf{y}$ if $x < d$ or $y < d$ and then perform K-means clustering with the remaining half bits with $K = 2$ and set $\hat{h}'_A$, $\hat{h}'_B$ equal to the two cluster heads.

3.2.4 Performance

Fig. 3.8(a) and Fig. 3.8(b) show the performance of the proposed methods with respect to packet error rate (PER) compared to the joint detection algorithm with perfect CSI when we are interested only in decoding one and both tags respectively.



(a) A packet error occurs when both tag responses are incorrect.

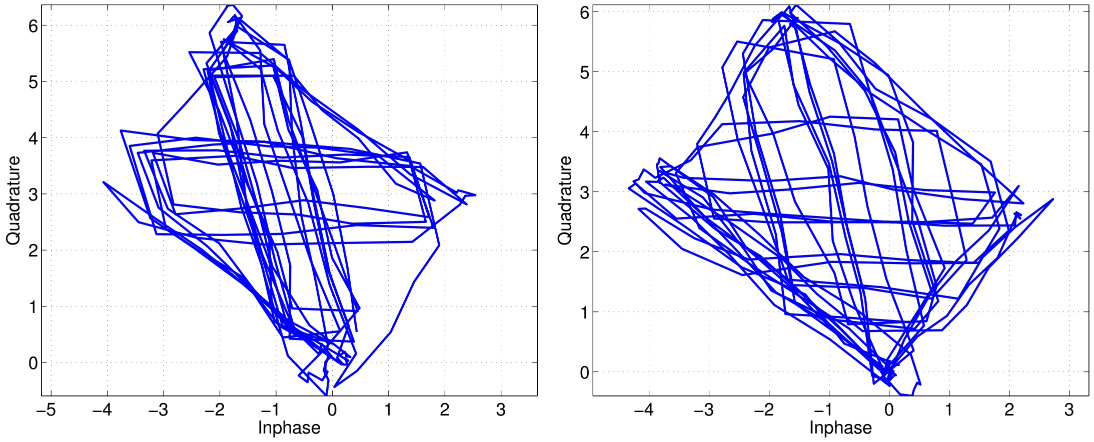
(b) A packet error occurs when at least one tag response is incorrect.

Figure 3.8: PER of different channel estimation methods when $E\{|h'_A|^2\} = E\{|h'_B|^2\}$.

3.3 Impact of Synchronization Errors

There are two sources of errors regarding the synchronization between tags transmissions. The most important factor (that was observed obtaining measurement data) is the different time instant that the two tags start transmitting. Another factor that causes timing errors is the different BLF among different tags.

Table 2.6 shows the nominal, minimum and maximum values for the timing parameters. When working on the minimum BLF frequency of 40KHz $T_1^{min} = 238$us and $T_1^{max} = 262$us. T_{pri} is the period duration equal to 25us. That means that a tag may start transmitting when the first tag has already sent its first bit. Let τ_A, τ_B denote the delay of tag A and B respectively. We assume that the reader can estimate τ_A. Fig. 3.9(a) shows the constellation diagram of a two-tag transmission when $\tau_B - \tau_A = 10\%L$ $(L = T/T_s)$.



(a) Received samples after matched filtering when $\tau_B - \tau_A = 10\%L$.

(b) Received samples after matched filtering when $L_B = L + 20\%L$.

Figure 3.9: Received signal when synchronization errors occur.

Assuming that frame synchronization is performed with respect to the first tag and that $\tau_A - \tau_B = \alpha L/2$ where $0 \leq \alpha \leq 1$, the output of the matched filter is given by

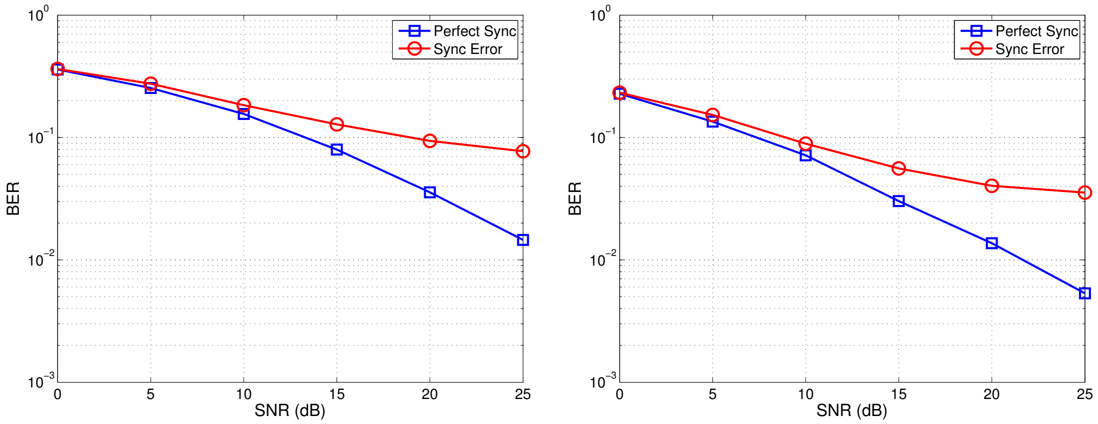
$$\mathbf{y}_k[0] = \frac{L}{2} h_A \mathbf{x}_A^k[0] + \alpha \frac{L}{2} \mathbf{x}_B^{k-1}[1] + (1-\alpha)\frac{L}{2}\mathbf{x}_B^k[0] \tag{3.46}$$

$$\mathbf{y}_k[1] = \frac{L}{2} h_A \mathbf{x}_A^k[1] + \alpha \frac{L}{2} \mathbf{x}_B^{k}[0] + (1-\alpha)\frac{L}{2}\mathbf{x}_B^k[1] \tag{3.47}$$

The impact of synchronization error on the performance of the joint ML detection is shown in Fig. 3.10. We have set $\tau_A - \tau_B = 10\%L$.

Fig. 3.9(b) shows the matched filter output when both synchronization errors are present; i.e., the tags start modulating at different time instants with a different data rate. To deal with this problem we propose an approach based on correlation bank similar to that of [24]. We focus on the decoding of the strongest tag. Two parameters need to be estimated τ and L. The received signal is correlated with a bank of different preamble sequences. The pair that maximized the normalized correlation is chosen as the estimate for the parameters τ and L.

$$\hat{L}, \hat{\tau} = \underset{L,\tau}{\text{argmax}}\ corr(L,\tau) = \frac{\left|\sum_{n=0}^{N_p^L-1} s_p^L[n] y[\tau+n]\right|}{\|\mathbf{s}_p^L\|}, \tag{3.48}$$



(a) BER at tag A when $\mathbb{E}[|h'_A|^2] = \mathbb{E}[|h'_B|^2]$. (b) BER at tag A when $E\{|h'_A|^2\} = 4E\{|h'_B|^2\}$.

Figure 3.10: Impact of synchronization error at tag A. Joint detection is performed.

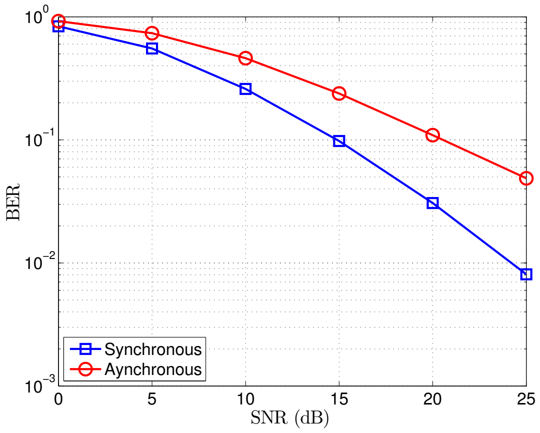


Figure 3.11: Performance of detection method using correlation bank.

where $\mathbf{s}_p^L$ is a preamble sequence where the length of each bit is equal to L. We performed simulations to test the performance of the correlation based method. Each tag selects uniformly its symbol period in the interval $[L - 4\%,\ L + 4\%]$ where L is the nominal symbol period. The reader correlates the received signal with the preamble sequences. After estimating the parameters τ, L, it performs single tag detection ignoring the second tag. The performance of the detection method is shown in Fig. 3.11.

Chapter 4

Reader Architecture

4.1 Hardware

A commodity USRP N200 software defined radio (SDR) is utilized, equipped with a single RFX900 daughterboard and a laptop. The transmit and receive ports of the RFX900 daughterboard are connected with two circularly-polarized antennas, one for transmitting reader commands and one for capturing tag's reply in full duplex mode. The circularly-polarized antennas have a 7dBic gain.

The universal software radio peripheral (USRP) platform is a software-defined radio designed by Ettus Research. USRPN200 includes a Spartan FPGA, 100 MS/s dual ADC, 400 MS/s dual DAC and connects to a PC using Gigabit Ethernet for streaming data. The host code that provides functions for communicating and programming the USRP is called universal hardware driver (UHD).

The RFX900 is a transceiver designed specifically for operation in the 900 MHz band. It has a typical power output of 200 mW, 8 dB noise figure. It supports full duplex mode; i.e. simultaneous transmission and reception. Without any modifications the RFX900 covers the frequency range between $900 - 920$ MHz. However, by replacing the ISM filter in the transmission path with a 100 pF capacitor, the daughterboard can cover the whole frequency band for RFID communication. The modification also increases the output power to 500 mW.

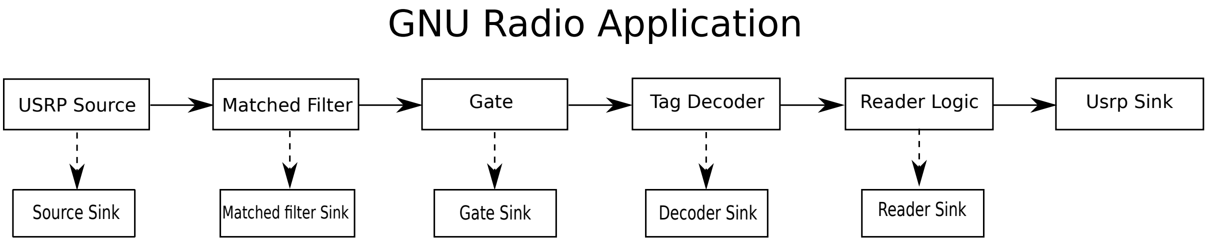


Figure 4.1: SDR Reader Architecture.

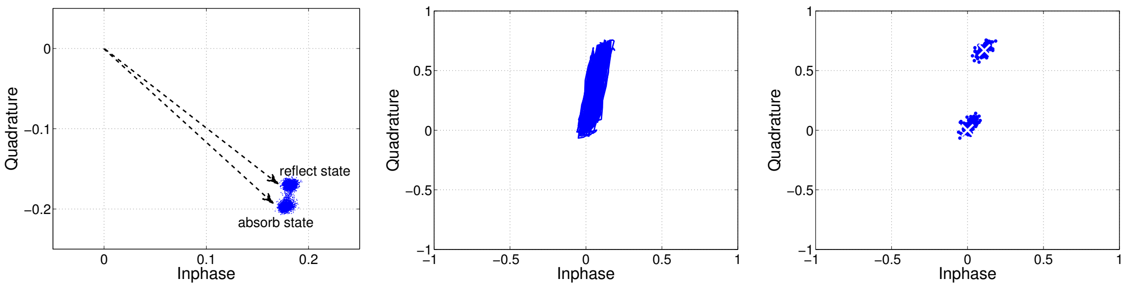
4.2 Software

The developed readers are built on top of GNU Radio. GNU Radio is a free software development toolkit that provides signal processing blocks to implement software-defined radios. It can be used both with RF hardware such as USRP, or in a simulation environment. GNU Radio also provides a framework that defines how different blocks are connected together and controls the flow of the data from one block to another. Two types of scheduler exist; single-threaded scheduler (STS) and thread-per-block scheduler (TBS). Applications are developed in Python and consist of two or more blocks that are written in C++. Each application should have at least one block declared as source that produces data and one block as sink which consumes data. The most recent version of GNU Radio is v3.7.

4.3 Gen2 UHF RFID Reader

The Gen2 reader architecture follows the six-block structure of [8]. It consists of the following blocks: USRP source, Matched Filter, Gate, Tag Decoder, Gen2 Logic and USRP sink (Fig. 4.1). Each processing block is connected with a buffer (File sink) and stores its output for debug purposes.

- **USRP source**: The first block is called USRP source and is responsible for the acquisition of samples from the USRP. The ADC is configured at 2MS/s and thus, each tag bit consists of $L = 50$ samples. The inphase and quadrature components of a received tag EPC message are shown in Fig.4.2(a). Two arbitrary I/Q states appear in the constellation diagram corresponding to the two tag states.



(a) Received samples.

(b) Received samples after matched filtering and DC offset removal.

(c) Received samples after symbol period estimation and synchronization.

Figure 4.2: I-Q constellation diagram of a tag's EPC response using measurement data

- **Matched Filter**: The Matched Filter block is responsible for filtering the received signal with a square pulse of length $L/2 = 25$. The signal is also downsampled by a factor of 5 to reduce computation cost.

- **Gate**: The Gate block is responsible for identifying the reader queries (since the reader is full duplex, transmitting and receiving simultaneously); by tracking the amplitude of the received signal the reader is able to identify the transmitted commands, and thus process only samples that follow and correspond to the tag's response. Immediately after a reader command has ended, the block estimates the DC offset component and removes it from each sample. These samples are given as input to the next block for further processing. Fig. 4.2(b) shows the output of Gate block for an EPC tag message, with DC component removed.

- **Tag Decoder**: The Tag Decoder block is responsible for the frame synchronization, channel estimation and detection of the tag responses. Synchronization for the RN16 and tag's ID (EPC) sequences is performed by correlating the received signal with the known preamble. Then channel estimation is performed as described in Section 3.1.1. A major problem in RFID readers is the variation in the tag's nominal bit duration, which can differ up to 22% from the nominal value depending on the selected data rate. The reader in this work operates at the minimum data rate (40KHz), where these variations are not critical. Error in symbol level synchronization was observed in some cases, when decoding the tag ID (EPC) plus

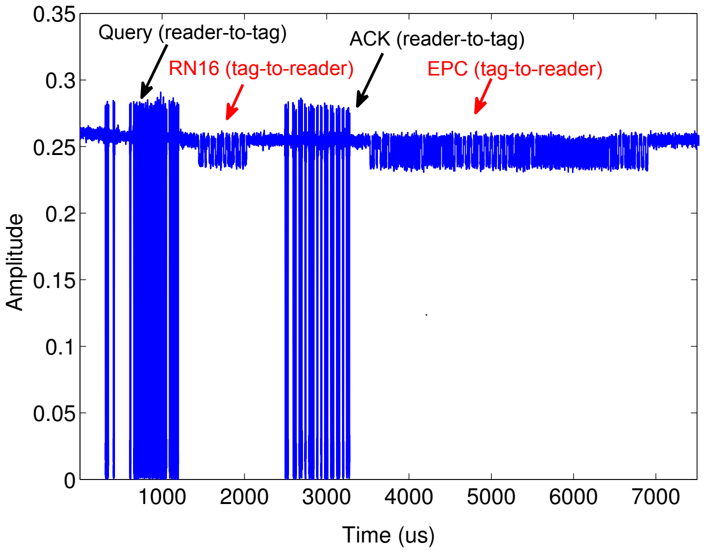


Figure 4.3: Gen2 frame captured by the developed reader.

CRC and were due to the large sequence size (135 bits). That problem did not occur in the shorter RN16. To deal with that synchronization problem, an initial sampling instant τ^* is obtained, by correlating with the preamble; then the symbol rate T and thus, the right sampling instants are chosen, such that signal energy is maximized:

$$T^* = \underset{T}{\operatorname{argmax}} \sum_{n=0}^{2(N-1)} \left| y_f \left[\tau^* + n\frac{T}{2} \right] \right|^2, \tag{4.1}$$

where N is the number of transmitted bits that follow the preamble sequence and y_f the received signal after matched filtering and DC offset removal. The received signal is then sampled at the end of each half symbol period. Fig. 4.2(c) shows the I/Q constellation diagram after frame synchronization, symbol period estimation and sampling. The channel estimate is marked with an x mark. Next, tag decoding is performed.

- **USRP sink**: Depending on the output of the tag decoder block, the reader creates the next command and propagates it to the transmit chain. Currently the commands supported by our reader are the Query, ACK and QueryRep commands. The DAC rate is configure to 1 MS/s.

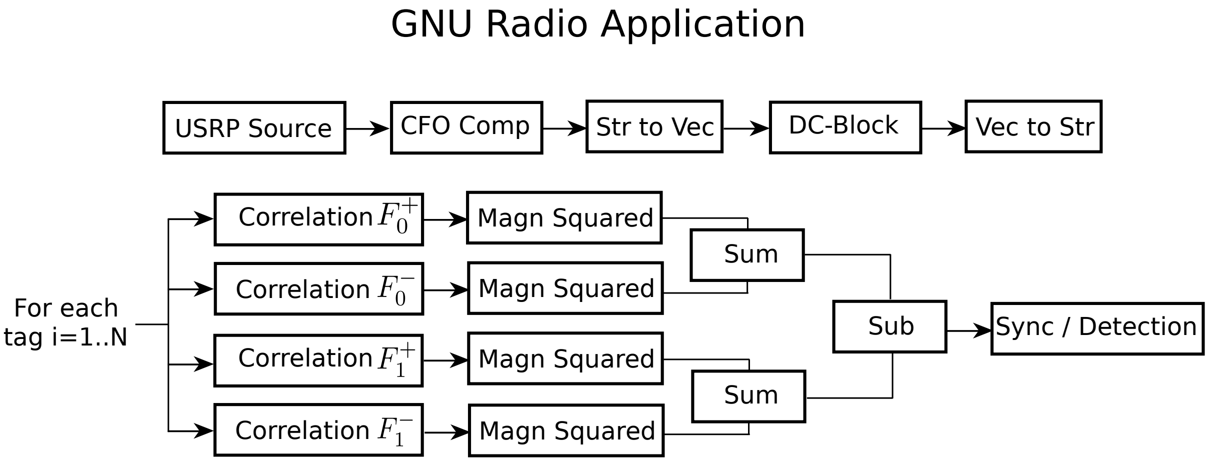


Figure 4.4: SDR Reader Architecture for WSN.

4.4 Reader for Backscatter Sensor Network

The implemented reader for the bistatic backscatter network follows a different architecture shown in Fig. 4.4. It consists of the following blocks. A more detailed description of the implemented algorithm is given in [3].

- **USRP Source**: The first block is called USRP source and is responsible for the acquisition of samples from the USRP. The ADC is configured at 1MS/s and thus, each tag bit consists of $L = 1000$ samples.

- **CFO Comp**: The second block is responsible for CFO compensation. The CFO is estimated by finding the periodogram peak (which corresponds to the transmitted carrier). CFO term is cancelled by shifting the periodogram to DC.

- **Str to Vec**: The input stream is converted to a vector (packet).

- **DC-Block**: DC-blocking is implemented by estimating and removing the received signal's mean value.

- **Vec to Str**: The vector is converted again to a stream.

- **Correlation**: Matched filtering is performed with the two sub-carriers for each frequency. The convolution is implemented in the frequency domain using the GNU Radio block filter.fft_filter_ccc.

- **Magn Squared**: The block computes the squared magnitude of each sample.
- **Sum**: The block takes as input pairs of samples and performs addition.
- **Sub**: The block takes as input pairs of samples and performs subtraction.
- **Sync/Decode**: The last block is responsible for locating the preamble and detecting the transmitted bits.

Chapter 5

Experimental Results

In this chapter we present the results of our work. We perform four different experiments studying the performance of the reader in terms of reading rate and range. In addition we compare in practice two detection methods as well as a collision recovery algorithm. We used an RFX900 daughterboard with two circularly-polarized antennas with a gain of 7 dBic.

5.1 Performance of Detection Methods

In the first experiment one tag was placed approximately 1.5 m away from the reader. We set the number of slots equal to 1 and set the number of queries to 5000. We run the application configuring the reader to perform coherent detection and noncoherent detection. We repeated the above experiment for different transmission power values. The results are shown in Fig. 5.1. After each experiment we computed the success ratio.

$$\text{Success Ratio} = \frac{\text{Number of correctly decoded EPC}}{\text{Number of queries}} \tag{5.1}$$

We observe that when the transmission power is low, the reader is able to correctly decode 20 % more EPC messages using coherent detection. Increasing the transmission power, the gap in the performance of the two detection methods decreases.

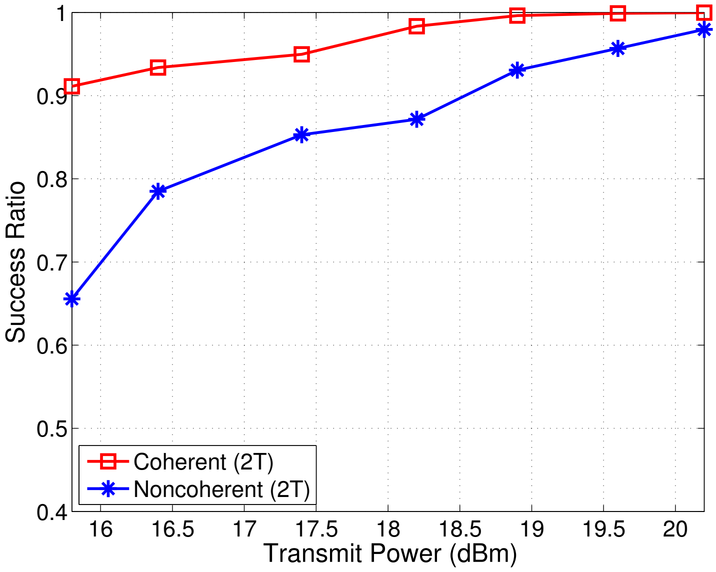


Figure 5.1: Performance of detection methods: experimental results

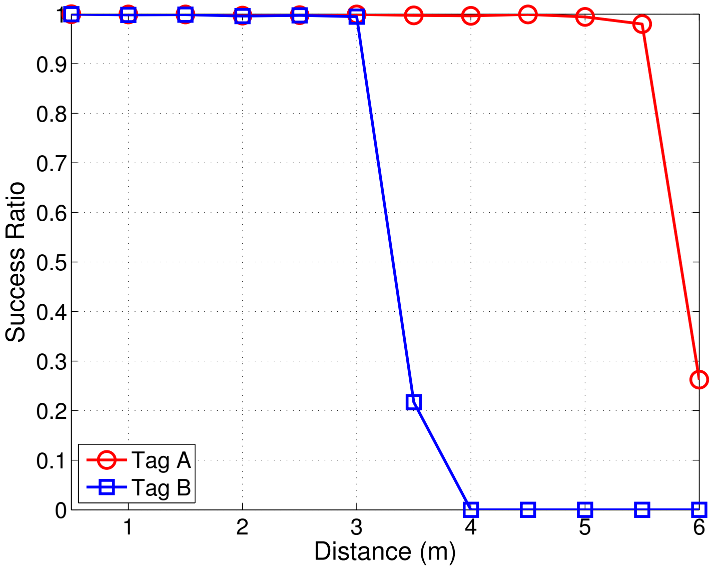


Figure 5.2: Range performance of reader.

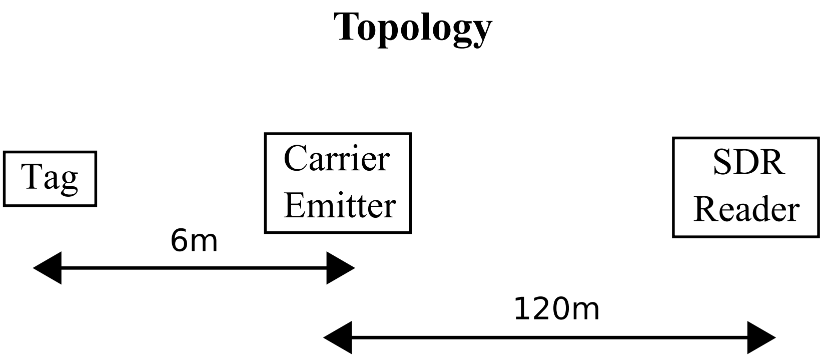


Figure 5.3: Experimental setup for WSN reader.

5.2 Range Measurements

In the second experiment we studied the read range of the developed reader. We set the RX gain to 20 dB, the transmit power to 22.75 dBm. One commercial UHF RFID tag was placed in front of the reader at different distances. At each distance the reader issued 2000 queries and measured the success ratio. The above experiment was repeated using a different type of RFID tag. The results are shown in Fig. 5.2. We observe that the success ratio is nearly 100 % up to a 6 meters and 3 meters for tag A and tag B respectively. After a certain distance the two tags stop being energized.

Ranging measurements were also conducted for the reader for the backscatter WSN 5.3. A carrier emitter was used with 13 dBm transmission power configured at 867 MHz. A semi-passive RF tag was used to modulate the reflected CW with FSK modulation at 1 kbps bit-rate. Omnidirectional antennas were employed on both emitter, tag and SDR reader. The emitter was placed at approximately 120 m away from the reader. The tag was placed 6 m further away in the same direction. We observed nearly optimal detection verifying that a semi passive tag with a bistatic configuration can achieve increased communication ranges compared with a passive tag with a monostatic configuration.

5.3 Reading Rate

We evaluated the reader with respect to the reading rate. In the third experiment, 16 Gen2 tags were attached to books in a bookcase, 1.5 meters away for the reader antennas, as shown in Fig. 5.4. Number of slots per round was set equal to the number of tags.

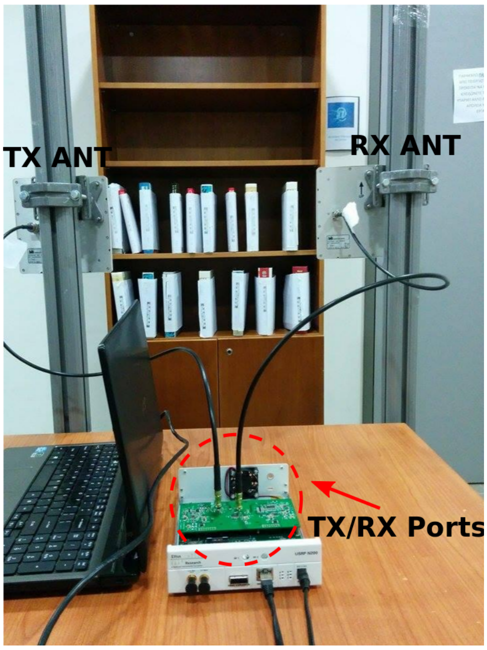
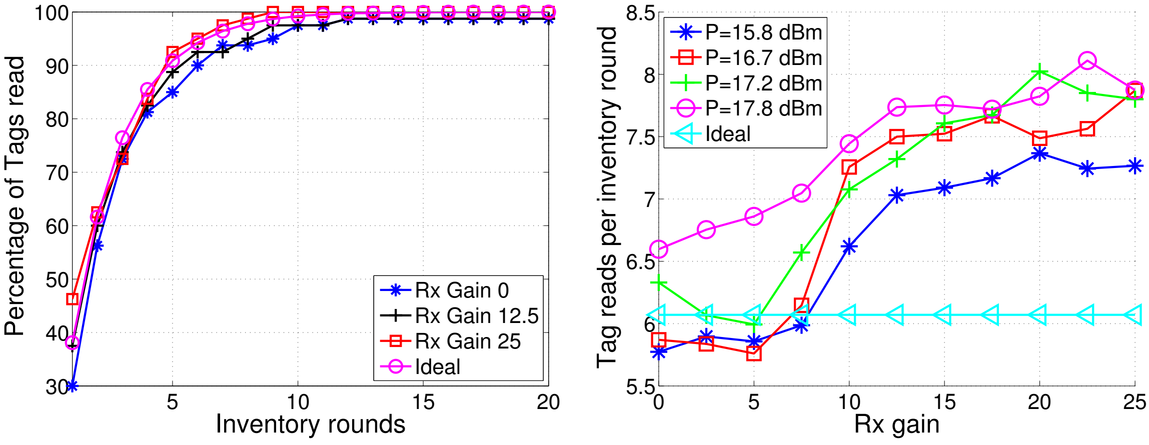


Figure 5.4: Experimental setup.

Reader query command was configured such that a tag replied in each inventory round, regardless of whether it had already been read. The total number of inventory rounds was set to 60 thus, offering a total number of $60 * 16 = 960$ slots. Experiments were repeated for various levels of transmission power at $15.8, 16.7, 17.2$ and 17.8 dBm.

Fig. 5.5(a) shows the percentage of identified tags when the signal transmission power was 17.8 dBm. In the same Figure we present the performance of an ideal reader which can perfectly decode single tag slots. We observe that the performance of the reader is increased while we increase the receiver gain and reaches the performance of the ideal reader. The reading rate is above the expected due to the capture effect i.e slots of collided tag signals can be decoded when there is a significant power difference between them.

Fig. 5.5(b) shows the reading rate of the reader. The theoretical throughput (reads per round), when the number of slots is equal to the number of tags, is $\rho = N\left(1 - \frac{1}{N}\right)^{N-1} = 6.08$, when $N = 16$ [20].



(a) Reading rate vs round.

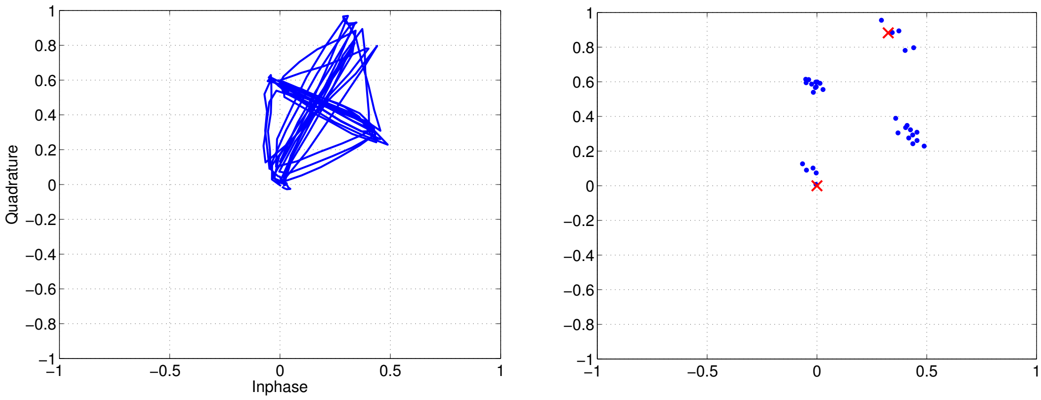
(b) Reading rate vs gain.

Figure 5.5: Reading rate vs time and tx power.

5.4 Collision Recovery

To verify whether joint detection can be applied to decode commercial UHF RFID tags, we conducted the following experiment using our SDR RFID reader. Ten different pairs of RFID tags were placed 1.5m away from reader and 2000 inventory rounds of one slot were carried out leading to two tag collisions. Single tag (ignore second tag) and joint ML detection were alternatingly used for the detection of the RN16 sequence. The performance of the two schemes was evaluated in terms of the number of correctly decoded EPC responses.

Fig. 5.6(a) shows the output of the gate block after simultaneous transmission of two tags. We can observe the transition between four possible states. Fig. 5.6(b) shows the output of the decoder block after symbol period estimation and sampling. Table 5.1 shows the results of the experimental measurements. It is verified that the joint ML detection scheme achieves better success ratio performance compared to the single tag detection. The use of two-tag anti-collision algorithm can increase significantly the reading rate.



(a) Received samples after matched filtering

(b) Received samples after matched filtering and sampling

Figure 5.6: I/Q constellation diagram using experimental data.

Table 5.1: Ratio of correctly decoded EPC responses for 10 pairs of tags

Algorithm	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
Ignore second tag	90%	61.8%	62.2%	86.4%	86%	45.1%	87.6%	54.1%	87.5%	82.1%
Joint ML	99.6%	66.4%	72.8%	96.6%	96.2%	68.3%	88.8%	80.2%	92.3%	92.9%

Chapter 6

Conclusions

This work developed a Gen2 UHF RFID reader using the USRP SDR platform and GNU Radio framework. A thorough description of the SDR signal processing was presented. The Gen2 reader can be found online at [25]. It is the only available GNU Radio compliant software that can be used to study commercial RFID systems.

In addition the two tag collision problem was studied. The two tag system model is described and verified using experimental measurements. We present difficulties that arise in a real world system and propose possible solutions to overcome them. Experimental results show that collision recovery algorithms have the potential to increase the performance of RFID systems.

Finally the implementation of a reader for a bistatic backscatter network is described. The reader is able to detect multiple tags that use binary FSK modulation in real time. Experiments have shown that the reader can identify semi-passive tags up to 130 m.

Bibliography

[1] H. Stockman, “Communication by means of reflected power,” in *Proc. IRE*, Oct 1948, pp. 1196–1204. 1

[2] G. Vannucci, A. Bletsas, and D. Leigh, “Implementing backscatter radio for wireless sensor networks,” in *Proc. IEEE Personal, Indoor and Mobile Radio Commun.*, Sep. 2007, pp. 1–5. 1

[3] J. Kimionis, A. Bletsas, and J. N. Sahalos, “Increased range bistatic scatter radio,” *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1091–1104, March 2014. 1, 2, 3, 5, 43

[4] N. Fasarakis-Hilliard, P. Alevizos, and A. Bletsas, “Coherent detection and channel coding for bistatic scatter radio sensor networking,” *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1798–1810, May 2015. 1

[5] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice.* Newton, MA, USA: Newnes, 2007. 3

[6] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, “Improving backscatter radio tag efficiency,” *IEEE Trans. Microw. Theory Tech.*, vol. 58, no. 6, pp. 1502–1509, Jun. 2010. 5

[7] “EPC Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHZ-960 MHZ, version 2.0.1. EPC Global,” 2015. 7, 21, 23, 27

[8] M. Buettner and D. Wetherall, “A software radio-based UHF RFID reader for PHY/-MAC experimentation,” in *Proc. IEEE International Conference on RFID*, Orlando, FL, Apr. 2011, pp. 134 –141. 17, 18, 19, 40

[9] M. Buettner. Gen2 rfid. [Online]. Available: https://github.com/ransford/gen2_rfid 17

[10] M. Buettner and D. Wetherall, "A "gen 2" rfid monitor based on the usrp," *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 3, pp. 41–47, Jun. 2010. 17

[11] G. Smietanka, S. Brato, M. Freudenberg, and J. Götze, "Implementation and extension of a GNU-Radio RFID reader," *Advances in Radio Science*, vol. 11, pp. 107–111, 2013. 17

[12] L. Catarinucci, D. De Donno, R. Colella, F. Ricciato, and L. Tarricone, "A cost-effective SDR platform for performance characterization of RFID tags," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 4, pp. 903–911, April 2012. 17, 19

[13] D. De Donno, F. Ricciato, and L. Tarricone, "Listening to tags: Uplink RFID measurements with an open-source software-defined radio tool," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 1, pp. 109–118, Jan 2013. 18

[14] A. Briand, B. Albert, and E. Gurjao, "Complete software defined RFID system using GNU radio," in *Proc. IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, Nov 2012, pp. 287–291. 18, 19

[15] Y. Zheng and M. Li, "ZOE: Fast cardinality estimation for large-scale RFID systems," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, April 2013, pp. 908–916. 18, 19

[16] Y. Zheng. usrp2reader. [Online]. Available: https://github.com/yqzheng/usrp2reader 18

[17] A. Bothe, C. Schraeder, and N. Aschenbruck, "An UHF RFID performance evaluation architecture based on traces from a software defined transceiver," in *Proc. IEEE International Conference on RFID Technology and Applications (RFID-TA)*, Sept 2014, pp. 72–77. 18, 19

[18] F. Galler, T. Faseth, and H. Arthaber, "SDR based EPC UHF RFID reader DS-SS localization testbed," in *Proc. 16th Annual Conference on Wireless and Microwave Technology (WAMICON), 2015*, April 2015, pp. 1–4. 18, 19

[19] C. Angerer, "Design and exploration of radio frequency identification systems by rapid prototyping," Ph.D. dissertation, Institut für Nachrichtentechnik und Hochfrequenztechnik, Vienna University of Technology, 2010, advisor Prof. M. Rupp. 18, 26

[20] A. Bletsas, J. Kimionis, A. G. Dimitriou, and G. N. Karystinos, "Single-antenna coherent detection of collided FM0 RFID signals," *IEEE Trans. Commun.*, vol. 60, no. 3, pp. 756–766, Mar. 2012. 21, 30, 48

[21] M. Simon and D. Divsalar, "Some interesting observations for certain line codes with application to RFID," *IEEE Trans. Commun.*, vol. 54, no. 4, pp. 583–586, Apr. 2006. 21, 26

[22] J. G. Proakis and M. Salehi, *Communication Systems Engineering*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, August 2001. 25

[23] C. Angerer, G. Maier, M. Bueno Delgado, M. Rupp, and J. Alonso, "Single antenna physical layer collision recover receivers for RFID readers," in *Proc. IEEE International Conference on Industrial Technology (ICIT)*, March 2010, pp. 1406–1411. 32

[24] K. Fyhn, R. Jacobsen, P. Popovski, A. Scaglione, and T. Larsen, "Multipacket reception of passive UHF RFID tags: A communication theoretic approach," *IEEE Trans. Signal Process.*, vol. 59, no. 9, pp. 4225–4237, Sept 2011. 36

[25] N. Kargas. Gen2-UHF-RFID-Reader. [Online]. Available: https://github.com/nikosl21/Gen2-UHF-RFID-Reader 51