Separation of Multiple Passive RFID Signals Using Software Defined Radio

Separation of Multiple Passive RFID Signals Using Software Defined Radio

Dawei Shen, Grace Woo, David P. Reed, Andrew B. Lippman
Media Lab, Viral Communications Group
Massachusetts Institute of Technology
Cambridge, MA, 02139
Email: {dawei, gracewoo, dpreed, lip}@media.mit.edu

Junyu Wang
Fudan University
Email: junyuwang@fudan.edu.cn

***Abstract*—We present a practical design of an RFID reader that is capable of reading multiple passive tags through joint decoding. The reader is implemented and analyzed using the GNU Software Defined Radio system. We use low frequency (LF) 125kHz commodity MIT ID cards in the experiment, and discuss extensions to decoding high frequency (HF) tags. This design reconsiders opportunities available in the lower layers of RFID design. Physical layer communication is analyzed rigorously and a complete system design is introduced as a result. We demonstrate this by exploring the differences in amplitudes and phase offsets among signal components, multiple tags can be separated and efficiently decoded using joint decoding. System performance is analyzed with both implementation and simulation. Based on these results, we summarize opportunities for improving industrial auto-collision algorithms with multiple-tag decoding capability.**

I. Introduction

Radio Frequency IDentification (RFID) is a tagging technology which has enabled simple wireless protocols to be implemented on inexpensive hardware. Passive RFID is an area of design where small electronic chips may be remotely powered with no onboard power source. Similar to active devices, these chips may be interrogated for identifiers and data. As RFID becomes ubiquitous in daily life, many well-studied scenarios [1] emerge which require the need for decoding multiple passive RFID cards with a single inquiry:

- Multiple identification cards in a single wallet
- A gate reader at a dock door with multiple signals within a read range
- Ubiquitous applications with multiple embedded passive devices

To address the vastness of these applications, many standards have been developed by organizations such as the International Standards Organization (ISO) to regulate devices which are compatible across many different industrial platforms. The ISO[2] specify widely used standards for developing passive devices at various frequencies. We demonstrate the practicality of our proposed source separation methods by implementing and testing under these guidelines.

Although these standards state guidelines for developing each component of a proximity RFID card system, there are many design choices which are left open to the specificity of the transmitter and receiver application. Here, we explore the design space allowed by and compatible with a class of ISO standards:

- ISO 11784, ISO11785, ISO14223, ISO18000-2 for low frequency (LF)
- ISO14443, ISO15693, ISO18000-3 for high frequency (HF)
- ISO 18000-6 (A, B, C), EPC Gen2(ISO18000-6C) for (UHF)

With these guidelines in mind, we develop a software-defined radio architecture capable of reading multiple passive RFID proximity signals with a single inquiry.

In this work, we develop and analyze source separation methods available in the physical layer. In order to demonstrate the validity of our multiple card reader, we choose the mature 125KHz band proximity card system. While the Indala FlexCard 125kHz system is a closed-source and legacy LF system unregulated by modern ISO standards, there are many reasons for following this design choice. Among them, at the time of writing, the Indala FlexCard 125KHz band proximity card system [3], [4] is the deployed commodity system of choice at MIT. We demonstrate the compatibly of our software radio multiple-card receiver by integrating it with this currently deployed commercial system.

A. Related Work

The theme of simultaneous decoding of multiple cards has been long discussed in the context of co-channel source separation algorithms. The existing literature of co-channel source separation is rich in analyzing methods to achieve source separation. Giridhar et al. produced a set of works in [6] addressing the fundamental problems that exist in signal source separation. Independent Component Analysis (ICA) has been discussed in great detail for use in source-separation systems [7]. An insightful analysis by Hamkins [8] considers the cross-coupled phase-locked-loop, the joint Viterbi decoder and an analytic technique resulting in a considerably fewer number of detection choices.

These works represent a movement toward the deployment of practical source separating decoders. We develop our design in the context of this prior work and adapt them for use in a practical system. To the best of our knowledge, this is the

978-1-4244-3338-4/09/$25.00 ©2009 IEEE

first implementation of an interactive and commodity multiple-card RFID card reader using software-defined radio which conforms to industrial guidelines.

II. Goals and Challenges

The challenge of developing a collision-free receiver is discussed in almost every passive RFID ISO standard. While the problem of designing a short-range collision-free at the MAC layer is a challenge itself, we present a fundamental departure from this industrial viewpoint by designing a *practical* passive RFID multiple-card reader.

Decoding multiple passive RFID cards with a single antenna receiver demonstrates an opportunity for achieving higher bit rate. Unlike the classic viewpoint of improving strong signal decoding via interference cancellation, we pursue simultaneous decoding of multiple RFID cards with sufficient reliability. Most importantly, this design viewpoint dramatically improves user experience by resolving conflicts such as multiple RFID cards in a single wallet. We evaluate our analysis with practical implementation and measurement.

Rather than approaching the problem from a time-division multiplexing (TDM), frequency-division multiplexing (FDM) or code-division multiplexing (CDM) point of view; we follow a design principle which executes complexity at the decoder. This allows backward compatibility with existing passive card devices. This goal suggests the analysis of a class of algorithms describing the separation of multiple source signals impinging on a single antenna.

A. Approach

ISO standards for LF, HF and UHF all specify multiple layers of design. We emphasize that this work uses low-level advanced signal processing techniques to achieve multiple source signal separation rather than higher layer MAC scheduling. These design details are not highlighted in the receiver design standards and instead present an opportunity to reconsider traditional abstraction.

There are several drawbacks and tradeoffs to consider in this approach. The source separation algorithms developed in this work at the receiver may not be practical for classic hardware implementation. However, the emerging software radio availability allows for evaluation of these methods. The added burden of decoder complexity in the lowest layer is a trade-off in decoding multiple cards at once.

III. ISO Proximity Card Primer

In general, proximity cards refer to contactless RFID cards which work in close range. There are many commercial systems which implement full-blown proximity card devices including smart cards, photo identification and public transit applications. Modern proximity card systems are regulated with the ISO14443 standard in the HF range.

The system we use in this work, Indala's LF 125kHz Flexcard system, represents a legacy commercial system which is not an open-protocol and not strictly regulated under modern ISO standards. In order to clearly describe our source-separation techniques in the context of a practical system, we describe our system in the framework of ISO14443. We believe the ISO14443 is the best open-source description of the LF closed-source Indala Flexcard system which we integrate. More importantly, we use the ISO14443 guidelines to describe the relevant points in our system. Ultimately, as discussed in later sections, our source-separation methods should be employable regardless of whether we consider LF, HF or UHF standards.

Under ISO14443 dictated standards, the ID-1 cards which are modelled as the source signals which in this work are referred to as proximity cards (PICC). The reader device which uses inductive coupling to provide the power for modulation as well as does active data exchange is referred to as the proximity coupling device (PCD).

The standards regulating the construction and robustness of the PICC physical form include things such as dimension size, location of magnetic strip and performance under adverse scenarios (e.g. XRay and UV). The regulation for the physical characteristics of the PCD do not fall under the scope of the ISO14443 standard. Overall, the brief specifications for antenna form factor and coupling mechanisms in the ISO14443 are enough to develop a consistent channel model in Section III.

A. Signal Interface

The ISO14443 standard is officially designed for the 13.56MHz range. Hence, the details associated with carrier frequency f_c manipulation should be adopted for 125KHz RFID proximity card readers i.e. an older generation of RFID card systems.

There are two types of signals that a PICC may emit labeled Type A and Type B. The PCD must alternate between modulations in idle mode since it does not know whether the impinging signal is of Type A or Type B. In this work, we are not interested in signals from the PCD to the PICC and only in the signals from the PICC to PCD.

In Type A PICC cards, the source signal from PICC to PCD is a load modulated Manchester encoded on-off keying (OOK) signal at f_c/16 bits/s. In the legacy 125K system we implement, the symbol rate is 3.91kbit/s. In Type B mode, BPSK NRZ-L encoded signals are used. As a small note in the standard, inversion of bits is allowed.

The modulation used in the ISO14443 interface is simple Amplitude Shift Keying (ASK). The ISO standard regulates this modulation by providing time barriers for shifts between high and low amplitudes. The standard used here implies that a 0.5 μs should be employed between a rising and falling edge. Additionally, the rise and fall of each edge (i.e. between 95% and 5%) should occur within 0.5 μs. It is with these constraints in mind that a channel model, signal processing algorithm and real-time system is developed.

IV. Channel Model

In this work, we derive the channel model seen in practice from measurements and observations made from the Indala LF 125kHz Proximity RFID card [3] system.

We choose this legacy system as it is the current system deployed on campus at this university. The student ID cards are similar to the PICC interfaces described in the ISO14443 standard. Associated readers are similar to the PID interfaces described in the ISO14443 standard. The lower level and higher level protocols of this Indala system also resemble that of the later-drafted ISO14443 standard.

A. Modeling Physical waveforms

The reader constantly emits a 125kHz single-frequency signal. As a passive PICC proximity card approaches the reader, enough power is coupled on the internal antenna. As a result, the passive card begins to transmit digital information back to the reader. The resulting signal perceived by the receiver at the reader is a 125kHz carrier, whose amplitude is modulated by a 62.5kHz sine wave. Binary digital information is differentially encoded in the 62.5kHz signal using binary phase-shift keying (DBPSK). A '1' incurs a phase shift by π, while a '0' corresponds to no phase change. Mathematically, the received signal can be represented by:

$$\begin{aligned} y(t) &= \big(A + B(t)\cos(2\pi \cdot 62.5 \cdot 10^3 \cdot t + \phi)\big) \\ &\quad \cdot \cos(2\pi \cdot 125 \cdot 10^3 \cdot t + \theta), \end{aligned} \tag{1}$$

where A is the amplitude of the 125kHz carrier when no card is present, $B(t)\cos(\cdot)$ is the digital signal that AM-modulates the carrier. Note that the clock of the passive PICC card is derived from the external carrier. $B(t)$ itself is a two-level square waveform carrying digital information, which may be expressed as:

$$B(t) = h \cdot \sum_k d_k a(t - kT), \tag{2}$$

where h is the amplitude depicting the signal strength, k is a discrete time index, and $a(t)$ is a simple on-off square wave with a level of 1 when $0 < t \leq T$, and 0 elsewhere. d_k is a series of binary symbols valued $\{1, -1\}$, differentially encoded. T is the symbol period. The symbol rate of the Indala RFID system used in the experiment is $f_s = 125 \cdot 10^3/32 = 3.91$kHz. Thus, $T = 1/f_s = 2.56 \cdot 10^{-4}$s, which consists of 16 full cycles of 62.5kHz cosine waves.

In the system deployed on campus and unspecified by the standard, each PICC card is uniquely identified with a 224-bit binary sequence which we refer to as a frame. When excited, the card repeatedly transmits the 224-length sequence back to the reader until the signal fades. Each frame contains 30 consecutive zeros as the synchronization header. In the campus ID card system, only 32 out of the 224 bits vary, all the other 192 bits stay constant for each PIC card. [4].

Eq.(1) shows that the received signal has three major frequency components which are centered around 62.5kHz, 125kHz, and 187.5kHz. We are mainly interested in the 62.5kHz band since it bears the digital information in $B(t)$. A low-pass filter with a cut-off frequency of 95kHz spurns the 125kHz carrier component and the 187.5kHz-band signal, which in fact mirrors the 62.5kHz band. The low-pass filtered signal can be represented using:

$$y^L(t) = B(t)\cos(2\pi \cdot 62.5 \cdot 10^3 \cdot t + \varphi). \tag{3}$$

Note that here $\varphi = \phi - \theta$, and the constant 1/2 is absorbed into the amplitude h inside $B(t)$.

B. Channel Model for Multiple RFID Tags

When multiple PID RFID cards are presented to the reader, e.g. when a user taps his wallet containing two or more RFID cards in front of a reader, all cards are activated after accumulating enough power, and then they start to transmit signals back to the reader simultaneously. The reader receives the summation of all these individual signals and the low-passed version of it can be characterized by:

$$r_N(t) = \sum_{l=1}^{N} B_l(t - \tau_l)\cos(2\pi f_0 t + \varphi_0 + \rho_l) + n(t), \tag{4}$$

where N is the number of activated cards, indexed by l, and

$$B_l(t) = h_l \cdot \sum_k d_{k,l} a(t - kT). \tag{5}$$

There are several crucial properties of passive RFID cards that help simplify the interpretation of Eq.(4). The passive RFID cards synthesize their internal clocks with the incoming 125kHz carrier as a reference signal. φ_0 is a common component of phase offsets to be estimated for all signals. ρ_l's are phase offsets between different signals depending on when the card gets activated. Note that we use f_0 instead of $62.5 \cdot 10^3$ as the frequency because 62.5kHz is only a nominal frequency. In practice we need to estimate accurately the true value of f_0, which may be slightly different from 62.5kHz. In the model above, we assume $n(t)$ is a additive white Gaussian noise, with zero mean.

For the signal transmitted by a single card, both f_0 and φ_0 can be estimated using standard carrier frequency/phase recovery techniques such as a Costas loop. As introduced in the next section, applying a Costas loop has the effect of multiplying (mixing) $y^L(t)$ with a cosine wave generated by a local oscillator, which has the same frequency f_0 and phase φ_0. By cascading a low-pass filter after the mixer, we can recover the base-band signal $B(t)$ and further decode needed bits. However, when two or more signals present different phases, the recovery of multiple unknown phases cannot be solved using traditional approaches. They do share exactly the same frequency f_0, which can be estimated accurately by using Fast Fourier transforms (FFT) or Zero-Crossing methods.

We next compute the base-band equivalents. Assuming f_0 is accurately estimated, we can obtain both in-phase and quadrature components by multiplying $r_N(t)$ with $\cos(2\pi f_0 t + \psi)$ and $\sin(2\pi f_0 t + \psi)$ and low-pass filtering the resulting signals respectively. ψ is a judiciously chosen phase which we will analyze in depth later.

$$\begin{aligned} q_I^N(t) &= \mathcal{LPF}\left(r^N(t)\cdot\cos(2\pi f_0 t+\psi)\right)\\ &= \sum_{l=1}^{N} B_l(t-\tau_l)\cos(\psi-\varphi_0-\rho_l)+n_I(t)\\ q_Q^N(t) &= \mathcal{LPF}\left(r^N(t)\cdot\sin(2\pi f_0 t+\psi)\right)\\ &= \sum_{l=1}^{N} B_l(t-\tau_l)\sin(\psi-\varphi_0-\rho_l)+n_Q(t) \end{aligned} \tag{6}$$

In the 2D domain, the complex low-pass equivalent can be expressed as

$$q_L^N(t)=\sum_{l=1}^{N} B_l(t-\tau_l)\exp[j(\psi-\varphi_0-\rho_l)] \tag{7}$$

We again omit the 1/2 constant factor in each equation which is absorbed into the unknown amplitudes to be estimated.

C. Channel Model in the Discrete Domain

In a practical system design, signals are sampled and processed digitally. For example, in the experiment set up using the GNU Software Defined Radio platform, the signal is sampled by a 12-bit Analog-to-Digital Converter (ADC) with a sampling frequency of $f_{\text{ADC}} = 64$MHz. The discretized signal is further decimated by a factor of 128, leading to a sampling frequency of 500kHz.

Given that $B_l(t)$ has only two possible levels, h_l and $-h_l$, at any given time instant, the received signal in the discrete domain can be characterized by using:

$$r^N[m]=\sum_{l=1}^{N} h_l\cdot d_l[m]\cdot\exp[j(\eta-\rho_l)]+z[m], \tag{8}$$

where $\eta=\psi-\varphi_0$. Here, m indexes all samples at a frequency of $f_s = 500$kHz; h_l is the amplitude of the l^{th} signal, measuring its signal strength; d_l is either 1 or -1 depending on the symbol being transmitted by the l^{th} card at the time instant m; $z[m]$ is the additive complex Gaussian noise. Note that m is not an index for symbols, but for samples. As stated above, signals transmitted by multiple cards do not have symbol-level synchronization. We over-sample each carrier cycle by a factor of 500kHz/125kHz=4.

Analyzing the I/Q components of $r[m]$ individually, the result is

$$\begin{aligned} r_I^N[m] &= \sum_{l=1}^{N} h_l\cdot d_l[m]\cdot\cos(\eta-\rho_l)+z_I[m]\\ &= \sum_{l=1}^{N} g_l^I\cdot d_l[m]+z_I[m],\\ r_Q^N[m] &= \sum_{l=1}^{N} h_l\cdot d_l[m]\cdot\sin(\eta-\rho_l)+z_Q[m], \end{aligned} \tag{9}$$

where $g_l = h_l\cdot\cos(\eta-\rho_l)$. $r_I^N[m]$, used as an example here, presents a multi-level property. Given the 2^N possible combinations of N d_l's, $r_I^N[m]$ can have as many as 2^N possible levels, if no duplicated combinations are generated. We will fully explore this feature in the following section.

V. Signal Separation Principles and Algorithms

A. Basic Principles

If only one card is present, from Eq.(8), received samples constitute a two-point constellation on a 2-dimensional plane: $h_1e^{j(\eta-\rho_1)}$ and $-h_1e^{j(\eta-\rho_1)}$ when the noise is not considered.

Consequently, when two cards simultaneously transmit signals to the receiver, at most four focal points can show up in the constellation plane which are $\pm h_1e^{j(\eta-\rho_1)}\pm h_2e^{j(\eta-\rho_2)}$. The constellation is analogous to the one used for 4QAM modulation, though the points are placed in a more irregular manner. Therefore, there are two bits, instead of just 1 bit, being encoded on each received symbol. Similarly, when three cards coexist and emit signals, 8 points appear in the constellation, and 16 points are constructed by four co-channel RFID signals.

Each received symbol is decoded by seeking the closest constellation point with the shortest Euclidean distance, then mapping the point back to a length-N bit sequence, thus achieving separation of multiple card signals.

B. Parameter Estimation

1) Maximum Likelihood Estimation: A key step in the separation process is to accurately estimate the mean of each cluster. Note that the a-priori probability of each cluster is not necessarily uniform. Given Eq.(8), the log-likelihood function of all received samples is given by

$$\ln p(\mathbf{R})=\sum_{n=1}^{M}\ln\left\{\sum_{k=1}^{K}\pi_k\mathcal{N}(\mathbf{r}_n|\boldsymbol{\mu}_k,\sigma^2)\right\}, \tag{10}$$

where M is the number of samples in the processing window, $K = 2^N$ is the number of constellation points induced by N signal components. K $\boldsymbol{\mu}_k$'s to be estimated have actually only N degrees of freedom, since they are different summations of $\pm h_le^{j(\eta-\rho_l)}$. π_k's are a-priori probabilities of each cloud, and they satisfy $\sum_k \pi_k = 1$. The maximum likelihood estimation of parameters is to select $g_l = h_le^{j(\eta-\rho_l)}(1\le l\le N)$, such that Eq.(10) is maximized.

From a pattern recognition perspective, Eq.(10) is exactly in the format of a Gaussian mixture model [9]. Therefore, the problem of clustering and parameter learning can be solved efficiently using a modified EM algorithm, which takes advantage of the linear dependence among $\boldsymbol{\mu}_k$. However, the computational cost of an EM algorithm is not acceptable when fast acquisition of cards is crucial.

2) 2D Histogram Approach: A simpler and more effective approach is to use K-means clustering technique. This nonparametric algorithm only involves computing squares of Euclidean distances, and works very well in practice [9]. However, both the Gaussian mixture model and the K-means algorithm suffer from the fact that the recursive algorithms may converge to local optima instead of global ones. Thus, selecting initial starting points that are as close to the true means as possible is crucial for the algorithm to converge correctly.

A straightforward approach is to construct a 2D histogram of received samples within a processing window. The entire plane is paved with a $L \times L$ grid. As samples are received, we keep track of the number of samples that fall into each square. We select 2^N squares with the largest numbers of samples, and estimate the means by averaging samples within each square.

In practice, two key issues arise. First, based on the model analysis, two constellation points, such as g_l and $-g_l$ are circularly symmetric around the origin. Therefore, we only need to keep track of the square-regions within the right half-plane. When a sample falls within the left plane, the count for the grid that covers the symmetric point increases by one. Second, it is likely that adjacent grids all have high sample densities introduced by the same constellation point. They actually belong to the same peak. We need to constrain that selected peaks are at least D grids apart from each other.

Sample means of selected square-regions are accurate estimates of $\boldsymbol{\mu}_k$'s. They can also be used to feed the K-means clustering algorithm as initial points to improve accuracy. The number of clusters we seek in K-means is set to be larger than K to accommodate outliers.

3) 1D Projection: In order to further decrease the computational complexity, we can project data samples to a 1-D space, i.e. a real axis by using

$$y_n = \mathbf{r}'_n \cdot \mathbf{w}. \tag{11}$$

$\mathbf{w}$ is a direction vector of unit length to which 2D data samples are projected. The log likelihood of y_n's becomes

$$\ln p(\mathbf{y}) = \sum_{n=1}^{M} \ln \left\{ \sum_{k=1}^{K} \pi_k \mathcal{N}(\mathbf{y}_n | \boldsymbol{\nu}_k \cdot \mathbf{w}, \sigma^2) \right\}, \tag{12}$$

where $\boldsymbol{\nu}_k = \boldsymbol{\mu}'_k \cdot \mathbf{w}$ is the mean value in the 1D space, and they are symmetric around 0.

$\mathbf{w}$ should be chosen such that the best discriminability is achieved in the 1D space after projection. For labeled data, Fisher linear discriminant gives a direction that reaches good performance of separation. However, in this problem, data samples are unlabeled. Thus, we use the principle component as $\mathbf{w}$. While principle component analysis (PCA) does not use discriminability as its criteria, it performs well in practice.

With projected data, which are a sequence of scalar samples, we can again apply the hybrid approach of K-means clustering and peak detection on a histogram. The entire real axis is divided into L number of bins, and the number of samples that fall into each bin is counted. We show in implementation the tradeoffs between a 2D and a 1D histogram approach.

C. Cluster Proximity

It is clear from the methods presented that if two clusters are particularly close to one another, joint decoding becomes ambiguous. In the methods presented, joint decoding fails if the cards are indeed in close proximity. However, it may be shown in practice that these cases do not occur often.

We do not address solutions for cases where two clusters are in close proximity. Assuming the channel model of a ISO14443 RFID card system, it may be shown in practice the point at which the proposed algorithms fail. Assuming uniform distributions for the phase angle and magnitude estimation, we show in simulation that the region of failure due to cluster proximity is extremely low.

D. Card Count Estimation

In the methods presented, the assumption is that the number of sources is known at the time of decoding. Clearly, in practice this information is not always known at the time of decoding. Here, we discuss some drawbacks and advantages of various approaches to estimating the card count in real time.

One approach is to use a histogram approach where bin sizes are chosen ahead of time to be smaller. Following, thresholds are used to determine whether there are a sufficient number of datapoints observed in each bin. The two parameters which must be determined universally prior to running the recieve chain are (1) the resolution of the bin sizes and (2) the threshold per buffer-size which determines the presence of a card in that bin.

A second approach is to use a K-mean approach where correlation is computed assuming n number of cards are present. The result of the K-mean approach, however, produces the number of data points which surrounds each of the resulting cluster points. The number of data points corresponding to each cluster point may be used to determine whether a card is present. Here, the only parameter which must be determined universally prior to running the recieve chain is the threshold for the number of data points associated with a cluster point.

VI. System Design

A. Implementation

The GNU Software Defined Radio (SDR) software suite and the Universal Software Radio Peripheral (USRP) hardware are used as a testbed platform for testing the proposed methods.

The USRP is an open-source hardware device equipped with a RF-front end and general purpose analog to digital converters. The board operates with four 64 MS/s 12-bit analog-to-digital converters, and four 128 MS/s 14-bit digital-to-analog converters. Daughterboards associated with the USRP allow experimentation with a range of frequency from a few kilohertz to a few gigahertz. Ultimately, this platform is limited by the interface between the USRP and the computer. The USB interface delivering the samples to the computer limits the total processing to approximately 16MHz of baseband bandwidth.

The GNU SDR software is an ongoing and developing suite of open-source software tools which work in conjunction with the USRP. GNU SDR provide an architecture framework which provides scheduling and control of signal processing blocks. Interfacing and basic signal processing blocks are well developed within the framework. Additionally, the software

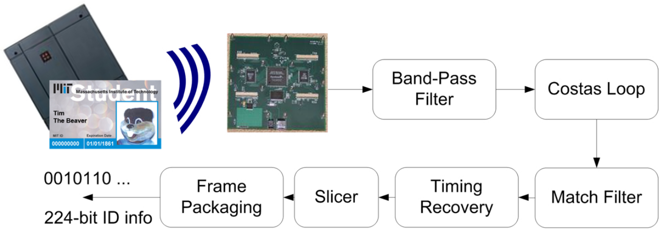

Fig. 1. System block diagram for a single RFID card reader

also comes complete with infrastructure for creating new blocks. This infrastructure implemented as a block diagram using Python wrapper code. The individual sample-processing blocks are written in C++. When used with the corresponding open source hardware, the GNU SDR configurable software becomes a powerful prototyping device.

In our experiment, we use a low-frequency RX (LFRX) daughter card, which covers a frequency range from DC to 30MHz. The software is implemented and tested on a Dell dual-core 3.2GHz workstation.

B. System Architecture

We first design and implement a standard receiver for single-card decoding using GNU Radio and USRP. The system diagram is shown in Fig. 1. The receiver is designed as a standard BPSK digital receiver.

The Costas loop jointly recovers both unknown frequency f_0 and phase φ. The resulting baseband match-filtered signal then goes through a Muller & Mueller timing recovery block to discover the best down-sampling timing. The output of the timing recovery block is a symbol-rate signal, which can be readily decoded into a binary sequence using a slicer. The frame packaging block searches for the header, which are 30 consecutive zeros. The 30 zeros and the following 194 bits are packaged together into a frame, if a card's ID information is successfully decoded. The 224-bit frames are continuously repeated until the card gets out of the receiving range.

Note that in the above decoding procedure, we have omitted the property that all bits are differentially encoded. Therefore, a frame, and its complementary frame with all bits flipped, correspond to the same identity information. The reason why DBPSK is treated as BPSK is that the joint decoding algorithm for multiple cards not rely on the differential properties, but only on the amplitude and phase of each component. The experiment shows the decoding works perfectly and error-free.

We decode several cards and record the decoded bits as references for comparison with the decoding of multi-card reader.

The system diagram for the multi-card reader is displayed in Fig. 2. The signal flow follows exactly what we introduce in Section IV and Section V. The separation block works at the sample rate, not the symbol rate. The outputs of the separation block are N streams of binary signals. After being separated, they still need to be processed by standard timing recovery and frame-sync blocks for the ultimate digital information to be decoded.

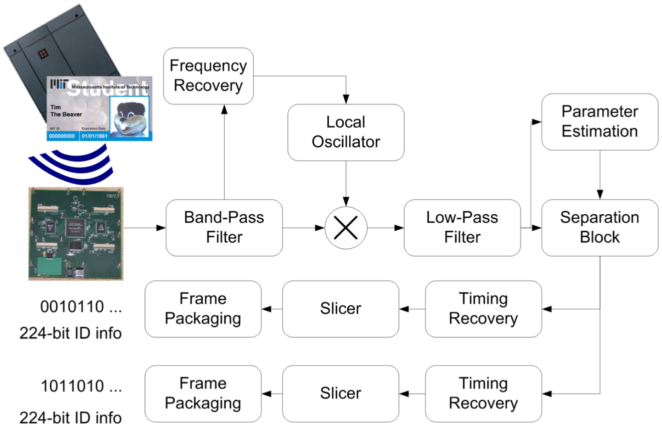

Fig. 2. System block diagram with modifications for decoding multiple RFID cards.

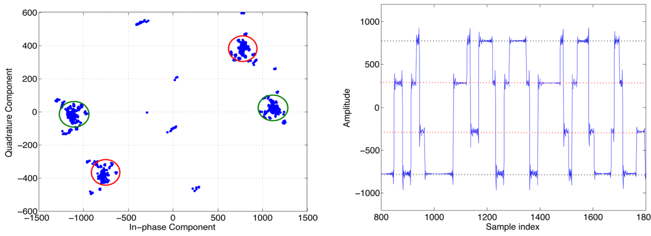

Fig. 3. Two cards: (L) Constellation map of received samples (R) The time domain waveform when the received signal is projected to 1 dimension

VII. Results

In order to demonstrate the results of physical-layer analysis, we implement the proposed methods on the GNU software defined-radio platform. Here, we are able to gather and process resulting RFID data from typical multiple-card usage scenarios.

A. Constellation Mapping

We validate and demonstrate the mathematical models and assumptions in the experiment. Fig.3,4,5 display constellation points represented by Esq. (8), as well as time domain waveforms when only a single dimension of the signal is observed.

Received signals are recorded by using the GNU Radio platform when 2, 3, and 4, MIT ID cards are presented to the antenna simultaneously. These figures clearly exhibit 2^N dense areas where received signals aggregate together. As the number

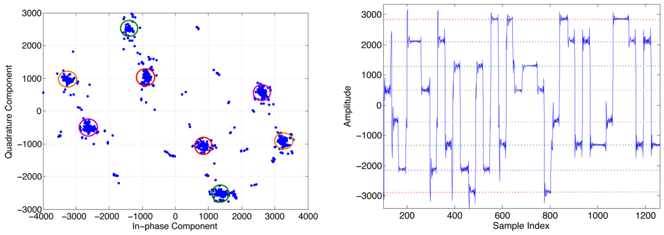

Fig. 4. Three cards: (L) Constellation map of received samples (R) The time domain waveform when the received signal is projected to 1 dimension

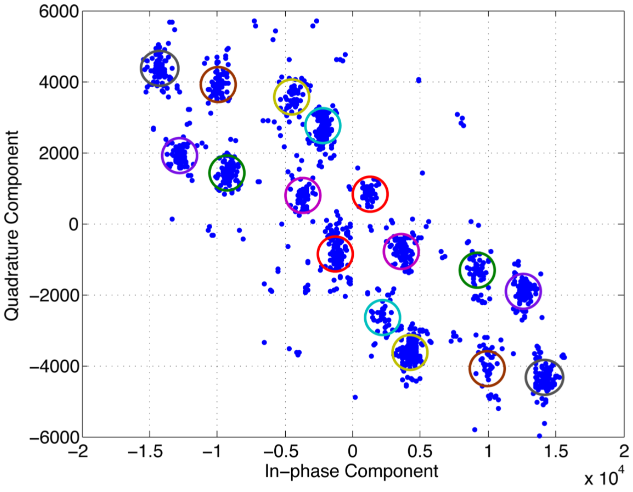

Fig. 5. Four cards: Constellation map of received samples

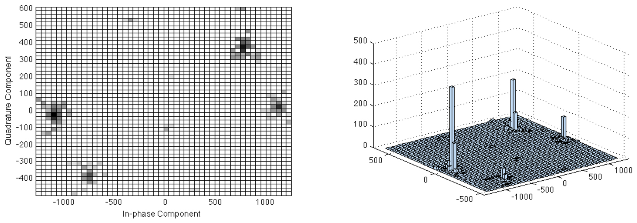

Fig. 6. A 2D histogram of received samples when two cards are present. (L) A color map of sample densities (R) A histogram in viewed in 3D

of cards, the boundary between these areas becomes more blurry which makes decoding of a symbol more ambiguous. This is evident from the constellation plot for four cards in Fig. 5.

Note that there are certain number of outliers in the constellation plots which are distant from each of the constellation points. These are usually due to Gibbs effects of FIR filters applied before, and bit transitions when the signal switches between '0' and '1'. To more accurately estimate model parameters such as the coordinates of the constellation points, these outliers can be purged first by using an additional heuristic approach.

B. Amplitude and Source Detection

Fig. 6 shows the 2D histogram for the case when only two cards are present. A color map showing the logarithm of sample densities, and a 2D-histogram displaying in a 3D view are presented. Clearly, we can readily find the positions of peaks on a 2D-histogram. Fig.7 displays the histogram of projected samples when three and four cards are present, respectively.

From these histograms of actual data, we show that amplitude estimation is possible for commodity PID cards. The current buffer time is 8000 samples. For a real-time system, there is a tradeoff between the buffer time and accuracy of the amplitude estimation. With the prototype equipment available for these experiments, we demonstrate real-time amplitude estimation using clustering methods.

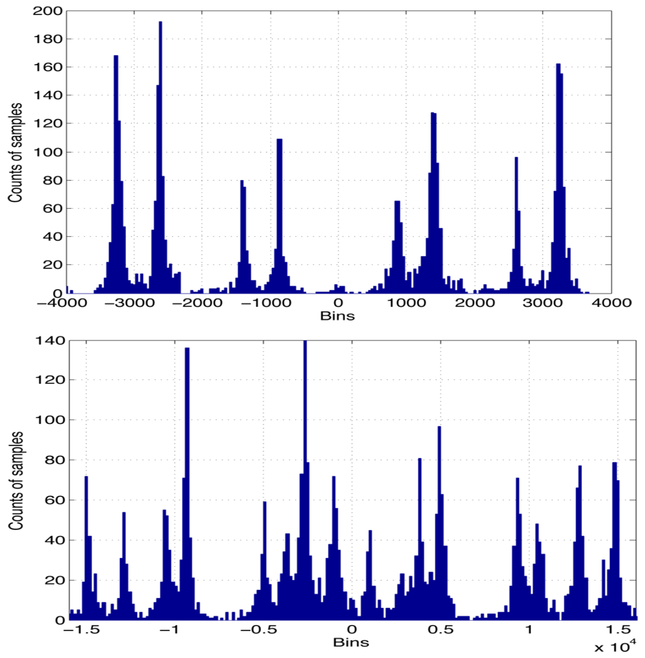

Fig. 7. A histogram of projected received samples in 1D space when three and four cards are present respectively.

VIII. Discussion

Data gathered from typical RFID data indicates that practical decoding of multiple sources is feasible on commodity hardware. From these experimental results, there are a few insights for separation of multiple signals which are observable from this implemented ISO14443 system which may be generalized for variant standards:

- estimation of number of cards present and amplitude levels is crucial for accurate decoding
- common continuous frequency pulse is required across all separable source signals
- precisely overlapping signals in amplitude are unlikely but will result in failure of the proposed methods
- distances defined for proximity RFID result in sufficient SNR for robust decoding

Ultimately, there is a theoretical limit to what we may achieve for joint decoding. Figure 8 depicts a simulation of the achievable error probabilities assuming each individual PID card results in a uniform distribution of observed SNRs at the PICC card. Here, we simulate by generating a constant SNR for 224 symbols. This Monte Carlo simulation shows the error probability for detection for 2, 3 and 4 impinging source signals.

From Figure 8, we can see that for high SNR greater than 30dB as in that of proximity RFID, the error probability decreases sharply. This addresses the theoretical capacity of decoding multiple RFID cards at the same time as well as the probability of aligning constellation points when the number of

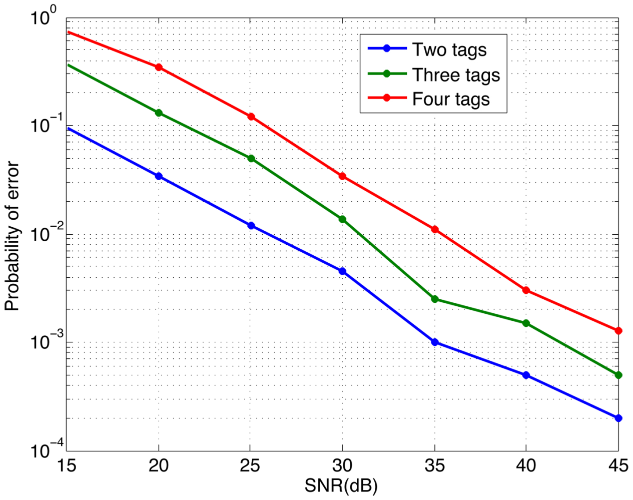

Fig. 8. Simulation results: Probability of error versus SNR for 2, 3, and 4 cards. Signal amplitudes are assumed to be uniformly distributed between 500 and 1500; phases are assumed to be uniformly distributed between 0 and 2π

cards increases. Furthermore, from this simulation, we can see how theoretical joint decoding scales with an increasing number of cards. From a practical standpoint, Figure 8 indicates that if amplitude estimation is done accurately, there is much room for joint-decoding at the the reciever. This simulation also underscores the the insight of the importance of accurate detection for the number of cards and amplitude levels.

A. Gen2 Protocol Extension to Higher Frequency (HF, UHF) systems

The experiments and results presented here are conducted using a low-frequency (LF) Proximity card RFID system. Joint decoding may also be possible in a high-frequency (HF) and ultra-high-frequency (UHF) RFID system such as that of the Gen2 protocol specifications. There are, however, a few differences which require consideration before drawing conclusions for joint decoding in the higher frequency system.

The Gen2 protocol is defined for higher frequencies from 860MHz - 960MHz. Similar to the older ISO14443 standard, the Gen2 protocol requires an interrogator-talks-first (ITF) strategy where passive-backscatter is not activated unless the interrogator (the card reader) asks first. This design allows for higher-level MAC control. The methods tested here on the low-frequency (LF) system should be used in conjunction with this higher level design in these higher frequency systems.

One difference between the LF/HF and UHF protocols for passive RFID is the way in which the passive card are excited. In LF systems, the cards are activated using an inductive coupling technique where a carrier frequency is loaded to generate a sub-carrier frequency. In UHF systems, the cards are activated by the generator with a continuous-wave (CW) signal to the tag (cards). Here the tag responds by modulating the reflection coefficient of its own antenna.

These mechanisms may result in different performance of the presented methods for some HF and UHF systems. However, we believe the extension is possible for two reasons. (1) For short range communication, the difference in channel model may not be significant enough to alter performance drastically. We expect there will be different channel models for inductive coupling vs. antenna reflection. However, for short range communication, we do not expect this to be significant.

(2) The crucial factor for performance of these methods lies in the consistency of deriving the continuous frequency clock waveform at the passive receiver. In LF systems inductive coupling results in activating all card tags within proximity to transmit with the same carrier frequency. In UHF systems such as the Gen2 protocol, all inquired card-tags send signals to the reader with approximately the same carrier frequency. As long as the frequency discrepancy does not incur a large phase offset within an observation window at the reader, our algorithm will perform equally well. As future work, we will experiment with UHF tags and examine the constellation plot of the frequency-corrected signal.

IX. Conclusion

We present a method for joint-decoding of multiple passive RFID promity cards which is implemented on a software-defined radio platform. We emphasize an alternative to MAC-layer approaches for collision-avoidance. With the complete implementation of a joint source-decoding LF RFID system, we are able to show backward compatibility with an existing commodity system and improvements in detection with real-time data. Although computationally heavy at the decoder, this is an opportunity for significantly greater throughput.

In order to achieve these results, we first developed a rigorous signal interference model. Based on this and practical data in mind, channel models are developed to aid in developing a practical algorithm. We point out several crucial estimation problems and provide analytical and practical solutions for separating multiple RFID card sources. Based on this analysis, we may generalize to variant protocols such as EPC Gen2 systems.

References

[1] C. Floerkemeier, "Infrastructure support for RFID systems," Ph.D. dissertation, ETH Zurich, Zurich, Switzerland, Jul. 2006.

[2] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. New York, NY, USA: John Wiley & Sons, Inc., 2003.

[3] "HID Global," http://www.hidglobal.com/, 2008.

[4] P. Agrawal and etc., "The MIT ID Card System: Analysis and Recommendations," MIT, Tech. Rep., December 2004.

[5] K. Giridhar, J. Shynk, A. Mathur, S. Chari, and R. Gooch, "Nonlinear techniques for the joint estimation of cochannel signals," *Communications, IEEE Transactions on*, vol. 45, no. 4, pp. 473–484, Apr 1997.

[6] K. Giridhar, S. Chari, J. Shynk, R. Gooch, and D. Artman, "Joint estimation algorithms for cochannel signal demodulation," *Communications, 1993. ICC 93. Geneva. Technical Program, Conference Record, IEEE International Conference on*, vol. 3, pp. 1497–1501 vol.3, May 1993.

[7] P. Comon, "Independent component analysis, a new concept?" *Signal Process.*, vol. 36, no. 3, pp. 287–314, 1994.

[8] J. Hamkins, "An analytic technique to separate cochannel fm signals," *Communications, IEEE Transactions on*, vol. 48, no. 4, pp. 543–546, Apr 2000.

[9] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer, 2007.