EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Intercepting UHF RFID signals through synchronous detection

Alexey Borisenko*, Miodrag Bolic and Majed Rostamian

Abstract

Recently, augmented ultrahigh frequency radio-frequency identification (UHF RFID) systems have been developed, and they contain additional components that can detect a tag's backscattered response and use this information for the localization of the tag and other applications. The methods currently employed either have poor performance because the detection of the tag's response is based on envelope detection or are costly because they are based on software-defined radio. The solution proposed in the paper is to use a method called synchronous detection to intercept tag signals. Using synchronous detection, we were able to use a conventional UHF RFID reader integrated circuit for the method, leading to a cost-effective, high-performance solution. We performed an analysis of its read rate and read range performance. The analysis showed that our receiver is capable of receiving tag signals with a read rate of 50% for passive and 66% for semi-passive tags at a 1-m distance between the tag and the receiver and is capable of receiving tag signals at a maximum distance between the tag and the receiver of 3.25 m for passive and 5.5 m for semi-passive tags, with the reader being within 8 m of the receiver. This augmented RFID system has a potential to facilitate localization and prevent the cross-read problem in RFID-based portals. In addition, it can be used as a protocol analyzer as well as a component of future Internet of Things.

Keywords: RFID; UHF RFID; EPC global class 1 generation 2; Synchronization; Synchronous detection

Introduction

Radio frequency identification (RFID) is a wireless automatic identification technology that uses radio waves to automatically scan and identify individual or bulk items [1]. In this paper, we will consider only passive ultrahigh frequency (UHF) RFID systems. A complete RFID system typically consists of a reader, one or more tags, and software for controlling the reader and processing the information. While a simple RFID system can help identify an item, only a coarse-grained awareness of its location can be achieved, i.e., the tag is located somewhere in the interrogation zone of the reader. For some applications, for example, the Internet of Things (IoT), more accurate localization is needed [2].

One approach to localization is the proximity method, which is easy to implement and is less affected by dynamic changes in the environment. This method requires scattered receivers to be deployed. The location of the tag is estimated as the location of the receiver that receives the tag response. The receivers on the market today are not suitable for this method to be implemented. Our goal is to implement a receiver for proximity methods for UHF RFID systems.

There are currently two receivers that detect signals from passive UHF RFID tags, which can be used for proximity localization: the Astraion Sensatag [3] and the Gen 2 Listener [4]. These designs have different architectures and implementations. The Sensatag uses an envelope detection architecture, has the advantage of simple implementation and low cost, but has poor sensitivity and selectivity. The Gen 2 Listener is a software-defined radio, based on the GNU Radio toolkit and running on the expensive Universal Software Radio Peripheral (USRP, Ettus Research, LLC, Mountain View, CA, USA) hardware. It offers good performance, but the high cost of the hardware prohibits it from being widely deployed.

In this paper, we introduce a novel device into the RFID system which can intercept UHF RFID tag signals called the augmented RFID receiver (ARR). This device uses a method called synchronous detection to overcome

*Correspondence: abori021@uottawa.ca
School of Electrical Engineering and Computer Science (EECS), University of Ottawa, Ottawa, Ontario K1N 6N5, Canada

challenges associated with intercepting tag signals using a non-envelope detection scheme. Two main challenges that have been addressed are frequency offset, which occurs because there are two different clock sources: on the transmitter and receiver, and frequency hopping, which makes determining the channel of the tag transmission difficult. To showcase the device, the performance of the implementation was compared to the other two outlined solutions: the Sensatag and Gen 2 Listener. A comparison of the read rate and range of the implementations was made.

The 'Background and related work' section shows related work in the field. The challenges of such a system are presented in the 'Challenges' section. The solution we propose to overcome these challenges is presented in the 'Synchronous detection - the solution' section. The implementation of the receiver is described in the 'Implementation' section. The 'Experimental results' section details the tests performed; the next section is the 'Applications' section, and last is the 'Conclusions' section.

Background and related work

Donno et al. [4,5] proposed an RFID receiver system, based on GNU Radio and implemented on a USRP. The receiver had a matched filter and a channel selector implemented in a digital radio. The applications proposed in other papers about localization, suggested implementation of a set of receivers for multilateral RSS-based localization, and protocol analysis. Further research was conducted in [6], where the system was used to evaluate the performance of a UHF RFID system. The use of the USRP makes the device expensive, especially if multiple devices are used to implement the anchor points.

Another device is implemented in [3] called the Sensatag. There, a special tag acts as a proximity-based localization device. The device can detect the responses of the tags and embed the detected electronic product codes (EPCs) into the tag's own EPC. The tag is battery-powered and has an field gate programmable array (FPGA) on board. Due to the power-hungry FPGA, the device suffers from short battery life.

Sensatag and Gen 2 Listener are based on different architectures. The Sensatag uses an envelope detection architecture, suffering from poor sensitivity and selectivity but has simple implementation and low cost. The Gen 2 Listener is a software-defined radio, based on the GNU Radio toolkit, running on the USRP. The USRP hardware is expensive but is flexible and offers good performance. The solution in this paper uses a direct conversion architecture.

The Astraion Sensatag is read by a standard EPC Gen 2 reader. The data Sensatag receives is encoded into its own EPC, through a technique called piggy backing [7]. The Gen 2 Listener runs directly on a PC, so any kind of interprocess communication is possible.

Table 1 compares the existing receivers with the proposed implementation. Note that *Architecture* concerns the radio architecture used. *Interface* refers to the way that data is extracted from the device. *Hardware* refers to the platform that is used. *Software* refers to the software component used in the receiver. The last column presents how the device is powered.

Challenges

Frequency hopping

UHF RFID operates in the industrial, scientific, and medical (ISM) unlicensed band and shares the spectrum with other devices. To mitigate potential interference, FCC mandates the use of frequency hopping. In the ISM band, 902 to 928 MHz, a device can occupy a channel for at most 400 ms [8]. The regulations also state that the next channel to be occupied must be selected pseudo-randomly.

The frequency hopping provision presents a problem for the receiver design. In a normal RFID system, the reader transmitter and receiver are integrated inside the reader, and the receiver knows the frequency at which the transmitter sent the signal. In this paper, the receiver is decoupled from the transmitter, so the receiver must have knowledge of the transmitter's channel frequency.

In general, three methods can be identified to overcome the channel-hopping issue. The first method is to listen to all the channels. Depending on the region of operation; this could be a simple task, like in Europe, where the number of channels is low. For North America, where there are 50 channels, in the frequency range from 902 to 928 MHz; this is not such a simple task.

Table 1 Receiver comparison

Device	Architecture	Interface	Hardware	Software	Power
Gen 2 Listener	SDR	USB	USRP	GNU Radio	External connector
Sensatag	Envelope detection	UHF RFID	Custom RF front end with FPGA	Custom LLRP application	Battery
This paper	Direct conversion	Ethernet	UHF RFID reader IC with FPGA	Custom LLRP application	External connector

The second solution involves predicting the next channel hop through a stepped serial search. A certain amount of time is required to acquire a lock on the channel, either by scanning the spectrum until finding the transmitting channel or randomly hopping, and then predicting the next hop. This will work if there is knowledge of the algorithm used for determining the next channel hop. Based on the FCC specifications, the algorithm is to be pseudo-random, so it is up to the manufacturer to implement the algorithm for channel hopping. In some cases, this can be determined by reverse-engineering the algorithm with the help of a spectrum analyzer.

The third solution is that the reader or host PC directly notifies the receiver where the next frequency hop is going to be. The most widespread communication protocol between PCs and RFID readers, low-level reader protocol (LLRP) [9], specifies a function called *NextChannelHop()* which informs about the next frequency channel. In this scenario, a PC calls this function through LLRP and reports it to the receiver device through ethernet. With this approach, there are time delay issues and not all UHF RFID readers support LLRP.

Frequency offset

Oscillators have a stability rating, i.e., offset from a desired frequency, expressed as parts per million (ppm). The EPC Gen 2 standard defines the minimum stability rating for the oscillator to be 10 ppm in dense reader mode [10]. The RFID reader uses the same local oscillator (LO) for sending the signal and receiving the backscattered signal, so no frequency offset will be present in the reader (except from Doppler shifts due to moving tags, but they are negligible even on fast moving tags, e.g., tags on trains [11]). The frequency offset is a problem for a receiver that is decoupled from the transmitter.

A frequency offset can be modelled as the multiplication of the signal by e^{jwt} where w is the frequency of the offset. This multiplication causes an instantaneous change in phase in the in-phase/quadrature (I/Q) constellation, which causes a rotation. An experiment was set up to showcase the problem of frequency offset. The analog outputs from two UHF RFID readers were connected to an oscilloscope. One reader was functioning as a receiver, while the other as a full transceiver. The readers were set to the same mixer frequency. The signal during a tag-reader exchange of the transceiver was then captured, and the I/Q constellation vs. time was plotted in LabView. Figure 1 shows the obtained results; the z-axis is time, and the y and x axes are I and Q components. Figure 1a shows the I/Q constellation of receiving a PR-ASK signal successfully by the transceiver reader. Figure 1b shows the obtained signal on the reader acting as a receiver. If two LOs are used without any provision to deal with frequency offset, a rotation appears, as seen in Figure 1b, and the signal cannot be successfully demodulated.

If a radio was tuned to the same channel as the transmitter, e.g., 902.75 MHz, then it would see a large signal adjacent to the tag channel in the $\leq$10-kHz range, which is the DC signal that would be removed if the transmitter and receiver were synchronized. Figure 2 shows how the frequency offset problem looks in the time domain. The top row is the clean reader and tag signal, as seen on the RFID reader. The tag signal is the high-frequency square wave at the end. The bottom row is the received response with frequency offset. The strong signal from the reader is modified, but the high-frequency weak tag signal cannot be seen, but rather the large blocker signal at around 8 kHz is seen.

Synchronous detection - the solution

Both envelope and homodyne detection techniques are simple and reliable demodulation techniques. The problem with the envelope detector is that its performance is limited by the relative amplitudes of the signal being demodulated. One of the goals of this paper was to make a system more sensitive than the system based on envelope detectors. Synchronous detectors are more complex than envelope detectors, and they require a phase-locked loop and a mixer. Demodulation is performed by multiplying

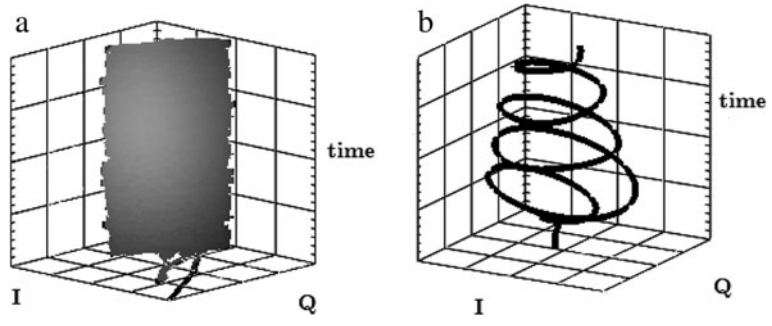

Figure 1 Frequency offset in I/Q constellations. (a) Without frequency offset. **(b)** With frequency offset.

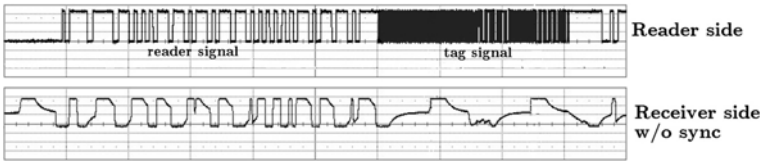

Figure 2 Frequency offset in time domain.

the received signal by a sine wave that is phase-locked to the incoming carrier.

On the reader side, the carrier frequency is known and the signal at that frequency is also used in the demodulation process. This frequency is not known by the ARR. However, since the reader transmits continuous wave (CW) signal during tag transmission, we proposed to use the CW signal as the input to the mixer. So the clock is retrieved through the air, instead of using a LO. Figure 3 shows conceptually the signals in frequency domain during tag transmission. The reader sends a signal at a fixed frequency called the CW, f_{CW}, and the tag responds with a weak backscatter signal, f_{bsck}. The CW signal is used as an input to the mixer instead of the LO.

In the EPC Gen 2 standard, the reader initiates query process by transmitting a specific command or a set of commands at a particular frequency channel. This leads to a handshaking process that ends, most frequently, with the tag transmitting its ID. Therefore, two types of reader signal appear as inputs to the mixer: (1) unmodulated CW signal during tag transmission and (2) modulated signal during reader transmission. The synchronous detection method for the first type of reader signal is shown in Figure 4. The dotted lines display the frequency components at the various stages of the design. The signal to the LO is taken from RF signal path and is amplified and filtered to remove any modulation, i.e., the backscatter signal. The mixer outputs the difference of the frequencies (the sum of the frequencies is filtered out). At the output of a baseband filter, only the tag backscatter signal remains.

Let us now consider a situation when the reader transmits the modulated signal as presented in Figure 5. The reader signal is self-mixed with an attenuated or amplified version of itself. At the output of the mixer is the down-converted reader signal. The same bandpass filter as that in the case of tag transmission is used.

In order to implement this system, an external low gain loop antenna was used to provide an attenuated version of the signal for synchronous detection. Therefore, the ARR contains two antennas: one that performs 'listening' of tag communication and another one for receiving the CW signal and using it as an input to the mixer. We performed a number of experiments regarding the type of the second antenna and relative positions of two antennas until we determined the configuration that provided satisfactory results.

There are a number of advantages of synchronous demodulation with the reader signal used as an input to the mixer. The design of the receiver is simplified since there is no need for a PLL while at the same time the problem of frequency offset is resolved. Synchronous detection also resolved frequency-hopping problem when the pattern of hopping is unknown. As mentioned before, the reader selects its next frequency channels pseudo-randomly and the pseudo-random sequence of frequencies is not known to the ARR. Using synchronous detection with the reader signal instead of the LO, the ARR obtains the CW signal directly from the reader and use it as a local oscillator. Thus, regardless whether the reader is in frequency-hopping mode or not, the ARR receives the reader-transmitted signal at any frequency and uses it as a reference frequency for demodulation.

The system has an additional advantage in common situations where multiple ARRs associated with one reader are used. All ARRs are synchronized because they use the same clock from the reader. This can be very important for further research on localization of passive tags based on the signals obtained from multiple synchronized ARRs. In addition, multiple synchronized ARRs can be used for cooperative reception techniques like soft combining and interference cancellation as presented in [5].

Recently, there have been several publications that deal with extending the read range of the UHF readers. The

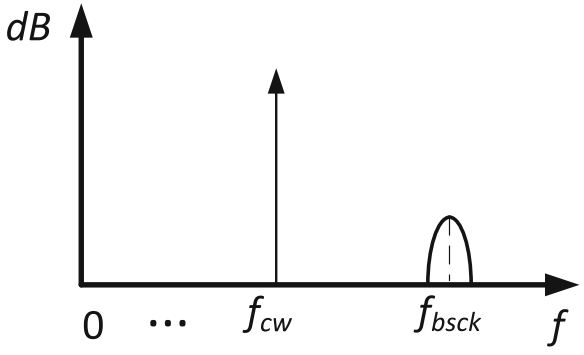

Figure 3 Spectrum during tag backscatter.

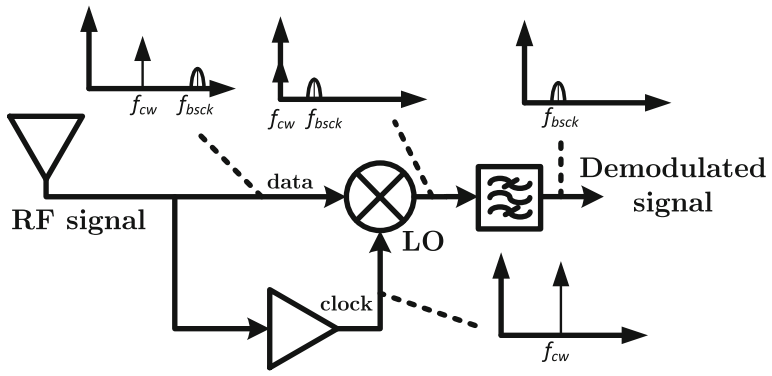

Figure 4 Synchronous detection during tag backscatter.

read range can be extended by adding the external exciters that provide CW signal [12] or by amplifying the signal from the reader [13]. Having external exciters will allow not only for providing additional energy, but also for using that signal as an external oscillator and having all elements in the system synchronized to the same clock. However, to the best of our knowledge, using CW from the external exciters to synchronize the RFID components has not been done yet; the same techniques as described in this paper can be used.

Limitations of our approach include the need to perform time multiplexing in case there are multiple readers in the same area, problems with a narrow-band interferers in the same frequency range, and the fact that the amplitude of the oscillator depends on the distance and on fading. Since tags are not frequency selective, some type of time scheduling of the readers would need to be done anyway in case of deployment with multiple readers. Regarding the amplitude of the signal, it is possible that the signal used instead of the LO received by the ARR is subject to deep fades in which case the ARR will not function properly.

Implementation

Figure 6 shows the high-level overview of receiver implementation. It consists of a UHF RFID reader IC acting as the RF front end and an FPGA with a soft-core CPU that implements the state machine for receiving the tag signals. Ethernet is used for communication with the host PC. The next sections will give the details of the subsystems in use.

Radio frequency integrated circuit

Austria Microsystems AS3992 was selected as the radio frequency integrated circuit (RFIC). The RFIC is an EPC Gen 2-compatible front end, which has a direct conversion RF section and EPC Gen 2 protocol handling capability.

Through register settings, the IC can support different modes and settings such as the gain of the receiver chain and filter selection. The reader IC also has provisions to decode tag signals by decoding the Miller and biphase space (FM0) encoding. By itself, the reader IC does not support receiving and decoding the pulse interval encoding (PIE) signal, so the decoding part was outsourced to another digital section.

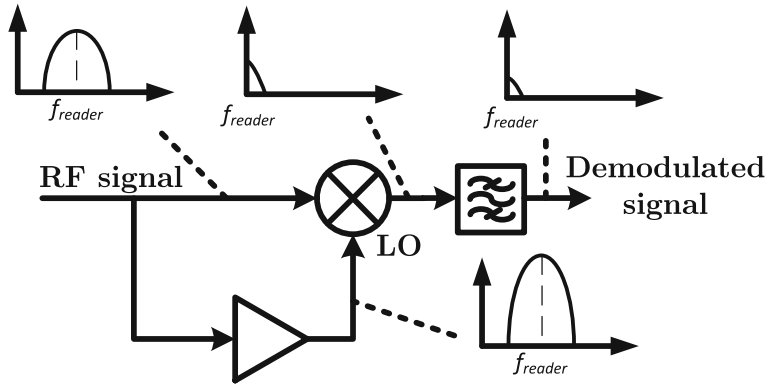

Figure 5 Synchronous detection during reader transmission.

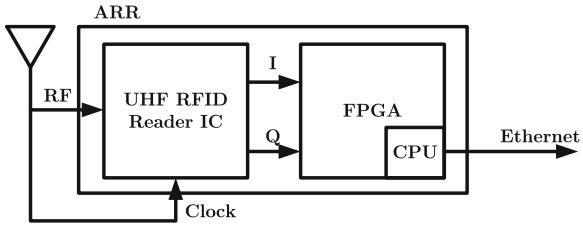

Figure 6 High-level block diagram.

Most reader ICs regularly operate solely, i.e., performing the demodulation, decoding, and protocol processing. The AS3992 was set to *direct mode*, where the protocol processing is bypassed and a demodulated analog or digital signal is output. In this mode, the chip acts only as an RF front end.

The IC also has an oscillator and timing system. Unfortunately, it cannot be used due to frequency offset problem. To mitigate the issue, synchronous detection was used. To achieve synchronous detection outlined in the previous section, the external VCO port, EXT_IN, was used on the AS3992. This pin allows us to set the frequency manually by retrieving it from the air.

An external low gain loop antenna was used to provide an attenuated version of the signal for synchronous detection. Another solution would be to use an amplifier on the RF signal path, but the power consumption and cost would rise.

The sensitivity of the receiver is configurable through register settings, which allows increasing or decreasing the read range of the receiver. The step size of the read range was experimentally determined to be around 50 cm.

The outputs from the RF section are the I and Q datapaths. Figure 7 shows the reader-tag exchange as seen by the AS3992 chip using synchronous detection. The Q-channel can be seen to have a higher amplitude than the I-channel. Figure 8 shows the block diagram of the components used from the IC. The output from the AS3992 to the digital section is the signal after passing through the comparator.

FPGA subsystem

Figure 9 shows the block diagram of the hardware. This section describes the details of each block in the system. The main blocks in the architecture are the reader PIE decoder, FM0 decoder for the tag signal, reader command decoder, and tag command decoder. Logic gates are used for enabling and disabling the decoding of tag signals. Once the ARR receives an *ACK* from the reader, the gates are opened for decoding the tag signal. The system was implemented in Verilog, and it is executed on a Xilinx Spartan 3E starter kit (San Jose, CA, USA).

Reader decoder

The PIE decoder module samples the input waveform and outputs the data symbols; it also provides a symbol clock, which rises whenever a symbol has been decoded. The symbols come in six varieties: *data-0*, *data-1*, *TRcal*, *RTcal*, *invalid*, and *delim* [10]. They convey information about the commands, data, and physical characteristics of the channel between the reader and tag. The symbols can also have different parameters depending on the *TARI* (length of data-0) value set by the reader.

The signal is over-sampled by 625 samples due to the default clock of 50 MHz on the FPGA, which can be lowered if power consumption is a concern. A lookup table is

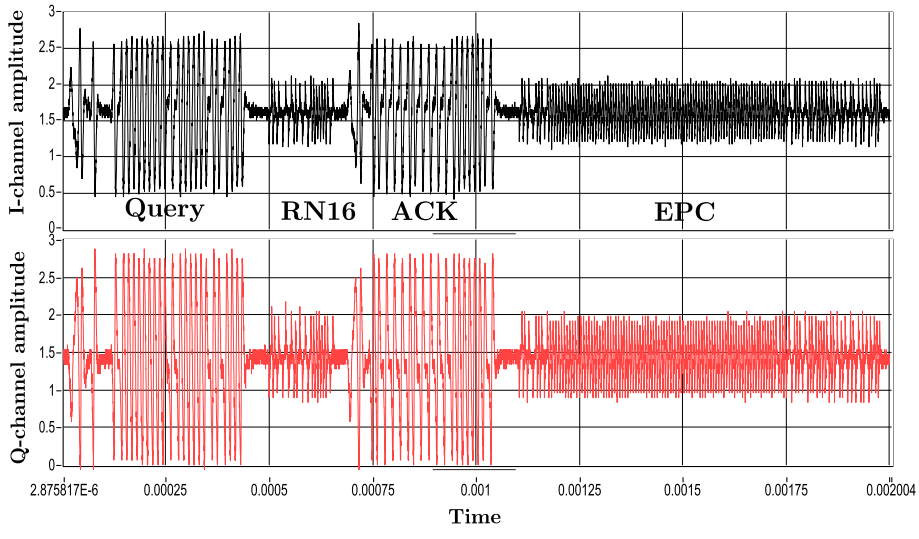

Figure 7 AS3992 analog output.

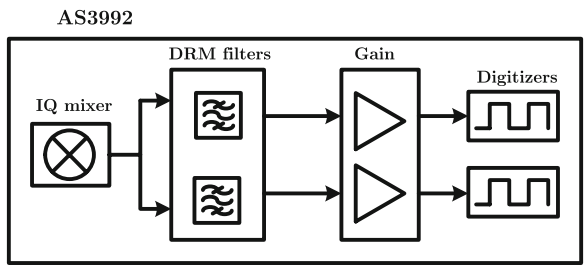

Figure 8 Block diagram of digital logic including decoders and a soft core processor implemented on FPGA.

used to determine the symbol. A counter *hi_cnt* is started on a high signal. Whenever a falling edge is detected, a counter *lo_cnt* is started and the *hi_cnt* is stopped. A rising edge indicates the end of a symbol. Furthermore, the type of symbol: *TRcal*, *RTcal*, *data-0*, *data-1*, *invalid*, and *delim* is determined from the length of the symbol, and the high count is determined through a lookup table. The low count is only needed to determine the mode of operation. The command decoder is a state machine that is sensitive to symbols from the PIE decoder and outputs commands from the reader.

Tag decoder

The tag decoder decodes the FM0 signal. The method used for decoding this signal is a modified version of an existing method [14]. A close look at the FM0 waveforms reveals that the rectangular waveform shown in Table 2 can be identified. The method based in [14] proposed looking at the duty cycles of the rectangular waveforms to decode them. Duty cycle requires a division operation which is not efficient in FPGAs. The method used in this implementation is a modified version, where a lookup table is used to compare the high and low counters to symbol values that are obtained experimentally. After receiving the decoded bits, they are passed through the tag command decoder which groups the bits together to determine commands, including the EPC of the tag.

Experimental results

Range

The first set of experiments on the ARR was performed to characterize its performance based on the distance from the reader. The design of the receiver relies both on the reader and tag signals to successfully decode EPCs. A tag is considered successfully read if an ethernet packet is received containing the tag's EPC. Wireshark [15] was used to count the number of packets, which was an indicator for performance. The reader was set to hybrid mode, 160-kHz FM0, 30-dBm output power for 60 s. A Higgs3 [16] passive dipole and PowerP [17] semi-passive tag were used for the tests.

Reader range

First a passive dipole and then a semi-passive tag were placed at a distance of 1 m away from the receiver. The reader antenna was set to output at full power. The distance between the ARR and the reader antenna, *d*, was increased from 1 to 8 m, with an interval of 1 m. Figure 10 shows the read rate results for both semi-passive and passive tags, where read-rate is defined as the number of ethernet packets received by the host per minute. At some distances, the effects of multipath propagation and fading made the tag unreadable. In such cases, the reader antenna was slightly moved to the side to mitigate this effect.

The results show that the distance from the reader to the receiver does not affect the performance when the distance is within 8 m, which is the room length. Semi-passive tags have a read rate of about 140 to 160 packets per minute, while passive tags read at under 100 packets per minute.

Maximum range

The goal of this experiment was to determine the maximum distance that the receiver can detect the tag response. A similar setup was made in the previous experiment, but the distance *d* was fixed at 8 m, while the distance from tag to receiver was varied. The reader was

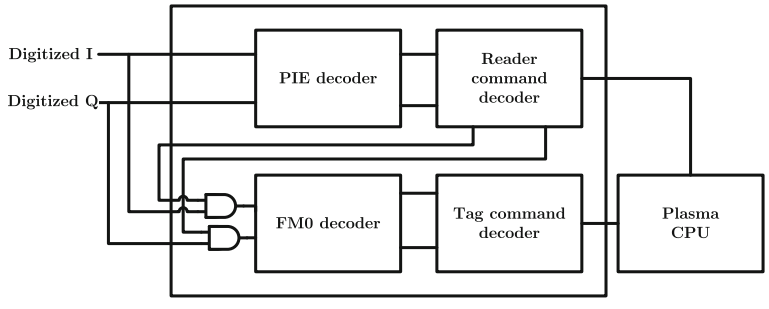

Figure 9 FPGA system.

Table 2 Rectangular waveform decoding

Symbol	Waveform	Bit(s)
RW0		10
RW1		11
RW2		0
RW3		1

set to transmit for 60 s, and the tag was moved away from the receiver until the receiver could not detect the EPC anymore. A test was made without ethernet sending: a counter was implemented on the FPGA and ethernet was disabled. The reader was set to transmit a *query* every second for 60 s. A logic analyzer was then used to get the counter value. A tag was considered detected if the receiver could read more tag signals than 5% of the EPCs. For passive tags, this distance was determined to be 3.25 m, and for semi-passive, it was determined to be 5.5 m. Depending on the application, the range can be reduced by adjusting the attenuation registers of the AS3992 chip.

Reader power

This experiment tests the relationship between the reader power and the receiver performance. The reader antenna was placed at a fixed distance of 5 m, and the reader output power was varied from 15 to 30 dBm. A passive tag was placed in between the reader and the receiver, which is 1 m away from the receiver. The read rate of the receiver was recorded. Figure 11 shows the results.

At the 22-dBm mark, the performance decreases significantly. This is the threshold where the receiver does not receive enough power to its local oscillator to correctly decode the tag. Based on the Friis equation, the power at the LO port can be estimated to be −12 dBm at this power and distance. Thus, theoretically, if the reader is located at a distance of 12.5 m and is transmitting at full strength, the receiver will have enough power for its LO port.

Comparison

Table 3 presents a comparison of the maximum read ranges of the different receivers. The Sensatag and ARR implementations were determined experimentally, while the Gen 2 Listener value is based on [4].

The values of the table are to be expected. The Sensatag, based on an envelope detector, provides the worst performance of the three. The Gen 2 Listener, based on an software-defined radio (SDR), provides the best performance. The ARR implementation shows results that fall in between the Sensatag and Gen 2 Listener. Table 4 compares the success rate at which the EPC packets were successfully decoded at a 1-m distance. The results for the Gen 2 Listener were taken from [5], while the ARR and Sensatag results were obtained experimentally. For the experimentally obtained results, a passive tag was placed 1 m away from the receiver, and the tag antenna was placed 5 m away from the receiver. The reader was programmed to send a query every second for 60 s.

Analysis

The Gen 2 Listener offers the best performance in read range and read rate, but it has a limitation due to frequency hopping. The results presented were obtained with a reader transmitting at a fixed channel. The Gen 2 Listener was originally designed to operate in Europe,

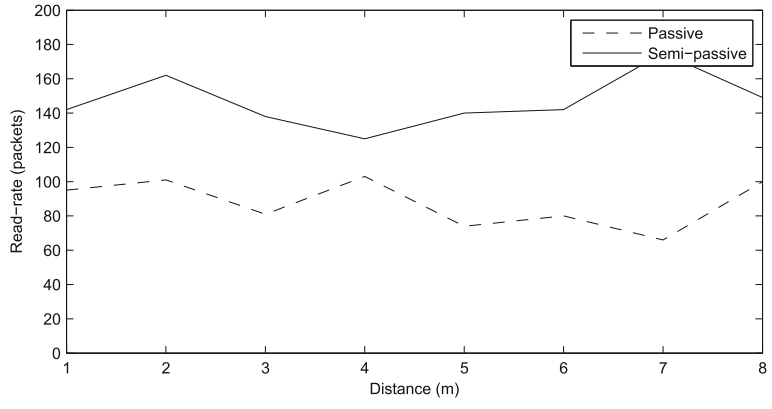

Figure 10 Reader range vs read rate.

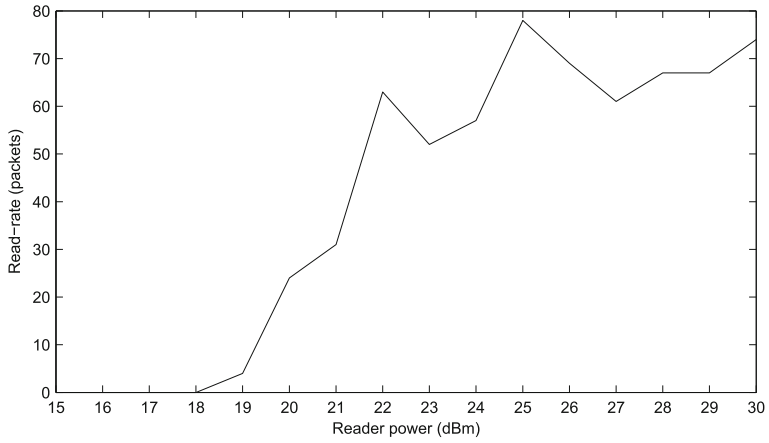

Figure 11 Reader power vs read rate.

where UHF RFID has 2 MHz allocated to it. In North America, the device is able to listen to only four channels at a time due to this limitation. EPC responses being sent from the other 46 channels will not be captured. Another limitation is the cost of the hardware. The USRP, on which the SDR is running on, costs around $1,000, limiting wide-scale deployment needed in cases such as for proximity localization.

The Sensatag is a low-cost solution compared to the Gen 2 Listener and the ARR. The device consists of mostly passive components, making it to have low power consumption and can be run from batteries. The use of an envelope detection scheme limits its performance as can be seen from the tests. Another issue is variable selectivity due to the architecture in use: in some channels, the device will be able to decode EPCs, while in others, it may not. The ARR offers better performance than the Sensatag but worse than the Gen 2 Listener. Its advantage is that it overcomes the limitations of both approaches. The use of an industry UHF RFID reader IC as the RF section cuts down costs compared to the USRP, allowing it to be widely deployed for use in localization methods. Using synchronous detection deals with the frequency-hopping issue and the limitation of the Gen 2 Listener. An issue for the ARR is the time to form a packet to be transmitted over the ethernet: EPCs could be discarded if the reader is sending queries continuously. This problem can be corrected by implementing a counter for the EPCs and sending ethernet packets at fixed intervals with the counter value, not in real-time, as soon as an EPC has been received, as it is done now. Another limitation is that two readers cannot be used at the same time, unless they transmit in a time-multiplexed fashion.

Applications

Besides the aforementioned receiver for localization, the device can be adapted by other applications. These include a portal, protocol analyzer, and Internet of Things sensor.

An RFID portal can be used to track people or packages passing through some area. For the ideal RFID portal system, the reader should achieve 100% read accuracy when tags pass through the confined area. The reader should not read them when they are not present in the confined area. The read accuracy performance is the most important factor for RFID portal systems, but they experience the problems of cross-reads - a tag that is outside of the confined area is read. Using the device described in this paper, a confined area can be created, without having to lower the power of the reader antennas.

During the development and implementation of a wireless system, it can be beneficial to have a test tool to debug, analyze, and monitor the wireless network. Industry test tools have limited specific functionality and very high costs. The device outlined in this paper can be used as a low-cost test tool for UHF RFID. Researchers will have the ability to test their hypotheses for new anti-collision algorithms, frequency-hopping techniques, channel coding optimizations, etc., without delving into time-consuming simulations and expensive equipment.

Table 3 Maximum read ranges

Tag type	Sensatag (m)	ARR (m)	Gen 2 listener (m)
Passive	0.6	3.25	*>12*
Semi-passive	1.45	5.5	N/A

Table 4 Ratio of the tag EPCs sent to device EPCs received

Tag type	Sensatag	Receiver	Gen 2 listener
Passive	17%	50%	70% [5]

The Internet of Things refers to a concept of devices connected in an Internet-like structure and having unique identifiers [18]. Since passive RFID tags are inexpensive and provide automatic identification, they are a good candidate technology for IoT. By themselves, they only provide limited information, but by introducing localization and proximity detection, more complex operations can be performed and a more capable IoT network can be created. A potential application for the ARR is an IoT sensor. The ARR acts as a gateway between the tags and the Internet-like structure. The gateway attaches a location identifier to the tags which are in its proximity, thereby allowing a more capable system.

Conclusions

UHF RFID systems offer only coarse-grained knowledge of the location of the tag. One localization method, which is easy to implement and is not affected by dynamically changing environments, is proximity localization. This paper proposes a new receiver, called the ARR, which can be used for proximity localization. In this work, a conventional UHF RFID IC, in combination with an FPGA was used to create the receiver, which augmented the RFID system. The use of conventional IC allows for a cost-effective way of implementing the system. The conventional IC is modified to use synchronous detection to overcome synchronization issues - frequency hopping and frequency offset.

The augmented RFID receiver offers good performance and low cost due to the use of an industry UHF RFID reader IC and novel way of synchronizing with the reader. Quantitatively, the receiver achieved a read rate of 50% for a passive tag and 66% for a semi-passive tag that are placed 1 m away. With the maximum range, between the ARR and the tag with the reader located within 8 m of the ARR, the receiver can decode EPCs properly at 3.25 m for passive and 5.5 m for semi-passive tags.

Abbreviations

ARR: augmented RFID receiver; CW: continuous wave; DC: direct current; EPC: electronic product code; FPGA: field gate programmable array; I/Q: in-phase/quadrature; IC: integrated circuit; IoT: Internet of Things; ISM: industry: medical: scientific; LLRP: low-level reader protocol; LO: local oscillator; PIE: pulse interval encoding; PR-ASK: phase reversal amplitude shift keying; RFIC: radio frequency integrated circuit; RFID: radio frequency identification; RSS: received signal strength; SDR: software-defined radio; UHF: ultrahigh frequency; USRP: universal radio peripheral; VCO: voltage-controlled oscillator.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

We would like to thank Natural Sciences and Engineering Research Council of Canada for supporting this work through the NSERC Discovery grant. We would also like to thank Astraion LLC for providing us with the equipment (Sensatags).

Received: 7 October 2012 Accepted: 9 August 2013
Published: 27 August 2013

References

1. M Bolić, D Simplot-Ryl, *RFID Systems: Research Trends and Challenges* (Wiley, New Jersey, 2010)
2. L Jing, Z Cheng, Y Zhou, J Wang, From U-tile to indoor-tracer: an indoor location sensing platform based on passive RFID. The 2011 IEEE International Conference on Internet of Things and The 4th IEEE International Conference on Cyber, Physical and Social Computing, Dalian, 19–22 Oct 2011 (IEEE, Piscataway, 2011), pp. 89–93
3. A Athalye, V Savic, M Bolic, P Djuric, A radio frequency identification system for accurate indoor localization. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Prague, 22–27 May 2011 (IEEE, Piscataway, 2011), pp. 1777–1780
4. D Donno, F Ricciato, Design and applications of a software-defined listener for UHF RFID systems, *in Microwave Symposium Digest (MTT)*. 2011 IEEE MTT-S International Microwave Symposium Digest, Baltimore, June 2011 (IEEE, Piscataway, 2011), pp. 6–9
5. D Donno, F Ricciato, L Catarinucci, Challenge: towards distributed RFID sensing with software-defined radio, in *MobiCom '10.* Proceedings of the Sixteenth Annual International Conference in Mobile Computing and Networking, Chicago, Sept 2010 (ACM, New York, 2010), pp. 97–104
6. L Catarinucci, D Donno, Performance analysis of passive UHF RFID tags with GNU-radio. 2011 IEEE International Symposium on Antennas and Propagation (APSURSI), Spokane, July 2011 (IEEE, Piscataway, 2011), pp. 541–544
7. H Chen, A Bhadkamkar, Piggyback modulation for UHF RFID sensors, in *Microwave Symposium Digest (MTT).* 2010 IEEE MTT-S International Microwave Symposium Digest, Anaheim, May 2010 (IEEE, Piscataway, 201), pp. 1776–1779
8. GS1, *Regulatory status for using RFID in the UHF spectrum,* Technical report, GS1, 2011
9. EPC Global, Low level reader protocol. http://www.gs1.org/gsmp/kc/epcglobal/llrp/llrp_1_1-standard-20101013.pdf. Accessed 8 Mar 2010
10. EPC Global, Specification for RFID air interface EPC™ radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz - 960 MHz. Technical report, GS1, 2008
11. X Zhang, M Tentzeris, Applications of fast-moving RFID tags in high-speed railway systems. Int. J. Eng. Bus. Manag. **3**, 1 (2011)
12. JS Park, JW Jung, SY Ahn, HH Roh, HR Oh, YR Seong, YD Lee, K Choi, Extending the interrogation range of a passive UHF RFID system with an external continuous wave transmitter. Instrum. Meas IEEE Trans. **59**(8), 2191–2197 (2010)
13. SY Ahn, JS Park, YR Seong, HR Ohd, Jm Kim, BoMR: a booster for mobile RFID readers. 2011 International Conference on ICT Convergence (ICTC), Seoul, Sept 2011 (IEEE, 2011), pp. 161–165
14. N Bautista, Enhanced FM0 decoder for UHF passive RFID readers using duty cycle estimations (RFID-TA), vol. 2011 (IEEE, Piscataway, 2011). http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6068654. Accessed 18 July 2013
15. Wireshark Foundation, WireShark (2012). http://www.wireshark.org/. Accessed 18 July 2013
16. Alien Technology, Higgs-3 (2013). http://www.alientechnology.com/wp-content/uploads/Alien-Technology-Higgs-3-ALC-360.pdf Accessed 8 September 2013
17. PowerID, PowerP RFID labels for people (2012). http://www.power-id.com/Data/pdf/PowerP_0311.pdf Accessed 18 July 2013
18. IoT-a, Internet of Things Architecture (2013). http://www.iot-a.eu/public Accessed 18 July 2013

doi:10.1186/1687-1499-2013-214
Cite this article as: Borisenko *et al.*: Intercepting UHF RFID signals through synchronous detection. *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:214.