7

Development of Sensing and Computing Enhanced Passive RFID Tags Using the Wireless Identification and Sensing Platform

Alanson Sample[1,2], Daniel Yeager[1], Michael Buettner[1] and Joshua Smith[2]
[1]*University of Washington,*
[2]*Intel Research Seattle*
USA

1. Introduction

Passive RFID tags are becoming increasingly common in home and work environments. As RFID tags find new applications beyond shipment tracking, they are being embedded in objects throughout our environment. RFID tags are already being incorporated in credit cards for touch-free payments, in clothing for merchandise tracking, and in ID cards for building access control.

All these "non-shipping" RFID tags are powered wirelessly and are capable of wireless communication and rudimentary computation. Thus they can be viewed as micro-computing platforms with wireless power and communication capabilities. While the functionality of today's passive RFID tags is extremely limited, today's tags can already be thought of as a layer of invisible computing that is seamlessly embedded in objects throughout the environment. This primitive layer of embedded intelligence could grow in sophistication if additional sensing and computation capabilities could be added to RFID tags.

The authors' goal is to evolve this layer of passively powered embedded intelligence by creating RFID tags that support sensors and can execute general purpose computer programs. This chapter reviews several years' work on the development of our open, programmable passive RFID tag, the Wireless Identification and Sensing Platform (WISP). It also shows how to use the EPC Class 1 Generation 2 RFID protocol to implement advanced RFID sensing applications that go far beyond simple tag ID inventorying applications.

Our first venture into sensor-enhanced RFID was the α-WISP shown in Figure 1 (Philipose et al., 2005). With this device, one bit of sensor data was encoded by using anti-parallel tilt switches to multiplex one of two RFID tag ICs to a single antenna. Thus, a reader could infer three states about a tagged item (tag right side up, upside down, or not present). This simple example of overloading the EPC ID to encode sensor data allowed inference of very coarse orientation information. However, the use of commercial RFID tag ICs restricted our ability to control the RFID communication channel and in turn our ability to configure WISPs for new applications.

Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria

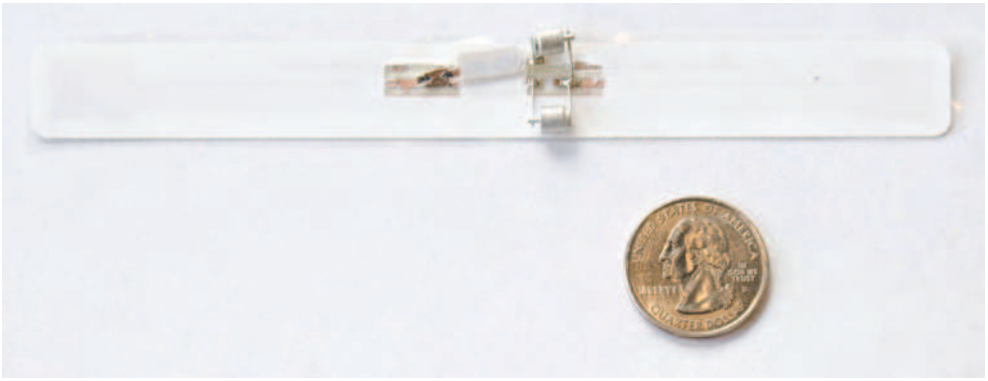

Fig. 1. The α-WISP uses two tilt switches orientated in opposite directions as a simple one bit RFID accelerometer.

In order to fully investigate passive RFID applications, we developed the general purpose Wireless Identification and Sensing Platform (simply called WISP) (Sample et al., 2008). Shown in Figure 2, the WISP is a battery-free, programmable RFID sensor device. Compliant with the Electronic Product Code (EPC) Class 1, Generation 2 protocol, the WISP can transmit multiple bytes of data per query and is fully configurable due to its ultra-low power 16-bit general-purpose microcontroller. Similar to conventional passive UHF RFID tags, the WISP has no batteries and is completely powered via the RF energy transmitted by an RFID reader.

The architecture of the WISP allows measurement of virtually any low power sensor which can also be wirelessly powered by the RFID reader. The WISP is implemented as a printed circuit board (PCB), which offers a flexible platform for exploring new sensor integration schemes and applications. To the authors' knowledge, the WISP is the first passive UHF RFID tag with an integrated microcontroller and has an operating range of several meters.

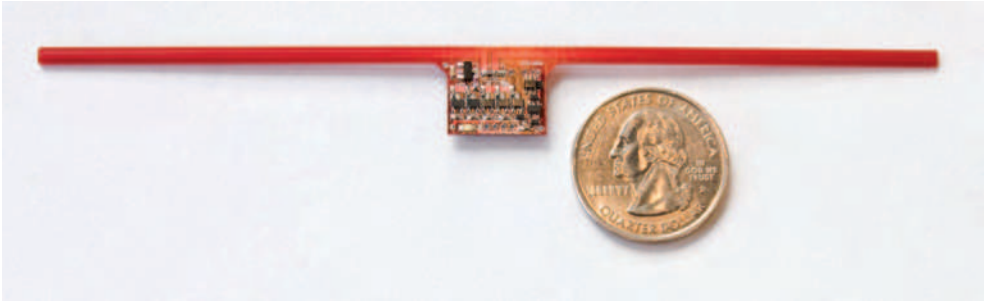

Fig. 2. Wireless Identification and Sensing Platform (WISP)

The first few section of this chapter presents an overview of the WISP platform including a detailed explanation of the architecture and power management algorithm. In particular, performance metrics describing operational range and real world performance are presented. Section 5 presents an over view of how the Electronic Product Code (EPC) Generation 2 Class 1 protocol is used to create a bi-directional communication channel for sending data to and from the a RFID reader. Section 6 explores the application space of the

WISP. This platform is intended to be a vehicle with which researchers can quickly investigate new and innovative applications in RFID. To highlight this concept several case studies of recent applications using the WISP are presented; for example, using the WISP to increase the security of RFID systems, and as a passive data logging device.

2. Prior work

To date there are several approaches to enhancing RFID tags with sensing capabilities. One method is to use standard commercial tag ICs and alter their functionality to transmit sensor data, as was done in the case of the α-WISP. The authors in (Johan et al., 2007) describe a humidity sensor for detecting moisture in walls of buildings and houses by placing a sponge in front of a tag. Moisture in the sponge detunes the tag's antenna, allowing the approximation of humidity levels from the read range of the tag. Another approach uses a custom tag with a built in fuse for sensing high temperatures in food products. The fuse melts above a particular threshold which enables or disables the tag (Watters et al., 2002). These passive tags based on physical properties are extremely limited in what they can report and are not reusable.

Other efforts have been made to retrieve richer, multi-bit sensor data from RFID tags for a wide variety of applications. Possible applications include infrastructure and object monitoring, automatic product tamper detection, identification of harmful agents, and biomedical devices for noninvasive monitoring (Want, 2004). To enable these applications two regimes have been explored: active battery-powered tags and passive battery-free tags.

Active tags, a subclass of RFID, are essentially wireless sensor nodes (Polastre & Szewczyk, 2005) (Savi Technology, 2006). They use batteries to power their communication circuitry, sensors, and microcontroller. Active tags benefit from a relatively long wireless range (approximately 30 m) and can achieve high data and sensing rates. An active tag with adaptive analog sensor thresholds for triggering sensor measurements was proposed in (Malinowski, et al., 2007). However, these devices require batteries which are a drawback when considering the cost, weight and volume of the device, and the need to replace the dead batteries.

In contrast, passive sensor tags receive their operating energy from the RFID reader which gives them a life time of years, if not decades. Examples of application-specific, non-programmable UHF passive tags with integrated temperature and light sensors, as well as an Analog to Digital Converter (ADC) can be found in (Namjun et al., 2005) and (Kocer & Flynn, 2006). One attractive feature of passive sensor tags is the prospect of permanently embedding them in objects for structural, medical, or product monitoring. Another advantage is their suitability for applications in which neither batteries nor wired connections are feasible, for weight, volume, cost, or other reasons. Of course, the limitation of purely passive sensor tags is the requirement of proximity to an RFID reader. However, methods such as solar, thermal, or kinetic energy harvesting could be used as a secondary power source if needed.

A further consideration is the configurability and computational power of RFID sensor tags. Existing devices are generally fixed-function with respect to sensory inputs and lack computational capabilities. A commercially available RFID tag with limited additional functionality is described in (Microchip Technology Inc, 2005); however, this device can only transmit one bit of sensor data in addition to its ID. Furthermore, it is limited by a short read range due to its 125 kHz operating frequency.

3. WISP architecture

The WISP is manufactured as a printed circuit board (PCB) which offers a number of advantages compared to traditional Integrated Circuit (IC) tag designs. Primarily low development cost, fast design cycles, and easy debugging and measurement of circuit parameters. The PCB implementation allows the flexibility to physically add and remove sensors and/or peripherals to create devices for new applications. In contrast, IC implementations offer the ability to customize components and decrease power consumption (yielding better range), as well as creating devices with a smaller form factor and at a lower cost when manufactured in high volume.

A block diagram of the WISP is shown in figure 2 and is similar in function to traditional IC RFID tags. The antenna is balanced by an impedance matching network and is fed into the RF power harvester. The Radio Frequency (RF) signal transmitted by the RFID readers is rectified into DC power to power the rest of the tag. The demodulator block converts the Phase-Reversed Amplitude Shift Keyed (PR-ASK) data that is superimposed on the RF carrier into a logic level steam of serial data. This extracted serial data is parsed by the MSP430 microcontroller (MCU) to receive downlink data from the reader. Uplink data is sent via the modulator circuit, which "back-scatters" the signal by changing the antenna impedance. Finally, the microcontroller's internal temperature sensor, as well as any external sensors, are powered and measured by the MCU.

As the power consumption of the microcontroller, sensors, and peripherals are much greater then that seen in traditional passive RFID technology, the WISP duty cycles between active and sleep mode. In sleep mode, the WISP shuts down and reduces its current consumption to a few micro-amps and energy is accumulated by the harvester block over multiple EPC queries. Once sufficient voltage is obtained, the WISP polls sensors and communicates with the RFID reader.

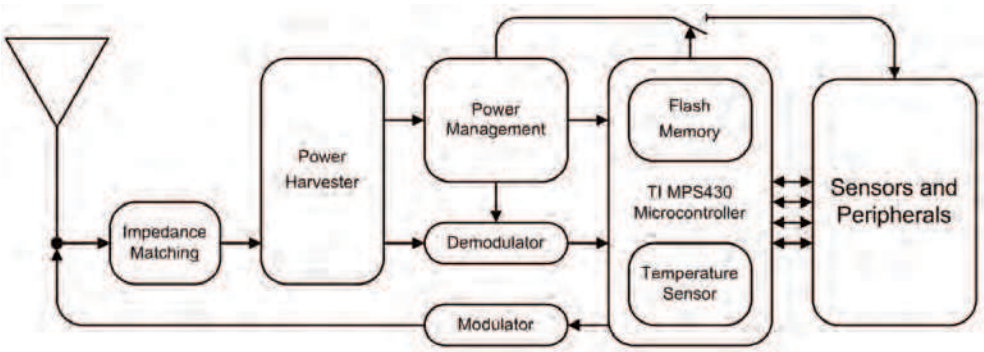

Fig. 3. Block Diagram of the WISP

Figure 3 depicts the WISP platform, made of a four layer FR4 PCB with components on both sides and an integrated dipole antenna. The WISP in its base configuration has several onboard sensors: a circuit for measuring the rectified supply voltage, a temperature sensor, and a 3D accelerometer. Small header pins expose all ports of the microcontroller for expansion to daughter boards, external sensors, and peripherals. Finally, a low current surface mount LED is included in the design.

3.1 RF power harvesting

The defining characteristic of far field RFID systems is that tags can be read at a significant distance, generally on the order of 2-10 meters. For passive RFID this requires that the RFID reader transmits sufficient energy to power the tag at large distances. However, due to regulatory limits on the amount of power that can be transmitted and the path loss associated with electromagnetic propagation, there is very little power that actually reaches the tags. Therefore, the power harvesting circuit must maximize the operating distance by converting the very limited incoming RF power to DC power with sufficient voltage to activate the tag.

The RF power received by the WISP's dipole antenna is fed to the analog front end depicted in figure 4. A discrete matching network is used to provide the maximum power transfer from the antenna to the rectifier. RF Schottky diodes specifically designed for 915MHz low power application were selected to make a five-stage voltage doubling circuit. This circuit converts the AC input signal to DC power which is fed into a storage capacitor.

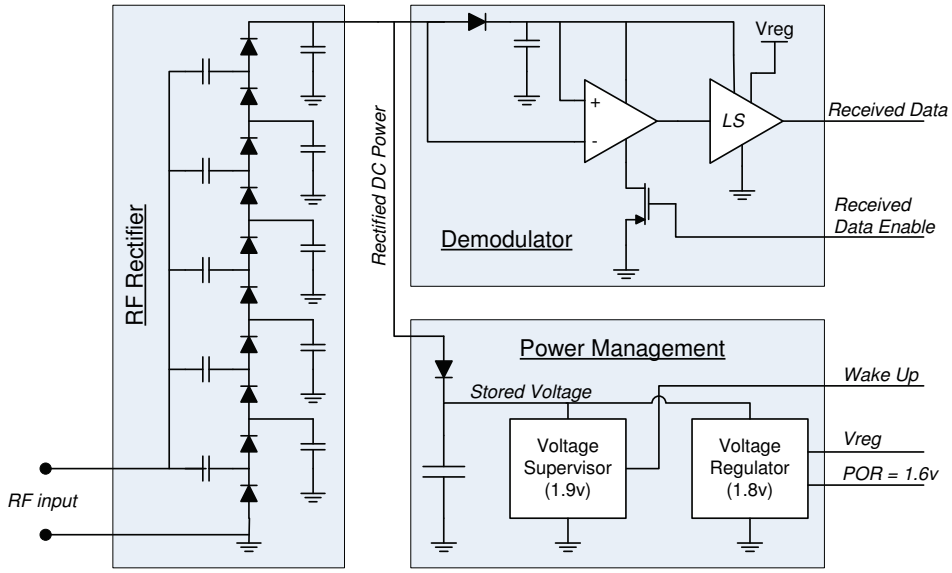

Fig. 4. Schematic of the Analog Front End

For RF rectifiers of this type, the input and output impedances are not well isolated. Further confounding the problem is that the output impedance of the rectifier is fairly high; an undesirable trait for any power source. This means that as the load on the rectifier changes the input impedance also changes, resulting in the analog front end becoming mismatched to the antenna. This leads to the problem of selecting values for the impedance matching network when it is not possible to guarantee constant input impedance.

To determine the correct values for the matching network the operating cycle of the WISP must be taken into account. First, the WISP is most effective at storing harvested energy when it is in sleep mode, as the current consumption is minimal. Second, the WISP will spend most of its time repeatedly charging up to 1.9v and then discharging to approximately 1.8v. Thus, to determine the correct values the WISP is put in sleep mode and

we find the impedance matching network that produces 1.9v for the lowest possible input power. Stated another way, the key parameter for maximizing the read distance of the WISP is minimizing the quiescent current consumption so that the minimum operating voltage of 1.9V (supervisor threshold) can be rectified with the lowest possible input power.
To characterize the system, a network analyzer was used to inject a continuous 915 MHz waveform into the antenna ports of the WISP. Using the minimum input power needed for activation, the expected operating distance for the WISP can be calculated with the logarithmic form of the Friis path loss equation (1), with a term for polarization mismatch included.

$$P_R = P_T - 20\log\left(\frac{4\pi d}{\lambda}\right) + G_T + G_R - L_P \quad (1)$$

The transmit power of the reader P_T = 1 W = 30 dBm. Its center frequency is 915 MHz, corresponding to a wavelength (λ) of = 0.33 m. The transmit antenna gain G_T = 6 dBi (this yields an effective isotropic radiated power (EIRP) of 4 W, the United States regulatory limit for this ISM band). The receive antenna gain G_R = 2 dBi (the standard gain figure for a dipole antenna), and the polarization loss L_P = 3dB. Loss L_P occurs because only half of the power transmitted from the circularly-polarized transmit antenna is received by the linearly-polarized receive dipole antenna. Using the experimentally determined operating thresholds of -9.5 dBm, equation 1 predicts a maximum operational range of 4.3m.
It should be noted that practical implementation of the WISP yields an operating range of approximately 3 meters. There are a number of contributing factors: the WISP antenna gain used in equation 1 is estimated not measured, and in the above experiment a continuous 915MHz signal was injected and the storage capacitor was charge to its steady state. Real RFID systems send out bursts of packets (power and data) with long periods of no signal between them. In this case the discharge rate of the storage capacitor must be taken into account. Finally, as with any far field RFID system, constructive and destructive interference due to multi-path plays a large role in real world results.

3.2 Demodulation and modulation

The EPC Gen 2 standard defines that reader-to-tag communication uses ASK modulation on a carrier wave in the range of 902-928 MHz. When not transmitting data the carrier waveform remains at a constant amplitude; when bits are transmitted, the amplitude of the carrier drops to at least ten percent of its normal value and the phase of the carrier may be reversed. The duration of the continuous waveform between these low amplitude pulses indicates logical "ones" or "zeros."
Figure 3 shows a schematic of the WISP's demodulator circuit. The output of the harvester is fed through the diode, which supplies power to the comparator and acts as a reference for the level shifter. A capacitor is used to filter out transients while allowing proper biasing at varying distance and receive power levels. When activated, the current consumption of the comparator functions as a constant-current source, pulling current through the diode. In this way, the voltage drop across the diode is used as a detector, where current supplied by the harvester (high amplitude RF modulation) results in positive voltage, and a lack of current (low amplitude RF modulation) yields negative voltage. The comparator is used to generate a rail-to-rail logic level waveform, and the level shifter converts the unregulated logic level to the regulated logic level. It is important to optimize current consumption and speed when

choosing a comparator. Further savings can be achieved by disabling the comparator when there is insufficient voltage to start up the MSP430.
Passive RFID tags do not actively transmit radio signals. Instead, they modulate the impedance of their antenna which causes a change in the amount of energy reflected back to the reader. This modulated reflection is referred to as back-scatter radiation. To change the impedance of the antenna a transistor is placed between the two branches of the dipole antenna. When the transistor conducts current, it short-circuits the two branches of the antenna which changes the antenna impedance; in the non-conducting state the transistor has no effect on the antenna, and thus the power harvesting and data downlink function as if it were not present.

3.3 Digital section and power conditioning

As the power available to RFID tags is extremely limited, careful component selection is critical to minimize current consumption. With advances in IC manufacturing that allow discrete components with current consumption in the range of 1 μA and operation at 1.8 V, it is now possible to construct functional, wirelessly powered RFID tags with discrete components.
The general purpose computation capability of the WISP is provided by an ultra low power microcontroller. This 16-bit flash microcontroller, the MSP430F2272, can operate at up to 4 MHz with a 1.8 V supply voltage and consumes approximately 600 μA when active at this frequency and voltage. Of particular interest for low power RFID applications, the MSP430 has a number of low power modes. Its minimum RAM-retention supply current is 0.1 μA at 1.5 V. The device provides over 8 kilobytes of flash memory, 256 bytes of RAM and a 10-bit, 200 kilo-samples-per-second Analog to Digital Converter (ADC). The low power consumption of this device is a critical factor in enabling a general purpose microcontroller in passive RFID systems.
Another critical design consideration is operation with uncertain power supply conditions. Because the available RF power varies greatly during device operation, supervisory circuitry is necessary to wake and sleep the device based on the supply voltage level. The WISP uses a 1.9 V supervisor and a 1.6 V power-on-reset to control device state and reset the microcontroller, respectively. The supervisor provides roughly 100 mV of headroom on the large storage capacitor above the 1.8 V regulator voltage. This serves to buffer the supply voltage from dropping below 1.8 V due to the large power consumption of the microcontroller in active mode.

4. Low level firmware and power management algorithm

The WISP is essentially a software defined RFID tag which uses the MSP430 to implement the EPC Gen 2 Class 1 protocol and performs sensing and computation tasks. There are significant challenges when developing applications on the WISP as compared to battery powered embedded systems. Primarily, there is no guarantee that a given task can be completed before running out of power. Although the voltage supervisor provides headroom above 1.8 V, the rate at which the energy stored in the supply capacitor is consumed is directly affected by the design choices of the programmer. Failure to properly manage sleep cycles, when the WISP harvests energy, or inefficient coding practices can result poor performance.

The WISP software can be described on three levels. At the lowest level is the power management algorithm which is responsible for managing the device state, including sleep vs. active modes. Built on that is the communication layer, which enables bi-directional communication by sampling downlink data bits, implementing a Gen 2 state machine, and generating uplink data bits. The third level is the application layer where users implement costume function and encoding data in the appropriate EPC packets.

4.1 Power management algorithm

Meeting the low power requirements of passive RFID tags requires that the MCU consumes, on average, as little power as possible. As mentioned previously, this is achieved by duty cycling between active and low power sleep states. The key is that the WISP receives a constant amount of power as defined by Friis path loss equation 1 for a set distance. When the WISP is in active mode the power consumption far exceeds the power harvested. However, when the WISP is in sleep mode the total current consumption of all the circuits is a few micro-amps and there is a net power gain which charges the storage capacitor. Therefore, duty cycling does not simply yield lower power consumption; it represents two different states, power harvesting and active operation.

The state diagram for the power management layer is shown in figure 5. State transitions are primarily driven by hardware interrupts from the voltage supervisor, which indicate if there is sufficient energy stored for operation. Initially the WISP is way from a RFID reader and is in a power down state. When the WISP is brought with in range of a reader it begins to harvest power and the voltage on the storage capacitors begins to rise. At approximately 1.6 V the MSP430 powers up in a reset state and begins executing code. Since this event is not driven by the supervisor it is important to enter sleep mode (LMP4) as quickly as possible in order to avoid browning out and thrashing on start up. Once in LMP4 the WISP waits for sufficient voltage (1.9 V) as indicted by the supervisor interrupt. Next, the state machine transitions to the application layer which performs user defined functions such as sensor measurements. Here an EPC packet is generated and the WISP sets up and waits from a commutation interpret which indicates the beginning of an EPC packet. In the communication layer the WISP processes the incoming data, executes the EPC Gen 2 protocol and transmits its response. While not shown in figure 5, the communication layer often reports the same date twice to increase communication reliability.

4.2 Communication and application layers

A considerable challenge when programming the MSP430 involves meeting the timing constraints of the EPC protocol while still maintaining a low clock frequency. RFID tags that have custom state machines are designed at the hardware level to receive and send using the EPC protocol. The general-purpose MSP430 must be carefully tuned to perform EPC communication, both for receiving and transmitting data. In particular, a mix of C and assembly language is used where the C code maintains ease of configurability for the firmware for different sensor applications and the assembly code allows fine-grained control of the timing of the MSP430 for EPC communication.

As previously described, the demodulator envelopes and thresholds the Phase-Reversed Amplitude Shift Keyed (PR-ASK) signal from the reader into a serial date stream representing the data bits 1 and 0 as long and short pulses, respectively. To interpret data from the reader, the MSP430 uses the periodic edge of the waveform as a hardware

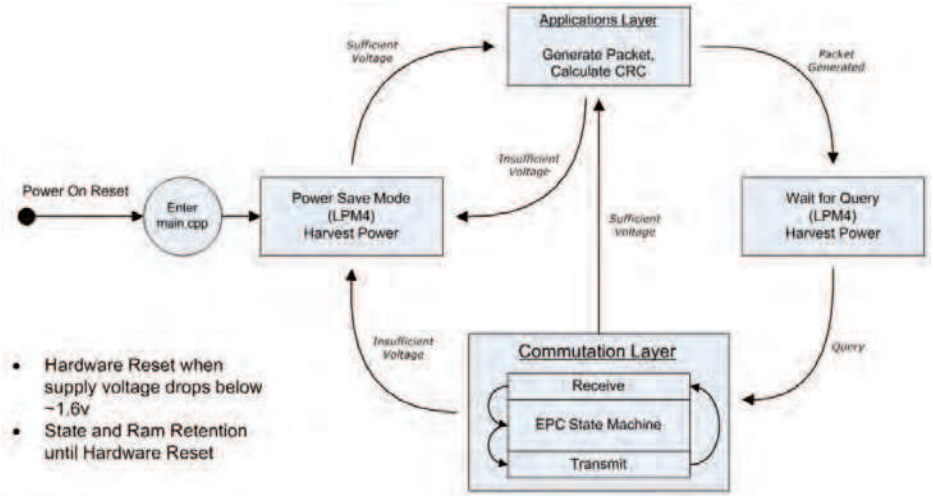

Fig. 5. Power Management Algorithm

interrupt, and then during the interrupt service routine re-samples the bit line to detect a 1 or 0 during the differentiated part of the waveform. This data is quickly shifted into memory before repeating this process. To detect the end of a transmission, a timer is refreshed during each bit. When bits are no longer received the timer expires, the packet is interpreted and, if appropriate, a response is sent to the reader. A detailed description of how the WISP uses and implements the EPC specification is described in section 5.

Figure 6 shows a set of EPC queries and responses along with the charge/discharge cycle of the WISP. Since the operating range of the WISP occurs between 1.9v-1.8v the rectified voltage appears to be nearly constant. In actually the WISP enters active mode at 1.9v, consumes the energy in the storage capacitor till ~1.8v, then enters a sleep state and harvests power until 1.9v is reached. This duty cycling can be seen in the packet transmitted plot. Here the WISP does not to responded to every packets sent by the reader, instead it spends most of its time in a sleep state.

Performing application level tasks such as sensor measurement is generally done in tight conjunction with the EPC protocol. In this scenario the completion of a receive/transmit cycle triggers the application layer to immediately take a sensor measurement, generator the desired EPC packet and setup for a Query. This protocol centric approach works well for sensor driven applications where data is requested from the RFID tag at regular intervals. However, applications which leverage the wirelessly powered computing capability of the WISP benefit from a loose coupling with the communication layer.

5. EPC class 1 generation 2 collecting sensor data

The Gen 2 MAC protocol used by the WISP provides primitives that can be used for gathering sensor data and transmitting queries. In this section, we give an overview of the Gen 2 protocol and discuss these primitives and their limitations.

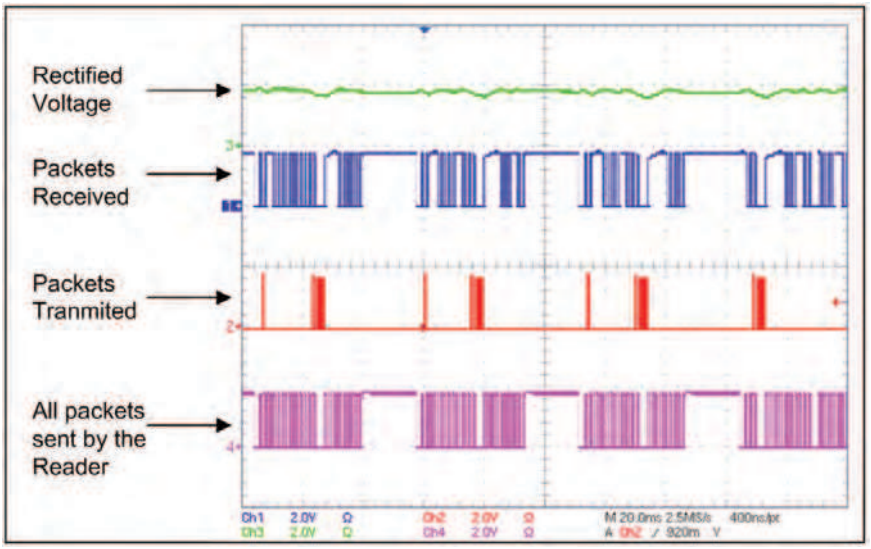

Fig. 6. Scope plot of the WISP responding to EPC queries along with the its rectified voltage.

5.1 Gen 2 background

5.1.1 MAC

The MAC protocol for Gen 2 systems is based on Framed Slotted Aloha (Roberts, 1975), where each frame has a number of slots and each tag responds in one randomly selected slot per frame. The number of slots in a frame is determined by the reader and can be varied on a per frame basis. Before starting a frame, a reader can optionally transmit a Select command which limits the number of active tags by providing a bit mask and a memory location, as only tags with IDs (or memory locations) that match this mask will respond in the subsequent frame.

To begin a frame the reader transmits a Query command which indicates the number of slots. Upon receiving a Query, each tag randomly chooses a slot in which to reply. If a tag chooses zero for its slot counter it responds immediately with a 16 bit random number (RN16). The reader echoes this RN16 in an ACK command and the tag responds with its ID. At this point, the tag is singulated. When a tag is singulated the reader can read and write tag memory as will be described in a later section.

After singulating a tag the reader transmits a QueryRepeat command which indicates the end of the slot. This signals to the tag that its ID has been read successfully and it should not respond in subsequent frames. Additionally, all other tags decrement their slot counter and transmit an RN16 if their counter reaches zero. Of course, tags may choose the same initial value for their slot counter. In this case, their transmissions will collide, the tags will not be singulated, and they will remain active in the next frame. A series of frames are conducted, each with a decreasing number of active tags, until all tag IDs have been read. This mechanism enables the rapid identification of tags and is supported by the WISP.

5.1.2 Tag memory

The Gen 2 standard specifies a memory architecture that includes banks for storing tag configuration information and the tag identifier, and also user memory with a size bounded

only by the device hardware. In the case of the WISP, this user memory is used to store sensor data and the layout and semantics are defined by the WISP software. For instance, data for a particular sensor can be written to a given memory location or a time series can be written to a sequential range of memory locations.

5.2 Gathering sensor data

The Gen 2 protocol was designed to rapidly identify tags. However, when using the WISP for sensing applications the sensor data must be transmitted along with, or in lieu of, the simple identifier. The Gen 2 protocol provides two mechanisms that can be used for this: overloading the identifier and the Gen 2 Read command.

5.2.1 Overloading the identifier

The Gen 2 protocol efficiently reads tag identifiers, and by overloading the identifier to include sensor data a collection of WISPs can report data efficiently as well. In our initial applications the identifier was replaced with the sensor data of interest. However, when using more than one WISP, data from different devices cannot be differentiated. Additionally, this approach breaks the semantics of the protocol and limits the interoperability of WISPs and standard tags.

The Gen 2 specification allows for the transmission of up to 496 bits of identifier, while current tags generally have an identifier of only 96 bits. Hence, up to 400 bits of sensor data can be piggybacked along with the ID, enabling data from different devices to be differentiated and at least partially maintaining the original semantics. Unfortunately, by sending sensor data along with the identifier the read time per tag is increased and the time required to read data from a particular tag can be prohibitively high. For many sensing applications, particularly those that use a large number of devices, reading all sensor data from every tag will be undesirable and overloading the identifier may be insufficient to meet the application requirements.

5.2.2 Gen 2 read command

After singulating a tag, the reader can issue a series of Read commands to read the contents of tag memory, with each command eliciting up to 512 bytes of data. Before issuing a Read command the reader requests a temporary, random 16 bit handle from the tag. This handle is used in the Read command to address the tag, and an arbitrary number of Read operations can be issued in sequence. Using this mechanism, a reader can selectively read sensor data stored in the user memory of a single WISP.

Using the Read command to gather sensor data has drawbacks with respect to efficiency and flexibility. First, to read new data from a WISP the device must again be singulated and a new handle must be obtained. With a large number of tags, singulation is time intensive. Even in the best case where a single device is selected with the Select command, the singulation process must still be conducted, albeit with only a single tag responding, and a new handle must be obtained; only then can data be read from the WISP. This results in a large amount of the read time being protocol overhead. Additionally, the identifier of the device with the desired data must be known a priori, along with detailed knowledge of the memory layout with respect to sensor data location.

By overloading the identifier or using the Read command, basic sensing applications can be implemented using the WISP. However, when deciding which technique to use, the energy cost must also be considered. Specifically, using the Read command consumes more energy

than returning the data with the ID. This presents a trade-off between range and speed, with the proper balance being largely application specific.
However, for many deployments these mechanisms will likely be insufficient. This stems from the fact that such deployments are interested in sensor data and not simple object identities. Where object identification requires that all of the tags respond all of the time, the model for sensing protocols is very different. These protocols must express high level semantics explicitly in terms of sensor data, resulting in some of the tags relaying some of their data some of the time.

5.3 Transmitting data to the WISP

Along with gathering sensor data from the WISP, applications need to transmit data to the WISP, e.g. to actuate its behavior. While most of the Gen 2 commands implement specific functionality, the protocol does provide two commands which enable general purpose down-link communication: the Select command and the Write command.

5.3.1 Gen 2 select command

The Select command is intended to limit the number of tags that respond in a Query round. For example, a collection of retail items may have identifiers that indicate their model number, and the Select command can be used to inventory only items of a given model by providing a memory pointer and bitmask which matches only that model. However, this mechanism can be repurposed to function as a general purpose broadcast channel, with the pointer and mask being interpreted by the WISP software as opcodes and data. As an example, we have implemented software for the WISP which interprets Select commands as instructions to blink LEDs.

5.3.2 Gen 2 write command

Along with the general purpose broadcast facility of the Select command, the Gen 2 Write command can be used for unicast down-link communication. After a tag is singulated, the reader can write arbitrary memory locations on the tag in 2 byte words. Additionally, the BlockWrite command can be used to write up to 256 words at a time. This mechanism can be used to transfer data to the WISP, for example to store location information on the tag as it moves through a supply chain. Additionally, a WISP could be programmed to look to certain memory locations for parameters that affect its operation. For example, to modify the sampling rate of the WISP the Write command could be used to transmit the desired rate to a known memory location, and the WISP would refer to this value when setting its sampling rate.

5.4 Querying and tasking

To enable rich sensing applications, the reader must be able to query a collection of WISPs for particular types and ranges of sensor data. With this, a subset of the tags will reply and then only when their sensor data is relevant to the application. As a first approximation, the Select command can be used to match a bit mask on a particular user memory location. For integer valued sensors, a Select command could be used to select tags with specific sensor values over a given threshold and only tags that meet this criterion would respond in the following frame. Such an approach requires detailed knowledge of the memory layout and only works for queries that can be specified using a simple bit-mask.

As the WISP can perform general purpose computation, functionality at the device can be used to interpret abstract queries. For example, the WISP can be programmed to interpret SQL style queries, and the bit-mask of the Select command can be interpreted as commands instead of simple masks. Additionally, the Gen 2 protocol allows for the specification of Custom Commands which enable vendor specific functionality. Custom Commands are transmitted after singulation, and consequently can be used for sending unicast queries to a device.
More generally, by implementing high level functionality on the WISP, the Select command can be used as a broadcast channel to transmit opcodes and data to all devices, and Custom Commands can be used to send unicast messages to a single device. These two primitives enable the implementation of a wide range of protocols and a high degree of application flexibility and performance.

6. Applications

The longstanding goal throughout the development of WISP has been to facilitate RFID innovation. The WISP platform is designed as a research vehicle that allows people inside and outside the RFID community to explore new applications and usage models for RFID. Traditionally, RFID tag designers have been specialists in integrated circuit design (IC). They have generally focused on innovating CMOS circuit blocks such as RF rectification, power management, and low power state machines, with the goal of increasing tag read range. The process of manufacturing these custom IC tags presents a significant barrier to entry when considering the high cost of software, servers, chip fabrications, and specialized testing equipment; not to mention the long fabrication cycles.
Consequently, when researchers do add additional functionality, such as ADC and light sensors (Namjun et al., 2005) (Kocer & Flynn, 2006), the focus is on the device and is not driven by any particular applications. It is important to note that custom IC tag design will undoubtedly offer longer range, better performance vs. power consumption, and lower manufacturing cost in large volumes. However, it is difficult under this design paradigm to develop new applications that will take RFID beyond simple item tracking and identification.
In contrast, WISPs are flexible PCB based platforms that allow a relative novice to prototype both hardware and software RFID designs in a bench-top setting. The full-featured TI MSP430 allows for fast code development with debugging support. Sensors and peripherals can be easily added via the exposed headers or by using an optional daughter board. Testing equipment generally consists of an RFID reader and an oscilloscope. When compared to IC tags, probing and debugging circuit elements is easy and straightforward, as many of the signal lines are exposed by the PCB design.
The WISP fundamentally lowers the barrier to entry and allows people from a wide variety of fields to develop RFID technology. Whether it is students as part of a class project, security specialists, consumer electronics designers, or even artists, it is believed that a diverse group of people will be able to push RFID technology and find new and useful usage models. The hope is that this will lead to the discovery of compelling applications and that the IC tag designer will be able to draw upon the lessons learned from the WISP implementation. The following sections describe research being done with the WISP and focus on lessons learned.

6.1 Security

As RFID tags have become ubiquitous in the consumer marketplace for merchandise tracking and financial transactions, serious privacy and security concerns are being raised.

In many ways, the strengths of RFID are also its greatest weaknesses: RFID tags are mass produced, tiny, wireless transponders, which can be embedded in virtually any object and can be uniquely identified from a distance without the explicit consent of the owner. While this enables many valuable applications, it can also result in tagged items being used to identify and track individuals without their knowledge. In addition, RFID is increasingly being used to communicate sensitive data and not simple identifiers. Most notably, the banking industry has adopted RFID enhanced credit cards to enable fast, contactless payment. While the information transmitted via RFID is identical to that printed on the card, gathering this information no longer requires the conscious act of removing the card from a wallet and swiping the card through a magnetic reader. Consequently, thieves can steal the card information wirelessly, even while the card remains securely in the cardholder's wallet or purse; these attacks have already been seen in the wild.
To mitigate the privacy and security concerns inherent to RFID, there has been considerable interest in protecting the communication channel of RFID tags. One low-tech approach is to use a conductive sleeve to store RFID enabled devices, and the user must remove this sleeve for the device to be read. However, this relies on the diligence of the user and limits the usefulness of the technology. Consequently, more sophisticated approaches have been proposed that use cryptographic techniques to assure data authenticity and protect the data during transmission. Such techniques are generally beyond the capabilities of IC RFID tags, but are well matched to the WISP platform.

6.1.1 RC5 encryption

Conventional wisdom states that strong cryptographic algorithms are unrealistic for RFID considering the computational constraints and power issues of IC tags. As a result, various lightweight cryptographic protocols have been proposed and implemented. However, many of these protocols have serious vulnerabilities and were subsequently hacked or exploited (MBTA et al., 2008). However, the computational power and flexibility of the WISP enables the realization of stronger, more conventional cryptographic techniques designed to enhance both privacy and security.
In (Chat et al. 2006), the WISP was used to demonstrate RC5 based symmetric cryptography for use on UHF RFID tags. The particular RC5 variant implemented uses a 32-bit word, 12 rounds, and a 16-byte secret key which is stored in flash. While there were practical challenges in implementing RC5 on such a resource-constrained platform, the authors showed that with careful implementation strong cryptography is within the scope of UHF RFID. Additionally, their choice of RC5 was partly because RC5 can be efficiently implemented in both hardware and software, so their work can be used as a basis for IC implementations.

6.1.2 Context aware communication

Even when strong cryptography is used, RFID is still susceptible to "man in the middle" attacks. For instance, RFID is widely used for access cards where an RFID enabled employee badge uses a cryptographically strong challenge/response mechanism to open doors to a secured building. An attacker in this scenario does not need to break the encryption but only needs to generate the correct response to the RFID reader challenge. Attacks on such systems, referred to as "ghost and leech" attacks, involve one device near the reader (the "ghost") and one near the badge (the "leech"). The "ghost" receives the reader transmissions and forwards them over the internet to the "leech". The "leech" echoes these transmissions to the badge and when the badge responds, its response is forwarded back to the "ghost".

The "ghost" then transmits the badges response to the reader and the door is unlocked. In this scenario, the "ghost" may be at the building door while the "leech" is in a coffee shop down the street where the employee is having lunch.
The enabler of this attack is that the context of the badge is not factored into the access system protocol. This is largely because standard RFID offers no input vector to detect the context of the device. The sensing capabilities of the WISP can provide this context awareness, and in the case of "ghost and leech" attacks it can be used to detect user intent. In (Czeski et al., 2008), the 3D accelerometer of the WISP was used to implement a "secret hand shake" based authentication system to protect against "ghost and leech" attacks. When the user wants to authenticate a transaction or gain building access, they first perform a gesture with the card which unlocks the card and enables communication. The gesture could be a figure eight or any unique movement that the card would not experience in everyday activity. Only if this handshake is correct will the WISP unlock and transmits its ID to the reader. This approach leverages not only the computational power of the WISP, but also its sensing capabilities to provide a level of security that is not possible using standard IC tags.

6.2 Passive data logger

Several authors have demonstrated novel applications of passive RFID technology, which benefit from wireless, battery-free operation. However, these systems are inherently limited by the requirement of tag proximity to a reader for power and finite wireless range due to RF path loss over distance. One particularly interesting class of applications involves a tagged item that travels between two reader-equipped locations but does not have reader proximity during transit. For example, this situation occurs during cold chain transport for food and chemicals between warehouses. One may be interested in tracking the temperature or vibration of goods during transit where there is no reader coverage.

Fig. 7. WISP data logger with operational Super capacitor

To enable these applications, the authors have proposed a new tag device called a passive data logger (PDL). A PDL is a battery-free RFID tag with a large capacitor for energy storage. The PDL seamlessly recharges its capacitor when it is near a reader and uses the stored energy to measure attached sensors and log data to non-volatile memory (NVM) when it is away from a reader. Data is retrieved from the PDL using EPC Class 1 Generation 2 (Gen2) User-Memory "Read" commands. Additionally, the PDL can report an EPC ID like a conventional RFID tag.
There are several considerations in the design of a PDL. The most important design parameter is the reader-free runtime. Operating with a mean current I_{ave}, the expected runtime $\Delta t = C * \Delta V / I_{ave}$ where Δt is the runtime in seconds, C is the capacitance, ΔV is the difference between the maximum operating voltage V_{max} and the minimum operating voltage of the system, Vdd. Equation 2 defines the average current where T_{on} and T_{off} are

the active and sleep mode durations, T_o is the period and I_{active} is the active mode current and I_{sleep} is the sleep mode current.

$$I_{ave} = (I_{active} * T_{on} + I_{sleep} * T_{off}) / T_o \quad (2)$$

Figure 8 illustrates several calculated operating times given a fixed capacitance and current consumption

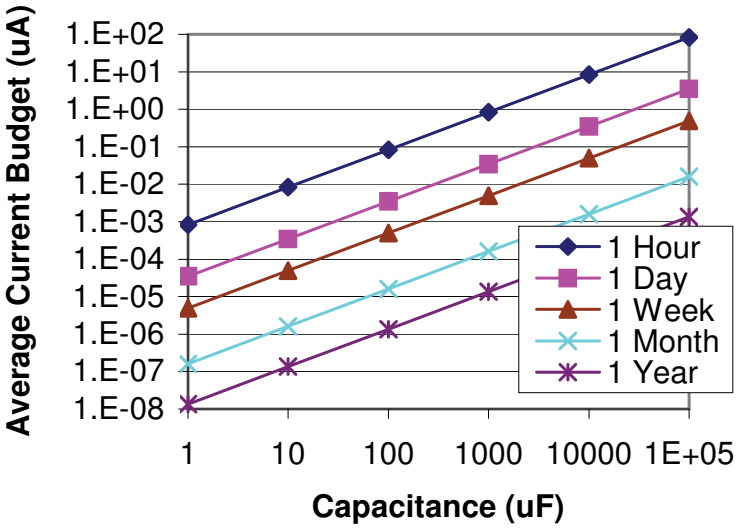

Fig. 8. Average current budget for various runtimes and storage capacitor

Another important parameter is the wireless charge time. The charge time is determined by capacitor size, Vmax and the available power at a distance d from the reader.

$$E_{stored} = \frac{1}{2} C\left(V_{charged}^{\ 2} - V_{dd}^{\ 2}\right) = P_{charge} * T_{charge} \quad (3)$$

The available power is modeled by Friis' transmission equation for path loss (equation 1), with terms for rectifier efficiency and polarization included.

The authors have implemented a PDL based on the WISP platform (WISP-PDL), which benefits from a programmable microcontroller for rapid, flexible prototyping. As a proxy for cold chain monitoring, a refrigerated milk container was instrumented with a WISP-PDL and monitored throughout its consumption (Yeager, et al., 2008). For this study, the WISP-PDL sampled and logged data in 10 second intervals and consumed 1.8 μA on average from a 1.8 V supply. Over the course of 24 hours, the temperature and fill level of the carton was measured and written to memory. At the end of the study, the data was read from the WISP-PDL using the Gen 2 Read command showing the complete history of the milk carton. As the refrigerator acted as a faraday cage, the WISP-PDL harvested energy only when removed from the refrigerator but continued to sense when not directly powered by a reader.

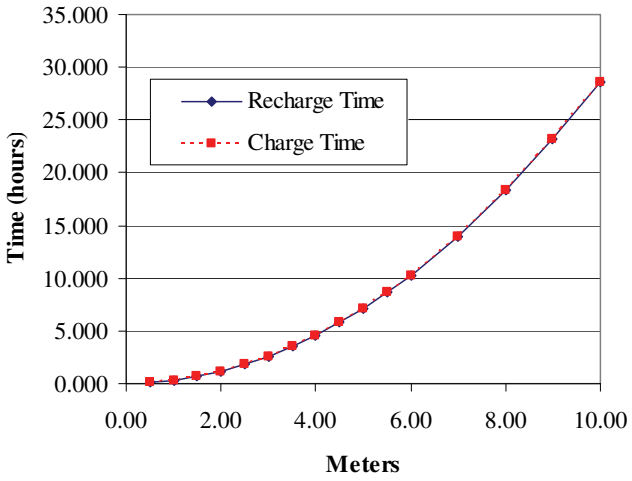

Fig. 9. Wireless charge rates for the data logger WISP

A second application of the PDL involved primate neural signal monitoring (Holleman, et al., 2008). To accurately measure neural activity, neural probes must be placed directly on the brain but the probes must also be powered. Consequently, transcutaneous wires are generally used which lead to a high risk of infection, or inductive power systems are used which require a bulky energy source that must be placed within a few centimeters of the implanted device.

The WISP platform provides key advantages for this application, as neural probes can be attached and the entire device can be implanted and powered wirelessly by an RFID reader. However, the RF transmissions from the reader overwhelm the sensitive neural probes, and thus the reader cannot be active while the neural probe is taking measurements. To overcome this limitation a WISP-PDL was used and a standard RFID reader charged the device for 3 seconds. The reader then powered down and the WISP-PDL began taking measurements for 5 seconds and storing the measurements to memory. After the sensing phase, the reader powered up and downloaded the measurement data from the WISP-PDL using the Gen 2 Read command. This process was repeated yielding high resolution neural pulse data.

7. Conclusions

This chapter presents the design of the Wireless Identification and Sensing Platform, a battery-free programmable RFID sensor device compliant with the Electronic Product Code Class 1 Generation 2 protocol. The WISP operates from wireless power at a distance of several meters and provides a robust bidirectional communication channel built on top of the RFID reader physical layer. The microcontroller allows the WISP to be reconfigured for new tasks and easily accommodating the integration of low power sensors. In a larger context the WISP demonstrates the feasibility of UHF RFID systems powering and reading complex tags which utilize compotes such as microcontroller and sensors.

The WISP has proven that is a flexible platform which allows research to quickly investigate new and innovative applications. Examples include the use of WISP for development of enhanced security measures on RFID tag, and for the development of a passive data logging device. It is believed that as more researchers use the WISP new and innovative RFID devices and applications will be discovers which can be later implemented in a integrated circuit design,

8. References

Holleman, J., Yeager, D., Prasad, R., Smith J., Otis, B., "Neural WISP: An Energy Harvesting Wireless Brain Interface with 1m Range", IEEE Biological Circuits and Systems (BioCAS) 2008, accepted, expected to publish November 2008.

Johan, S.; Xuezhi Zeng; Unander, T.; Koptyug, A.; Nilsson, H.-E., "Remote Moisture Sensing utilizing Ordinary RFID Tags," *Sensors*, 2007 IEEE , vol., no., pp.308-311, 28-31 Oct. 2007

Kocer, F. and M. P. Flynn. "A new transponder architecture with on-chip ADC for long-range telemetry applications," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 5, May 2006, pp. 1142-1148

Malinowski, M., Moskwa, M., Feldmeier, M., Laibowitz, M., and Paradiso, J. A. 2007. "CargoNet: a low-cost micropower sensor node exploiting quasi-passive wakeup for adaptive asychronous monitoring of exceptional events." *In Proceedings of the 5th international Conference on Embedded Networked Sensor Systems* (Sydney, Australia, November 06 - 09, 2007). SenSys '07. ACM, New York, NY, 145-159.

MBTA vs. Anderson, et al (United States District Court - District of Massachusetts August, 2008)

Microchip Technology Inc., *125 kHz Passive RFID Device with Sensor Input*, August 25, 2005

Namjun, Cho, et al, "A 5.1-μW 0.3-mm2 UHF RFID Tag Chip Integrated With Sensors for Wireless Environmental Monitoring," *IEEE European Solid State Circuits Conference*, September, 2005, Grenoble, France. P. 279- 282.

Philipose, M.; Smith, J.R.; Jiang, B.; Mamishev, A.; Sumit Roy; Sundara-Rajan, K., "Battery-free wireless identification and sensing," *Pervasive Computing, IEEE* , vol.4, no.1, pp. 37-45, Jan.-March 2005

Polastre, J.; Szewczyk, R.; Culler, D., "Telos: enabling ultra-low power wireless research," Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on , vol., no., pp. 364-369, 15 April 2005

Sample, A.P., Yeager, D.J., Powledge, P. S., Mamishev, A.V., and Smith, J. R., "Design of an RFID-Based Battery-Free Programmable Sensing Platform," *IEEE Transactions on Instrumentation and Measurement*, Accepted for future publication.

Savi Technology. Savi SensorTag ST-676. Datasheet, 11 June 2006. http://www.savi.com/products/SensorTag_676.pdf

Roberts, L. G., "Aloha packet system with and without slots and capture" *SIGCOMM Comput. Commun*. Rev., 5(2):28–42, 1975.

Want, R., "Enabling ubiquitous sensing with RFID," *Computer*, vol.37, no.4, pp. 84-86, April 2004

Watters, D. G., Jayaweera, P., Bahr, A. J., and Huestis, D. L., *Design and performance of wireless sensors for structural health monitoring*. In D. O. Thompson and D. E. Chimenti, editors, AIP Conf. Proc. 615: Quantitative Nondestructive Evaluation, pages 969–976, May 2002.

Yeager, D.J., Powledge, P.S., Prasad, R., Wetherall, D.; Smith, J.R., "Wirelessly-Charged UHF Tags for Sensor Data Collection," *RFID, 2008 IEEE International Conference on* , vol., no., pp.320-327, 16-17 April 2008

Development and Implementation of RFID Technology

Edited by Cristina Turcu

ISBN 978-3-902613-54-7
Hard cover, 450 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices but also for experienced technical professionals and RFID aficionados.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Alanson Sample, Daniel Yeager, Michael Buettner and Joshua Smith (2009). Development of Sensing and Computing Enhanced Passive RFID Tags Using the Wireless Identification and Sensing Platform, Development and Implementation of RFID Technology, Cristina Turcu (Ed.), ISBN: 978-3-902613-54-7, InTech, Available from: http://www.intechopen.com/books/development_and_implementation_of_rfid_technology/development_of_sensing_and_computing_enhanced_passive_rfid_tags_using_the_wireless_identification_an

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821