History of the WISP Program

Joshua R. Smith

1 Motivation

This chapter tells the story of the early years of the wireless identification and sensing platform (WISP) project, which created what we believe to be the first far field RF-powered sensing and computing platform. This chapter is about the history of the program: what were the motivations, who was involved, how did one piece of the project lead to the next, where we the dead ends, what other research grew out of it, and what were the impacts? This sort of background can be difficult to extract from the research papers themselves, which typically present self-contained results and do not convey the context. The context and background of the WISP program may be worth reflecting on because it has been such a fruitful research vein and because it bears on meta-research questions such as how to build a community. These meta-research questions are important because they affect the amount of impact that the research ultimately has.

While this present chapter focuses on the history and context of the WISP program, the next chapter "The Wireless Identification and Sensing Platform" is a detailed description of the WISP design and applications [16]. Also, this present chapter discusses just the work of my group and our collaborators. Other chapters of this book contain examples of related work by people who are not collaborators; some of these projects use the WISP, and some use different platforms. Projects on which my group did not collaborate are not discussed in this chapter, because I do not have the context.

J.R. Smith
Department of Computer Science and Engineering, Department of Electrical Engineering, University of Washington, Seattle, WA, USA
e-mail: jrs@cs.washington.edu

J.R. Smith (ed.), *Wirelessly Powered Sensor Networks and Computational RFID*,
DOI 10.1007/978-1-4419-6166-2_2,

I began trying to combine sensing, computing, and RFID at Intel Research Seattle (later renamed Intel Labs Seattle) in 2004, motivated by a problem my colleague Matthai Philipose was grappling with. Matthai was interested in human activity recognition, motivated by eldercare. He had developed a short-range (HF, 13.56 MHz) RFID reader in the form of a bracelet and could detect that a person was using a tagged object when the bracelet reader got close enough to read the object's tag, which typically occurred when the object was being manipulated [13]. In an effort to eliminate the bracelet reader, Matthai and Ken Fishkin had experimented with estimating the motion of RFID tags from changes in the read rate of the (then relatively new) long-range UHF RFID tags [9]. Was there a more direct way to measure tag motion? Clearly an RFID tag with accelerometer sensors would solve the problem, but no such thing existed. At the time it seemed impossible given the power constraints.

1.1 α-WISP

The α-WISP ("alpha WISP") was my first attempt to solve this problem: I used two mercury switches, in an antiparallel configuration, to multiplex two RFID chips (each with its own unique ID) to one antenna. The antiparallel arrangement ensured that if the tag were held stationary at a particular tilt angle, one switch would be open and the other closed. Each switch was connected in series to an ID chip, and the whole assembly of switches and chips was connected to an antenna. Thus when tilted one way, the α-WISP returns one ID to the reader; when tilted the other way, it returns a different ID. The two IDs can be thought of as two code words that (together, via the choice of one or the other of the code words) encode one bit of sensor information. The α-WISP thus enabled us to use an unmodified commercial RFID reader, and the existing unmodified EPC class 1 generation 1 (C1G1) UHF RFID protocol (which was not designed to transmit sensor data), to communicate one bit of sensor data, as well as many bits of ID data, from a battery-free, RF-powered uniquely identified sensor unit. I described the α-WISP as a one bit accelerometer sensor, because the mercury switches can be thought of as accelerometers with one bit of precision; they can be used to sense tilt because their state is determined by the direction of gravitational acceleration relative to the sensor axis [14, 27]. Later, Anthony Lamarca built a beautiful wooden box with a permanently "implanted" α-WISP that allowed the box's state (open or closed) to be read, along with the box's ID, by an EPC Gen 2 RFID reader. In this new form of α-WISP, a permanent magnet was built into the box top; in the body of the box was an α-WISP with an SPDT magnetic reed switch. The proximity of the magnet in the lid to the magnetic reed switch in the box body determined which of the two IDs the box returned when interrogated by the reader [31].

1.2 π-WISP

With the π-WISP ("pi WISP"), I wanted to send more than one bit of sensor data. I built a 3 axis × 1 bit accelerometer from three orthogonal mercury switches. Graduate student Bing Jiang designed a small UHF power harvester board that used Schottky diodes to rectify the 915 MHz RF signal emitted by the reader, converting the RF power collected by the harvesting antenna into a DC power output. This RF harvester was used to power the TI MSP430 microcontroller. The microcontroller read the state of the mercury switches and then encoded the data using what I called "ID modulation": the micro was connected to a gallium arsenide single pole double throw (SPDT) switch that multiplexes two RFID chips to one tag antenna. The mechanical switch of the α-WISP had been replaced by a solid-state, electronically controlled switch. (A gallium arsenide switch was chosen because the switch had to pass ultra-high-frequency RF signals, which are too high in frequency for typical silicon devices to handle.) But because the IDs were now being selected by software (instead of by a mechanical modulator, the mercury switch), the π-WISP could produce an arbitrarily complex time series, in the patterns of ID response. Having previously worked on information hiding (the problem of embedding one signal in another, e.g., a digital watermark in an image), I liked to think of this as "hiding" a stream of sensor data in another stream of data, the sequence of RFID reads. Because the RFID reader (which might be called "the warden" by steganographers) does not notice any strange behavior, we were essentially able to overlay or embed a new protocol (for sensor data) in an old one (for IDs). This embedded (or overlay) protocol was very inefficient: its net data rate was less than one bit of sensor data per second, since the sensor data was encoded in a long stream of ID reads, which included "packet headers" composed of multiple RFID read events. The packet headers were necessary for synchronization: without them (or some other channel sharing scheme in the overlay layer), it would not have been possible for the reader to distinguish bit one of the sensor data from bits two and three of sensor data. Although this protocol for overlaying sensor data in a stream of ID reads was painfully slow, it was exciting that we could now communicate an arbitrarily large amount of sensor data, collected in a battery-free fashion, using apparatus that was not designed to support this functionality [26, 28, 29].

1.3 WISP

Next we built a battery-free, RF-powered EPC C1G1 RFID tag entirely from scratch discrete components. The tag logic was implemented entirely in microcontroller software. Unlike the α-WISP and the π-WISP, the WISP did not include commercial RFID chips. The path from the π-WISP to the WISP was not an entirely

straight line. I had hired new UW graduate student Alanson Sample as an intern to help design a chip, to be fabbed through the new Intel Research Shuttle program. The Research Shuttle was intended to allow researchers to design chips to be built on Intel processes. The chip we designed was the analog front end of an RFID tag: it included a power harvester, a demodulator to extract data from the RFID reader, and a modulator to backscatter information to the reader. The plan was to power the MSP430 via the output of the harvester and (similar to the π-WISP) to use the MSP430 as a software radio to implement the protocol (in this case the full RFID protocol, not an overlay). The result would be a fully programmable RFID tag consisting of two chips, plus whatever sensors were desired.

Soon after the chip was designed and simulated, the Intel Research Shuttle program was canceled. Disappointed, we decided to use discrete components to build an RFID analog front end based on the one that had already been designed, despite the fact that the design had originally been intended to become an IC. While most people think of RFID tags as chips, in fact, a printed circuit board implementation has a number of advantages: one can include low-threshold Schottky diodes (which are not available in many CMOS processes) for efficient power harvesting, one can include capacitor values that would be infeasibly large on an IC, and one can integrate sensors without constraints on fabrication process—mixing and matching is allowed.

Instead of a two-chip tag, the WISP ended up including the microcontroller, passive components, Schottky diodes, and sensors. Some versions included a comparator (in the demodulator) and voltage supervisors (to wake the MSP430 from low-power deep-sleep states). We were uncertain whether the MSP430 would be fast enough to implement the EPC C1G1 protocol. Software engineer Pauline Powledge wrote the first working WISP firmware. The most challenging moment in the entire WISP program was getting the WISP to successfully talk to a commercial RFID reader for the first time. There were numerous advantages to using commercial RFID readers, but ease of debugging tag-reader interactions was not one of them. The problem is that commercial RFID readers are built as black boxes; if the reader does not feel that the tag is behaving properly, the reader just ignores it—it does not provide helpful error messages, or any feedback whatsoever, to the newbie tag designer. At one point, in desperation, we put oscilloscope probes across the antenna of a well-behaved commercial UHF RFID tag, to see how its behavior differed from our tag. We discovered the Generation 1 Alien reader deviated substantially from the published protocol. Once this discovery had been made, we were able to get our first WISP working.

Building on the ID modulation idea used in π-WISP, we allocated certain bits of the tag ID to sensor data. As with the α- and π-WISPs, the reader would simply pass on these sensor bits (the low eight bits of the tag ID, say) without knowing that it was handling sensor data; to the reader it simply looked like a stream of IDs from a quickly changing tag population. This technique was far more efficient than the

ID modulation scheme used by the π-WISP, since a single RFID read even could convey as many bits of sensor data as we were willing to "steal" from the ID space. Suddenly we could send sensor data at what seemed like blistering speeds [17, 30].

1.3.1 Gen 2 WISP

While the WISP was maturing, so were RFID standards. The original EPC C1G1 specification was supplanted by the EPC Class 1 Generation 2 specification. Seong Ho Kim, together with UW graduate student intern Dan Yeager, created the first version of the WISP firmware that supported the Gen 2 specification. The Gen 1 WISP firmware had been written in C. The higher bit rates of the Gen 2 specification required the most time-sensitive parts of the firmware to be written in hand-optimized assembly language to squeeze enough performance from the MSP430. The earlier experiments referenced in this chapter used the C1G1 spec; later ones used "Gen 2." Michael Buettner did an implementation of the Gen 2 MAC (medium access control) layer, which is described in the chapter "Implementing the Gen 2 MAC on the Intel-UW WISP" of this volume [2].

1.4 Accelerometer WISP

The summer after the first WISP (described in [30]) came to life, I asked Dan Yeager to connect a new, very low power three-axis accelerometer to our latest WISP. The accelerometer, the Analog Devices ADXL 330, consumed only 200 uA at 1.8 V. Before this accelerometer, it would not have been feasible to power and read an accelerometer using RF signals. We believe that this WISP with accelerometer was the first UHF-powered and -read accelerometer. Having started with a very primitive RF-powered one bit accelerometer, we finally had a real three-axis accelerometer, with eight bits of real accelerometer data for each axis, entirely powered and read by a commercial RFID reader [23, 36]. Later Matthai Philipose, working with Michael Buettner and David Wetherall, used the WISP's accelerometer for activity recognition, the original inspiration for the project [5].

1.5 WISP Passive Data Logger

In "cold-chain monitoring," the goal is to verify that temperature-sensitive items, such as vaccines, blood products, or frozen food, have been kept within a required temperature envelope. In this application, and many other "shipping" applications,

it is not feasible to assume that the sensor is near an RFID reader at all times. Dan Yeager and I proposed a Passive Data Logger to address this application space. The Passive Data Logger is a WISP with a large energy store and large memory, likely nonvolatile. The model is that the WISP, mounted on an item whose temperature is to be monitored, accumulates energy while it is waiting at its original location, perhaps a warehouse freezer with a built-in RFID reader. While the item is in transit, the stored energy is used to sense and log data. At the receiving end, the logged data is downloaded via the RFID interface, and the tag begins harvesting power to replenish the energy that was consumed during transit [35].

1.6 Neural WISP

Dan Yeager created a WISP to drive a custom neural amplifier IC designed by members of Brian Otis's group. This effort was successful, although we encountered some interference between sensing and communication in this application. The carrier emitted by the reader is amplitude-modulated to encode downlink data (data that flows from the reader "down" to the tag). The downlink data modulations caused sensor noise. In the application, we solved the problem by time multiplexing between sensing and communication [37].

1.7 Strain Gage WISP

Working with Professor Paolo Feraboli's group and researchers from Boeing, we created a WISP strain gage sensor system targeted at health monitoring for structures such as wings or car bodies made from composite materials. One can imagine permanently embedding battery-free sensors in wings, since they are capable of perpetual operation and can be temporarily energized only when read [10].

1.8 Solar WISP

In the Passive Data Logger [35], the problem of sensor data logging for items in transit (away from a reader) was solved by accumulating energy during time spent near the RF source and then using it later when the tag is no longer near the RF source. In the Solar WISP, Alanson Sample and then-undergraduate Aaron Parks decided to use a secondary energy source, solar, to power the data logger. The elegant result in this project is that a solar cell can be used directly as the RFID antenna: separate structures are not needed. Using the solar cell for both solar and

RF harvesting saves area and cost. The flexible solar cell used in this project showed that the resulting system could potentially take the "sticker" form factor common in RFID tags [20].

1.9 RFID Localization with the LED WISP

RFID localization is a difficult and important problem. If an RFID tag can be precisely localized, it makes capabilities like robotic retrieval of the object much more feasible. For a robot to pick up an object, it needs to know quite precisely where the object is. Localizing RFID tags via reflected RF signal strength is generally unreliable because of multipath. Relatively small changes in the environment, including a person walking by, can dramatically change RF signal strength readings. The RF signals can take multiple paths from the source to the destination; the "ray" along each path has its own phase, affected by the length of the path. The rays sum at the destination location and can interfere constructively or destructively, depending on the detailed geometry of the environment and the paths taken by each ray. Changing the path length (and thus the phase) for one ray can drastically change the resulting signal strength at the destination.

Dan Yeager and I, together with Ali Rahimi, a computer vision colleague at Intel Research Seattle, realized that we could build an LED WISP that could be powered and read by an RFID reader but localized precisely by a camera looking at the LEDs. Dan designed a WISP that included four LEDs, one in each corner. A robot-mounted RFID reader might detect the desired object on a shelf in a warehouse, along with many other tagged objects that are not of interest. With the LED WISP, it should be possible for the reader to command the single tag of interest to flash its LED and hopefully be localized well enough for the robot to retrieve it.

While this idea itself was enough to generate a patent [32], we were not able to get the idea to actually work at that time. Given the power constraints, it turned out to be difficult for the camera to detect the LED. It was only possible to light the LED for a very short period of time, and with a free running camera, not synchronized with the tag, the chance of missing the flash was high.

A couple of years later, at UW, my group returned to the problem. We realized that we needed to synchronize the camera with the RFID reader in order for the idea to work. Since the commercial RFID reader is still essentially a black box that does not provide access to its internal state, we built a "trigger WISP" that monitors the traffic from the reader to the tag of interest. By mimicking the state of the LED WISP (inferred from the reader traffic), the trigger WISP can reliably determine when the LED WISP will flash. The trigger WISP then triggers a camera to capture a frame when the LED is guaranteed to be on. By taking another image with the LED off and differencing the images, the LED can be found very reliably. The team included undergraduate Craig Macomber, who did the smart camera and image processing work, Liang–Ting Jiang, who programmed our PR2 robot, and Alanson Sample, who put the whole system together and did the optical localization work [21].

1.10 SOCWISP

For his master's thesis, Dan Yeager worked with Brian Otis to design a "System On Chip" WISP. This chip includes the EPC RFID analog front end, as well as the digital state machine for an EPC C1G2 tag. A separate application microcontroller can provide data to the SOCWISP via a serial interface. The data becomes the ID that the SOCWISP returns to the RFID reader. One of the remarkable things about this chip was that the first design to be fabricated actually functioned. Part of the reason is that Dan was able to extensively test and debug the digital state machine against a real RFID reader, by implementing the state machine in an FPGA connected to a WISP analog front end. The SOCWISP was so small and light that Dan was able to fly it on a moth and make in-muscle temperature measurements while the live moth was flying. The paper describing SOCWISP appears in this volume as the chapter "SOCWISP: A 9 μA, Addressable Gen2 Sensor Tag for Biosignal Acquisition" [39]; it was originally published as [38].

1.11 Security

Although the WISP had been conceived as a platform for sensing and computing, it received immediate interest from the security community. Because RFID tags had been black boxes and could not run software, it had not been feasible to implement and test security protocols and encryption algorithms that required nonstandard behavior from UHF RFID tags. The WISP suddenly made this possible.

1.11.1 Encryption

Kevin Fu, a computer science professor then at University of Massachusetts, immediately saw the possibilities of WISP for security research. We gave him some WISPs, and his group became the first outside users of WISP. The first joint publication between the two groups was an implementation of the RC5 block cipher algorithm on the WISP. One school of thought in RFID security is that, because of the limited power and computing cycles, special "minimalist" cryptographic algorithms are required. This paper, entitled "Maximalist Cryptography and Computation on the WISP UHF RFID Tag," introduced a contrary approach, by implementing a full-blown conventional "desktop" cryptographic algorithm on an RF-powered device. The paper was presented at a conference [6], but never published; an updated version appears as the chapter "Maximalist Cryptography and Computation on the WISP UHF RFID Tag" [7] of this volume.

Kevin coined the term computational RFID as a generic term for WISP-like devices, and his group went on to publish many of their own papers on computational RFID. His group has even built their own computational RFID units,

which they named the MOO, for its key feature: the very beefy microcontroller (a larger model MSP430) [40]. The larger micro allows implementation of more sophisticated software, but the increased power consumption limits range.

The security community has continued to innovate using the WISP platform. For example, Pendl, Pelnar, and Hutter implemented elliptic curve cryptography (ECC) on the WISP [12].

1.11.2 Security Through Sensing

One of the challenges in RFID security is that tags can easily be read without their owner's knowledge or permission. Sensors can help with this, by giving the tag's owner a user interface to the tag that can be used to authorize tag responses.

Secret Handshakes

Alexis Czekis and Karl Koscher, two UW CSE graduate students working with Tadayoshi Kohno, proposed using WISP to prototype an RFID access control tag that would be resistant to "ghost and leech" attacks, an attack that is specific to RFID access control tags. This attack relies on the promiscuity of ordinary RFID tags, which will respond to any reader. One of the attackers, the "leech," draws close to a person who is known to be carrying an RFID access control card for a space that the attackers wish to enter. The leech's RFID reader queries the access control tag and relays the response to the "ghost," whose programmable RFID tag responds to the RFID reader responsible for access control. This relay attack causes the ghost of the authorized person to appear in front of the access control reader. Note that even if the reader engages in a challenge-response scheme with the tag, suitable versions of this attack will still work.

The solution they proposed was to use the WISP's sensing capabilities to enhance security. Rather than respond promiscuously to any reader, the tag will respond to the reader only after it is moved through a certain gestural trajectory, essentially a gestural password. The accelerometer was used to sense the trajectories, and the microcontroller performed the gesture recognition computations via a template correlation scheme [8].

Capacitive Touch WISP

Another way to add user input to an RFID tag is to use the tag antenna as a capacitive sensor. The paper demonstrating this idea using WISP won the best paper award at IEEE RFID in 2009 (after being flatly rejected the previous year—persistence pays off!) [18]. This technique is described in more detail elsewhere in this volume [16].

1.12 Networking

David Wetherall, Michael Buettner, and Ben Greenstein led an effort to start exploring networking issues raised by WISP sensors [3, 4]. This volume contains a very interesting contribution (Chap. 7, by Molina–Markham et al. [11]) to this space, an overlay to the RFID protocol that allows WISP to WISP communication. This overlay abstraction is implemented at the lower levels by having the RFID reader relay messages from one WISP to another.

2 Commercial Impact

In this section we consider the potential for commercial impact of WISPs and WISP-like devices. It appears that the dream of arbitrarily inexpensive RFID tags will not come to pass. This is largely because the fixed costs associated with each tag, such as dicing, testing, antenna manufacturing, and tag assembly (i.e. mounting the tag IC on the antenna) do not benefit from technology scaling. It seems that these per-tag costs may put a price floor on low-end RFID tags, even if the silicon area required per tag continues to decrease. Even if the silicon area itself were cost free, these tag assembly and test costs would remain.

Given these dynamics, it appears that technology scaling should allow more functionality to be added to RFID tags for little cost above that of the most minimal RFID tag. If this analysis is correct, we would not expect to see the cost of RFID tags drop much below their present prices, but for that price, the tags can become more and more capable. The next few sections consider possible commercial applications for sensing and computing enhanced RFID tags.

2.1 Secure RFID

The ability to implement strong cryptographic algorithms such as RC5 (described in Chap. 15 [7]) and AES (described in Chap. 16 [33]) on passive RF-powered tags will likely be attractive for commercial applications. Using a WISP-like hardware platform, it would be possible to implement a secure RFID tag for applications such as access control or automotive tolling that could communicate securely via a conventional EPC Gen 2 reader. Ciphers such as AES, RC5, or ECC can be implemented in software, avoiding the time and expense of creating custom silicon for these functions.

2.2 Embedded RFID

WISP-like circuitry could be embedded in larger systems, such as phones or laptops, to provide some level of functionality, even when the host system is powered completely down. Configuration state for the system could be stored in "dual-ported" nonvolatile memory. With the device fully off, the configuration data or firmware could be read and (after modification) rewritten via the RFID interface. When the system powers up, it would read the data from nonvolatile memory via a conventional wired interface. This could allow configuration edits while the device is off, firmware upgrades while the device is still in its original manufacturer's packaging. Dirk Haehnel and I received a patent for this idea [25].

The chapter "Passive RFID-Based Wake-Up Radios for Wireless Sensor Networks" of this volume is another nice example of combining a WISP with a larger, battery-powered device in order to save power in the battery-powered device. They use the WISP, which consumes zero standby current, to wake up a conventional battery-powered sensor node. Using a conventional radio receiver to wake a sensor node consumes nonzero standby current consumption. Using a timer to wake the sensor node on a schedule also requires more power than waking from the interrupt that the WISP is used to generate [1].

2.3 Building Community: Open Source, the WISP Challenge, and the WISP Summit

It was clear that a platform like the WISP had many more possible applications than we could possibly explore ourselves. We open-sourced the firmware (via the BSD license) and posted all the schematics and design files on the web. With the support and encouragement of David Wetherall and Intel, we started a program, the "WISP Challenge," to make WISPs available to academic researchers. We solicited applications and awarded WISPs to the best proposals. Our aim was to seed the growth of a community of researchers interested in perpetually powered sensing and computing systems. Several of the chapters in this volume are the result of WISP Challenge awards.

After WISP Challenge users had some time to work with the WISP, our first "customer," Kevin Fu, suggested we organize a WISP Summit, to exchange information and see what sorts of results the community was generating. We held the first WISP Summit in Berkeley, CA, in conjunction with ACM Sensys 2009 (a major sensor networks conference). Videos of the first WISP Summit are available on the web.

3 Outgrowths

Other exciting projects exploring different forms of RF power harvesting have emerged from WISP, taken on lives of their own, and become major new projects in their own right. These projects are briefly described here; each has a chapter later in this volume.

3.1 WARP: Wireless Ambient Radio Power

Having become comfortable with harvesting "planted" RF power that had been deliberately emitted by an RFID reader for the purpose of powering electronic devices, we wondered if it would be possible to harvest "wild" RF power from ambient RF sources, such as TV, radio, or cell phone towers. Alanson found that there was a 1 MW (one million watt) digital TV tower about 4 km Intel Labs Seattle, and the balcony had an excellent view of the tower. Based on Friis's simple propagation model, we expected to see about 200 uW on the balcony. Our harvester delivered about 60 uW of rectified DC, which is about what we expected to see given the efficiency of our harvester, around 25% [15]. The chapter "Wireless Ambient Radio Power" of this volume presents new results on the WARP project [22].

3.2 WREL: Wireless Resonant Energy Link

When a group of physicists at MIT published their work on wireless power using magnetically coupled resonators (MCRs), I was the natural person at Intel to engage with it, since I had been working on wireless power for several years by then. Alanson Sample joined me again and began what would become the core of his Ph.D. thesis on wireless power. Alanson and I, together with undergraduate David Meyer, modeled the system using lumped circuit elements. This allowed us to clearly see the effects of mode splitting and opportunities to compensate for it. We built what we believe was the first MCR-based wireless power system that could adapt to changes in transmit–receive distance, coil orientation, or load. We called the system WREL, wireless resonant energy link [19].

3.2.1 FREED: Free-Range Resonant Electrical Energy Delivery

The chapter "A Portable Transmitter for Wirelessly Powering a Ventricular Assist Device Using the Free-Range Resonant Electrical Energy Delivery (FREE-D) System" [34] of this volume, by my U.W. graduate student Ben Waters (together with Alanson Sample, Yale heart surgeon Pramod Bonde, undergraduates Kara Kagi

and Jordan Reed, and me), describes our FREED system, which is a very exciting application of MCR-based wireless power. FREED supplies energy to the heart pumps known as LVADs (left ventricular assist devices). The goal is to eliminate the infection-prone "drive line," a thick cable that protrudes from the abdomen of present-day LVAD patients.

4 The Future

If the range scaling phenomenon described in the chapter "Range Scaling of Wirelessly Powered Sensor Systems" [24] continues, then capabilities that work with insufficient or barely sufficient range today should become feasible at much longer range in the future. But realizing this promise will require research effort.

4.1 Power Harvesting

Even if we assume that the power requirements and RF power available scale together (as they will if the technology follows the range scaling trajectory suggested in the chapter "Range Scaling of Wirelessly Powered Sensor Systems"), the voltage presented to the harvester will drop as range increases, unless measures are deliberately taken to boost the input voltage. An open fundamental question, raised in the chapter "Range Scaling of Wirelessly Powered Sensor Systems" is whether received voltage puts any fundamental bounds on the efficiency with which the energy can be harvested. Then there are the open practical questions of how to build the best possible harvester for any particular range (input voltage) and load. Agile harvesting is one exciting area of research: how to design harvesters that can tune themselves for different frequencies, amplitudes, and load levels.

Biological organisms are highly effective energy harvesters. Animals typically use previously stored energy to "fund" their present energy-harvesting efforts. Could RF power harvesters, using powered, active harvesting electronics, benefit from this strategy? Like biological creatures, active harvesters would not be able to let their energy supply drop to zero. Unlike today's simple energy harvesters, there might be no recovery from a starvation event.

4.2 Networking

As RFID tags evolve into RF-powered computers, the applications and usage models will become both more diverse and more complex. This will motivate the development of more sophisticated networking protocols. The BAT scheme, described in the chapter "BAT: Backscatter Anything-to-Tag Communication" [11],

is a step in the right direction. If future tags become full-fledged internet hosts, and RFID readers become access points (APs) connected to the internet, it will be possible to structure RFID systems in a completely new way. In a typical RFID system today, the tag is a simple "license plate" (i.e., a unique ID that is used as a pointer to additional information), and the reader is a straightforward conduit between the tag and a back end computer. It is the back-end computer that runs the application. Because the reader is tightly tied to an application, tags are only useful when they are read by readers that are prepared for those specific tags.

Contrast this with Wi-Fi networks today. As long as a client is authorized to use an AP, the client can communicate with any host on the internet. The client is not restricted to use a particular set of application software specific to each AP. If future highly capable computational RFIDs carry their own application software, and readers become APs that implement general purpose routing protocols, then from any reader in the world a tag could communicate sensor data or other information to its home base (server) or to another tag.

4.3 Big Power

While "big data" is currently a hot research topic throughout computer science, I believe that "big power" could be next, at least within the computational RFID community. Of course the notion of "big" is relative; "big power" for a WISP would seem very small to most other communities. The idea is to execute sensing and computing workloads, under RF power, that today seem impractically large, just as the RFID accelerometer seemed impossible when the WISP project started. Workloads such as cameras consume an amount of power that by RF-harvesting standards seems excessive initially; the standby current of the camera may exceed the power harvested from the RF source. One key to achieving "big power" computational RFID systems is that, as explained in the chapter "Range Scaling of Wirelessly Powered Sensor Systems" [24], power is not a conserved quantity (since it can be collected at one rate and spent at another); only energy is conserved. So the "big power" systems we are imagining would harvest energy at whatever (low) rate the source (RF or otherwise) is able to provide; the power-consuming portions of the system (such as the camera) would be completely powered off to avoid wasting the camera's standby current. Once sufficient energy has been accumulated after a long period of harvesting, the energy is spent suddenly, at high power levels for a short period of time. This approach should make it possible soon to RF power devices such as cameras that so far have seemed far too power hungry to ever be powered and read by an RFID reader.

Acknowledgments I thank James Landay, David Wetherall, Dieter Fox, Anthony Lamarca, and Matthai Philipose for the support and energy they gave to the WISP program at Intel Labs Seattle. Thanks to faculty collaborators Kevin Fu, Brian Otis, Tadayoshi Kohno, Paolo Feraboli, Sumit Roy, and Alexander Mamishev. I had the pleasure of working with many talented students on WISP and

related projects: Alanson Sample, Dan Yeager, Aaron Parks, Justin Reina, Bing Jiang, Seong–Ho Kim, Jeff Braun, Kishore Sundara–Rajan, Michael Buettner, Vamsi Talla, Yi "Eve," Zhao, Liang–Ting Jiang, Craig Macomber, Jim Youngquist, Ben Waters, Gunbok Lee, and others. I thank all the students for their fantastic work.

References

1. H. Ba, I. Demirkol, and W. Heinzelman. Passive RFID-based wake-up radios for wireless sensor networks. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
2. M. Buettner and D. Wetherall. Implementing the Gen 2 MAC on the Intel-UW WISP. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
3. M. Buettner, B. Greenstein, A. Sample, J.R. Smith, and D. Wetherall. Revisiting smart dust with RFID sensor networks. In *Proceedings of the 7th ACM Workshop on Hot Topics in Networks (HotNets-VII)*, 2008.
4. M. Buettner, R. Prasad, A. Sample, D. Yeager, B. Greenstein, J.R. Smith, and D. Wetherall. RFID sensor networks with the Intel WISP. In *Proceedings of the 6th ACM conference on Embedded network sensor systems*, pages 393–394. ACM, 2008.
5. M. Buettner, R. Prasad, M. Philipose, and D. Wetherall. Recognizing daily activities with RFID-based sensors. In *Proceedings of the 11th international conference on Ubiquitous computing*, pages 51–60. ACM, 2009.
6. H.-J. Chae, D.J. Yeager, J.R. Smith, and K. Fu. Maximalist cryptography and computation on the WISP UHF RFID tag. In *Conference on RFID Security (website)*, July 2007.
7. H.-J. Chae, M. Salajegheh, D.J. Yeager, J.R. Smith, and K. Fu. Maximalist cryptography and computation on the WISP UHF RFID tag. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
8. A. Czeskis, K. Koscher, J.R. Smith, and T. Kohno. RFIDs and secret handshakes: defending against ghost-and-leech attacks and unauthorized reads with context-aware communications. In *Proceedings of the 15th ACM conference on Computer and communications security*, CCS '08, pages 479–490, New York, NY, USA, 2008. ACM.
9. K. Fishkin, B. Jiang, M. Philipose, and S. Roy. I sense a disturbance in the force: Unobtrusive detection of interactions with RFID-tagged objects. *UbiComp 2004: Ubiquitous Computing*, pages 268–282, 2004.
10. F. Gasco, P. Feraboli, J. Braun, J. Smith, P. Stickler, and L. DeOto. Wireless strain measurement for structural testing and health monitoring of carbon fiber composites. *Composites Part A: Applied Science and Manufacturing*, 42(9):1263–1274, 2011.
11. A. Molina-Markham, S.S. Clark, B. Ransford, and K. Fu. Bat: Backscatter anything-to-tag communication. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
12. C. Pendl, M. Pelnar, and M. Hutter. Elliptic curve cryptography on the wisp uhf rfid tag. *RFID. Security and Privacy*, pages 32–47, 2012.
13. M. Philipose, K.P. Fishkin, M. Perkowitz, D.J. Patterson, D. Fox, H. Kautz, and D. Hahnel. Inferring activities from interactions with objects. *Pervasive Computing, IEEE*, 3(4):50–57, 2004.
14. M. Philipose, J.R. Smith, B. Jiang, A. Mamishev, S. Roy, and K. Sundara-Rajan. Battery-free wireless identification and sensing. *IEEE Pervasive Computing*, 4(1):37–45, 2005.
15. A. Sample and J.R. Smith. Experimental results with two wireless power transfer systems. In *IEEE Radio and Wireless Symposium, RWS '09*, pages 16–18, Jan. 2009.

16. A. Sample and J.R. Smith. The wireless identification and sensing platform. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
17. A.P. Sample, D.J. Yeager, P.S. Powledge, A.V. Mamishev, and J.R. Smith. Design of an RFID-based battery-free programmable sensing platform. *IEEE Transactions on Instrumentation and Measurement*, 57(11):2608–2615, Nov. 2008.
18. A.P. Sample, D.J. Yeager, and J.R. Smith. A capacitive touch interface for passive RFID tags. In *IEEE International Conference on RFID*, pages 103–109, April 2009.
19. A.P. Sample, D.A. Meyer, and J.R. Smith. Analysis, experimental results, and range adaptation of magnetically coupled resonators for wireless power transfer. *IEEE Transactions on Industrial Electronics*, 58(2):544–554, 2011.
20. A.P. Sample, J. Braun, A. Parks, and J.R. Smith. Photovoltaic enhanced UHF RFID tag antennas for dual purpose energy harvesting. In *IEEE International Conference on RFID*, pages 146–153, 2011.
21. A.P. Sample, C. Macomber, L.T. Jiang, and J.R. Smith. Optical localization of passive UHF RFID tags with integrated LEDs. In *IEEE International Conference on RFID*, pages 116–123, 2012.
22. A. Sample, A. Parks, S. Southwood, and J.R. Smith. Wireless ambient radio power. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
23. J.R. Smith. RFID tag with accelerometer, June 7 2011. US Patent 7,956,725.
24. J.R. Smith. Range scaling of wirelessly powered sensor systems. In Joshua R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
25. J.R. Smith and D. Haehnel. Device configuration with RFID, November 2 2010. US Patent 7,825,776.
26. J.R. Smith and J.A. Landay. Time domain embedding of application information in an RFID response stream, December 14 2005. US Patent App. 11/304,511.
27. J.R. Smith and M. Philipose. Inertially controlled switch and RFID tag, February 26 2008. US Patent 7,336,184.
28. J.R. Smith, K.P. Fishkin, B. Jiang, A. Mamishev, M. Philipose, A.D. Rea, S. Roy, and K. Sundara-Rajan. RFID-based techniques for human-activity detection. *Communications of the ACM*, 48(9):39–44, 2005.
29. J. Smith, B. Jiang, S. Roy, M. Philipose, K. Sundara-Rajan, and A. Mamishev. ID modulation: Embedding sensor data in an RFID timeseries. In *Information Hiding*, pages 234–246. Springer, 2005.
30. J.R. Smith, A.P. Sample, P.S. Powledge, S. Roy, and A. Mamishev. A wirelessly-powered platform for sensing and computation. In *Ubicomp*, pages 495–506, 2006.
31. J.R. Smith, A. Lamarca, and M. Philipose. Switch status and RFID tag, August 12 2008. US Patent 7,411,505.
32. J.R. Smith, D. Yeager, and A. Rahimi. Radio frequency identification tags adapted for localization and state indication, July 17 2012. US Patent 8,222,996.
33. A. Szekely, M. Hofler, R. Stogbuchner, and M. Aigner. Security enhanced wisps: Implementation challenges. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
34. B. Waters, K. Kagi, J. Reed, A. Sample, P. Bonde, and J.R. Smith. Powering a vad using the portable freed system. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
35. D.J. Yeager, P.S. Powledge, R. Prasad, D. Wetherall, and J.R. Smith. Wirelessly-charged UHF tags for sensor data collection. In *IEEE International Conference on RFID*, pages 320–327, 2008.
36. D.J. Yeager, A.P. Sample, J.R. Smith, and J.R. Smith. WISP: A passively powered UHF RFID tag with sensing and computation. *RFID Handbook: Applications, Technology, Security, and Privacy, pages 261–278, Boca Raton, FL*, 2008. CRC Press.

37. D.J. Yeager, J. Holleman, R. Prasad, J.R. Smith, and B.P. Otis. NeuralWISP: A wirelessly powered neural interface with 1-m range. *IEEE Transactions on Biomedical Circuits and Systems*, 3(6):379–387, 2009.
38. D. Yeager, F. Zhang, A. Zarrasvand, N. George, T. Daniel, and B. Otis. A 9μA, addressable Gen2 sensor tag for biosignal acquisition. *IEEE J. Solid-State Circuits*, 45(10):2198–2209, 2010.
39. D. Yeager, F. Zhang, A. Zarrasvand, N. George, T. Daniel, and B. Otis. System-On-Chip WISP: A 9 μA, addressable gen 2 sensor tag for biosignal acquisition. In J.R. Smith, editor, *Wirelessly powered sensor networks and computational RFID (this volume)*, New York, 2013. Springer SBM.
40. H. Zhang, J. Gummeson, B. Ransford, and K. Fu. Moo: A batteryless computational RFID and sensing platform. University of Massachusetts Computer Science Technical Report UM-CS-2011-020.

http://www.springer.com/978-1-4419-6165-5

Wirelessly Powered Sensor Networks and
Computational RFID
Smith, J.R. (Ed.)
2013, XIV, 271 p. 149 illus., 95 illus. in color., Hardcover
ISBN: 978-1-4419-6165-5