Revisiting Smart Dust with RFID Sensor Networks

Abstract
We argue that sensing and computation platforms that leverage RFID technology can realize “smart-dust” applications that have eluded the sensor network community. RFID sensor networks (RSNs), which consist of RFID readers and RFID sensor nodes (WISPs), extend RFID to include sensing and bring the advantages of small, inexpensive and long-lived RFID tags to wireless sensor networks. We describe sample applications suited to the space between existing sensor networks and RFID. We highlight the research challenges in realizing RSNs such as the use of intermittent power and RFID protocols suited to sensor queries.

1 Introduction
In the late 1990s, the vision of “smart-dust” was articulated by the research community. This vision was predicated on advances in microelectronics, wireless communications, and microfabricated (MEMS) sensing that were enabling computing platforms of rapidly diminishing size. The early proponents imagined devices one cubic millimeter in size with capabilities sufficient to power themselves, sense the environment, perform computation, and communicate wirelessly [9]. Large-scale deployments of such devices would enable a wide range of applications such as dense environmental monitoring, sensor rich home automation and smart environments, and self-identification and context awareness for everyday objects.

The past decade has seen significant effort and progress towards the original motivating applications. In particular, wireless sensor networks (WSNs) based on “mote” sensing platforms have been applied to many real-world problems. Remote monitoring applications have sensed animal behavior and habitat, structural integrity of bridges, volcanic activity, and forest fire danger [6], to name only a few successes. These networks leveraged the relatively small form-factor (approximately 1” x 2”) of motes and their multihop wireless communication to provide dense sensing in difficult environments. Due to their low power design and careful networking protocols these sensor networks had lifetimes measured in weeks or months, which was generally sufficient for the applications.

Despite this success, WSNs have fallen short of the original vision of smart-dust. They have not led to an approximation of sensing embedded in the fabric of everyday life, where walls, clothes, products, and personal items are all equipped with networked sensors. For this manner of deployment, truly unobtrusive sensing devices are necessary. The size and finite lifetime of motes make them unsuitable for these applications.

We argue in this paper that Radio Frequency Identification (RFID) technology has a number of key attributes that make it attractive for smart-dust applications. Passive UHF RFID already allows inexpensive tags to be remotely powered and interrogated for identifiers and other information at a range of more than 30 feet. The tags can be small as they are powered by the RF signal transmitted from a reader rather than an onboard battery; aside from their paper thin antennas, RFID tags are approximately one cubic millimeter in size. Moreover, their lifetime can be measured in decades as they are reliable and have no power source which can be exhausted. These advantages have resulted in the widespread deployment of RFID for industrial supply-chain applications such as tracking pallets and individual items. However, RFID technology is limited to only identifying and inventorying items in a given space.

The RFID Sensor Networks (RSNs) we advocate in this paper extend RFID beyond simple identification to in-depth sensing. This combines the advantages of RFID technology with those of wireless sensor networks. In our previous work, we have demonstrated the technical feasibility of building small, battery-free devices that use the RFID PHY and MAC layer to power themselves, sense, compute, and communicate; we refer to these devices as Wireless Identification and Sensing Platforms (WISPs) [15, 16]. While other research efforts such as [3] have combined RFID with sensing, to the best of our knowledge, the Intel WISP is the only RFID sensor node with computational capabilities and that operates in the long range UHF band.

While the feasibility of WISPs has been established by this earlier work, how to harness many such devices to create RSNs is an open question. An RFID sensor network consists of multiple WISPs and one or more readers. Consequently, realizing full-scale RSNs will require development at both the WISP and the reader, as new protocols and techniques must be developed unlike those of either RFID or WSNs.

The focus of this paper is the applications that RSNs enable and the systems challenges that must be overcome for these to be realized. As the traditional RFID usage
model is very different from that of WSNs, RSNs face substantial challenges when trying to integrate the two
technologies. For example, unlike WSNs, RSNs must
cope with intermittent power and unlike RFID must sup-
port sensor queries rather than simply identification.

2 FROM MOTES AND RFID TO RSNs

Two technologies have been widely used to realize real-
world monitoring applications: wireless sensor networks
via motes, and RFID via standard tags and readers. We
describe and contrast each technology and then present
their combination (Table 1) as RFID sensor networks
(RSNs). We use prior work on the WISP [15, 16] to
demonstrate the technical feasibility of this combina-
tion. Representative devices for the three technologies
are show in Figure 1.

2.1 Wireless Sensor Networks (Motes)

Currently, most WSN research is based on the Telos
mote [13], which is a battery powered computing plat-
form that uses an integrated 802.15.4 radio for commu-
ication. These motes are typically programmed to orga-
nize into ad-hoc networks [19] and transmit sensor data
across multiple hops to a collection point. To extend
network lifetime, motes duty cycle their CPU and radio
(e.g., with low-power listening [12]), waking up inter-
mittently to sense and communicate. With a duty cycle
of 1% motes can have a lifetime of up to three years be-
fore the batteries are exhausted.

The multihop communication paradigm of WSNs
means that they can be used to extend sensing capabil-
ities to great distances. This has made them ideal for a
wide range of sensing applications. However, the large
size of the mote and its finite lifetime makes it unsuit-
able for applications where sensing must be embedded
in small objects, or in inaccessible locations where bat-
teries cannot be replaced.

2.2 RFID

While there are a number of different RFID specifi-
cations, that of greatest interest for sensing applications
is the EPCglobal Class-1 Generation-2 (C1G2) proto-
col [4], as it is designed for long-range operation. The
C1G2 standard defines communication between RFID
readers and passive tags in the 900 MHz Ultra-High Fre-
quency (UHF) band, and has a maximum range of ap-
proximately 30 feet. A reader transmits information to a
tag by modulating an RF signal, and the tag receives both
down-link information and the entirety of its operating
energy from this RF signal. For up-link communication,
the reader transmits a continuous RF wave (CW) and the
tag modulates the reflection coefficient of its antenna. By
detecting the variation in the reflected CW the reader is
able to decode the tag response. This is referred to as
“backscattering”, and requires that a tag be within range
of a powered reader.

The MAC protocol for C1G2 systems is based on
Framed Slotted Aloha [14], where each frame has a num-
ber of slots and each tag will reply in one randomly se-
lected slot per frame. Before beginning a frame, a reader
can transmit a Select command which limits the number
of active tags by providing a bit mask, as only tags with
ID’s (or memory locations) that match this mask will re-
spond in the subsequent round. When a tag replies in
a slot, the reader can choose to singulate the tag. After
singulation the reader can read and write values to tag
memory. These mechanisms enable rapid identification
of tags and unicast read and write.

RFID tags are fixed function devices that typically use
a minimal, non-programmable state machine to report a
hard-coded ID when energized by a reader. As they are
powered by the reader the device itself can be very small,
though the antenna requires additional area. As the an-
tenna is flexible and paper thin, their small size means
they can be affixed to virtually any object and the object
can then be identified. However, RFID tags provide no
general purpose computing or sensing capabilities.

2.3 RFID sensor networks (WISPs + readers)

We define RFID sensor networks (RSNs) to consist
of small, RFID-based sensing and computing devices
(WISPs), and RFID readers that are part of the infra-
structure and provide operating power. RSNs bring the
advantages of RFID technology to wireless sensor net-
works. While we do not expect them to replace WSNs
for all applications, they do open up new application
spaces where small form-factor, long-lived, or inacces-
sible devices are paramount. Our hope is that they will
elegantly solve many sensor network applications, e.g.,
home sensing and factory automation where installing
readers is feasible.

Prior work at Intel Research demonstrates that WISPs
can be built today. The most recent Intel WISP is a wire-
less, battery-free platform for sensing and computation
that is powered and read by a standards-compliant UHF

Figure 1—Commercial UHF RFID tag, Accelerometer WISP, Telos
mote with batteries
RFID reader. The current version of the WISP has a range of up to 10 feet. It features a wireless power supply, bidirectional UHF communication with backscatter uplink, and a fully programmable ultra-low-power 16-bit flash microcontroller with analog to digital converter. This WISP includes 32K of flash program space, an accelerometer, temperature sensor, and 8K serial flash. Small header pins expose microcontroller ports for expansion daughter boards, external sensors and peripherals.

The Intel WISP has been used to implement a variety of demonstration applications that read data from a single sensor unit. These include the first accelerometer to be powered and read wirelessly in the UHF band, and also the first UHF powered-and-read strain gage [21]. Even without its sensing capabilities, the Intel WISP can be used as an open and programmable RFID tag: the RC5 encryption algorithm was implemented on the Intel WISP [2]. We believe this is the first implementation of a strong cryptographic algorithm on a UHF tag.

3 Example Applications

RFID sensor networks have broad applicability wherever sensing, small form factor, embeddability, longevity, and low maintenance are desired and fixed or mobile readers are feasible. This section highlights applications within this space and some of the key design considerations.

3.1 Blood

Blood transfusions save lives, replacing blood lost during surgery, illness, or trauma. After donation, blood is bagged and refrigerated between 1° and 6° C and has a shelf life of about 35 to 42 days. Refrigerators used to store blood are monitored for outages and temperature fluctuations, and collection dates are recorded on blood bags. However, the temperature of the bag itself is rarely monitored with any regularity. This makes it difficult to determine if a given bag was warmed to unsafe levels, such as if it is near the front of the refrigerator and the door is often opened. Additionally, it is difficult or impossible to gauge exposure during transport from a donor to a bank, between banks, and ultimately to a patient.

WISPs with temperature sensors could be attached directly to individual blood bags and queried for their measurements. Such sensors must be small (one could imagine affixing sensors with something like a price tag gun), and inexpensive to the point of being disposable.

To understand the challenges in building such an application, an Intel WISP was attached to a container of milk (a suitable and widely available approximation of a bag of blood), and its temperature was monitored over the course of 24 hours [20]. For this study, a storage capacitor (roughly the size of a pea) was attached to the WISP. This enabled the WISP to log sensor data for up to a day when out of range of a reader.

3.2 Brains

Recent research in neuroscience has explored using neural sensors for controlling prosthetic limbs [18]. Sensors placed outside the skull can capture neural activity but the signals are too coarse-grained and noisy to be effective. With surgery, sensors can be placed directly on the brain resulting in much higher resolution and finer control of the limb. Using conventional technologies (e.g., motes) presents difficulties with respect to power because batteries need to be replaced via invasive surgical procedures, as is the case with pacemakers.

An RFID sensor network is well suited to this application. A patient would have WISPs equipped with neural probes placed inside the skull. These could then draw power from and communicate with a device outside the body, e.g., an RFID reader worn as a cap, bracelet, or belt. We have completed initial studies that show the feasibility of integrating neural sensors with the WISP [7].

3.3 The Elderly

Providing care for the elderly is one of the largest healthcare costs facing us today, particularly as the “baby boomer” generation ages. Keeping people in their homes for as long as possible significantly reduces these costs and increases quality of life. The difficulty with this is detecting and reacting to emergencies, such as the patient falling or forgetting to take critical medication. Currently, families have no choice but to hire costly support personnel to regularly check-in on their loved ones.

Traditional RFID has been explored to help monitor the behavior of the elderly. For example, by having the patient wear a short range RFID reader bracelet and placing RFID tags on a toothbrush, toothpaste, and faucet, software can infer that an elderly person is brushing her teeth when these tags are read in succession [11]. Such fine-grained sensing requires very small devices, and is simpler and more respecting of privacy than competing

<table>
<thead>
<tr>
<th></th>
<th>CPU</th>
<th>Sensing</th>
<th>Communication</th>
<th>Range</th>
<th>Power</th>
<th>Lifetime</th>
<th>Size (inches)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSN (Mote)</td>
<td>Yes</td>
<td>Yes</td>
<td>peer-to-peer</td>
<td>Any</td>
<td>battery</td>
<td>&lt; 3 yrs</td>
<td>3.0 x 1.3 x .82 (2.16 in³)</td>
</tr>
<tr>
<td>RFID tag</td>
<td>No</td>
<td>No</td>
<td>asymmetric</td>
<td>30 ft</td>
<td>harvested</td>
<td>indefinite</td>
<td>6.1 x 0.7 x .02 (.08 in³)</td>
</tr>
<tr>
<td>RSN (WISP)</td>
<td>Yes</td>
<td>Yes</td>
<td>asymmetric</td>
<td>10 ft</td>
<td>harvested</td>
<td>indefinite</td>
<td>5.5 x 0.5 x .10 (.60 in³)</td>
</tr>
</tbody>
</table>

Table 1—Comparison of Technologies
approaches using computer vision, where video of the person is continuously recorded and analyzed.

Adding sensing (e.g., an accelerometer) to long range RFID tags would have several key advantages. Rather than requiring a person to wear a short-range reader, which can be taken off, a single long-range reader could be placed in the home and behavior could be determined via direct communication with the objects that are being interacted with. This explicit information would be more accurate in detecting behavior than inference based only on object identifiers.

RSNs are an appropriate solution for the above applications and those like them. Our initial studies using the WISP show the potential of existing RFID sensing devices for use in such applications. However, these studies involved only a single WISP. Combining many such devices into a full RSN will require further research.

4 Challenges

RSNs combine the technology of RFID and sensing with the usage models of sensor networks. At the device level, the WISP shows that it is feasible to combine sensing with RFID. However, at the systems level, challenges arise due to the mismatch between the RFID usage model and that of wireless sensor networks. We detail several challenges in this section.

4.1 Tasks and Intermittent Power

RFID tags are powered only when they are in range of an RFID reader. For regulatory and other reasons, readers do not transmit a signal continuously. Instead, they power tags for a brief period of time before changing channels or entirely powering down. Thus, tags have an unpredictable and intermittent source of power. Moreover, the RFID model assumes that if a tag is powered it will have sufficient energy to respond to a command, e.g., to transmit its identifier.

The above is a poor fit for sensor networks that seek to complete a task that may span many RFID commands. For example, the WISP harvests energy only when a reader is transmitting and at a rate largely determined by its proximity. This energy is stored in a capacitor and when enough energy is harvested the WISP powers up and can begin sensing and communicating. However, sensing and communication drain power from the WISP. This can result in the WISP losing power in the middle of an operation depending on the task and the reader behavior. A further complication is that receiving, transmitting, performing computation, and reading/writing to memory all consume different amounts of energy.

To run tasks to completion, or at least in a manner that can tolerate power interruptions, WISPs are likely to require support for intermittently powered operation. They will need to be able to estimate the energy required to complete a task, perhaps based on task profiling or energy budgets, and compare it with estimated reserves. To work well in this regime, it is also likely that RSN devices will need to cooperate with RFID readers for power management. This would involve signaling by either the reader, of its intended transmission time, or by the WISP, of its needs. Even with signaling, it may be difficult to predict power expectations because the rate at which energy can be harvested depends on the frequency of the reader and the proximity of the device to the reader, both of which will change over time. Thus, to increase the kinds of tasks that can be supported, large tasks must be split into smaller, restartable stages and device storage (flash or RAM) can be used to pass intermediate results between the stages.

4.2 Unpowered Operation

In many cases, WISPs may need to gather sensor data when they are not in the proximity of an active RFID reader. For example, the temperature of blood plasma should be monitored while it is out of the refrigerator; even though these periods should be relatively short they are crucial for the application.

To extend functionality when away from a reader, one approach is to provide a small amount of energy storage on the device, e.g., a capacitor, and store excess energy when close to an active reader. This storage capacitor can be small relative to a battery, because it is intended only for short term usage and is wirelessly recharged over time. The Data Logger WISP used for the milk carton study takes this approach, using a super-capacitor that, when fully charged, sustains low duty-cycle operation for more than a day. The type of tasks that this enables is limited, due to energy requirements, and the period of functionality is limited due to leakage.

This use of stored energy for unpowered operation raises many of the same issues as completing tasks given intermittent power. We believe that a single power API could support both situations. Stored energy is even likely to help by providing a known buffer period for loss of power. However, unpowered operation is likely to stress tradeoffs between stages. For example, writing to flash is significantly more energy intensive than computing with RAM but preserves valuable data for later use. Unpowered operation is also likely to benefit from task adaptation. For example, the duty-cycle or sensor sampling rate might be increased or decreased depending on the long-term power harvesting trends.

4.3 Sensing Protocols

WSN nodes are peers in terms of the physical and link layers of their communication, e.g., each mote has an 802.15.4 radio capable of sending and receiving transmissions with other nodes that are in range. In con-
trast, because they draw on RFID, RSN nodes will be highly asymmetric in terms of their communication abilities. With RFID, readers are able to transmit messages to all tags and tags can transmit messages to the reader. However, tags can do so only when the reader initiates communication, and tags cannot communicate directly with each other even when powered by the reader.

These differences complicate protocols designed to gather and process sensor data. Currently, WISPs with new sensor data must wait until they are interrogated by a reader. This increases the likelihood of many devices wanting to use the bandwidth limited channel at the same time. Techniques to perform data pre-processing within the network (on each RSN device) can help to some extent. However, the standard RFID strategy of identifying and then communicating with each device is wasteful as most devices may not have relevant data—a more dynamic strategy based on the value of the sensor data would be more effective.

Consider the eldercare application. A reader might have hundreds of accelerometer WISPs in its field of view. Because all the WISPs share a single reader channel, the update rate per tag would be very low if every tag were simply queried for sensor data sequentially. However, at any given moment, only a few objects will typically be in motion (and therefore producing non-trivial accelerometer sensor values). Furthermore, the set of objects that are moving changes dynamically, as objects are put down and picked up. One might want a protocol which gives priority to the most active objects, politely “yielding” to new objects when they start to move.

Existing RFID solutions do not support anything like this functionality. As a first step, one could have WISPs with sensor activity below a threshold not respond to the reader. But an appropriate threshold level may depend on what is occurring in the room, and such a simple scheme would not support the “polite yielding” described above.

For another example of what RSN protocols might be asked to do, consider the blood application. When many blood bags are read simultaneously, one might want to interrogate the bags with the largest temperature excursions first. But since the distribution of temperature excursions is not known a priori by the reader, the protocol would need to (implicitly) estimate this information. It might for example ask if any WISP has a larger temperature excursion than $E$. If no device responds, the $E$ response threshold would be repeatedly halved until the appropriate scale was found. The key requirement is to estimate an aggregate property of the data without exhaustively collecting that data. Finally, RSN protocols might be power aware as well. A WISP that was about to lose power might be given priority over those with ample power.

New tools will be needed to explore RSN communication protocols. As a first step, we are developing an RFID reader platform based on the Universal Software Radio Peripheral (USRP). This platform used in conjunction with the WISP allows for the development of new protocols at both the MAC and PHY layers. Thus far we have used it for RFID monitoring [1].

### 4.4 Repurposing C1G2

There would be substantial practical benefit to realizing RSN protocols using the primitives of the C1G2 standard: commercial off-the-shelf readers could then be used for RSN research and deployment, and WISPs would interoperate with ordinary (non-sensing) tags. However, the extent to which RSN protocols can be implemented within the C1G2 standard is an open research question. Additionally, there is the practical consideration of commercial readers not exposing low-level functionality and not implementing the complete C1G2 specification. Because of this, even RSN protocols built on top of the C1G2 specification may not be implementable using standard readers.

Our experience with the Intel WISP suggests that basic RSN applications can be approximated using standard C1G2 readers. To read sensor data from a C1G2 WISP, the device must first be *singulated*, at which point a temporary *handle* is requested from the tag. A reader can then use this handle to address the device and read sensor data from pre-defined memory locations. However, the handle persists only until the reader singulates another tag or the tag loses power. Thus, reading from more than one WISP incurs substantial protocol overhead due to singulation and handle management. Consequently, simple use of the existing C1G2 protocol can provide some level of sensing functionality, but at a significant cost in terms of efficiency.

Along with reading sensor data, the C1G2 protocol can support basic sensor queries using the *Select* command. If the reader knows that a sensor value is written to a particular memory location, it can issue a *Select* command with a mask which matches that location for sensor values over a given threshold. Consequently, only WISPs with sensor values over that threshold will reply during the next frame. More generally, the *Select* command could be used as a general purpose broadcast channel. The bit mask in the command could be repurposed and interpreted, in the most general case, as opcodes and data. As multiple *Selects* can be sent before each frame, complex tasking and querying could be achieved in this manner.

The above mechanisms show that there is potential for using the C1G2 standard to implement RSN protocols. This would have the advantage of being implementable using current reader technology, given a reader that is sufficiently programmable. However, these
mechanisms may prove too inefficient or may simply be poorly matched to many applications. Further experimentation is needed.

4.5 Tasking and Querying

Tasking can refer to a number of different things in the context of sensor networks. One extreme is the transfer of an entire code image to a device which changes its basic operation\(^\text{[8, 17]}\), while the other extreme is transmitting simple commands to trigger preconfigured behavior such as modifying the sampling rate of a sensor. Several WSN projects have chosen points in between, inventing high-level task construction languages\(^\text{[5]}\), or adopting SQL-style declarative queries\(^\text{[10]}\). Generally, for non-trivial applications some method must be available to actuate the behavior of devices.

The communication model of RFID results in different trade-offs with respect to tasking than are seen in WSNs. When tags are being powered sufficiently, the energy cost of transmission is essentially zero and transferring large amounts of code is feasible. This allows for the complete retasking of WISPs with costs in terms of latency only. Conversely, because downlink communication is cheap when in range of the reader, WISPs may not need to be as “smart” as motes. For example, requirements for precomputation and aggregation may be relaxed and filtering could be done through complex queries.

In RFID terminology querying refers to identifying tags, while in WSNs it refers to expressively indicating the sensor data of interest. In order to realize the latter idea using WISPs, query languages and methods of communicating queries need to be developed. As in WSNs, there is a fundamental trade-off between expressiveness and efficiency. In some regards, querying is closely coupled with tasking as the complexity is split between the reader and the WISP.

However, as discussed in the previous sections, energy concerns play a part in determining how to divide functionality between the reader and the device. For example, interpreting complex queries on the WISP may be efficient with respect to latency but inefficient with respect to energy. Quantifying these trade-offs is an open question.

5 Conclusion

By exploiting RFID technology, we believe that we can expand the application space of wireless sensor networks to ubiquitous, embedded sensing tasks. We have sketched sample sensor network applications in the space between traditional mote networks and RFID for supply-chain monitoring. We have described key systems and networking challenges related to intermittent power and RSN protocols for sensor queries. We expect RSNs to be a fruitful new space for networking and systems research, as there is significant work that must be done to translate the capabilities of the WISP into full-fledged RSNs.

References