

Sensors, Tags, and Security

Joshua R. Smith

Abstract

Sensors and Radio Frequency Identification (RFID) tags promise to create environments that are safer, smarter, and more secure---benefiting persons with disabilities, and everyone else. First I present several examples to illustrate the promise of sensors and tags. Then I describe an obstacle to realizing the vision---the high cost of tags---and a possible solution: bifurcating future tags into one class that is less capable but far cheaper than the tags of today, and another that is much more capable, though expensive.

The Promise of Sensors and Tags

Giving our houses, cars, and other everyday environments the ability to sense and identify every object, every person, and their respective activities and histories would create enormous benefits, for persons with disabilities, and everyone else. Every physical object would have a “digital shadow,” a set of electronic information that corresponds to the physical object. This vision would enable everyday environments to become smarter, safer, and more secure.

The technology necessary to realize this vision includes novel sensors, wireless networks, and Radio Frequency Identification (RFID) tags.

Examples

I will start with some examples to illustrate the promise of sensors and tags to create smart spaces.

First I'll describe Electric Field Imaging, the subject of my PhD thesis.¹ Electric Field Imaging is fairly new to humans, but several species of fish sense their environments using this sensor modality. The still image below is taken from a video illustrating the behavior of the system. In the image, my "School of Fish" sensor array is tracking the position and orientation of a hand by looking at how its conductivity distorts electric fields being generated by the sensor units.²

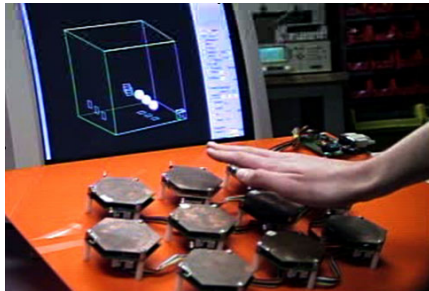


Figure 1 "School of Fish" Electric Field Imaging array tracking hand position and orientation.

What is it good for? Neil Gershenfeld and I used the technology to invent a smart car seat that uses Electric Field Imaging to unobtrusively measure the passenger in the front seat of a car, and prevent airbag deployment when it would be dangerous, for example if the passenger is an infant or small child.³ Electric Field Imaging turns the interior of the car into a smarter and safer environment.⁴

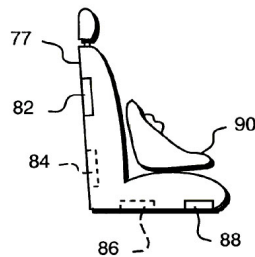


Figure 2 Schematic illustration of smart car seat..



Figure 3 The smart car seat is now commercialized by Elesys, and is standard equipment in many Honda cars, such as the CR-V pictured above.

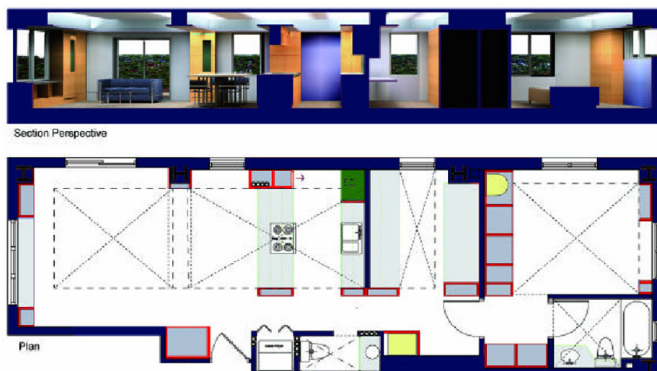


Figure 4 MIT-TIAX PlaceLab "living laboratory," a highly instrumented home of the present

As another example of a smart space, I'll describe a "smart apartment," the MIT-TIAX PlaceLab⁵. PlaceLab is not a home of the future, but rather a highly instrumented home-of-the present. It is a laboratory for evaluation of present-day in-home behavior, and to help prototype and evaluate technologies that may have a place in future homes. The home is encrusted with sensors. All the utilities--every water facet and light switch---and all the appliances can be individually monitored. Applications envisaged for PlaceLab include monitoring and

prompting inhabitants to improve health and wellness (“Proactive Health”), tracking Activities of Daily Living, and evaluation of wearable devices. Changes in patterns of Activities of Daily Living can be indicators of the onset of cognitive disabilities, such might be caused by Alzheimer’s disease.

The next example is work I did at Escher Group involving Radio Frequency Identification. In the first example, we’ve created a smart door that can recognize who you are and unlock itself if you’re allowed to enter. All you have to do is touch the doorknob. It instantly unlocks if you’re authorized.



Figure 5 Smart Door. Radio Frequency Identification (RFID) Tag is embedded in a shoe. An RFID reader connected to the door handle interrogates the tag through the person’s body, and unlocks the door only if they are authorized.

Here’s how it works. A commercial off-the-shelf Radio Frequency ID (RFID) chip is mounted in a shoe. It is connected to two electrodes, one of which “sees” the floor, the other of which sees the person’s body. Connected to the (metal) door handle is a special RFID reader that is designed to couple electrically to tags, instead of magnetically like most comparable readers. Because it couples electrically, the human body can act as a conductor that guides the fields, bringing them from the doorknob to the tag in the shoe.

When the person touches the doorknob, a tiny amount of power travels from the doorknob, through the person’s arm, down to their shoe, where it powers up the tag. When the tag in the shoe is powered up, it transmits its ID back through the body to the reader in the doorknob, by modulating the load it presents to the reader.



Figure 6 Radio Frequency Identification (RFID) tagged package. The reader is embedded in the shoe of the postal delivery person (orange shirt). When the package is handed off, the recipient’s body provides a ground path that completes a circuit and causes the ID to be read.

The same technology can be configured in a different way to let your hand act as a barcode reader. In this case, an RFID tag is affixed to a package that needs to be tracked. Figure 6 is a still from a demonstration video. The author (in orange shirt) is playing the role of the postal delivery person, and has an RFID reader mounted inside the sole of his shoe. Noah (in glasses) is the postal customer. A priority mail package has been tagged with an RFID. When the package is handed off, Noah’s body provides a ground return path that completes the circuit and allows the ID to be read. This circuit includes the reader, the postal worker’s body, the RFID tag, and the recipient’s body. The act of handing off the package has been “activated,” so that the important act of handing off the package automatically generates the digital record, with no explicit “scan” or other action required.

A Problem for the Promise of Tags

Hopefully the examples above have conveyed a sense of the promise of sensors and tags. Now I’ll describe a problem that is holding back the vision. The problem is that they’re far

We are seeing two new classes of ID tags emerge. One class is even more expensive than present-day tags, but delivers far more functionality. The other class does not use chips and is far cheaper, but delivers less functionality.

to expensive for the high volume, individual item-level tracking applications that get people excited.

Many people are familiar with Moore's law, the observation that the number of transistors on a top of the line Integrated Circuit (IC) doubles every 18 months. Thanks to Moore's law, IC performance has improved by many orders of magnitude since their invention; at the same time, the cost of the largest ICs has remained roughly constant, meaning that the price/performance ratio has been dropping exponentially.

Can't we just wait for Moore's law to take care of the RFID price problem? Unfortunately not. The exponential drop in price to performance ratio only applies to top-of-the line ICs, not to the bottom of the heap, where by definition RFID chips live. Why? In addition to the "per transistor" cost of a chip, which has been dropping exponentially, there is also a "per chip" cost associated with things like handling the individual physical chip. That cost isn't dropping exponentially---it stays about the same. For a complex microprocessor with hundreds of millions of transistors, the chip-handling cost is small when amortized over all the transistors on the chip. For a tiny RFID with just tens of thousands of transistors, the per-chip costs represents a persistent floor that is hard to break through.

That is not to say that RFIDs will never break through this cost floor. But Moore's law scaling will not take care of the problem "automatically." Other fabrication processes, like polymer electronics, may provide a solution. But it is at present unclear when, if ever, this cost breakthrough will occur.

A Surprising Solution?

I believe that, in the absence of such a breakthrough, we will see RFID technology bifurcate to address the problem. We are seeing two new classes of ID tags emerge. One class is even more expensive than present-day tags, but delivers far more functionality. The other class does not use chips and is far cheaper, but delivers less functionality.

More capable than RFID: WiFi Tag

Caveo Technology has created a family of so-called WiFi tags.⁶ These are battery powered and communicate to the increasingly omnipresent WiFi (also known as IEEE 802.11) wireless Local Area Network (LAN) Access Points, gadgets that are being found in the corners of more and more homes and offices. The benefits of WiFi are (1) the cost of the Access Points is now very low; (2) WiFi Access Points are already widely deployed for Local Area Network access, and (3) WiFi range is very long---up to hundreds of meters---much farther than ordinary RFID.

However, the power required to transmit a WiFi signal is substantial. With the naïve approach of periodically "pinging" each tag, virtually any battery would be drawn down quite quickly.

But Caveo has realized that for many applications, it's only necessary to track objects when they move. Caveo has a lot of expertise in motion sensing and other applications of accelerometers. The WiFi tags are ordinarily dormant, drawing virtually no power. Each of the WiFi tags wakes up and transmits its location only when it is moved. These tags are projected to cost much more than an ordinary RFID---\$65 to \$100---but they deliver much more functionality.

Cheaper than RFID: FiberFingerprint

The FiberFingerprint technology I invented at Escher Group can be viewed as the other end of the identification spectrum.⁷ Every square centimeter of every piece of paper has a unique pattern of hills and valleys, much like a person's fingerprint. Like an ordinary fingerprint, this unique characteristic can be used either for authentication, or for identification. I originally created the technology to address the problem of electronic postage authentication. Electronic postage promises to add digital security to postage by using public key digital signatures, which anyone can verify but only the post office can issue. While standard digital postage technology effectively prevents forgery (the creation of apparently valid postage from scratch), it provides no protection against the copying of genuine postage. FiberFingerprint can add this protection, without adding the cost of an RFID chip, which is far too expensive for ordinary mail pieces.

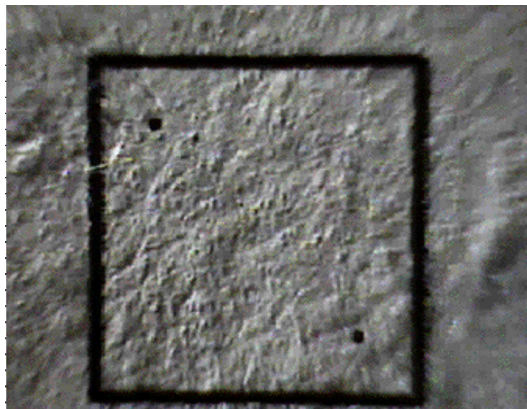


Figure 7 FiberFingerprint. Each square centimeter of paper has a unique pattern of hills and valleys that can serve as a unique identifier, much like a person's fingerprint. This costs far less than RFID, though the capabilities it delivers are less as well.

To generate a new piece of electronic postage, a postage meter would examine the unique characteristics of the individual, original envelope, turn these unique characteristics into a number, append postage-related information such as the value, date, meter number, and so forth, and then generate a digital signature of all this information together. It would then print all the information and the signature in machine-readable form on the envelope, as a two-dimensional barcode or as a digital watermark. At verification time (in a postal sorting center, for example), all the machine-readable information would be read, the digital signature would be verified, and the FiberFingerprint information would be compared to the physical envelope. If the FiberFingerprint information printed on the envelope does not match the characteristics of the actual envelope in the sorting center, it indicates that a copy has been made.

Just like ordinary fingerprints, it turns out that FiberFingerprint technology can be used for identification as well as authentication. For a major watchmaker, my colleagues and I at Escher Group demonstrated that individual watches could be uniquely identified based on intrinsic, naturally occurring variations in their surface characteristics.⁸ Figure 8 shows a watch logo being examined by the FiberFingerprint software. The logo outline is used for registration purposes. Random variations in the watch logo in the region between the cross and the shield function as a unique identifier. This allows individual watches to be identified and tracked without having to add a chip, or anything else, to the watch.

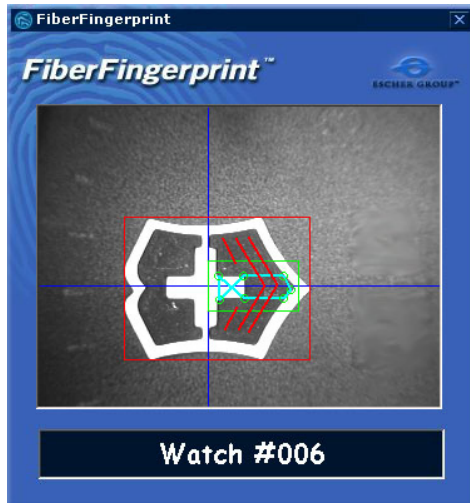


Figure 8 FiberFingerprint Identification of watches. The surface inside the shield region has inhomogeneous characteristics, just like the paper surface, that can be used to uniquely identify the watch.

Both the authentication and identification applications of FiberFingerprint overlap with RFID---RFID is routinely proposed as a solution for both problems. FiberFingerprint has the advantage of being orders of magnitude cheaper than RFID, because no chip is required. It's also easier to integrate into a product, since nothing has to be added to the product. On the other hand, FiberFingerprint is less capable than RFID. FiberFingerprint requires an optical line of sight from a camera to the object---the "reader" has to be able to see the object. While FiberFingerprint authentication can occur offline, with no network or database access required, FiberFingerprint identification requires a database search in order to identify the item. In that sense, it offers less functionality than ordinary RFID, which provides a stable, repeatable ID without requiring a database search. Thus the back end infrastructure costs of very low end tags like FiberFingerprint are higher

than those of conventional RFID.

Conclusion: What does it mean for People with Disabilities?

As some of the examples I've discussed show, sensors and tags are already enabling smarter, safer, and more secure environments. Much more is on the way. This technology will enable environments that support proactive healthcare, aging in place, and assist with autonomous living for people with cognitive disabilities.

RFID will likely be an important piece of future smart infrastructure. Unfortunately, the price-performance ratio that many people are hoping for from RFID may not be achievable any time soon, or ever. This is a roadblock that is impeding realization of the promise of sensors and tags. A possible solution is for RFID products to bifurcate into a lower cost, lower functionality class, and a higher cost, higher functionality class.

The lower cost tags will have higher back end costs. However, thanks to Moore's law, the cost of this back end infrastructure is dropping exponentially, so perhaps this approach offers a way for Moore's law to solve the RFID price problem after all, and deliver on the promise of sensors and tags to improve life both for persons with disabilities, and for the general public.

About the author:

Joshua R. Smith is a Ubiquitous Computing Researcher at
Intel Research Seattle
1100 NE 45th Street
Seattle, WA, 98105
joshua.r.smith@intel.com

At the time of the State of Technology Conference, he was a Senior Technologist with TIAX LLC, a collaborative Research and Development company in Cambridge, Massachusetts.

References

- ¹ Smith, J.R. Electric Field Imaging, MIT PhD Thesis, 1999.
- ² Smith, J.R. FieldMice: Extracting Hand Geometry from Electric Field Measurements. IBM Systems Journal, Volume 35, No. 3&4, 1996, pp 567-608.
- ³ Gershenfeld, N, and Smith, J.R. US Patents 5844415, 5914610, 5936412, 6025726, 6051981, 6066954.
- ⁴ www.elesys-na.com
- ⁵ www.tiaxllc.com
- ⁶ Kirsner, S., Lost and Found, http://www.boston.com/business/technology/biotechnology/articles/2004/03/22/nanotech_biotech_at_key_juncture?mode=PF, published 3/22/04.
- ⁷ Metois, E., Yarin, P.M., Salzman, N., Smith, J.R. FiberFingerprint Identification. Proceedings of the Third Workshop on Automatic Identification. Tarrytown, NY, 2002, pp. 147-154.
- ⁸ Smith, J.R. Imperceptible Sensory Channels. IEEE Computer, Vol. 37. No. 6, pp. 84-85 June 2004.