New uses for RFID and security for the internet of things

May 31 2017, by Bernadette Esposito

Sanjay Sarma. Credit: David Sella

On the 25th anniversary of the universal barcode in 1999, the barcode community gathered around Sanjay Sarma and his colleagues and said, "Let's do this."

"Our idea," says Sarma, vice president for open learning and the Fred Fort Flowers (1941) and Daniel Fort Flowers (1941) Professor of Mechanical Engineering at MIT, "was to track everything in the supply chain." Some companies knew they had too much inventory. Others didn't know where their inventory was. Consumers couldn't find the right sized shirt while that shirt was sitting in the back room. Food was going bad and shelves went un-stocked. Things got lost in the supply chain. So, Sarma, along with research scientist David Brock of MIT and Kevin Ashton, a visiting researcher from Proctor and Gamble, came up with a low-cost radio frequency identification (RFID) tag. "At the time, it was a crazy idea," says Sarma. "But it stuck."

RFID tags, which had been around for several decades, were clunky and expensive—partly because of the amount of data placed on the tags. "We used to say, 'Someday the internet will be everywhere'—this was late 90s—and we didn't have the word 'cloud' yet. So, we used to say, 'Someday, you can write the data in the sky,'" says Sarma, who developed new standards for RFID, new manufacturing processes, and innovative ways to use them in the supply chain. The supply chain industry adopted the protocol, and standards-making efforts shifted. Auto ID Labs laid the groundwork for the standardization of RFID technology. It took sensing of identity—the job of RFID and barcodes—and made it universal. Auto ID Labs, where Sarma remains active today, emerged from the MIT Auto ID Center. "In many ways that effort also laid the groundwork for what is now called the internet of things," Sarma says.

Internet of things

"If you look at the world today, you may have a Nest Thermostat in your home; you may have an Amazon Echo in your home; if you're lucky enough to own a Tesla car, you can actually track your Tesla car over the internet. More appliances are becoming fundamentally internet-

connected and intelligent in ways that make our lives safer, the world safer, help with climate change, help with saving costs, help with better health care," says Sarma. All of this comes from a network of objects embedded in intelligence that interact with the environment. That is called the internet of things.

"When we start connecting things," says Sarma, "we enable a level of resource management, a level of marshalling of the planet, of what the planet offers us. When we have little or no information on something, we over-compensate. We burn more electricity, more energy and we're doing more damage to the planet." He asserts that hundreds of rooms are consuming electricity they should not, that are heating when no one is there. If you knew that a person was still driving and that there's no need to turn the heat on, just imagine how much energy one could save and what impact this technology would have on the planet. "To me, saving the planet is sort of an existential question and we have an enormous amount of work to do to do that," Sarma explains.

Risks, norms, and rules

With any new technology, there are risks. The first and most fundamental one for the internet of things is privacy. "If I have a Nest Thermostat in my house, I can turn the heating off when I'm not at home. If I forget to turn off the heat when I go on vacation, it can detect that I'm away and turn itself off." The flipside is that it can tell the wrong person you're not there, thereby increasing the risk of theft and burglary. A sort of extreme version of that, he explains, is a malicious party claiming control of a nuclear power plant. This is the great fear of the internet of things: Many people are adopting it and they're moving fast, but they're not thinking about security, and that is a recipe for disaster. "My research deals with balancing the two," Sarma says.

In any system with an agreed-upon architecture and with easy-to-

understand methods, safeguards and security can be built into the system. "Imagine if you were concerned about safety on the roads—and we did have those worries a hundred years ago," says Sarma. Over time, certain standards are implemented. "In the U.S. we drive on the right side of the road; we have traffic lights; we have stop signs; we have behavioral norms. If a parent and a child want to cross the street at a crosswalk, traffic stops. If a school bus in front of you flashes its lights, you stop. These behavioral norms—these standards—help recognize when something goes awry." Sarma explains that if one of these behavioral norms is broken, one can deduce that the driver's eyesight isn't good, or that they weren't paying attention, or maybe they were texting, or maybe that person is malicious.

The problem with the internet of things is that within this newly established world, there are few norms. When different people implement it in their own way, it's very hard to detect malice, he says. It's also hard to put together a protection. Unlike the road systems, in which there are police cars and cameras, "we don't have any of those. The internet of things is the wild west. My own research is directed toward establishing those norms and rules, so that at least you have some orderliness, so the remnant disorderliness stands out and can be detected."

Avatar

One protection Sarma and his team are promoting is something called the avatar, a cloud-things concept. "The basic idea we're saying is don't have Object A talk to Object B, have Object A talk to its cloud avatar of itself. Have Object B talk to its Cloud Avatar of itself. Then, have the Avatars talk to each other." The reason it works is because physical connections between A and B are many. "If you just say, the real object only talks to its avatar and the avatars talk to each other, we can bring to bear all the stuff we know from the WorldWideWeb, etc. That's a clean

way to look at the future of the internet of things and, strangely enough, that's what Tesla does, that's what Nest does, but unfortunately implementations are a little bit all over the place," he says.

"The internet of things will go through its ups and downs, but when we look back on our lives in 10 years, pretty much anything you do you'll back on a day when it wasn't connected and you'll sort of wonder how life was then."

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology