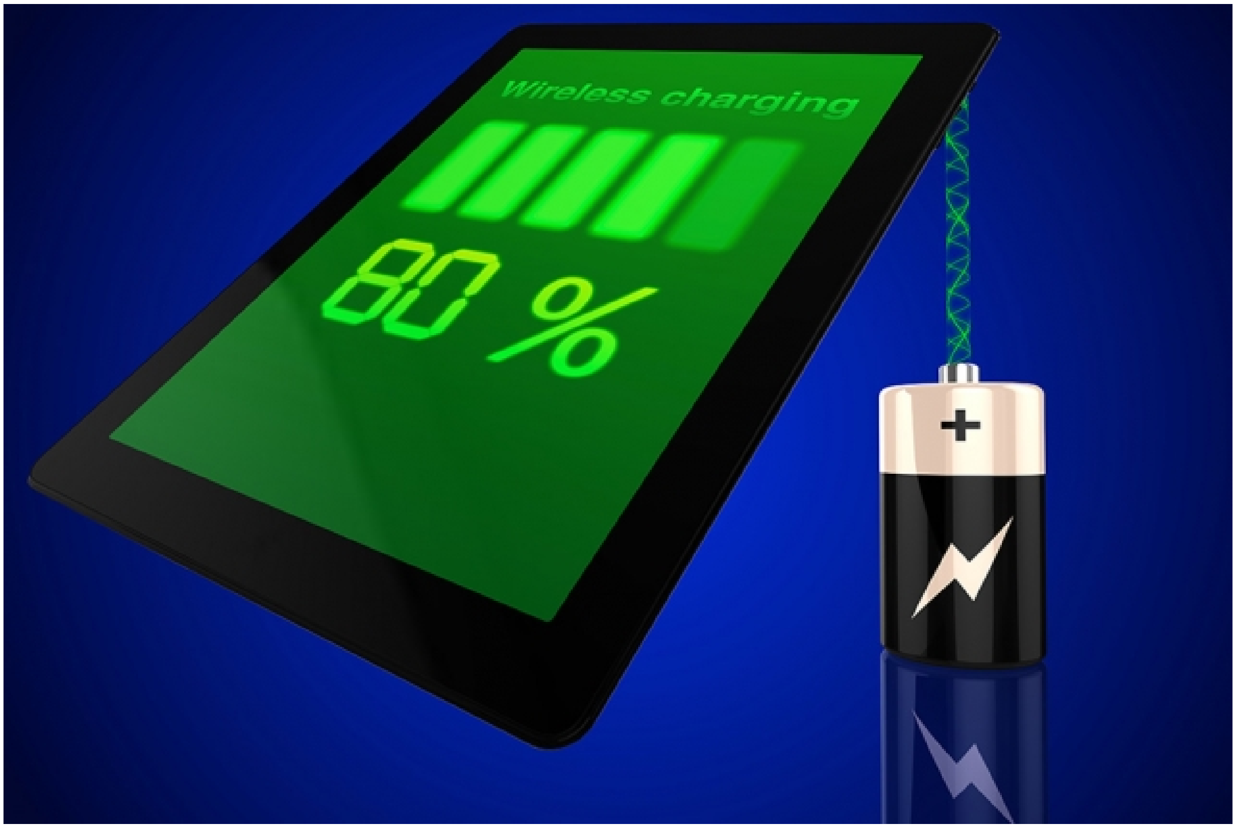
New chip would thwart the counterfeiting that plagues the market for wired device chargers

February 10 2017, by Larry Hardesty



In an effort to get ahead of the problem of counterfeit wireless chargers, MIT researchers have built a chip that blocks attempts to wirelessly charge a device's battery unless the charger first provides cryptographic authentication. Credit: Christine Daniloff/MIT

Counterfeit chargers for portable electronics are a major problem. At the end of 2016, Apple claimed that of 100 Apple-branded charging accessories it bought on Amazon, 90 were counterfeits. Around the same time, Britain's Chartered Trading Standards Institute reported that of 400 counterfeit chargers it bought from a range of online retailers, 397 failed a basic safety test.

In the last few years, portable electronics that can be recharged wirelessly have started coming to market. In an effort to get ahead of the problem of counterfeit wireless chargers—which could cause power surges that fry a device's circuitry—researchers from MIT's Microsystems Technology Laboratories have built a chip that blocks attempts to wirelessly charge a device's battery unless the charger first provides cryptographic authentication.

The same technology also solves another problem with wireless chargers. When two devices share a single charger, if they are different distances from the charger's electrical coil, their charging rates can vary enormously, to the extent that one device might charge fully while the other remains virtually uncharged. In the same way that the researchers' chip can block power transfer from an unauthorized charger, it can slow the power transfer to a device nearer the charging coil, ensuring more equitable charge rates.

"Security is one of the most critical issues in the 'internet of things [IoT],'" says Anantha Chandrakasan, the Vannevar Bush Professor of Electrical Engineering and Computer Science, referring to the popular idea that vehicles, appliances, civil-engineering structures, manufacturing equipment, and even livestock will soon have sensors that report information directly to networked servers. "We will see security functionality embedded into virtually every function and component of an IoT node."

The researchers presented the new chip this week at the International Solid-State Circuits Conference. Chandrakasan is the senior author on the conference paper, and the first author is Nachiket Desai, who was an MIT graduate student in electrical engineering and computer science (EECS) when the work was done. They're joined by Chiraag Juvekar, also an EECS graduate student at MIT, and Shubham Chandak, a graduate student in electrical engineering at Stanford University.

Switched out

In a wireless charging system, both the charger and the target device contain metal coils. An alternating current—an electrical current that changes direction at a regular rate—passing through the charger's coil produces a magnetic field, which induces a current in the device's coil. The rate at which the current in the charger alternates defines a frequency, much like the frequency of a radio transmission. The device's coil must be "tuned" to the transmission frequency in order to receive power.

The MIT researchers' chief innovation is a more compact and efficient circuit for tuning the frequency of the receiving coil. A standard tuning circuit connects the coil to a series of capacitors, electronic components that can store charge. Between each pair of capacitors is a switch, and switching capacitors on and off changes the receiver's frequency.

"Those switches have very severe requirements," Juvekar says. "They either have to block a very large voltage when they're off, or they have to carry a very large current when they're on, or in some cases both. If a switch needs to block a very big voltage, then it's very hard to put that on the chip. So it has to be a discrete component on the [circuit] board, outside the chip. Or if it's on the chip, it requires a specialized [manufacturing] process that might be very expensive."

Instead of a single coil attached to a bank of capacitors, the MIT researchers' design uses a pair of coils attached to one capacitor each—no switches required. "The fact that those switches aren't there anymore is a big advantage," Juvekar says.

Tuned in

In the researchers' chip, one of the coils—the main coil—is much larger than the other—the auxiliary coil. The main coil carries the chief responsibility for charging a device's battery. When a current is flowing through the auxiliary coil, it produces a magnetic field that changes the tuning frequency of the main coil.

In the circuit connected to the auxiliary coil, the resistance—the efficiency with which it conducts electricity—can be continuously varied. When the resistance is low, the auxiliary coil produces a strong magnetic field, which changes the main coil's tuning frequency so drastically that charging is impossible.

When the resistance in the auxiliary coil's circuit is higher, the magnetic field is weaker, and the detuning is less drastic. Some power transfer will still occur, but the charge rate is lower. That permits other, more distant devices to harvest more of the power transmitted by the charger coil.

The chip uses an authentication technique called elliptic curve cryptography, which is a "public-key" cryptographic technique. Using publicly available information, the chip can generate—and verify the response to—a question that only a charger with valid private information can answer. The chip doesn't need to store a secret key of its own.

Elliptic curve cryptography is a well-established technique. But Chandrakasan's group has developed a battery of methods for reducing chips' power consumption, and the researchers found a way to simplify the encryption circuit so that it takes up less space on the chip and consumes less power.

"This paper describes an innovative approach to accurately and securely managing more than one wireless charging load," says Baher Haroun, director of signal-path research at Texas Instruments' Kilby Labs. "The need for security in wireless energy distribution is critical to ensure authorized and efficient use of the energy delivered. This work could have benefits for safety but also for [determining] 'Who is a legitimate user for this delivered energy?'"

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

Citation: New chip would thwart the counterfeiting that plagues the market for wired device chargers (2017, February 10) retrieved 16 April 2024 from https://techxplore.com/news/2017-02-chip-thwart-counterfeiting-plagues-wired.html