IEEE Spectrum

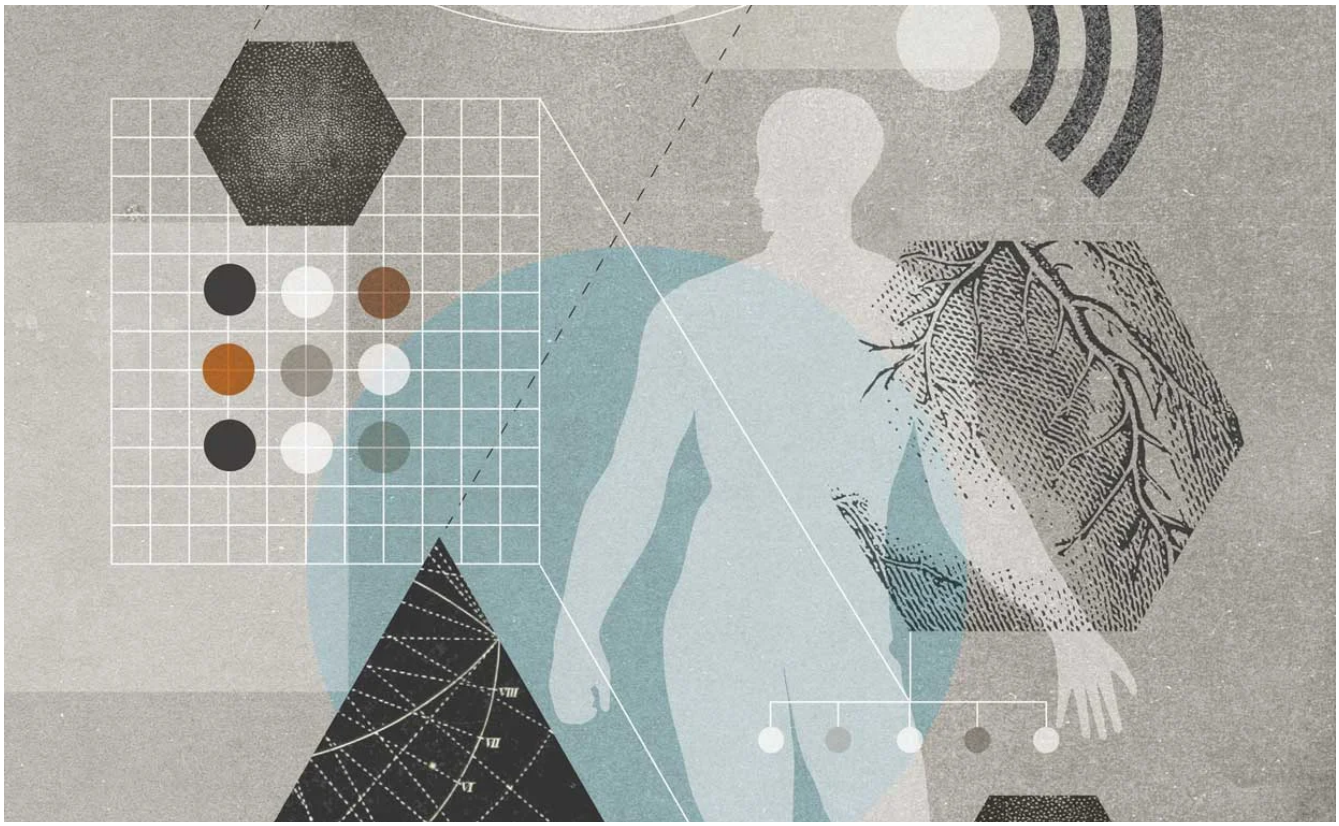
FEATURE BIOMEDICAL

Turning the Body Into a Wire

When the human body is the communications channel, it's hard to hack the data

BY SHREYAS SEN SHOVAN MAITY DEBAYAN DAS

24 NOV 2020



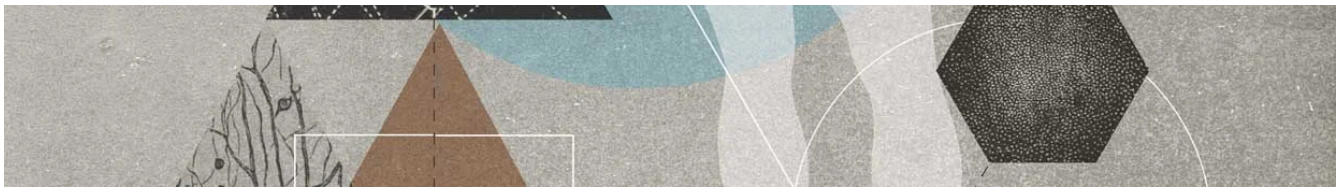


ILLUSTRATION: CHAD HAGEN

IN 2007, U.S. VICE PRESIDENT DICK CHENEY ordered his doctors to disable all wireless signals to and from his Internet-connected pacemaker. Cheney later said that the decision was motivated by his desire to prevent terrorists from being able to hack his pacemaker and use it to lethally shock his heart. Cheney's command to his doctors might seem to some to be overly cautious, but wirelessly connected medical devices have a history of exploitable vulnerabilities. At a series of conferences in 2011 and 2012, for example, New Zealand hacker Barnaby Jack showed that connected medical devices could be remotely attacked. Jack used a high-gain antenna to capture the unencrypted electromagnetic signals transmitted by an insulin pump on a mannequin 90 meters away. He then used those signals to hack into the pump and adjust the level of insulin the pump delivered. He also hacked a pacemaker and made it deliver deadly electric shocks.

Eight years after those demonstrations, connected medical devices remain vulnerable. In June 2020, for example, the U.S. Department of Homeland Security recalled a model of

Department of Homeland Security recalled a model of connected insulin pumps. The pumps were transmitting sensitive information without encryption, making the data accessible to anyone nearby who might want to listen in.

Medical devices are only the tip of the iceberg when it comes to the wireless devices people are putting in or on their bodies. The list includes wireless earbuds, smartwatches, and virtual-reality headsets. Technologies still in development, such as smart contact lenses that display information and digital pills that transmit sensor data after being swallowed, will also be at risk.

All of these devices need to transmit data securely at low power and over a short range. That's why researchers have started to think about them as individual components of a single human-size wireless network, referred to as a body-area network. The term “Internet of Bodies" (IoB) is also coming into use, taking a cue from the Internet of Things.

At the moment, IoB devices use established wireless technologies, mainly Bluetooth, to communicate. While these technologies are low power, well understood, and easy to implement, they were never designed for IoB networks. One of Bluetooth's defining features is the ability for two devices to easily find and connect to one another from meters away. That

feature is precisely what allows a hypothetical attacker to snoop on or attack the devices on someone's body. Wireless technologies have also been designed to travel through air or vacuum, not through the medium of the human body, and therefore they are less efficient than a method of communicating designed to do so from scratch.

Through our research at Purdue University, we have developed a new method of communication that will keep medical devices, wearables, and any other devices on or near the body more secure than they are using low-power wireless signals to communicate with one another. The system capitalizes on the human body's innate ability to conduct tiny, harmless electrical signals to turn the entire body into a wired communication channel. By turning the body into the network, we will make IoB devices more secure.

Sensitive personal data like medical information should always be encrypted when it's transmitted, whether wirelessly or in an email or via some other channel. But there are three other especially good reasons to prevent an attacker from gaining access to medical devices locally.

The first is that medical data should be containable. You don't want a device to be broadcasting information that someone

might eavesdrop on. The second reason is that you don't want the integrity of the device to be compromised. If you have a glucose monitor connected to an insulin pump, for example, you don't want the pump to release more glucose because the monitor's data was compromised. Not enough glucose in the blood can cause headaches, weakness, and dizziness, while too much can lead to vision and nerve problems, kidney disease, and strokes. Either situation can eventually lead to death. The third reason is that the device's information always needs to be available. If an attacker were to jam the signals from an insulin pump or a pacemaker, the device might not even know it needed to respond to a sudden problem in the body.

So if security and privacy are so important, why not use wires? A wire creates a dedicated channel between two devices. Someone can eavesdrop on a wired signal only if they physically tap the wire itself. That's going to be hard to do if the wire in question is on or inside your body.

Setting aside the benefits of security and privacy, there are some important reasons why you wouldn't want wires crisscrossing your body. If a wire isn't properly insulated, the body's own biochemical processes can corrode the metal in the wire, which could in turn cause heavy-metal poisoning. It's

the wire, which could in turn cause heavy-metal poisoning. It's also a matter of convenience. Imagine needing to repair or replace a pacemaker with wires. Rethreading the wires through the body would be a very delicate task.

Rather than choose between wireless signals, which are easy for eavesdroppers to snoop, and wired signals, which bring risk to the body, why not a third option that combines the best of both? That's the inspiration behind our work to use the human body as the communication medium for the devices in someone's body-area network.

Your Body Is a Smart Home

Illustration: Chris Philpot

EOPLE ARE PUTTING MORE AND MORE DEVICES IN AND ON THEIR BODIES. Whether they're medical devices like pacemakers, insulin pumps, and

Pbody-temperature sensors, or consumer tech like wireless earbuds, smartwatches, and fitness trackers, they all have one thing in common. None of them need to send data beyond the range of the human body. Any communications beyond the body can be handled by a central wireless hub.

The network that these devices create is called an Internet of Bodies (IoB) network, borrowing from the Internet of Things concept. IoB networks share some of the same needs as a smart home, for example. A smart home can be filled with wildly different devices—an Amazon Alexa, a smart fridge, and a system that adjusts lights automatically when people enter and exit rooms—that all use Bluetooth or Wi-Fi to communicate. Likewise, consumer tech and medical devices in an IoB network can both use the common medium of the body itself to send signals.

We call the method of sending signals directly through the body electro-quasistatic human-body communication. That's a mouthful, so let's just think of it as a body channel. The important takeaway is that by exploiting the body's own conductive properties, we can avoid the pitfalls of both wired and wireless channels.

Metal wires are great conductors of electric charge. It's a simple matter to transmit data by encoding 1s and 0s as different voltages. You need only define 1s as some voltage, which would cause current to flow through the wire, and 0s as zero voltage, which would mean no current flowing through the wire. By measuring the voltage over time at the other end of the wire, you end up with the original sequence of 1s and 0s. However, given you don't want metal wires running around or through the body, what can you do instead?

The average adult human is about 60 percent water by weight. And though pure water is a terrible electrical conductor, water filled with conductive particles like electrolytes and salts conducts electricity better. Your body is filled with a watery solution called the interstitial fluid that sits underneath your skin and around the cells of your body. The interstitial fluid is responsible for carrying nutrients from the bloodstream to the body's cells, and is filled with proteins, salts, sugars, hormones, neurotransmitters, and all sorts of other molecules that help keep the body going. Because interstitial fluid is everywhere in the body, it allows us to establish a circuit among two or more communicating devices sitting pretty much anywhere on the body.

Imagine someone with diabetes who uses an insulin pump and a separate monitor on the abdomen to manage blood glucose levels. Suppose they want their smartwatch, among its many other functions, to display current glucose levels and the operational status of the pump. Traditionally, these devices would have to be connected wirelessly, which would make it theoretically possible for anyone to grab a copy of the user's personal data. Or worse, potentially attack the pump itself. Today, many medical devices still aren't encrypted, and even for those that are, encryption is not a guarantee of security.

Here's how it would work with a body channel instead. The pump, the monitor, and the smartwatch would each be outfitted with a small copper electrode on its back, in direct contact with the skin. Each device also has a second electrode not in contact with the skin that functions as a sort of floating ground, which is a local electrical ground that is not directly connected with Earth's ground. When the monitor takes a blood glucose measurement, it will need to send that data to both the pump, in case the insulin level needs to be adjusted, and to the smartwatch, so that the individual can see the level. The smartwatch can also store data for long-term monitoring, or encrypt it and send it to the user's computer, or their doctor's computer, for remote storage and analysis.

The monitor communicates its glucose measurements by encoding the data into a series of voltage values. Then, it transmits these values by applying a voltage between its two copper electrodes—the one touching the human body, and the one acting as a floating ground.

This applied voltage very slightly changes the potential of the entire body with respect to Earth's ground. This tiny change in potential between the body and Earth's ground is just a fraction of the potential difference between the monitor's two electrodes. But it's enough to be picked up, as an even smaller

fraction after crossing the body, by the devices elsewhere. Because both the pump on the waist as well as the smartwatch on the wrist are on the body, they can detect this change in potential across their own two electrodes—both on-body and floating. The pump and the smartwatch then convert these potential measurements back into data. All without the actual signal ever traveling beyond the skin.

One of the biggest challenges for realizing this method of body communication is in selecting the best wavelengths for the electrical signals. Electrical wavelengths like the ones we're considering here are much longer than the RF wavelengths for wireless communications.

Photos: John Underwood/Purdue University

TAYING GROUNDED: DAVID YANG [RIGHT], A PH.D. STUDENT OF SHREYAS SEN [left], wears a transmitter on his right wrist. The transmitter sends a code through his body to unlock a computer connected to the receiver in his left hand. On the left is a close up of the wrist wearable and another prototype of the receiver that has been miniaturized into a USB insert.

S

The reason selecting a frequency is a challenge is that there is a range of frequencies at which the human body itself can become an antenna. An ordinary radio antenna creates a signal when an alternating current causes the electrons in its material to oscillate and create electromagnetic waves. The frequency of the transmitted waves depends on the frequency of the alternating current fed into the antenna. Likewise, an alternating current at certain frequencies applied to the human body will cause the body to radiate a signal. This signal, while weak, is still strong enough to be picked up with the right equipment and from some distance away. And if the body is acting as an antenna, it can also pick up unwanted signals from elsewhere that might interfere with wearables' and implants' ability to talk with one another.

For the same reason you don't want to use technologies like Bluetooth, you want to keep electrical signals confined to the body and not accidentally radiating from or to it. So you have to avoid electrical frequencies at which the human body becomes an antenna, which are in the range of 10 to 100 megahertz. Above that are the wireless bands, and we've already mentioned the problems there. The upshot is that you need to use frequencies in the range of 0.1 to 10 MHz, in which signals will stay confined to the body.

Earlier attempts to use the human body to communicate have usually shied away from these lower frequencies because the body is typically high loss at low frequencies. In other words, signals at these lower frequencies require more power to guarantee that a signal will make it to its destination. That means a signal from a glucose monitor on the abdomen might not make it to a smartwatch on the wrist before it's unreadable, without a significant boost in power. These previous efforts were high loss because they focused on sending direct electrical signals, rather than information encoded in potential changes. We've found that the parasitic capacitance between a device and the body is key to creating a working channel.

Capacitance refers to the ability of an object to store electrical charge. Parasitic capacitance is unwanted capacitance that occurs unintentionally between any two objects. For example, two charged areas in close proximity on a circuit board, or between a person's hand and their phone. Typically, parasitic capacitance is a nuisance, although it also enables certain applications like touch screens.

Astute readers may have picked up that we haven't mentioned one key aspect of circuits before now: A circuit needs to be a closed loop for electrical communication to be possible. Up until now, we've restricted our discussion to the forward path, meaning the part of the circuit from the transmitting electrode to the receiving electrode. But we need a path back. We have one thanks to parasitic capacitance between the floating ground electrodes on the devices and Earth's ground.

Here's how to picture the circuit we're using. First, imagine two circuit loops. The first loop begins with the transmitting device, at the electrode touching the skin. The circuit then goes through the body, down through the feet to the actual ground, and then back up through the air to the other (floating) electrode on the transmitting device. We should note here that this is not a loop through which direct current can flow. But because parasitic capacitances exist between any

two objects, such as your feet and your shoes, and your shoes and the ground, a small alternating current can exist.

The second loop, in a similar fashion, begins with the receiving device, at its electrode that is touching the skin. It then goes through the body—both loops share this segment—to the ground, and back through the air to the floating-ground electrode on the receiving device.

The key here is to understand that the circuit loops are important not because we have to push a current through them necessarily, but because we need a closed path of capacitors. In a circuit, if the voltage changes across one capacitor—for example, the two electrodes of the transmitting device—it creates a slight alternating current in the loop. The other capacitors, meaning both the body and the air, “see" this current and, because of their impedances, or resistances to the current, their voltages change as well.

Remember that the circuit loop with the transmitting device and the one with the receiving device share the body as a segment of their respective loops. Because they share that segment, the receiving device also responds to the slight change in the body's voltage. The two electrodes making up the receiving device's capacitor detect the body's changing

voltage and allow that measurement to be decoded as meaningful information.

Body Language

Illustration: Chris Philpot

USING THE BODY AS THE COMMUNICATIONS CHANNEL FOR IOB DEVICES AVOIDS the fundamental problem with radiative technologies like Wi-Fi and Bluetooth by keeping the electrical signals under the skin.

Take an insulin pump that needs to send blood-glucose levels to a smartwatch. The technique creates two circuit loops in the body. The first loop [blue] starts with the pump. Two electrodes, one touching the body, the other floating, create an electric-potential difference between them. The voltage change also slightly modulates the body's potential. This causes a slight

alternating current to flow from the pump, through the air to the ground, and up through the body.

The change in the body's potential causes a similar voltage change between the electrodes of the smartwatch, which also has one touching the body and one floating. This creates a second small alternating current [yellow] to flow in a similar loop. These two closed circuits make it possible to send electrical signals between the devices.

We have found that we want any IoB device's capacitor to have high capacitance. If this is the case, relatively high voltages created by the transmitting device will result in extremely low currents in the body itself. Obviously, this makes sense from a safety perspective: We don't want to run high current through the body, after all. But it also makes the communications channel low loss. That's because a high-impedance capacitor will be particularly sensitive to minor changes in current. The upshot is that we can keep the current low (and safe) and still get clear voltage measurements at the receiving device. We've found that our technique results in a reduction in loss of two orders of magnitude compared with previous attempts to create a wireless channel in the body, which relied on sending an electrical signal via current directly through the body.

Our method for turning the human body into a communications channel shifts the distance at which signals can be intercepted from the 5- to 10-meter range of Bluetooth and similar signals to below 15 centimeters. In other words,

we've reduced the distance over which an attacker can both intercept and interfere with signals by two orders of magnitude. With our method, an attacker would need to be so close to the target that there's no way to hide.

Not only does our method offer more privacy and security for anyone with a medical implant or device, but as a bonus, the communications are far more energy efficient as well. Because we've developed a system that is low loss at low frequencies, we can send information between devices using far less power. Our method requires less than 10 picojoules per transferred bit. For reference, that's about 0.01 percent of the energy required by Bluetooth. Using 256-bit encryption, it drew 415 nanowatts of power to transmit 1 kilobit per second, which is more than three orders of magnitude below Bluetooth (which draws between 1 and 10 milliwatts).

Medical devices like pacemakers and insulin pumps have been around for decades. Bluetooth earbuds and smartwatches may be newer, but neither life-saving medical equipment nor consumer tech is leaving our bodies any time soon. It only makes sense to make both categories of devices as secure as possible. Data is always most vulnerable to a malicious attack when it is moving from one point to another, and our IoB communication technique can finally close the loop on

communication technique can finally close the loop on keeping personal data from leaving your body.

This article appears in the December 2020 print issue as "To Safeguard Sensitive Data, Turn Flesh and Tissue Into a Secure Wireless Channel."

About the Author

Shreyas Sen is an associate professor of electrical and computer engineering at Purdue University. He is a Senior Member of the IEEE. Shovan Maity and Debayan Das are graduate students of Sen at Purdue University.