Novel transmitter uses ultrafast 'frequency hopping' and data encryption to protect signals from being intercepted

June 7 2018, by Rob Matheson

Credit: CC0 Public Domain

Today, more than 8 billion devices are connected around the world, forming an "internet of things" that includes medical devices, wearables,

vehicles, and smart household and city technologies. By 2020, experts estimate that number will rise to more than 20 billion devices, all uploading and sharing data online.

But those devices are vulnerable to hacker attacks that locate, intercept, and overwrite the data, jamming signals and generally wreaking havoc. One method to protect the data is called "frequency hopping," which sends each data packet, containing thousands of individual bits, on a random, unique radio frequency (RF) channel, so hackers can't pin down any given packet. Hopping large packets, however, is just slow enough that hackers can still pull off an attack.

Now MIT researchers have developed a novel transmitter that frequency hops each individual 1 or 0 bit of a data packet, every microsecond, which is fast enough to thwart even the quickest hackers.

The transmitter leverages frequency-agile devices called bulk acoustic wave (BAW) resonators and rapidly switches between a wide range of RF channels, sending information for a data bit with each hop. In addition, the researchers incorporated a channel generator that, each microsecond, selects the random channel to send each bit. On top of that, the researchers developed a wireless protocol—different from the protocol used today—to support the ultrafast frequency hopping.

"With the current existing [transmitter] architecture, you wouldn't be able to hop data bits at that speed with low power," says Rabia Tugce Yazicigil, a postdoc in the Department of Electrical Engineering and Computer Science and first author on a paper describing the transmitter, which is being presented at the IEEE Radio Frequency Integrated Circuits Symposium. "By developing this protocol and radio frequency architecture together, we offer physical-layer security for connectivity of everything." Initially, this could mean securing smart meters that read home utilities, control heating, or monitor the grid.

"More seriously, perhaps, the transmitter could help secure medical devices, such as insulin pumps and pacemakers, that could be attacked if a hacker wants to harm someone," Yazicigil says. "When people start corrupting the messages [of these devices] it starts affecting people's lives."

Co-authors on the paper are Anantha P. Chandrakasan, dean of MIT's School of Engineering and the Vannevar Bush Professor of Electrical Engineering and Computer Science (EECS); former MIT postdoc Phillip Nadeau; former MIT undergraduate student Daniel Richman; EECS graduate student Chiraag Juvekar; and visiting research student Kapil Vaidya.

Ultrafast frequency hopping

One particularly sneaky attack on wireless devices is called selective jamming, where a hacker intercepts and corrupts data packets transmitting from a single device but leaves all other nearby devices unscathed. Such targeted attacks are difficult to identify, as they're often mistaken for poor a wireless link and are difficult to combat with current packet-level frequency-hopping transmitters.

With frequency hopping, a transmitter sends data on various channels, based on a predetermined sequence shared with the receiver. Packet-level frequency hopping sends one data packet at a time, on a single 1-megahertz channel, across a range of 80 channels. A packet takes around 612 microseconds for BLE-type transmitters to send on that channel. But attackers can locate the channel during the first 1 microsecond and then jam the packet.

"Because the packet stays in the channel for long time, and the attacker only needs a microsecond to identify the frequency, the attacker has enough time to overwrite the data in the remainder of packet," Yazicigil

says.

To build their ultrafast frequency-hopping method, the researchers first replaced a crystal oscillator—which vibrates to create an electrical signal—with an oscillator based on a BAW resonator. However, the BAW resonators only cover about 4 to 5 megahertz of frequency channels, falling far short of the 80-megahertz range available in the 2.4-gigahertz band designated for wireless communication. Continuing recent work on BAW resonators—in a 2017 paper co-authored by Chandrakasan, Nadeau, and Yazicigil—the researchers incorporated components that divide an input frequency into multiple frequencies. An additional mixer component combines the divided frequencies with the BAW's radio frequencies to create a host of new radio frequencies that can span about 80 channels.

Randomizing everything

The next step was randomizing how the data is sent. In traditional modulation schemes, when a transmitter sends data on a channel, that channel will display an offset—a slight deviation in frequency. With BLE modulations, that offset is always a fixed 250 kilohertz for a 1 bit and a fixed -250 kilohertz for a 0 bit. A receiver simply notes the channel's 250-kilohertz or -250-kilohertz offset as each bit is sent and decodes the corresponding bits.

But that means, if hackers can pinpoint the carrier frequency, they too have access to that information. If hackers can see a 250-kilohertz offset on, say, channel 14, they'll know that's an incoming 1 and begin messing with the rest of the data packet.

To combat that, the researchers employed a system that each microsecond generates a pair of separate channels across the 80-channel spectrum. Based on a preshared secret key with the transmitter, the

receiver does some calculations to designate one channel to carry a 1 bit and the other to carry a 0 bit. But the channel carrying the desired bit will always display more energy. The receiver then compares the energy in those two channels, notes which one has a higher energy, and decodes for the bit sent on that channel.

For example, by using the preshared key, the receiver will calculate that 1 will be sent on channel 14 and a 0 will be sent on channel 31 for one hop. But the transmitter only wants the receiver to decode a 1. The transmitter will send a 1 on channel 14, and send nothing on channel 31. The receiver sees channel 14 has a higher energy and, knowing that's a 1-bit channel, decodes a 1. In the next microsecond, the transmitter selects two more random channels for the next bit and repeats the process.

Because the channel selection is quick and random, and there is no fixed frequency offset, a hacker can never tell which bit is going to which channel. "For an attacker, that means they can't do any better than random guessing, making selective jamming infeasible," Yazicigil says.

As a final innovation, the researchers integrated two transmitter paths into a time-interleaved architecture. This allows the inactive transmitter to receive the selected next channel, while the active transmitter sends data on the current channel. Then, the workload alternates. Doing so ensures a 1-microsecond frequency-hop rate and, in turn, preserves the 1-megabyte-per-second data rate similar to BLE-type transmitters.

Provided by Massachusetts Institute of Technology