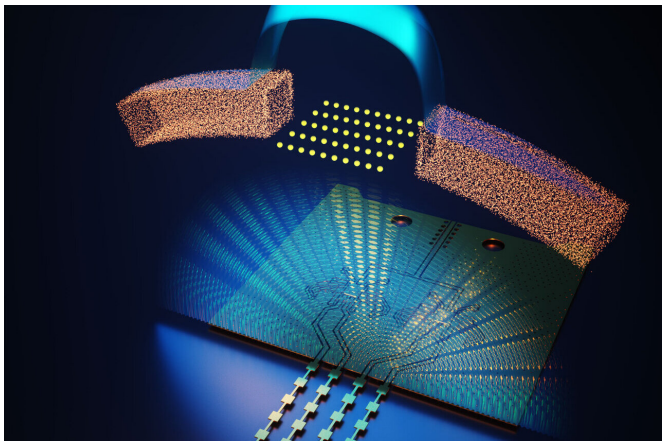
New chip hides wireless messages in plain sight

23 November 2021



Princeton researchers have developed a method to foil eavesdroppers by building security into the physical nature of wireless transmissions. The signal is clear for the intended recipient but noise for others. Credit: Ella Maru Studio/Princeton University

Emerging 5G wireless systems are designed to support high-bandwidth and low-latency networks connecting everything from autonomous robots to self-driving cars. But these large and complex communication networks could also pose new security concerns.

Encryption methods now used to secure communications from eavesdroppers can be challenging to scale towards such high-speed and ultra-low latency systems for 5G and beyond. This is because the very nature of encryption requires exchange of information between sender and receiver to encrypt and decrypt a message. This exchange makes the link vulnerable to attacks; it also requires computing that increases latency. Latency, the amount of time between sending instructions on a network and the arrival of the data, is a key measure for tasks like autonomous driving and industrial automation. For networks that support latency-critical systems such as self-driving cars, robots and other cyber-physical systems, minimizing time-to-action is critical.

Seeking to close this security gap, Princeton University researchers have developed a methodology that incorporates security in the physical nature of the signal. In a report published Nov. 22 in *Nature Electronics*, the researchers describe how they developed a new millimeter-wave wireless microchip that allows secure wireless transmissions to prevent interception without reducing latency, efficiency and speed of the 5G network. According to senior researcher Kaushik Sengupta, the technique should make it very challenging to eavesdrop on such high-frequency wireless transmissions, even with multiple colluding bad actors.

"We are in a new era of wireless—the networks of the future are going to be increasingly complex while serving a large set of different applications that demand very different features," Sengupta said. "Think low-power smart sensors in your home or in an industry, high-bandwidth augmented reality or virtual reality, and self-driving cars. To serve this and serve this well, we need to think about security holistically and at every level."

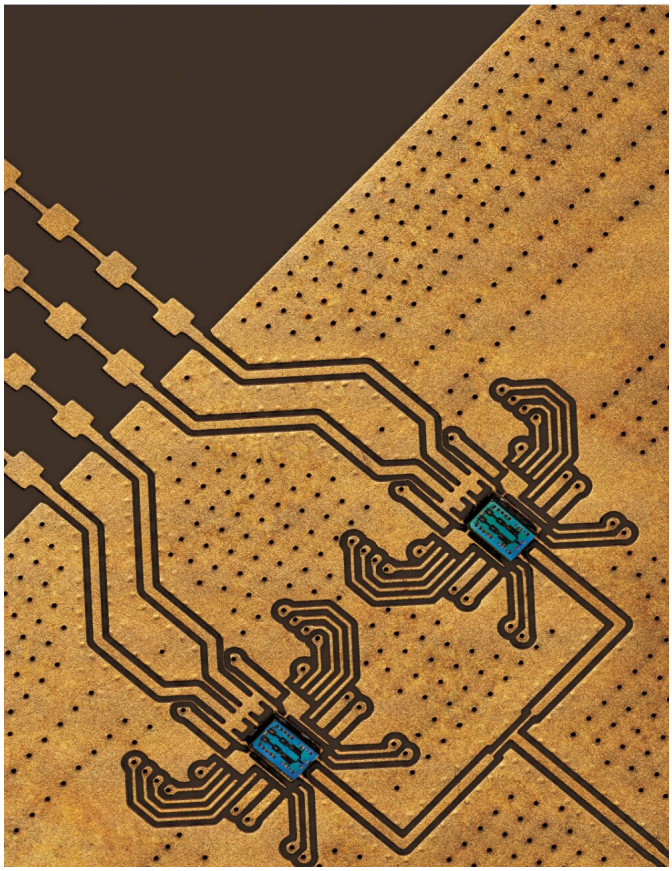
Instead of relying on encryption, the Princeton method shapes the transmission itself to foil would-be eavesdroppers. To explain this, it helps to picture wireless transmissions as they emerge from an array of antennas. With a single antenna, radio waves radiate from the antenna in a wave. When there are multiple antennas working as an array, these waves interfere with each other like waves of water in a pond. The interference increases the size of some wave crests and troughs and smooths out others.

An array of antennas is able to use this interference to direct a transmission along a defined path. But besides the main transmission, there are secondary paths. These secondary paths are weaker than the

main transmission, but in a typical system they contain the exact same signal as the main path. By tapping these paths, potential eavesdroppers can compromise the transmission.

Sengupta's team realized they could foil eavesdroppers by making the signal at the eavesdroppers' location appear almost as noise. They do this by chopping up the message randomly and assigning different parts of the message to subsets of antennas in the array. The researchers were able to coordinate the transmission so that only a receiver in the intended direction would be able to assemble the signal in the correct order. Everywhere else, the chopped up signals arrive in a manner that appear noise-like.

Sengupta compared the technique to chopping up a piece of music in a concert hall.



The researchers created the system in a chip that can be manufactured in a standard chip foundry. Credit: Princeton University

"Imagine in a concert hall, while playing Beethoven's symphony no.9, every instrument, instead of playing all the notes of the piece, decides to play randomly selected notes. They play these notes at correct times, and remain silent between them, such that each note in the original piece gets played by at least some instrument. As the sound waves carrying these notes from all the instruments travel through the hall, at a certain location, they can be made to arrive precisely in the correct fashion. The listener sitting there would enjoy the original piece as if nothing has changed. Everyone else would hear a cacophony of missing notes arriving at random times, almost like noise. This is, in principle, the secret sauce behind the transmission security —enabled by precise spatial and temporal modulation of these high-frequency electromagnetic fields."

If an eavesdropper tried to intercept the message by interfering with the main transmission, it would cause problems in the transmission and be detectable by the intended user. Although it is theoretically possible that multiple eavesdroppers could work together to collect the noise-like signals and attempt to reassemble them into a coherent transmission, Sengupta said the number of receivers needed to do that would be "extraordinarily large."

"We showed for the first time that it is possible to stitch several noise-like signatures into the original signal by colluding eavesdroppers applying AI, but it is very challenging. And we also showed techniques how the transmitter can fool them. It is a cat-and-mouse game."

Edward Knightly, a professor at Rice University who was not involved in the research, said Sengupta's work was "an important milestone" for securing future networks.

"He experimentally showed, for the first time, how to overcome even a sophisticated adversary employing machine learning data collected from multiple, synchronized observation points," he said.

The team created the entire end-to-end system in a silicon chip that is manufactured by standard silicon foundry processing.

Sengupta said it also would be possible to use encryption along with the new system for additional security. "You can still encrypt on top of it but you can reduce the burden on encryption with an additional layer of security," he said. "It is a complimentary approach."

"Secure space–time-modulated millimeter-wave wireless links that are resilient to distributed eavesdropper attacks" was published on Nov. 22 in *Nature Electronics*.

In addition to Sengupta, authors include Suresh Venkatesh, post-doctoral scholar and Xuyang Lu, graduate student of Princeton University and Bingjun Tang, a visiting researcher at Princeton University.

More information: Suresh Venkatesh et al, Secure space–time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks, *Nature Electronics* (2021). DOI: 10.1038/s41928-021-00664-z

Provided by Princeton University