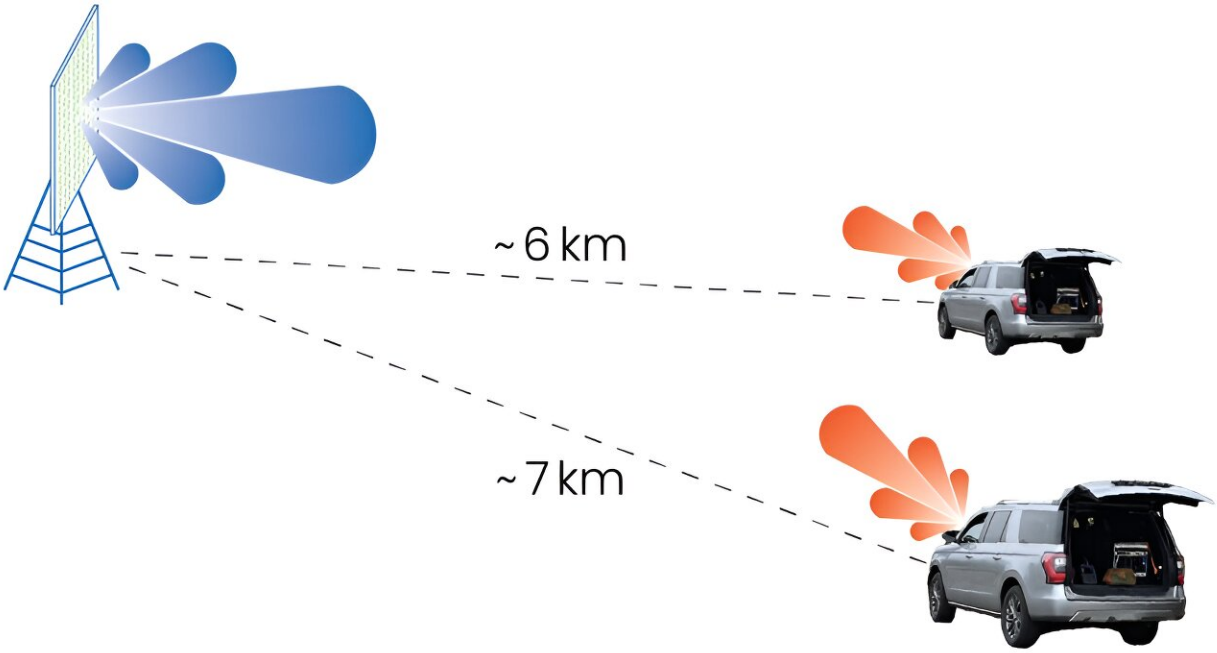
# Field campaign assesses vulnerabilities of 5G networks

August 8 2023, by Ariana Tantillo



The team deployed two trucks containing sensor systems to perform 5G signal geolocation based on angle-of-arrival estimates. Credit: Massachusetts Institute of Technology

Fifth-generation, or 5G, mobile network technology is all the hype these days. Compared to 4G, this newest way of connecting wireless devices to cellular networks is designed to provide higher data rates, ultralow latency, improved reliability, expanded configurability, increased network capacity and availability, and connectivity among a larger number of users.

The U.S. Department of Defense (DoD) would like to leverage these commercial advances in their communications systems, but 5G, like its predecessors, lacks sufficiently robust security features. For military applications, wireless connectivity leaves communications vulnerable to unwanted detection (identifying the presence of signals), unwarranted geolocation (determining the origin of signals), and purposeful jamming (hindering the transmission and reception of signals). Before the DoD can fully harness 5G technology, networking vulnerabilities must be identified, quantified, and mitigated.

"For commercial communications, you may worry about interference a bit, but you don't worry about anybody intentionally seeking to find you and disrupt your communications, as is the case in the military," explains Nicholas Smith, a researcher in the Tactical Networks Group, part of the Communication Systems R&D area at MIT Lincoln Laboratory. "The military also has to contend with more challenging mobility scenarios beyond people walking or driving around, such as airplanes traveling at Mach speeds."

Smith is part of a Lincoln Laboratory team assessing the vulnerabilities of 5G and developing potential solutions to make this latest-generation technology resilient enough for military use.

## Mountains of data

In April 2022, the Lincoln Laboratory 5G vulnerability assessment team headed to Hill Air Force Base (AFB) near Salt Lake City, Utah, to conduct an over-the-air test campaign at the newly opened 5G network test bed designed and installed by Nokia Corporation. The team is among the first to leverage this test bed at Hill AFB, which is one of five DoD FutureG and 5G Office test beds at U.S. military installations serving as locations for evaluating the capabilities and functionality of 5G networks. Though 5G vulnerabilities had previously been modeled, this testing campaign represented one of the first red-teaming campaigns against 5G in the field.

Over two weeks, the team deployed GPS-equipped antenna arrays connected to software-defined radios to collect network signals, which were then analyzed by a standalone computer server. Each day, the team drove three trucks, each containing one of these sensor systems, to different sites on base and asked the Hill AFB liaisons to tune certain network parameters—for example, to turn certain base stations on or off, increase or decrease the power of the base stations, or adjust the beam-steering directions. With each adjustment, the team collected data to determine how difficult it was to detect, geolocate, and jam 5G signals. The mountainous terrain enabled the team to obtain results from different elevations.

Before heading out to the field, the team performed modeling and simulation to prepare for their experimental setup, considering factors such as how far away from a 5G base station signals can be detected, where to place the sensors for the lowest geolocation error, and what the best sensor geometry is. They also verified the algorithms used for detection and geolocation.

On site at Hill AFB, the team consistently detected 5G signals through several types of detection algorithms, from general energy detectors (which measure the energy, or power, of a received signal) to more-specific matched-filter detectors (which compare the energy of an unknown received signal to the energy of a known signal). They detected signals up to the horizon (to around 20 kilometers out and verified further distances through simulation)—a very far range, particularly for a specific type of signal called the signal synchronization block (SSB). The SSB is detectable by design; mobile devices need to detect the SSB in order to synchronize to a wireless network's time and frequency and ultimately access the network. However, this detectability means the SSB poses a considerable vulnerability.

"Detection facilitates jamming," Smith says. "Once adversaries detect a signal, they can jam it. Because the SSB is periodic in time and frequency, it is quite easy to detect and then jam."

To geolocate the signals, the team performed angle-of-arrival estimation using the MUSIC (for MUltiple SIgnal Classification) algorithm, which estimates the direction of arrival of signals received by an antenna array. As Smith explained, if you have two sensors spaced out on opposite sides of the map and know the angle that the signal is coming from for both sensors, you can draw straight lines that will intersect; where they intersect is the geolocation point.

"One of our objectives was to see how inexpensive or easy it would be to detect, geolocate, and jam 5G signals," Smith explains. "Our results show that you don't need to be highly sophisticated; commercially available off-the-shelf, low-cost hardware setups and open-source algorithms are effective."

This 5G vulnerability assessment is an extension of previous 4G vulnerability assessments conducted by the laboratory.

## Generational advances

New generations of wireless communications technology typically appear once per decade. Focusing on voice, the first generation, 1G, paved the way for the first mobile telephones in the 1980s. The second generation, 2G, enabled more secure voice transmission with less static and introduced short message services (SMS), or text messaging.

With the debut of 3G in the early 2000s came the core network speeds needed to launch the first smartphones, bringing internet to our phones to support mobile applications such as maps and video calling. And 4G, providing even higher data-transfer rates, enabled high-definition video streaming, enhanced voice call quality (through long-term evolution, or LTE, technology), and internet-of-things devices such as smartwatches and digital home assistants.

The rollout of 5G, which began in earnest in 2019 and continues to evolve, comes with orders-of-magnitude improvements in several areas, including speed, latency, connectivity, and flexibility. For example, 4G theoretically tops out at 1 gigabit per second for data speed, while 5G tops out at 20 gigabits per second—a rate 20 times faster. In addition to operating at low-band frequencies (below 6 GHz), 5G can operate at less-crowded millimeter-wave frequencies (above 24 GHz). The abundant spectrum available at these higher frequencies enables extreme capacity, ultrahigh throughput, and ultralow latency.

However, because high-frequency signals experience scattering as they travel through the atmosphere, their range is limited. To address this limitation, researchers are introducing concepts to complement the currently large cellphone towers (macrocells), which are located miles apart, with smaller towers (microcells, picocells, or femtocells) spaced closer together, particularly in high-density urban areas. With these small cells, the high frequencies don't have to travel as far and can provide high data rates to lots of users.

Massive multiple-input, multiple-output (MIMO) antenna arrays provide another means to serve concurrent users. Providing a large number of antennas at 5G base stations means wireless signals can be tightly focused in targeted directions toward a desired receiving device such as a cellphone, laptop, or autonomous car, instead of spreading in all directions. Called beamforming, this focusing technique helps users get more precise, reliable wireless connections with faster data transfer and prevents the data from going to unintended recipients.

"5G presents an opportunity for communications to be much more based on beamforming and massive MIMO," Smith says. "With these technologies, 5G has the potential to be less detectable and geolocatable and more anti-jam than all of the previous generations. But we need to be informed on how to configure the network to do that, because 5G is not inherently secure."

## Improved resilience

Over the past year, the team has been applying the insights from their field-testing campaign to enhance the resiliency of standard 5G components and processes.

"Our goal is to make the resiliency enhancements as simple and cost-effective as possible for the DoD to implement, leveraging existing 5G technology and not having to modify 5G hardware, at least on the cellphone side," Smith says.

Going forward, Smith is excited to design more complex algorithms, especially ones that use machine learning to detect and geolocate 5G signals. He also expressed the team's interest in potentially using 5G for drone swarms, which, according to Smith, are "one of the hardest problems as far as communications go" because of factors like movement complexity and power limitations.

If the 10-year technology cycle keeps up, 6G will likely launch around 2030. New capabilities may include applying artificial intelligence to manage network resources; extending frequencies to even higher (terahertz) ranges; and integrating communications across land, air, sea, and space into a cohesive ecosystem.

"Our current program is actually called 5G-to-nG [next generation]," says Smith. "We're already looking ahead to 6G and the vulnerabilities it may bring for the DoD."

*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: Field campaign assesses vulnerabilities of 5G networks (2023, August 8) retrieved 6 May 2024 from https://techxplore.com/news/2023-08-field-campaign-vulnerabilities-5g-networks.html