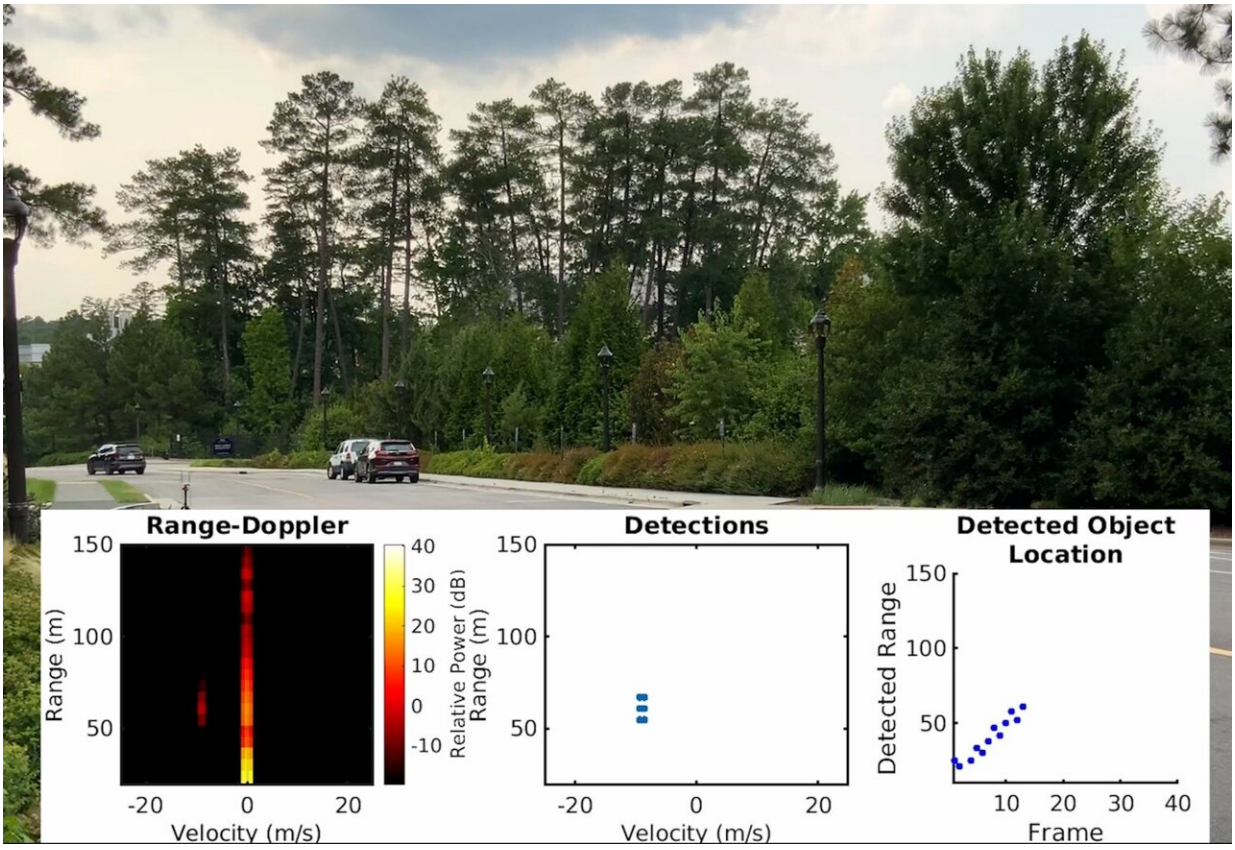
Engineers develop hack to make automotive radar hallucinate

January 31 2024



Credit: Duke University

A black sedan cruises silently down a quiet suburban road, driver humming Christmas carols quietly while the car's autopilot handles the driving. Suddenly, red flashing lights and audible warnings blare to life,

snapping the driver from their peaceful reprieve. They look at the dashboard screen and see the outline of a car speeding toward them for a head-on collision, yet the headlights reveal nothing ahead through the windshield.

Despite the incongruity, the car's autopilot grabs control and swerves into a ditch. Exasperated, the driver looks around the vicinity, finding no other vehicles as the incoming danger disappears from the screen. Moments later, the real threat emerges—a group of hijackers jogging toward the immobilized vehicle.

This scene seems destined to become a common plot point in Hollywood films for decades to come. But due to the complexities of modern automotive detection systems, it remains firmly in the realm of science fiction. At least for the moment.

Engineers at Duke University, led by Miroslav Pajic, the Dickinson Family Associate Professor of Electrical and Computer Engineering, and Tingjun Chen, assistant professor of electrical and computer engineering, have now demonstrated a system they've dubbed "MadRadar" for fooling automotive radar sensors into believing almost anything is possible.

The technology can hide the approach of an existing car, create a phantom car where none exists or even trick the radar into thinking a real car has quickly deviated from its actual course. And it can achieve this feat in the blink of an eye without having any prior knowledge about the specific settings of the victim's radar, making it the most troublesome threat to radar security to date.

The researchers say MadRadar shows that manufacturers should immediately begin taking steps to better safeguard their products.

The research, currently available on the *arXiv* preprint server, will be published in 2024 Network and Distributed System Security Symposium , taking place February 26–March 1 in San Diego, California.

"Without knowing much about the targeted car's radar system, we can make a fake vehicle appear out of nowhere or make an actual vehicle disappear in real-world experiments," Pajic said. "We're not building these systems to hurt anyone, we're demonstrating the existing problems with current radar systems to show that we need to fundamentally change how we design them."

In modern cars that feature assistive and autonomous driving systems, radar is typically used to detect moving vehicles in front of and around the vehicle. It also helps to augment visual and laser-based systems to detect vehicles moving in front of or behind the car.

Because there are now so many different cars using radar on a typical highway, it is unlikely that any two vehicles will have the exact same operating parameters, even if they share a make and model. For example, they might use slightly different operating frequencies or take measurements at slightly different intervals. Because of this, previous demonstrations of radar-spoofing systems have needed to know the specific parameters being used.

"Think of it like trying to stop someone from listening to the radio," explained Pajic. "To block the signal or to hijack it with your own broadcast, you'd need to know what station they were listening to first."

In the MadRadar demonstration, the team from Duke showed off the capabilities of a radar-spoofing system they've built that can accurately detect a car's radar parameters in less than a quarter of a second. Once they've been discovered, the system can send out its own radar signals to fool the target's radar.

In one demonstration, MadRadar sends signals to the target car to make it perceive another car where none actually exist. This involves modifying the signal's characteristics based on time and velocity in such a way that it mimics what a real contact would look like.

In a second and much more complicated example, it fools the target's radar into thinking the opposite—that there is no passing car when one actually does exist. It achieves this by delicately adding masking signals around the car's true location to create a sort of bright spot that confuses the radar system.

"You have to be judicious about adding signals to the radar system, because if you simply flooded the entire field of vision, it'd immediately know something was wrong," said David Hunt, a Ph.D. student working in Pajic's lab.

In a third kind of attack, the researchers mix the two approaches to make it seem as though an existing car has suddenly changed course. The researchers recommend that carmakers try randomizing a radar system's operating parameters over time and adding safeguards to the processing algorithms to spot similar attacks.

"Imagine adaptive cruise control, which uses radar, believing that the car in front of me was speeding up, causing your own car to speed up, when in reality it wasn't changing speed at all," said Pajic. "If this were done at night, by the time your car's cameras figured it out you'd be in trouble."

Each of these attack demonstrations, the researchers emphasize, were done on real-world radar systems in actual cars moving at roadway speeds. It's an impressive feat, given that if the spoofing radar signals are even a microsecond off the mark, the fake datapoint would be misplaced by the length of a football field.

"These lessons go far beyond radar systems in cars as well," Pajic said. "If you want to build drones that can explore dark environments, like in search and rescue or reconnaissance operations, that don't cost thousands of dollars, radar is the way to go."

More information: David Hunt et al, MadRadar: A Black-Box Physical Layer Attack Framework on mmWave Automotive FMCW Radars, *arXiv* (2023). DOI: 10.48550/arxiv.2311.16024

Provided by Duke University