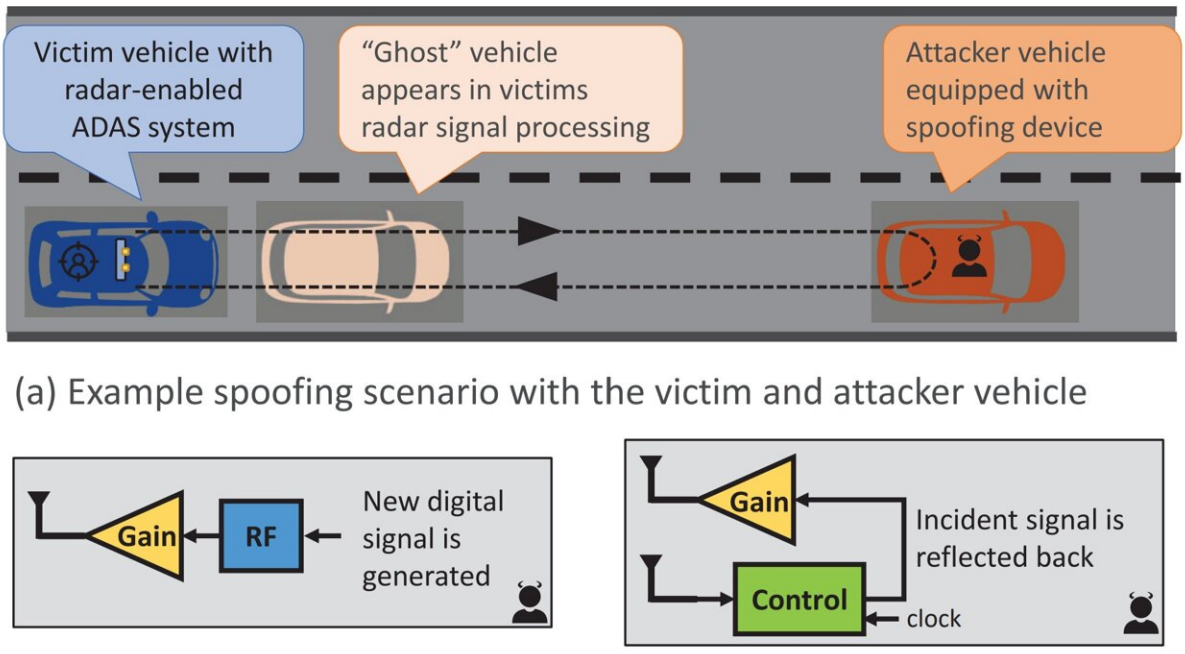
Team develops new 'attacker' device to improve autonomous car safety

May 24 2023



mmSpoof spoofing technique is based on a mmWave reflect array, and it does not require prior knowledge about victim radar, to spoof arbitrary distance and velocity values. Credit: *mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array* (2023)

Modern cars and autonomous vehicles use millimeter wave (mmWave)

radio frequencies to enable self-driving or assisted driving features that ensure the safety of passengers and pedestrians. This connectivity, however, can also expose them to potential cyberattacks.

To help improve the safety and security of autonomous vehicles, researchers from the lab of Dinesh Bharadia, an affiliate of the UC San Diego Qualcomm Institute (QI) and faculty member in the university's Jacobs School of Engineering Department of Electrical and Computer Engineering, and colleagues from Northeastern University devised a novel algorithm designed to mimic an attacking device.

The algorithm, described in the paper "mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array," lets researchers identify areas for improvement in autonomous vehicle security.

"The invention of autonomous systems, like self-driving cars, was to enable the safety of humanity and prevent loss of life," said Bharadia. "Such autonomous systems use sensors and sensing to deliver autonomy. Therefore, safety and security rely on achieving high-fidelity sensing information from sensors. Our team exposed a radar sensor vulnerability and developed a solution that autonomous cars should strongly consider."

Defending against cyberattacks

Autonomous cars detect obstacles and other potential hazards by sending out radio waves and recording their reflections as they bounce off surrounding objects. By measuring the time it takes for the signal to return, as well as changes in its frequency, the car can detect the distance and speed of other vehicles on the road.

Like any wireless system, however, autonomous cars run the risk of cyberattacks. Attackers driving ahead of an autonomous unit can engage

in "spoofing," an activity that involves interfering with the vehicle's return signal to trick it into registering an obstacle in its path. The vehicle may then brake suddenly, increasing the risk of an accident.

To address this potential chink in autonomous cars' armor, Vennam and colleagues devised a novel algorithm designed to mimic a spoofing attack. Previous attempts to develop an attacking device to test cars' resistance have had limited feasibility, either assuming the attacker can synchronize with the victim's radar signal to launch an assault, or assuming both cars are physically connected by a cable.

In its new paper, presented by Vennam at the IEEE Symposium on Security and Privacy in San Francisco on May 22, the team describe a new technique that uses the victim vehicle's radar against itself. By subtly changing the received signal's parameters at "lightspeed" before reflecting it back, an attacker can disguise their sabotage and make it much harder for the vehicle to filter malicious behavior. All of this can be done "on the go" and in real-time without knowing anything about the victim's radar.

"Automotive vehicles heavily rely on mmWave radars to enable real-time situational awareness and advanced features to promote safe driving," said Vennam. "Securing these radars is of paramount importance. We—mmSpoof—uncovered a serious security issue with mmWave radars and demonstrated a robust attack. What's alarming is that anyone can build the prototype using off-the-shelf hardware components."

To counter this type of attack, Vennam suggests, researchers seeking to improve the safety of autonomous vehicles can use a high-resolution radar capable of capturing multiple reflections from a car to accurately identify the true reflection. Researchers might also create backup options for radar by incorporating cameras and "light detecting and

ranging" (LiDAR), which records the time it takes for a laser pulse to hit an object and return to measure its surroundings, into their defense.

Alternately, the team presents mmSpoof as a means of preventing dangerous tailgating. By placing an mmSpoof device on the back of their car, drivers can trick a tailgating car into registering a decelerating car in front of them and activating the brakes.

More information: Conference: www.ieee-security.org/TC/SP2023/

Paper: www.computer.org/csdl/proceedi … 3600b971/1Js0EwtonDy

Provided by University of California - San Diego