Protecting connected, self-driving vehicles from hackers

August 21 2024, by Patricia DeLacey

This Lincoln MKZ is an open connected and automated vehicle for academic and industry testing at Mcity, a world-class proving ground for advanced mobility vehicles operated by University of Michigan's Mobility Transformation Center. Credit: Joseph Xu, Michigan Engineering

Emerging self-driving vehicle networks that collaborate and

communicate with each other or infrastructure to make decisions are vulnerable to data fabrication attacks, according to a University of Michigan-led study that also outlines preventive measures for fleet operators.

The researchers presented the work recently at the 33rd USENIX Security Symposium in Philadelphia. The paper is published on the *arXiv* preprint server.

Although this network of collaboration and communication known as vehicle-to-everything or V2X is not yet out on the roads, many countries support the development of the technology and have begun small-scale testing. The U.S. Department of Transportation recently released a V2X deployment plan to guide implementation of the technology as it progresses.

"Collaborative perception allows connected and autonomous vehicles to 'see' more than they could on their own by leveraging the collective sensing power and data insights of a network of vehicles, but this power comes with serious security risks," said Z. Morley Mao, a professor of computer science and engineering at U-M and senior author of the study.

Sharing information among vehicles creates an opportunity for hackers to introduce fake objects or remove real objects from perception data, which could lead vehicles to brake hard or crash.

"Understanding and countering attacks is a key step forward in not only advancing connected and autonomous vehicle security but also protecting passengers and other drivers," said Qingzhao Zhang, a doctoral student in computer science and engineering at U-M and lead author of the study.

While prior studies focused on individual sensor security or simpler

collaboration models, this study introduced sophisticated, real-time attacks tested both in rigorous virtual simulations and real-world scenarios at U-M's Mcity Test Facility, a proving ground for connected and automated vehicles and technologies.

To understand security vulnerabilities, the researchers administered falsified LiDAR-based 3D sensor data that appears realistic to the system but contains malicious modifications via physical access to the hardware and software system. They used zero-delay attack scheduling, a high-risk cyber attack that uses precise timing to introduce malicious data without lag or delay.

In virtual simulated scenarios, the attacks were highly effective with success rates at 86%. On-road attacks on three vehicles in the Mcity environment triggered collisions and hard brakes.

The countermeasure system, called Collaborative Anomaly Detection, leverages shared occupancy maps—2D representations of the environment—to cross-check data, allowing vehicles to quickly detect the geometric inconsistencies of abnormal data.

The system achieved a detection rate of 91.5% with a false positive rate of 3% in virtual simulated environments and reduced safety hazards in the Mcity scenarios.

The findings provide a robust framework not only for improving connected and autonomous vehicle safety, but for detecting and countering data fabrication attacks in collaborative perception systems used in transportation, logistics, smart city initiatives or defense.

"By providing comprehensive benchmark datasets and open-sourcing our methodology, our study sets a new standard for research in this domain, fostering further development and innovation in autonomous vehicle

safety and security," said Mao.

More information: Qingzhao Zhang et al, On Data Fabrication in Collaborative Vehicular Perception: Attacks and Countermeasures, *arXiv* (2023). DOI: 10.48550/arxiv.2309.12955

Provided by University of Michigan College of Engineering