

TraCR ADVANCES

FALL 2026



Director's Message

I am excited to share our latest milestones and upcoming initiatives at the National Center for Transportation Cybersecurity and Resiliency (TraCR). Our mission to strengthen the cybersecurity and resiliency of transportation systems continues to advance our work across research, education, strategic partnerships, and technology transfer.

As we progress, we are placing a stronger emphasis on technology transfer, ensuring that innovations developed through TraCR research move beyond the laboratory and into real-world transportation systems. A key highlight of this phase is our ongoing work to accelerate the deployment of practical cybersecurity solutions that enhance the safety and resilience of modern transportation infrastructure. Furthermore, our research teams continue to produce impactful studies ranging from leveraging Post-Quantum Cryptographic solutions to developing vision-language model-based frameworks for GNSS spoofing detection.

In addition to research focused on multimodal transportation systems, TraCR continues to invest heavily in workforce development and education. Addressing the transportation cybersecurity skills gap requires a coordinated system that connects specialized education, agency-level staffing and governance. We remain committed to expanding hands-on training, applied learning, and stronger education-to-employment pathways that inspire students to pursue careers supporting the future of secure and resilient transportation systems.

Looking ahead, we are excited to host the UTC National Transportation Cybersecurity Summit, which will be held in Fall 2026. This major event will bring together leading researchers, government agencies, industry experts, and transportation professionals to discuss emerging cyber threats, innovative defense strategies, and the future of secure multimodal transportation systems. We look forward to the continued impact of our research, education, technology transfer, and outreach efforts in the years ahead.



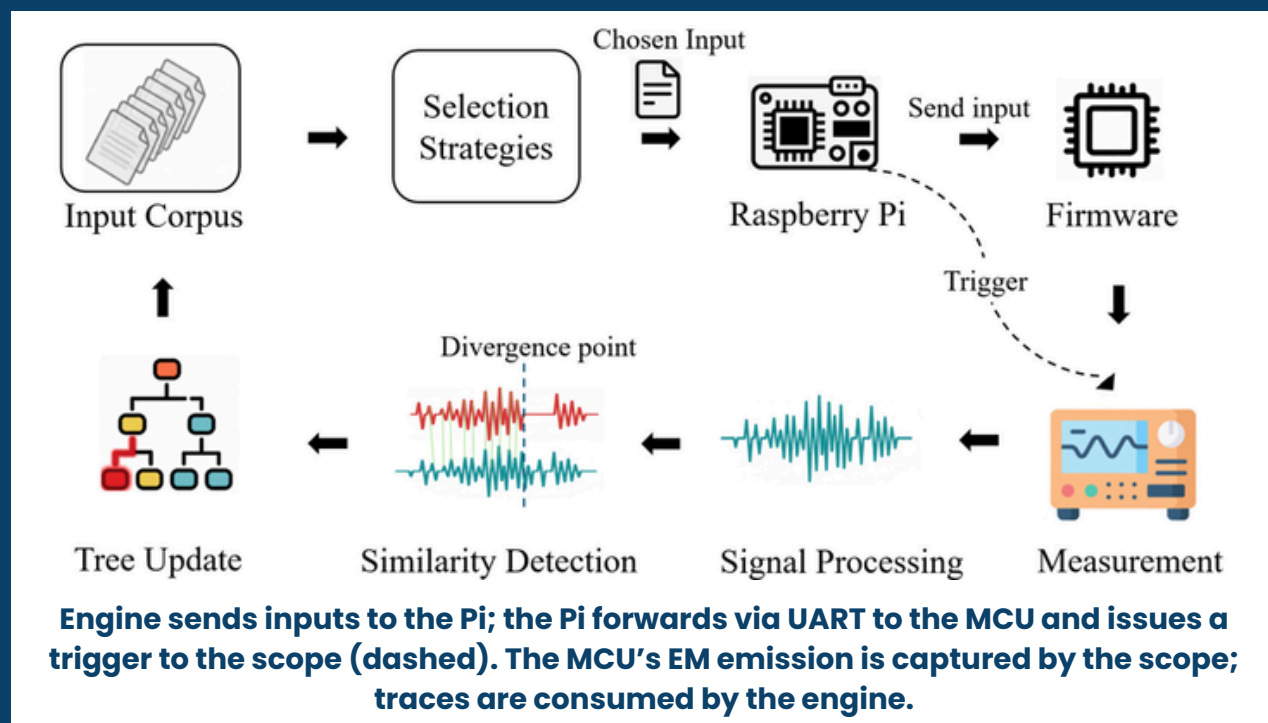
Dr. Mashrur "Ronnie" Chowdhury

In this Issue:

Director's Message
Research Spotlight
Webinars
News
Achievements

Fuzz'EMup: Leveraging EM Side-Channel Emanation to Guide Black-Box Embedded Firmware Fuzzing

Fatemeh Moradihaghighi, Zihao Zhan, Yanan Guo, Ziming Zhao, Mashrur Chowdhury, and Zhenkai Zhang



Securing firmware on modern transportation systems has become critical. Fuzzing is an automated software-testing technique that uncovers vulnerabilities by repeatedly executing a program with malformed or unexpected inputs. Its effectiveness improves significantly when code-coverage feedback is available, as this allows the fuzzer to identify and prioritize inputs that explore new program behavior. However, effective coverage-guided fuzzing typically requires access to the firmware binary, software instrumentation, or an accurate emulator. These options are often unavailable for protected or proprietary embedded devices, leaving security testers reliant on less efficient black-box fuzzing.

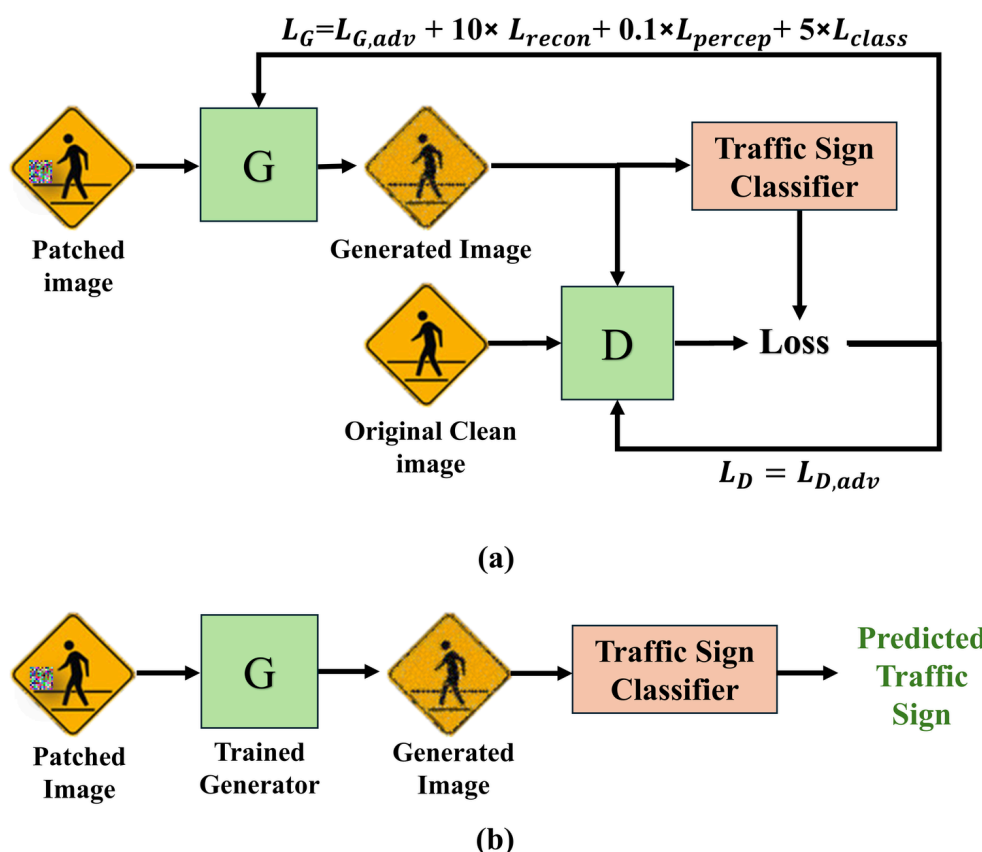
This work addresses such limitations by using electromagnetic (EM) side-channel emanations as an external source of feedback. Digital computation naturally produces EM signals that can be captured non-invasively using a probe positioned near the device's microcontroller. Because these signals vary as the firmware executes different instructions and control-flow paths, they can reveal information about internal program behavior without requiring access to the firmware itself. We demonstrate that EM side-channel signals can provide practical guidance for testing protected embedded devices. The approach enables more effective firmware fuzzing without requiring binary extraction, instrumentation, debug access, or an accurate emulator.

[Click here to view the full paper](#)

Generative Adversarial Network (GAN)-Based Single-Stage Defense for Traffic Sign Classification Under Adversarial Patch

Abyad Enan and Mashrur Chowdhury

Autonomous vehicles rely heavily on computer vision to recognize traffic signs and make safe driving decisions. However, these perception systems are vulnerable to adversarial patch attacks, in which a carefully designed patch placed on a traffic sign can deceive a deep learning classifier, leading to potentially dangerous misclassification. To address this cybersecurity threat, this research develops a Generative Adversarial Network (GAN)-based single-stage defense strategy that directly reconstructs a patch-free traffic sign image from an adversarially patched input. Unlike conventional defense approaches that first detect or localize the adversarial patch and then mask or remove it, the method developed in this study performs the defense in a single forward pass through the generator, without requiring explicit patch detection, localization, or masking.



GAN-based single-stage defense pipelines, (a) Training, and (b) Inference, developed in this study

The GAN model is trained using a combination of adversarial, reconstruction, perceptual, and classification losses to remove patch effects while preserving the structural and semantic features required for accurate traffic sign classification. Importantly, the generator is trained using randomly generated patches rather than the adversarial patches used during testing, allowing the defense to remain effective against unseen patch designs, different patch sizes, and multiple traffic sign classes.

Experimental results demonstrate substantial improvements in classification performance. Adversarial patch attacks reduced overall traffic sign classification accuracy to approximately 39%, whereas incorporating the defense restored accuracy to 93%. The method also introduced very little computational overhead, with an average end-to-end classification latency of approximately 5 ms compared with approximately 1.46 seconds for the multi-stage defense strategy from the literature. Additional evaluation on the MNIST benchmark further demonstrated the approach's scalability across a larger number of image classes. Together, these findings demonstrate the potential of the single-stage defense developed in this study to support cyber-resilient, real-time perception systems for autonomous vehicles.

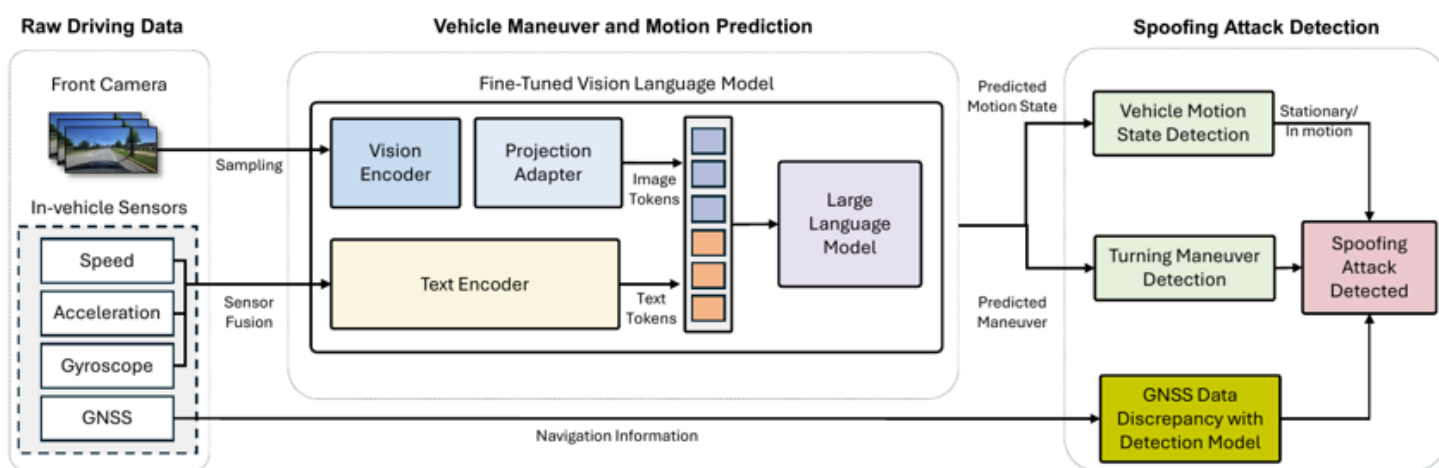
[Click here to view the full paper](#)

Vision-Language Model-Based GNSS Spoofing Detection for Autonomous Vehicle Navigation

Mohammed Aldeen, Muhammad Sami Irfan, Sagar Dasgupta, Long Cheng, Mizanur Rahman, and Mashrur Chowdhury

Autonomous vehicles rely on Global Navigation Satellite System (GNSS) signals to know where they are and where to go next. Those signals can be faked. In a spoofing attack, an adversary broadcasts counterfeit satellite signals that send a vehicle into a wrong turn, or make it believe it is stopped while it is still moving. Current defenses check whether GNSS agrees with another position estimate, so an attacker who keeps the fake route on real roads can slip past them.

This project developed the first Vision-Language Model (VLM) based framework for GNSS spoofing detection. Instead of comparing positions, it compares behavior. The VLM reads front camera frames together with vehicle speed, longitudinal acceleration, and yaw rate, then reports what the vehicle is actually doing: going straight, turning left, turning right, or stopped. In parallel, a GNSS pipeline reports what the satellite data claims the vehicle is doing. When the two answers disagree, the system flags a spoofing attack.



System overview of the VLM-based spoofing detection framework

The model was trained on public driving data from Tokyo, Japan, then tested on new data collected with an instrumented vehicle on public roads in Tuscaloosa, Alabama. Three attacks were generated on that data: wrong turn, overshoot, and stop. Maneuver recognition accuracy rose from 23 to 32 percent before fine tuning to 95 percent after. The framework caught every wrong turn and stop attack, and 88 to 93 percent of overshoot attacks, while calling the VLM on only 14 percent of time windows to keep computation low.



This work adds a practical on-road layer of defense that runs alongside existing signal level checks. Ongoing work is compressing the model for automotive grade hardware and testing it against live radio frequency spoofing signals.

Spotlight

Recorded WEBINARS

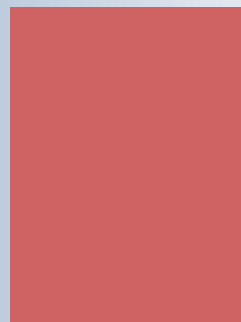
As part of our workforce development/training activities, TraCR hosts monthly webinars from transportation experts. The recordings of all webinars are available on our YouTube channel



INVESTIGATING DRIVER BEHAVIOR UNDER CYBER- ATTACKS IN A CONNECTED VEHICLE ENVIRONMENT

Dr. Mansha Swami

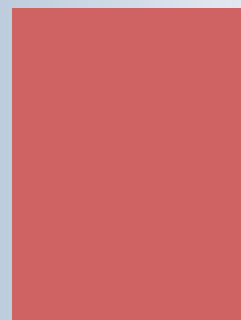
Research Engineer, The National Transportation Center
Morgan State University



ENHANCING AUTONOMOUS VEHICLE TESTING UNDER DYNAMIC WEATHER CONDITIONS

Dr. Balaji Iyengar

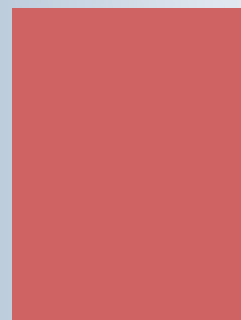
Associate Professor, Computer Science
Benedict College



MEDA: MEASUREMENT-EFFICIENT DISORDER- AWARE MAJORANA ZERO MODE DETECTION AND ITS APPLICATIONS TO THE TRANSPORTATION INDUSTRY

Nathan Jones

School of Computing's Scalable Computing Lab
Clemson University

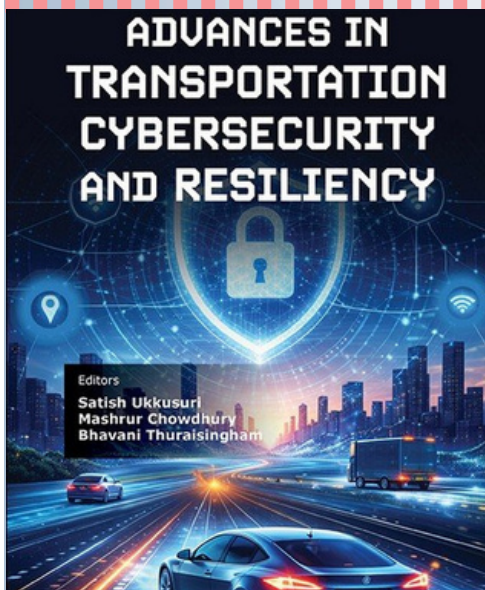


ROBOT OPERATING SYSTEM (ROS)-BASED REAL-TIME MIXED-CRITICALITY SYSTEMS IN AUTONOMOUS TRANSPORTATION

Dr. Abdullah Arafat

Assistant Professor
Florida International University

Watch the recordings here and keep an eye out for future ones!



New Book "Advances in Transportation Cybersecurity and Resiliency" Now Available

After 18 months of hard work, TraCR leadership is pleased to announce the release of *Advances in Transportation Cybersecurity and Resiliency*, edited by Dr. Satish Ukkusuri, Dr. Mashrur Chowdhury, and Dr. Bhavani Thuraisingham and published by World Scientific. The volume offers a comprehensive roadmap for securing connected and autonomous transportation against the vulnerabilities introduced by rapidly expanding vehicle and infrastructure networks, covering state-of-the-art attack modeling, AI/ML-enabled detection, and mitigation techniques validated on both simulated and real-world testbeds. Drawing on

contributions from leading researchers across academia, industry, and government, the book provides professionals and public agencies with actionable strategies for building trustworthy, zero-trust mobility ecosystems, and serves as a graduate-level textbook for courses in Cyber-Physical Systems Security and Intelligent Transportation Systems. Congratulations to the editors and all contributing authors on this milestone and thank you to everyone across the TraCR consortium who helped make it happen!

USDOT Assistant Secretary Visits UC Santa Cruz, Meets with TraCR-Affiliated Researchers

University of California, Santa Cruz (UCSC) recently welcomed Seval Oz, Assistant Secretary for Research and Technology at the U.S. Department of Transportation, for a visit highlighting UCSC's research on secure and trustworthy embodied AI for transportation. Oz met with UCSC Chancellor Cynthia Larive and campus leadership and heard directly from Baskin Engineering faculty, including TraCR Associate Director Alvaro Cardenas, Daniel Fremont and Leilani Gilpin, about their work to secure embodied AI and to test and validate autonomous transportation systems. "This kind of engagement strengthens partnerships and ensures our work directly supports the department's mission to advance U.S. transportation security and competitiveness," Dr. Cardenas said about the visit. The visit reflects the broader TraCR partnership: UCSC's participation in these national conversations grew directly out of the consortium led by Clemson and Dr. Mashrur Chowdhury, bringing complementary expertise from across member institutions to the table.



Dr. Chowdhury Honored with National Award for Transportation Education and Research

Congratulations to Dr. Mashrur "Ronnie" Chowdhury, Director of TraCR, on receiving the American Road & Transportation Builders Association's (ARTBA) S.S. Steinberg Award. The honor recognizes individuals who have made remarkable contributions to transportation education. His research has helped advance ideas in intelligent transportation systems, cybersecurity, and connected mobility from early concepts to real, deployed systems. He's also mentored more than 60 graduate students and postdocs, along with hundreds of undergraduate, high school, and middle school students, shaping not just the technology but the next generation of people who'll build on it.



Dr. Cardenas Receives Test of Time Award at The 2026 ACM Asia Conference on Computer and Communications Security



Congratulations to Dr. Alvaro Cardenas, TraCR Associate Director at UC Santa Cruz, on receiving the Test of Time Award at the 2026 ACM Asia Conference on Computer and Communications Security (AsiaCCS). The award recognizes his paper, "Attacks against process control systems: risk assessment, detection, and response," which helped establish that securing critical infrastructure, such as power plants, factories, and other physical systems, requires defenses informed by the physical processes being controlled, not just traditional network security. It's a well-deserved recognition of research whose influence continues to shape the field today.

TraCR Purdue Ph.D. Ruichen Tan Student Wins Best Paper Award at ECCV Workshop

Congratulations to Ruichen Tan, a Ph.D. student advised by Dr. Satish Ukkusuri at Purdue University, a TraCR partner institution, on receiving the Best Paper Award at the ECCV Workshop on Safe and Defensive Autonomous Driving. The paper, "Worst-Case Hidden-Vehicle Trajectory Search in Spatiotemporal Occlusion Regions," tackles a core challenge in autonomous driving: how a vehicle should reason about traffic participants it can't see, such as pedestrians or cars hidden behind buildings, parked vehicles, or other obstructions. The team's method, HC-MTS, uses a vehicle's observation history to rule out implausible hidden threats, then searches for the worst-case hidden trajectory the vehicle should still be prepared to handle. ECCV is a top-tier computer vision conference, and recognition at one of its workshops reflects the strength of the Purdue team's contributions to TraCR's mission of building safer, more resilient transportation systems.

TraCR Awarded Patent at the Intersection of AI, Security, and Resilience

Congratulations to Dr. Hadi Amini and his group at Florida International University, a TraCR partner institution, on being granted U.S. Patent No. 12,688,476, "Systems and Methods for Advancing the Restoration Process for Interdependent Critical Infrastructures." This is the group's third patent in this space, and it tackles a real operational challenge: when a disaster knocks out power, water, and other interdependent infrastructure at once, the operators of each system must coordinate restoration decisions without necessarily sharing sensitive operational details with one another. The team's approach combines reinforcement learning and optimization to enable operators to coordinate their restoration schedules while preserving their autonomy and limiting unnecessary information sharing, with the goal of deploying recovery crews more efficiently, avoiding conflicting decisions, and restoring essential services faster after a disruption.

That's It for Now!

Stay tuned for our next newsletter in the Spring of 2027.
In the meantime, please follow us on our social media pages, including X, LinkedIn, and YouTube.



Mashrur "Ronnie" Chowdhury, Ph.D., P.E., F. ASCE

Director, National Center for Transportation Cybersecurity and Resiliency (TraCR)
mac@clemson.edu | 864-656-3313 | 216 Lowry Hall, Clemson University | Clemson, SC 29634