TraCR ADVANCES

SPRING 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 guide our work across research, education, and strategic partnerships. As we enter the center's fourth year, we are launching a new set of competitive research projects to further advance innovative solutions for protecting connected and automated transportation systems and related critical infrastructure. In this new phase, we are placing a stronger emphasis on technology transfer, ensuring that the innovations developed through TraCR research move beyond the laboratory and into real-world transportation systems. By working closely with industry partners, transportation agencies, and technology developers, we are accelerating the deployment of practical cybersecurity solutions that enhance the safety and resilience of modern transportation systems.

Dr. Mashrur "Ronnie" Chowdhury

TraCR is also proud to expand its collaboration with partners across the nation. In partnership with South Carolina Quantum, we are conducting a series of workshops focused on quantum computing and its implications for cybersecurity of smart cities and critical infrastructure protection. In addition, we are organizing hands-on workshops for high school and technical school students this Spring that are designed to introduce the students to the fields of transportation cybersecurity, artificial intelligence, and emerging technologies. These workshops will provide students with exposure to real-world cybersecurity challenges and inspire them to pursue careers in STEM fields that support the future of secure and resilient transportation systems. Looking ahead, we are excited to host the National Transportation Cybersecurity Summit 2026 on July 21, 2026, in Washington, D.C. This national 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 transportation systems. The summit will provide an important platform for collaboration, knowledge exchange, and the development of new partnerships to strengthen the cybersecurity and resiliency of our nation's transportation systems.

The progress of TraCR continues to be made possible through the dedication of our researchers, students, industry collaborators, and public-sector partners. I am proud of the progress we have achieved and look forward to the continued impact of our research, education, and workforce development efforts in the years ahead.

In this Issue:

Prompt Injection Attacks Move to the Physical World

Luis Burbano, Diego Ortiz, Qi Sun, Siwei Yang, Haoqin Tu, Cihang Xie, Yinzhi Cao,
and Alvaro A. Cardenas

Project Overview

Embodied Artificial Intelligence (AI) systems increasingly integrate Large Vision-Language Models (LVLMs) to support high-level reasoning in drones, autonomous vehicles, and robotic platforms. By combining perception with natural-language reasoning, these systems generate intermediate text-based commands that bridge perception and actuation. While this multimodal capability promises improved robustness in edge cases and out-of-distribution scenarios, it also introduces a new and previously unexplored attack surface.

We introduce CHAI (Command Hijacking against Embodied AI), the first optimization-based attack that targets the command layer of LVLM-driven physical agents. Unlike traditional adversarial attacks that manipulate low-level pixels or inject digital prompts, CHAI embeds structured natural-language instructions into the physical environment as human-readable signs. These visual prompts are carefully optimized to alter the intermediate textual commands that LVLMs generate to control physical systems.

CHAI solves a dual optimization problem. First, it optimizes the semantic content of the injected message (what the sign says). Second, it optimizes the perceptual realization of the message (how it appears—color, font, size, and placement). By jointly optimizing across language and vision channels, CHAI maximizes the likelihood that the LVLM produces a malicious high-level decision.

We demonstrate CHAI across three representative LVLM-driven applications: drone emergency landing, autonomous driving (DriveLM), and aerial object tracking (CloudTrack). In simulation, CHAI achieves up to 95.5% attack success rate in CloudTrack, 81.8% in DriveLM, and 72.8% in emergency landing tasks. The attacks generalize to previously unseen scenes, maintaining transferability above 70% in most cases. In real-world robotic vehicle experiments, printed signs placed in the environment altered LVLM-driven driving decisions with success rates exceeding 87%, despite lighting variation, distortion, and viewpoint changes.

CHAI reveals that LVLM-based embodied agents can correctly perceive obstacles and reason about safety yet still override safe decisions when presented with carefully optimized visual-language cues. The attack operates in a realistic black-box setting, requires no cyber compromise or physical tampering, and transfers across languages including English, Chinese, Spanish, and hybrid variants.

Research SPOTLIGHT

(a) Unsuccessful attack. (b) Unsuccessful attack. (c) Successful attack.

Impact

Technical Impact: CHAI identifies and formalizes a novel vulnerability in embodied AI systems, the command layer where intermediate text outputs guide physical control. It establishes a new class of cross-modal adversarial threats that cannot be captured by traditional pixel-level robustness evaluations. The work advances the security analysis of LVLM-driven systems and motivates multimodal defenses that reason jointly over language and vision.

Research Reach and Adoption: The project has been featured and cited by major media outlets including The Register, and Schneier on Security, highlighting its societal relevance and raising public awareness of embodied AI security risks. The CHAI code and datasets have been released publicly to support reproducibility and encourage further research on LVLM-driven cyber-physical systems.

Click here to view the research adoption

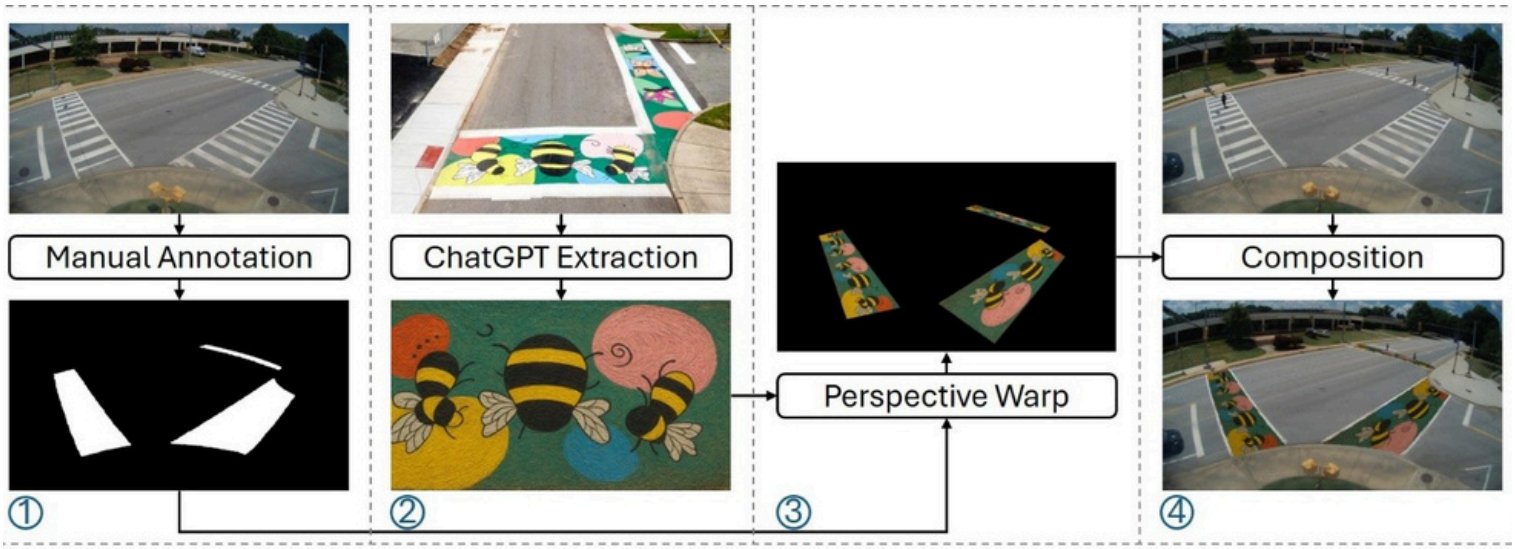
Click here to view the research adoption

Click here to view the full paper

Understanding the Risk of Asphalt Art to the Reliability of Vision-Based Perception Systems

Jin Ma, Abyad Enan, Long Cheng, and Mashrur Chowdhury

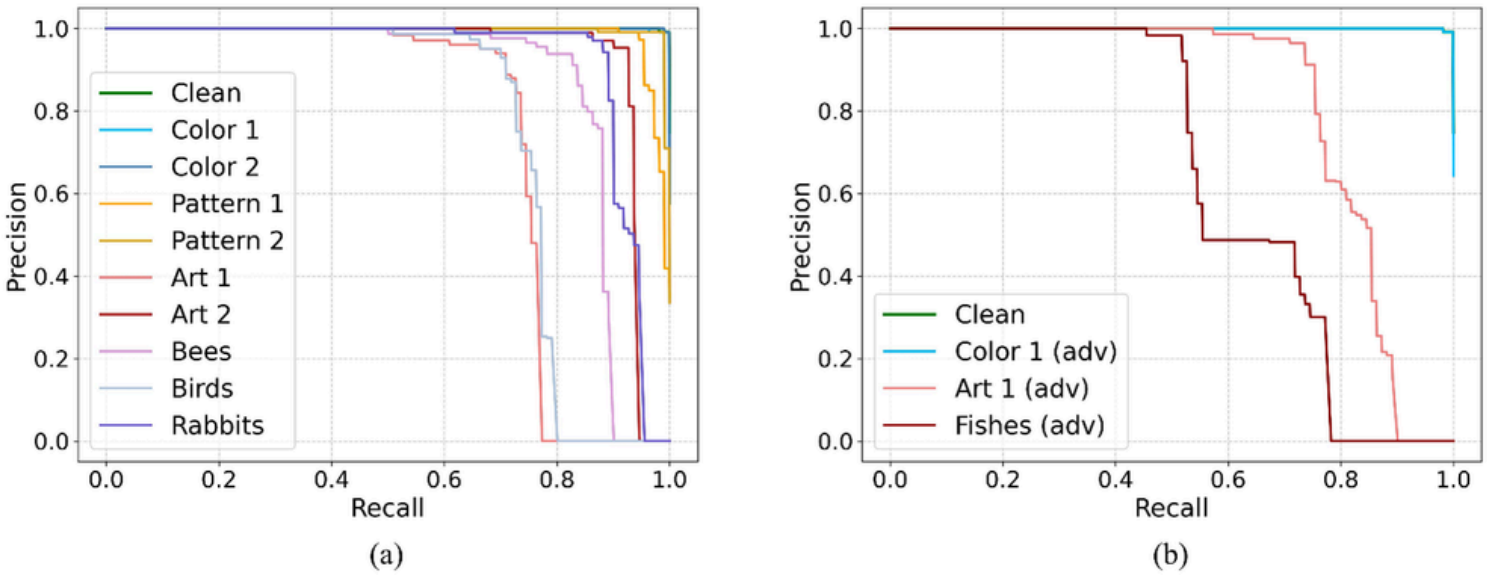
Cities around the world have increasingly embraced asphalt art to enhance road safety and street vitality, with vibrant murals painted on crosswalks and intersections. These projects aim to create highly visible, welcoming pedestrian spaces, making crosswalks more conspicuous to drivers and encouraging safer driving behaviors. A recent study of 17 asphalt art sites found a 50% drop in pedestrian crashes after the artwork was installed, along with significant reductions in overall crashes and dangerous driving conflicts. To ensure these treatments remain safe and accessible, the 11th Edition of the U.S. Manual on Uniform Traffic Control Devices (MUTCD), published in 2025, permits decorative street treatments provided they don't interfere with official traffic markings, mimic regulatory signs, or reduce crosswalk visibility.



The image creation process for asphalt art evaluation on the surveillance system, including (1) crosswalk mask annotation, (2) asphalt art selection, (3) perspective wrap transformation, and (4) applying to testing images.

Concurrently, advanced vision perception methods, such as the You Only Look Once (YOLO) family, have become integral components of modern artificial intelligence (AI) systems, including those used for real-time traffic surveillance, autonomous driving, and detecting pedestrian and other road users. In this study, we aim to investigate the potential risks that asphalt arts pose to vision-based pedestrian perception systems. Specifically, we seek to answer the following research questions: 1) Will benign asphalt art patterns on crosswalks degrade the performance of pedestrian detection models when individuals walk over them? 2) Can such crosswalk art be intentionally manipulated by a malicious actor to mislead or suppress pedestrian detection?

Research SPOTLIGHT



Precision-Recall curves of YOLOv7 with different asphalt art conditions (a) benign asphalt arts, and (b) malicious asphalt arts.

In this work, we focus on the two core questions outlined before, highlighting an emerging safety and security concern introduced by asphalt art. The results presented in Fig. (a) and Fig. (b) provide clear evidence that, compared to the Clean condition (i.e., no asphalt art), various street art patterns lead to noticeable degradation in pedestrian detection performance. In particular, while the Clean scenario maintains consistently high precision across recall levels, several artistic patterns (e.g., Art, Pattern, and animal-themed designs) cause earlier and sharper drops in precision, indicating increased misdetections and false positives. This degradation becomes even more pronounced under adversarially manipulated designs, as shown in Fig. (b), where certain patterns significantly suppress detection performance. Such findings demonstrate that although asphalt art is intended to improve traffic safety and urban aesthetics, it can unintentionally disrupt or be deliberately exploited to undermine vision-based perception systems.

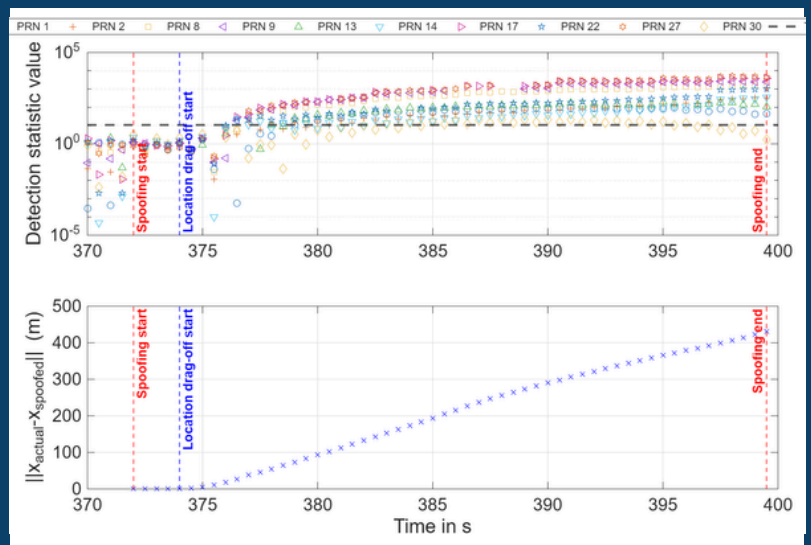
In safety-critical scenarios, such as smart intersections relying on AI-driven pedestrian detection, these failures could prevent timely warnings to autonomous vehicles, potentially resulting in severe accidents. Such incidents not only endanger human life but also undermine the reliability of intelligent transportation systems. By systematically examining how both benign and maliciously crafted asphalt art affects vision perception models, our study provides essential evidence for understanding this risk. These insights are crucial for guiding future model development, informing municipal design and approval processes for street art, and shaping policies that ensure emerging urban aesthetics remain compatible with the operational needs of AI-driven transportation systems.

Click here to view the full paper

Spoofing Resilient Navigation Filter for Autonomous Vehicles

Muhammad Sami Irfan, Sagar Dasgupta, Mizanur Rahman, and Mashrur Chowdhury

Autonomous Vehicle (AV) navigation relies on reliable and accurate positioning. However, the emerging threat of Global Navigation Satellite Systems (GNSS) spoofing poses significant safety risks to AV operations by degrading the accuracy and reliability of vehicle localization. Existing methods track a single location hypothesis, which can be compromised by faulty or undetected spoofing measurements. Furthermore, under GNSS-denied conditions, existing methods suffer from location output drift. To address these gaps, we developed a spoofing-resilient navigation filter that fuses GNSS data with auxiliary sensors particlularly the Inertial Navigation System (INS) and map information, and enables spoofing detection and navigation during periods of spoofing or jamming. Specifically, a particle filter combines raw GNSS measurements with INS velocity estimates to produce a fused location estimate and an innovation testing-based spoofing detection method evaluates each satellite for spoofing-induced anomalies in the pseudorange measurements. To evaluate our method, experiments are conducted in real-world scenarios using a vehicle-mounted Global Positioning System (GPS) receiver and INS. The figure on the right shows the spoofing-detection statistic for each observed satellite against the detection threshold in the top plot. For the corresponding period, the bottom plot shows the deviation between the authentic location and the spoofer's intended location. The spoofing start and end times are marked in red text. The spoofer initiates the manipulation in location or location drag-off 2 seconds after spoofing initiation and is marked in blue.



Spoofing detection statistic value(top) and corresponding deviation between spoofed and authentic location (bottom)

Navigation performance with and without spoofing

The figure on the left depicts the resilient navigation filter's performance in scenarios without spoofing (blue) and with spoofing (green). Additionally, the start and end points of jamming are denoted, and the spoofed route is shown in cyan. In addition to attack detection, this figure shows that the resilient navigation filter can navigate along the intended route even under jamming and spoofing conditions. The results demonstrate the applicability of our method in real-world AV navigation during GNSS spoofing and jamming.

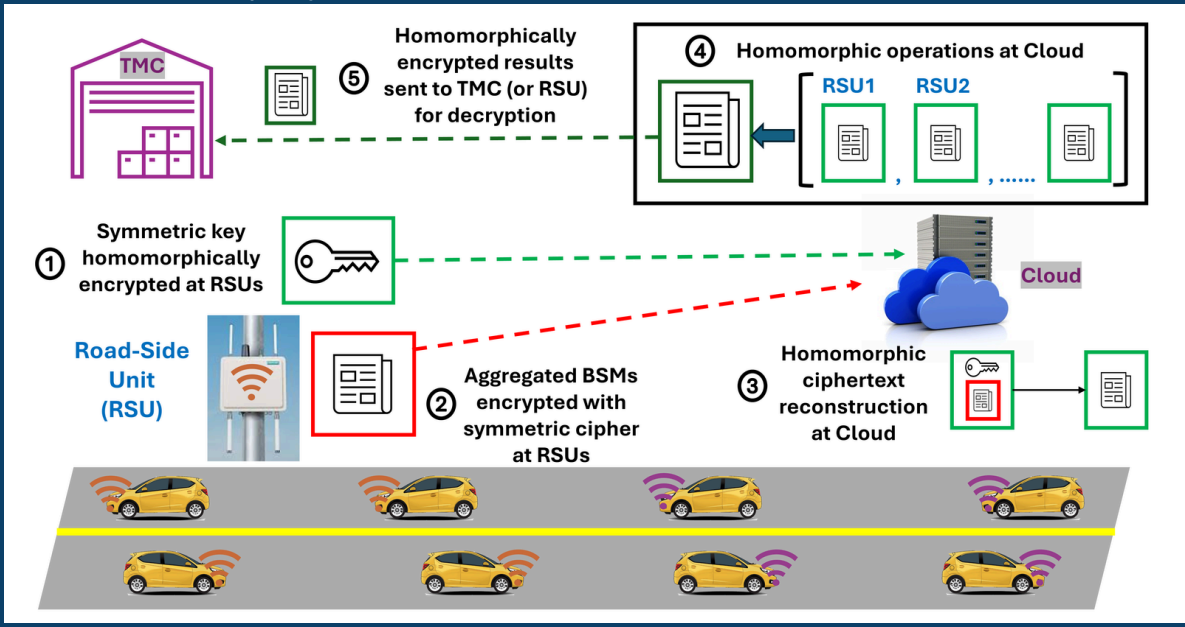
Click here to view the article

Research SPOTLIGHT

On the Feasibility of Hybrid Homomorphic Encryption for Intelligent Transportation Systems

Kyle Yates, Abdullah Al Mamun, and Mashrur Chowdhury

Intelligent Transportation Systems (ITS) rely on continuous data exchange between vehicles, roadside units (RSUs), and cloud-based infrastructure to support computation-heavy applications such as congestion monitoring, queue estimation, and traffic flow optimization. However, centralized processing of these data streams in the cloud may raise privacy concerns, as sensitive vehicular information, including location, speed, and trajectory, and personally identifiable information such as a driver's identification information,could be exposed to an untrusted third party.



This research investigates the feasibility of Hybrid Homomorphic Encryption (HHE) for enabling privacy-preserving analytics in ITS communication systems. Traditional fully homomorphic encryption (FHE) allows computation on encrypted data but produces extremely large ciphertexts (often >100 kilobytes), which cause packet fragmentation and significant communication latency. HHE addresses this limitation by combining homomorphic encryption with lightweight symmetric encryption. Instead of transmitting large homomorphic ciphertexts, RSUs send compact symmetric ciphertexts (typically about 100-200 bytes) while the cloud reconstructs the homomorphic form needed for encrypted computation. This approach drastically reduces communication overhead while preserving the ability to perform privacy-preserving analytics.

This study presents a theoretical feasibility analysis of HHE for ITS scenarios by developing representative application models and evaluating expected performance using parameters derived from the Rubato symmetric cipher used within a post-quantum FHE framework. By estimating ciphertext sizes, packet structures, and bandwidth requirements for V2X and infrastructure-to-infrastructure (I2I) communication, such as the RSU-cloud pipeline, the analysis demonstrates that HHE can significantly reduce communication latency and improve the practicality of privacy-preserving data analytics for latency-constrained ITS applications.

Click here to view the full paper

WEBINARS

Recorderd 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

EXPERIMENTAL EVALUATION OF POST-QUANTUM HOMOMORPHIC ENCRYPTION FOR PRIVACY-PRESERVING V2X COMMUNICATION

Dr. Kyle Yates
School of Mathematical and Statistical Sciences
Clemson University

CYBERSECURITY OF INTEGRATED AUTONOMOUS NAVIGATION SYSTEMS: VULNERABILITIES, DETECTION, AND RESILIENCE

Dr. Sagar Dasgupta
Postdoctoral Researcher,
The University of Alabama

GENERATIVE AI AND LARGE LANGUAGE MODELS (LLMS) FOR TRANSPORTATION SECURITY AND RESILIENCY

Dr. Latifur Khan
Professor, Department of Computer Science
University of Texas at Dallas

SECURING NEXT GENERATION EMBODIED AI ROBOTIC VEHICLES

Dr. Alvaro Cardenas
Professor of Computer Science and Engineering
The University of California, Santa Cruz

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

Student Recognition

2025 Outstanding UTC Student of the Year Award!

TraCR is proud to celebrate Kyle Yates, who has been recognized as the **2025 Outstanding UTC Student of the Year Award!**

Each year, the U.S. Department of Transportation recognizes exceptional students from each of the University Transportation Centers for their achievements and potential contributions to the transportation field. Awardees are selected based on technical merit, research excellence, academic performance, professionalism, and leadership.

This honor highlights Dr. Yates's outstanding contributions to transportation cybersecurity research and his dedication to advancing innovative solutions in the field. Dr. Yates was a Ph.D. student in Clemson University's School of Mathematical and Statistical Sciences, and his research sits at the intersection of post-quantum lattice-based cryptography and transportation cybersecurity. His work focuses on advancing privacy-preserving Intelligent Transportation Systems (ITS) by applying homomorphic encryption to secure cloud-based infrastructure-to-infrastructure (I2I) data analytics, enabling encrypted computation between distributed roadside and backend systems without exposing sensitive traffic or infrastructure data. This recognition reflects not only Dr. Yates's technical excellence but also the broader mission of the UTC program to elevate research, leadership, and real-world transportation impact. This is a well-deserved recognition, and we look forward to his continued contributions to the center and the field. Congratulations, Dr. Yates!

CONTACTS

That's It for Now!

Stay tuned for our next newsletter in the Fall of 2026.
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