TraCR ADVANCES

FALL 2025

Director's Message

I am excited to share our latest TraCR milestones with you. Our mission to strengthen transportation cybersecurity and resiliency drives every effort across the center, from research to education to partnerships. Several of our first-year projects have now wrapped up, and once peer review is completed for final reports, all of them will be available on our website. Highlights from our projects include enabling the adoption of Scenic, a probabilistic programming language that models and generates data for autonomous systems. TraCR-funded research has also contributed to patent applications and the launch of Resilient Timing Systems, LLC, a start-up focused on resilient Global Navigation Satellite System (GNSS) solutions for intelligent transportation. Innovative cybersecurity solutions, such as a transportation-focused automated threat modeling tool, a large language model for transportation cybersecurity, a privacy-preserving secure training framework for federated learning, and a particle filter-based GNSS spoofing attack detection, are already gaining attention from researchers and industry partners, showing the real-world impact of TraCR's work on transportation safety and security.

Across all our projects, partnerships between the industry, state Departments of Transportation, and our researchers have ensured our work aligns with cybersecurity and cyber-resilience in real-world systems. We are offering a hands-on graduate course, titled Cybersecurity of Cyber-Physical Systems, this fall at Clemson University, which is a part of the Cybersecurity Certificate Program offered at Clemson University. This multidisciplinary course enables students from Civil Engineering, Computing, Automotive, and Industrial Engineering to identify, analyze, and mitigate vulnerabilities in connected and automated transportation systems. Our education efforts are designed to continue to inspire the next generation of cybersecurity professionals. In June and July 2025, we hosted workshops and demonstrations, engaging college and high school students with hands-on experiences in transportation cybersecurity research.

TraCR has contributed to two pending patents, the founding of a start-up company, and the adoption of research by industry, among other accomplishments. From patents, to start-ups, to technologies adopted, TraCR's research is making a tangible impact on transportation systems and infrastructure. I am proud of our accomplishments and look forward to continuing to advance knowledge, foster collaboration, and build secure and safer transportation systems.

Dr. Mashrur "Ronnie" Chowdhury

In this Issue:

TraCR IMPACTS

Patents

TraCR marks two groundbreaking milestones in research and innovation with new patent filings to the U.S. Patent and Trademark Office (USPTO):

- The pending patent "Systems and Methods for Advancing the Restoration Process for Interdependent Critical Infrastructures" (Serial No. 19/058,257) introduces a novel approach to strengthening emergency response and accelerating infrastructure recovery.
- The pending patent "A Privacy-Preserving Federated Fine-Tuned Large Language Model" (Serial No. 19/272,726) addresses the growing demand for AI solutions that safeguard sensitive data.

These innovations underscore TraCR's commitment to advancing transportation-related technology, infrastructure resilience, and cybersecurity.

TraCR Technologies Developed

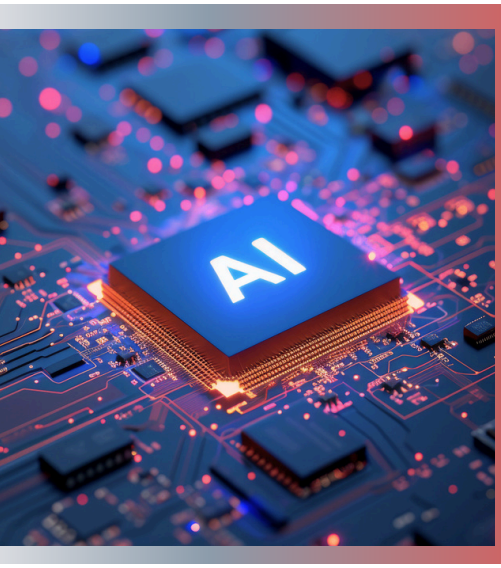
Several innovations developed by TraCR researchers have gained attention by external researchers and industry partners:

- CAROT: An open-source, cyber-resilient electronic control unit (ECU) incorporating a trusted execution environment (TEE).
- QuanCrypt: A privacy-preserving, communication-efficient framework for federated learning.
- TraCR-TMF: A large language model-supported threat modeling tool for transportation systems and infrastructure.
- TraCR-AI: A transportation-specific large language model for legal analyses of cybersecurity legislations.
- A particle filter-based GNSS spoofing attack detection framework
- Scenic: A probabilistic programming language for environment modeling and data generation for autonomous systems.

TraCR IMPACTS

Start Up Company Launched

TraCR project contributed to Resilient Timing Systems, LLC (Entity ID: 001-092-469), a startup launched in 2025. This startup is dedicated to developing resilient GNSS solutions for intelligent transportation systems. The company marks a significant step in advancing digital security and robust timing technologies for the transportation sector.



Peer-Reviewed Publications

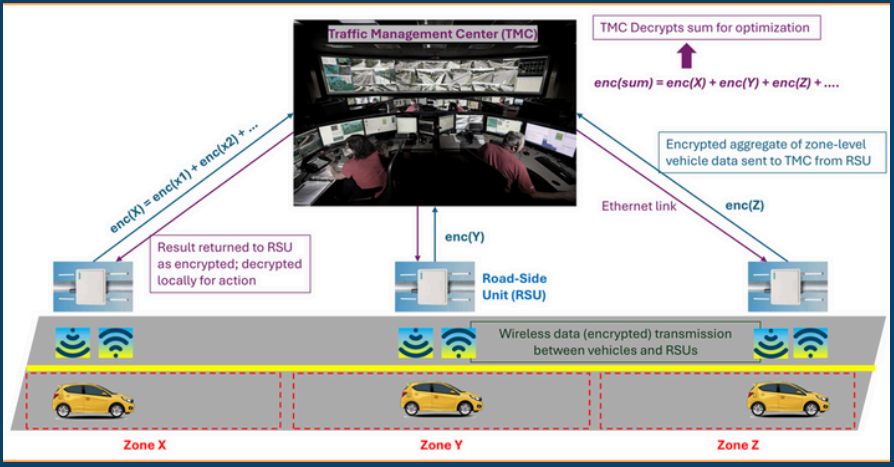
TraCR researchers have published more than 175 peer-reviewed papers addressing emerging threats and presenting innovative quantum-supported and AI-based defensive technologies. The contributions of these studies span key areas, such as cyber threat intelligence, risk mitigation, security of transportation-related software and hardware, and quantum-supported and/or AI-driven security tools development. These peer-reviewed publications underscore TraCR's commitment to advancing both foundational knowledge and practical solutions in cybersecurity and emerging technologies for transportation systems and infrastructure.

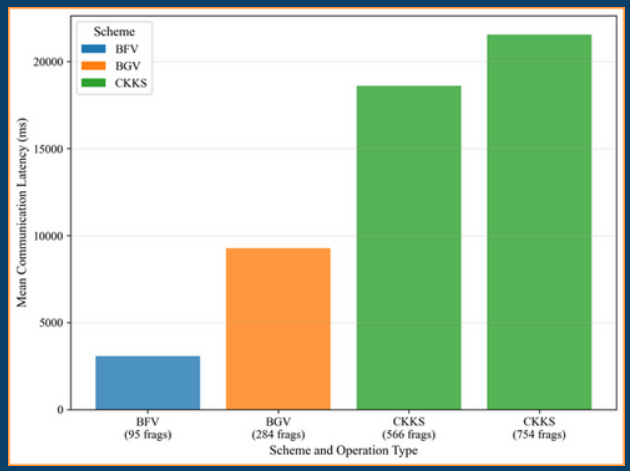
Webinars and Technology Demonstrations

TraCR continues to host technology demonstrations that highlight cutting-edge tools and innovations emerging from its funded research. These sessions feature capabilities, such as real-time attack simulations, along with their detection and mitigation, AI-driven incident response and recovery, and quantum-safe V2X communications that showcase advanced cyber defense strategies. The demonstrations offer researchers, students, and industry professionals a hands-on opportunity to explore the latest cybersecurity advancements and their real-world applications for transportation systems and infrastructure.

Experimental Evaluation of Post-Quantum Homomorphic Encryption for Privacy-Preserving V2X Communication

Abdullah Al Mamun, Kyle Yates, Antsa Rakotondrafara, Mashrur Chowdhury, Ryann Cartor, and Shuhong Gao





Vehicle-to-everything (V2X) communication in Intelligent Transportation Systems (ITS) enables applications such as congestion monitoring, speed advisory, and route optimization, but also raises serious privacy concerns. Sensitive data, including location and speed, can be intercepted or misused by untrusted services.

This study presents the first real-world experimental evaluation of three post-quantum secure homomorphic encryption (HE) schemes: Brakerski-Fan-Vercauteren (BFV), Brakerski-Gentry-Vaikuntanathan (BGV), and Cheon-Kim-Kim-Song (CKKS), for privacy-preserving ITS applications. HE allows computation directly on encrypted data, ensuring that raw vehicle data remains inaccessible even during processing. Two representative scenarios were tested: encrypted vehicle counting (addition-only) and encrypted average speed aggregation (addition + multiplication). Experiments were conducted over Wi-Fi and Ethernet to reflect both wireless and wired V2X environments. The results show:

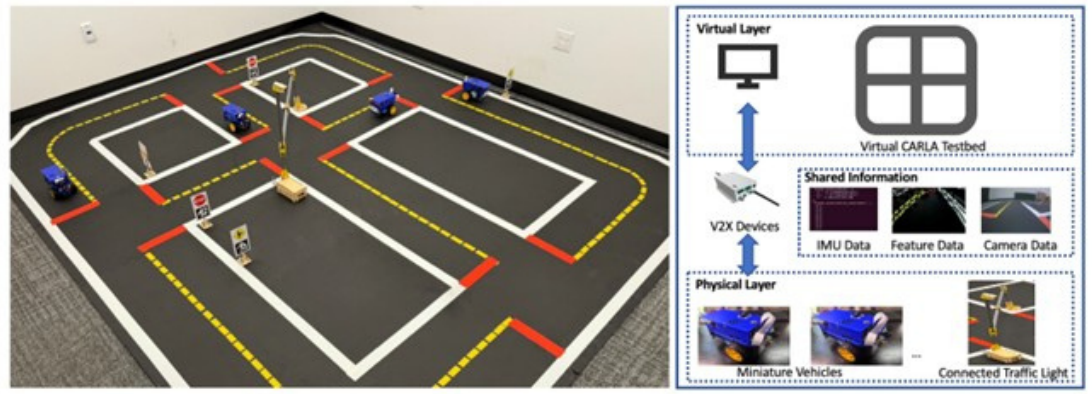
- BFV achieved sub-5-second updates, making it practical for intersection-level congestion monitoring.
- BGV produced ~9-second latencies, suitable for regional traffic analysis and periodic updates.
- CKKS, while offering encrypted floating-point aggregation, incurred 21–32 second delays, limiting it to latency-tolerant applications such as eco-driving feedback or historical analytics.

Across all schemes, communication latency, driven by ciphertext expansion and packet fragmentation, was the primary performance bottleneck. While none of the tested configurations meet sub-second safety-critical requirements (e.g., collision warning), they demonstrate strong potential for privacy-preserving, latency-tolerant ITS use cases under 128-bit post-quantum security. This work provides the first end-to-end, hardware-tested benchmarking of post-quantum HE in real V2X conditions, offering valuable insights for future deployment and optimization.

Click here to view the full paper

Cybersecurity Testbed for Connected and Autonomous Vehicles: Phases I &II

Zengxiang Lei, Ruichen Tan, Shiveswarran Ratneswaran, and Satish V. Ukkusuri



The safe operation of connected and autonomous vehicles (CAVs) requires test environments that faithfully capture real-world conditions across perception, localization, communication, and timing. However, simulation-only pipelines remain limited by the sim-to-real gap and are highly susceptible to unintentional disturbances such as sensor noise, synchronization drift, and communication irregularities, as well as to deliberate cyber-physical threats, including fabricated or erased sensor evidence and manipulated V2X messages. Moreover, physical vehicle testbeds incur prohibitively high costs, as each experimental collision risks substantial property damage. To address these challenges, we introduce the SENTINEL (Secure Evaluation of Networked Transportation via Integrated Network Emulation and Logic) testbed, an open-source, integrated platform that extends prior co-simulation research by combining traffic simulation, V2X communication protocols, and adversarial scenarios. SENTINEL supports both virtual and physical experiments, enabling the study of how cyber-physical attacks impact traffic operations and facilitating controlled investigations across diverse laboratory environments.

This project addresses the challenge of testing autonomous and connected vehicle (AV/CV) systems under cyber-physical threats without incurring the risks and costs of physical trials. The platform is released as open-source software, enabling contributions from AV developers, transportation researchers, and government agencies. It supports real-time streaming, batch simulation, and integration with external co-simulation environments, with documentation and examples provided for adoption. In parallel, a physical testbed is being developed to form an integrated cyber-physical platform. It employs real V2X communication devices to emulate authentic scenarios and miniature vehicles with onboard sensors for signal sharing. A Sim2Real mapper synchronizes physical and virtual vehicle behaviors, bridging the two environments. The testbed supports adversarial scenarios such as V2X spoofing, fake demand signals, and charging station manipulation, along with defensive strategies including anomaly detection and secure communication protocols. By combining open-source code, documentation, and demonstrations, SENTINEL enables low-cost, reproducible cybersecurity studies. Its integrated design bridges the sim-to-real gap, providing a unique environment to validate resilience strategies, analyze cascading failures, and accelerate the deployment of trustworthy, cyber-secure CAV systems.

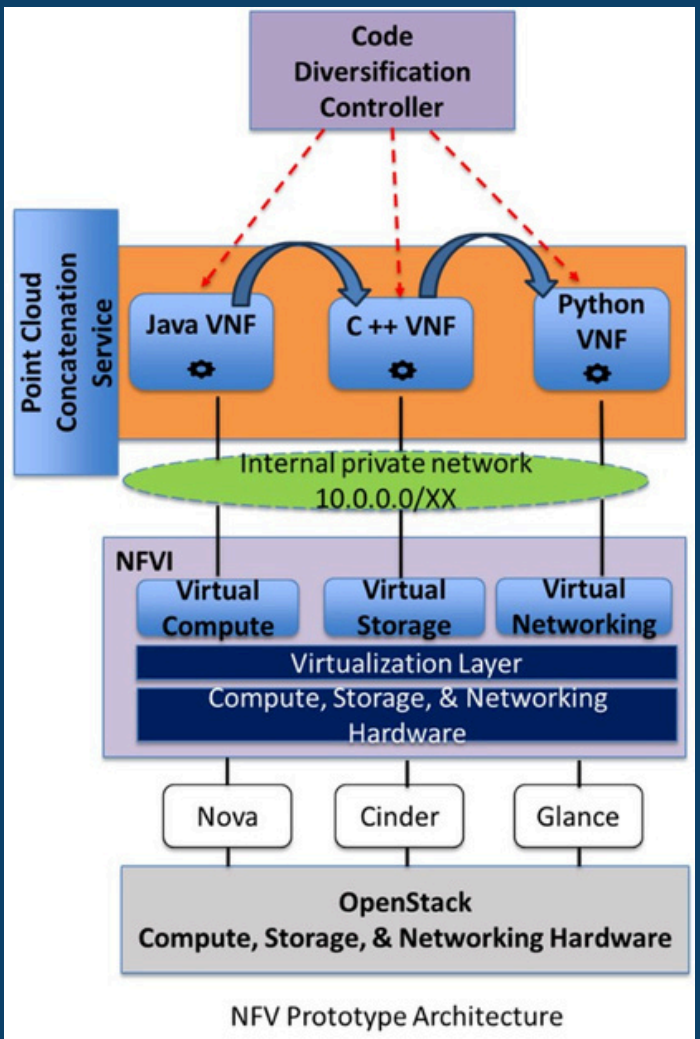
Click for more information on the software

NFV-Based Code Diversification Framework for Resilient Connected and Autonomous Vehicle (CAV) Software

Jagruti Sahoo, Judith Mwakalonge, Nikunja Swain, Biswajit Biswal, and Gurcan Comert

Security vulnerabilities in the CAV software enable hackers to compromise critical modules and perform malicious actions, ranging from draining batteries and taking control of the steering wheel to disabling the alarm system. CAV software is subject to several cyber-attacks, including memory corruption, code injection, remote code execution, and malware attacks. Securing CAV software is therefore of paramount importance to ensure the safe and reliable operation of CAVs.

We designed a Network Functions Virtualization (NFV)-based framework that integrates a code diversification approach to secure CAV software by executing multiple variants of a functionally equivalent code. Our code diversification approach is designed based on the principles of Moving Target Defense (MTD), which involves changing the attack surface at fixed intervals to increase the system's complexity and make it difficult for hackers to discover and exploit vulnerabilities. To efficiently manage the code variants and facilitate their dynamic execution, our framework allows CAV software to be implemented as Virtual Network Functions (VNFs). Moreover, NFV technology allows our platform to scale as needed to support the accelerated growth in CAV software. In addition, it reduces the maintenance efforts and the operational cost.



NFV Prototype Architecture

We implemented a prototype of our NFV framework using the OpenStack platform. We created three VNFs (C++, Java, and Python) that implement the functionality of a point cloud concatenator node and are deployed on a Network Function Virtualization Infrastructure (NFVI). The point cloud concatenator node receives 3D point cloud fragments from publishers that generate synthetic LiDAR data, combines them, and publishes the combined cloud data. The combined data is useful for various perception applications, including object detection, tracking, and localization. We proactively switched the VNFs using a code diversification controller. We demonstrated that the concatenator node continued to operate even when a hacker attempted to exploit a buffer overflow vulnerability, thereby ensuring the resilience of CAV software. Our prototype shows the practical feasibility of using a code diversification approach in CAVs to prevent cyber intrusions.

TraCR-TMF: A Large Language Model-Supported Threat Modeling Framework for Cybersecurity Practitioners and Intelligent Transportation Systems Engineers

M Sabbir Salek, Mashrur Chowdhury, Muhaimin Bin Munir, Yuchen Cai, Mohammad Imtiaz Hasan, Jean-Michel Tine, Latifur Khan, and Mizanur Rahman

Modern transportation relies on cyber-physical systems (CPS), where computing infrastructure integrates with physical components such as sensors and actuators. These interactions improve safety and mobility, but also increase exposure to cyber vulnerabilities due to growing automation and connectivity. Existing threat modeling frameworks are often narrow in scope, labor-intensive, and require substantial cybersecurity expertise. To this end, we introduce the Transportation Cybersecurity and Resiliency Threat Modeling Framework (TraCR-TMF), a large language model (LLM)-based threat modeling framework for transportation CPS that requires limited cybersecurity expert intervention.

As presented in the figure in the following page, TraCR-TMF is a multi-stage threat modeling framework including the following stages:

- **STRIDE-based Threat Identification (Stage 1):**

A threat report is generated using the open-source Microsoft Software Development Lifecycle (MS SDL) threat modeling tool for each transportation CPS application under threat assessment. MS SDL applies the STRIDE threat model to each element and interaction of the CPS application architecture to identify spoofing, tampering, repudiation, information disclosure, denial-of-service, and elevation of privilege related threats.

- **LLM-based ATT&CK Technique Identification (Stage 2)**:

In this stage, MITRE ATT&CK techniques that are relevant to the transportation CPS application under threat assessment are identified based on the threats identified in Stage 1. Three LLM-based approaches support these identifications: (i) a retrieval-augmented generation (RAG) approach requiring no cybersecurity expert intervention, (ii) an in-context learning approach with low expert intervention, and (iii) a supervised fine-tuning approach with moderate expert intervention.

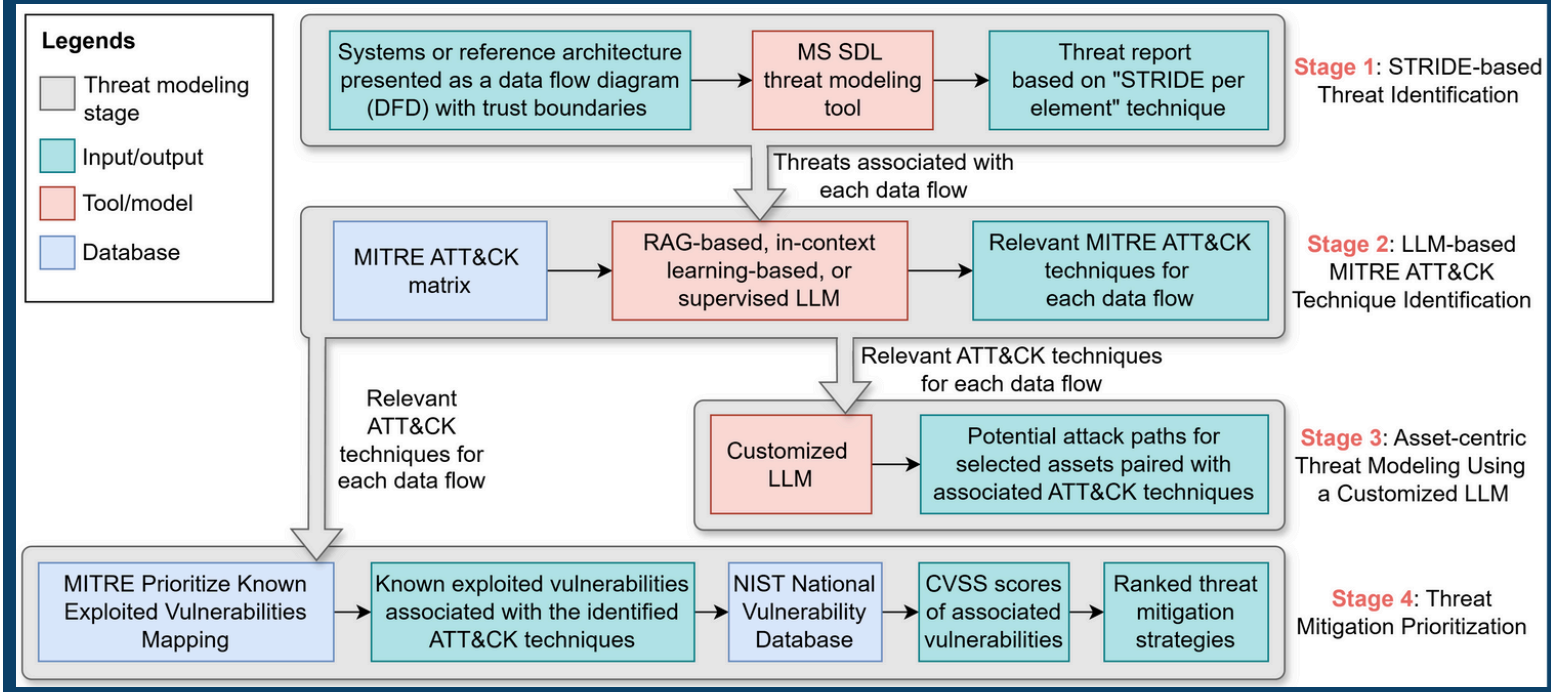
- **Asset-centric Threat Modeling Using a Customized LLM (Stage 3):**

In this stage, potential attack paths and associated attack techniques leading to the compromise of any specified critical asset in a transportation CPS application are identified using a customized LLM with an engineered prompt. This asset-centric threat modeling offers insights into the chains of vulnerabilities across multiple CPS entities that can be exploited together to perform an attack that aims to compromise one or more critical assets.

Research SPOTLIGHT

- **Threat Mitigation Prioritization (Stage 4):**

This stage helps prioritize mitigations of the threats identified through prior stages of TraCR-TMF. TraCR-TMF utilizes several open frameworks and databases such as the Common Vulnerability Exposure (CVE), the Known Exploited Vulnerabilities (KEV) catalog, and the National Vulnerability Database, to identify the severity of the associated vulnerabilities and prioritize the threat mitigations accordingly.



TraCR-TMF was evaluated through two cases. First, the framework identified relevant attack techniques for various transportation CPS applications, 73% of which were validated by cybersecurity experts as correct. In addition, we present how LLMs can be utilized to prioritize the threats to be mitigated, along with specific mitigation approaches for each threat, for a given transportation CPS application data flow. Second, the framework was used to identify attack paths for a target asset in a real-world cyberattack incident, i.e., the infamous Colonial Pipeline double-extortion ransomware attack. TraCR-TMF successfully predicted exploitations, like lateral movement of adversaries, data exfiltration, and data encryption for ransomware, as reported in the incident. These findings show TraCR-TMF's efficacy in transportation CPS threat modeling, while reducing the need for extensive involvement of cybersecurity experts. To facilitate real-world adoptions, all our codes are shared via an open-source repository.

Click here to view the full paper

WEBINARS

Recorderd WEBINARS

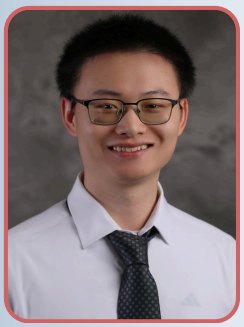
As part of our workforce development/training activities, TraCR hosts monthly webinars from transportation experts. The recordings of all webinars are available on our YouTube channel

HYPOTHESES OF SYSTEMS ORDER TO ADDRESS AMBIGUITY AND RISK IN COMPLEX SYSTEMS

Dr. James Lambert
Director, Center for Risk Management of Engineering Systems
University of Virginia

CYBER RESILIENCE IN TRANSPORTATION: NAVIGATING QUANTUM COMPUTING THREATS AND OPPORTUNITIES (PART 2)

Dr. M. Sabbir Salek
Senior Engineer, National Center for Transportation Cybersecurity & Resiliency (TraCR)
Clemson University



TRANSPORTATION CYBERSECURITY: A NETWORK-LEVEL PERSPECTIVE

Dr. Zengxiang Lei
Postdoctoral Researcher, Transportation Engineering
Purdue University

ADVANCES AND CHALLENGES IN USING EDGE AI TO ADDRESS TRANSPORTATION SAFETY CHALLENGES

Dr. Yinhai Wang
Professor in Transportation Engineering at Civil and Environmental Engineering
The University of Washington

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

ACHIEVEMENTS

2025 IEEE Intelligence and Security Informatics (ISI) Technical Achievement Award

Dr. Mashrur "Ronnie" Chowdhury, TraCR Director and Professor of Civil Engineering at Clemson University, has been awarded the 2025 IEEE Intelligence and Security Informatics (ISI) Technical Achievement Award. This distinguished honor recognizes his pioneering research and transformative contributions to cybersecurity and resiliency in intelligent transportation systems.

Presented virtually on July 12 during the IEEE ISI Conference in Hong Kong, the award highlights Chowdhury's innovations that are shaping the future of transportation, supporting the safe integration of connected and autonomous vehicles, and fortifying infrastructure against cyber threats. This recognition underscores his national leadership in next-generation mobility solutions.

Tenured and 2025 IEEE Big Data Security Junior Research Award

We are proud to share that Dr. Hadi Amini, TraCR Associate Director at Florida International University, has been awarded tenure and promotion to Associate Professor in the Knight Foundation School of Computing and Information Sciences. Dr. Amini is the founding director of the SOLID Laboratory (Sustainability, Optimization, and Learning for InterDependent networks), where he leads pioneering research in distributed machine learning, federated learning, interdependent networks, and cyber-physical-social resilience and cybersecurity. This well-deserved promotion reflects his outstanding contributions to research, teaching, and service in computing and information sciences.

In addition, Dr. Amini has received the 2025 IEEE Big Data Security Junior Research Award for his contributions to Big Data Security in Cyber-Physical Systems. This prestigious award highlights the impactful work, including TraCR students and collaborators, in advancing research at the intersection of AI, cybersecurity, and cyber-physical systems.

Please join us in congratulating Dr. Amini on these remarkable milestones!

EDUCATION

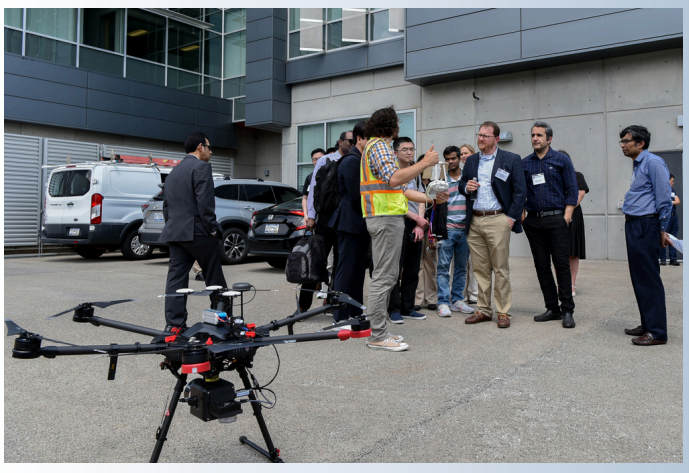
Cybersecurity Graduate Certificate

We are glad to report that TraCR has become a part of the Cybersecurity Graduate Certificate Program in association with the School of Computing at Clemson University. To earn the certificate, a graduate student must complete four courses (12 credits), including a core course called Computer Security Principles, and three additional electives.

Two of the elective courses were developed and are offered by TraCR researchers: Cybersecurity of Cyber-Physical Systems (CPS) and Intelligent Transportation Systems (ITS).

The course, Cybersecurity of Cyber-Physical Systems, provides students with a hands-on, systems-focused learning experience that builds a rigorous foundation for protecting CPS. Topics include CPS architecture and vulnerabilities, the Confidentiality, Integrity, and Availability (CIA) Triad, the NIST Cybersecurity Framework, and operational defenses, such as cyber threat intelligence, cloud security for CPS, AI-based detection and response, encryption for CPS communications, blockchain for integrity, quantum computing, and hardware security. Application areas span transportation CPS, smart buildings, smart grid, healthcare and medical devices, natural gas networks, etc. The course concludes with a capstone focused on holistic CPS security.

Another of the electives, Intelligent Transportation Systems (ITS), focuses on integrated applications of traffic flow principles, advanced sensors, computation, control, electronics, and communications technologies and management strategies to increase the safety and efficiency of transportation. Transportation cyber-physical systems (TCPS) merge the physical and cyber realms within ITS. Physical elements like sensors and traffic centers interact with control elements such as traffic lights and connected vehicles, supported by big data, AI, and automation to deliver safety, security, and mobility services. As infrastructure and different modes of transport increasingly integrate with the cyberworld, services become safer and more efficient. With exponential growth in connectivity and intelligence integrated within ITS, this course introduces students to the planning, design, deployment, operation, and evaluation of TCPS.



CONTACTS

That's It for Now!

Stay tuned for our next newsletter in the Spring 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