TraCR ADVANCES

SPRING 2025

Director's Message

As we enter our third year, TraCR continues to drive advances in transportation cybersecurity and resilience. This spring, we launched 17 new research projects that tackle key cybersecurity challenges. This brings us to a total of 31 projects in progress, with 14 ongoing projects from our first year concluding soon. Our key focus areas include post-quantum cryptography, intrusion monitoring, and diffusion models to protect vehicle-to-everything (V2X) communication and machine learning models. In addition, we are investigating cyber-physical incident analysis, perception system resilience, and the impact of denial-of-service (DoS) attacks on connected and automated vehicles (CAVs). Other initiatives we are involved in emphasize workforce development in transportation cybersecurity and emerging technologies like quantum computing. Also, we are working on a collaborative research project with all our consortium members. It focuses on developing a cybersecurity platform that enables threat modeling for transportation systems and infrastructure. The platform will help to identify vulnerabilities and potential attacks, leading to the development of countermeasures to address them.

This spring, we celebrated Eric Vin, a computer science Ph.D. candidate at UC Santa Cruz, as TraCR's 2024 Outstanding UTC Student of the Year. His work on cyber-physical system verification and the Scenic 3.0 programming language exemplifies the excellence we aim to foster. Also, TraCR has been actively engaged in technology transfer, collaborating with industry and stakeholders to bring innovations to the market. Finally, our webinar series has been featuring leading researchers who are exploring new directions in transportation cybersecurity. We will be hosting several more such webinars in the coming months. As always, please visit the TraCR website for news about our latest work.

Dr. Mashrur "Ronnie" Chowdhury

In this Issue:

Director's Message
Newly Funded Projects
Research Spotlight
Webinars
Achievements
Outreach

Newly Funded Year 2 PROJECTS

This spring, TraCR awarded funding to 17 new research Year 2 projects. These projects align with our mission to enhance cybersecurity, resilience, and safety in autonomous and connected vehicle systems by addressing cyber threats, adversarial attacks, and AI-driven vulnerabilities. These projects were made possible through funding from the U.S. Department of Transportation University Transportation Centers program. The projects are briefly described here; more details can be found on the TraCR website.

Cybersecurity Analysis and Guidance to Support Secure Transportation Cyber-Physical Systems

Lead Principal Investigator: Trayce Hockstad (The University of Alabama Tuscaloosa)

This project evaluates the United States cybersecurity transportation laws and policies, and then compares them with existing international models. Currently, we are contextualizing what we have learned in our first year of research. The objectives of this project are to evaluate United States cybersecurity transportation law and policy compared to existing international models to support continued domestic regulatory development and update our policy toolkit (including LLM and guidance report) with insights from an expanded legislative corpus, visualized data, extended industry feedback and training, to provide a comparative analysis model of transportation cybersecurity research (identifying how the U.S. can improve its policy based on industry and international input).

Defending Object Detectors in Autonomous Vehicles Against Adversarial Attacks with Diffusion Models

Lead Principal Investigator: Dr. Long Cheng (Clemson University)

Object detection is a cornerstone task in computer vision and is a foundation for autonomous vehicles. Although machine learning-based object detectors achieve remarkable accuracy and efficiency, they are vulnerable to adversarial attacks which exploit the inherent weaknesses of machine learning models to mislead them into producing incorrect outputs. In particular, physical adversarial patch attacks (e.g., stickers placed on real-world objects) have attracted significant attention from the security community, since their potential implications for the safety and functionality of object detection systems are severe. We are utilizing the latest advances in generative models, particularly diffusion models, to preprocess input images before feeding them into object detection systems. Our goal is to develop a defense mechanism that can address different physical adversarial patch attacks, regardless of their shape or format. Our method is both patch-agnostic and attack-agnostic. Leveraging the generative power of diffusion models, the system we are developing will automatically detect and replace adversarial patches with contextually consistent content drawn from surrounding areas.

Experimental Evaluations and Analysis of the Impacts of Denial-of-Service (DoS) Cyber Attacks on the Performance of Connected and Automated Vehicles (CAVs)

Lead Principal Investigator: Dr. Yunyi Jia (Clemson University)

The project is conducting experimental studies that evaluate and analyze the impacts of denial-of-service (DoS) cyberattacks on the performance of connected and automated vehicles (CAVs). Our results will lead to a deeper understanding of the cybersecurity of CAVs to safeguard future intelligent transportation systems.

Newly Funded Year 2 PROJECTS

Resilient Autonomous Vehicle Perception Under Adversarial Settings

Lead Principal Investigator: Dr. Bing Li (Clemson University)

Modern autonomous vehicle systems depend heavily on deep learning-based perception modules for tasks such as object detection, automated lane centering, and traffic sign recognition. However, these systems remain vulnerable to adversarial attacks, such as environmental modifications designed to mislead AV sensors and compromise decision-making. This research is addressing these threats by developing robust model-based defenses that employ adversarial training and integrate vision-language models (VLMs). This will ensure the integrity of AV perception systems and guarantee they are resilient to both known (white-box) and unknown (black-box) adversarial scenarios. The goal is to ensure safer and more secure transportation systems as AV adoption accelerates.

Cyber-Physical Investigation of Autonomous Vehicle Incidents and Attacks

Lead Principal Investigator: Dr. Dave (Jing) Tian (Purdue University)

This project is developing a framework to enhance the investigation of autonomous vehicle incidents and attacks. It focuses on improving the infrastructure for offline incident investigation, including minimizing manual effort in identifying the root causes of AV failures. The project consists of three main components: a deterministic replay tool for autonomous driving systems, a whole-system provenance infrastructure, and a provenance-guided root cause investigation tool.

Secure and Robust Machine Learning for Autonomous Driving Systems

Lead Principal Investigator: Dr. Yongkai Wu (Clemson University)

As autonomous driving systems (ADS) become increasingly prevalent, critical concerns have emerged regarding their security vulnerabilities and performance inconsistency, particularly in pedestrian detection and natural language processing. Current machine-learning technologies, while effective, can introduce variability where model performance remains uniform across different scenarios and is susceptible to security attacks that may compromise both safety and robustness. This project is identifying and analyzing security and robustness vulnerabilities in ADS, in order to develop novel strategies to promote robustness and enhance security in pedestrian detection systems, improve robustness in automotive large language models, and implement prototype systems for real-world evaluation. The research methodology encompasses four integrated tasks. First, we will develop a novel consistency poisoning attack framework to assess system vulnerabilities. Second, we will analyze and mitigate consistency vulnerabilities in pedestrian detection systems through advanced machine-learning techniques. Third, we will enhance consistency in large language models through innovative prompt engineering and model fine-tuning. Finally, we will implement prototype systems and conduct comprehensive evaluations using real-world datasets to validate our approaches.

Newly Funded Year 2 PROJECTS

Increasing Cybersecurity Workforce in the Transportation Systems Sector: An Interdisciplinary and Collaborative Approach

Lead Principal Investigator: Dr. Amjad Ali (Morgan State University)

The aim of this research project is to address the shortage of cybersecurity talent in the transportation systems sector. Developing a qualified cybersecurity workforce is critical to creating a workforce capable of protecting our nation's transportation infrastructure. There is a critical need to identify challenges to developing a steady pipeline of qualified talent in the cybersecurity workforce and find innovative solutions to increase talent training in the rapidly growing field of cybersecurity. In response to this need, this proposed research will investigate, identify, and analyze barriers to developing a steady pipeline of cybersecurity talent and develop innovative solutions to train the cybersecurity workforce needed to protect our nation's transportation systems. To address the cybersecurity challenges of transportation systems in a holistic manner, we need an interdisciplinary cybersecurity workforce that is equipped with knowledge and skills specifically relevant to the security of transportation systems. Therefore, developing the cybersecurity workforce specialized in securing transportation systems requires separate study and investigation. In addition, it ensures the needs and cybersecurity awareness of the ridership are met.

Vulnerability Assessment of Sensor Fusion for Transformer-Based End-to-End Autonomous Driving Models

Lead Principal Investigator: Dr. Pierluigi Pisu (Clemson University)

This project is conducting a comprehensive vulnerability assessment of transformer-based end-to-end autonomous driving models that use sensor fusion, specifically the TransFuser and InterFuser architectures. We will evaluate robustness against evasion attacksthat target misclassifications and incorrect trajectory generation. In addition, we will analyze natural corruptions like adverse weather conditions. We will develop an evaluation framework, implement attack strategies, and validate findings using both simulation and real-world testbeds.

Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents

Lead Principal Investigator: Dr. Zulqarnain Khattak (Morgan State University)

Cooperative driving automation (CDA) or vehicles which are connected and automated, continuously communicate with surrounding vehicles, which can potentially help relieve congestion and improve roadway efficiency and safety. However, the wider use of communications and wireless networks in CDA and transportation operations and management systems has made these systems vulnerable to the risk of cyberattacks. These systems rely on the internet of things (IoT), and connectivity and provide wider accessibility. The XML messages used by the National Transportation Communication for Intelligent Transportation Systems Protocol (NTCIP) are considered to be vulnerable to relatively small intrusions that are initiated by hackers, and have no built-in security. The USDOT has initiated a credential management system for security (SCMS) of vehicle and infrastructure-based communications. However, the increased dependency on communication provides hackers with multiple access points, resulting in vulnerability to cyberattacks. These risks are currently not well understood and thus are the focus of this research.

Newly Funded Year 2 PROJECTS

High-Fidelity Attack Modeling and Resilience Analysis of Autonomous Vehicle Software Stack

Lead Principal Investigator: Dr. Z. Berkay Celik (Purdue University)

This project aims to improve the resilience of autonomous vehicles (AVs) against physical attacks. It will develop a high-fidelity modeling environment and integrate it with a resilience analysis framework. This will allow for a deeper understanding of how robust AV systems are under various scenarios and environmental conditions, ultimately contributing to safer AV technology.

Cybersecurity Testbed for Connected and Autonomous Vehicles: Phase II

Lead Principal Investigator: Dr. Satish Ukkusuri (Purdue University)

COMET Phase II will continue to develop an integrated physical testbed for connected and autonomous vehicles. This will allow us to test cyber threats and countermeasures in the field, beyond using simulation techniques. By integrating real-world sensors, V2X infrastructure, and miniature autonomous vehicles, the ongoing project is bridging simulation and reality to enhance CAV cybersecurity and resilience.

Towards Deployment-Ready Post-Quantum Cryptography Enabled Vehicle-to-Everything Communication

Lead Principal Investigator: Dr. Mizanur Rahman (The University of Alabama Tuscaloosa)

Today's vehicle-to-everything (V2X) communication in intelligent transportation systems relies on the IEEE 1609.2 standard, which definessecure message formatsand processing. V2X communication relies heavily on cryptographic security to protect and safeguard sensitive information transmitted between vehicles, transportationinfrastructure, and otherentities. However, the rise of quantum computers poses significant cyber threats because they can break the security provided by current cryptographic algorithms. In addition, directly integrating the National Institute of Standards and Technology (NIST) approved post-quantum cryptography (PQC) schemes presents challenges due to largerkey sizes, high computational demands,and stringent latency requirements. Moreover, current PQC schemes require innovative adaptations to fit within the strict packet size constraints imposed by IEEE 1609.2 without compromising system performance. The goal of this project is to address these challenges by enhancing the security and quantum resilience of V2X communication systems. To do this,we will: (1) develop efficient algorithms for solvingthe complex problems that form the securityfoundation of PQC schemes, and assess the trade-offs betweenkey sizes and security levels; (2) design and implement a certificate segmentation algorithm for integrating PQC into the IEEE 1609.2 security standard, enabling reliable, low-latency, and quantum-resilient C-V2X communication; and (3) evaluate the performance of PQC schemes utilizing federated learning (FL)-based C-V2X applications in connected transportation systems. These steps will contribute to a secure, reliable, and deployment-ready PQC-enabled V2X communication system.

Newly Funded Year 2 PROJECTS

Resilience-Enhanced Intrusion Monitoring Against Emerging and Uncertain Threats in V2X Networks

Lead Principal Investigator: Dr. Lan Emily Zhang (Clemson University)

This project focuses on enhancing the cybersecurity and resilience of vehicle-to-everything (V2X)networks in connected and autonomous vehicle ecosystems. By developing a resilience-enhanced intrusion monitoring framework, we will detect, mitigate, and adapt to emerging and uncertain threats in dynamic, heterogeneous transportation environments. The project framework includes the development of novel resilience metrics, a resilience-based intrusion detection system (IDS) leveraging advanced AI techniques, and adaptive intrusion mitigation protocols to maintain network performance and security.

Safe and Reliable Autonomous Vehicle Navigation through Cyber Resilience

Lead Principal Investigator: Dr. Mizanur Rahman (The University of Alabama Tuscaloosa)

The reliable operation of autonomous vehicles hinges on robust and reliable positioning, navigation, and timing (PNT) services, which are predominantly provided by global navigation satellite systems (GNSS). The U.S.-owned global positioning system (GPS)consists of ground control stations (GCS), space vehicles (SV), and user segment receivers, all of which could be susceptible to natural interference and cyber threats. GCS, which is vulnerable to physical and cyberattacks, can transmit compromised correction data to satellites, posing significant risks to navigation integrity. GNSS signals are inherently weak and susceptible to unintentional interference, such as signal blocking, urban canyon multipaths, and atmospheric effects, as well as deliberate threats like jamming and spoofing, which can significantly amplify uncertainties in PNT services. Although alternative PNT solutions, including low earth orbit (LEO) satellites, Wi-Fi, and cellular-based technologies show promise, they remain limited in coverage, are underdeveloped, and/or are vulnerable to intentional interference. High-definition (HD) map-based navigation systems are also at risk of exploitation by hackers. Multi-sensor fusion systems, which integrate GNSS with inertial measurement units (IMU) and perception sensors (PS) such as cameras, lidar, and radar offer potential solutions by complementing individual sensor outputs in contested environments. However, IMUs suffer from error accumulation, and PS performance is compromised by limited line-of-sight or adverse weather conditions (e.g., snow and heavy rain), which degrade positioning accuracy. To overcome these challenges, this project aims to enhance the security of GNSS-based navigation systems through four key steps: (1) identifying and analyzing vulnerabilities in GNSS ground control and user segments in order to develop intelligent cyber-attack models, (2) designing and implementing sensor fusion algorithms that leverage loosely-coupled GNSS, IMU, and perception sensor data for the detection of GNSS cyber-attacks, (3) developing advanced mitigation strategies to counter spoofing attacks and restore authentic GNSS signal lock, and (4) deploying these detection and mitigation algorithms in secured execution environments in order to safeguard operational integrity against software-based threats. By addressing GNSS vulnerabilities, we will significantly enhance the safety and reliability of GNSS-based navigation for autonomous vehicles, foster public and industry trust in the reliability in these technologies, and support broader advances in transportation cybersecurity.

Newly Funded Year 2 PROJECTS

Investigating Driver Behavior Under Cyber-Attacks in Connected Vehicle Environments

Lead Principal Investigator: Dr. Mansoureh Jeihani (Morgan State University)

This research focuses on investigating driver behavior under cyber-attacks in connected vehicle environments. Using controlled testbeds with driving simulators at Morgan State University and Clemson University, we will simulate cyber-attacks, such as falsified vehicle-to-everything (V2X) information, to evaluate drivers' behavioral and psychological responses. The findings will fill gaps in our understanding of human factors in cybersecurity for CV systems, enhancing road safety and advancing resilient vehicle technologies.

Towards Securing Electric Vehicle Charging Systems Against Passive and Active Attacks

Lead Principal Investigator: Dr. Ahmad Alsharif (The University of Alabama Tuscaloosa)

This project addresses cybersecurity vulnerabilities in electric vehicle (EV) charging infrastructure, specifically focusing on the power line communication (PLC) systems used to connect EVs and charging stations (EVSE). We will develop protective measures against both passive eavesdropping and active interference attacks that can disrupt charging services.

Quantum Annealing-Based Optimal Identification of Vulnerable Software Components in Connected and Autonomous Vehicles

Lead Principal Investigator: Dr. Jagruti Sahoo (South Carolina State University)

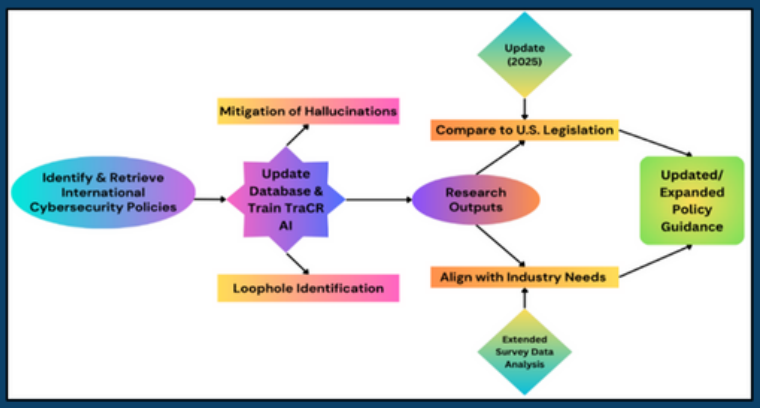
Automotive software is a critical component for the safe operation of a connected and autonomous vehicle (CAV). The software interacts with various sensors including lidar, radar, cameras, and the global positioning system (GPS), and executes complex algorithms to generate commands for the actuators such as the steering wheel and brake and gas pedals. The complexity of automotive software has grown over the last few years and is expected to grow exponentially in the next few. This accelerated growth is being fueled by factors including the integration of advanced driver assistance features, autonomous driving, and, most importantly, electric vehicles. Such significant growth will bring immense challenges in terms of ensuring the safety and reliability of automotive software. The increase in code is leading to an expanded attack surface that will allow hackers to discover vulnerable software and exploit it with malicious attacks against the CAV. An in-depth analysis of the attack surface, along with a meticulous identification of the most vulnerable software components/modules, can help in deciding the appropriate countermeasures to avoid cyber-attacks.

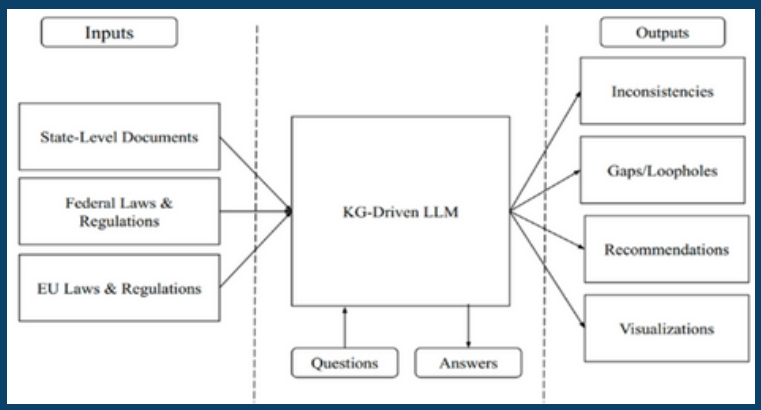
This project will develop a novel optimization model of the quadratic unconstrained binary optimization (QUBO) form to optimally identify the most vulnerable software modules, taking into account several factors (e.g., the attack surface of the automotive software, the downtime of modules, the cost of protecting the modules, etc.). We will investigate quantum annealing, a technique for solving QUBO. We will also design classical metaheuristics, simulated annealing, and genetic algorithms as benchmarks to assess the effectiveness of the quantum annealing-based approach. Our goals are to (1) analyze the attack surface of automotive software and produce interaction graphs, (2) define vulnerable S/W module identification problems and develop a QUBO model, (3) implement QUBO on a quantum annealer, (4) design simulated annealing and genetic algorithms to solve the optimization problem, and (5) compare the optimal performance of the quantum annealing-based approach with simulated annealing and genetic algorithms.

Research SPOTLIGHT

Cybersecurity Analysis and Guidance to Support Secure Transportation Cyber-Physical Systems

Trayce Hockstad, Mizanur Rahman, Steven Jones, Latifur Khan, Bhavani Thuraisingham, Mashrur Chowdhury, M Sabbir Salek, Sagar Dasgupta





The unprecedented cybersecurity threats facing the transportation sector make it urgent to develop robust and adaptive policy frameworks. So our research team has developed TraCR AI, a large language model (LLM) specifically designed to analyze cybersecurity legislation at both state and federal levels. In its first year, TraCR AI successfully identified key regulatory trends and inconsistencies, demonstrating superior performance in this legal analysis when compared to commercial AI models.

Building on our initial successes, year 2 of this project is expanding TraCR AI's capabilities to provide more comprehensive policy assessments. The next phase focuses on:

- Expanding Our Legislative Database: Integrating international cybersecurity regulations alongside anticipated U.S. policy updates, such as CISA's 2025 Guidance, to offer a global perspective on transportation security.
- Developing Advanced Knowledge Graphs: Utilizing AI-powered visualizations to highlight regulatory gaps, inconsistencies, and emerging legal challenges.
- Engaging with Industry Stakeholders: Conducting in-person workshops with state Departments of Transportation (DOTs) to refine TraCR AI's analytical precision and ensure real-world applicability.
- Creating a Decision-Support Tool: Assisting policymakers in evaluating cybersecurity measures, optimizing legislative strategies, and proactively addressing vulnerabilities.

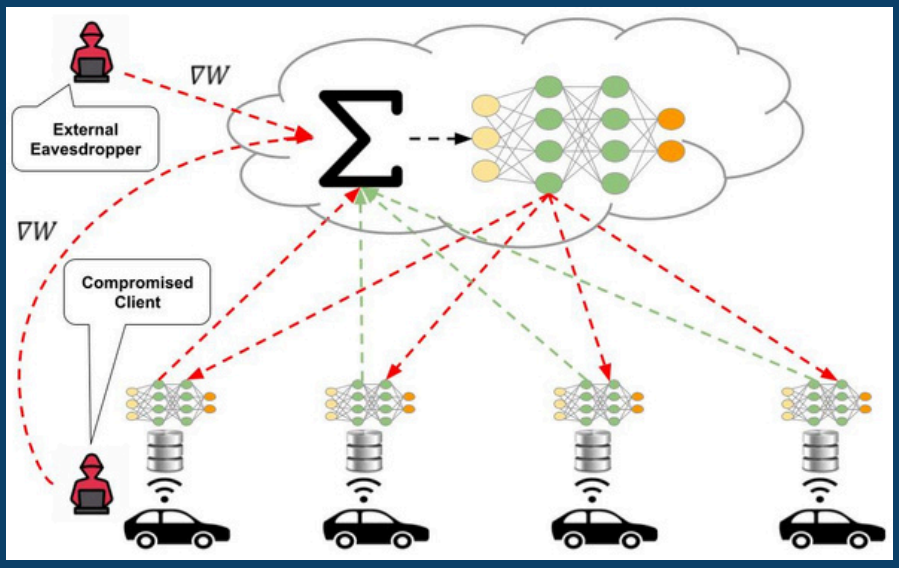
By leveraging AI for in-depth legal analysis, TraCR AI will empower stakeholders to make informed decisions about cybersecurity policies affecting transportation networks. This will not only enhance regulatory compliance, but will also strengthen national and global cybersecurity resilience, which is critical for policymakers, industry leaders, and transportation agencies striving to navigate the evolving cybersecurity landscape. As we move forward, our focus remains on delivering actionable insights that bridge the gaps between policy, technology, and transportation security.

Click for more information on the article

Research SPOTLIGHT

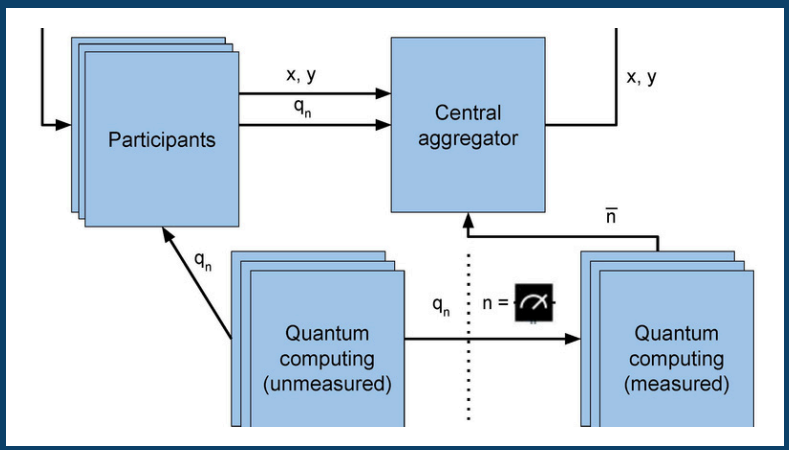
Quantum-Encrypted AI for Secure Connected and Autonomous Vehicles

M. Hadi Amini, Md Jueal Mia, Ervin Moore III
Florida International University,
Security, Optimization, and Learning for InterDependent networks laboratory (solid lab)



Autonomous and intelligent transportation systems rely heavily on machine learning and AI for object detection, decision-making, and real-time navigation. However, these systems are vulnerable to adversarial cyber-threats, including data poisoning, backdoor attacks, and inference attacks during the training and inference phases. Our research identifies and quantifies these vulnerabilities within federated learning (FL)-based object detection models deployed in autonomous transportation networks. By analyzing security gaps in edge-based FL models, we are uncovering the limitations of existing defense mechanisms against targeted cyberattacks in autonomous vehicle applications. To address these threats, we introduce a novel quantum-encrypted FL framework designed to protect against adversarial learning algorithms, particularly generative adversarial network (GAN)-based reconstruction attacks. Our approach integrates randomly generated quantum noise into the FL environment, enhancing security by creating an additional cryptographic layer resistant to traditional computational attacks. This hybrid model ensures that adversarial entities cannot infer private model updates, thereby strengthening both data integrity and privacy within edge computing environments.

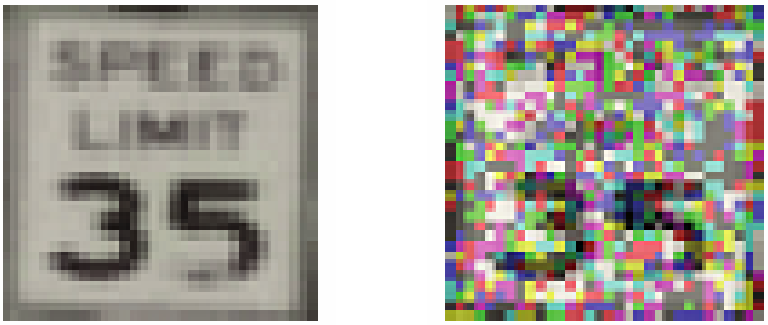
Our research is paving the way for secure distributed learning in next-generation CAVs by securing FL-based object detection against GAN attacks and data inference threats. Our future research will extend these security mechanisms to real-time multi-modal sensor fusion and post-quantum cryptographic protocols, ensuring robust and adaptable cybersecurity defenses for transportation infrastructures and CAVs.



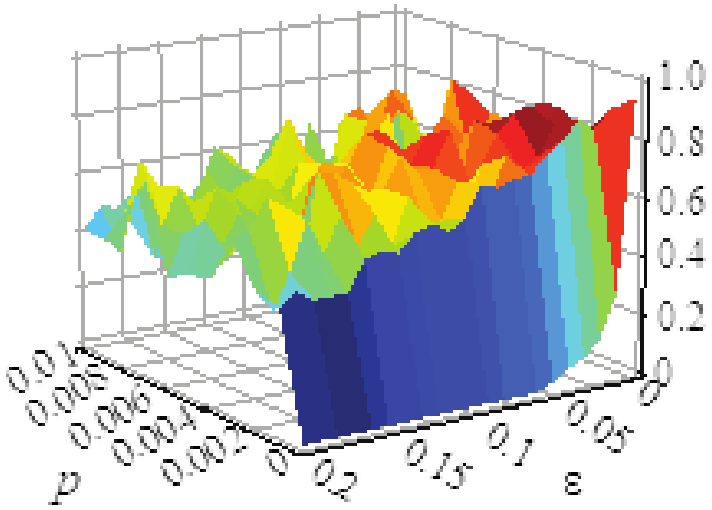
Click for more information on the article

Quantum-Inspired Weight-Constrained Neural Network

Shaozhi Li, M Sabbir Salek, Binayyak Roy, Yao Wang, Mashrur Chowdhury



(a) No Attack (b) Under Attack



(c) Resilience

(a) Traffic image. (b) Traffic image under adversarial attack. (c) The accuracy of the weight-constrained neural network. Here, *p* denotes the dropout probability, and *e* denotes the attack intensity.

Autonomous vehicles utilize deep learning techniques to detect and classify different roadway objects and traffic control devices. However, research has demonstrated that neural networks are particularly vulnerable to adversarial samples, posing significant safety risks. To address this critical issue and improve the safety of autonomous driving systems, we propose a novel machine learning framework: the weight-constrained neural network. Unlike traditional neural networks, our approach employs a unique weight structure where each weight is constructed from a set of independent variables. We generate thousands of weights using only dozens of independent variables, significantly reducing the memory requirements compared to conventional neural network architectures.

To further enhance the robustness of our weight-constrained neural network, we introduce a randomized dropout mechanism for the independent variables. This process involves selectively dropping certain independent variables and reconstructing the weight elements using the remaining variables. The figure on the left shows that this dropout strategy significantly improves the network's resilience to adversarial attacks. Thus, our proposed method not only reduces the memory overhead for image identification systems but also strengthens their robustness against adversarial perturbations, thereby contributing to safer and more efficient self-driving technologies.

Click for more information on the article

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

TOWARDS COMPOSITIONAL SECURE AUTONOMY: FROM PERCEPTION TO CONTROL

Dr. Z. Berkay Celik
Assistant Professor, Computer Science
Co-Director, Purdue Security (PurSec) Laboratory,
Purdue University

LEVERAGING GENERATIVE AI FOR SENSOR DATA FALSIFICATION ON DRONES AND AUTOMATED VEHICLES

Dr. Kemal Akkaya
Professor, School of Computer and Information Sciences
Florida International University

CYBER RESILIENCE IN TRANSPORTATION: NAVIGATING QUANTUM COMPUTING THREATS AND OPPORTUNITIES

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

RESILIENT CONNECTED AND AUTOMATED VEHICLE (CAV) SOFTWARE USING REINFORCEMENT LEARNING BASED VIRTUALIZED SECURITY FRAMEWORK

Dr. Jagruti Sahoo
Associate Professor, Computer Science
South Carolina State University

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

ACHIEVEMENTS

White House Presidential Award

In January, the White House honored Dr. Ronnie Chowdhury, the Eugene Douglas Mays Chair of Transportation at Clemson and founding director of TraCR, with the **Presidential Award for Excellence in Science, Mathematics and Engineering Mentoring**. The award is among the nation's highest honors for mentors who work with students to develop the nation's human resources in STEM. The National Science Foundation (NSF) manages the award for the White House Office of Science and Technology Policy.

Student Recognition

2024 Outstanding UTC Student of the Year Award!

TraCR is proud to honor Eric Vin, a Computer Science Ph.D. candidate at the University of California, Santa Cruz (UCSC), as the recipient of the **2024 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.

Eric earned a B.S. degree from UCSC, double majoring in Computer Science and Computational Mathematics, and is pursuing his Ph.D. in Computer Science at UCSC. His research focuses on the verification and analysis of cyber-physical systems such as automobiles and aircraft. Notably, he has made significant contributions to the probabilistic programming language Scenic, expanding its capabilities beyond testing and analysis toward a full verification framework. Specifically, his work on Scenic 3.0 introduces precise 3D scenario representation, integrates assume-guarantee contracts for compositional testing and verification, and enhances the program's compatibility with the METS-R traffic simulator.

Eric's outstanding academic journey reflects his deep commitment to intelligent transportation systems and cyber-physical system verification. TraCR salutes him for this well-deserved recognition and looks forward to his continued contributions to the center and the field. Congratulations, Eric!

ACHIEVEMENTS

Fellow of the American Association for the Advancement of Science

Congratulations to Dr. Latifur Khan on being elected a **2024 Fellow of the American Association for the Advancement of Science (AAAS)**. This honor adds to his distinguished list of accolades; he is also a Fellow of IEEE and an ACM Distinguished Scientist. Also, he has received the prestigious IEEE Technical Achievement Award, a joint award from the IEEE Systems, Man, and Cybernetics Society and from the IEEE Intelligent Transportation Systems Society, and several IEEE best paper awards.

Student Recognition

Sefatun-Noor Puspa, a Ph.D. student in the Glenn Department of Civil Engineering at Clemson University who is advised by TraCR Director Dr. Ronnie Chowdhury, earned the **Second Place Poster Presentation Award** at the annual SC EPSCoR State Conference in Columbia, SC. Puspa's research focuses on side channel power analysis-based non-invasive detection of hardware trojans in cyber-physical systems.

Tosin Jimoh, a student at Benedict College, received the **First Place Undergraduate Poster Presentation Award** at the SC EPSCoR State Conference.
Tosin's poster was titled "Autoencoders vs FGSM: Comparison of Machine Learning Models for Detecting Adversarial Perturbations in Image Classification." It featured work that he conducted under the mentorship of Dr. Balaji Iyangar and Dr. Ronnie Chowdhury.

OUTREACH

SC EPSCoR Conference

The SC EPSCoR Conference was held in Columbia, SC, on April 5, 2025. Its primary objective was to bring together South Carolina faculty, postdoctoral fellows, graduate and undergraduate students, and STEM professionals in order to foster networking and encourage collaborative efforts.

TraCR was strongly represented. Dr. Ronnie Chowdhury gave a keynote on the Cybersecurity of Cyber-Physical Systems in a Connected and Automated World as part of the SC State Science and Technology Plan.

TraCR faculty and staff participated in the sessions on cybersecurity featuring talks from:

- Dr. Xiaoyong Yuan, from Clemson University speaking on Towards Trustworthy Machine Learning: Exploring and Addressing Emerging Threats to Security, Privacy, and Safety.
- Alyssa Gerhart, from Benedict College speaking on Saving AI from Itself: Defending Healthcare Systems Against Adversarial Threats.
- Dr. Abdullah Al Mamun, from Clemson University speaking on Future-Proofing Transportation Cyber-Physical Systems: The Role of Post-Quantum Cryptography.
- Tosin Jimoh, from Benedict College speaking on Autoencoders vs FGSM: Comparison of Machine-Learning Models for Detecting Adversarial Perturbations in Image Classification
- Dr. M. Sabbir Salek, from Clemson University, speaking on Cyber Resilience in Transportation: Navigating Quantum Computing Opportunities

TraCR students also actively participated in the poster session, with two students receiving the best poster awards as shown above.

CONTACTS

That's It for Now!

Stay tuned for our next newsletter in the fall of 2025.
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