TraCR ADVANCES

SPRING 2024

Director's Message

Dr. Mashrur "Ronnie" Chowdhury

As the Director of the National Center for Transportation Cybersecurity and Resiliency, or TraCR, it brings me great pleasure to present our latest updates and accomplishments. Our mission to advance transportation cybersecurity and resiliency is at the core of everything we do. Through innovative research and collaborative efforts, we aim to push the boundaries of knowledge in this rapidly evolving frontier.

I'm happy to share that we had our inaugural TraCR conference on May 6-7, 2024, at the Clemson University International Center for Automotive Research (CU-ICAR) in Greenville, SC. This event facilitated engaging discussions, generated fresh insights, and provided valuable networking opportunities for researchers and industry professionals. We will share more updates from the conference in our next newsletter.

This year, we've funded fourteen innovative projects at our nine partner institutions, broadening our research portfolio and demonstrating our commitment to hardening the nation's transportation systems by developing state-of-the-art technologies, policies, and practices. In this newsletter, you'll find summaries of these projects, which showcase the innovative work being done across the TraCR community.

I'm particularly proud to highlight some notable research advances achieved by our team. From enhancing 3-D object detection for tackling security threats to developing cutting-edge security solutions for autonomous vehicles, our researchers continue to break new ground and address complex challenges head-on.

As we look to the future, I'm excited about the opportunities ahead of us. Together, let's keep pushing the boundaries of knowledge, fostering collaboration, and making a lasting impact on transportation cybersecurity and resiliency.

In this Issue:

Newly Funded PROJECTS

This spring, TraCR awarded funding to 14 new research projects. These projects focus on technologies ranging from connected and autonomous vehicles (CAVs), to cybersecured autonomous navigation, to quantum AI-based approaches to combatting cyberattacks, to deep learning-based optimization of eco-driving strategies and much more. These projects were made possible through funding from the U.S. Department of Transportation through the University Transportation Centers program.

Intersectionality of Infrastructural Cybersecurity, Digital Equity and Social Agency

Lead Principal Investigator: Dr. Asha Layne (Morgan State University)

The COVID-19 pandemic exposed various cybersecurity threats as more people relied on digital communication modes to survive socially and financially. Many of these threats were associated with social inequalities. Significantly, the "digital divide" negatively affected the knowledge economy and knowledge management in urban areas, impacting economic production and opportunities. Coined by Wendy Nather, the term "security poverty line" explains that organizations that do not have enough money to obtain significant security are the most vulnerable, and because new security information is constantly emerging, they will remain vulnerable.

Despite recent research efforts, the breadth of digital disparity is still not widely known. These have examined the lack of racial or gender diversity in cybersecurity and criticized the systemic issues in the cybersecurity discourse. These can be primarily attributed to the inability of traditional cybersecurity studies to link social equity with technological knowledge. As the digital divide exposed higher rates of digital dis-connectivity among inner-city residents, we cannot overlook how it exacerbated the gaps in education, healthcare, and transportation services, to name a few.

This project's research is necessary because limited studies explore cyber insecurity among at-risk populations. Furthermore, conversations about transportation development and access must focus on infrastructural cybersecurity issues affecting marginalized populations, such as broadband access and digital literacy. To better address the issue of cyber insecurity, it is crucial to examine cybersecurity through an intersectional lens. The work this project produces will focus on allowing users with diverse and at-risk backgrounds to express their understanding and knowledge of cybersecurity while exploring the nature and impacts of any cybersecurity challenges they encounter. Therefore, the results will contribute to the existing literature that deals with the causes and characteristics of the digital divide, specifically examining how geographic restrictions and a lack of affordable transportation options impede access to cybersecurity training or workshops.

Cybersecurity Testbed for Connected and Autonomous Vehicles

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

Many state and local administrators have vowed to advance transportation systems by enhancing autonomy and connectivity. While integrating new technologies and algorithms into transportation holds promise for promoting efficiency and safety, it also introduces vulnerabilities. Previous research has demonstrated viable attacks on connected and autonomous vehicles (CAVs), such as GPS spoofing and tactics involving the manipulation of traffic signals. However, most studies are based on small-scale scenarios (e.g., one vehicle, one intersection, or one link), which can only reflect the local and limited impact

of the attacks. A faithful testbed capable of handling multi-scale system dynamics is needed to comprehensively evaluate the threats associated with cyberattacks against CAVs, and, further, to judge whether specific defense mechanisms effectively address a threat. This project aims to develop a sophisticated testbed capable of assessing the multi-scale impact of cyber-attacks against CAV fleets. Unlike existing testbeds, this project will adopt a co-simulation framework to model multi-scale system dynamics resulting from V2X communication, vehicle maneuvering, and car-following, as well as vehicle scheduling, routing, and network-level cascading congestion effects. Ultimately, this project aims to construct a reliable environment as a foundational platform for future cybersecurity studies.

Secure and Privacy-Preserving Federated Learning for Connected and Automated Vehicles

Lead Principal Investigator: Dr. Mohammadhadi Amini (Florida International University)

There is a significant dearth of systematic methods for monitoring autonomous transportation systems, specifically connected and automated vehicles (CAVs), in the face of adversarial cyber-attacks and privacy leakages. Hence, new technical and domain-specific challenges must be addressed. This will be done by developing effective privacy-preserving and secure decision-making algorithms that can detect threats and protect CAVs against them while at the same time ensuring data privacy.
This project aims to deploy, integrate, and validate privacy-preserving and secure learning solutions for CAVs by producing four main outputs:

- An integrated anomaly detection technique to identify and isolate backdoor attacks in federated CAV learning settings;
- A novel approach to cyber-defense that maintains concrete security against backdoor attacks in CAV applications;
- A privacy preservation mechanism to ensure CAV data is protected against data leakage,
- Learning models that will be trained using real-world and synthetic CAV data for assessment and validation purposes.

This project will thus develop a distributed learning architecture to serve as a platform for future projects, such as work that will develop and evaluate other privacy-preserving techniques for intelligent transportation systems.

A Multi-Resolution Simulation Platform for Transportation System Security Testing and Evaluation

Lead Principal Investigator: Dr. Yiheng Feng (Purdue University)

Due to the nature of transportation cybersecurity problems, it is usually too risky to evaluate attack and defense models in real-world environments. Therefore, it is necessary to develop a simulation environment to validate proposed models and evaluate the impact of cyber threats on transportation safety and mobility. However, existing simulation tools suffer from the following limitations, including:

- Single modality: For example, SUMO is a popular microscopic traffic simulation tool but is limited in modeling vehicle-level behaviors (e.g., perception and path planning). On the other hand, CARLA can mimic autonomous vehicle functions but lacks realistic road network construction and traffic level behaviors.

- No cybersecurity component: Some simulators integrate multiple levels of simulation details, but they do not have the capabilities to conduct cybersecurity-related simulation analysis.
- No transportation applications: A few simulation platforms developed for cybersecurity research only mimic lower-level security functions but lack the capacity to simulate transportation impacts. For example, the VASP platform mainly focuses on simulating V2X communication network level attacks (e.g., security credential management, V2X messages) attacks but has limited functions in replicating traffic-level applications.

In this project, a multi-resolution simulation platform will be built to test and evaluate the cybersecurity of transportation systems. It will be built on an open-source co-simulation environment for cooperative driving automation (CDA) developed by the FHWA. Based on the co-simulation environment, APIs will be developed to support various attack scenarios, including sensor attacks, data spoofing attacks, infrastructure attacks, vehicle-level attacks, and network-level attacks. Further, the impact of these attacks on V2X infrastructure applications, machine learning algorithms, and network routing applications will be investigated.

Reinforcement Learning-Assisted Virtualized Security Framework for CAVs

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

Connected and autonomous vehicle (CAV) technology is bringing about a major transformation in transportation by significantly improving the mobility of people and goods through advanced communication, sensing, and computing capabilities. However, CAVs can be hacked due to vulnerabilities in the in-vehicle software, resulting in physical damage and jeopardizing the safety of drivers and passengers. By exploiting vulnerabilities, hackers can perform malicious actions ranging from draining batteries to taking control of the steering wheel to disabling the alarm system. The existing security solutions implemented in CAVs are static and cannot withstand evolving security threats such as advanced persistent threats (APTs) and ransomware attacks. Moreover, costly update procedures can leave the CAV software unpatched for a long time, making the CAVs vulnerable to new exploits. This project aims to develop a virtualized security framework to improve the resiliency of CAV software. The framework will allow the execution of different code variants of CAV software to introduce uncertainty in the attack surface. It will integrate the Network Functions Virtualization paradigm to implement the code variants of CAV software as virtual network functions and will offer the ability to optimally deploy the appropriate virtual network functions using a reinforcement learning agent. The agent perceives the threat environment of CAVs and provides the optimal code variant that maximizes the resiliency of CAV software while ensuring it meets its Quality of Service (QoS) requirements.

This project aims to accomplish the following goals:

- Develop a virtualized security framework that allows fast and dynamic provisioning of different code variants of CAV software,
- Design novel and efficient algorithms designed based on game theory and Artificial Intelligence (AI) techniques including Deep Learning and Generative Adversarial Networks (GANs) to determine the optimal code variant,
- Evaluate the performance of reinforcement learning algorithm using simulations,
- Build a proof-of-concept of the proposed security framework and evaluate its performance using real-world experiments.

Newly Funded PROJECTS

Policy Analysis and Guidance to Support Secure Transportation Cyber-Physical-Social Systems

Lead Principal Investigator: Dr. Steven Jones (The University of Alabama Tuscaloosa)

Rapidly evolving, advanced transportation systems rely on automation and communication technologies. These integrate and optimize our systems for moving goods and people, equitably advancing society. However, the more we rely on automation and connectivity, the more we give malicious actors unprecedented opportunities to steal data, invade privacy, demand ransom, generate misinformation, and attack the systems on which our lives, prosperity, and security depend. Although regulatory and enforcement measures are needed, no U.S. federal law or regulatory framework governs cybersecurity or data privacy, focusing on transportation. Innovative but legally unprecedented technological advances are creating policy issues for legislative and regulatory bodies in a world of automated mobility. These include problems surrounding the amount, nature, and potential exploitation of data collected from connected transportation systems. Perhaps most concerningly, current cybersecurity regulations overwhelmingly fail to require or even encourage machine learning and predictive analysis to understand privacy threats, cyberattacks, and data theft. The unregulated use of such technologies can even raise equity and discrimination issues. This project attempts to answer two questions:

- What federal and/or state agencies are responsible for governing cybersecurity practices in the U.S., including risk assessment, preventative measures, detection of breaches, and remedial enforcement?
- How do industry experts assess the greatest risks/threats to cybersecurity in the transportation sector?

The project will focus on performing a nationwide survey of existing federal and state cybersecurity and privacy regulatory measures and analyze the legislative landscape, considering identified risks and threats to the transportation industry. The results will then be analyzed using natural language processing methods to identify inconsistencies and gaps in the nation's cybersecurity policy and what the industry indicates needs to be cybersecure. Finally, this analysis will be used to develop a policy guidance document and/or toolkit to share with stakeholders who wish to develop and implement effective cybersecurity legislation, regulations, policy, and governance.

Hybrid Classical-Quantum AI Approach for Detecting Cyberattacks in Vehicles

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

This project aims to develop a hybrid classical-quantum machine learning library to detect vehicle cyberattacks. By leveraging quantum supremacy, the library could improve the speed of training and the accuracy of intrusion-detection systems. Specifically, the performance of the quantum neural network in feature extraction and feature analysis will be analyzed. After understanding this performance, a hybrid classical-quantum architecture that generates the best performance will be sought. In addition, hybrid libraries in different quantum devices, including superconducting and optical quantum computers, will be tested. Different quantum error mitigation techniques based on different quantum devices will be included in the project's library. Moreover, a tensor network approach will be developed to improve the training efficiency of the variational quantum circuits. In sum, the research focuses on investigating the architecture of the hybrid system and the optimization method in training. With the library developed by the project, various vehicle cyberattacks will be detected, improving driving security.

Newly Funded PROJECTS

Finding Vulnerabilities of Autonomous Vehicle Stacks to Physical Adversaries

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

Autonomous driving (AD)-enabled vehicles must interact with and respond in real-time to multiple sensor signals, indicating how other autonomous robots, targets, and the environment behave near the ego vehicle. While autonomous vehicle (AV) developers tend to generate numerous test cases in simulations to detect problems, to the best of our knowledge, they are not testing for malicious physical interactions from attackers. For example, a technique whereby a hostile driving maneuver causes a victim vehicle to crash, while the malicious vehicle does not crash, could be identified by malicious actors and reproduced and spread worldwide, causing traffic accidents for vehicles with vulnerable AD stacks.

TraCR members recently introduced two frameworks to explore adversarial driving maneuvers, a new class of physical attack against AD software. Here, the attacker aims to find a (plausible) trajectory near the victim's vehicle to cause it to behave unintendedly, such as crashing or driving off the road. The frameworks differ in their assumptions about the attacker and the target AV software components. However, both frameworks provide an overview of the challenges, a means of discovering adversarial driving maneuvers in practice, and potential solutions to defend against them. While both frameworks are effective to some extent in discovering adversarial driving maneuvers against a variety of AD software, the research on adversarial driving is still in its early stages. This project will explore the weaknesses and strengths of both frameworks. Guided by the findings, the project will pursue a unified framework leveraging the best ideas and exploring rigorous measures for building a safe and secure AD software stack

Privacy-Preserving Transportation Data Analytics Using Synthetic Data Generation

Lead Principal Investigator: Dr. Murat Kantarcioglu (The University of Texas at Dallas)

Large-scale user data collection has enabled various new services to improve transportation with crowdsourced vehicle routing applications or public transit metrics. This fine-grained user data benefits society but raises privacy concerns since attackers can obtain location and trajectory data from various users. Researchers need realistic data to perform experiments that can improve the efficiency of transportation systems; however, the sensitive nature of these data, which can include personally identifiable information, often prevents them from being openly shared or utilized for broader research and the public benefit. Thus, while transportation data hold significant potential for improving infrastructure and services, privacy considerations create a barrier that must be carefully navigated.

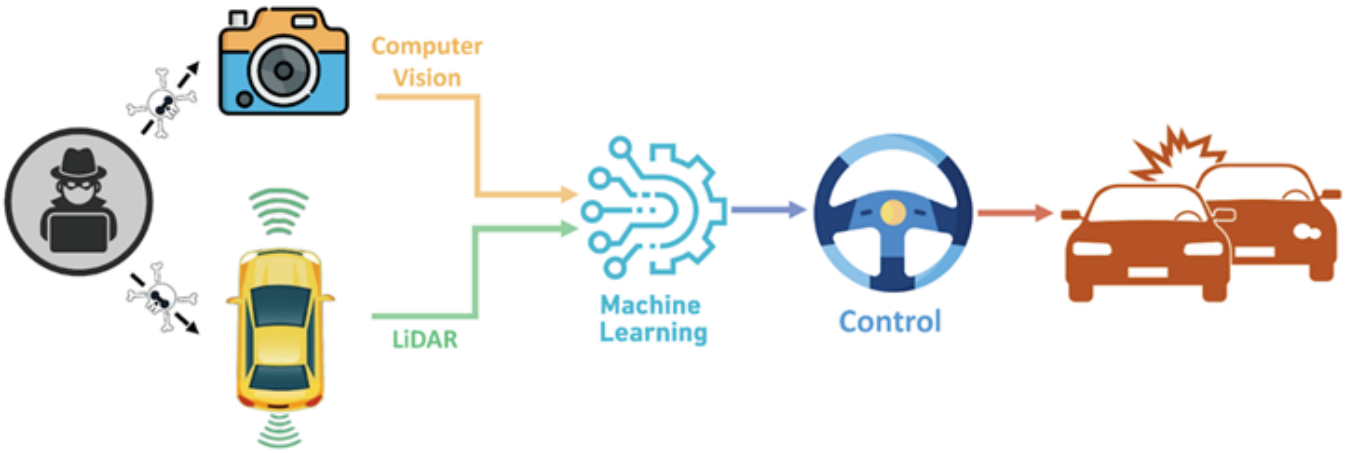
Privacy-preserving synthetic data generation represents a promising avenue for addressing the challenges of sharing transportation data. It can be engineered to retain the essential characteristics and statistical properties of the original dataset while removing or altering information that could compromise individual privacy. This approach enables researchers, policymakers, and urban planners to gain valuable insights into transportation patterns, traffic congestion, and infrastructure needs without violating individual privacy. This project focuses on developing novel privacy-preserving synthetic transportation data generation techniques.

Newly Funded PROJECTS

Identifying and Patching Vulnerabilities of Camera-LiDAR Based Autonomous Driving Systems

Lead Principal Investigator: Dr. Cihang Xie (The University of California, Santa Cruz)

The rise of autonomous vehicles (AVs) is transforming the transportation sector, potentially enhancing road safety, optimizing traffic flow, and bringing about a more sustainable future. Central to this revolution lie two interlinked technological keystones: integrating advanced sensor systems and applying cutting-edge machine-learning techniques. Specifically, the fusion of high-resolution imagery from cameras and the depth precision of Light Detection and Ranging (LiDAR) sensors can equip AVs with unparalleled perceptual prowess, allowing them to capture a holistic, 360-degree spatial awareness of their surroundings. Subsequently, machine learning algorithms transform the sensor data into actionable insights, empowering the vehicle to make accurate and informed driving decisions. But while machine learning algorithms help autonomous driving systems exhibit remarkable capabilities in recognizing patterns and making decisions, they also harbor an Achilles' heel — adversarial vulnerability. It has been previously shown that attacks can lead the vehicle into misrecognizing traffic signs, misjudging obstacles, or misinterpreting road conditions. Such vulnerabilities pose profound safety risks, as malicious actors could exploit them to induce unintended behaviors in AVs, potentially leading to hazardous situations.



This project aims to provide a multi-dimensional security analysis for advanced autonomous driving systems. It focuses on Bird's Eye View (BEV) — a cutting-edge, 3D perception system now gaining traction in real-world self-driving systems. The perceptual capabilities of this system will be further enhanced via integration with LiDAR signals. It is noteworthy that despite its growing prevalence in modern AVs, the BEV system remains a relatively untapped area in adversarial machine learning research. Moreover, beyond merely focusing on threats that fool AVs' perception system to recognize objects of interest incorrectly, this project is oriented towards adversarial scenarios where attackers can induce tangible, real-world disruptions — such as instigating traffic congestion or triggering vehicular collisions, especially when interacting with other dynamic agents like vehicles or pedestrians.

Newly Funded PROJECTS

Building a Secure Electronic Control Unit Hardware Platform for Connected Vehicles

Lead Principal Investigator: Dr. Zhenkai Zhang (Clemson University)

This project aims to develop a secure Electronic Control Unit (ECU) hardware platform for connected vehicles utilizing the Reduced Instruction Set Computing 5th version (RISC-V) architecture. The core innovation lies in integrating the Trusted Execution Environment (TEE) and Moving Target Defense (MTD) into the ECU. The project tasks include:

- Tailoring the Keystone TEE: The researchers will adapt the Keystone TEE specifically for ECU applications. This task involves creating a new firmware-level security monitor optimized for the controller area network (CAN) bus to enable device authentication and message encryption. The team will also modify FreeRTOS to function as the enclave runtime, efficiently managing resources.
- Implementing a Randomization Module: A randomization module will be incorporated within the RISC-V core to facilitate MTD. This step will include modifying the core to include instruction set randomization logic and developing a new firmware-level configuration manager.
- Developing a Recovery Mechanism: A key project component is developing a robust recovery mechanism to ensure uninterrupted vehicle operations during an attack. This will involve setting up a fail-safe enclave that contains backup programs for each essential controller and integrating a recovery module within the configuration manager to activate these backup controllers as needed.

Moreover, the proposed platform on field programmable gate array (FPGA) boards will be implemented to demonstrate effectiveness against potential attacks in environments created by autonomous vehicle simulators. In sum, this project aims to provide a comprehensive hardware solution capable of protecting connected vehicles from a range of cyber threats, even in the presence of software vulnerabilities.

A Zero Trust Architecture for Secure Connected and Autonomous Vehicles

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

Connected and Autonomous Vehicles (CAVs) are the future of personal and public transportation. Security has become a pressing concern as CAVs increasingly rely on cyber-based control, navigation, and communication. The complexity and inter-connectedness of CAVs offer myriad opportunities for security compromise, potentially resulting in unsafe operation or leakage of confidential information about the user. Zero Trust Architectures (ZTA) for networks have emerged as a fundamentally new way of approaching security. It offers new paradigms for defining and enforcing policy through various means rooted in modeling trust relationships. The zero-trust security model does not automatically trust any user or device inside or outside the network perimeter. Instead, it enforces a set of policies (i.e., rules that are dynamically maintained and enforced) to verify and ensure the security of resources. ZTA can aid in reducing potential risks to CAVs by guaranteeing that only approved users and devices can access sensitive systems and data. This project will investigate how ZTA can be adapted to CAVs to provide fundamental protection for individual components within CAV systems and their supporting infrastructure.

Newly Funded PROJECTS

Multimodal In-Vehicle Sensor Fusion for Cyber-Secured Autonomous Navigation

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

Successful navigation of autonomous vehicles relies on positioning, navigation, and timing (PNT) services. Global Navigation Satellite Systems (GNSS),such as GPS (USA), BeiDou/BDS (China), Galileo (Europe), GLONASS (Russia), IRNSS/NavIC (India), and QZSS (Japan) provide PNT services. However, GNSS signals are vulnerable to unintentional interference (e.g., jamming caused by walls and ceilings in garages and tunnels, and multipath issues due to high-rise buildings in urban areas) as well as deliberate cyber threats(e.g., jamming and spoofing of GNSS signals). Prior research shows that multi-sensor fusion systems could use different sensors — i.e., GNSS with an inertial measurement unit (IMU) and perception sensors (PS) (e.g., camera, LiDAR, RADAR) — to complement each other, correcting individual sensor outputs and determining reliable navigation solutions under deliberate threats and in GNSS-denied environments (e.g., GNSS outage, INS error accumulation issues, and/or PS view obstruction). However, IMU and PS can only provide relative positioning and rely on GNSS for absolute positioning. Advanced INS (GNSS+IMU) provides cm level accuracy; however, during a GNSS outage, position errors could accumulate up to 3.8 meters in just one minute due to the error accumulation of inertial sensors. Thus, a major research gap is our inability to comprehensively identify and understand GNSS vulnerabilities in autonomous vehicles, investigate realistic attack modeling and detection, and develop cyber-resilient navigation solutions for GNSS-based navigation. This project aims to understand the vulnerabilities of GNSS-based navigation, develop intelligent slow-drifting cyberattacks, create corresponding attack detection models, and devise cyber-resilient navigation solutions to enhance the GNSS-based navigation system.

The research will:

- Investigate and develop intelligent slow-drifting GNSS spoofing attacks by manipulating GNSS signal's navigation data;
- Investigate and develop GNSS cyber-attack detection algorithms for slow-drifting GNSS spoofing attacks; and
- Develop a secure in-vehicle sensor fusion-based navigation module using deep fusion algorithms during a GNSS-denied environment.

The outcomes of this project will be the implementation and validation of intelligent slow-drifting GNSS spoofing attack models using a GNSS receiver in both laboratory and real-world environments, in order to evaluate algorithms that detect such attacks through field testing. Further, the project will demonstrate proof-of-concept of an in-vehicle sensor fusion-based cyber-resilient navigation solution in a controlled, real-world environment.

Newly Funded PROJECTS

Secured Small-Key-Based Post Quantum Cryptographic Scheme for Blockchain-Based VANET

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

Blockchain-based Vehicular Ad-Hoc Network (VANET) architecture has been gaining popularity due to its distributed and decentralized architecture, efficient data transmission capability, and secure data generation and broadcasting ability over VANET networks. Blockchain's trust management system could ensure privacy-protected and secured vehicle-to-everything communication because of its ability to ensure the veracity of the exchanged messages via a digital signature of a message sender (e.g., a vehicle). However, due to the high mobility of vehicles, small key-based encryption is necessary in VANET as it requires less complex computational operations and storage.

Existing studies prove that a non-quantum computing-based or classical attack cannot generate a cyber attack on blockchain-based VANET because blockchain can identify the attacker through consensus-based or rating-based mechanisms, hashing, encryption, and the distributed nature with transparency in the public ledger-based approach. The blockchain-based architecture relies on two cryptographic mechanisms to provide security and trust:

- Checking the integrity of the data itself using hash functions and
- Checking the ownership of the data with asymmetric cryptography.

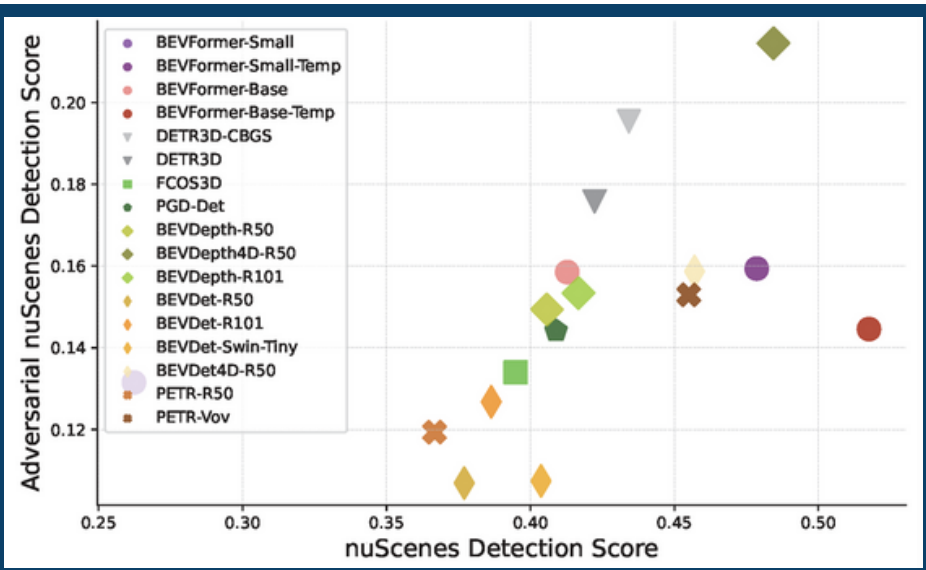
However, if a quantum algorithm can break the hash function or the cryptographic algorithm, it can create security concerns for any secure communication architecture. Although prior studies have been conducted on improving the ownership mechanism of blockchain and making it quantum-safe through post-quantum cryptography and quantum key distribution, post-quantum cryptography suffers from periodicity and symmetry. It uses large-size keys, which increase the complexity of the decryption of the key, such as a lattice-based architecture. Hash-based cryptography and multivariate cryptography exhibit a drawback regarding large signature sizes, leading to a larger block size and, consequently, larger memory size. Similarly, code-based cryptography encounters the issue of increasing complexity due to larger key sizes, demanding extensive memory storage, and the risk of decoding failures when utilizing smaller keys in specific scenarios.

Therefore, a novel lightweight Post Quantum Cryptographic (PQC) solution, which could adapt to the dynamic VANET scenario and ensure security against quantum-based attacks, is needed according to the US NIST's cybersecurity framework. This project aims to develop a new small key-based PQC solution for VANET, the Diophantine Isogeny Key Exchange (DIKE) scheme, to ensure security against quantum-based attacks. Specifically, the objectives of this project are to:

- Develop and implement a quantum-based attack model utilizing both quantum Shor's and Grover's algorithms on a blockchain-based VANET, which will highlight the need for a quantum-secured blockchain and
- Formulate a new PQC solution, DIKE, which integrates Diophantine equations and isogenies to provide a secure key exchange mechanism that is resilient against quantum attacks.

On the Adversarial Robustness of Camera-Based 3D Object Detection

Shaoyuan Xie, Zichao Li, Zeyu Wang, Cihang Xie



Vision-based Bird's Eye View (BEV) perception has emerged as a promising approach for autonomous driving, striking a favorable balance between cost and performance compared to LiDAR and monocular camera-based detection systems. This research provides a comprehensive adversarial vulnerability analysis of these vision-based BEV detection models. Specifically, by conducting a range of attacks, including PGD-Attack, FGSM-Attack, C&W-Attack, and AutoPGD, it was revealed that, despite their advanced capabilities, these algorithms are easily compromised by pixel perturbations and adversarial patches, undermining their classification and localization accuracy.

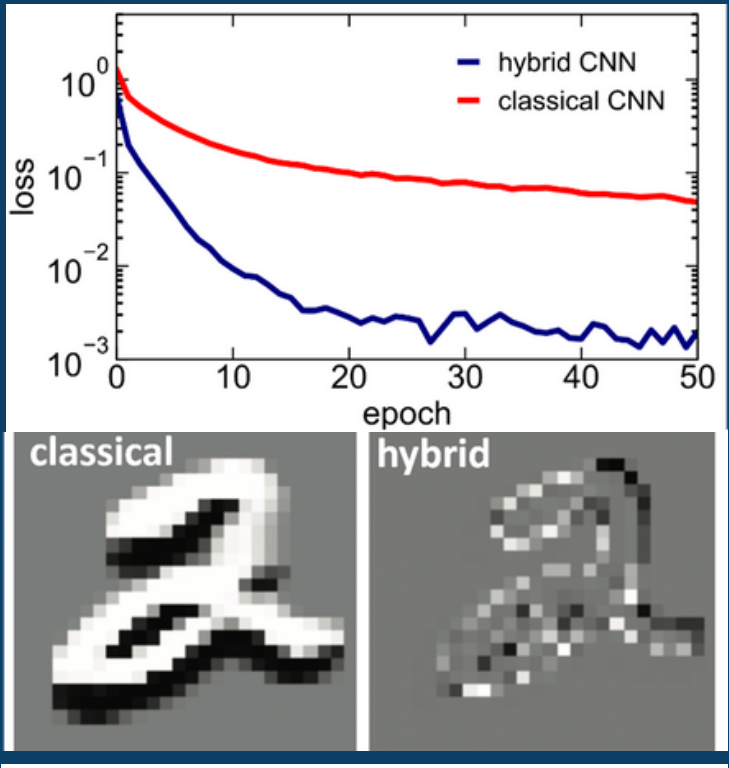
A key finding of the study is that BEV models do not inherently possess stronger robustness against adversarial attacks than monocular approaches. Interestingly, precise depth estimation, crucial for the perspective of BEV transformation, is a pivotal factor in enhancing robustness for models with explicit depth estimation. This observation also highlights the robustness potential of transformer-based frameworks, which bypass the need for explicit depth estimation through implicit view transformation and information aggregation. Furthermore, incorporating temporal information enhances model performance and paradoxically expands the attack surface. Separately, the discovery of universal adversarial patches presents a different challenge, which is capable of affecting various objects, backgrounds, and models. This indicates a significant security risk in real-world applications, underscoring the complexity of ensuring robustness in BEV detection systems.

In summary, this research calls for a heightened focus on adversarial robustness in designing BEV detection models, emphasizing the need for comprehensive security measures to mitigate these vulnerabilities in practical settings. It paves the way for future research to make autonomous vehicles more robust against sophisticated cyber-physical threats.

Click for more information on the article

Quantum-Inspired Activation Function in the Convolutional Neural Network

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



Training loss and feature selection for classical and hybrid quantum-classical convolutional neural networks

Quantum supremacy, including exponential information storage, quantum speedup, and better solutions to NP problems, has spurred extensive research on meaningful applications, especially in machine learning. To harness this supremacy, we developed a hybrid quantum-classical convolutional neural network library and applied it to classify handwritten digits using the MNIST dataset. Compared to the classical convolutional neural network, the hybrid approach provided a faster convergence in the loss function, which is attributed to the expedited selection of crucial image features. However, the current quantum computing landscape has a limitation: the bandwidth, in terms of the number of operations per second. In our envisioned future quantum computer, the peak input-output (I/O) bandwidth could reach 10 Gbit/s, which is considerably less than the I/O bandwidth offered by existing NVIDIA A100 GPU chips for classical computing. This constraint poses a significant obstacle to accelerating the training process of quantum AI models, particularly those needing access to several terabytes of data.

To confront this challenge, we conducted an in-depth analysis to uncover the source of the expedited feature selection we observed for our hybrid quantum-classical approach. This led us to find a generalized efficient quantum-inspired activation function that can be used in classical computers but could provide the expedited feature selection of the hybrid approach. Notably, this quantum-inspired activation function can be seamlessly integrated into popular machine learning libraries, such as Tensorflow and PyTorch, without incurring additional costs.

Integrating this quantum-inspired activation function empowers classical computers to harness the benefits of quantum supremacy without suffering from the I/O limitation of our near-term quantum computers. This strategy could be utilized for a broad array of machine learning application areas, including but not limited to autonomous vehicles, cybersecurity, healthcare, and finance.

Click for more information on the article

Multimodal In-Vehicle Sensor Fusion for Cyber-Secured Autonomous Navigation

Mizanur Rahman, Mashrur Chowdhury, Long Cheng

Real-world Experiments in a Controlled Environment

Successful mission execution and the navigation of autonomous vehicles rely on accurate and reliable Global Navigation Satellite Systems (GNSS)-based positioning, navigation, and timing (PNT) services. However, GNSS signals are inherently weak (often compared to the visibility of a 25-watt light bulb from a distance of about 20,000 kilometers) and vulnerable to unintentional interference and deliberate cyberthreats. Unintentional interference includes jamming caused by buildings, walls, tunnels and other large physical structures, multipath issues due to high-rise buildings in urban areas, atmospheric effects like scintillation and solar flares, and GNSS segment errors resulting from signal distortion, delay, orbit, or clock error. These unintentional interferences are dynamic in nature and create uncertainties in autonomous vehicle navigation. Deliberate cyber threats could include spoofed (fake) GNSS signals that mimic legitimate signals, leading to receivers obtaining inaccurate positions and timing information. In addition, deliberate jamming can flood the surrounding area with high-power radio signals in frequency bands close to those of GNSS signals, causing the receiver to lose its accurate positioning. Thus, deliberate cyber threats exponentially increase the uncertainties in PNT services.

This project aims to investigate the vulnerabilities of GNSS-based navigation models to intelligent, slow-drifting cyber-attacks, develop corresponding attack detection models, and devise an alternative cyber-resilient navigation tool leveraging multimodal in-vehicle sensor fusion approaches for autonomous ground vehicles. A proof-of-concept showcasing a multimodal in-vehicle-sensor fusion-based cyber-resilient navigation solution will be demonstrated in a controlled, real-world setting. Upon completion, industries related to autonomous ground vehicles could adopt GNSS cyber-attack detection algorithms and alternative cyber-resilient navigation tools to protect and navigate autonomous vehicles in GNSS-compromised and contested environments.

Recorded 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

INTEGRATING CYBER SECURITY AND MACHINE LEARNING FOR APPLICATIONS IN TRANSPORTATION SYSTEMS

Bhavani Thuraisingham, Ph.D.
Founders Chair Professor, Department of Computer Science
The University of Texas at Dallas

PREVENTING, DETECTING, AND RESPONDING TO ATTACKS AGAINST AUTONOMOUS VEHICLES

Alvaro A. Cardenas, Ph.D.
Associate Professor, Department of Computer Science and Engineering
The University of California, Santa Cruz

MASTERING SCIENTIFIC COMMUNICATION IN THE DIGITAL AGE: STRATEGIES AND TOOLS FOR CAPTIVATING PRESENTATIONS AND ARTICLES IN A TIKTOK-DOMINATED WORLD

Rachelle Beckner
Lecturer, Clemson University

ADVANCES IN QUANTUM CRYPTOGRAPHY AND NEXT GENERATION QUANTUM INTERNET

Paul Wang, Ph.D.
Chair and Professor of Computer Science
Morgan State University

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

Upcoming EVENTS

2024 CUTC Summer Meeting - June 10-12, 2024

The 2024 Council of University Transportation Centers (CUTC) Summer Meeting is being hosted by the University Transportation Center for Railway Safety (UTCRS) at the University of Texas Rio Grande Valley (UTRGV) at the South Padre Island, Texas from June 10-12, 2024. The CUTC represents the nation's leading university-based transportation research and education programs. The CUTC members work to advance the state of the art in all modes and disciplines of transportation. Don't miss out on this excellent opportunity to connect with transportation professionals and researchers. Register now!

Find more information and register here!

USDOT Future Of Transportation Summit - August 13-15, 2024

The 2024 USDOT Future Of Transportation (FoT) Summit is scheduled for August 13-15, 2024, at the USDOT Headquarters in Washington, D.C. The event will include keynotes from prominent speakers, including USDOT and other federal agency leaders, and presentations, posters, and demonstrations by several USDOT UTCs (University Transportation Centers). The program also includes multiple panels featuring leaders from Congress, industry, nonprofit organizations, investors and other stakeholders.

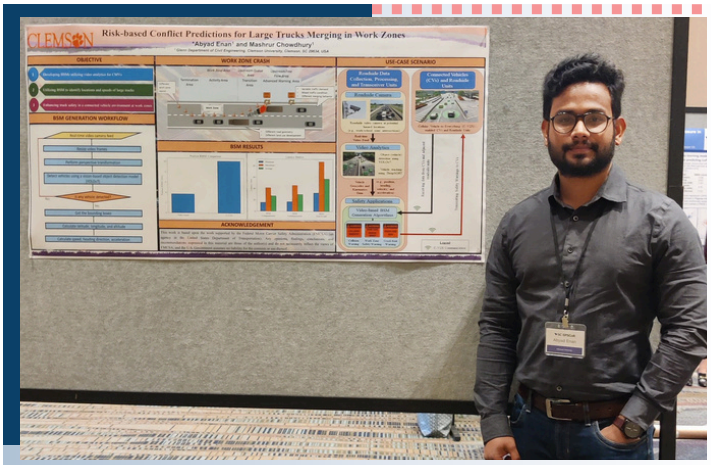
Find more information and register here!

ACHIEVEMENTS

Dr. Mizanur Rahman, TraCR member, has received the prestigious Faculty Early Career Development (CAREER) Award from the National Science Foundation (NSF). Dr. Rahman is an assistant professor in the Department of Civil, Construction and Environmental Engineering at the University of Alabama (UA), Tuscaloosa. He will receive $536,016 over five years from NSF's Secure & Trustworthy Cyberspace program. With the award, Dr. Rahman aims to advance the discovery of fundamental dynamics in cyber threat uncertainties for autonomous navigation under evolving attack surfaces, and in formulating a robust, efficient, flexible, and reliable positioning and navigation system. Dr. Rahman's education plan addresses the increasing demand for a future cybersecurity workforce by exposing engineering students to cybersecurity knowledge and skills, and by inspiring engineering and K-12 students through game-based learning platforms to think beyond traditional cybersecurity solutions in addressing grand engineering challenges holistically.

Dr. Ronnie Chowdhury received the Clemson University's 2024 Frank A. Burtner Award for Excellence in Advising. This award is presented to an advisor who excels in developing students in the areas of leadership, devotion to duty, and service. Additionally, Dr. Chowdhury received the 2024 Senior Researcher of the Year Award from Clemson University.

Student Recognition



Abyad Enan, a Ph.D. student in the research group of TraCR Director Dr. Ronnie Chowdhury, won second place Poster Presentation Award at annual SC EPSCoR State Conference scheduled for April 9th, 2024, in Columbia, SC. The primary objective of the SC EPSCoR State Conference is to unite South Carolina faculty, postdoctoral fellows, graduate and undergraduate students, and STEM professionals, fostering networking and encouraging collaborative efforts. Abyad is currently working toward his Ph. D. degree in the Glenn Department of Civil Engineering under the supervision of Dr. Mashrur "Ronnie" Chowdhury. His research focuses on Transportation Cyber-Physical Social Systems, Transportation Cyber Security, and Quantum Computing.

OUTREACH

Dr. Chowdhury and Clemson's TraCR Team with visitors from the Habitat for Humanity and Goodwill showcasing cybersecurity technologies

Habitat for Humanity - TraCR Visit

TraCR hosted a technology demonstration for visitors from Habitat for Humanity and Goodwill on February 19th, 2024. The day started with a presentation from Dr. Ronnie Chowdhury, the TraCR director. Attendees were introduced to transportation cyber-physical-social systems (TCPSS) and self-driving cars. The attendees learned about: (1) hybrid classical-quantum deep learning models to detect adversarial attacks that affect the performance of the perception module of autonomous vehicles, (2) virtual traffic signal control with cloud-based quantum computers, and (3) distributed machine learning models or environmental emission detection with unmanned aerial vehicles.

TRB Annual Conference

Several TraCR members participated in the 103rd TRB Annual Conference, from January 7-11, 2024 in Washington, D.C. Staff and students presented their research findings, engaged in discussions, and networked with professionals in the transportation field. TraCR Associate Director Dr. Steven Jones and Senior Engineer Dr. M Sabbir Salek presented at the Cybersecurity Subcommittee meeting on January 10th, engaging in a fruitful and constructive exchange with the experts. We thank all TraCR members, especially our students, for their active participation.

OUTREACH

SC EPSCoR Conference

TraCR organized a session entitled "Cybersecurity: Threats and Opportunities" at the annual SC EPSCoR State Conference on April 9th, 2024, in Columbia, SC. The primary objective of the SC EPSCoR State Conference is to unite South Carolina faculty, postdoctoral fellows, graduate and undergraduate students, and STEM professionals, fostering networking and encouraging collaborative efforts. The session organized by TraCR and moderated by Dr. Chowdhury harmonized seamlessly with the center's mission of the USDOT-funded center by featuring talks from:

- Dr. Zhenkai Zhang, Assistant Professor, Clemson University, focusing on computer systems security, especially hardware security and cyber-physical/real-time/embedded systems.
- Mr. Rick Siebenaler, who is heading up SC's newly formed Maritime Cybersecurity Institute and serving as the CEO of a related NSF-funded SC initiative on maritime (and related intermodal) cybersecurity innovation.
- Mr. Leon Geter, Interim Dean, School of Communication, Arts, and Social Sciences (CASS), Benedict College.

Men of Color Summit

TraCR led a session highlighting careers in quantum information systems at The Men of Color National Summit organized by Clemson University. The summit aims to narrow the educational disparity among African American and Hispanic males in colleges. The summit is a nationwide platform for students and professionals to convene, engage with expert speakers, and motivate one another. This year's event on April 11th at the Greenville Convention Center in Greenville, SC, marked the seventh iteration of the summit. The summit drew over 2,000 attendees, including high school and college students, business professionals, educators, government officials, and industry leaders, the two-day conference promises valuable insights and networking opportunities.

CONTACTS

That's It for Now!

Stay tuned for our next newsletter in the summer of 2024.
In the meantime, please follow us on our social media pages, including Twitter, 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

Contact