TraCR ADVANCES

FALL 2024

Director's Message

Dr. Mashrur "Ronnie" Chowdhury

Welcome to the third edition of TraCR Advances, the newsletter where we share the latest updates from TraCR, our USDOT-funded National Center for Transportation Cybersecurity and Resiliency.

As always, TraCR's focus is on empowering our researchers to advance their groundbreaking work, delivering specialized training and outreach, and building strong connections that enrich our community and propel us toward our ambitious goals. This quarter has been marked by significant progress toward all these goals as we continue to drive innovation in transportation cybersecurity.

A highlight of the past quarter was the inaugural TraCR Conference at Clemson University. This two-day event showcased cutting-edge projects from our undergraduate, graduate, and postdoctoral researchers, and it fostered meaningful exchanges within the transportation and cybersecurity community. The conference set the stage for future breakthroughs in transportation cybersecurity. I extend my heartfelt thanks to the dedicated staff and students at Clemson University, who played a crucial role in making this event a resounding success. I am also deeply grateful to our advisory board members who participated. Your insights and support are invaluable as we work to position TraCR as a globally recognized innovation center for transportation cybersecurity.

This summer, we intensified our efforts to promote cybersecurity education through various outreach initiatives. At the Habitat Tech Fair, our team inspired young students and informed their parents about the plentiful career opportunities in cybersecurity and cyber resilience technology. We also hosted two cybersecurity workshops for middle and high school students, offering hands-on experiences in hardware and software security and data privacy protection. Additionally, we led sessions at the Benedict College Summer Transportation Institute and the Cybersecurity and E-Sport Summer Camp, where students were introduced to quantum computing and its future role in cybersecurity. These initiatives aimed to empower students to pursue careers in this rapidly growing field.

In August, we played a leading role at the USDOT Future of Transportation Summit 2024, showcasing our research and building on the momentum we have established at TraCR. The summit brought together participants from the USDOT-funded UTCs; the cutting-edge research I saw presented there reinforced my confidence that the future of transportation is bright. Together, as a transportation research community, we are poised to reach even greater heights.

Thank you for your continued dedication and commitment to our shared vision.

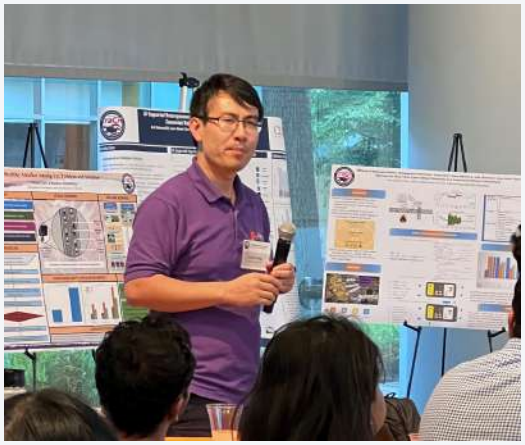
In this Issue:

Annual CONFERENCE

TraCR proudly hosted its inaugural annual conference on May 6-7, 2024, at the Clemson University International Center for Automotive Research (CU-ICAR) campus in Greenville, South Carolina. These gatherings are aimed at fostering collaboration and innovation among leaders in transportation cybersecurity research. The conference brought together a group of researchers, scholars, and professionals from Clemson and its partner institutions, including Benedict College, Florida International University, Morgan State University, Purdue University, South Carolina State University, the University of Alabama at Tuscaloosa, the University of California, Santa Cruz and the University of Texas at Dallas.

Over the course of two days, attendees showcased their latest research findings, presented innovative technologies, and discussed cutting-edge solutions to protect future transportation systems from the ever-growing threat of cyberattacks. The presentations underscored the critical importance of collaborative efforts in tackling the multifaceted challenges confronting our transportation infrastructure today and tomorrow. Industry leaders and government representatives also attended, and their contributions added depth and perspective to the discussions.

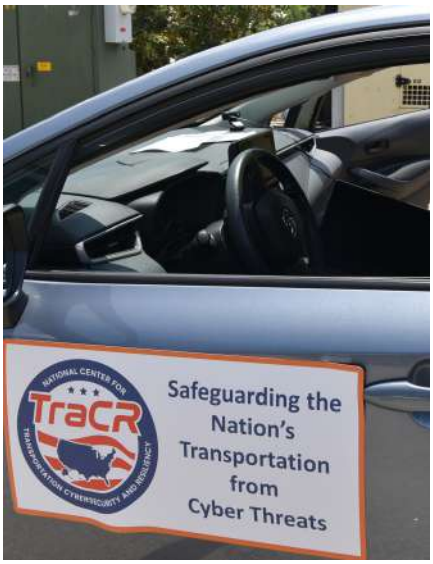
Annual CONFERENCE



One of the standout moments of the conference was the keynote address delivered by Dr. Kerry Buckley, Vice President of the Center for Integrated Transportation at the MITRE Corp. Her speech, which centered on the theme of "Building a Resilient Transportation Ecosystem," provided insights into the strategic approaches necessary for fortifying our transportation networks against emerging cybersecurity threats. In addition to the keynote, the conference program was rich and varied, featuring a range of activities including technical presentations, poster sessions, and panel discussions. These sessions explored the latest advances in transportation cybersecurity research and facilitated the exchange of ideas among attendees.

Annual CONFERENCE

TECHNOLOGY DEMONSTRATIONS



The annual conference also featured technology demonstrations led by Clemson students and researchers who are involved in both TraCR and the Center for Connected Multimodal Mobility (C2M2), a TIER 1 UTC headquartered at Clemson. The conference also included an exclusive tour of the Clemson University International Center for Automotive Research (CU-ICAR) campus. This offered cutting edge laboratories, which included autonomous vehicle development and testing facilities and advanced driving simulators.

Overall, the inaugural TraCR annual conference served as a dynamic platform for knowledge exchange, collaboration, and the forging of new partnerships. It laid a foundation for future conferences and reaffirmed the commitment of TraCR and its consortium partners to advancing transportation cybersecurity research.

Annual CONFERENCE

STUDENT POSTER AWARDS

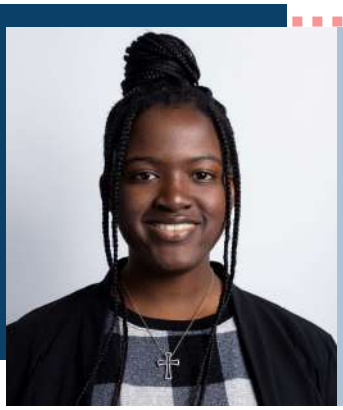
The TraCR conference included poster sessions where 24 student posters from the nine partner institutions were presented. These sessions provided a platform for the next generation of transportation researchers to showcase their research and foster academic exchange and collaboration. Members of the TraCR advisory board judged the posters, with awards given to the top three presenters.

FIRST PLACE WINNER

Eric Vin
University of California, Santa Cruz,
"Scenic: A Language for Scenario Specification and Data Generation."

SECOND PLACE

Sagar Dasgupta
University of Alabama, Tuscaloosa,
"Experimental Validation of Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles."



THIRD PLACE

Ostonya Thomas
Clemson University,
"Transportation Cybersecurity Vulnerabilities, Failures, and Improvement Strategies."

Future of Transportation SUMMIT

The U.S. Department of Transportation (USDOT) hosted the inaugural Future of Transportation (FoT) Summit at its headquarters in Washington, D.C. from August 13-15, 2024. The event was focused on the transformative research in mobility, safety, infrastructure, sustainability, and cybersecurity that is being conducted at the University Transportation Centers, with funding from the FAST Act and the Bipartisan Infrastructure Law.

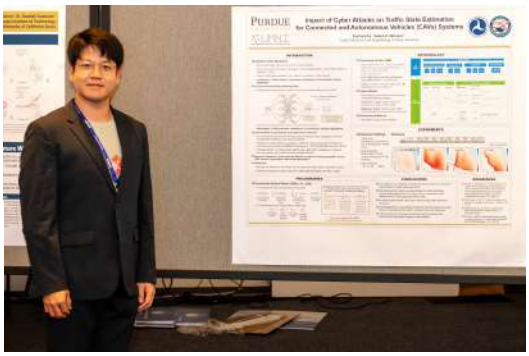
Over 500 attendees, including researchers, congressional staff, federal and state agency personnel, and stakeholders from industry, nonprofits, and community organizations attended the conference, which was held at the headquarters of the USDOT in the Navy Yard neighborhood in Washington, D.C. The summit featured three days of technical presentations by UTC researchers as well as panels of stakeholders such as USDOT administrators, representatives of nonprofit organizations, and industry leaders. The summit also included a keynote presentation by Robert C. Hampshire, USDOT Principal Deputy Assistant Secretary for Research and Technology and Chief Science Officer, who highlighted the summit as pivotal in bringing together research, development, and technology to redefine the boundaries of transportation.

Future of Transportation SUMMIT

The event also included over 100 research posters and an afternoon of live multimodal transportation technology demonstrations from nearly two dozen UTC research teams. These highlighted advances in autonomous vehicles, drones, robots, work zone safety technology, flood monitoring, cybersecurity, and innovative bridge materials.

TraCR and C2M2 had a robust presence at the event. Dr. Ronnie Chowdhury, TraCR Director, spoke on Cybersecurity and Resiliency of Transportation Systems and Infrastructure, and he also moderated the cybersecurity session. Other TraCR leadership team members also presented, including Dr. Bhavani Thairaisgham from UT Dallas, who spoke on Trustworthy Artificial Intelligence for Securing Transportation Systems; Dr. Alvaro Cardenas from UC Santa Cruz, whose presentation focused on Building Blocks for Connected and Autonomous Transportation Cybersecurity; and Ms. Trayce Hockstad from University of Alabama at Tuscaloosa, whose talk covered Resolving Legislative Gaps in Transportation Cybersecurity.

Future of Transportation SUMMIT



In addition to the talks, TraCR contributed to both indoor and outdoor demonstrations as well as the poster sessions.

Demonstrations:

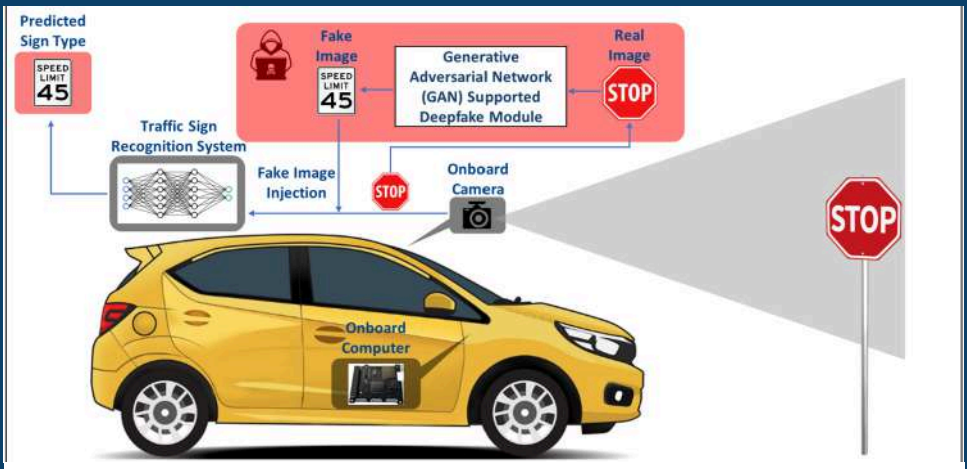
- Securing GNSS-Based Autonomous Vehicle Navigation
- Real-time Collision Warning Application Using V2V and V2I Communication
- Vision-Based Pedestrian Safety Alert System
- Low-Cost Flood Monitoring for Bridges
- Silent Threats Posted by Hardware Trojans and Their Detection
- Quantum Supremacy
- Hardware Security Attacks and Detection

Posters:

- Performance Degradation Prediction and Channel Switching in a Vehicular Network Under Harsh Weather, *Jian Liu*
- Impact of Cyber Attacks on Traffic State Estimation for Connected and Autonomous Vehicles Systems, *Eunhon Ko*
- Adversarial Booking Attacks for Autonomous On-Demand Mobility Services, *Zengxiong Lei*

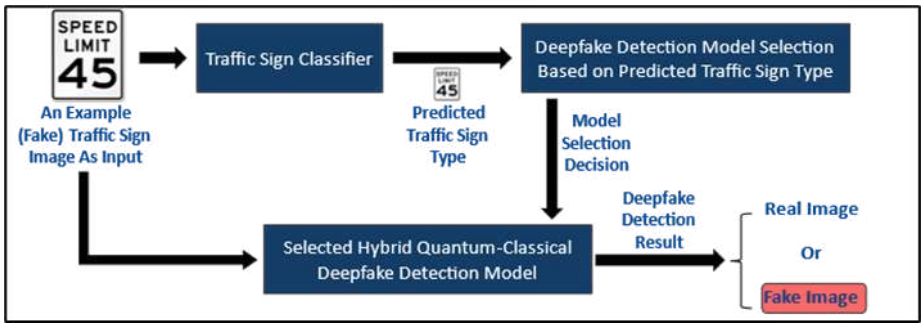
Deepfake Risks and Quantum Detection Methods for Autonomous Vehicle Security

M Sabbir Salek, Shaozhi Li, Mashrur Chowdhury



Deepfake Attack on Autonomous Vehicles

The perception module in autonomous vehicles (AVs) relies heavily on deep learning models to detect and identify various objects in their surrounding environment. An AV traffic sign classification system is integral to this module, enabling AVs to recognize roadway traffic signs. However, deepfake technology can be exploited to perform an attack on an AV traffic sign classification system, where a deepfake-generated fake traffic sign image replaces a real-world traffic sign image. This attack is performed before a a traffic sign image captured by an onboard camera is processed by the AV's traffic sign classification system, resulting in misclassification. In this study, we explored how a generative adversarial network (GAN)-enabled deepfake attack can be designed to deceive AV traffic sign classification systems. We developed a Wasserstein GAN-based deepfake attack model capable of generating fake traffic sign images that closely resemble real-world traffic sign images. The GAN-enabled attack model employs an optimization-based deterministic process to decide the type of fake traffic sign image the generator should create, ensuring the fake traffic sign image differs as much as possible (quantified using a pixel-by-pixel comparison) from the corresponding real traffic sign image.



Deepfake Detection Strategy

To counter such deepfake attacks on AV traffic sign classification systems, we developed a deepfake traffic sign image detection strategy using hybrid quantum-classical neural networks (NNs). This hybrid approach employs amplitude encoding to represent the features of an input traffic sign image as quantum states, significantly reducing the memory requirements compared to that of classical methods. We evaluated this hybrid deepfake detection strategy alongside several baseline classical convolutional NNs (CNNs) using real-world and deepfake traffic sign images. Our analyses indicate that the hybrid quantum-classical NNs can achieve similar or superior performance compared to baseline classical CNN-based deepfake detection methods in most cases while using less than one-third of the memory required by the shallowest classical CNN considered in this study.

Click Here to View the Full Paper

Trustworthy Artificial Intelligence for Securing Transportation Systems

Latifur Khan, Sadaf Md. Halim, Amin Birashk, Bhavani Thuraisingham

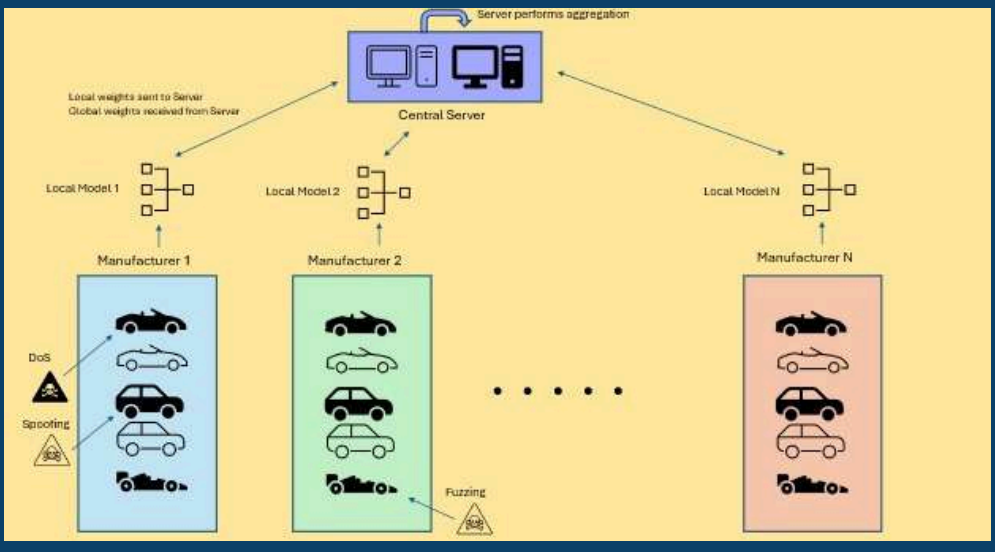
Security, privacy, and fairness are major concerns when applying Artificial Intelligence (AI), particularly when dealing with sensitive domains such as identifying individuals, handling medical records and financial applications, and even in transportation systems. The conventional centralized approach to training AI, such as Machine Learning (ML) models, where data from multiple sources is pooled into a central server, raises several security and privacy risks. For instance, data for AI needs to be shared among multiple manufacturers of transportation systems, including autonomous vehicles, so that they are all present in one location. However, this raises privacy concerns, for example, because of potential data breaches of centralized storage. As part of our cutting-edge research in applying "trustworthy AI" for transportation systems, we are developing novel ML models that are distributed so that each manufacturer or organization has control of their data. This will ensure security, privacy, and fairness, while at the same time, the system will selectively share the data with others as needed. This approach has come to be known as Federated Learning (FL).

FL is designed to tackle various privacy and security challenges by training models across decentralized devices or servers without sharing raw data. The model is trained locally on individual devices, and only the model updates (gradients or weights), rather than the data itself, are sent to a central server. Then the weights of the local models together are used to build a global model.

FL systems face their own challenges. One of the biggest complexities relates to non-independent and identically distributed (non-IID)data. This arises because different data sources typically have different data distributions, so when individual models built on top of different data distributions are combined, the resulting model often does not show strong performance. Addressing this challenge is an essential area of research in FL. The goal is to build a global model that is robust to changes and differences in data distributions, and that also shows strong performance and accuracy overall. The following figure shows an FL learning system that we have developed. It builds a global federated model to detect cyber attacks in transportation data while at the same time ensuring data privacy.

Our groundbreaking technique is called Federated Augmented Synthetic Training for Smart Vehicles (FAST-SV). It addresses the heterogeneity in the federated setting for vehicle/car security data. Specifically, we assume that different car manufacturers experience different types of attacks on their vehicles and would thus reasonably have very different attack data distributions. To counter this, we developed an approach that involves creating fully synthetic car attack data derived from the real data via augmentation techniques. Then we share a small volume of such synthetic data across manufacturers. Our experiments show that our approach is very successful at tackling the heterogeneity in attack distribution data across different car manufacturers. We performed experiments on publicly available vehicular data as well as an in-house dataset and observed results that provided high accuracy and performance. Furthermore, we experimented with adding noise to the synthetic data as an additional privacy measure and showed that accuracy and performance remains robust. This is one of the pioneering efforts that not only provides security with respect to detecting various types of attacks but also ensures the privacy of the data.

Research SPOTLIGHT



Federated Augmented Synthetic Training for Smart Vehicles (FAST-SV) Architecture

We developed another approach for addressing non-IID data inspired by advances in optimization. Utilizing metaheuristic optimization techniques is central to our solution. We propose that the global model in FL systems is often trapped in local optima when optimizing over non-IID data. To encourage the model to explore more of the optimization space, we rely on the concepts of exploration (searching the entire solution space) and exploitation (focusing on areas around the current solution). Essentially, we add randomness to the optimization process in a systematic manner to encourage the model to find more promising areas in the solution space. We call this model FedEvo. Experiments show that FedEvo is able to significantly outperform baselines, while converging to a viable solution faster.

The following table shows the results of applying FedEvo to a popular smart vehicle security dataset called the Car-Hacking Dataset. We observed similar results across a range of datasets with different types of data, and we partitioned the data across clients in highly heterogeneous ways. Thus, we successfully showed that adding guided exploration to the optimization process leads the system toward better solutions for the final global model.

	FedAvg	FedProx	Scaffold	FedDC	FedEvo
Accuracy	0.78	0.62	0.62	0.78	0.99
Macro Avg	0.72	0.50	0.50	0.73	0.99

Performance of FedEvo compared to popular baselines on the Car-Hacking Dataset

The challenges we are faced with don't only involve ensuring the security and privacy of transportation systems, but also involve guaranteeing the fairness of the AI models, such as not showing bias when giving speeding tickets. Our AI techniques also have to be safe and recover from faults, malicious or otherwise. How can the transportation system continue operating safely even when some of its major components have failed? We are looking forward to providing solutions to such complex problems under TraCR.

Click Here to View the Full Paper

Upcoming EVENT & WEBINAR

Transportation Research Board 2025 Annual Meeting

The Transportation Research Board (TRB) will host its annual meeting on January 5-9, 2025 in Washington, DC. The TRB is a division of the National Academy of Sciences, Engineering, and Medicine, and its mission is to leverage expertise, experience, and knowledge to anticipate and address complex transportation challenges. TRB's Annual Meeting attracts thousands of transportation professionals from around the world. The program covers all transportation modes and features sessions and workshops on topics relevant to policymakers, administrators, practitioners, and researchers, with representatives from government, industry, and academia. Members of TraCR are excited to participate and contribute to the 2025 conference, bringing their expertise and insights to this gathering.

Find more information and register here!

Upcoming WEBINAR

TOWARDS COMPOSITIONAL SECURE AUTONOMY: FROM PERCEPTION TO CONTROL

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

OCTOBER 4TH, 2:00 PM (ET)

Find more information and register here!

Recorderd WEBINARS

CYBER RESILIENT GNSS-BASED NAVIGATION FOR AUTONOMOUS GROUND VEHICLES UNDER THREAT UNCERTAINTIES AND CONTESTED URBAN ENVIRONMENTS

Dr. Mizanur Rahman
Assistant Professor, Department of Civil, Construction, & Environmental Engineering,
Director, Connected and Automated Mobility Laboratory (CAM Lab),
The University of Alabama, Tuscaloosa

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

The TraCR Request for Proposals (RFP) is out

TraCR recently released its second request for proposals (RFP) that solicits research projects for the 2024-2025 year. Applications will be competitively selected for funding. All proposals for the 2024-2025 funding cycle should focus on TraCR's core mission statement: **To Pioneer the Advancement of Cybersecurity and Resilience, Ensuring Robust Protection for Transportation Systems and Infrastructure Against Both Current and Emerging Threats.** One focus of this RFP is to encourage proposals that feature collaborations across multiple partner institutions. All projects should also contain a technology transfer plan so that they can lead to real-world impacts.

Proposals should be submitted by 11:59 pm on Monday, October 7th, 2024, to tracr@clemson.edu.

Find more information here!

Recognition

Dr. Bhavani Thuraisingham, Associate Director of TraCR and a pioneering professor at UT Dallas, has shared her remarkable academic journey in a new book celebrating women in computer science. The book, *Rendering History: The Women of ACM-W*, highlights her experiences from growing up in Sri Lanka's minority Tamil community to becoming a leading figure in cybersecurity. Despite challenges, she achieved significant academic and professional success, balancing her career with family life. Dr. Thuraisingham continues to inspire and mentor women in the field, and is a much-esteemed partner of TraCR.

Click for more information on the article

OUTREACH

City of Greenville Summer Camp

On July 12, 2024, Dr. Chowdhury gave a talk to the the City of Greenville summer camp's students called on “STEM: the Path to Exciting Careers in New Frontiers.” He encouraged the students to explore careers in science, technology, engineering, and math, showing them how these fields offer exciting opportunities. The TraCR students also ran a fun and interactive workshop on cybersecurity, where they taught the campers about real-world threats and the importance of securing digital information, making the session both educational and interactive.

CONTACTS

That's It for Now!

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