NATIONAL CENTER FOR TRANSPORTATION CYBERSECURITY AND RESILIENCY
A USDOT National Transportation Center

Project Title:	Hybrid classical-quantum AI approach for detecting cyberattacks in vehicles
PI Name and Contact:	Shaozhi Li Postdoc Clemson University Phone: 8658982068 Email: shaozhl@g.clemson.edu
Submission Date:	January 31, 2025
Version:	1.0
Project Performance Period	January 1, 2024 – May 31, 2025

Project Summary

In self-driving vehicles, deep learning methods have been applied for object detection. Enhancing both the accuracy and efficiency of these methods is crucial to ensuring their safety. With advancements in quantum technologies, quantum supremacy has been demonstrated in machine learning. Here, we report that a hybrid quantum-classical convolutional neural network can be trained faster for image classification compared to a classical convolutional neural network. This improved performance originates from the quantum activation function, which can be integrated into classical neural networks to enhance the efficiency of image recognition systems. Additionally, we develop a quantum-inspired weight-constrained neural network, which reduces the number of variables by a factor of 135 compared to classical neural networks. This finding is essential for minimizing the complexity of artificial intelligence models used in vehicle image recognition. Based on this weight-constrained neural network, we develop a novel defense system to enhance the resilience of image identification in self-driving vehicles. Beyond supervised learning, we developed the Quantum Natural Policy Gradient (QNPG) algorithm, which achieves improved sample complexity of $O(\epsilon^{-1.5})$, surpassing the classical lower bound of $O(\epsilon^{-2})$. Additionally, we formulate the Vehicle Routing Problem with Arc Interdiction as a quantum unconstrained binary optimization (QUBO) problem and demonstrate its solution using D-Wave quantum annealers, showing near-optimal performance on small instances. Collectively, these results highlight the potential of quantum methods to reduce computational complexity, accelerate training, and enhance system resilience, thereby paving the way for safer and more efficient autonomous transportation systems.

1. Data Description

Reports and data produced as part of this project are expected to include, but are not limited to, websites, publications, and archival-quality data curated from various sources. These reports will include technical documents with detailed figures such as tables, graphs, and scripts essential for analyzing and interpreting the data. The project will generate data by training different machine learning models.

2. Data format and metadata standards

Detailed data will be documented corresponding to each metadata set available in at least one of the following formats: XML, CSV, plain text, PDF, HTML, MS Word, or LaTeX. The generated data can be accessed from our published papers.

3. Access Policies

Access to, sharing, and distributing of documentation will be via web sites and publishing and presenting in conferences, journals, and monographs. The data will be shared via the TraCR website and USDOT Repository & Open Science Access Portal enabling the research community to access and reproduce research activities. The Principal Investigator (PI) will coordinate with the UA Associate Director as well as TraCR's Director, Associate Directors and staff to oversee data management.

4. Policies and Provisions for Re-use, Redistribution, derivatives

The author(s) and the researcher(s) reserve all rights of intellectual property. All sensitive personal information will be removed from the datasets before they are shared to avoid any ethical issues. Should any third-party data used, proper attribution will be provided, and licensing requirements will be strictly adhered to.

5. Plans for Archiving and Preservation of Access and Data Integrity

Data of long-term value includes simulating results and programming scripts. The long-term strategy for maintaining, curating, and archiving the data is to seek support from Dropbox.

6. Change Log

Version	Date	Description
1.0	February 10, 2025	Initial submission of the Data Management Plan.