Impersonation Attack using Quantum Shor's Algorithm against Blockchain-based Vehicular Ad-hoc Network [Link to Preprint]

Kazi Hassan Shakib, Mizanur Rahman, Mhafuzul Islam, and Mashrur Chowdhury

(Accepted for publication in the IEEE Transactions on Intelligent Transportation Systems)

Abstract: Blockchain-based Vehicular Ad-hoc Network (VANET) is widely considered a secure communication architecture for a connected transportation system. With the advent of quantum computing, there are concerns regarding the vulnerability of this architecture against quantum algorithm-based attacks. In this study, a potential threat is investigated in a blockchain-based VANET with an impersonation attack using quantum Shor's algorithm. Specifically, the impersonation attack using Shor's algorithm is created by compromising the Rivest-Shamir-Adleman (RSA) encrypted digital signatures of VANET, and thus a threat to the trust-based blockchain scheme of VANET is successfully established. We implemented an integrated simulation platform combining OMNET++, vehicles-in-network simulation (VEINS), and simulation of urban mobility (SUMO) traffic simulator. In addition, we incorporated vehicle-to-everything (V2X) communication in OMNET++ using the extended INET library. An impersonation attack on a blockchain-based VANET is implemented using IBM Qiskit, which is an open-source quantum software development kit. The findings reveal that an impersonation attack is feasible on the Blockchain-based VANET, which compromises the trust chain of a blockchain-based VANET. This research highlights the need for a quantum-secured blockchain for VANET.

Quantum-Inspired Weight-Constrained Neural Network: Reducing Variable Numbers by 100x Compared to Standard Neural Networks [Link to Preprint]

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

(Under review with the Proceedings of the National Academy of Sciences)

Abstract: Although quantum machine learning has shown great promise, the practical application of quantum computers remains constrained in the noisy intermediate-scale quantum era. To take advantage of quantum machine learning, we investigate the underlying mathematical principles of these quantum models and adapt them to classical machine learning frameworks. Specifically, we develop a classical weight-constrained neural network that generates weights based on quantum-inspired insights. We find that this approach can reduce the number of variables in a classical neural network by a factor of 135 while preserving its learnability. In addition, we develop a dropout method to enhance the robustness of quantum machine learning models, which are highly susceptible to adversarial attacks. This technique can also be applied to improve the adversarial resilience of the classical weight-constrained neural network, which is essential for industry applications, such as self-driving vehicles. Our work offers a novel approach to reduce the complexity of large classical neural networks, addressing a critical challenge in machine learning.

A Secure Object Detection Technique for Intelligent Transportation Systems [Link to Full Published Paper]

Md Jueal Mia and M. Hadi Amini

(Published in the IEEE Open Journal of Intelligent Transportation Systems, Volume 5)

Abstract: Federated Learning is a decentralized machine learning technique that creates a global model by aggregating local models from multiple edge devices without a need to access the local data. However, due to the distributed nature of federated learning, there is a larger attack surface, making cyber-attack detection and defense challenging. Although prior works developed various defense strategies to address security issues in federated learning settings, most approaches fail to mitigate cyber-attacks due to the diverse characteristics of the attack, edge devices, and data distribution. To address this issue, this paper develops a hybrid privacy-preserving algorithm to safeguard federated learning methods against malicious attacks in Intelligent Transportation Systems, considering object detection as a downstream machine learning task. This algorithm involves the edge devices (e.g., autonomous vehicles) and roadside units to collaboratively train their model while maintaining the privacy of their respective data. Furthermore, this hybrid algorithm provides robust security against data poisoning-based model replacement and inference attacks throughout the training phase. We evaluated our model using the CIFAR10 and LISA traffic light dataset, demonstrating its ability to mitigate malicious attacks with minimal impact on the performance of main tasks.

FLID: Intrusion Attack and Defense Mechanism for Federated Learning Empowered Connected Autonomous Vehicles (CAVs) Application [Link to Publication]

Md Zarif Hossain, Ahmed Imteaj, Saika Zaman, Abdur R. Shahid, Sajedul Talukder, and M. Hadi Amini

(Published in the 2023 IEEE Conference on Dependable and Secure Computing (DSC))

Abstract: Connected autonomous vehicles (CAVs) are transforming the transportation business by incorporating advanced technology such as sensors, communication systems, and artificial intelligence. However, the interconnectedness and complexity of CAVs pose security vulnerabilities, making them possible targets for assaults. Intrusion detection is critical in protecting CAVs from harmful actions. This research investigates the use of federated learning, a privacy-preserving machine learning approach, for intrusion detection in CAVs. Federated Learning (FL) can improve the detection capabilities and robustness of intrusion detection systems in the CAV ecosystem by using the collective capacity of various CAVs while protecting data privacy. This paper provides an in-depth analysis of tailoring FL for collaborative intrusion detection in CAVs, as well as prospective future research areas in this domain. The findings of this study contribute to the advancement of secure and dependable CAV systems, opening the path for the widespread use of connected autonomous vehicles in the transportation industry. All code, data, and experiments are accessible on our Github repository.

Fast Attack Recovery for Stochastic Cyber-Physical Systems [Link to Publication]

Lin Zhang, Luis Burbano, Xin Chen, Alvaro A. Cardenas, Steven Drager, and Matthew Anderson

(Published in the 2024 IEEE 30th Real-Time and Embedded Technology and Applications Symposium (RTAS))

Abstract: Cyber-physical systems tightly integrate computational resources with physical processes through sensing and actuating, widely penetrating various safety-critical domains, such as autonomous driving, medical monitoring, and industrial control. Unfortunately, they are susceptible to assorted attacks that can result in injuries or physical damage soon after the system is compromised. Consequently, we require mechanisms that swiftly recover their physical states, redirecting a compromised system to desired states to mitigate hazardous situations that can result from attacks. However, existing recovery studies have overlooked stochastic uncertainties that can be unbounded, making a recovery infeasible or invalidating safety and real-time guarantees. This paper presents a novel recovery approach that achieves the highest probability of steering the physical states of systems with stochastic uncertainties to a target set rapidly or within a given time. Further, we prove that our method is sound, complete, fast, and has low computational complexity if the target set can be expressed as a strip. Finally, we demonstrate the practicality of our solution through the implementation in multiple use cases encompassing both linear and nonlinear dynamics, including robotic vehicles, drones, and vehicles in high-fidelity simulators.

On the Adversarial Robustness of Camera-based 3D Object Detection [Link to Publication]

Shaoyuan Xie, Zichao Li, Zeyu Wang, and Cihang Xie

(Published in the Transactions on Machine Learning Research)

Abstract: In recent years, camera-based 3D object detection has gained widespread attention for its ability to achieve high performance with low computational cost. However, the robustness of these methods to adversarial attacks has not been thoroughly examined, especially when considering their deployment in safety-critical domains like autonomous driving. In this study, we conduct the first comprehensive investigation of the robustness of leading camera-based 3D object detection approaches under various adversarial conditions. We systematically analyze the resilience of these models under two attack settings: white-box and black-box; focusing on two primary objectives: classification and localization. Additionally, we delve into two types of adversarial attack techniques: pixel-based and patch-based. Our experiments yield four interesting findings: (a) bird's-eye-view-based representations exhibit stronger robustness against localization attacks; (b) depth-estimation-free approaches have the potential to show stronger robustness; (c) accurate depth estimation effectively improves robustness for depth-estimation-based methods; (d) incorporating multi-frame benign inputs can effectively mitigate adversarial attacks. We hope our findings can steer the development of future camera-based object detection models with enhanced adversarial robustness. The code is available at: https://github.com/Daniel-xsy/BEV-Attack.