Integrating Machine Learning for Enhanced Security in Autonomous Driving and In-Vehicle Networks of Connected and Autonomous Vehicles

Shibly Kabid Hassan
Laboratory for Cyber Resilience
Prof. Youki Kadobayashi

Abstract

The emergence of Connected and Autonomous Vehicles (CAVs) heralds a transformative epoch in vehicular transportation, characterized by unprecedented advancements in operational efficiency and experiential enhancements. This technological ascendance, however, concurrently ushers in a plethora of formidable challenges in cybersecurity. Foremost among these are the exigencies of assuring impenetrable security in autonomous driving models and the intricate labyrinth of in-vehicle network systems, amidst an escalating milieu of sophisticated cyber threats and latent systemic vulnerabilities. This dissertation is an endeavor to confront these multifarious security conundrums by orchestrating an integration of cutting-edge machine learning paradigms, with the objective of reinforcing the security apparatus within CAVs. The research encapsulates a holistic and intricately layered strategy, with a precise focus on the autonomous driving algorithms and the Controller Area Network (CAN) bus, while simultaneously extending its purview to the overarching in-vehicle network infrastructures. In its initial exposition, the study discloses a pioneering machine learning-based defensive schema for autonomous driving models. This schema, which integrates an autoencoder with a compressive memory module, is assiduously engineered to maintain the integrity of authentic image features, thereby circumventing potential aberrations in model generalizations and adeptly attenuating the repercussions of adversarial inputs. The validation of this innovative solution is undertaken through an extensive regimen of testing, employing formidable adversarial attack vectors such as the Fast Gradient Sign Method (FGSM) and Advanced Generative Adversarial Networks (AdvGAN), in tandem with the Nvidia Dave-2 Driving model. The empirical results from this testing campaign unequivocally affirm the preeminence of this defense mechanism, which markedly eclipses existing defense stratagems, recording an exceptional defense success rate in both Whitebox and Blackbox experimental paradigms. The subsequent discourse of the dissertation transitions to the enhancement of security within the CAN bus system, an indispensable communication nexus within CAVs. Herein, the dissertation propounds a trailblazing Personalized Federated Learning-based Intrusion Detection System, ingeniously conceived to pinpoint CAN bus attacks with unparalleled precision, whilst obviating the necessity for data sharing. This system, leveraging both Supervised and Unsupervised Federated Learning modalities, accomplishes a prodigious accuracy, heralding a seminal advancement in the fortification of the CAN bus system. Further augmenting the breadth of this study is the focus on the broader in-vehicle network infrastructure, particularly emphasizing the imperative for robust and resilient communication protocols, as epitomized by Automotive Ethernet. To surmount the intricate challenges endemic to intrusion detection within this network, the dissertation champions a semi-supervised learning approach. This approach, through its meticulous engineering, adeptly segregates salient features from extraneous noise, thereby substantially enhancing the algorithm's acumen in identifying attack activities. This approach has demonstrated formidable detection efficacy, achieving elevated detection rates across a diverse array of attack typologies.

In summation, this dissertation epitomizes a seamless and meticulous integration of machine learning techniques, adeptly tailored to confront and surmount the diverse security challenges inherent in autonomous driving models and in-vehicle networks of CAVs. Through an array of radical methodologies and stringent empirical experimentation, the research not only significantly amplifies the security paradigm of CAVs but also imparts a profound and indelible contribution to the discipline. This scholarly endeavor paves the pathway towards the inception of safer and more dependable autonomous vehicle technologies, thereby sculpting the future trajectory of intelligent transportation systems.