論文内容の要旨

博士論文題目　Integrating Machine Learning for Enhanced In-Vehicle Security of Connected and Autonomous Vehicles

氏　名　Kabid Hassan Shibly

（論文内容の要旨）

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 in-vehicle security of the Connected and Autonomous Vehicles which includes autonomous driving algorithms and the In-Vehicle networks, 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 under- taken 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 pin-point 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.

氏　名	Kabid Hassan Shibly

（論文審査結果の要旨）

技術革新の到来は、特に交通分野において、Connected and Autonomous Vehicles（CAVs）の画期的な発展をもたらし、交通のパラダイムを大きく変革した。本論文では、自動運転システムの深層学習アルゴリズムおよび車載ネットワークの制御プロトコルにおいて生じる課題と潜在的な脆弱性を入念に分析している。シミュレータとデータセットを用いた効果検証を通じて、CAVs の認識と制御にまたがるセキュリティフレームワークを強化し、より安全で回復力のある交通システムの開発に貢献することを目指している。本論文の主な成果は、以下に要約される。

1. 認識系におけるセキュリティ対策として、自動運転システムにおける敵対的脅威を軽減するための戦略を検討し、様々なタイプの敵対的攻撃を検討し、Nvidia DAVE-2 自動運転モデルを用いて防御手法の精度評価を行い、オートエンコーダーに記憶モジュールを導入することで先行研究と比較して精度の高い防御手法を提案している。

2. 制御系におけるセキュリティ対策として、CANbus における連合学習を用いた侵入検知アルゴリズム、ならびに Automotive Ethernet 車載ネットワークにおける半教師あり学習を用いた侵入検知アルゴリズムを提案し、研究用データセットを用いた精度評価を行い、いずれも高い精度を確認している。

以上のように、本論文はコネクテッドカーおよび自動運転車のセキュリティ向上に資する理論的分析および実証的分析を実施し、研究用データセットならびに自動運転モデルを用いた防御精度の向上を示すことでその有効性を検証している。それぞれの成果は1編の学術論文と3編の査読付き国際会議論文として発表されており、研究成果の有効性を見ることができる。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。