論 文 内 容 の 要 旨

博士論文題目　Studies on Deep Learning-based Intrusion Detection Systems for Computer & In-vehicle CAN Bus Networks

氏　　名　Md Delwar Hossain

（論文内容の要旨）

The rapid growth of the Internet of Things (IoT) and the ubiquitous nature of the Internet have made life more convenient for human beings. The rise of that social convenience is accompanied by incessant efforts of miscreants to create new tools, techniques, and tactics to destabilize the comfort of the dwellers by attacking computer networks and applications. Even worse, these attacks are being transferred into the increasingly connected cyber-physical systems (CPS), especially the automotive system where the in-vehicle CAN bus network lacks encryption and authentication mechanisms, making them even more vulnerable to some of the attacks that are well-known in traditional computer networks. Addition- ally, some automotive systems (e.g., the modern car) employ advanced technologies –the Telematics Unit, in-vehicle infotainment (IVI), V2X, etc.—accessible through Bluetooth, Wi-Fi, GPS, etc., thus, augmenting their attack surface. Intrusion Detection Systems are known to be the solution by excellence for detecting and mitigating network attacks, however, based on the recrudescence of attacks, we can affirm that traditional IDSs have failed. Elsewhere, artificial intelligence (AI) or, more specifically, deep learning has shown immense promise in solving lingering issues in other domains: we contend that deep learning can also help make IDSs more efficient.

Hence, in this dissertation, our imperative is to devise new IDS methodologies to protect computer networks and in-vehicle CAN bus networks of automotive systems by leveraging deep learning. First, we thoroughly study the deep learning-based IDS for several kinds of critical network attacks such as DoS (Denial of Service), DDoS (Distributed DoS), Brute Force, etc. Subsequently, we investigate how to optimize the deep learning models. Our results illustrate that Long Short-Term Memory (LSTM) can effectively detect network attacks with high accuracy and reasonable detection rates. After ensuring security in computer networks by using deep learning, we also transfer our solutions to the automotive systems. Therefore, we propose a deep learning-based IDS for in-vehicle CAN bus networks. Furthermore, for efficiency reasons, we also develop CAN bus network attacks (DoS, Fuzzing, and Spoofing) datasets by using the CAN messages of three distinct car models (Toyota, Subaru, and Suzuki). The results of our experiment demonstrate that our deep learning-based IDS is more effective and robust than existing methodologies.

氏　名	Md Delwar Hossain

（論文審査結果の要旨）

本研究では、コンピュータネットワークや車載 CAN バスネットワークに有効な深層学習ベースの侵入検知システムを開発することを第一の目的としている。本研究ではまず、いくつかの重要なネットワーク型攻撃を徹底的に調査し、LSTM ベースの深層学習モデルを用いて検知実験を行っている。その結果、いくつかの致命的なネットワーク型攻撃の検知において、提案モデルにより性能改善を達成している。また既知のネットワーク型攻撃が、セキュリティメカニズムの欠如により、車載 CAN バスネットワークに転移していることを指摘し、自動車のサイバー攻撃検知に関する標準的な解決策が存在しないため、安全運転を阻害する可能性について問題提起を行っている。本研究では、ネットワーク型検知システムの考え方を車載 CAN バスむけ IDS に応用し、高度な CAN バスネットワークへの攻撃を検知することに成功している。まず、実車から車載 CAN バス攻撃データセットを開発し、3 つの異なる車種でデータセットを拡張している。さらに、ロバストな IDS を開発するために不可欠な、効果的な前処理手法を提供している。最後に、LSTM と 1 次元 CNN の深層学習アプローチに基づいて、車載 CAN バスむけの IDS を設計・開発している。本研究が提案する効率的な IDS により、脅威を軽減し、安全運転に寄与することが期待される。

以上のように、本論文はコンピュータネットワークや車載 CAN バスネットワークのセキュリティ向上に資する異常検知方式を提案し、テストベッドでの比較実験と性能評価によって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 4 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。