論 文 内 容 の 要 旨

博士論文題目

In-Vehicle Network Attack Detection Using Deep Neural Networks Trained On Features Extracted From CAN Data

氏　名

Araya Kibrom Desta

(論文内容の要旨)

Advanced Electronic Control Units (ECU) have been included in automobiles to ensure safe and comfortable driving. ECUs are connected by a de facto automobile networking standard known as the controller area network (CAN). CAN is vulnerable to cyber attacks because it fails to secure the network by utilizing authentication, encryption, and network segmentation. The dissertation proposes an intrusion detection systems (IDS) for the CAN bus using deep learning that is trained on the CAN bus data. Four methods are experimented to secure the CAN bus. In the first two methods, the arbitration ID of the CAN frames is used to train Long Short-Term Memory Networks (LSTM) and Convolutional Neural Networks (CNN). The LSTM based IDS is trained to learn the sequence of arbitration IDs in the CAN bus. The trained model is used to predict the future sequence of arbitration IDs with wrong predictions being flagged as an attack. In such a way, LSTM-based IDS has improved the conventional IDS method that studies arbitration ID patterns. Even though LSTM managed to improve the conventional method performance in detecting spoofing the gear attack and spoofing the RPM attacks, its results are not very accurate. CNN based IDS called Rec-CNN is proposed as an improvement to the LSTM-based IDS. Images generated using recurrence plots from the CAN bus arbitration IDs are used to train the CNN architecture. Using recurrence plots helps in capturing the temporal data in the CAN bus data through images. Using these images of recurrence plots, the experiment is done on how CNNs can easily be trained to classify attack and benign sequences of arbitration ID for a secure CAN bus communication. Both the works use CAN arbitration IDs to train LSTMs and CNNs. If the arbitration ID is not affected during an attack, attacks will be left undetected. To improve this drawback, two other methods are proposed using the data section of the CAN frame. The first work, named MLIDS, trains an LSTM architecture that is capable of handling the high dimensional CAN bus data without requiring reveres-engineering of the CAN bus data. Training LSTM can be difficult in the CAN bus data as it contains millions of parameters. Our last work called U-CAN is proposed as an improvement to the MLIDS. U-CAN is trained using the hamming distance (HAMD) distribution of CAN frame bits. All the works have been tested against different sets of attacks including fuzzy attacks, drop attacks, denial of service (DoS) attacks, insertion attacks, and spoofing attacks.

氏　名	Araya Kibrom Desta

（論文審査結果の要旨）

自動車の運転や機器の制御を行うために、電子制御ユニット(Electronic Control Units: ECUs)が搭載されており、これらは事実上の標準規格である Controller Area Network (CAN)と呼ばれるバス型ネットワークによって接続されている。CAN は、認証機構、暗号化通信、ネットワークセグメンテーション機能を持たないため、サイバー攻撃に対しては、非常に脆弱である。本論文では、通常時の CAN 上に流れるデータのトラフィックパターン等を機械学習により分析することにより、CAN に対する攻撃トラフィックの侵入を検知するシステムの提案を行っている。

具体的には、4 つの手法を提案しており、最初の 2 つの方法では、CAN フレームの Arbitration ID を活用して、Long Short-Term Memory (LSTM)ネットワークと畳み込みニューラルネットワーク(Convolutional Neural Network: CNN)で学習を行う。LSTM ネットワークを利用した場合には、Arbitration ID のシーケンスを予測するが、攻撃の種類によっては、検知精度が従来研究よりも向上しないため、CAN フレームの時間を考慮した CNN による検知モデルの確立を行っている。

最初の 2 つの方法では、Arbitration ID に着目しているため、ここに変化が見られない場合は、侵入検知ができないため、CAN フレームのデータ部分に着目した方法をさらに提案している。データ部分は情報量が多いため、どの部分を学習すると効率良く検出精度が高められるかを検証し、あらゆる種類の攻撃手法に対応することができるようになっている。

これらの提案手法は、既存の研究と比較して、侵入検知率を高めることができている。また、さまざまな攻撃方法にも網羅的に対応することができており、自動車ネットワークにおける侵入検知システムをある程度確立することができたと言える。

本論文は、自動車ネットワークにおける侵入検知手法の提案、ならびに、その優位性を客観的に評価を行っていることより、一定の学術的意義があるものと評価できる。よって、論文は、博士(工学)の価値があるものと認める。