In-vehicle network attack detection using deep neural networks trained on features extracted from CAN data

Name: Araya Kibrom Desta

Laboratory's name: Internet Architecture and Systems

Supervisor's name: Kazutoshi Fujikawa

Abstract

Unlike in the past, automobiles nowadays employ a de facto networking standard known as the controller area network (CAN). CAN is vulnerable to cyber-attacks because it doesn't utilize authentication, encryption, and network segmentation. The dissertation proposes an intrusion detection system (IDS) for the CAN bus using deep learning 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. Even though LSTM managed to improve the conventional method performance in detecting 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. 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 can handle 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.