Fingerprinting Automobiles With CAN Bus Data Samples

2d Lt David R Crow

Today's vehicle manufacturers do not tend to publish proprietary controller area network (CAN) packet formats. This is a form of *security through obscurity*—it makes reverse engineering efforts more difficult for would-be intruders—but obfuscating the CAN data in this way does not adequately hide the vehicle's unique signature. Specifically, modern methods can effectively identify a vehicle's signature in a segment of its CAN data, even if this data is unprocessed or limited in scope. In machine learning, this is a multiclass classification problem which asks the following question: given a sample of CAN data, can we successfully determine which vehicle generated the sample?

This research employs two datasets, one from Oak Ridge National Laboratory (ORNL) and one from Stone et al (2018). ORNL's corpus is comprised of nearly 2.5 gigabytes of data captured on the CAN buses of nine different vehicles; Stone et al's corpus contains over 230 megabytes of data from 11 different vehicles. In this research, 1,024 bytes of sequential CAN data constitute one data sample, so formatting and partitioning the datasets gives a new dataset of nearly three hundred thousand individual samples. We label every sample with its generating vehicle to enable fully supervised learning.

We train two distinct machine learning models on this dataset. The results indicate that a standard multilayer perceptron (MLP) can effectively classify these CAN data samples. The results also indicate that a deep convolutional neural network (CNN) can classify the samples at a greater performance level than can the MLP, but both models still surpass a balanced classification accuracy of 80% on the full dataset. Clearly, one can effectively determine which vehicle generated a given sample of CAN data. This erodes consumer safety: a sophisticated attacker who establishes a presence on an unknown vehicle can use similar techniques to identify the vehicle and better format attacks.